International Journal of Academic Research and Development
ISSN: 2455-4197, Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 2; Issue 3; May 2017; Page No. 110-115

Cloud computing: Features and Issues

[1] Swati M Suryawanshi, [2] Vaishali L Kolhe

[1] ME Scholar, D.Y. Patil College of Engineering, Akurdi, Pune, Maharashtra, India
[2]Assistent Professor, D.Y. Patil College of Engineering Akurdi, Pune, Maharashtra, India

Abstract
Since the phenomenon of cloud computing was proposed, there is a continuous interest for research across the globe. Cloud computing has been seen as entire of the technology that poses the next-generation computing revolution and rapidly becomes the hottest topic in the field of IT. This fast move towards Cloud computing has sustained concerns on a fundamental point for the success of information systems, communication, virtualization, data availability and integrity, public auditing, scientific application and information security. Therefore, cloud computing research has attracted tremendous interest in recent years. In this paper, we aim to precise the current issues of Cloud computing. We have discussed the paper in two-fold: first we discuss the cloud computing architecture and the numerous services it offered. Secondly we highlight several security issues in cloud Computing based on its service layer.

Keywords: cloud computing; virtualization; service models; deployment models

1. Introduction
Cloud computing has recently emerged as a buzz word in the distributed computing community. Many believe that Cloud is going to reshape the IT industry as a revolution. So, what is Cloud Computing? Although many formal definitions have been proposed in both academia and industry, the one provided by U.S. NIST (National Institute of Standards and Technology) [1] appears to include common key elements widely used in the Cloud Computing community.
Cloud computing is a model for enabling comfortable, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly supply and released with minimal management effort or service provider interaction [1]. Cloud computing gives a flexible online environment which encourages the capability to handle an expanded volume of work without affecting on the execution of the framework.
Utilization of cloud services makes a developing relationship among both public and private sector phenomenon and the people served by these elements. Cloud computing is attractive to business owners as it eliminates the requirement for users to plan ahead for provisioning, and allows enterprises to start from the small and increase resources only when there is a rise in service demand [2].
The rest of the paper is organized as follows. Section II presents a study on the cloud computing architecture and highlights the recent available computing tools. In section III, we list out several security issues in cloud computing. Finally in Section IV, we conclude the paper.

2. Cloud Computing Architecture
A) The essential characteristics of cloud computing [1, 2]
- **On-demand self-service:** Registering could resources be obtained and utilized whenever without the requirement for human association with cloud administration suppliers. Computing resources include processing power, storage, virtual machines, etc.
- **Broad network access:** The beforehand said resources could be gotten to over a system utilizing heterogeneous gadgets, for example, laptops or mobiles telephones.
- **Resource pooling:** Cloud administration suppliers pool their resources that are then imparted by numerous clients. This is alluded to as multi-tenure where, for instance, a physical server may have a few virtual machines having a place with distinctive clients.
- **Rapid elasticity:** A client can rapidly gain more resources from cloud by scaling out and can scale back in by discharging those resources once they are no more needed.
- **Measured service:** Resources utilization is measured by monitoring storage usage, CPU hours, bandwidth usage, etc. The said metrics are applied to all clouds, but each cloud provides users with services at a different level of abstraction, which is an alternate to an administration.

B) The three most common service models of cloud computing [3]
A cloud can collaborate with customer/client in a mixed bag of courses, through capacities called services. Across the web, three major types of models, of services have emerged, Fig. 2 shows the details of cloud computing service model.

Software as a Service (SaaS)
Cloud consumers release their applications on a presenting environment, which can be accessed through networks from various clients (e.g. web browser, PDA, etc.) by application users. Cloud consumers do not have

control over the Cloud infrastructure that often employs a multi-tenancy system architecture, namely, different cloud consumers' applications are organized in a single logical environment on the SaaS cloud to achieve economies of scale and optimization in terms of speed, security, availability, disaster recovery, and maintenance. Examples of SaaS include Sales Force.com, Google Mail, Google Docs, and so forth.

Platform as a Service (PaaS)

PaaS is a development platform supporting the full "Software Lifecycle" which allows cloud consumers to develop cloud applications and services (e.g. SaaS) directly on the PaaS cloud. Hence the difference between PaaS and SaaS is that PaaS offers a development platform that hosts both completed and in-progress cloud applications whereas SaaS only hosts completed cloud applications. This requires PaaS, in addition to supporting application hosting environment, to possess development infrastructure including programming environment, tools, configuration management, and so forth. An example of PaaS is Google AppEngine.

