A REVIEW ON SECURITY ISSUES AND CHALLENGES IN CLOUD COMPUTING MODEL OF RESOURCE MANAGEMENT

T. Vaikunth Pai* & Dr. P. S. Aithal**

Srinivas Institute of Management Studies, Pandeshwar, Mangalore, Karnataka

Abstract:
Cloud computing services refer to set of IT-enabled services delivered to a customer as services over the Internet on a leased basis and have the capability to extend up or down their service requirements or needs. Usually, cloud computing services are delivered by third party vendors who own the infrastructure. It has several advantages include scalability, elasticity, flexibility, efficiency and outsourcing non-core activities of an organization. Cloud computing offers an innovative business concept for organizations to adopt IT enabled services without advance investment. Being a model for enabling convenient, on-request network accessibility to a shared pool of IT computing resources like networks, servers, storage, applications, and services, cloud computing can be quickly provisioned and released with negligible management exertion or service provider interaction. Despite many benefits of cloud computing, the organizations are slow in accepting cloud computing service model because of security concerns and challenges associated with management of this technology. Security is one of the major issues which hinder the growth of cloud computing service model. The idea of handing over confidential data to third party is risky such that the consumers need to be more attentive in understanding the risks of data breaches in this new environment. This paper reviews the security issues and the challenges in the adoption and management of cloud computing services in an organization.
Index Terms: Cloud Computing Model, Security Issues in Cloud Computing, Cloud Computing Services & Cloud Computing Model of Resource Management

1. Introduction:

During last several years, the Internet has been used on system graphs by a cloud image when an assortment of newly added innovation began to materialize that permitted computing resources to be accessed over the Internet termed as cloud computing technology. Cloud computing is mainly concerned with accessing online software applications, data storage and processing power of the system. Cloud computing supports the organizations to enhance their capacity dynamically without investing in new infrastructure, training new IT personnel, or purchasing new licensed software that are required for the automation of various processes. It extends the capabilities of Information Technology. During recent years, cloud computing model has developed from being a promising business concept to one of the fast rising innovations of the IT industry. Since all information of individuals and companies are placed on the cloud, the concern starts to grow about security issues. Cloud computing has profited many organizations by decreasing IT expenses and permitting them to focus on their core business competence and skills rather than IT infrastructure. Cloud-based services are ideal for the organizations with growing or fluctuating bandwidth demands from consumers. Depending on the need of the user, it is possible to expand cloud services capability and then it is possible to scale down again due to the reason that the adaptability is baked into the cloud service. This level of nimbleness can give organizations utilizing cloud computing a real advantage over contenders. Despite many advantages of the cloud computing model, customers are still hesitating to deploy their business operations on the cloud because of security concerns of business data. Since Cloud services are internet based and may serve many clients each day, they can become inundated and may even come up against technical blackouts. This can lead to suspension of business processes temporarily at the point when web association is disconnected, and hence the user will not have the capacity to get to any of his applications, server or information from the cloud. The security could improve because of data centralization and security on resources but the concerns continue about the loss of control over certain sensitive data and the security of stored information handed over to the cloud service providers. If those providers have not provided with the efficient security system in their own environments, the consumers could be in difficulty. Measuring the quality of security measures implemented by the cloud providers is difficult because many cloud providers will not expose their infrastructure facilities to customers. Section 2 narrates the literature review on related work son security issues in cloud computing. Section 3analyses security issues in cloud computing laying accentuation on Software as a service, Platform as a service and Infrastructure as a service and cloud computing deployment methods. Section 4 addresses the challenges of the organizations on cloud computing resource management and section 5 conclude the entire work.

