International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

ANALYTICAL STUDY ON DEVELOPMENT OF ARCHITECTURE AND SYSTEM SOFTWARE IN CLOUD COMPUTING MODEL

Mr. Rokesh Kumar Y

Ph.D Research Scholar, Sri Satya Sai University of Technology & Medical Sciences
(SSSUTMS), Sehore, Madhya Pradesh, India.

ABSTRACT

Cloud computing is altering numerous biological communities by giving associations computing assets including simple arrangement, availability, setup, automation and adaptability. This paradigm move raises an expansive scope of security and protection issues that must be thought about. Multi-tenancy, loss of control, and trust are entering challenges in cloud computing situations. This paper surveys the current advances and a wide exhibit of both prior and best in class extends on cloud security and protection. We sort the current research as per the cloud reference architecture organization, asset control, physical asset, and cloud benefit administration layers, notwithstanding auditing the current improvements in security safeguarding sensitive information approaches in cloud computing, for example, protection threat modeling and security upgrading conventions and arrangements.

In this architecture, security is noteworthy concerns particularly in organize, host, application, and data levels. For particular application for example in cloud computing that is the significant concentration in this paper, information security is the primary concern. Due to decent variety in benefit models which are given in cloud computing, accomplishing satisfactory level of security is critical. These administration models are Software as a Service, Platform as a Service and Infrastructure as a Service. The proposed display affirms that our technique can enhance security levels in benefit situated frameworks, particularly in cloud computing applications.

I INTRODUCTION

Cloud computing is changing huge numbers of our biological systems, including healthcare. Contrasted and before techniques for preparing information, cloud computing conditions give critical advantages, for example, the accessibility of mechanized apparatuses to gather, associate, design and reconfigure virtualized assets on demand. These make it substantially less demanding to meet hierarchical objectives as associations can undoubtedly send cloud administrations.

In any case, the move in worldview that goes with the selection of cloud computing is progressively offering ascend to security and protection contemplations identifying with features of cloud computing, for example, multi-tenancy, trust, loss of control and responsibility. Thus cloud stages that handle touchy data are required to send specialized measures and authoritative shields to keep away from information security breakdowns that may bring about tremendous and expensive harms.

The cloud computing works from the idea that work done on the customer side can be moved to some inconspicuous cluster of assets on the Internet. Cloud computing applies a virtual stage with versatile assets assembling by on-demand arrangement of hardware, software, and data sets, powerfully. Cloud computing use its minimal effort and straightforwardness to the two suppliers and clients.

In any case, the Internet isn't a place that suppliers have finish control over it. In light of security concerns, cloud computing isn't worried about a few clients. As a virtual domain cloud computing has its extraordinary security dangers and these dangers are totally not the same as dangers in physical frameworks.

II MODELS OF CLOUD COMPUTING

- **Cloud Computing Service Models And Their Security Concerns**

In this area, cloud benefit models and their security concerns are examined. Each administration has its own security issues. These models depend on various SLAs that are amongst suppliers and clients.

A. Software as a Service Model

In the SaaS model, the client purchases a membership to some software item, yet a few or the greater part of the information and code lives remotely and clients can access to this services by means of web. In this model, applications could run totally on the network, with the UI living on a thin customer.

With SaaS, clients must depend intensely on their cloud suppliers for security. Level of control by suppliers is high and they are in charge of classification, trustworthiness and accessibility of their services. Clients have no obligations about anything.

B. Stage as a Service Model

This model gives the client to convey client manufactured applications onto the cloud infrastructure that are fabricated utilizing programming dialects and software instruments upheld by the supplier (e.g., Java, python, .Net). The client does not deal with the basic cloud infrastructure. PaaS supplies every one of the assets required to fabricate applications and administrations totally from the Internet, without downloading or introduce software. A defeat to PaaS is an absence of interoperability and portability among suppliers. That is, whether you make an application with one cloud supplier and choose to move to another supplier, you will most likely be unable to do as such or you'll need to pay a high cost. Likewise, if the supplier leaves business, your applications and your data will be lost. Level of control by suppliers is medium and they are in charge of trustworthiness and accessibility of their administrations. Be that as it may, clients' duty is medium and they are capable of secrecy and data protection. For instance, clients can utilize their data encryption and authentication frameworks in application level however security in different levels is in the supplier's hands and they should have the capacity to ensure that the data stays secure from different applications.

