International Journal of Innovative Information Systems
& Technology Research 9(3):58-66, July-Sept., 2021

© SEAHI PUBLICATIONS, 2021 www.seahipaj.org ISSN: 2467-8562

Cloud Computing: Review of Architecture, Security Risks, Threats and Countermeasures

Mission Franklin & Ojekudo, Nathaniel Akpofure

Department of Computer Science,
Ignatius Ajuru University of Education,
Rumuolumeni, Port Harcourt, Rivers State, Nigeria

ABSTRACT

The paper explored the vast literature on the subject of cloud computing architecture, security risk, threats and countermeasures, to critically analysis the risks factors and threat vectors in cloud ecosystem and enumerated the risks connected with cloud services deployment models. At the same time enlisted cloud security strategies to minimize the risks and provided countermeasures to limit the attack vectors in the cloud computing space. We draw conclusions of the adoption of an integrated approach to securing cloud resources and infrastructure, and making recommendations for stable and reliable cloud computing ecosystem.

Keywords: Cloud computing, Information Technology, Service provider, Service consumer

INTRODUCTION

Cloud computing represents a computing architectural model of aggregate Information Technology (IT) resources, to express a multi-tenancy approach to utilization of sharable resources for the benefits of the service providers and the consumers. Sidella (2012) described Cloud computing as computing model, consisting of hardware, service components, networks and software which supports the development of cloud services and delivery of same via internetwork. In a typical cloud computing model, computing resources are provided on demand basis according to changing desires of the client. (Tang, 2014).

In cloud computing the resources that are aggregated and provided in the cloud are consumable by the cloud consumer. This is a multi-tenancy approach where services provided are consumed through subscriptions. With this approach the service consumer does not need to invest so much financial resources to acquire the infrastructure required and the services, as provided by the cloud service provider. Several organizations require data storage services and cloud computing efficiently satisfies that need within a short time frame, minimal cost, and flexibility. (Qaisar & Khawaja, 2012).

Cloud computing has different deployment models which describes the relationship between the cloud service consumers and the cloud service producers. According to NIST Cloud Computing Security Reference Architecture, there are four cloud deployment models: Public, Private, Hybrid, Community (NISTCCSRA, 2013). Therefore a consumer may have access to one or more of the deployment models.

Cloud computing architecture has numerous benefits in relation to cloud computing. However, there are various security challenges associated with cloud computing models which service consumers and providers are faced with. These issues exist as providers ensure to maintain confidentiality/privacy, reliability and integrity for the consumers of the services (Qaisar & Khawaja, 2012). While these security issues exist, there are countermeasures that must be adopted to reduce the security risk associated with these issues and find standard procedures and mechanisms to foil attempts at creating vulnerabilities in the cloud and disruption of service (Sidella, 2012).

Statement of the problem

The challenges of cloud infrastructure and services are the threats to vulnerabilities that are inherent in the system, which is common in a networked environment. The risk associated with adopting a cloud service model. How the cloud service provider ensures that services provided do not compromise the data privacy of consumers, as well as ensuring security of consumers information and related services.

Aim and Objectives

The aim of this paper is to highlight the intricacies of the cloud architecture and its security risks, threats and strategies to mitigate the challenges. The paper propose to (i) Review existing body of literatures on the subject of cloud computing, (ii) Highlight the architecture framework, service models and deployment models, (iii) Highlight the security challenges cloud computing services are exposed to, (iv) Develop strategies to counter know threats and mitigation risks in the infrastructure

Review of Related Works

Cloud computing has provided services beyond the boundaries of the premises for consumers in different parts of the global, without limitation due to geographical boundaries. This architecture has been made possible due to the accessibility of the global information highway, the internet. Cloud computing integrates technology resources to be delivered to consumer in a multi-tenancy fashion to users. Cloud computing has grown as a widely held and global concept for service base computing architecture where IT resources are delivered as solution in the form of service (Kong et al., 2018).

NISTCCRS(2013) defines “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. There is a huge growth prospect for the Cloud industry (Tang, 2014), and has provided its community of users different services. There are five important features of a cloud model, four deployment models and three service models (NISTCCRS, 2013).

