International Journal of Engineering Research & Management Technology
ISSN: 2348-4039
Volume 9, Issue-1 Jan-Feb 2022
Email: editor@ijermt.org www.ijermt.org

CLOUD COMPUTING SECURITY ISSUES AND ITS CHALLENGES

Abu Salim, Rajesh Kumar Tiwari

Department of Computer Science and Engineering

Glocal School of Technology and Computer Science.

Glocal University, Saharanpur, U.P.

ABSTRACT:

Cloud computing is a new paradigm in computing that enables the sharing of resources on distant servers, such as hardware, networks, and storage, via the use of the internet. It offers a means through which applications, computing power, and computing infrastructure may be provided to the user in the form of a service. The user will benefit from the unique characteristic of cloud computing's, a cost-effective Information Technology Solution (IT Solution). The Cloud Service Provider (CSP) is responsible for meeting all of the user's computing requirements, and these requirements may be dynamically expanded or contracted in response to the user's demands. Because both the data and the application are stored on the server, which may be situated outside of the user's geographical area, this raises a variety of concerns from the user's point of view. The purpose of this article is to investigate the primary problems with cloud computing that are holding back its widespread adoption.

Keywords: *Cloud Computing, Security concern, Key Characteristics, Limitation Delivery Model*

[I] NTRODUCTION

Cloud computing is the outcome of extensive study being conducted by academics in academia and industry with the goal of developing superior technology. As a consequence of their efforts, cloud computing has been developed.

Distributed computing may take several forms, including the grid and cloud computing, both of which are based on the service provisioning concept. Users make a payment to the service provider in exchange for utilizing the service. One definition of a distributed computer system is one in which the various software components are located on system. It is comparable to the traditional networks of individual computers that are used to solve complex issues by delegating tiny pieces of the issue to a large number of computers and then merging the answers generated by those computers.

Using grid computing, you are able to treat computer resources like a utility that can be switched on or off at

any time. The delivery of resources on demand is a further advancement made possible by cloud computing. It does away with the need of the practice of providing more than is necessary in order to satisfy the requirements of a large number of consumers.

The term "cloud computing" refers to a model in which computing is delivered more as a service than as a product. With this model, shared resources such as hardware and software are made available to personal computers and other devices (tablets, mobile phones, etc.) as a utility across a network.

It makes use of self-service, pay-as-you-go, high-availability, high-performance, and scalable computing services that are delivered through the internet. These services are available on a pay-per-use basis. There is a vast selection of services accessible today, ranging from basic infrastructure hosting (also known as IaaS) to complete development platform hosting (also known as PaaS), and applications hosting (also known as SaaS).

Cloud computing may shorten the amount of time it takes to bring a product to market since a new server can be set up or brought online in a hurry. Users are able to avoid making expensive initial capital expenditures in the infrastructure thanks to this. Enhance the adaptability of the company as well as the IT organization, which enables companies to pay for extra capacity only when it is really required by the business.

Cloud computing, like many other wonderful prospects, also provides a large number of obstacles and hazards [1,2] all of which IT personnel and decision makers need to be aware of.

The paper is structured as described below. In Section II, we are going to talk about the Key Characteristics of cloud computing. In Section III, we will talk about the services that may be obtained using cloud computing. In Section IV, we talk about the model for providing services. In Section V, we will cover cloud providers and organizations, and in Section VI, we will go through the most important security concerns related to cloud computing environments. The limitations of cloud computing are discussed in Section VII, and the work is concluded in Section VIII.

[II] CHARACTERISTICS OF CLOUD COMPUTING

The cloud computing paradigm utilizes three delivery models and four deployment models, has five important qualities, and has critical properties.

Key features include:

Ubiquitous Network Access enables users to access applications and data via a variety of various types of

devices, including mobile phones, tablets, and personal computers.

On demand self-service, Customers have access to and control over their own computer resources on demand, which is known as "on demand self-service."

Rapid elasticity, the user is able to acquire or release resources in a fast and automated manner according to their needs, which is referred to as rapid elasticity.

Measured Service, the user's usage of the cloud's resources may be monitored, and the user will be paid based on the resources that they really put to use.

Pooling Available Resources, a Cloud Service Provider (CSP) may make their available resources (hardware and software) available to many users. The user is able to either acquire or release resources depending on their needs.

