International Journal of Engineering & Technology, 7 (4) (2018) 3897-3901

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet. v7i4.20742
Research paper

A Comprehensive Study of Security in Cloud Computing

Deepak Chahal [1 *], Latika Kharb [2], Akash Bhardwaj [3], Diksha Singla [4]

[1,2]Professor, [3,4] MCA Student, Jagan Institute of Management Studies (JIMS), Delhi , India
**Corresponding author E-mail:deepak.chahal@jimsindia.org*

Abstract

Cloud computing has become a popular model for reducing cost of business, improvise quality of services, and provide good & secure computing. It acts as a spectrum of substantial interest among IT professionals, technocrats & business leaders due to these proven potentials. Numerous emerging computing paradigms a.k.a database outsourcing serves as future advantages of cloud computing. With the increasing speed of its popularity, many security questions are arising with their respective solutions aiming to give a better understanding of their complex scenario, in this paper we will provide a comprehensive view over security in context of cloud computing and also provide a view of current status of security at present. To start with, we'll take a look at various Cloud computing models, cloud computing deploy-ment models, key issues in security along with challenges in provocation of permissions to various platforms.

Keywords: *Cloud Computing; Challenges; Database Outsourcing; Deployment Models; Secure Computing.*

1. Introduction

Since its inception, the cloud computing paradigm has gained the widespread popularity in the industry and academia [1]. Worldwide organizations are dealing with data security issues by using cloud computing leading to increasing of breaches as stated by silicon republic report. Security is one of the biggest obstacles that hamper the widespread adoption of cloud computing [2]. Don Smith, senior vice president of engineering and technology at Dell, encouraged companies on how they are risking their data security by moving to cloud. As cloud technology is growing faster the cost of saving and managing ease we are moving towards large scale deployment. Companies are becoming self-admiring after they are considering their data is safe behind firewall. Companies are moving towards Software-as-a-Service, Infrastructure- as-a-Service and Platform-as-a-Service encouraging them to adopt formal risk assessment. Before having faith in cloud providers, Organizations must seek information about data segregation, parties that can access it and how to control it and how migration of their data will be possible and what type of security precautions are being adopted. As per NSIT report, Cloud computing is a model for enabling 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 [3].

Comparing with IT traditional model, certain type of advantages are provided by cloud computing. 74% of IT managers along with CIOs believed cloud computing security issues are blocking them from using it, According to IDCI survey in 2009. Above 70% CTOs says due to data security and privacy concerns they are not using it, According to Garter survey in 2009. Several accidents occurred in 2009, Amazon Storage Service got interrupted in February and July twice forcing their network sites to standstill, user private information of Google Docs is leaked in March, and in May Google Gmail failed globally for 4 hours due to security breach in VMware Software virtualization for Mac version. Microsoft's Azure cloud computing went outage for 22 hours in which 45% user data is lost, forcing closing of link-up's of cloud storage vendors. In 2014, "Big Billion Day" of Flipkart's failed drastically receiving 83% more than expectations failing the server desolately, making them adopt Microsoft Azure Cloud in 2017. World's leading IT organization Microsoft, experienced a breach in 2010 allowing access to employee contact information from their offline address books. LinkedIn, Business-focused social networking site lost its information of 6 million user passwords which were published in Russian forum in 2012. The largest high-profile security breach was suffered by Apple, Leaking of private photos on internet of famous celebrities. To deal with this security breach, iCloud service urged its users to employ strong passwords and notifications system was introduced sending alerts on any suspicious activity. One of the largest data breach occurred in YAHOO exposing 500 million accounts information. Leading Business Organizations are adopting cloud services without caring taking as much preventions as they can for its data security so the moral of the story is while there is plenty to love about it, addressing the security concerns is the only way to take full advantages offered by cloud.

