iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.53993

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

A Study of Hypervisor Based Virtualization and Related Major Security Issues in Cloud Computing Architecture

Neha Kumari[1], Dr. Uday Narayan Singh[2]
[1]*Research Scholar, Magadh University, Bodh-Gaya*
[2]*Associate Prof & Head, Dept. of Physics, K.S.M. College, Aurangabad (Bihar)*

Abstract: ***With the use of cloud computing, a comprehensive web platform made up of many different services may be created and used as needed. Through the internet, cloud computing offers its services in an affordable, dependable, and productive manner. By offering services on a rental basis, cloud computing lowers the expenditure required to buy gear, software, and software licenses. It offers backups to maintain multiple copies of the data and lowers the cost of licensing. With the use of cloud computing, a comprehensive web platform made up of many different services may be created and used as needed. One of today's most fascinating technologies is cloud computing, which is scalable, versatile, and can lower the cost and complexity of applications. These advantages turned cloud computing from a far-fetched notion into one of the most rapidly expanding fields of technology today. Actually, virtualization technology is based on an older technique called virtualization, which contains security flaws that need to be fixed before they influence cloud computing. Additionally, limited security features of virtualization technology are needed to protect a wide-area system like the cloud. Therefore, modifications to the conventional virtualization design are needed to create an effective security solution. In order to safeguard the cloud environment, this article suggests novel security architecture in a virtualization technology based on hypervisors.***
Key Terms: Virtualization, Cloud computing, Services, characteristics, data centre. Security Architecture;

I. INTRODUCTION

Sharing computations and resources is the main focus of the network-based system known as cloud computing. Actually, a pool of virtualized computer resources is how cloud computing is characterized. Numerous virtual machines are typically hosted on a single physical server, and cloud providers typically leverage virtualization technologies along with self-service capabilities for computing resources across network infrastructures, particularly the Internet.

The cloud computing paradigm, which is based on virtualization, enables speedy deployment and scaling-out of workloads through the quick supply of Virtual Computers or real machines.

The redundant, self-recovering, highly scalable programming paradigms supported by cloud computing platforms enable workloads to bounce back from numerous unavoidable hardware/software failures. Customers just pay for the resources they really use in the cloud; they do not have to pay for infrastructure or storage that is located locally. Because the majority of maintenance, software upgrades, configuration, and other management chores are automated and centralized at the data centre by the cloud provider responsible for them, a virtual appliance alleviates some of the most significant management challenges. Because virtualization is an older technology and lacks sufficient security features for large networks like the cloud.

The presented paper is is divided into the following 6 sections:

1) Section - 1: Presents introduction to the topic
2) Section – 2: Deals with Cloud Computing Infrastructure
3) Section – 3: Demonstrate Virtualization Concept
4) Section – 4: Elaborates Hypervisors and its prominent types
5) Section – 5: Discusses Security Issues and Reliability of Hypervisors
6) Section –6: Includes Major Threats and Security Issues with Hypervisor based Virtualization
7) Section – 7: Incorporates References

©IJRASET: All Rights are Reserved

II. CLOUD COMPUTING

A network or the internet is referred to as the "cloud." It is a system that substitutes remote internet servers for local hard drives while storing, managing, and accessing data online. Whatever you choose can be considered data, including files, photos, documents, audio, video, and more. Similarly, other computing and network services, such as compute service, infrastructure, platform and bandwidth services are available for the cloud users on demand and in self-service mode.