[III] MODELS FOR THE DELIVERY OF CLOUD COMPUTING SERVICES

Cloud computing makes use of three main delivery models, each of which facilitates the delivery of a certain category of service to the end user. The software as a service (SaaS), the platform as a service (PaaS), and the infrastructure as a service (IaaS) delivery models are the three models that supply the user with infrastructure resources, application platforms, and software respectively. Additionally, each of these service models imposes a unique degree of security need on the underlying cloud infrastructure.

3.1 Software as a Service (SaaS):

Software as a Service, often known as SaaS, is a software deployment paradigm in which applications are remotely installed on a server by the cloud service provider, and cloud customers are then able to access the services that have been installed on the server. SaaS provides customers of cloud computing with a variety of advantages, including a reduction in both the initial investment and the ongoing costs of operation. However, the majority of corporations are still hesitant because of a variety of concerns, including trust, privacy, and security. Companies like Salesforce and Gmail are examples of companies that provide PaaS. Salesforce put cloud computing by putting a cloud-based CRM software as a service product on the market. Another well-known SaaS product is Google's email service, Gmail.

3.2 Infrastructure as a Service (IaaS):

Infrastructure as a Service, often known as IaaS, is a model that totally alters the application deployment process for developers. They can simply go to one of the IaaS providers, have a virtual server operating in a matter of minutes, and pay only for the resources that they use as opposed to investing a significant amount of money on their own data centers, managed hosting businesses, or co-location services and then paying operational employees to get it going. IaaS and other linked services have, in a nutshell, made it possible for start-ups and other enterprises to concentrate on their primary areas of expertise without being distracted by concerns over their IT infrastructure. IaaS only offers the most fundamental level of security; applications migrating into the cloud will demand greater degrees of security and will need to comply with regulatory standards. Amazon Web Services, GoGrid, and Rackspace are a few examples of companies that provide IaaS.

3.3 Platform as a Service (PaaS):

PaaS is one layer above IaaS on the stack, and it abstracts everything up to and including the operating system, middleware, and other software. This provides a unified environment for software developers, which includes, developer may use to construct their apps without having any knowledge about what is happening underlying the service they are using. It provides developers with a service that manages the whole software development life cycle, from planning to designing to creating applications to deploying to testing to maintaining software. This service is offered to developers. The developers don't have a "view" on anything else since it has been abstracted away. The disadvantage of PaaS is that its benefits may make it easier for hackers to use the PaaS cloud infrastructure as a command and control center for malware and to circumvent IaaS applications. This is the "dark side" of PaaS. PaaS services includes force.com, Google App Engine, and Microsoft Azure, as few examples.

[IV] MODELS FOR THE DEPLOYMENT OF CLOUD COMPUTING SERVICES

There are four different deployment models that are used by cloud computing.

Public Cloud is a sort of cloud computing in which the cloud infrastructure is controlled by an organization that sells cloud services and is made accessible to the general public or to a big industry group. A cloud service provider is another name for an organization that sells cloud services.

Community cloud refers to a specific kind of cloud computing in which the cloud infrastructure is used by a number of different organizations that have similar concerns (for example, mission, security).

Private Cloud, a private cloud is a kind of cloud computing in which the cloud infrastructure is used by a single business that may be physically situated on or away from the company's premises.

Community Cloud:

Hybrid Cloud is a type of cloud computing that consists of two or more clouds (private, community, or public) that continue to exist as separate entities but are connected through the use of standardized or proprietary technology that enables data and application portability (for example, cloud bursting for load-balancing between clouds).