C. Infrastructure as a Service Model

IaaS model gives the advancement association a chance to characterize its own software condition. Where SaaS and PaaS are giving applications to clients, IaaS doesn't. It basically offers the hardware with the goal that your association can put whatever they need onto it. This essentially conveys virtual machine pictures to the IaaS supplier, rather than programs, and the machines can contain whatever the developers need.

Level of control by suppliers is low and they are in charge of accessibility of their administrations. Be that as it may, clients 'duty is high and they are capable of secrecy, data protection and uprightness. Fig.1 demonstrates supplier and client obligation in security of cloud service models.

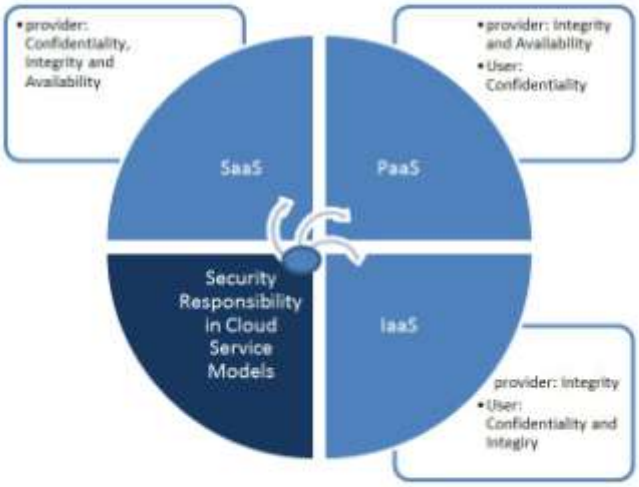

• provider: Confidentiality, Integrity and Availability
• provider: Integrity and Availability
• User: Confidentiality
SaaS
PaaS
Security Responsibility in Cloud Service Models
IaaS
provider: Integrity
• User: Confidentiality and Integiry

Fig.1 Responsibility of users and providers in security of cloud service models

DATA SECURITY MODEL

In this segment, specifically data security in cloud computing is inspected. In this day and age the most essential security issue in the utilization of cloud computing at all levels is data security issue. In data security, privacy, respectability and accessibility of data in cloud computing are alluded.

1. Data Confidentiality in Cloud

Privacy is the term used to keep the revelation of information to unapproved people or frameworks. Data classification is a standout amongst the most troublesome things to ensure in a cloud computing condition. In Cloud computing condition, two classifications of secrecy exists: classification in private cloud and privacy in public cloud. Since the secrecy in private cloud resembles a straightforward private system, we experience the public ones. In public cloud there are some potential worries about classification. To start with, are there any access controls to secure the information? Access control comprises of confirmation and approval. Today the ways suppliers guarantee that clients are satisfactorily verified when utilizing programs to access services in the cloud are constrain. They should utilize strong routes notwithstanding username and password checking. Some new ways are 2 or 3 factor confirmation or web intermediary logon and utilizing Security Assertion Markup Language (SAML) standard. With SAML, every association deals with its own clients and through trust connections share validation between locales. SAML is an exquisite answer for adaptable verification. Verification for the cloud will depend on SAML and give the double advantage of decreasing the quantity of passwords that clients must recall and additionally enhance client encounter through Single Sign on (SSO). Second, are there any data encryption techniques while data is traveling between end - user's customer and the cloud's server? Data encryption is helpful for sort of data that is put away on cloud servers and the clients don't have to list or hunt them. About data very still in IaaS encryption is a smart thought, yet scrambling data very still in that a PaaS and SaaS cloud-based application is utilizing as a repaying control isn't possible there are a few works which enables data to be prepared without being decoded, for example, homomorphic encryption and predicate encryption that are in progress.

