Journal of Management and Service Science, 2022,
Vol. 02, Iss. 01, S. No. 003, pp. 1-11
ISSN (Online): 2583-1798

Security Issues in Cloud Computing

Aryan Srivastava[1], Pawan Singh[2]

[1,2]Amity School of Engineering & Technology, Amity University Uttar Pradesh, Lucknow, India
aryansri1607@gmail.com[1], pawansingh51279@gmail.com[2]

How to cite this paper: A. Srivastava and P. Singh (2022) Security Issues in Cloud Computing. Journal of Management and Service Science, 2(1), 2, pp. 1-11.

http://doi.org/10.54060/JMSS/002.01.003

Received: 24/05/2021
Accepted: 15/02/2022
Published: 25/02/2022

Abstract

Cloud computing has aided the evolution of IT by improving the ability and flexibility of data storage, as well as providing scalable computation and processing capabilities that match the dynamic data sets. Many corporate application programs have been transferred to public and hybrid clouds due to the multiple benefits of cloud computing. On the other hand, many businesses identify privacy and data security as major concerns that prevent them from adopting cloud computing. The only way to achieve successful cloud implementation is to improve and manage data security and privacy in the cloud. This research paper looks at data privacy and security in cloud computing at all stages of the data lifecycle, providing a general overview of the technology while highlighting important security difficulties and concerns that must be addressed. It also examines a number of existing solutions and gives recommendations for new ones that can improve data privacy and security in the cloud. Finally, future research on data privacy and security in cloud systems is discussed in the study report.

Keywords

Cloud computing, Models, Threats, Countermeasures

1. Introduction

The internet sector changes almost every day. As technology advances and changes, it may be tough to keep up with all the new developments and creations. While cloud computing isn't technically a new concept, it's just lately become popular among organizations. It's impossible to exaggerate cloud computing's impact on the data industry and end users in general. Many aspects of daily life have been modified and revolutionized as a result of this breakthrough digital solution. Cloud computing has helped businesses of all sorts, from start-ups to large companies, cut costs and expand their offerings. This is due to the fact that they do not necessitate any additional hardware or software. Cloud computing is a model that is based on an internet-centric open standard. This model contains a wide range of services, including both hardware and software. The provision and maintenance of these services do not necessitate extensive management effort on the part of the service providers. The term "cloud computing" refers to a method of extending the capabilities of high-performance computing systems. One of the

primary problems related with cloud computing security is data privacy, as data must be safeguarded from any third party, which is regularly reported by users. Because cloud computing is used to share data, data theft is a highly prevalent and serious problem that affects both customers and service providers.

Virtualization is one of the methods used by cloud computing to suit the needs of consumers. Though virtualization is used to help consumers, it has its own drawbacks, such as challenges with data separation and communication among infected computers. Cyberattacks are more likely to occur as a result of cloud computing. Many of these cyber-crimes are related to the most prevalent as well as prospective online interactions, such as hostile insider, DDOS attack, nefarious usage and misuse of cloud computing, programming interface of vulnerable application, and so on. It is critical for cloud computing service providers to improve their cyber security and access control systems to their resources to keep track of who has interacted with them. This document gives a list of issues relating to concerns that affect information security. To keep track of who interacted with them, this document also presents the three main kinds of risks, attacks, and other security concerns. This document gives a list of issues relevant to information security concerns. This paper also discusses the three major categories of security threats, attacks, and other difficulties.