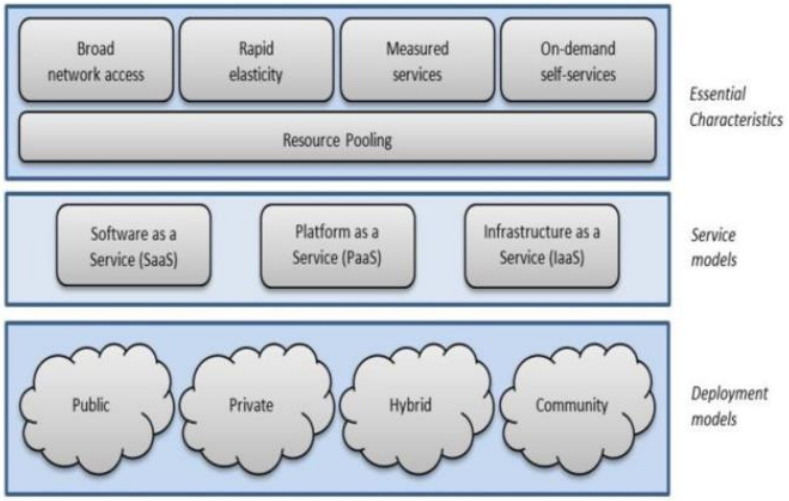

Fig. 1: NIST visual model for cloud computing

[V] USERS AND PROVIDERS OF CLOUD SERVICES

Cloud computing involves participation from a variety of parties, including cloud users, cloud providers, cloud resellers, and cloud service brokers, among others.

5.1 Cloud Providers:

Internet service providers, telecommunications firms, and big business process outsourcers are examples of the types of organizations that fall under the umbrella term "cloud providers." These companies either supply the infrastructure (hosted data centers) or the media (Internet connections) that allow customers to access cloud services. In addition, system integrators might be considered service providers. These companies construct and maintain data centers that host private clouds, and they provide a variety of services (such as SaaS, PaaS, IaaS, and so on) to end users, service brokers, and resellers.

5.2 Cloud Service Brokers:

Cloud Service Brokers are comprised of individuals and organizations such as technology consultants, business professional service companies, licensed brokers and agents, and influencers that assist customers in making decisions about cloud computing solutions. Without really owning or controlling the whole Cloud infrastructure, service brokers focus on the negotiation of the agreements that exist between customers and suppliers of cloud services. In addition to that, they provide further services in addition to infrastructure belonging to a Cloud provider that will be used to construct the user's own Cloud environment.

5.3 Cloud Resellers:

Cloud resellers are local businesses who have been selected by a cloud service provider in order to expand that provider's customer base. They provide the impression of being a cloud provider in a certain location, but in reality, they are supplying services with the assistance of another Service Provider.

5.4 Cloud Users:

Cloud Users are at the very bottom of this food chain since they are the ones who really utilize the services that are provided by cloud service providers.

[VI] MAJOR OBSICLES INCLOUD COMPUTING

In this part, we will highlight some of the major obstacles that cloud computing must overcome.

6.1 Unauthorized Access

Contrary the company's on-premises architecture, cloud-based installations are accessible directly from the public Internet and are located outside of the company boundary. Because of these users and customer will find the infrastructure to be more accessible. However, Attackers are also given an easier time gaining unauthorized access to a company's cloud-based services as a result of this development. If security is set incorrectly or credentials are stolen, an attacker may be able to bypass the company's protections and get direct access to the system without the company awareness.

6.2 Insufficient visibility

The cloud-based resources of an organization are kept at a physical location that is remote from the corporate network and are operated using hardware that the organization does not own. As a consequence of this, many of the conventional tools that are used to get network visibility do not perform well in cloud settings, and some organizations do not have cloud-focused security solutions. This may make it more difficult for an organization to manage the cloud-based services they use and safeguard those resources from being attacked.

6.3 Unintentional Disclosure of Credentials

Phishers often make use of cloud apps and platforms as a pretext in the assaults that they launch against their victims. People have become familiar to getting emails with links that may ask them to verify their login information before gaining access to a specific document or web page

6.4 Data Privacy:

The capacity of an individual or organization to conceal themselves or information about themselves and reveal themselves only when they want to do so selectively is what we mean when we talk about data privacy [3].

In cloud computing, protecting the privacy of one's data is another important consideration. It is necessary for businesses to organize teams of staff members to investigate customers' concerns about data protection. The Information Technology Act, 2000 (often known as the "IT Act") and its several sub sections control the data security and privacy related concerns in India. It is possible for data stored in the cloud to be disseminated across geographical borders, which may not be following the privacy laws of the area in question. Laws prevent the use of some data for purposes other than the one(s) for which it was originally obtained, which is because such use is against the law.

Information that is held in the cloud is subject to the legal requirements of one or more legislation, such as the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLBA), the cloud provider is legally obligated to preserve the data's privacy in an acceptable way.