2. Data Integrity in Cloud

Uprightness is the affirmation that the information is true and complete. The respectability of data isn't just whether the data is accurate; however whether it can be trusted and depended upon. Since 1980's we utilize "ACID" (atomicity, consistency, isolation, and durability) standards in our database administration frameworks to guarantee about data integrity however distributed computing is sufficiently new that not all specialist co-ops have attractively consolidated these data integrity standards in their answers. In addition, clients in some cases utilize such an assortment of specialist organizations that no single one of them assumes liability for guaranteeing data integrity at the level of data passage and exchange management. There are some new gauges that are identified with cloud data management and over the time they are creating. Cloud Service suppliers must utilize and grow such standard to guarantee their clients about the integrity of cloud data. Web is the media that are utilized as a part of cloud computing and regularly its passage, is web applications. A portion of the models that are creating in the present cloud world are Data Integrity Field (DIF), SNIA Cloud Data Management Interface (CDMI), and XML-based arrangements.

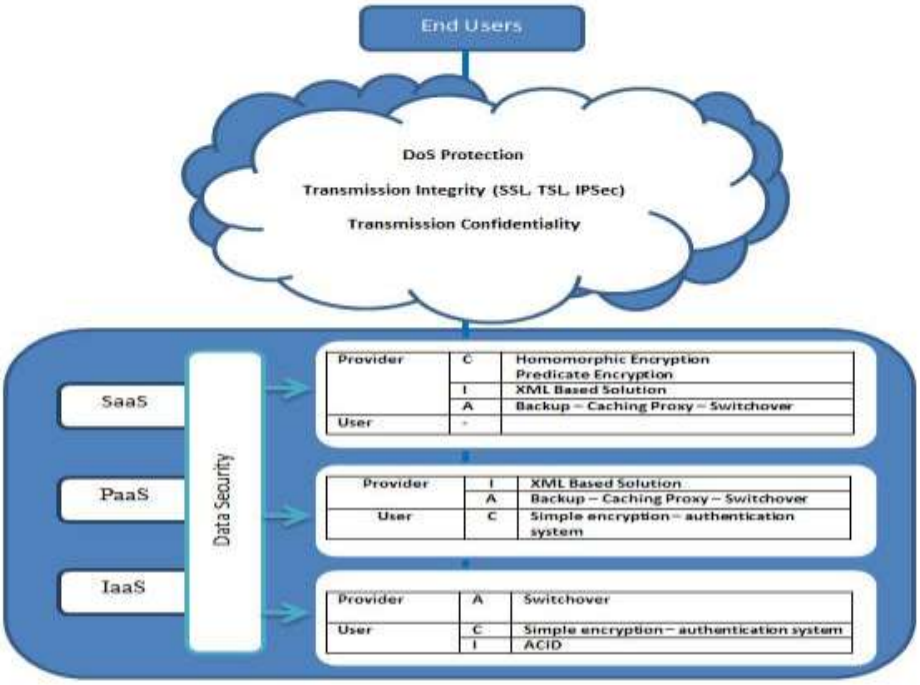
3. Data Accessibility in Cloud

Accessibility is the confirmation that the frameworks in charge of conveying, storing and preparing information are open when required, by the individuals who require them. The most risky issue in security of distributed computing is accessibility. A considerable lot of cloud service providers experienced downtime. There are some approaches to give data accessibility to clients for instance some cloud specialist co-ops do go down client data, or a superior way is a caching proxy server that can answer to benefit demands without reaching the determined server, by recovering substance spared from a past demand, made by a similar client or even different clients. Another approach to have accessibility is switchover from the online-server to the hot-standby server. These range from capacity reflecting over numerous servers which guarantees that a server disappointment never brings about data misfortune, to the capacity to recuperate from a disappointment of the cloud controller, to high - accessibility highlights incorporated with the inventory apparatuses. The capacity to effectively run two indistinguishable examples of the application on a similar cloud, or in various data focuses, give a definitive way to deal with high accessibility.