The cloud service models are classified into three classic models: (i) Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) (Qaisar & Khawaja, 2012; Tang, 2014; Pandey & Farik, 2015). The following services are enumerated (NISTCCRS, 2013).

- **Software as a Service (SaaS).** These are applications operating within the infrastructure which is made available for use by the service consumer. These applications are made available from different clients IT resources via a web browser or a thick client.
- **Platform as a Service (PaaS).** This is a platform to enable the consumer of the service to deploy applications on the could infrastructure, application created using libraries, languages, tools and services of the service provider.
- **Infrastructure as a Service (IaaS).** This is a provision of access to the platform to allow the consumer of services of networks, storage, processing etc., to enable the consumer to applications and operating systems that necessitates service provision through the provision of the infrastructure.

In the services model enumerated, the management of the cloud infrastructure is beyond the control of service consumer. For instance in Saas, (operating systems, network, servers, storage, application configuration settings. Etc.), Paas (servers, storage, network, operating systems, except for deployed applications) are not within the control and management of consumer, while in Iaas (storage, applications and operating systems have inadequate control over components of the network, which are resident within the control of consumer.

Cloud infrastructure also has some deployment models, which define the connection between Service provider and Service consumer(s). In NISTCCSRA (2013) specification documentation for security architecture identified four cloud arrangement models: Private, Community Public and Hybrid. Public cloud is provisioned to be used by generality of the people in public space. Although the cloud infrastructure may exists with the buildings of the service provider. Public cloud could be operated, managed, or possessed by a corporate, governmental agency or academic organization. Where a cloud architecture that is established by a specific organization is made available for use exclusively is called a private. Such service is useable by different consumers. A service of this nature could be operated, rented or facilitated for use be a specific organization. Also such physical infrastructure could be place with or outside the premises of the owner. The entire architecture and service is kept for a private use (Kong et al., 2018).

Community cloud is kept for use by select group of people from a precise community of consumers from different groups with common objectives. The infrastructure as in the case of a community cloud, may be owned by multiple organizations and managed by a party with the community. The physical infrastructure could be located within the facility of the owners or outside premises of the owners. In some cases, multiple self-governing cloud resources may be joined together to support the activities of data transfer and applications interfacing different clouds (Kong et al., 2018).

Hybrid cloud is the establishment of integration of multiple clouds from separately existing cloud structures. With novel features as a separate entity, the cloud is joined by a standard technology that facilitated application interoperability and data portability (NISTCCSRA, 2013).

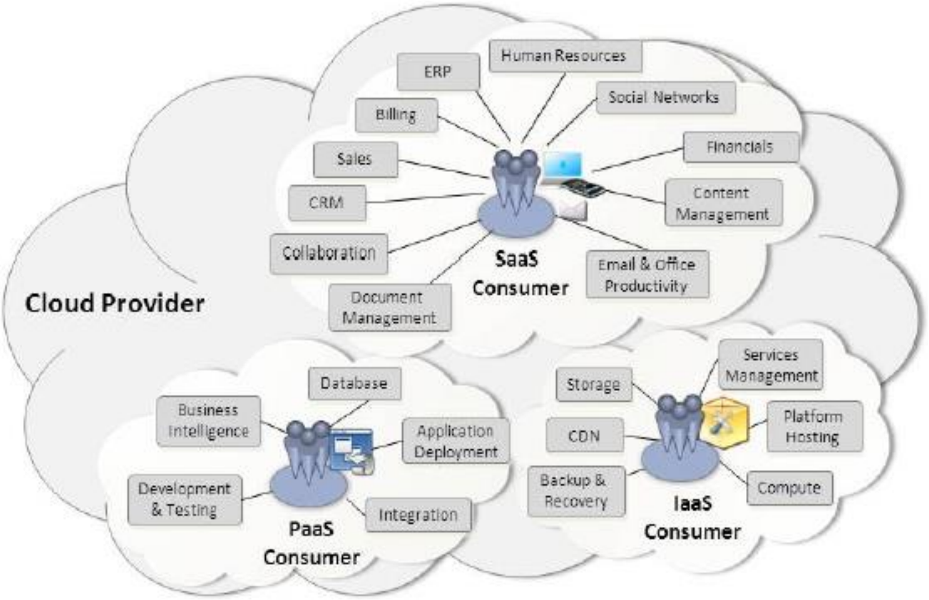

Figure 1: Cloud Computing consumable services (NIST SP500-292) (Source: NISTCCSRA, 2013)

