IAIC Transactions on Sustainable Digital Innovation (ITSDI)
Vol. 1 No. 2 April 2020

p-ISSN: 2686-6285
e-ISSN: 2715-0461

Cloud Computing and its role in the Information Technology

Tanweer Alam
Faculty of Computer and Information Systems, Islamic University of Madinah
Saudi Arabia
e-mail: tanweer03@iu.edu.sa

Author Notification
22 March 2019
Final Revised
27 March 2019
Published
31 March 2019

To cite this document:
Alam, T. (2020). Cloud Computing and its role in the Information Technology. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, *1*(2), 82-93. Retrieved from https://pandawan.aptisi.or.id/index.php/att/article/view/59

Abstract

The concept of Cloud Computing has been distinguished as one of the major computing models in recent years. Cloud computing has become a great innovation that has important consequences not just for services on the internet but also for the entire Information technology (IT) market. Its emergence aims to optimize on-demand technology, hardware and information provisioning as a service, reaching the economy of scale in the distribution and operation of IT strategies. A great deal of cloud computing research has been concerned over some obstacles and challenges that rely upon behind the lure of cloud computing. Security has been always raised as one of the most critical issues of cloud computing where resolving such an issue would result in constant growth in the use and popularity of the cloud. Security requirements represent a major issue that has to be met in order of easing some of these obstacles. This article presents the role of cloud computing in the IT sectors.

Keywords: Cloud Computing; Information Technology; cloud security; challenges; service availability.

1. Introduction

The Cloud computing has now been considered as one of the best computing paradigms in the field of information technology in recent years. That happened as a result of advances in existing computing paradigms which include parallel computing, grid computing, distributed computing, and other paradigms of computing [1]. Theses technological strategy allows its consumers to introduce communication connection in a smooth manner to a system of computing resources, where users can easily scale up or down their demands with minimal engagement from third parties. This computing offers its consumers three basic service models: SaaS, PaaS, IaaS. The Software as a Service (SaaS) is mainly intended for end-users who have to use the software as part of their everyday actions [2]. The Platform as a Service (PaaS) is intended primarily for developers of applications that need platforms to build up their software or applications. The Infrastructure as a service (IaaS) is primarily intended for network architects requiring development resources. Further, each of the prior customers has their concerns about flaws in cloud computing and challenges that could prevent them from achieving their goals. Data can be stored and accessible through the cloud, where users can retrieve the information without having to know the storage location [3].

Throughout fact, users are free of the servicing and resource management costs involved with the utilization [4].

The cloud provider is responsible to maintain and manage information over the cloud storage. Securing the information is obviously one of the cloud provider's primary goals [5]. Now the information security is provided as a magnificent aspect of adapting any innovation. Although maintaining security will result in this technology's tremendous popularity, undermining it can lead to the catastrophic reality that can lead to the technology being abandoned. Standards and policies have been set in place since the early days of grid computing to conquer any threat, vulnerability that violates information securities [6]. Considering that the cloud paradigm is a distributed architecture, many concerns have been raised about its vulnerabilities, security as well as difficulties (Figure 1).

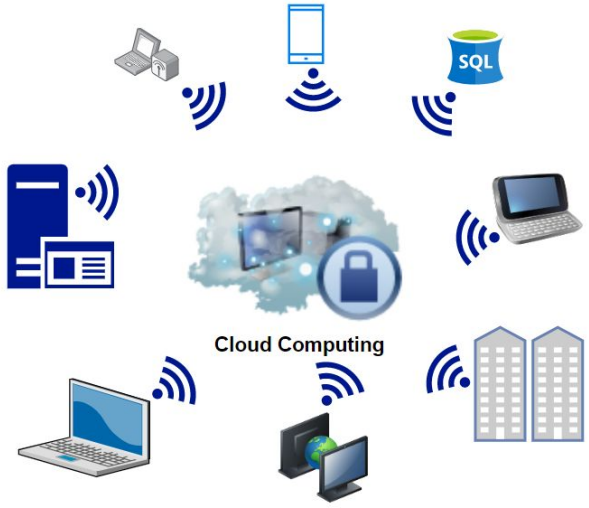

Figure 1: Cloud Computing

The Cloud does have a range of features, with the major ones becoming:

