African Scholars Multidisciplinary Journal (ASMJ), Vol.4, August 2023. Pg.219- 226

SECURITY ISSUES IN CLOUD COMPUTING: CHALLENGES AND SOLUTIONS

MADUMERE, SMART ONYEMAECHI (PhD)
ALVAN IKOKU FEDERAL UNIVERSITY OF EDUCATION, OWERRI IMO STATE.

Abstract
Cloud computing services enabled through information communication technology delivered to a customer as services over the Internet on a leased basis have the capability to extend up or down their service requirements or needs. In this model, the infrastructure is owned by a third party vendor and the cloud computing services are delivered to the requested customers. Cloud computing model has many advantages including scalability, flexibility, elasticity, efficiency, and supports outsourcing non- core activities of an organization. Cloud computing offers an innovative business concept for organizations to adopt IT enabled services without advance investment. This model enables 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. Even though organizations get many benefits of cloud computing services, many organizations are slow in accepting cloud computing service model because of security concerns and challenges associated with management of this technology. Security, being the major issues which hinder the growth of cloud computing service model due to the provision of handling confidential data by the third party is risky such that the consumers need to be more attentive in understanding the risks of data breaches in this new environment. In this paper, we have discussed the security issues, the challenges and the opportunities in the adoption and management of cloud computing services model in an organization.

Keywords: *Cloud computing model, Security issues in cloud computing, Cloud computing services, Challenges in cloud computing model, Opportunities cloud computing in resource management.*

Introduction

The Internet has been used on system graphs since several years 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 tarts 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 (Kandukuri, & Rakshit, 2009).

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 (Grobauer, Walloschek, & Stocker, 2011).

The Concept of Cloud Computing

According to Cloud Security Alliance (CSA) (2010), cloud computing means that instead of all the computer hardware and software you're using sitting on your desktop, or somewhere inside your company's network, it's provided for you as a service by another company and accessed over the Internet, usually in a completely seamless way. Exactly where the hardware and software is located and how it all works doesn't matter to you, the user-it's just somewhere up in the nebulous cloud that the Internet represents.

Cloud computing is a buzzword that means different things to different people. For some, it's just another way of describing IT (information technology) outsourcing; others use it to mean any computing service provided over the Internet or a similar network; and some define it as any bought-in computer service you use that sits outside your firewall.

Advantages of Cloud Computing

According to Gens (2009), the advantages of cloud computing includes;

It's managed

Most importantly, the service you use is provided by someone else and managed on your behalf. If you're using Google Documents, you don't have to worry about buying umpteen licenses for word-processing software or keeping them up-to-date. Nor do you have to worry about viruses that might affect your computer or about backing up the files you create. Google does all that for you. One basic principle of cloud computing is that you no longer need to worry how the service you're buying is provided: with Web-based services, you simply concentrate on whatever your job is and leave the problem of providing dependable computing to someone else.

It's "on-demand"

Cloud services are available on-demand and often bought on a "pay-as-you go" or subscription basis. So you typically buy cloud computing the same way you'd buy electricity, telephone services, or Internet access from a utility company. Sometimes cloud computing is free or paid- for in other ways (Hotmail is subsidized by advertising, for example). Just like electricity, you can buy as much or as little of a cloud computing service as you need from one day to the next. That's great if your needs vary unpredictably: it means you don't have to buy your own gigantic computer system and risk has it sitting there doing nothing.

It's public or private

Now we all have PCs on our desks, we're used to having complete control over our computer systems and complete responsibility for them as well. Cloud computing changes all that. It comes in two basic flavors, public and private, which are the cloud equivalents of the Internet and Intranets. Web-based email and free services like the ones Google provides are the most familiar examples of public clouds. The world's biggest online retailer, Amazon, became the world's largest provider of public cloud computing in early 2006. When it found it was using only a fraction of its huge, global, computing power, it started renting out its spare capacity over the Net through a new entity called Amazon Web Services. Private cloud computing works in much the same way but you access the resources you use through secure network connections, much like an Intranet. Companies such as Amazon also let you use their publicly accessible cloud to make your own secure private cloud, known as a Virtual Private Cloud (VPC), using virtual private network (VPN) connections

Security Issues in Cloud Computing

During 2008, the IT consultancy - 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 withdraw an agreement and all information if the present provider is bought out by another firm (Brodkin, 2008).

Security Issues in Cloud Computing Model

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:

(1) Private Cloud Model

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 center. 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 (Arnold, 2009).

According to Kresimir, & Zeljko, (2010), 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.

(2) Public Cloud Model

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 (Dubey, 2016). 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.