A. Characteristics of Cloud Computing

The principal features of Cloud Computing are:

1) *High Scalability:* Cloud computing allows large-scale "on-demand" resource provisioning without the need for IT engineers during peak loads.
2) *High Availability:* Due to the low likelihood of infrastructure failure, server availability is high and more reliable.
3) Agility: A distributed computing environment is used by the cloud. Users share resources, and it operates quickly.
4) *Cost as Pay-per-Use:* Application Programming Interfaces (APIs) are made available to users so they can use them to access cloud services and pay for those services as they are used.
5) *Multi-tenancy:* By sharing a common infrastructure, cloud computing enables multiple users and applications to operate more effectively and affordably.
6) *Independent from Location and Device:* Using a web browser, users can access systems using cloud computing regardless of where they are or what device they are using, such as a PC, smart-phone, etc. Users can connect from anywhere because the infrastructure is off-site, usually provided by a third party, and accessed through the Internet.
7) *Easy Maintenance and Lower Cost:* Since they may be accessed from several locations and do not need to be installed on each user's computer, cloud computing programmes are simpler to maintain. Therefore, it also lowers the cost.

B. Types Cloud Architecture

According to the requirements of the enterprise, you can deploy the following 4 types of clouds:

1) *Public Cloud:* Everyone can use the public cloud, which uses a pay-per-usage model, to store and access information through the Internet. In a public cloud, the cloud service provider manages and controls the computer resources (CSP). Example: Amazon EC2, Azure Service Platform, Google App Engine, etc.
2) *Private Cloud:* An internal or corporate cloud is another name for private cloud. Organizations use it to construct and operate their own data centres, either internally or through a third party. Opensource tools like Eucalyptus and Openstack can be used to deploy it.

The National Institute of Standards and Technology (NIST) divides private cloud into the following two categories based on location and management:

- Private on-premises cloud
- Private cloud that is outsourced

3) *Hybrid Cloud:* Public and private clouds are combined to create hybrid clouds. Hybrid cloud is only partially safe because only users within the business can access services that are running on a private cloud, while anyone can access those that are running on a public cloud. Example: Office 365, Google Application Suit, AWS, etc.
4) *Community Cloud:* In order to share information between an organization and a particular community, a collection of various organizations can access systems and services through a community cloud. One or more community-based organizations, a third party, or a combination of them own, manage, and run it.

C. Cloud Service Models

The following three cloud service model types exist:

1) *IaaS:* Hardware as a Service (HaaS) is another name for IaaS. It is an online-managed computing infrastructure. The primary benefit of using IaaS is that it saves users the money and hassle of having to buy and maintain physical servers.
2) *PaaS:* For the purpose of developing, testing, running, and managing applications, the PaaS cloud computing platform was developed.
3) *SaaS:* Another name for SaaS is "on-demand software." It is software where a cloud service provider hosts the apps. Internet access and a web browser are required for users to access these applications.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

III. VIRTUALIZATION

Cloud computing is built on the virtualization technique, which makes it possible to use actual computer hardware more effectively. Through the use of software, virtualization can divide the hardware components of a single computer, such as its processors, memory, storage, and other components, into several virtual computers, also known as virtual machines (VMs). Despite only using a small percentage of the actual underlying computer hardware, each virtual machine (VM) runs its own operating system (OS) and functions like a separate computer.

Today, enterprise IT architecture uses virtualization as a best practise. The economics of cloud computing are likewise based on this technology. Cloud users can buy only the computing resources they require at the time they require them, and they can scale those resources affordably as their workloads increase thanks to virtualization, which enables cloud providers to provide users with services using their existing physical computer hardware.

A. Virtual Machines

Virtual environments that imitate a physical computer in software are called virtual machines (VMs). They typically consist of a number of files, including those storing the virtual machine's settings, storage for the virtual hard drive, and a few snapshots that capture the status of the virtual machine at specific times. The terms virtual server, virtual server instance (VSI), and virtual private server (VPS) are all used to refer to this technology.

An emulated version of a physical computer is known as a virtual machine. The host is the actual machine they run on, and VMs are frequently referred to as guests. On a single physical machine, virtualization enables the creation of many virtual machines, each with its own operating system (OS) and applications. Direct communication between a VM and a real machine is impossible. Instead, it requires a thin layer of software called a hypervisor to act as a communication channel with the underlying physical hardware. Each VM is given a certain amount of physical computing resources, such as processors, memory, and storage, by the hypervisor. In order to prevent interference, it maintains each VM isolated from the others.