Infrastructure as a Service (IaaS)

Cloud consumers directly use IT infrastructures (processing, storage, networks, and other fundamental computing resources) provided in the IaaS cloud. Virtualization is extensively used in IaaS cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers. The basic strategy of virtualization is to set up independent virtual machines (VM) that are detached from both the underlying hardware and other VMs. Notice that this strategy is different from the multi-tenancy model, which aims to transform the application software architecture so that multiple instances (from multiple cloud consumers) can run on a single application (i.e. the same logic machine). An example of IaaS is Amazon's EC2.

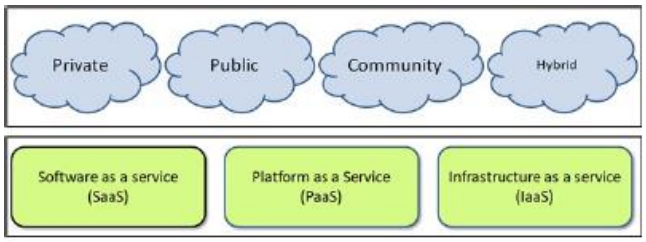
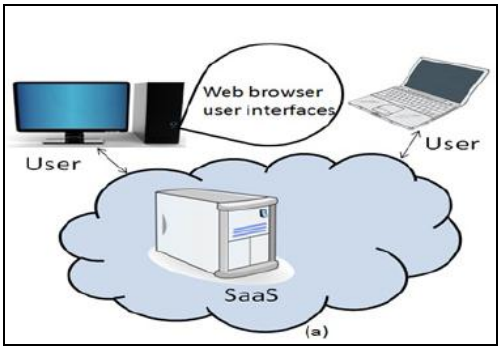
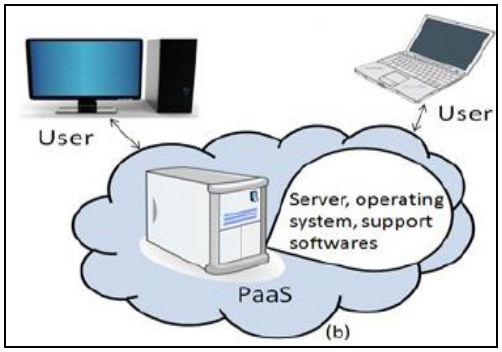


Fig 1: Cloud solutions based on the system's deployment and service model [4].





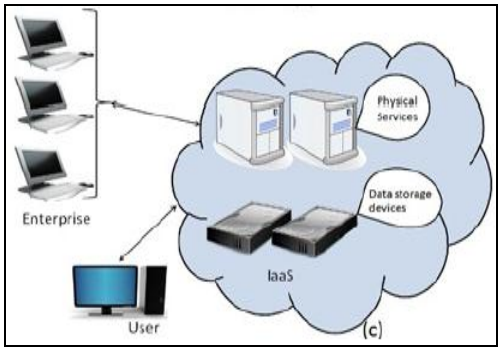


Fig 2: Service model of Cloud: (a) Software as a service (SaaS), (b) Platform as a Service (PaaS), and (c) Infrastructure as a service (IaaS) [4].

C) The four deployment models of cloud computing

A cloud organization model indicates how resources inside the cloud and shared. Fig. 1, shows four different cloud deployment models: private cloud, public cloud, community cloud, and hybrid cloud. Each model impacts the comparing scalability, reliability, security, and cost [4].

Private cloud

The cloud infrastructure is operated fully within a single organization, and managed by the organization or a third party regardless whether it is located premise or off premise. The motivation to setup a private cloud within an organization has several aspects. First, to maximize and optimize the utilization of existing in-house resources. Second, security field including data privacy and trust also make Private Cloud an option for many firms. Third, data transfer cost [12] from local IT infrastructure to a Public Cloud is still rather considerable. Fourth, organizations always require full control over mission-critical activities that reside behind their firewalls. Last, academics often build private cloud for research and teaching purposes.

Community cloud

Several organizations jointly construct and share the same cloud infrastructure as well as policies, requirements, values, and concerns. The cloud community forms into a degree of economic scalability and democratic stability. The cloud infrastructure could be introduced by a third-party vendor or within one of the organizations in the community.

Public cloud
This is the dominant form of current Cloud computing deployment model. The public cloud is used by the general public cloud consumers and the cloud service provider has the full ownership of the public cloud with its own policy, value, and profit, costing, and charging model. Many popular cloud services are public clouds including Amazon EC2, S3, Google AppEngine, and Force.com.