Cloud Computing Characteristics

Cloud architecture and services possesses certain features that define the characterization of cloud architecture. NIST Cloud Computing Standards Roadmap NISTCCSR (2013) specifies the following characteristics that define a cloud infrastructure which includes:

- **Self-service-on-demand.** This is an automatic individualistic provisioning of capabilities of computing (network storage and server-time) resources without the need for human intervention.
- **Broad network access.** The cloud should make features and capabilities available through the network accessible via tools that promote use by different thick or thin client (e.g., mobile device, tabs, desktops).
- **Resource pooling.** The computing resources of the cloud are accessible to serve multiple consumers on a need basis. The different virtual and physical resources (storage, processing, memory, and network bandwidth) are assigned actively according to demands of the consumer.
- **Location independence:** The location of the service is virtually out of the authority of the customer. The consumer may only have idea of possible locations of the infrastructure.

- **Rapid elasticity.** The services and capabilities provisioned and released are elastic and automatic in some cases. Also based on the demand for resources, the infrastructure should be able to scale rapidly and appropriated dynamically.
- **Measured service.** The cloud service ensured optimized resource utilization through leverage of measuring capability of service type at some level.

The utilization of resources can be observed, measured, audited, and informed. These measures provide evidence of service utilization for both the provider and consumer of the service.

Tang (2014) argued that other useful characteristics of cloud services include: Scale of enormous application, as many applications are built for the cloud infrastructure. The virtualization capabilities are very powerful to ensure the provisioning different users with performance capabilities. The cloud environment also supports high scalability, with dynamic resources management. The high reliability of the cloud has necessitated its common usage and data integrity is maintained across the platform. The application of a "cloud" has strong compatibility with interoperability, while keeping cost moderately affordable and user accessibility is in accordance to purchased services.

Despite the benefits that cloud computing has generated through its service oriented-multi-tenancy approach, is has also open up a worm of effect and issues to privacy and security of information of user, and in the course of improvement of asset protection efficiency(Tang, 2014). For instance, the virtualization of the software layer could lead to a vulnerabilities of shared physical resources, under the control of the server, including virtual machines (VMs), memory, and data (Bhadoria, 2015). In cloud computing, the service consumer neither controls nor manages the underlying cloud infrastructure.

The service provider would normally have authority of the infrastructure. Therefore several security risk exist on the usage of the cloud infrastructure, some at the provider and others at the consumer (Qaisar & Khawaja, 2012).

In SaaS, the burden of security lies on the cloud provider. The responsibility for security compliance and liabilities are within the provider's domain. This is because the model is based on elevated level of an integrated role. And minimal control and extensibility on the service model is within the consumer authority. The security provisions in IaaS are shared between the consumer and the provider. This is because PaaS offers consumer control and greater extensibility and has less advanced attribute. IaaS also offers greater user control when compared in terms of security than the other models.

NISTCCSR (2013). In a public cloud, level of control available to a user is marginal, compared to a private cloud where the user control is maximized. When compared to hybrid and community cloud, the level of control lies between public and private (Sidella, 2012).