IV. HYPERVISOR

The software layer that manages VMs is called a hypervisor. It acts as a bridge between the virtual machine and the underlying physical hardware, making sure that each has access to the resources it requires to run. Additionally, it makes sure that the VMs don't conflict with one another by using up each other's memory or computing resources.

There are two major types of hypervisor listed below:

1) *Type – 1 (Bare-Metal) Hypervisor:* It completely replaces the conventional operating system and interacts with the underlying physical resources. They frequently show up in situations involving virtual servers.
2) *Type – 2 Hypervisor:* On an existing Operating System, hypervisor functions as an application. They are most frequently used on endpoint devices to run alternative operating systems, but because they rely on the host OS to access and manage the underlying hardware resources, they have a performance cost.

A. Hypervisor and Virtualization

In order to manage the distribution of system resources among numerous virtual machines, the hypervisor is accessible at machine startup time. Some of these virtual machines (VMs) are privileged partitions that control the virtualization platform and hosted VMs. The privileged partitions in this design have access to and control over the virtual machines.

The most controllable environment is created using this method, which also allows for the use of extra security measures like intrusion detection systems. The hypervisor has a single point of failure, making it susceptible. All VMs are in the attacker's control if the hypervisor crashes or the attacker seizes control of it. Yet, it is challenging, though not impossible, to take control of the hypervisor at the virtual machine level. This attribute led to the selection of this layer for the implementation of the suggested security architecture.

A hypervisor is one of many virtualization tools that enable hardware virtualization, the capability of running multiple operating systems concurrently on a host machine as "guests." It is conceptually one degree higher than a supervisor, hence its name. The hypervisor provides a virtual operating environment to the guest operating systems and keeps track of how they are running. The hardware resources that have been virtualized may be shared by multiple instances of different operating systems. Hypervisor is installed on server hardware whose only task is to run guest operating systems.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

V. SECURITY ISSUES AND RELIABILITY OF HYPERVISORS

Performance of the cloud can be impacted by reliability-related virtualization problems in addition to security-related ones. For instance, the provider might place an excessive number of virtual machines on a real server. Performance issues may come from repercussions like constrained CPU cycles or I/O bottlenecks. These issues can arise in a conventional physical server, but they are more likely to do so in a virtualized server because numerous Virtual Machines are connected to a single physical server, competing for the same limited resources. Therefore, in a virtualized environment compared to a comparable physical environment, management duties like performance management and capacity planning management are more crucial.

Because of this, IT companies need to be able to continuously track how both physical servers and virtual machines are being used. This capability enables IT companies to allocate and reallocate resources based on shifting business requirements, preventing both over- and underutilization of server resources like CPU and memory. Additionally, with the aid of this capability, IT organizations can put in place policy-based corrective measures that help the company make sure service levels are being reached **[1]**.

The fact that cloud-based companies now have to control virtual machine sprawl presents another challenge in virtualization. Virtual machine proliferation occurs when new virtual machines are created that are not required for business, increasing the number of virtual machines operating in a virtualized environment. Infrastructure overuse is one concern related to virtual machine proliferation. Virtual machine managers should carefully assess the need for all new virtual machines and make sure that any that are not required migrate to other physical servers in order to prevent virtual machine sprawl. Additionally, an unnecessary virtual machine will be able to transfer with high availability and energy economy from one physical server to another. However, bear in mind that it may be difficult to guarantee that the migrated virtual machine maintains the same security, QoS, and required privacy policies. It must be guaranteed that the destination keeps all necessary migrated virtual machine configurations.

There are a number of virtual machines in a virtualization system that might have independent security zones that are inaccessible from other virtual machines that have their own zones. A hypervisor is the governing entity for everything inside a virtualization host and has its own security zone. The actions of the virtual machines operating on the virtualization host can be touched and influenced by the hypervisor **[2]**. There are different security zones, but they are all part of the same physical infrastructure, which in a conventional sense would only be found in one security zone. When an attacker seizes possession of the hypervisor, this could result in a security problem. The attacker then has complete authority over all data located within the hypervisor's domain.