6.5 Data Security:

When it comes to cloud computing, one of the most important concerns is the safety of the data that is kept at the Cloud Service Provider (CSP). In more conventional applications, the client owns the computer on which the data are kept, so that it is on their property. The client is responsible for providing both the physical and logical security measures. The user does not have control over the data storage environment in a cloud computing environment since the data are stored on a shared environment. The data must be protected by the SaaS provider at all times. They are required to apply a rigorous encryption method and provide fine-grained access control to the data. Once the data has been erased by the user, the SaaS provider should not be able to recover access to it by utilizing any means. The customer should have control over the data life cycle.

whatsoever means. Before data is stored, it is possible for it to be encrypted automatically. The encryption that is offered by hard disk manufacturers has a less impact on the performance overhead.

The following test may be used in order to determine whether or not the data kept at the cloud service provider

is secure [4].

- [XSS] stands for "cross-site scripting."
- Flaws in the access control system
- OS and SQL injection vulnerabilities.
- Forgery of cross-site requests, often known as CSRF.

6.6 Data integrity:

Integrity in data, software, and hardware indicates that assets can only be changed by authorized persons or in permitted methods. Integrity refers to the fact that assets can be adjusted in any of these ways. The term "data integrity" refers to the process of defending data against illegal changes, deletions, or fabrications [5].

In a typical system, ensuring the integrity of the data is not difficult. The integrity of the data is preserved in a system like this one via the use of database constraints and transactions. For the sake of preserving the integrity of the data, transactions need to adhere to the ACID (atomicity, consistency, isolation, and durability) criteria. ACID features, which maintain the database's integrity, are supported by the majority of the database system software, such as Oracle and SQL.

The information that is produced by cloud computing services is stored in the cloud. Users run the risk of losing control of their data when they store it in the cloud and must instead depend on cloud operators to ensure the data's access control and integrity.

6.7 Data Lock in:

If a company chooses a platform offered by a cloud service provider (CSP) that is based on proprietary file formats, then the company runs the risk of being locked into a position known as data lock-in. This scenario makes it far more difficult for the company to switch service providers at some time in the future. Changing your Cloud Service Provider (also known as CSP) is essential in the event that your current cloud provider modifies the terms of service they provide or has service outages that force you to look for other options.

As cloud service providers attract consumers at a quick rate, there has been a rise in the amount of attention paid to the issue of lock-in. The European Network and Information Security Agency (ENISA) identified lock- in as one of the most significant hazards associated with cloud computing in a study that was published in November 2009 and titled Cloud Security Risk Assessment. According to the research, "there is currently very little that can be offered in the way of tools, procedures, standard data formats, or service interfaces that could guarantee

data and service portability." Because of this, it could be difficult for the consumer to go from one supplier to another or back to an environment located inside the company itself.

The issue of data lock-in may be solved with the assistance of SNIA's Cloud Data Management Interface (CDMI), which was created by the Storage Networking Industry Association (SNIA). The Cloud Data Management Initiative (CDMI) is the first open standard for cloud computing to be produced by the industry. CDMI offers the capability to control service levels that data gets when it is stored in the cloud as well as a single interoperable data exchange format for securely transporting data and its associated data needs from cloud to cloud [6]. In addition, CDMI allows for the management of service levels that data receives when it is retrieved from the cloud.

6.8 Data Location:

The location of the data is another factor that must be considered while working with cloud computing. Cloud Service Providers (also known as CSPs) each have their own data center located globally, Due to the fact that different nations have different laws regarding data privacy, the fact that the datacenters are situated in different geographical regions may be a reason for worry. Because of the potentially sensitive nature of particular data, it is imperative that information does not leave the nation. In the event of an inquiry, certain data would be necessary, and gaining access to that data might provide a challenge [7].

6.9 Data Availability:

The term "availability" refers to the quality of a system in which it is possible for an authorized entity to get access to and make use of the system at any time. One of the most important worries that companies have is the availability of their data. When storing data at distant systems that are held by someone else, the owner of the data may be at risk for experiencing system failures caused by the service provider. Due to the fact that the data is dependent on a single service provider, it will be rendered inaccessible in the event that the Cloud stops functioning.

It is the obligation of the cloud service provider to guarantee that cloud customers get service without any breaks or interruptions 24 hours a day, seven days a week. In order to guarantee this, modifications may be required on both the hardware and software levels. It is necessary to adopt and promote a multi-tier architectural design. via the use of a farm of application instances that are load-balanced and operate on a changeable number of servers. Within the application itself, resiliency against failures in hardware or software, as well as resistance to assaults that deny service, has to be constructed from the ground up. At the same time, it is necessary to take into consideration an effective action plan for business continuity (BC) and disaster recovery (DR) in case any unanticipated events occur.