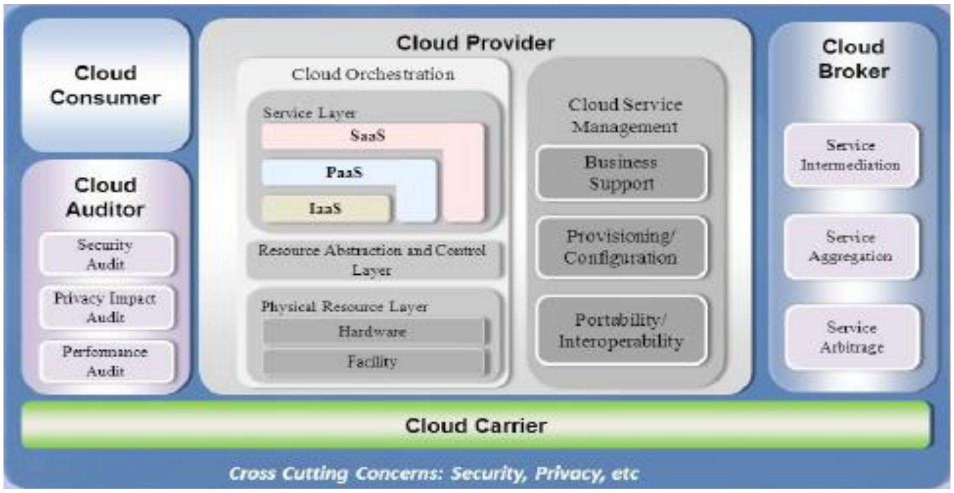

Figure 2: The NIST Cloud Computing Combined Reference Architecture (Source: NISTCCSRA, 2013)

Security Threats in the Cloud

Generally the threats faced by cloud computing platforms are synonymous with other computing platforms. Sidella(2012) recognized several major threats that cloud computing environments are exposed to, such as : Unethical and abuse usage of cloud resources, Application Programming Interface vulnerability (API), Shared technology vulnerabilities, Malicious insiders, Unknown Risk Profile, Account, Data Loss/Leakage Service & Traffic Hijacking.

While various risks and vulnerabilities exist, the enlisted threats are common in cloud computing environment; risk factors are also present in the environment. Tang (2014) acknowledged the following risks: Inherent platform, virtualization, storage data sharing, human resources management, security, operational management, misuse, network security, interoperability, of multi-directional audit and multi-party audit. Security risks and threat are major sources of concern in cloud computing for many organizations, largely due to the dispersal of the location of the physical infrastructure and the residency of the data which is spread geographically. The data protection laws are general country depended, therefore the location of data is an issue: were data resident in a country without adequate laws to protect sensitive data, therefore making user data vulnerable (Sidella, 2012).

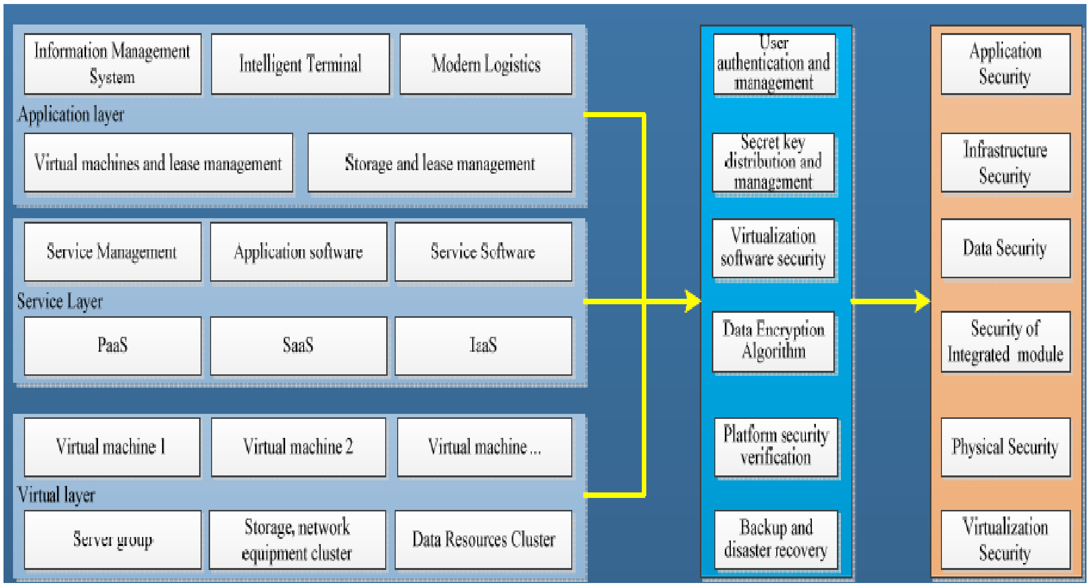
Information Management System
Intelligent Terminal
Modern Logistics
Application layer
Virtual machines and lease management
Storage and lease management
Service Management
Application software
Service Software
Service Layer
PaaS
SaaS
IaaS
Virtual machine 1
Virtual machine 2
Virtual machine ...
Virtual layer
Server group
Storage, network equipment cluster
Data Resources Cluster
User authentication and management
Secret key distribution and management
Virtualization software security
Data Encryption Algorithm
Platform security verification
Backup and disaster recovery
Application Security
Infrastructure Security
Data Security
Security of Integrated module
Physical Security
Virtualization Security