2. Related Works:

During 2008, Gartner identified seven security issues which should be addressed before enterprises consider switching to the cloud computing model. They are as follows: (1) privileged user access - data transmitted from the client through the Internet represents a specific level of hazard because of issues of data proprietorship; enterprises should spend time getting acquainted with their providers and their regulations as much as possible before assigning some inconsequential applications first to test the water, (2) regulatory compliance - clients are responsible for the security of their solution, as they can choose between providers that permit to be reviewed by third party organizations that check levels of security and providers that don't (3) data location - relying upon contracts, a few clients may never comprehend what nation or what locale their information is found (4) data segregation - encoded data from various organizations may be stored on the same hard disk, so a mechanism to separate data ought to be conveyed by the service provider. (5) recovery - every cloud service provider ought to have a disaster recovery system to store user information, (6) investigative support - if a client speculates faulty activity from the provider, it might not have numerous lawful ways pursue an enquiry, (7) long-term feasibility - refers to the ability to withdrawn agreement and all information if the present provider is bought out by another firm [2]. The Cloud Computing Use Case Discussion Group discusses the distinctive Use Case situations and related prerequisites that may exist in the cloud model. They consider use cases from alternate points of view including clients, designers and security engineers [3].ENISA explored the distinctive security risks related to adopting cloud computing along with the affected resources, the risks probability, effects, and vulnerabilities in the cloud computing may lead to such risks[4]. Balachandra et al, (2009) discussed the security Service Level Agreement's requirement and objectives related to data locations, isolation and data recovery [5]. Kresimir et al, (2010) discussed high level security concerns in the cloud computing model such as information trustworthiness, payment, and protection of sensitive information [6]. Bernd et al, (2010) discuss the security vulnerabilities existing in the cloud platform. The authors gathered the conceivable vulnerabilities into innovation related, cloud qualities related, security controls related [7]. Subashini et al discuss the security difficulties of the cloud service delivery model, concentrating on the SaaS model [8]. Ragovind et al, (2010) discussed the administration of security in Cloud computing concentrating on Gartner's list of cloud security issues and the discoveries from the International Data Corporation enterprise [9]. Morsy et al, (2010) investigated cloud computing issues from the cloud design, cloud offered qualities, cloud partners, and cloud service delivery models perspectives[10]. A recent survey conducted by Cloud Security Alliance (CSA) & IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security are required both to quicken cloud appropriation on a wide scale and to react to administrative drivers. It also details that cloud computing is molding the fate of IT yet the nonattendance of a consistence domain is having a sensational effect on cloud computing growth [11]. Puthal, Deepak, et al, (2015) discussed the advance scientific features of cloud computing with the layer wise classification of the cloud services and highlighted the subsequent guidelines of research facing the both industry and academic community [12]. Hussein, N. H., et al, (2016) discussed the different threats and solutions in the environment of cloud computing with special emphasis on privacy and security of user's sensitive data [13]. Jafarpour, S., et al, (2016) reviewed the current major security issues in cloud computing such as lack of control of data, lack of trust and multi-tenancy [14]. Sarkar, S., et al, (2016) discussed the security issues in the service and deployment models of cloud computing, challenges faced during cloud security and the encryption techniques used to improve the security of the cloud [15]. Dubey, A. (2016) discussed the issues related to cloud computing which involves data location, security, storage, confidentiality, integrity and availability [16].

3. Security Issues in Cloud Computing:

3.1 Cloud Deployments Models: In the cloud deployment model, the services like platform, networking, storage, and software infrastructure are provided as services that scale up or down depending on the demand. The Cloud Computing model has three main deployment models which are:

Private Cloud: Private cloud model is a new technology that some vendors have recently used to describe offerings that imitate cloud computing on private networks. It is implemented within an organization's internal enterprise data enter. This architecture is implemented and executed exclusively for an implemented organization and is only utilized and used by their workers at the authoritative level and is managed and controlled by the organization or third party. The cloud infrastructure in this model is installed on organizational premise or off premise. Thus in deployment model, management and maintenance are easier, security is very high and the organization has more control over the infrastructure and accessibility. In the private cloud, adaptable resources and virtual applications are pooled together and made accessible for cloud service consumers to share and utilize. It varies from the public cloud model in that all the resources and application services on the private cloud are managed and maintained by the organization itself, like Intranet functionality in an organization. Working on the private cloud can be much more secure than that of the public cloud because of its specified predefined internal secured exposure in an organization. In private cloud only, the organization and assigned stakeholders may have access admittance to work on resources [17]. Private Cloud models can give noteworthy advantages to an organization as long they are implemented and managed successfully and safely. In

consolidated, multi-tenant configurations such as Private Clouds, tenant isolation becomes a very important aspect of the architecture. It is obvious that without proper isolation, tenants may intentionally or unintentionally abuse the shared resources or compromise the security of their neighbours. Appropriate segregation empowers the reasonable and secure utilization of the environment's shared resources.