6.10 Data Segregation:

Data Segregation is the separation of data to guarantee that each cloud client may only access the information that pertains to him without influencing the information belonging to other cloud customers. Make sure that your Cloud Service Provider (CSP) applies encryption when data is segregated or aggregated, and have security professionals evaluate the encryption techniques.

Multi-tenancy is a feature of cloud computing that allows for several users to simultaneously use the same set of resources (hardware and software). Because of multi-tenancy, the data for several users may coexist in the same place on the same piece of physical infrastructure at the same time. In this context Intrusion is fairly feasible. This breach may be introduced into the system in one of two ways: either by hacking via the application's security flaws or by injecting client code into the SaaS platform. A client is able to compose code using a mask and then inject it into the application. If the program performs this code without first doing verification, there is a significant risk of unauthorized access to the data of other users. The cloud service provider is responsible for ensuring that there is a distinct barrier between each user's data. It is not enough to just secure the border at the physical level; it must also be done so at the application level. It is necessary for the service to have sufficient intelligence to separate the data from the many users.

6.11 Security Policy and compliance:

Compliance with the Security Policy A security policy should be robust enough to safeguard people as well as information, and it should outline the anticipated behavior of all entities, including all types of users, system administrators inside the company, management, and security staff. It is also important that the policy be followed. Monitoring, analyzing, and conducting investigations into an organization's infrastructure are all essential skills for a security manager. The policy needs to identify and approve the penalties of violation, describe the business consensus baseline attitude on security, contribute to risk reduction, and contribute to tracking compliance with rules and legislation. When developing a policy to ensure the safety of data sent between a cloud hosting provider and a client, it is necessary to consider a number of significant aspects, such as the presence of inside threats and the configuration of access restrictions [9]. Security auditing and certification are requirements for traditional service providers. Cloud service companies strive to earn more of their customers' confidence. Requirements of these security audits must be met. Enterprises are under a great deal of pressure to comply with a variety of rules and standards, including PCI, HIPAA, and GLBA, in addition to auditing techniques, such as ISO and SAS70. It is assumed that every company will comply with these security requirements for every kind of server, regardless of whether the server is hosted on the organization's

premises or off-site in a distant location.

6.12Multitenancy:

Cloud computing is distinguished by a number of essential properties, one of which is multitenancy. It is possible for several users to execute software on the same hardware resources, which maximizes the use of those resources. Despite the advantages of this configuration[10], it offers security and privacy risks. Customers of the cloud are kept separate from one another by a technology called virtualization; yet, a customer may get access to another customer's real or residual data, network traffic, and processes by taking advantage of vulnerabilities in the applications. For the purpose of resource management in the cloud, various virtualized application instances must be regularly supplied, assigned, or even transferred between several physical computers located either off the premises or on the premises. Attackers may target shared resources like as hard disks, RAM, or CPU caches. As a result of this property of cloud computing, known as dynamic provisioning, the work of maintaining security becomes more difficult. Security Alliance for the Cloud proposed solutions to this problem include completing vulnerability assessment and repair, supporting strong authentication and monitoring illegal activity, and applying security best practice for installation and setup. These are only a few of the eight suggested solutions.

Finding a solution to the issue of multitenancy, security and privacy, which is one of the most significant difficulties facing the public cloud, is essential if one wishes for the cloud to achieve widespread adoption.

6.13 Non-Repudiation:

This term refers to the standards that must be met in order to prohibit a party to a contact with the cloud from denying that the interaction took place. The use of a digital signature has the potential to clarify roles and responsibilities in a given engagement. In [11], the researcher employs a method in order to track down the user and discover where they are from. It makes it exceedingly difficult for users to mislead about their identification information and facilitates the storage of information pertaining to users. The Multi-party Non-Repudiation (MPNR) protocol [12] not only protects against roll-back attacks but also offers a fair non-repudiation storage cloud.