1) Virtual Infrastructure: Provides a virtualized technology platform that allows physical resources, processing, and network capabilities to have been virtual. Whatever the deployment structure, cloud technology aims to make the most of the available technology across a number of participants [7].
2) Dynamic procurement: Enables provider requirements based on current demand criteria. It is done automatically by software technological advances, allowing service capability to be expanded and contracted as required. Its dynamic scaling must be achieved while maintaining high levels of security and reliability.
3) Network Access — Allows Internet access from a wide range of devices, such as PCs, laptops and mobile devices. The cloud-based service deployments include anything from the use of business applications to the latest application on the latest smart device.
4) Controlling — Use processing to control and automate the infrastructure and provide information on monitoring and billing. Users are therefore charged for services according to how much they used during the billing cycle [7].

The rest of the paper is divided into the following sections: section 2 represents the literature survey, section 3 represents the security paradigms for cloud computing, section 4 shows the cloud security challenges, section 5 shows the discussion and section 6 represents the conclusion.

2. Literature survey

Cloud computing would have the capability over the Internet to access a pool of computing resources built and maintained by a third party. Cloud computing came because of the continued development of computer paradigms, as previously mentioned. The basis of evolving computing was developed in the 1980s with the advent of the internet. In 2008, Lizhe Wang et. Al. published a paper on recent advances in Cloud computing. They identify the concepts and characters of scientific Clouds, also they present an example of a scientific Cloud for data centers in the cloud [8].

In 2010, S Bhardwaj et. Al. published an article on cloud computing. In this article, they discussed cloud computing in the light of Infrastructure as a service (IaaS) [9].

In 2013, Fernando, N and et.al. published an article on mobile cloud computing. The authors are provided an extensive survey of mobile cloud computing research. They also highlighted the specific concerns in mobile cloud computation. They also presented a taxonomy based on the key issues and discussed the different approaches taken to tackle several challenges [10].

In 2016, A Botta, W De Donato, V Persico, A Pescapé have published an article on the Integration of cloud computing and the internet of things. They presented a framework to integrate cloud computing to the internet of things [11].

In 2019, Sasikala, P has published an article entitled “Cloud computing: present status and future implications”. In this article, the author provides the cloud computing in the present and future perspective [12].

3. Security paradigms for cloud computing

In general terms, security is a vast issue that must be dealt with from a variety of perspectives. Different parties participating have different objectives within the cloud framework [13]. Consequently, their concerns regarding threats and vulnerabilities in the cloud environment can be varying. These issues may also be eased or exacerbated depending on the delivery model being introduced.

A) Deployment models

Throughout cloud computing, multiple application models may be deployed on the service models mentioned earlier. Such specific deployment models can be used based on their nature of delivery which depends on the location of the cloud service as follows (Figure 2):

p-ISSN: 2686-6285
e-ISSN: 2715-0461

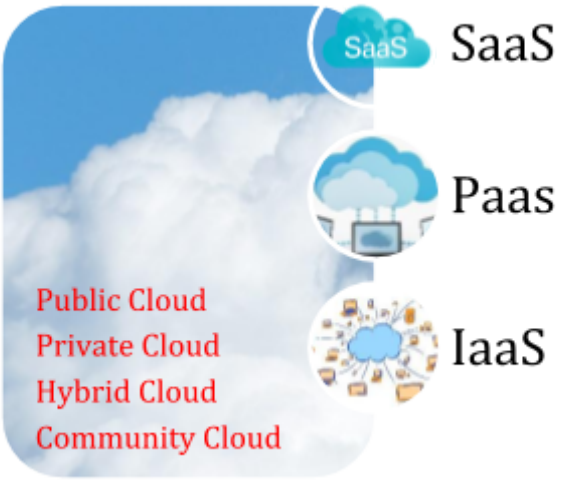

Figure 2. Cloud-based services and deployment model

1) Public cloud

Most services are offered in a public environment in which consumers can access a resource pool that is managed by a host corporation [14]. Because of its existence, this type of environment will pose important concerns regarding security issues [15].

2) Private cloud

A third party vendor provides the services which distinguish it from public accesses [16]. Therefore it is better than the previous development model because it prevents unauthorized access.

3) Community cloud

The cloud services are provided to a specified group where all members are entitled to equal access to the sheared services [17].