2. Cloud Computing

2.1. About

Distributed computing is an innovation which relies upon sharing of processing assets than having neighborhood workers or individual gadgets to deal with the applications. In Cloud Computing, "Cloud" signifies "The Internet", so Cloud Computing implies a sort of processing where administrations are conveyed through the Internet. The objective of Cloud Computing is to utilize expanding figuring ability to execute a great many directions each second. Distributed computing utilizes organizations of a huge gathering of workers with specific associations with circulate information handling among the workers. Rather than introducing a product suite for every PC, this innovation needs to introduce a solitary programming in every PC that permits clients to sign into a Web-based assistance and which additionally has every one of the projects needed by the client. There's a huge responsibility shift, in a distributed computing framework. Nearby PCs at this point don't need to take the whole weight with regards to running applications. Distributed computing innovation is being utilized to limit the use cost of registering assets. The cloud organization, comprising of an organization of PCs, handles the heap all things being equal. The main thing that should be done at the client's end is to run the cloud interface programming to associate with the cloud. Distributed computing comprises of a front end and back end. The front end incorporates the client's PC and programming needed to get to the cloud organization. Back end comprises of different PCs, workers and data set frameworks that make the cloud. The client can get to applications in the cloud network from anyplace by interfacing with the cloud utilizing the Internet. A portion of the constant applications which use Cloud Computing are Gmail, Google Calendar, Google Docs and Dropbox and so on.

2.2. Advantages of cloud computing

Data backup and restoration- It is considerably easier to back up and restore data once it has been saved in the cloud. Collaboration has improved - Cloud applications improve collaboration by allowing groups of people to quickly and easily share information on the cloud via shared storage. Accessibility is excellent- We can quickly and easily access and preserve information from anywhere on the planet, at any time, using an internet connection. An internet cloud architecture promotes productivity and efficiency by ensuring that our data is constantly available. Low-cost maintenance- Cloud computing saves money on both hardware and software upkeep. Mobility-We can simply access all cloud data through mobile. Storage capacity is limitless - The cloud gives us a lot of storage capacity so we can keep important data like papers, photos, audio, video, and other sorts of

media in one place. In the pay-per-use model, iServices - Customers can use Application Programming Interfaces (APIs) to access cloud services, and they are charged based on how much they use them.

Table 1. Essential charecterstics of cloud computing.

Essential characteristics	
On-demand self-service	1- Provisioning of computing capabilities to the customer. 2- Automatic provisioning on demand.
Broad network access	1- Capabilities are accessible through standard networks, primarily Internet. 2- Devices that can access these capabilities include mobile phones, workstations, laptops etc.
Resource pooling	1- Multi-tenancy 2- Resources are shared by all customers. 3- Resources are location independent. 4- Resources may be physical or virtual
Rapid elasticity	1- Elastically provisioning /releasing of resources. 2- Must be scalable and flexible enough to meet maximum demands.
Measured service	1- Measuring capabilities for the type of services provisioned. 2- Automatic control and optimization of resources usage. 3- Monitoring and controls. 4- Reports and accounting of utilized services for both customer and service provider.

2.3. Cloud computing development models

2.3.1 Cloud

A cloud-based application is completely installed in the cloud and runs entirely in the cloud. To take use of the benefits of cloud computing, applications in the cloud were either created in the cloud or transferred from an existing infrastructure. Cloud-based apps can be built on low-level infrastructure components or on higher-level services that abstract away from basic infrastructure management, architecting, and scaling requirements.

2.3.2 Hybrid

A hybrid deployment is a method of connecting infrastructure and applications across cloud-based resources and non-cloud-based resources. The most typical hybrid deployment strategy is to combine cloud and on-premises infrastructure to extend and grow an organization's infrastructure while linking cloud services to internal systems. Visit our hybrid website for additional information on how AWS can assist you with your hybrid setup.

2.3.3 On-premises

The term "private cloud" refers to the deployment of resources on-premises using virtualization and resource management techniques. Although on-premises deployment does not offer many of the advantages of cloud computing, it is occasionally preferred since it can give dedicated resources. In most cases, this deployment approach is similar to legacy IT infrastructure, with the addition of application management and virtualization technologies to improve resource use.

Table 2. Development Models

Deployment Models	
Private cloud (on-premises)	1. Cloud infrastructure is exclusively provisioned to single organization. 2. Ownership, management and operation may be of organization or third party or by both. 3. Commonly exist on premises of organization, may exist off premises.
Community cloud	1. Cloud services are provided to some specific community. 2. Community belongs to the organizations having shared concerns. 3. Ownership, management and operation may be of multiple organizations or third party or by both. 4. No restriction of on premises may exist off premises.
Public cloud	1. Services are provisioned to general public. 2. Ownership, management and operation may be of business/ government/ academic organization or third party or by both. 3. Commonly exist on premises of cloud owner.
Hybrid cloud	1. Combination of two or more above mentioned infrastructure types. 2. The infrastructures are only bound together by application portability and data. 3. Their distinctness remains preserved.