Hybrid cloud
The cloud infrastructure is a combination of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). Organizations use the hybrid cloud model in order to optimize their resources to increase their core capabilities by communicating out peripheral business functions onto the cloud while controlling core activities on-premise through private cloud.

D) Features of the cloud computing [4]
The cloud is now hosting wide range of large scale and small scale applications. Many organization or companies are now moving key applications from expensive internal data centers to cost effective and resourceful cloud solutions.

Scalability
When a user lunch website scalability defines a site or application's skill to use traditional solutions on demand. The site may scale up to available additional resources the system is experiencing high user demand and later may scale down recourse when the user demand turns down.
Applications that run within the cloud are normally highly scalable. An applicant can manually add or remove resources or application can be configured to scale automatically.

Virtualizations
Virtualization is to use hardware or software to create the observation of something. Must server have their own CPU that is capable of running specific a specific operating system (OS), such as Windows, Linux, or Mac OS. By using special software, server can be shown as it has multiple CPUs and are running the same or different operating systems and the server CPU switches its processing power frequently among the various operating systems.
In the same way, desktop PCs typically run one operating system. Again, by using special virtualization software, a desktop PC/ laptop can be run simultaneously different operating systems. This provides an excellent platform for developer's application testers, and help desk support personal which support multiple operation systems. Without having multiple systems on the desk, the user can use multiple operation systems in a single desktop PC.

E) Cloud Computing Simulators
During the study we compared various available cloud simulators, their properties and unique features. The comparison study along with the research group working on these tools are summarized in Table 1.

Table 1: Comparison of Currently Available Cloud Simulators

Simulator	Base Platform	Developer	Available	Language	GUI	Energy Model
CloudSim [13]	SimJava	University of Melbourne, Australia.	Open Source	Java	No	Yes
CloudAnalyst [14]	CloudSim	University of Melbourne, Australia.	Open Source	Java	Yes	Yes
NetworkCloudSim [15]	CloudSim	University of Melbourne, Australia.	Open Source	Java	No	Yes
iCanCloud [16]	SIMCAN	Universidad de Madrid, Spain.	Open Source	C++	Yes	No
EMUSIM [17]	CloudSim, AEF	University of Melbourne, Australia.	Open Source	Java	No	Yes
GroudSim [18]	-	University of Innsbruck, Austria	Open Source	Java	Limited	No
MRCloudSim [19]	CloudSim	eoul National University, South Korea	Not available	Java	No	Yes
DCSim [20]	-	University of Western Ontario, Canada.	Open Source	Java	No	No
SimIC [21]	SimJava	University of Derby, UK	Not available	Java	No	Rough
GreenCloud [22]	NS2	University of Luxembourg, Luxembourg	Open Source	C++, otcel	Limited	Yes
MDCsim [23]	CSIM	Pennsylvania State University, USA	Commercial	Java, C++	No	Rough
SPECI [24]	SimKit	University of Bristol, UK	Open Source	Java	-	Rough
MalStone [25]	-	University of Illinois, Chicago, USA	Open Source	Java, Python	-	Rough

3. Security Issues in Cloud

Here in this section we described several cloud computing security issues based on different service layer. The Fig. 3 shows the overlay architecture of security issues and trust requirement in a top-down service model [5]. Trust basically works in a top-down design, as every layer needs to trust the layer instantly beneath it, and obliges a security ensure at an operational, specialized, procedural and lawful level to empower secure correspondences. But the security is treated as individually in each service layer. Trust could be seen as a sequence from the end client to the application holder, who thusly believes the provider.

a) Security issues in SaaS

In SaaS, the client needs to rely on upon the supplier for fitting efforts to establish safety. The supplier must do the work to keep numerous clients' from seeing one another's information. So it gets to be hard to the client to guarantee that right efforts to establish safety are set up furthermore hard to get confirmation that the application will be accessible when required [6]. Based on SaaS, client can substitute net program or software applications over old one. Hence, the center is not upon portability of uses, yet on safeguarding or upgrading the security usefulness gave by the legacy application and attaining effective information relocation [8].