III PROPOSED MODEL

In this segment, another model for securing data in cloud computing situations utilizing the information expressed in the past area is advertised.

Open Security Architecture (OSA) gives free structures that are effectively coordinated in applications, for the security architecture group. In, there are the segments of cloud computing architectures alongside depictions of components that influence it to secure. In this paper, the model is improved to another model for data security in cloud computing. In proposed demonstrate, every one of the procedures that are helpful for securing data in all levels of cloud conditions from unsecure access are outlined. Distinctive systems for securing diverse sort of cloud service providers are depicted in Fig. 2 in subtle elements. End users access the cloud condition through web as an entry point that this section must be secure. Strong sign in to access the cloud is favorable for the cloud provider yet disadvantageous for the clients. This model must guarantee security on the end users and on the cloud alike. The cloud should be secure from any client with malignant purpose that may endeavor to access information or close down an administration. Hence, the cloud ought to incorporate a denial of service (DoS) insurance. Utilizing more data transmission and better computational power is a decent way which the cloud has copiously.


End Users
DoS Protection
Transmission Integrity (SSL, TSL, IPSec)
Transmission Confidentiality
SaaS
PaaS
IaaS
Data Security

Provider	C	Homomorphic Encryption Predicate Encryption
	I	XML Based Solution
	A	Backup – Caching Proxy – Switchover
User	-	

Provider	I	XML Based Solution
	A	Backup – Caching Proxy – Switchover
User	C	Simple encryption – authentication system

Provider	A	Switchover
User	C	Simple encryption – authentication system
	I	ACID

Fig.2 A New Model for Data Security in Cloud Computing

In the wake of signing in to cloud, it must be focus on data transmission amongst users and the cloud supplier. Encoding data before sending them by users is a decent way. For sending data, some transmission techniques like SSL, TSL and IPSec are smart thoughts. Another center point between end users and the cloud that must be secure is that nobody must tune in on the discussion between authenticated users and the cloud.

Similar mechanisms specified above can likewise ensure privacy. The cloud providers have the fundamental duty regarding ensuring data and each service providers utilize particular strategies for securing the assets. In this model as indicated by past segment, it sorts in three layers and in each layer it orders to principle part of security that is secrecy, integrity and accessibility.

IV KEY IDEAS AND TECHNOLOGIES

In the course of recent years, significant IT merchants, (for example, Amazon, Microsoft and Google) have given virtual machines (VMs), by means of their clouds, that clients could lease. These clouds use hardware assets and bolster live migration of VMs notwithstanding powerful load-adjusting and on-demand provisioning. This implies, by leasing VMs by means of a cloud, the whole data center impression of a cutting edge undertaking can be lessened from a huge number of physical servers to a couple of hundred (or even only dozens) of hosts.

While it is reasonable and savvy to utilize cloud computing along these lines, there can be issues with security when utilizing frameworks that are not given in-house. To investigate these and find suitable arrangements, there are a few key ideas and advances that are broadly utilized as a part of cloud computing that should be seen, for example, virtualization mechanisms, assortments of cloud services, and "container" innovations.

- **Virtualization Mechanisms**

A hypervisor or virtual machine monitor (VMM) is a key part that dwells amongst VMs and hardware to control the virtualized asset. It gives the way to run a few secluded virtual machines on the same physical host. Hypervisors can be sorted into two gatherings:

- **Type I:** Here the hypervisor runs straightforwardly on the real framework hardware, and there is no operating system (OS) under it. This approach is effective as it disposes of any go-between layers. Another advantage with this kind of hypervisor is that security levels can be enhanced by separating the visitor VMs. That way, if a VM is traded off, it can just influence itself and won't meddle with the hypervisor or other visitor VMs.
- **Type II:** The second sort of hypervisor keeps running on a facilitated OS that gives virtualization services, for example, input/output (IO) gadget support and memory administration. All VM Interactions, for example, IO asks for, network operations and interferes, are taken care of by the hypervisor.