4) Hybrid cloud

The cloud services are provided as multiple cloud combustion (public cloud, private cloud, and community cloud) [18]. It might just inherit any kind of vulnerability or risk which resides within the parties listed above.

B) Parties participated in cloud

Security has been seen as a popular barrier towards adopting the cloud model of internet realism. Because the cloud environment is a distributed infrastructure that can be accessed anywhere in the world in its resource storage and control, several concerns have been raised about its limitations, security concerns and difficulties [19], [20], [21]. Different parties' participation has broadened those issues based on both the perspective and purpose of each community [22]. There are three major groups that have been able to participate in cloud computation [23], [24].

i. **Service providers:** Its issues might be heightened over the public and hybrid cloud whereby issues relating to unauthorized access and cyber-attacks can undermine the quality of service [25].

ii. **Service consumers:** Information protection and quality of service issues might be the subject of their concerns. Specifically, their issues concern the provision of infrastructure and interoperability [26].
iii. **Service regulators:** The issues might be focused on violation of service quality-related activities. Therefore, interoperability problems will significantly affect it. This is reasonable to assume that all of the above-mentioned party's issues may be associated and linked with the other participants [27].

C) Service Availability & Interoperability

Cloud computing users are expecting the quality of service that means providers are obliged to prevent even a failure on a single point. Therefore, the providers are compromising customer satisfaction which affects their credibility. Because cloud computing such an active environment, consistency of service may be highly alert, particularly with consumers moving from one service provider to the next [28], [29].

1) Service availability

In particular, a service provider must consider the possibility that critical information will not be available when appropriate. The absence of information may be the result of physical or non-physical faults. Requirements of the region, regulatory regulations, business requirements may trigger these information blackouts. This blackout may also be caused by a faulty tool, suspicious attacks or glitches in the software. Whereas the odds of disappearing the above reasons may be trivial, suppliers should not ignore it [30].

2) Service interoperability

This implies the potential of a community of service providers to exchange and manage information in accordance with agreed standard rules. This applies, from a consumer perspective to the ability to move between service providers and not to be placed in an exclusive cloud service. Maintained customers continue to be surprised by the temptation of freedom to move between the cloud providers. Moreover, moving from one cloud provider to another is a rigid process for it, because of the lack of cloud computing principles [31].

4. Cloud Security Challenges

The following are the challenges for cloud security.

1) Denial of service attacks

A key innovation concept behind such attacks is coordination between various sources to bring down targeted service providers by producing huge amounts of packets at the entry of the victim's network. If it comes to separating the illegitimate packet from the legitimate packet, confusion occurs. Clearly, these attacks involve time cooperation, where inexperienced hackers may cause them. Prevention of such attacks can be dealt with using different tools. The intrusion detection system is one of these technologies. This is a software that shows its effectiveness particularly when the period of the attack is long. Currently, efforts are made to create new innovations for detecting hybrid intrusion that can maintain a range of threats [32].

2) Service hijackings

This is an overlooked problem that provides a marginal challenge, but it may undermine customer credentials. The Intruders aim to target a vulnerability in software or utilize defined software to access sensitive information such as passwords and identities of users. This would result in attackers gaining full control of the cloud service and putting it in danger.

3) Virtual machine attacks

Because cloud infrastructure is entirely built on the virtualization concept, cloud providers must implement virtual machine architectures. Another more technology is a hypervisor that is responsible for running and handling the virtual machine. The weakness of hypervisors must be critically considered by service providers. Ultimately, developers who are conscious of their limitations and how to overpass them have built and coded such technologies.

5. Discussion

The cloud environment guarantees the influence of shared resources for its end users. Cloud provider utilizes multitenancy to arise the concept of sharing. Cloud providers preferably maintain network infrastructure, storage facilities, and application software that promote reliability, performance, and usability. Such a sharing of resources could compromise information security, integrity, and confidentiality.

For the execution of this process, a server placement engine will be deployed to maintain a pool of resources available and dispense it to clients. Resource distribution is done by means of a migration technique to relocate services from a physical entity to the next entity or from a logical cloud to the next cloud to meet the tenant's satisfaction. In practice, these intense demands could lead to confidentiality concerns. Cloud providers must ensure that the necessary legal and security aspects within the placement engines are enforced to mitigate the above risk. This will stress the preservation of knowledge within the property of owners.