Figure 3. Cloud Computing Security Model Framework (Tang, 2014).

METHODOLOGY

The method adopted in the research was the review of existing literatures (in academics, industry and business) on the subject of cloud computing. A critical insight at the security architecture, associated risks, threats and countermeasures was explored and established. Proper analysis of the threats was carried out, and mitigation strategies to foil emerging risks profiles and attack vectors were devised. Solutions and recommendations were suggesting that would arrest the challenges in the short term, mid-term and the long term.

RESULT/DISCUSSION

The Cloud computing ecosystem describes the cloud composition and its deployment models that is the service models as well as the deployment models (NISTCCSRA, 2013). Many different Big Tech firms are providing cloud services according to the service models described earlier. Pandey & Farik (2015) itemized the different service models and their respective players in each model. SaaS has CiscoWebX, Netsuite, GoogleApps, Salesforce.com, Zoho ; PaaS has Windows Azure, GoogleApp engine, Rollbase, VMware Cloud, Force.com, Herok, Foundry; whle IaaS has Amazon web Service(AWS), Google Cloud Storage, VMWare, Rackspace. The ecosystem is a mix of the service and deployment models as shown in Table 1.

Table 1: Tabular mix of Deployment and Service models

Deployment Model	**Service Model**		
	SaaS	**PaaS**	**IaaS**
Private	*	*	*
Public	*	*	*
Hybrid	*	*	*
Community	*	*	*

The ecosystem being in the global space has challenges related to network security (Qaisar & Khawaja, 2012). There are several network performance related issues within the cloud computing ecosystem, some of such are attack vectors that impact the network in many different ways: (Denial of Service:- limits the available of service to consumers, Man in the Middle Attack:- to uncover information communicated between parties, Network Sniffing:-accessing network packets on transmission, SQL Injection Attack:- to attack database by injecting vulnerable codes into the SQL query to retrieve confidential information, Cross Site Scripting , which a security threat that originates in web applications by code injection to execute scripts in a web browser. While network related challenges exist for cloud service providers to mitigated or solve, security issues also exist in different dimension and proportions.

Qaisar & Khawaja (2012) also itemized some of the common security threats that cloud service provider are challenged with such as Malware Injection Attack, Browser Security, XML Signature Element Wrapping, Data Protection, Flooding Attacks, Incomplete Data Deletion, Locked in. In addition to the highlights above, Pandey & Farik (2015) further cited other Breaches that could result in vulnerable API, data losses, Denial of Service, Account Hijacking, Abuse of Cloud Service Malicious Insider, Shared Technology, inadequate due diligence.

Cloud Service Security Challenges

The cloud computing ecosystem is laden with security issues and challenges which the stakeholder in the system must solve while protecting their service consumers. Several attacks of different forms are initiated to upset normal operation of the infrastructure's service. Data while in storage and in transmission are compromised, violating integrity and confidentiality. Rapid increase in scale of attacks due to homogeneity and power of cloud ecosystems, malicious exploitation of vulnerability through unauthorized access to resources provisioned for another user , exploitative attacks on network resources and reconnaissance on vulnerabilities, limited capability to encrypt data in storage; Issues of inadequate or non-existent standards of cloud services leading to manageability and migration constraints on the service consumer; Exploitation attacks of cloud services due to non-transparency of audit procedures; Attacks on vulnerabilities in obsolete patches and virtual machines, Exploitative attacks due to discrepancies in worldwide privacy policies and global regulations; Insider abuse of privileges in high risk roles, interception and modification of data in-transit.