The SaaS programming seller may have the application on its own private server farm or convey it on a cloud computing framework administration gave by an outsider supplier (e.g.Amazon, Google, etc.). The utilization of cloud computing coupled with the pay-as-you-go (develop) methodology helps the application administration supplier diminish the interest in foundation benefits and empowers it to focus on giving better administrations to clients. Over the past decade, computers have become widespread within enterprises while IT services and computing has become a commodity. Enterprises today view data and business processes (transactions, records, pricing information, etc.) themselves as strategic and guard them with access control and compliance policies. However, in the SaaS model, enterprise data is stored at the SaaS providers data center, along with the data of other enterprises. Moreover, if the SaaS provider is leveraging a public cloud computing service, the enterprise data might be stored along with the data of other unrelated SaaS applications. The cloud supplier may, also, imitate the information at numerous areas crosswise over nations for the reasons of keeping up high accessibility.

Most enterprises are acquainted with the conventional on reason model, where the information keeps on residing inside the endeavour limit, subject to their approaches. Therefore, there is a lot of inconvenience with the absence of control and information of how their information is put away and secured in the SaaS model. There are strong concerns about data breaches, application vulnerabilities and availability that can lead to financial and legal liabilities [7].

There are several highlights security issues in SaaS such as data security, network security, data locality, data integrity, data segregation, data access, authentication and authorization.

b) Security issues in PaaS

In PaaS, the administration supplier may give some control to the customer to manufacture applications on top of the stage. However any securities beneath the application level, for example, have and system interruption anticipation will at present be in the extent of the supplier and the supplier brings to the table solid affirmations that the information stays distant between applications. Paas is proposed to empower designers to assemble their own particular applications on top of the platform. As a result, it tends to be more extensible than SaaS, at the expense of customer-ready features. This exchange off stretches out to security gimmicks and abilities, where the implicit capacities are less finish, however there is more adaptability to layer on extra security [7].

Applications sufficiently perplexing to influence an Enterprise Service Bus(ESB) need to secure the ESB straightforwardly, leveraging a convention, for example, Web Service (WS) Security. The capability to portion ESBs is not accessible in PaaS situations. Measurements ought to be set up to survey the viability of the application security programs. Among the immediate application, security particular measurements accessible are defencelessness scores and patch scope. These measurements can show the quality of application coding. Consideration ought to be paid to how malignant on-screen characters respond to new cloud application architectures that the darkened application parts from their examination. Programmers are liable to the assault noticeable code, including but not constrained to code running in the client connection. They are prone to assault the foundation and perform extensive black box testing. The vulnerabilities of cloud are connected with the web applications as well as vulnerabilities connected with the machine-to-machine Service- Oriented Architecture (SOA) applications, which are progressively being conveyed in the cloud [7].

c) Security issues in IaaS

In IaaS, the developer has better control over the security the length of there should not any security gap in the virtualization 1179 director. Likewise, however in principle virtual machines may have the capacity to address these issues yet in practice there are a lot of security issues [9]. The other element is the unwavering quality of the information that is put away inside the supplier's equipment. Because of the developing virtualization of "everything" in data society, holding a definitive control over information to the holder of information paying little respect to its physical area will turn into a subject of most extreme investment. To accomplish most extreme trust and security on a cloud asset, a few procedures would need to be connected [10]. The security obligations of both the supplier and the client incredible contrast between cloud administration models. Amazons Elastic Compute Cloud (EC2) (Amazon, 2010) IaaS offering, as a case, incorporates

merchant obligation regarding security up to the hypervisor, importance they can just address security controls, for example, physical security, natural security, and virtualization security. The client, thus, is in charge of the security controls that identify with the IT framework including the OS, applications and information [8].

Based on the cloud deployment IaaS inclined to various security issues. Private cloud is more protected compared to a public cloud. The most important issue is to protect the physical infrastructure of data centers. It can be damage by any natural disaster or damage is acquired to the framework deliberately. Infrastructure doesnt mean the hardware where data is processed and stored, it also include the where it is getting transmitted. In cloud environment data transmitted from the source to destination through large number of third

party. So there is huge possibility that information could be directed through an interloper's foundation [7]. Despite the fact that cloud construction modeling is an extemporized engineering, the underlying advances continue as before. As cloud services are available online, it builds over internet and securities in web are postured by the cloud. It provides client access resources over the internet whenever supplier dwells at distinctive area.