Public Cloud: Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provided on a self-service, fine-grained basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. Generally, the service is based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization [18]. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks. Data and communication protection plays a vital role in Cloud computing. Services can be accessed through a thin client, laptop or mobile phone. The reasons that your data is easily accessible through these channels are your data is transferred across multiple networks, when your cloud service provider is extremely far away from your location. All communication should be protected using encryption and key management. To safeguard server failure Public Cloud service providers should implement strong data replication mechanisms to distribute customer's data across the globe in various geographies. It might conflict with the customer's requirements to keep their data within a specified region.

Hybrid Cloud: The hybrid cloud model is a merger of two or more kinds of cloud deployment models such as private, public or hybrid. The participating clouds are bound together by a standard set of protocols. It enables the involved organization to serve its requirements in their own private cloud and in the case of critical needs cloud bursting for load-balancing occur they can avail services from the public cloud. It caters the virtual IT enabled services through a mixture of both public and private clouds services. Hybrid cloud provides more secure control of the data &applications and allows various clients to access data/information over the Internet. The hybrid cloud has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local computing device, such as a Plug computing system with cloud working administrations. It can also depict configurations combining virtual and physical, collocated virtualized environment that requires physical servers, routers, or other hardware components. Cloud architects need redundancy across data centers to moderate the impact of failure in a single data center in the cloud. An absence of repetition can turn into a genuine security hazard in the hybrid cloud when redundant copies of data are not distributed across data centers. It is convenient to shift instances of the virtual machine within data centers rather than between large sets of data. Cloud can implement redundancy using multiple data centers from a single provider, multiple public cloud providers or a hybrid cloud when you improve business continuity with a hybrid cloud, that shouldn't be the only reason to implement this model. Using multiple data centers from a single cloud provider cost could be saved and attain same levels of risk improvement using multiple data centers from a single cloud provider.

3.2 Cloud Computing Service Delivery Models: After developing the cloud deployment models for basic business process security over the cloud, the next security consideration relates to the various cloud computing service delivery models. The three main cloud service delivery models useful for organizations are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

Infrastructure as a Service (IaaS): In this service model, the service provider delivers the infrastructure to the user over the internet. The user is able to deploy and execute various software including system software and application software. The user has the ability to provision computing power, storage, networks. Infrastructure as a Service is a kind of cloud computing that provides virtualized computing resources over the Internet and it is a single tenant cloud layer service where the Cloud computing vendor's dedicated resources are only shared and benefited contracted clients at a pay-per-use fee basis. It reduces the need for huge initial investment on computing hardware such as data servers, networking devices, and processing power. They also allow varying levels of financial and functional elasticity not found in internal data centers or with collocation services, due to the fact that cloud computing resources can be broadened or discharged on request substantially more rapidly and cost-viably than in an internal data center or with a collocation service that is given [2]. IaaS and other associated services have enabled start-ups and other businesses concentrate on their core competencies without worrying much about the provisioning and management of IT infrastructure. IaaS completely abstracted the hardware underneath it for implementation and allowed clients to consume infrastructure as a service without worrying anything about the underlying complexities in implementation. The cloud has a convincing value scheme in terms of cost, but when it comes to security concern, IaaS just gives essential security such as firewall, load balancing, etc. and applications moving into the cloud will require more elevated amounts of security gave at the host.It offers highly scalable resources that can be modified and adjusted on-demand. Such flexibility makes IaaS well-suited for workloads that are temporary, experimental or change unpredictably during the process. Data stored in IaaS infrastructure in both private and public cloud needs to be monitored personally. This is must when it is implemented in public cloud. In this, it should be monitored who is accessing the information, how information is accessed, the location from where it is accessed and impact to accessed