Xen and kernel virtual machine (KVM) are two prominent open-source hypervisors (separately of Type I and Type II). Xen runs straightforwardly on the hidden hardware and it embeds a virtualization layer between the framework hardware and the virtual machines. The OSs running in the VMs interact with the virtual assets as though they were really physical resources. KVM is a virtualization highlight in the Linux Kernel that makes it conceivable to securely execute visitor code straightforwardly on the host CPU.

- **Cloud Computing Characteristics**

Cloud computing conveys computing software, stages and foundations as services in light of pay-as-you go models. Cloud service models can be conveyed for on-demand storage and computing power in different courses: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). Cloud computing service models have been developed amid the previous couple of years inside an assortment of areas utilizing the "as-a-Service” idea of cloud computing, for example, Business Integration-as-a-Service, Cloud-Based Analytics-as-a-Service (CLAaaS), Data-as-a-Service (DaaS). This paper alludes to the NIST cloud service models includes that are outlined in Table 1 that can be conveyed to consumers utilizing distinctive models, for example, a private cloud, group cloud, open cloud, or hybrid cloud.

Table 1 Categorization of Cloud Service Models and Features

Service Model	Function	Example
SaaS	Enables consumers to run applications by virtualizing hardware on the assets of the cloud providers	Salesforce Customer Relationship Management (CRM)
PaaS	Gives ability of sending custom applications with their conditions inside a situation called a container.	Google App Engine, Heroku
IaaS	Gives a hardware stage as an administration, for example, virtual machines, preparing, storage, systems and database administrations.	Amazon Elastic Compute Cloud (EC2)

The NIST cloud computing reference architecture, characterizes five noteworthy on-screen characters in the cloud field: cloud consumers, cloud suppliers, cloud carriers, cloud examiners and cloud agents. Each of these on-screen characters are an element (either a man or an association) that partakes in a cloud computing exchange or process, and additionally performs cloud computing undertakings.

A cloud shopper is a man or association that utilizations services from cloud providers with regards to a business relationship. A cloud supplier is a substance makes cloud services accessible to intrigued clients. A cloud auditor conducts free evaluations of cloud services, operations, execution and security in connection to the cloud arrangement. A cloud agent is an element that deals with the utilization, execution and conveyance of cloud services, and furthermore builds up connections between cloud providers and cloud consumers. A cloud transporter is an element that gives availability and transport of cloud services from cloud providers to cloud consumers through the physical systems.

The exercises of cloud providers can be isolated into five principle classifications: service sending, resource abstraction, physical assets, service administration, security and protection. Service arrangement comprises of conveying services to cloud consumers as per one of the service models (SaaS, PaaS, IasS). Resource deliberation alludes to furnishing interfaces for communicating with systems administration, stockpiling and compute assets. The physical assets layer incorporates the physical hardware and facilities that are available by means of the resource deliberation layer. Service incorporates giving business bolster, resource provisioning, arrangement administration, probability and interoperability to other cloud providers or agents. The security and protection obligations of cloud providers incorporate coordinating answers for guarantee authentic conveyance of cloud services to the cloud shoppers. The security and protection includes that are fundamental for the exercises of cloud providers are depicted in Table 2.

Table 2 Security and Privacy Factors of the Cloud Providers

Security Context	Description
Authentication and Authorization	Authentication and authorization of cloud customers utilizing pre-characterized identification plans.
Identity and Access Management	Cloud buyer provisioning and de-provisioning by means of heterogeneous cloud service suppliers
Confidentiality, Integrity, Availability	Guaranteeing the privacy of the data objects, approving data alterations and guaranteeing that resources are accessible when required
Monitoring and Incident Response	Constant observing of the cloud framework to guarantee consistence with consumer security strategies and auditing necessities.
Policy Management	Characterizing and authorizing rules for specific activities, for example, auditing or evidence of consistence.
Privacy	Protect personally identifiable information (PII) inside the cloud from adversarial assaults that expect to discover the character of the individual that PII identifies with.