Moreover, due to its technical and operational requirements, some of these risks escalated overcloud. Such risks could be mitigated by using a reliable encryption technique to secure transit data. The cloud providers must fundamentally enforce a reliable backup plan with a remote replication of most critical data. The robust access control can be implemented to prevent confidential data. Furthermore, cloud providers should clean up persistent information before they dispense it into the collection.

6. Conclusions

Information technology has been evolutionary progressing and leading to the concept of cloud technology. This identified as one of the major computing models, in which the interest of several educational and industrial organizations in the research on the successful paradigm increased. However, there is also an interesting question about security threats and problems that depend on cloud computing's attraction. Because the cloud architecture is based on a distributed framework, inheriting those threats and vulnerabilities that are relevant to distributed concepts would then be usual. Moreover, almost all of those risks over the cloud concept have strengthened. Problems related to the effects of the inaccessibility of the data have been addressed in this article. Although there was considerable discussion of the factors of interoperable, an open standardized framework was suggested in each of the influential usage examples. This paper focused mainly on major cloud paradigm security threats, one of those threats related to service disruption that can result from attacks such as a denial of service attacks, service hijacking, and VM-level attacks, etc.

References

[1]. Jouini, Mouna, and Latifa Ben Arfa Rabai. "A security framework for secure cloud computing environments." In Cloud security: Concepts, methodologies, tools, and applications, pp. 249-263. IGI Global, 2019.

[2]. Alam T, Benaida M. “The Role of Cloud-MANET Framework in the Internet of Things (IoT)”, International Journal of Online Engineering (iJOE). Vol. 14(12), pp. 97-111. DOI: https://doi.org/10.3991/ijoe.v14i12.8338

[3]. Alam, Tanweer. "Middleware Implementation in Cloud-MANET Mobility Model for Internet of Smart Devices", International Journal of Computer Science and Network Security, 17(5), 2017. Pp. 86-94
[4]. Alam T, Benaida M. CICS: Cloud–Internet Communication Security Framework for the Internet of Smart Devices. International Journal of Interactive Mobile Technologies (iJIM). 2018 Nov 1;12(6):74-84. DOI: https://doi.org/10.3991/ijim.v12i6.6776
[5]. Tanweer Alam, Baha Rababah, "Convergence of MANET in Communication among Smart Devices in IoT", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.9, No.2, pp. 1-10, 2019. DOI: 10.5815/ijwmt.2019.02.01
[6]. Tanweer Alam, "IoT-Fog: A Communication Framework using Blockchain in the Internet of Things", International Journal of Recent Technology and Engineering (IJRTE), Volume-7, Issue-6, 2019.
[7]. Logo, Small. "Introduction to Cloud Computing.", Dialogic
[8]. Wang, Lizhe, Jie Tao, Marcel Kunze, Alvaro Canales Castellanos, David Kramer, and Wolfgang Karl. "Scientific cloud computing: Early definition and experience." In 2008 10th ieee international conference on high performance computing and communications, pp. 825-830. Ieee, 2008.
[9]. Bhardwaj, Sushil, Leena Jain, and Sandeep Jain. "Cloud computing: A study of infrastructure as a service (IAAS)." International Journal of engineering and information Technology 2, no. 1 (2010): 60-63.
[10]. Fernando, N., Loke, S.W. and Rahayu, W., 2013. Mobile cloud computing: A survey. Future generation computer systems, 29(1), pp.84-106.
[11]. Botta, Alessio, Walter De Donato, Valerio Persico, and Antonio Pescapé. "Integration of cloud computing and internet of things: a survey." Future generation computer systems 56 (2016): 684-700.
[12]. Sasikala, P. "Cloud computing: present status and future implications." International Journal of Cloud Computing 1, no. 1 (2011): 23-36.
[13]. Tanweer Alam, "Blockchain and its Role in the Internet of Things (IoT)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 5(1), pp. 151-157, 2019. DOI: https://doi.org/10.32628/CSEIT195137
[14]. Alam, Tanweer. (2018) "A reliable framework for communication in internet of smart devices using IEEE 802.15.4." ARPN Journal of Engineering and Applied Sciences 13(10), 3378-3387.
[15]. Jula, Amin, Elankovan Sundararajan, and Zalinda Othman. "Cloud computing service composition: A systematic literature review." Expert systems with applications 41, no. 8 (2014): 3809-3824.
[16]. Tanweer Alam, "A Reliable Communication Framework and Its Use in Internet of Things (IoT)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), Volume 3, Issue 5, pp.450-456, May-June.2018 URL: http://ijsrcseit.com/CSEIT1835111.
[17]. Alam, Tanweer, and Mohammed Aljohani. "Design and implementation of an Ad Hoc Network among Android smart devices." In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, pp. 1322-1327. IEEE, 2015. DOI: https://doi.org/10.1109/ICGCIoT.2015.7380671
[18]. Alam, Tanweer, and Mohammed Aljohani. "An approach to secure communication in mobile ad-hoc networks of Android devices." In 2015 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), pp. 371-375. IEEE, 2015. DOI: https://doi.org/10.1109/iciibms.2015.7439466
[19]. Aljohani, Mohammed, and Tanweer Alam. "An algorithm for accessing traffic database using wireless technologies." In Computational Intelligence and Computing