2. Literature Review: Cloud Computing

2.1. Various Cloud computing Models

The cloud service model is referred to as SPI (software, platform, and infrastructure) [4]. Services provided by Cloud computing are categorized into:

2.1.1. Software as a service

Software as a service is where different Application Service Provider (ASP) provides various applications of software over the Internet, making the client for ejection of installation and operation of application on their computer as well as elimination of load for perpetuation, safeguarding, support and process continuation

of the software. The vendor takes the responsibility of deployment and management of software and the processes required to run and solution is managed. The customers pay for the usage and do not own the software [5].Google Apps, Salesforce.com are some of its examples.

2.1.2. Platform as a service

Platform as a service provides transportation in computing platform and resolution stack in the absence of installing and downloading software for being used by developers, IT-Managers and end-users i.e. Platform-as-a-service in the cloud is defined as a set of software and product development tools hosted on the infrastructure [6]. It contributes an infrastructure with a remarkable assimilation to contrivance and to examine cloud applications. No need of infrastructure organization is required for user but controls the deployed applications as well as its configurations. Some of its examples are Google-App-Engine, Microsoft-Azure and Force.com.

2.1.3. Infrastructure as a service

Infrastructure as a service is defined just as distribution of hardware resources for execution of services via Virtualization technology. Creation of resources which are more readily available to applications and operating systems by offering on-demand services as well as taking the benefit of Application Programming Interface (API) for interacting in the company of hosts, switches, routers and providing potential for accumulation of new equipments in visible manner is its main purpose. Elastic Cloud Computing (EC2) of Amazon, GoGrid, and Amazon S3 are some of its examples.

2.2. Types of cloud computing

There are three types of cloud namely: public cloud, private cloud, and hybrid cloud [7]:

2.2.1. Private cloud

It can be owned by an organization existing at on-premises and off-premises providing no additional regulations, legal requirements, controlled optimization of improved security by restricting user access and network. It is more expensive and secure. Eucalyptus Systems is private cloud.

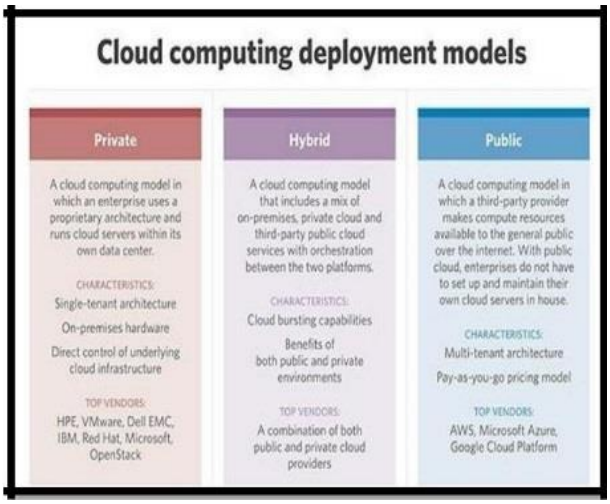

Fig. 1: Cloud Computing Models.

2.2.2. Public cloud

The third party manages the infrastructure which is provided to many users i.e. numerous enterprises works at the same infrastructure at identical time using same resources. Public clouds are managed as well as hosted by cloud providers, Customers be only charged for the resources they are using providing no authorization and authentication techniques. Microsoft Azure, Google App Engine is its various examples.

2.2.3. Hybrid cloud

The structure of more than two cloud deployment models, linking them for data transfer between each other without affecting each other.

Fig. 2: Pros & Cons of Cloud Computing.

3. Key security issues in cloud computing: a layout

IT managers look to cloud computing as a means to maintain a flexible and scalable IT infrastructure that enables business agility [8].Cloud computing contains applications, platforms and framework segments in which each fragment performs various operations by offering products for pursuit and individuals around the world. These applications include Software-as-a-Service, Viability Computing, Services provided by web, Platform-as-a-Service, Managed-Service-Providers (MSP), Service-Commerce and Internet-Integration. Frequent security circumstances are there in cloud environment which includes networking, database-management, operating systems handling, virtualization, resource scheduling, management of transactions, load balancing, controlling concurrency and managing memory i.e. why these security issues are applicable to cloud computing. Securing of data includes encrypting the information and even confirms appropriate policies to be required for sharing of data. Security issues of cloud environment are as follows:

- Accessing Servers or Applications: While accessing data by the user data access issue is the major concern. Small business organizations use cloud services provided by third parties providing access to each employee of the organization. Unauthorized users access should be taken care under these policies.
- Transmission of Data: Data is transmitted by using Encrypting techniques following SSL/TLS protocols. For data processing, application must decrypt data to maintain confidential and integration of data-transmission form with access controls such as approval, authentication and auditing for resource usage while ensuring the accessibility of Internet-facing possessions at cloud provider.
- Virtual Machine Safety: Virtualization, dynamic component of cloud i.e. can rapidly be regressed to former instances, halted and re-established. The major task of virtualization is isolation of different instances on same machine i.e. why they are difficult to maintain consistent security. Two types of virtualization, Para and Full exist in cloud computing. Complete hardware structural design replicates virtually in Full virtualization whereas modification of operating system

is required to run concurrently with other operating systems in Para virtualization.

Table 1: Merits of Cloud Computing

Features	Merits
Effortless execution	Cloud hosting allows business processestokeeppossessionof identical applications and without goinginspecificationwiththe backend technicalities.
Approachability	Accessibility of data from anywhere anytime maximizes the productivity and efficiency of enterprises for easy collaborationandmultiple users sharing at multiple locations.
Reduces hardware necessity	Everything will be hosted on cloud whichdecreasesthenecessityof hardware requirements. Time to time backupshouldbedonefor preventing disasters.
Cost per shot	With cloud hosting services minimum technology cost are kept to enablebusinessesforextratime usability and resources for improving company infrastructure.
Extensible growth	Duetohighcloudscalability, resourcescanbeaddedand subtractedbasedontheirneeds which help companies to grow more and more.
Efficient recovery	Retrieval of data and applications is moreaccurateandfasterthrough cloud computing with less downtime.
Saving of Cost	Usingcloudcomputing,youcan save considerable capital costs with zeroin-houseserverstockpileand application requirements.
Reliability	On server failure hosted applications and services can easily be transited to any of the available servers which improve reliability of cloud sources.
Manageability	Cloud computing provides intensified simple IT management and maintenance potential through central administration of resources, vendor managed infrastructure and SLA backed agreements.

Table 2: Demerits of Cloud Computing

Features	Demerits
Reduces data privacy control	When services transfer to the cloud, you are Relinquishing your data and information. For an organisation that has an in-house IT staff, they will not be able to handle problems on their own.
Not getting full features	All cloud services are not the same. Some cloud providers offers limited versions and provides the popular features only, so you may not obtain every feature you want.
Less significance provided to servers	Less server handling, less staff required for handling IT problems. Redundancy removal should be done using backups and recovery.
No Redundancy	A cloud server is not redundant nor is it backed up. As technology failure can arise having a backup can work in that situation.
Bandwidth issues	For ideal performance, no large amounts of servers and storage devices should be kept into a small set of data centers.
Downtime	If your internet connection is offline, you are unable to access any of your applications, server or data from the cloud.
Security	In a multi-tenant cloud architecture where same server is used by multiple users, an unauthorized person can try to hack in order to steal data of other users on same server.
Vendor Lock-In	Organizations find it hard to drift their resources from one vendor to another. Hosting and integration of current cloud

Restricted Power	applications on another cloud platform increases compatibility and support issues. Cloud Infrastructure is owned by service providers so the customer can only control and manage applications, data and services operated. No Backend Storage Information is provided to the customer.

- Securing Network: Different types of networks such as shared-not shared, public and private as well as small or long system having plenty of security threats to deal with. Network security problem comprises of DNS and Sniffer attacks and issue of reused IP address etc. Applications that capture flowing of packets through network without encryption leaving information to be traced come under sniffer attacks; sniffer program ensures linking of data to systems on network. Assigning IP address of former user to new user is of major concern risking the security of new user due to time gap between changes of IP address and address clearing in DNS caches.