The greater part of cloud computing frameworks comprise of dependable administrations conveyed through data focuses to accomplish high accessibility through excess. A data center or PC center is a facility used to house computer frameworks and related parts, for example, storage and network frameworks. It by and large incorporates excess or backup power units, repetitive network associations, cooling, and fire safety controls.

• Containers Technology

Clouds based on Linux container (LXC) innovation are thought to be cutting edge clouds, so LXCs has turned into an essential piece of the cloud computing frameworks in light of their capacity to run a few OS-level disconnected VMs inside a host with a low overhead. LXCs are based on present day kernel highlights. A LXC takes after a light-weight execution condition inside a host framework that runs guidelines local deeply CPU while killing the requirement for direction level imitating or in the nick of time assemblage. LXCs contain applications, designs and the required storage conditions, in a way like the just enough OS (JeOS).

Utilizing containers, a few applications can share an OS, doubles or libraries, which brings about noteworthy increments in effectiveness contrasted with utilizing hypervisors. For instance, the versatility of utilizations and the provisioning time of VMs are low with container innovations.

LXC advancements were presented in the 1980s, beginning with the chroot (change root) charge, and developing into to prevalent container managers, for example, Docker.

- **Chroot**: The UNIX chroot system call, which was presented as a component of UNIX version 7 of every 1979, can be considered as the initial phase in the advancement of containerization. The chroot call changes the root registry of the calling procedure to a predefined way, where the root index is known by all offspring of the calling procedure. This component is utilized by a few containers for disconnection and sharing the basic file system. Chroot is regularly utilized when building system pictures by changing root to an impermanent catalog, downloading and introducing bundles in chroot or packing chroot as a system root file system.
- **FreeBSD Jail** stretched out chroot in 1998 to give upgraded security. FreeBSD imprison settings can unequivocally confine access outside the sandbox condition by files, procedures, and user accounts (counting accounts made by the jail definition). Jail can along these lines characterize another root user, who has full control inside the sandbox; however who can't achieve anything outside.
- **Namespaces** were presented in 1992 for process-based asset isolation. Namespaces give devices to segregating the perspective of worldwide assets, for example, insights about file systems, processes, network interfaces, Inter Process Communication (IPC), host names, and client IDs. Processes in a specific namespace are undetectable to different processes since they feel that they are the main processes on the framework and in light of the fact that "connectivity" is just allowed with the parent namespace
- **Control Groups (c groups)** are kernel mechanisms acquainted by Google in 2007 with give fine-grained control by gathering forms and their youngsters into a tree structure for asset administration. Each gathering

can be doled out an undertaking for operations identified with CPU, memory, disk and network. For instance, to disconnect two gatherings, for example, applications resources and OS resources, two gatherings (assemble 1 and 2) can be made to allocate resource profiles to each gathering.

- **Linux Security Modules (LSMs)** are kernel modules which give a system to mandatory access control (MAC) security usage. In MAC usage, the overseer (client or process) doles out access controls to subject/initiator. In discretionary access control (DAC), the resource proprietor (client) doles out access controls to the subject or initiator. Existing LSM executions incorporate App Armor, SELinux et cetera to keep virtual machines from assaulting other virtual machines or the host. For this reason, approaches are utilized to characterize what activities a procedure can perform on a specific framework.

- **Containers** are based on the hardware and operating system however they make utilization of kernel highlights called chroots, c gatherings and namespaces to build a contained domain without the requirement for a hypervisor. The latest container advances are Solaris Zones, Open VZ and LXC.