International Journal of Engineering Research and Modern Education (IJERME)
Impact Factor: 6.525, ISSN (Online): 2455 - 4200
(www.rdmodernresearch.com) Volume 2, Issue 1, 2017

information later. These problems can be solved by using modern Rights Management services applying the restriction to business data and intelligence. Suitable policies for information need to be created and deployed. In addition, the transparent process can be created that monitors information usage. Robust logging and reporting system helps to keep track the location of information, who has accesses it, in which machines are handling it and which storage arrays are responsible for it. These implementations are important for cloud service management and optimization. To prevent offline attacks disk encryption can be used to encrypt all the data including user files on the disk which helps to keep data secured.

Platform as a Service (PaaS): Platform as a service (PaaS) is a cloud computing model that delivers application services over the Internet to users. In a PaaS model, a cloud provider delivers hardware resources and software tools needed for application development to its users as a service. Here, software and development tools are hosted on the provider's servers and they deliver consumer with a platform including all the systems and technical environments comprising of the software development life-cycle components such as developing, testing, deploying, required tools and software applications for software development. PaaS provider hosts the hardware and software requirements on its own infrastructure that are required by the clients. So it relieves users from installing hardware and software requirements to develop or run a new application on site. The user does not have any control over network, servers, operating system, and storage of data in the cloud but it can manage and control the deployed application and hosting environments configurations remotely. This service is one layer above IaaS on the delivery service model and abstracts away internal working of operating system services, middleware tools, etc. It offers an integrated set of developer environment and tools that a developer can use to build their applications without having any clue about what is happening on background service. It offers developers a service that provides a complete software development life-cycle management, from planning to design, from building applications to deployment, from testing to maintenance etc. Everything else is abstracted away from the "view" of the developers. Platform as a service cloud layer operates like IaaS but it provides an additional level of pay for use functionality required. The PaaS service users transfer even more costs from initial investment needs to operational and functional expenses but must admit the additional constraints and possibly some degree of lock-in posed by the additional functionality layers [19]. The use of virtual processing system act as a mechanism in the PaaS layer in Cloud computing. Virtual machines must be safeguarded against different harmful security attacks such as cloud malware. So during the data transfer over network channels, it is must to maintain the integrity of applications and enforce accurate authentication checks for the secured transfer of data.

Software as a Service: Another well-known distribution model called Software as a Service is a system in which software applications are provided by a third party vendor or service provider and made available to users over the Internet. It removes the need for organizations to install and run applications on their own computers or in their own data centers and eliminates the expense of hardware acquisition, installation, provisioning, and maintenance, as well as software licensing, and support. SaaS is becoming an increasingly widespread delivery model as primary technologies that support online web services and service-oriented architecture (SOA), mature and new developmental approaches become popular. SaaS is also often associated with a pay-as-you-go payment licensing model. In the meantime, broadband network service has become increasingly available to support user access services from more areas around the world. SaaS is most often implemented to provide business software functionality to enterprise customer sat any required time and at low cost while allowing those customers to obtain the same benefits of commercially licensed, internally operated software without the associated complexity of installation, management, licensing, support, and high initial cost. The architecture of SaaS-based applications is specifically designed to support many concurrent users (multitenancy) at once. In Software as a service model, the applications are accessed using web browsers over the Internet, therefore, web browser security is crucially important. Security architect needs to consider various methods of securing SaaS applications such as Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and the available methods and facilities used in enforcing protection to data transmitted over the Internet [8]. By merging all the above three types of cloud Service Delivery Models one can get a holistic cloud environment surrounded by connectivity devices coupled with information security themes. This also includes virtualized physical resources, virtualized infrastructure, and virtualized middleware platforms, and various business applications are being provided and consumed as services in the Cloud [20-26]. Cloud vendors and clients need to preserve cloud computing security issues at all interfaces.