Fig. 3: Security Issues in Cloud Computing.

- Data safety: Service providers of cloud like Amazon, Elastic-Compute-Cloud (EC2) administrators have no contact to client's specimen having no access to customer instances. EC2 Administrators uses their independent cryptographically Strong-Secure-Shell (SSH) key for having access to host for their business needs. All these accesses need logging and routinely auditing. Users have to encrypt data prior to uploading to Amazon S3 so that it is not available to any unconstitutional party.
- Privacy of Data: Data privacy is the major concern of cloud environment. A private navigating committee should be made for taking decisions associated with data privacy. The main necessity is the organization preparation to meet demands of data privacy for their customers.
- Integrity of Data: Integrity monitoring plays an essential role in cloud storage which is a difficult task to maintain, it is effortlessly achieved in a standalone system in the company of single database system by maintaining database constraint and connections following ACID (Atomicity, Consistency, Isolation and Durability) property.
- Location of Data: No exact location of data centreis provided to data users and no control to physical access mechanism to provided to user to access that data. Multiple databases and applications are there in distributed systems, to preserve the integrity of transactions across several data sources than they must be handled in a secure manner using global transaction manager.
- Availability of Data: The cloud service providers must ensure the availability of data to the user at any time which involves architectural level transformations by applications and infrastructural level transformations for improving flexibility and elevated opportunity. Multi-tier architectural view should be adopted for bracing low-balance farm of application illustrations, running on multiple servers.
- Segregation of Data: Encryption of data must be provided at all stages to provide a solution to data segregation problems. Encryption schemes must be planned and debugged by experienced professionals.
- Safety of Policy and Compliances: Customer shows its trust those service providers which have external audits and security certificates. An organization must implement audit and consent to interior and exterior processes that follows the requirement categorization which must stand to fulfil customer commitment, rules and regulations, determined by business intention, inner commercial policies and checking or monitoring of all policies, procedures and progressions.
- Securing Data-Storage: To prevent information loss, the superlative practice for securing information is using cryptographic encrypting techniques and distribution of self-encryption must be performed by hard drive manufactures to provide mechanical encryption with production or nominal charge blow.
- Management of Patch: Intellect favouring nature of cloud environment generates uncertainty for managing patch services endeavour. If it is impractical or uncontrollable, remunerating control methods like "virtual patching" required measurement.

4. A comprehensive view on challenges of security in cloud environment

The process of building applications has been a journey and it varies depending on one's application requirements and purpose [9]. The research of Cloud environment address the provocation for assembling the needs of private cloud, public cloud and hybrid cloud environment construction and provocation for granting permission to application and developed platforms to use benefits of cloud. Here we have provided a comprehensive view of available security issues in cloud environment:

- Service-Level-Agreements: Various instances of an application for simulating on numerous servers are implemented by priority scheme are monitored by these agreements. Major issues such as data security, disconnections and price structures required to be occupied for caring before signing contract with the provider. The SLA specification must reflect customer's needs to address the required issues at the significant time.
- Safety and Management of Data: Cloud data is characterized as text based, unstructured or semi-structured and text which rarely appends at rare updates. The infrastructure provider must achieve confidentiality to acquire secure access and transferring and skill evaluating for verifying application safety temptation. Confidentiality is attained by cryptographic etiquettes and evaluation of skills is attained via remote attestation techniques.
- Encryption of Data: Encryption is key equipment for securing data. Storage of object is being done using decryption process once it approaches the cloud.
- Virtual Machines Migration: Virtualization provides significant benefits by enabling load balance across data centresand also provides provisions for robust and highly responsive data centres. Xen and VMWare have executed live migration of virtual machines. Avoiding hotspots is the major benefit for Virtual Machine Migration.