Regardless of the fact that gigantic measure of security is placed set up in the cloud, still the information is transmitted through the ordinary underlying Internet. So threaten on the Internet is leading to cloud threaten. But, in a cloud, the dangers are devastatingly high. Cloud frameworks still use ordinary conventions and efforts to establish safety that are utilized within the Internet yet the prerequisites are at a higher degree. A dynamic set of arrangements and conventions are obliged to help secure transmission of information inside the cloud. Encryption and secure conventions coddle the needs to a certain degree yet they are not connection situated. Concerns with respect to interruption of information by outer non-clients of the cloud through the web ought to additionally be considered. Measures should be set in place to make the cloud environment secure, private and isolated on the Internet to avoid cyber criminals attacking the cloud [7, 11].

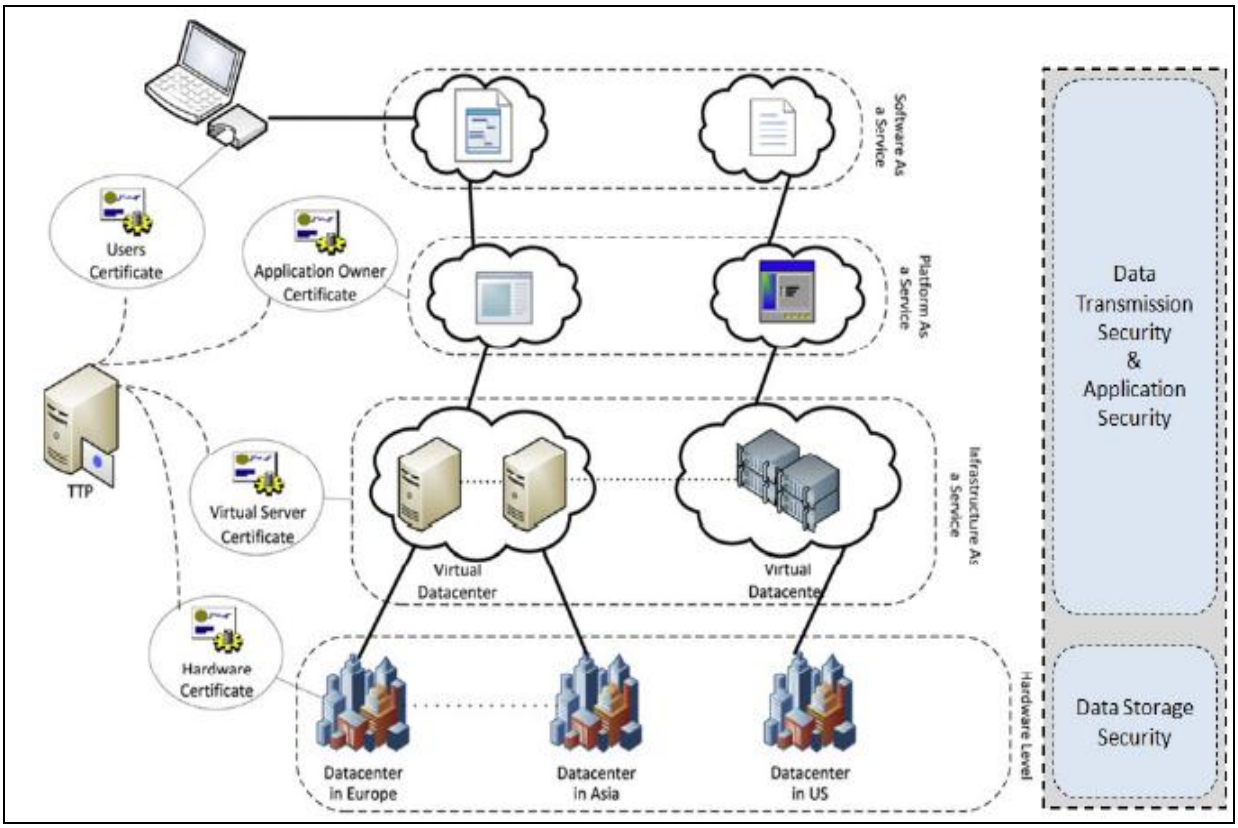


Fig 3: Overlay architecture of security issues and trust requirement in a top-down service model

4. Conclusion

This paper discussed the issues of Cloud computing. That-assist the advance scientific features of cloud computing with layer wise classification of the cloud services. This survey and future issues demonstrated that there are a few routes in which the cloud research group can gain from related groups. There is given an extensive outlook of current research issues cloud computing and available platform to simulate the research idea. They exhibited scientific classification of issues found here, and the methodologies in which these issues have been handled, concentrating on an operational level, client level, service level and application level, security and context-awareness.

5. References

1. Mell P, Grance T, Draft nist working definition of cloud computing, 2009; 15, 21
2. Sasikala P. Research challenges and potential green technological applications in cloud computing.