Security Objectives Implementation for Cloud Computing

NISTCCRS (2013) observed that Cloud computing services need to be secured to ensure that consumer data and information is not compromised. There are security objectives that service providers must aim at satisfying for the safety, privacy and safety of information saved in cloud.

Some of the objectives to secure the cloud services would include: (i) Prevention of unauthorized access to cloud computing infrastructure resources, (ii) consumer data protection from unauthorized monitoring, disclosure, access, and modification (iii) Deployment of internet threat free web applications for implementation in the cloud, (iv) Mitigate end-user security vulnerabilities to prevent Internet browsers attacks, (v) Initiate mechanism for access control and intrusion detection and preventive solutions , (vi)

Carry out a self-governing assessment to validate the functionality of solutions installed, (vii) Outline trust restrictions between consumers and providers, certifying the duties to implement security controls are clearly well-known., (viii) Ensure that standardized APIs are defined for use interoperability and portability to sustenance easy migration of consumers' data to other cloud. (NISTCCRS, 2013).

While the objectives mention earlier are relevant to keeping the cloud service safe for the consumer community, it is also imperative that some other factors that affects data privacy and regulatory compliance are also checked as a means of due diligence when choosing a service provider. This in-turn ensures that the security architecture: physical, logical and regulatory are in tandem with best practice. That is the way to safeguard the system security and the consumer is also protected from known and unknown vulnerability. The essence is to reduce the risk associated with cloud infrastructure and services to the barest minimum.

Sidella (2012) highlighted some important considerations. For instance, a service provider in compliance to regulation should demonstrate willingness to submit to external inspections and safety accreditations. A provider ought to be in abeyance to privacy rules of data storage and processing at specific geographic locations. The cloud service provider has in place backup and recovery policies and procedures, when and where data loss or a disaster occurs. Ensure that encryption algorithms, key lengths and hash algorithms are used to protect data in backup devices. Long-term viability of the data should also be considered; How can a cloud consumer get back data stored in the provider's storage, when the going concern is affected, ensuring that data could easily be imported into a auxiliary application, in other formats. Shared environment possess a lot of threat to cloud services, due to client's organization sharing of resources with other consumers.

Attacks posing as consumer can exploit weaknesses within the cloud space and gain unapproved access. System availability is a critical consideration.

The guarantee to provide sufficient system accessibility and quality of service during the period of cloud service operations, having the understanding that access to the infrastructure is influenced by various factors like technical issues, poor software version control, denial of service attacks, and poor change management processes.

Cloud Security Strategies

As a result of the risks and threat vectors in the cloud computing service space, there is need for comprehensive cloud security strategy. These strategies would dispel threats and mitigate these vectors with countermeasures and mechanisms to ensure cloud safety for providers' activities and consumers' service and data protection. Tang (2014) stated that a comprehensive approach to securing the cloud is through (i) Protection of the infrastructure security by ensuring physical and logical safety of device. (ii) Establishment of governance principle via laws and regulations that would safeguard the protection of the security of the associated host and network. In addition, the protection of application and its secure management is eminent, as the cloud computing virtualization portends a new set security issues, therefore virtualized security must be critically be assessed. Careful identity and access management of the service consumer to mitigate data theft, this is achievable through the application of adequate security of application security mechanism and policies of the cloud services. This will go on to prevent illegal use of cloud resources, while maintaining the security of the API, since most cloud resources security will depend on the API, as clients would access cloud resources API to interact and manage cloud services. Cloud security must innovate security measures since data security requirements of cloud and risk tolerance varies, so that the threat mitigation strategies must be adopted that keep service model safe and deployment models secure without any compromise of the security of data and privacy of consumer information.