Escape the Virtual Machine, or the capacity to access the hypervisor from within the Virtual Machine level, is a significant virtualization security issue. The development of more APIs for virtualization systems will raise the importance of this even further. Controls to turn off features inside a virtual machine that could harm performance and availability are being developed alongside new APIs.

A. Advantages of Hypervisor Based Security

In addition to managing resources, the hypervisor also has the capacity to protect the cloud's infrastructure. The best method for applying techniques to achieve a secure cloud environment is virtualization technology based on hypervisors. The following factors led to the selection of this technology:

1) The only method to access the hardware is through the hypervisor. Because of this ability, virtualization built on hypervisors can have a secure infrastructure. The hypervisor can serve as a firewall and guard against malicious users infiltrating the hardware architecture.
2) Because the hypervisor is implemented lower in the cloud computing hierarchy than the guest OS, it can identify attacks that get past the guest OS's defenses.
3) The virtual world is separated from the underlying hardware by means of the hypervisor, which functions as an abstraction layer.
4) All access between the operating systems of the guests and the common hardware underneath is controlled at the hypervisor-level of virtualization. As a result, the hypervisor can make the process of transaction monitoring simpler in a cloud setting.

B. Disadvantages of Hypervisor Based Security

In addition to some of the advantages of the virtualization, there are some flaws that can impair the effectiveness of the security measures that have been put in place.

1) Because there is only one hypervisor in a hypervisor-based virtualization, the system becomes a singular point of failure. All the systems and VMs will be impacted if the hypervisor crashes as a result of a load or an effective attack.
2) The hypervisor is susceptible to some assaults, such as buffer overflow, just like other technologies.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

VI. MAJOR THREATS AND SECURITY ISSUES WITH HYPERVISOR BASED VIRTUALIZATION

Despite the fact that each user is serviced by the same machine, in the hypervisor, each user sees their systems as separate computers that are not connected to any other users. An operating system that is controlled by an underlying control programme is referred to in this sense as a virtual machine.

1) *VM-Level Attacks:* The processor or other components could be vulnerable. An issue with multi-tenant design could be caused by cloud vendors' use of virtual machine technology [3]. These technologies use "virtual Machines," which are distant replicas of conventional on-site computer systems that include the operating system and hardware. These virtual machines' number can be instantly increased or decreased to accommodate demand, resulting in enormous savings.
2) *CSP Exposure:* These could be platform-level flaws, like a cross-site scripting or SQL-injection vulnerability present in the cloud service tier that leads to an unsafe environment.
3) *Increased Network Attack Surfaces:* The job of protecting the infrastructure used to connect to and communicate with the cloud by the cloud user is made more difficult by the fact that the cloud is frequently outside the firewall.
4) *Lock-in in the Cloud:* Lock-in in cloud computing seems to be the source of a lot of anxiety. If a user chooses to switch to another vendor or something similar, the cloud provider can encrypt user data in a specific format [4].
5) *Authentication and Authorization:* The framework for corporate authentication and authorization does not logically apply to the cloud. Enterprises must integrate their own security metrics and rules with cloud security policies.
6) *Data Control in Cloud Computing:* Moving even some components into the cloud can create operational "blind spots" for midsize businesses used to having full visibility and control over their entire IT portfolio, with little prior notice of service degradation or interruption [5].
7) *Communication Among VMs:* Virtual machines must exchange information and interact with one another. These messages could be targets of attacks if they didn't comply with stringent security requirements.
8) *DDoS Attack:* DDoS attacks typically target specific network entry points with large numbers of IP packets; typically, any hardware that follows the Blacklist pattern is soon overwhelmed. DDoS attacks could potentially have a much bigger effect on cloud computing than they would on single tenanted architectures because the infrastructure is shared by many VM clients. Unwanted DDoS assaults may result if the cloud does not have enough resources to support its VMs. The conventional answer to this problem is to increase the quantity of these vital resources. However, a severe issue arises when a malicious user purposefully conducts DDoS attacks using bot-nets.
9) *Client-to-Client Attack:* All virtual machines on a real server could become infected by a single malicious virtual machine. The greatest security risk in a virtualized environment is that an attack on one client VM can spread to other VMs that are hosted in the same physical. The attacker must invest time attacking one virtual machine, which can result in infecting other VMs, before escaping the hypervisor and reaching the environment level that isn't formally accessible from the VM level when malicious users make virtual machines easy to access. Therefore, "client to client attacks" pose the greatest security risk in virtualization environments.
10) *Data Leakage:* There are two changes for customers' data when migrating to the cloud. The info will first be kept off of the client's local machine. The data will then be transferred from a single-tenant setting to a multi-tenant one. Data leakage is a significant worry that these changes may bring up. They have caused them to become one of the biggest organizational security threats [6].
11) *Data Remanence Issue:* The physical remnant of data that has been erased in some manner is known as data remanence. There may be some physical traits that make it possible to reconstruct data after storage media has been erased [7]. There might be some physical traits left over after storage media is erased that make it possible to reconstruct data. Therefore, it is crucial that any essential data be securely erased at the end of its life cycle in addition to being protected against unauthorized access.