Research (ICCIC), 2015 IEEE International Conference on, pp. 1-4. IEEE, 2015. DOI: https://doi.org/10.1109/iccic.2015.7435818

[20]. Alam, Tanweer, and Mohammed Aljohani. "Design a new middleware for communication in ad hoc network of android smart devices." In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, p. 38. ACM, 2016. DOI: https://doi.org/10.1145/2905055.2905244

[21]. Alam, Tanweer. "Fuzzy control based mobility framework for evaluating mobility models in MANET of smart devices." ARPN Journal of Engineering and Applied Sciences 12, no. 15 (2017): 4526-4538.

[22]. Sharma, R. and Trivedi, R.K., 2014. Literature review: Cloud computing-security issues, solution and technologies. International Journal of Engineering Research, 3(4), pp.221-225.

[23]. Alam, Tanweer, Arun Pratap Srivastava, Sandeep Gupta, and Raj Gaurang Tiwari. "Scanning the Node Using Modified Column Mobility Model." Computer Vision and Information Technology: Advances and Applications 455 (2010).

[24]. Alam, Tanweer, Parveen Kumar, and Prabhakar Singh. "SEARCHING MOBILE NODES USING MODIFIED COLUMN MOBILITY MODEL.", International Journal of Computer Science and Mobile Computing, (2014).

[25]. Alam, Tanweer, and B. K. Sharma. "A New Optimistic Mobility Model for Mobile Ad Hoc Networks." International Journal of Computer Applications 8.3 (2010): 1-4. DOI: https://doi.org/10.5120/1196-1687

[26]. Singh, Parbhakar, Parveen Kumar, and Tanweer Alam. "Generating Different Mobility Scenarios in Ad Hoc Networks.", International Journal of Electronics Communication and Computer Technology, 4(2), 2014

[27]. Sharma, Abhilash, Tanweer Alam, and Dimpi Srivastava. "Ad Hoc Network Architecture Based on Mobile Ipv6 Development." Advances in Computer Vision and Information Technology (2008): 224.

[28]. Alam, Tanweer. "Tactile Internet and its Contribution in the Development of Smart Cities." arXiv preprint arXiv:1906.08554 (2019).

[29]. Tanweer Alam, “5G-Enabled Tactile Internet for smart cities: vision, recent developments, and challenges”, JURNAL INFORMATIKA, Vol. 13, No 2, July 2019, pp. 1-10, DOI: 10.26555/jifo.v13i2.a13426

[30]. Alam, Tanweer, Abdulrahman A. Salem, Ahmad O. Alsharif, and Abdulaziz M. Alhejaili. "Smart Home Automation Towards the Development of Smart Cities." APTIKOM Journal on Computer Science and Information Technologies 5, no. 1 (2020). DOI: https://doi.org/10.11591/APTIKOM.J.CSIT.153

[31]. Tanweer Alam, “Efficient and Secure Data Transmission Approach in Cloud-MANET-IoT Integrated Framework”, Journal of Telecommunication, Electronic and Computer Engineering, Vol 12(1), 2020.

[32]. Novais, Luciano, Juan Manuel Maqueira, and Ángel Ortiz-Bas. "A systematic literature review of cloud computing use in supply chain integration." Computers & Industrial Engineering 129 (2019): 296-314.