Countermeasures for Cloud Security Threats

The security of cloud against threats necessitates counter mechanisms to proactively foil and mitigate possible attack vectors due to susceptibilities in the cloud ecosystem. The countermeasures are technical approaches to use high level of guarantee to strengthen the security protocol. Pandey & Farik (2015) identified encryption mechanism, digital signature, fragmentation-redundancy scattering, homographic, strong password , bring your own device(BYOD), encryption as possible counter measures. In the case of account hijacking, they suggested two factor authentications; identify access management guidance, dynamic credentials as countermeasures. In addition for Insecure API, the countermeasure that would reduce vulnerabilities are documentation, open authorization penetration tests, updates, security standards. Intrusion detection systems: Isolation, Net flows, Access Control list are the suggested countermeasures (Pandey & Farik, 2015). Other vulnerabilities are issues of sharing technology and malicious insiders. While proffering countermeasures, use of chain management, understanding of vendor's security, management policies, and strengthening of collaboration with supply chain stakeholders are suggested mitigation strategies to prevent attacks.

CONCLUSION

Cloud computing services under constant threats are risk for many consumers. The Cloud computing ecosystem security requires an all-inclusive security approaches and policies to safeguard the protection and reliability of cloud services. Since cloud models for service and deployment necessitates adequacy of security architecture. Cloud computing models that are secure contains several aspects of information security including cloud computing architectures in data centers, cloud services, virtualization platforms, and cloud terminal interfaces, etc., (Tang, 2014).

Security of cloud resources needs to be assessed from diverse angles of prevention, monitoring, response management and protection. Computing security in the cloud necessitates an integrated approach to govern the security framework for security of cloud services and infrastructure, where government departments, agencies, corporates and technical professionals in industry and academia would work collaboratively to establish architectural framework for cloud services. The security of cloud services through mechanisms such as authentication technology, security service level agreements, data security technology would establish a security system for cloud applications that guarantees reliability, safety and availability of cloud service without compromising confidentiality, integrity and availability.

RECOMMENDATION

Cloud computing resources security is an important aspect of the entire operation of Information technology ecosystem. Therefore an integrated approach of all stakeholders' involvement to design a security framework for adoption by cloud service providers and service consumers would safeguard and stabilize the operations of the cloud, its depended IT business ecosystem and its benefits for both provider and consumers of service and the entire community of users of cloud resources.

REFERENCES

Bhadoria, R.S.(2015).Security Architecture for Cloud Computing. Indian Institute of Technology Indore, India

Qaisar,S.,Khawaja, F.K.(2012).Cloud Computing: Network/Security Threats And Countermeasures. Interdisciplinary Journal Of Contemporary Research In Business Copy Right © 2012 Institute Of Interdisciplinary Business Research 1323 January 2012 Vol 3, No 9 Ijcrb.Webs.Com

Pandey,S., Farik,M.(2015). Cloud Computing Security: Latest Issues & Countermeasures. International Journal Of Scientific & Technology Research Volume 4, Issue 11, November 2015 ISSN 2277-8616

Kong, W., Lei, Y., Ma, J.(2018). Data security and privacy information challenges in cloud computing. Int. J. Computational Science and Engineering, Vol. 16, No. 3, 2018 215 Copyright © 2018 Inderscience Enterprises Ltd.

Harauz,J., Kaufman, L.M., Potter, B.(2009).Data Security in the World of Cloud Computing. IEEE Security & Privacy. www.computer.org/security

NISTCCSRA(2013). NIST Cloud Computing Security Reference Architecture, NIST Cloud Computing Security Working Group. NIST Cloud Computing Program, Information Technology Laboratory. NIST Special Publication 500-299

NISTCCSR(2013). NIST Cloud Computing Standards Roadmap. NIST Cloud Computing Program, Information Technology Laboratory. Special Publication 500-291, Version 2

Chen,J., Wang,Y., Wang, X.(2012).On-Demand Security Architecture for Cloud Computing. Published by the IEEE Computer Society

Sidella, P.(2012). Security Concerns And Countermeasures In Cloud, University Of Tennessee, Chattanooga

Tang,J.(2014).The Research on Cloud computing security model and Countermeasures. Applied Mechanics and Materials Vols. 511-512 (2014) pp 1196-1200. Trans Tech Publications, Switzerland, doi:10.4028/www.scientific.net/AMM.511-512.1196