In 2004, Solaris variant 10 utilized zones as offices to give secured virtualized conditions inside a solitary host. Each Solaris system incorporates a worldwide zone for both system and extensive managerial control, and may have at least one non-worldwide zone. All procedures keep running in the worldwide zone if there is no non-worldwide zone. The worldwide zone knows about all gadgets and all document systems, while non-worldwide zones don't know about the presence of some other zones. Zone-based containers give disengagement, security and virtualization. Zones are like jails with extra highlights, for example, depictions and cloning that make it conceivable to clone proficiently or to copy a current zone into another zone.

In 2005 Open VZ containers were presented utilizing a changed Linux kernel with an arrangement of expansions. Open VZ depends on the namespace and control group ideas as opposed to jails, which were utilized as a part of FreeBSD.

Later in 2008, LXC developed as a container administration device and it consolidated namespaces and control gatherings to make a completely secluded condition. It gives libraries and command-line support to empower overseers to make new containers. LXC containers can be utilized as a part of either favored (as a root user) or unprivileged (as a non-root user) modes to effectively alter kernel abilities or arrange c gatherings to fulfill the specific prerequisites.

Docker is another container administration device – it was presented in 2013 and depends on namespaces, c gatherings and SE Linux. Docker gives automation to the arrangement of containers through remote APIs and has extra highlights that make it conceivable to make standardized conditions for creating applications. This has made Docker a prevalent innovation. Making the standardized conditions is accomplished utilizing a layered image format that empowers clients to include or evacuate applications and their conditions to frame a put stock in image. Docker includes portable deployment of LXCs crosswise over various machines. In cloud terms, one can consider LXC the hypervisor and Docker as both the open virtualization machine and the provision engine.

Docker images can run unaltered on any stage that backings Docker. In Docker, containers can be made from assemble documents, for example, Web service management.

The utilization of containers in cloud figuring is progressively getting to be plainly prominent among cloud suppliers, for example, Google and Microsoft. Noteworthy enhancements in execution and security are the principle driving components for utilizing containers contrasted with virtualization utilizing hypervisors in cloud frameworks.

CLOUD SECURITY AND PRIVACY CHALLENGES

Cloud computing has raised a few security dangers, for example, data breaks, data misfortune, disavowal of service, and malicious insiders that have been broadly considered in. These dangers essentially start from issues, for example, multi-tenancy, loss of control over data and trust.

Thusly the greater part of cloud providers – including Amazon's Simple Storage Service (S3), the Google Compute Engine and the Citrix Cloud Platform - don't ensure particular levels of security and protection in their service level agreements (SLAs) as a component of the legally binding terms and conditions between cloud providers and shoppers. This implies there are critical concerns identified with security and protection that must be contemplated in utilizing cloud computing by all gatherings engaged with the cloud computing field.

➢ Security Issues in Cloud Computing

- **Multi-tenancy:** Multi-tenancy alludes to sharing physical gadgets and virtualized assets between various free clients. Utilizing this sort of course of action implies that an assailant could be on an indistinguishable physical machine from the objective. Cloud providers utilize multi-tenancy highlights to construct frameworks that can productively scale to address customers' issues; however the sharing of assets implies that it can be less demanding for an aggressor to access the objective's data.
- **Loss of Control:** Loss of control is another potential breach of security that can happen where consumers' data, applications, and assets are facilitated at the cloud supplier's possessed premises. As the clients don't have unequivocal control over their data, this makes it workable for cloud providers to perform data mining over the clients' data, which can prompt security issues. Also, when the cloud providers' reinforcement data at various data focuses, the buyers can't make sure that their data is totally erased wherever when they delete their data. This can possibly prompt abuse of the un-erased data. In these sorts of circumstances where the consumers lose control over their data, they see the cloud supplier as a black-box where they can't specifically screen the assets straightforwardly.
- **Trust Chain in Clouds:** Trust assumes a critical part in drawing in more consumers by guaranteeing on cloud providers. Because of loss of control cloud clients depend on the cloud providers utilizing trust instruments as another option to giving clients straightforward control over their data and cloud assets. In this manner cloud providers construct certainty among their clients by guaranteeing them that the provider's

operations are affirmed in consistence with hierarchical protections and standards.