- Compatibility: When more than two systems work cooperatively for swapping data by utilizing the swapped data.
- Controlling Access: Management of identity and authentication is important in cloud computing. The user must be aware of the password strengths; recovery methods for password and account name, logs and audit access, these all must be taken care.
- Managing Resources: Energy saving without oblation of SLA is an admirable economic encouragement for specifics centre operators and would make a momentous involvement to environment sustainability. For achieving first-class collaboration involving energy saving and application rendering is most challenging.
- Multiple User Handling: several customers access the similar hardware, application servers as well as databases affects response times and recital for former clients. Resources are shared at each framework layer with authentic security and recital concerns in multi-tenancy application layer.
- Consolidation of Server: It is a worthwhile approach to capitalize on resource consumption while diminishing energy utilization in a cloud-computing environment and the system should swiftly respond for stuffing of resources as they arise.
- Reliable & accessible Server: Cloud computing service providers must available data at the correct time as needed by the user and the data must be correct and updated at any instant of time.
- Principles of Universal Cloud: Security derived approval in cloud environment would wrap three major areas specified as technologies, cadre or actions. Techie's standards are predictably to be determined by associations like, Jericho-Forum1 before accredited by recognised organizations like International Standard Organization (ISO2).
- Management of Manifesto: Provocation in transporting middleware potentials for build, deployed, merging or governing applications in multi-user environment, flexible as well as ductile environment. Cloud's Platform provides an assortment or podium for programmers to scribble down applications that hasten on cloud environment, or utilize service being delivered by the cloud environment or both.

5. Conclusion

As cloud offers, many advantages there are still many problems related to data security which must be taken care of. As per Gartner survey about income, emporium size for public and hybrid cloud is $59 billion and will outstretch USD 149B by 2014 having per annum growth rate of 20. Existing vulnerabilities in cloud models increases threats to hackers. Deployment models and their essential features, data security and private protection issues needs to be solved as possible, as per service delivery miniatures. Sharing of data while defending private information is a major challenge in privacy protection, typical systems such as e-commerce for storing credit data and vigour based systems for vigour related data. The potential of controlling information revealing techniques and access to that information is of major concern including stored personal information glance by mediator without agreement, or tracking the web sites visited by someone and sites being visited can collect, store or share information with others. Detachment of responsive data from non-responsive data using encryption of responsive data is the key to private protection.

References

[1] M. Sadiku, S. Musa, O. Momoh, Cloud computing: opportunities and challenges, IEEE Potentials 33 (1) (2014) 34–36.https://doi.org/10.1109/MPOT.2013.2279684.

[2] D. AB. Fernandes, L. FB. Soares, J.V. Gomes, M.M. Freire, P. RM Inácio, Security issues in cloud environments: a survey, Int. J. Inform. Sec. 13 (2) (2014), 113–170.https://doi.org/10.1007/s10207-013-0208-7.

[3] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." 2011.

[4] Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "Security in cloud computing: Opportunities and challenges." *Information Sciences* 305 (2015): 357-383.https://doi.org/10.1016/j.ins.2015.01.025.

[5] L. FB Soares, D. AB Fernandes, J.V. Gomes, M.M. Freire, P. RM Inácio, Cloud security: state of the art, in: Security, Privacy and Trust in Cloud Systems, Springer, Berlin, Heidelberg, 2014, pp. 3–44.https://doi.org/10.1007/978-3-642-38586-5_1.

[6] Alessandro Iudica, Understanding the Cloud v1.0, December 2014, IBM Education Understanding the Cloud 1, © 2013 IBM Corporation.

[7] Chahal D, Kharb L, "Data security in Cloud Computing", International Journal of Engineering and Science Invention, Vol. 6 (12), 2017, pp. 31-36.

[8] H. Yu, N. Powell, D. Stembridge, X. Yuan, Cloud computing and security challenges, in: Proceedings of the 50th Annual Southeast Regional Conference, ACM, 2012, pp. 298–302.https://doi.org/10.1145/2184512.2184581.

[9] Kharb L, "IBM Blue mix: Future development with open cloud architecture", International Journal of Information Communication and Computing Technology, Vol. 3(2), 2015, pp. 165-168.