In general, IT organisations that own their own servers have complete control over those servers. Additionally, they use a variety of tools that are accessible to them for privacy purposes, giving them the ability to destroy sensitive data that is unwanted or unnecessary. However, when moving to a cloud setting, they have virtual servers that are managed by a third party. Overwriting is a conventional method for securely deleting data, but this approach is ineffective without cooperation from the cloud service. Customers cannot view the physical device in a cloud environment, only the data level. There is only one option, and that is for customers to encrypt their data using a secret key to prevent data reconstruction from leftovers after erasure.

©IJRASET: All Rights are Reserved

VII. CONCLUSION

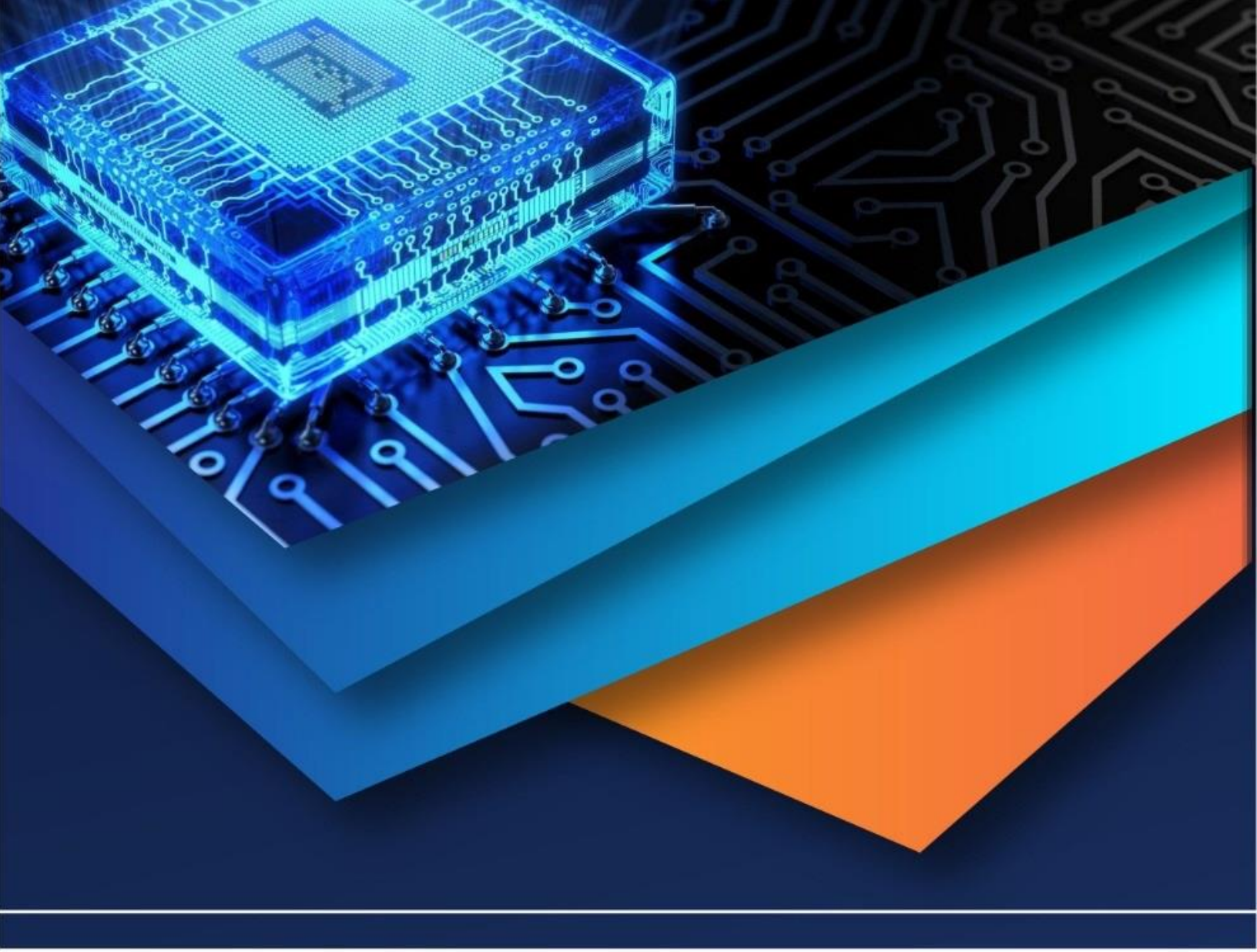
Although there are many users and active applications in the cloud, everyone should prioritize security. No matter what application is running on the cloud, the cloud must function correctly and establish an environment that is immune to attacks. Anything that can be made is also breakable in the realm of computers. Furthermore, cloud computing is an Internet-based technology, but creating root-of-trust cloud computing platforms appeared to be impossible. Therefore, it appears that security is the primary area of worry in the cloud, and cloud providers will experience countless vicissitudes as their cloud grows larger than it is now.