4. Challenges of Cloud Computing Model:
The adoption and usage of cloud computing model by organizations for the optimum management of their computing resources are associated with numerous challenges because organizational users are still sceptical about its authenticity. Based on a survey conducted by International Data Corporation during 2008, the major challenges that prevent the usage Cloud Computing model by organizations are as follows:

Security Challenges: The security aspect has played an important role in hindering the acceptance of Cloud computing. Storing organizational crucial data, executing them using a software on someone else's hard disk, and using someone else's processor appears daunting to many. Well-known security issues such as data loss,

International Journal of Engineering Research and Modern Education (IJERME)
Impact Factor: 6.525, ISSN (Online): 2455 - 4200
(www.rdmodernresearch.com) Volume 2, Issue 1, 2017

phishing, running remotely on a collection of machines will cause serious threats to organization's data and software. Moreover, the multi-tenancy model and the collective computing resources in cloud computing has introduced new security challenges that require advanced security techniques to tackle with. For example, hackers can setup a Cloud service and provide it to client organizations with more reliable infrastructure services at a relatively cheaper price for them to start an attack [9].

Costing Model Challenges: Cloud users must consider the tradeoffs amongst computation, communication, and integration. Migration to the Cloud model can significantly reduce the infrastructure cost, but it does raise the cost of data communication, i.e. the cost of shipping an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher in many cases. This cost is particularly prominent if the consumer organization uses the hybrid cloud deployment model where the organization's data is distributed amongst a number of public/private/community clouds. Thus, on-demand cloud computing resource usage makes sense only for CPU intensive jobs [9].

Charging Model Challenges: The flexible computing resource pool has made the cost investigation significantly more convoluted than standard data centers, which often calculates their cost based on utilization of static computing. Moreover, creating virtual server has become the unit of cost analysis for the client organizations rather than the underlying physical server. For SaaS cloud providers, the cost of developing architecture in which a single instance of a software application serves multiple customers within their offering can be very substantial. Which include: reconstruction of the software that was originally used for single-customer, the cost of providing new features that allow for intensive customization of software, performance and security enhancement for concurrent multi-user access, and dealing with complexities induced by the above changes in the software. Consequently, SaaS providers need to consider the exchange between the provision of multi-occupancy and the cost reduction yielded by multi- occupancy such as reduced overhead through paying off, reduced number of on-site software licenses, etc. Therefore, a strategic and feasible charging model for SaaS provider is critical for the gainfulness and supportability of SaaS cloud providers in cloud environment [9].

Service Level Agreement (SLA) Challenges: In spite of the fact that cloud consumer organizations do not have control over the fundamental computing resources, they do need to guarantee the quality, accessibility, dependability and performance of provided resources when consumer organizations have relocated their core business activities onto their entrusted cloud. In other words, it is essential for consumer organizations to obtain a guarantee from service providers on service delivery. Usually, these are given through Service Level Agreements (SLAs) negotiated between the providers and users of cloud. The issue in this is the definition of SLA details in such a way that has suitable level of granularity, specifically the tradeoffs amongst articulacy and multifaceted nature, so they can cover a large portion of the client's desires and is generally easy to be weighted, confirmed, assessed, and implemented by the resource allocation and management mechanism on the cloud. In addition, different types of cloud offerings (IaaS, PaaS, and SaaS should characterize distinctive SLA meta specifications. This also causes a number of implementation issues for the cloud providers. Furthermore, advanced SLA mechanisms need to always consider and incorporate user feedback and customization highlights into the SLA assessment framework [16].

Cloud Interoperability Issue Challenges: At present, each cloud offering has its own way on how cloud clients, applications, and users collaborate with the cloud, leading to the "Foggy Cloud" phenomenon. This extremely prevents the advancement of cloud ecosystems by constraining vendor locking, which restricts the ability of users to choose from alternative vendors/offering simultaneously in order to improve resources at different levels within an organization. More importantly, proprietary cloud application programming interface makes it extremely hard to coordinate cloud services with an organization's own existing legacy frameworks. The primary aim of interoperability is to understand the flawless transfer of data across clouds and between cloud and local applications of an organization which works as client. There are a number of levels where the interoperability is essential for cloud computing for smooth functioning. First, need to optimize the IT asset and computing resources of the organization often need to keep in-house IT assets and capabilities associated with their core competencies while outsourcing marginal functions and activities on the cloud. Second, more important for the purpose of optimization is an organization may need to outsource a number of marginal functions to cloud services offered by different service providers. Standardization emerges to be a good solution for interoperability problem. However, as cloud computing just begins to take off, the interoperability issue has not shown up on the pressing agenda of major industry cloud vendors [9].