6.14 Energy Management:

The infrastructure in the cloud should use as little power as possible while yet being kind to the environment. It was discovered that the costs associated with just powering and cooling the data center amounted for 53% of

the entire operating cost [13]. Bringing down one's overall energy use would not only save money, but it will also be better for the environment. Cloud Computing Service Providers (CSPs) are increasingly paying attention to the need of maintaining an energy efficient data center. They are putting up effort in a number of different avenues. For instance, an energy-efficient hardware design that allows the CPU speeds to be slowed down and some hardware components to be turned off. The statement [14] is now taken for granted. Turning off computers that aren't being utilized is one more approach to cut down on power usage. Other options include energy-aware work scheduling and server consolidation [15]. The current emphasis of research is not just on reducing the required amount of energy but also on improving application performance.

6.12 Governance and regulatoryCompliance:

Governance and regulatory Compliance Cloud Service Providers (CSP) are not only responsible for providing Infrastructure and their maintenance, but they also have to incorporate and follow the rules and regulations that are specific to a region's government, such as SOX, HIPAA, FISMA, FIPS 140-2, GLBA, ITAR, ISAE 3402, and SAS 70. In addition, CSPs are responsible for governance and regulatory compliance.

Policies pertaining to governance and regulation that are important are

- Sarbanes and Oxley (SOX)
- The Health Insurance Portability and Accountability Act (often known as HIPAA) ,1996.
- The Federal Information Security Management Act, 2002, or FISMA.
- The Federal Information Processing Standard (FIPS) Publication 140-2, "FIPS 140-2."
- The Gramm-Leach-Bliley Act, abbreviated as GLBA.
- ITAR stands for the International Treaty on the Regulation of Arms.
- INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS (ISAE) 3402.
- The Statement on Auditing Standards, (SAS70)

6.15 Insecure API:

API that is not secure Cloud computing companies often make available to clients a collection of software interfaces, sometimes known as APIs, which are comprehensive structural documents used by customers to administer and interact with cloud services. All of the cloud's operations, including provisioning, administration, orchestration, and monitoring, are carried out with the help of these APIs. Because these API are accessible to the public, malicious actors may exploit any vulnerabilities they include in order to breach the security of cloud infrastructure.

Cloud service providers make their API specifications available to the broader public.

- They want to communicate to the services that this information is accessible.
- to make it easier for customers to alter their architecture so they can make more effective use of services.

API is accessible to the public, which means that they need to be meticulously built to ensure that there are no cloud services may be used without any trouble by both malicious users and lawful users. They need to use caution when selecting up to what degree or extent the user should be familiar with the features of the system.

6.16 Service level agreement:

A service level agreement, often known as a SLA, is a contract that discusses the level of services that are anticipated to be given by the cloud provider to the cloud user. It identifies attributes, priorities and obligations. In most cases, it also outlines the corrective actions that will be performed in the event that the service falls below the level that was specified in the SLA. Users of the cloud may choose to form a committee in order to work out SLA. It should fulfill customers' requirements while being cost efficient, and users of the cloud should explicitly identify their demands before signing any contracts.

This is obviously a very significant legal agreement between a cloud service provider and a cloud user, and it should include the following characteristics [16].

- Determine which services are needed by the user and define them.
- Determine the necessary levels of security and privacy.
- Determine the most important aspects of the services.
- Determine who is responsible for what in the cloud. both users and providers.
- Reduce the conflict.
- a crystal-clear articulation of each party's duties and expectations of the other.
- Determine whether legal and regulatory requirements are met or not.

6.17 Trustworthy Service Metering:

Service Metering That Can Be Trusted Cloud service providers make use of a variety of characteristics in order to bill their customers in accordance with the quantity of services that they have used. For instance, customers are charged by Amazon Elastic Compute Cloud (EC2) based on the amount of time that their particular EC2 instances are in a running state. On the other hand, Google AppEngine users are charged according to the number

of CPU cycles that their applications utilize. In cloud computing, multiple users share different resources that are not perfectly isolated and software bugs or intruders may use the services and there uses charges has to be paid by users. This is because users may have little or no visibility into the cloud infrastructure. However, because users may have little or no visibility into the cloud infrastructure, they are often unable to directly connect their actual cloud resource consumption and the usage charges. If we want the cloud computing paradigm to be successful, figuring out how to assure the reliability of the services being provided is of the utmost importance.

[VII] CLOUD COMPUTING LIMITATIONS AND WEAK POINTS

In addition to the issues listed above, cloud computing comes with a number of additional drawbacks, including outages, restrictions on data transmission, slow support response times, increased latency, limited control, a lack of understanding, and challenges in connecting various devices.