Even so, before transferring data to a cloud, it is important to take into account the unique challenges and security issues that this method of decentralizing applications and enabling global access to data produces. The most crucial of these is security, which must be taken into account before moving towards cloud computing.

REFERENCES

[1] G. Rowel, "Virtualization: The next generation of application delivery challenges," 2009.
[2] G. Texiwilsl, Is Network Security the Major Component of Virtualization Security?, 2009.
[3] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masouka, and J. Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," presented at the ACM Cloud Computing Security Workshop, Chicago, Illinois, USA., 2009.
[4] P. Sefton, "Privacy and data control in the era of cloud computing."
[5] D. Rowe, “The Impact of Cloud on Mid-size Businesses,” 2011.
[6] C. Almond, "A Practical Guide to Cloud Computing Security," 2009
[7] P. R. Gallagher, A Guide to Understanding Data Remanence in Automated Information Systems: The Rainbow Books, ch.3 & ch.4, 1991.
[8] L. Litty, "Hypervisor-based Intrusion Detection," M.S. thesis, Dept. Computer Science, University of Toronto, 2005.
[9] Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition. ACM SIGCOMM Computer Communication Review, 39(1), 50-55.
[10] Zaharescu, E., &Zaharescu, G. A. (2012). Enhanced virtual e-learning environments using cloud computing architectures. International Journal of Computer Science Research and Application, 2(1), 34-39.
[11] Bianchini, R., & Rajamony, R. (2004), “Power and energy management for server systems”, Computer, Vol. 37, No. 11, pp. 68-76

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)