V CONCLUSION

As computing steps forward to cloud computing, we should focus on security issues of it. In view of security concerns, cloud computing isn't worried about a few clients. As a virtual situation cloud computing has its uncommon security dangers and these dangers are totally unique in relation to dangers in physical frameworks. In this paper, security worries about data security in cloud computing is inspected and another model recommended for this situations. In this model security concerns and their answers are sorted in three layers of security administrations to secure getting to data assets in cloud universes.

In spite of the fact that you might exchange a portion of the operational duties to the supplier, the level of obligations will shift and will rely upon an assortment of elements, including the service delivery model (SPI), provider service-level agreement (SLA), and provider particular abilities to help the expansion of your internal security administration procedures and apparatuses. In this model, the connection between end clients and cloud service suppliers is appeared and as per their obligations in giving data security in cloud condition, another answer for it is proposed.

This paper reviewed late advances in cloud computing security and privacy examine. It portrayed a few cloud computing key ideas and advancements, for example, virtualization, and containers. We likewise examined a few security challenges that are raised by existing or pending privacy enactment, for example, the EU DPD and the HIPAA.

REFERENCES

1. J. Viega and McAffee, “Cloud Computing and the Common Man,” Published by the IEEE Computer Society. 2009.
2. A. Costanzo, M. Assuncao, and R. Buyya, “Harnessing Cloud Technologies for a Virtualized Distributed Computing Infrastructure,” IEEE Internet Computing, Sept. 2009.
3. C. Hoffa, et al., “On the Use of Cloud Computing for Scientific Workflows,” IEEE Fourth Int’l Conf. one Science, Dec. 2008.
4. I. Foster, Ian; Y. Zhao, I. Raicu, and S. Lu, “Cloud Computing and Grid Computing 360-Degree Compared,” Grid Computing Environments Workshop, pp. 12-16, Nov. 2008.
5. B. Sotomayor, et al, “Virtual Infrastructure Management in Private and Hybrid Clouds,” IEEE Internet Computing, Sept. 2009.
6. E. Talmor, “Strong Authentication for Cloud Computing,” http://sentry-com.net/blog/?p=125.
7. T. Mather, S. Kumaraswamy, and Sh. Latif, “Cloud Security and Privacy”, Published by O’Reilly Media, September 2009.

8. D. Boneh, E. J. Goh, and K. Nissim, "Evaluating 2-DNF Formulas on Ciphertexts," LNCS vol. 3378/2005, pp. 325-341, ©Springer Berlin Heidelberg, 2005.
9. J. Katz, A. Sahai, and B. Waters, "Predicate Encryption, Supporting Disjunctions, Polynomial Equations, and Inner Products," LNCS vol. 4965/2008, pp. 146-162, ©Springer Berlin Heidelberg, 2008.
10. T. Andrei, "Cloud Computing Challenges and Related Security Issues. A Survey Paper," Open Security Architecture society.
11. S. Pearson, "Privacy, security and trust in cloud computing," in Privacy and Security for Cloud Computing (S. Pearson and G. Yee, eds.), Computer Communications and Networks, pp. 3–42, Springer London, 2013.
12. E. U. Directive, "95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data," Official Journal of the EC, vol. 23, 1995.
13. U. States., "Health insurance portability and accountability act of 1996 [micro form]: conference report (to accompany h.r. 3103)." http://nla.gov.au/nla.catvn4117366, 1996.
14. "Hypervisors, virtualization, and the cloud: Learn about hypervisors, system virtualization, and how it works in a cloud environment." Retrieved June 2015.
15. Cloud Security Alliance (CS A), "The Notorious Nine: Cloud Computing Top Threats in 2013". Available at: https://cloudsecu rityalliance.org.