(3) Hybrid Cloud Model

According to Hussein & Khalid (2016), 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 architects 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.

Cloud Computing Service Delivery Models

According to Subashini & Kavitha (2011), 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).

(1) 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. IaaS and other associated services have enabled startups 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 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.

(2) 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 (Lenk, Klems, Nimis, Tai & Sandholm, 2009). 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.

(3) 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 customers at 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 (Ramgovind, Eloff, & Smith, 2010).

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 skeptical 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:

(1) Security Challenges: The security aspects 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, 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 set up 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 (Puthal, Sahoo, Mishra & Swain, 2015).

(2) 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 (Almorsy, Grundy & Müller, 2010).

(3) 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 (Jafarpour & Yousefi, 2016).

(4) 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 (Sarkar & Vimal, 2016).

(5) 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 (Jensen, Schwenk, Gruschka & Iacono, 2009).

Solutions for Cloud Computing Model

1. **Cost Savings to the Management:** It is the most cost efficient method to use, maintain and upgrade the IT setup. An organization can undoubtedly get a financially savvy and on- premise IT services through cloud computing without the need to buy or assess hardware equipment or software or to enlist interior IT staff to keep up and benefit in-house infrastructure. The software license costs to a company a lot in terms of finances. Adding up of the license fees for multiple users can prove to be very expensive for the organizations. On the cloud, is accessible at considerably less expensive rates and subsequently, can altogether bring down the organization's IT costs. As a result, the organization can focus on critical tasks without having to incur additional costs with regard to IT staffing and training.
2. **Pay as per Use:** There are many one-time- payment or pay-as-you-use options available, which makes it very reasonable for the consumer company. The consumer company can demand for more cloud resources when required and can release when they are not in use.
3. **Unlimited Storage Space:** Storing information on the cloud gives consumer almost unlimited storage space. Hence, no more need to worry about running out of storage space. (e.g. Google Drive)
4. **Supports Green Computing:** The more efficient use of computer resources to help the environment and promote energy saving. Usage of ready-made computing resources tailored to an organization's needs certainly helps it to reduce electricity expenses. While it saves on electricity, it also saves on resources required to cool off computers and other components. This reduces the emission of dangerous materials into the environment.
5. **Scalability / Flexibility:** Organizations can begin with a small deployment on cloud and can develop quickly, then scale it back if required. Additionally, the adaptability of cloud computing permits consumer organizations to utilize additional resources as required, empowering them to fulfill their necessities.
6. **Backup and Recovery:** Services using multiple redundant backup sites, which can support business continuity and disaster recovery. Since all data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device.

7. **Work from anywhere and Mobile Accessible:** The access to the information is from anywhere using Internet connection with proper credentials and access rights. This convenient feature allows the user to move beyond time zones and geographic location issues and increased productivity due to systems accessible in an infrastructure available from anywhere.
8. **Quick Deployment:** Cloud computing gives the benefit of quick deployment of sought or required setup. The whole framework setup can be completely functional within a couple of minutes, condition the correct sort of innovation that client needs are accessible. Programmed Software Integration is simple as user/decision maker needs to handpick those services and programming applications that are best suit for that organization. Access to data is through APIs that does not require application installations on to PCs.

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.

References

Almorsy, M., Grundy, J., & Müller, I. (2010, November). An analysis of the cloud computing security problem. In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov.

Cloud Security Alliance (CSA). Available: http://www.cloudsecurityallia nce.org [Mar.19, 2010]

Gens, F. (2009). 'New IDC IT Cloud Services Survey: Top Benefits and Challenges', IDC eXchange, viewed 18 February 2010.

Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. IEEE Security & Privacy, 9(2), 50-57.

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.

Jafarpour, S., & Yousefi, A. (2016). Security Risks in Cloud Computing: A Review.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In 2009 IEEE International Conference on Cloud Computing (pp. 109-116).

Kandukuri, B. R., & Rakshit, A. (2009, September). Cloud security issues. In Services Computing, 2009. SCC'09. IEEE International Conference on (pp. 517-520). IEEE.

Lenk, A., Klems, M., Nimis, J., Tai, S., & Sandholm, T. (2009, May). 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).

Puthal, D., Sahoo, B. P. S., Mishra, S., & Swain, S. (2015, January). Cloud computing features, issues, and challenges: a big picture. In Computational

Ramgovind, S., Eloff, M. M., & Smith, E. (2010, August). The management of security in cloud computing. In 2010 Information Security for South Africa (pp. 17). IEEE.

Sarkar, S., & Vimal Kumar Bharadwaj, P. G. (2016). Security Issues and Challenges in Cloud Computing.

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.