International Journal of Cloud Computing, 2013; 2(1):1-19,
3. Tharam Dillon, Chen Wu, Elizabeth Chang, Cloud Computing: Issues and Challenges. 24th International Conference on Advanced Information Networking and Applications, IEEE, 2010.
4. D Puthal, Sahoo BPS, Mishra S, Swain S, Cloud Computing Features, Issues and Challenges: A Big Picture, International Conference on Computational Intelligence & Networks, 2015.
5. Zissis, Dimitrios, Dimitrios Lekkas. Addressing cloud computing security issues. Future Generation Computer Systems, 2012; 28(3):583-592.
6. Choudhary V. Software as a service: Implications for investment in software development. 40th Annual Hawaii International Conference on System Sciences, IEEE, 2007; 209-209,
7. Subashini S, Kavitha V, A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 2011; 34(1):1-11.
8. Seccombe A, *et al.* Security guidance for critical areas of focus in cloud computing. Cloud Security Alliance, 2009, 2(1).
9. Gajek S, *et al.* Breaking and fixing the inline approach. ACM workshop on Secure web services, ACM, 2007.
10. Descher M. *et al.* Retaining data control to the client in infrastructure clouds. International Conference on Availability, Reliability and Security, IEEE, 2009, 9-16.
11. Staten, James, *et al.* Is cloud computing ready for the enterprise. Forrester Research, 2008.
12. Armbrust M, Fox A, Griffith R, Joseph A, Katz R, Konwinski A *et al.* Above the clouds: A Berkeley view of cloud computing, EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS. 2009, 28.
13. Calheiros, Rodrigo N, Rajiv Ranjan, Anton Beloglazov, Csar AF De Rose, Rajkumar Buyya *et al.* CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Software: Practice and Experience, 2011; 41(1):23-50.
14. Wickremasinghe B, Calheiros RN, Buyya R, Cloud Analyst, A CloudSim-based Visual Modeller for analysing Cloud Computing Environments and Applications, 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.
15. Garg SK, Buyya R. Network Cloud Sim: modelling parallel applications in cloud simulations. In Utility and Cloud Computing (UCC), 4th IEEE International Conference on, pp. 2011, 105-113.
16. Nunez A. *et al.* Can Cloud: A Flexible and Scalable Cloud Infrastructure Simulator, Jr. of Grid Computing, 2012; 10(1):185-209.
17. Calheiros RN, Netto MAS, De Rose CAF, Buyya R, EMUSIM: an integrated emulation and simulation environment for modeling, evaluation, and validation of performance of cloud computing applications, Software-Practice and Experience, 2012; 43(5)595-612.
18. Ostermann S, Plankensteiner K, Prodan R, Fahringer Th, GroudSim: An Event-Based Simulation Framework for Computational Grids and Clouds, Euro-Par Parallel Processing Workshops Lecture Notes in Computer Science, 2011, 305-313.
19. Jung J, Kim H, MR-CloudSim: Designing and implementing MapReduce computing model on CloudSim, International Conference on ICT Convergence (ICTC). 2012, 504-509.
20. Tighe M, Keller G, Bauer M, Lutfiyya H, DCSim: A Data Centre Simulation Tool for Evaluating Dynamic Virtualized Resource Management, 8th international conference and workshop on systems virtualization management (svm) Network and service management (cnsm), 2012, 385-392.
21. Sotiriadis S, Bessis N, Antonopoulos N, Anjum A, SimIC. Designing a new Inter-Cloud Simulation platform for integrating largescale resource management, IEEE 27th International Conference on Advanced Information Networking and Applications, 2013, 90-97.
22. Kliazovich, Dzmitry, Pascal Bouvry, Samee Ullah Khan. Green-Cloud: a packet-level simulator of energy-aware cloud computing data centers. The Journal of Supercomputing. 2012; 62(3):1263-1283.
23. Lim, Seung-Hwan *et al.* MDCSim: A multi-tier data center simulation, platform. In Cluster Computing and Workshops, CLUSTER'09. IEEE International Conference on. 2009, 1-9.
24. Sriram, Ilango. SPECI, a simulation tool exploring cloud-scale data centres. In Cloud Computing, Springer, 2009, 381-392.
25. Bennett, Collin, *et al.* Malstone: towards a benchmark for analytics on large data clouds. In Proceedings of the 16th ACM SIGKDD Int. Conf. on Knowledge discovery and data mining, 2010, 145-152.