5. Conclusion:

In this paper security considerations and challenges which are faced by the Cloud computing are highlighted. Cloud computing has the potential to become a pioneer in advancing a secure, virtual and financially reasonable IT solution in the future. Although Cloud computing can be seen as a new trend which is set to transform the way we use the Internet, there is much to be cautious about. There are numerous new technologies developing at a rapid rate, each with innovative progressions and with the capability of making

human's lives simpler. However, the user must be very cautious to understand the security risks and challenges posed in utilizing these emerging technologies.

6. References:

1. Gens, F. (2009). New IDC IT Cloud Services Survey: Top Benefits and Challenges, IDC eXchange, viewed 18 February 2010.
2. Brodkin, J. (2008). Gartner: Seven cloud-computing security risks. InfoWorld, 2008, 1-3.
3. Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010.
4. European Network and Information Security Agency. (2009). Cloud Computing: Benefits, risks and recommendations for information security. ENISA.
5. Kandukuri, B. R., & Rakshit, A. (2009). Cloud security issues. In Services Computing, 2009. SCC'09. IEEE International Conference on (pp. 517-520). IEEE.
6. P. Kresimir and H. Zeljko, "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.
7. Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. IEEE Security & Privacy, 9(2), 50-57.
8. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
9. Ramgovind, S., Eloff, M. M., & Smith, E. (2010). The management of security in cloud computing. In 2010 Information Security for South Africa (pp. 1-7). IEEE.
10. Almorsy, M., Grundy, J., & Müller, I. (2010). An analysis of the cloud computing security problem. In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov.
11. Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org [Mar.19, 2010]
12. Puthal, D., Sahoo, B. P. S., Mishra, S., & Swain, S. (2015). Cloud computing features, issues, and challenges: a big picture. In Computational Intelligence and Networks (CINE), 2015 International Conference on (pp. 116-123). IEEE.
13. Hussein, N. H., & Khalid, A. (2016). A survey of Cloud Computing Security challenges and solutions. International Journal of Computer Science and Information Security, 14(1), 52.
14. Jafarpour, S., & Yousefi, A. (2016). Security Risks in Cloud Computing: A Review.
15. Sarkar, S., & Vimal Kumar Bharadwaj, P. G. (2016). Security Issues and Challenges in Cloud Computing.
16. Dubey, A. (2016). Cloud Computing and Its Security Issues. International Journal, 4(7).
17. Arnold, S. (2009). Cloud computing and the issue of privacy. KM World, 14-22.
18. A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." Platform Computing, pp6, 2010.
19. Global Netoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009].
20. Lenk, A., Klems, M., Nimis, J., Tai, S., & Sandholm, T. (2009). What's inside the Cloud? An architectural map of the Cloud landscape. In Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing (pp. 23-31). IEEE Computer Society.
21. Weinhardt, C., Anandasivam, A., Blau, B., & Stosser, J. (2009). Business models in the service world. IT Professional Magazine, 11(2), 28.
22. Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). On technical security issues in cloud computing. In 2009 IEEE International Conference on Cloud Computing (pp. 109-116). Ieee.
23. Leavitt, N. (2009). Is cloud computing really ready for prime time. Growth, 27(5), 15-20.
24. Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). On technical security issues in cloud computing. In 2009 IEEE International Conference on Cloud Computing (pp. 109-116).
25. Soghoian, C. (2010). Caught in the cloud: Privacy, encryption, and government back doors in the web 2.0 era. J. on Telecomm. & High Tech. L., 8, 359.
26. Aithal, P. S. & Pai, V. T. (2016). Concept of Ideal Software and its Realization Scenarios. International Journal of Scientific Research and Modern Education (IJSRME), 1(1), 826-837. DOI: http://doi.org/10.5281/zenodo.160908.