- Even the most reliable cloud service providers might have outages and downtime at some point. The user's own internet connection could also be the source of the issue.
- Data send Restriction, the ability to send a big volume of data could provide certain difficulties.
- Support Response Time: If there is a delay in providing answers to queries raised by customers, customers may have problems.
- latency is the amount of time that passes between when your computer attempts to interface with a server and when it actually does so. It's possible that this will become an issue if interaction is really sluggish.
- Users have limited control over the operation and execution of the hardware and software since the services operate on distant servers. This means that even cloud software may give less functionality than locally accessible software.
- Insufficient Understanding, the user may encounter difficulties due to the limited accessibility of information on the operation of cloud servers.
- Integration, users may have difficulties while attempting to integrate several pieces of technology, such as printers, mobile devices, and portable storage units.

[VIII] CONCLUSION AND FUTUREWORK

The program and data are sent to a distant location in the cloud computing paradigm, where they are then

executed on a virtual computing resource with the assistance of a virtual machine. This one-of-a-kind quality, on the other hand, creates a number of difficulties with regard to trust, privacy, and security.

In this study, we have examined a lot of research studies, especially those that dealt with concerns pertaining to security, and we concluded that security is the primary worry that is delaying the adoption of cloud computing.

Future work on cloud computing will include the proposal of a security framework that will cover concerns such as data security, data privacy, data integrity, trust management, multi-tenancy, non-repudiation, secure application programming interfaces (APIs), data lock-in, energy management, service level agreements (SLAs), and trustworthy service metering.

REFERENCES

[1] R. Velumadhava Rao a, K. Selvamani b, "Data Security Challenges and Its Solutions in Cloud Computing", Procedia Computer Science,Volume 48, 2015, Pages 204-209.

[2] M.Rajesh, A Ssytmetic Review of cloud secutity chalanges in higher education, The Online Journal of Distance Education and e-Learning, October 2017 Volume 5, Issue 4.

[3] Dawei Suna, Guiran Changb, Lina Suna and Xingwei Wanga [2011]. Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments. ELSEVIER . Pp. 2852- 2856.

[4] S. Subashini n, V.Kavitha [2011]. A survey on security issues in service delivery models of cloud computing. Journals of network and computer Applications. Volume 34, Issue 1, January 2011. Pp.1-11.

[5] Dimitrios Zissis, Dimitrios Lekkas [2012]. Addressing cloud computing security issues. Future Generation Computer Systems, Volume 28, Issue 3 . Pp. 583-592.

[6] http://www.snia.org.au/assets/document s/the danger of cloud lockin cs.pdf

[7] Rabi Prasad Padhy1 Manas Ranjan Patra2 Suresh Chandra Satapathy [2011]. Cloud Computing: Security Issues and Research Challenges. IJCSITS Vol. 1, No. 2, December 2011. Pp. 136-146.

[8] Kui Ren, Cong Wang, and Qian Wang .Security Challenges for the Public Cloud [2012], IEEE INTERNET COMPUTING, January/ February 2012. Pp. 69-73.

[9] Mathisen E. [2011]. Security Challenges and Solutions in Cloud Computing. In Proceedings of the IEEE International Conference on Digital Ecosystems and Technologies. Pp. 208- 212

[10] https://downloads.cloudsecurityalliance. org/initiatives/guidance/csaguide.v3.0.p df.

[11] Z. Shen and Q. Tong [2010]. The security of cloud computing system enabled by trusted computing technology. ICSPS : V2-11–V2-15.

[12] J. Feng, Y. Chen, D. Summerville, W.S. Ku, and Z. Su [2011]. Enhancing cloud storage security against roll-back attacks with a new fair multiparty non- repudiation protocol, CNNC. Pp. 521– 522.

[13] Hamilton J. [2009]. Cooperative expendable micro slice servers (CEMS): low cost, low power servers for Internet-scale services In: Proc of CIDR.

[14] Brooks D et al [2000]. Power-aware micro architecture: design and modeling challenges for the next-generation microprocessors, IEEE Micro. Pp. 26- 44

[15] Vasic N et al [2009]. Making cluster applications energy-aware. In: Proc of automated ctrl for data centers and clouds.

[16] http://www.etsi.org/deliver/etsi_tr/1031 00_103199/103125/01.01.01_60/tr_103 125v010101p.pdf.