2.4 Models of cloud computing

2.4.1 Infrastructure as a Services (IaaS)

Infrastructure as a Service (IaaS) is a term that refers to the basic building blocks of cloud computing. It ordinarily incorporates organizing abilities, PCs (virtual or devoted equipment), and information stockpiling limit. Infrastructure as a Service (IaaS) gives you the most flexibility and administrative control over your IT resources, and it's the most akin to what many IT departments and developers are used to today.

2.4.2 Platform as a service (PaaS)

Platforms as a service relieve enterprises of the burden of managing underlying infrastructure (often hardware and operating systems), allowing them to concentrate on the deployment and administration of their applications. This permits you to be more useful on the grounds that you will not need to stress over asset acquisition, scope quantification, programming support, fixing, or any of the other undifferentiated hard work that accompanies running your application.

2.4.3 Software as service (SaaS)

Software as a Service (SaaS) offers you a fully functional solution that is managed and maintained by the service provider. The majority of the time, when people talk about Software as a Service, they're talking about end-user apps. You don't have to worry about how the service is maintained or how the underlying infrastructure is managed when you utilise a SaaS solution; all you have to do is think about how you'll use that particular piece of software. Electronic email is a continuous illustration of a SaaS application since it permits you to send and get email without overseeing highlight moves up to the email item or keep up with the workers and working frameworks on which the email program is running.

Table 3. Service Models.

Service Models	
Software as a Service (SaaS)	1- Customer can use only the provided application running on underlying cloud infrastructure. 2- Capabilities are accessible through Internet or APIs. 3- No control of underlying infrastructure.
Platform as a Service (PaaS)	1- Customer can deploy/configure it's or third-party application, the only limitation is supported by underlying infrastructure. 2- No control of underlying infrastructure like operating system, servers, storage etc.
Infrastructure as a Service (IaaS)	1- Customer is provisioned computing resources of processing, network, storage. 2- Customer can run/deploy arbitrary software including operating system, applications. 3- Customer can only control components related to it. 4- No control of underlying infrastructure.

3. Security issues and threats

The cloud provider holds the responsibility for security in (SaaS). The SaaS model is predicated on a high degree of integrated functionality with low client control or expansion, in part because of the degree of abstraction. The PaaS approach, on the other hand, provides greater extensibility and customer control. IaaS provides greater tenant or customer control over security than PaaS or SaaS, owing to the lower degree of abstraction.

We need to understand the linkages and dependencies between various cloud service models before we can analyze security problems in Cloud Computing. Since both PaaS and SaaS are facilitated on top of IaaS, any security break in IaaS will impact the security of PaaS as well as SaaS administrations, but the opposite might be true as well. However, we must consider that PaaS provides a framework for developing and deploying SaaS apps, increasing the security reliance between them. Because of these deep dependencies, any assault on one of the cloud service tiers can affect the top layers. Each cloud service model has its unique security problems, but there are several challenges that are common to all of them. These interdependencies and linkages between cloud models could provide a security concern. A PaaS supplier may rent a development environment to a SaaS company, while an IaaS provider may rent infrastructure to a SaaS provider. Because each supplier is responsible for safeguarding his own services, an inconsistency in security models may result. It also makes it difficult to determine which service provider is to blame in the event of an attack.

3.1 Software-as-a-service (SaaS) security issues

Email, conferencing software, and business applications such as ERP, CRM, and SCM are examples of SaaS applications. Among the three basic cloud delivery methods, SaaS consumers have the least control over security. Security risks may arise as a result of the deployment of SaaS applications.

3.2 Application security

These programs are often provided through a Web browser over the Internet. Web application weaknesses, on the other hand, may expose SaaS applications to vulnerabilities. Attackers have been utilizing the internet to get access to users' computers and carry out destructive operations such as data theft. SaaS applications face the same security concerns as any other web application technology, but traditional security solutions are ineffective in protecting them from assaults, necessitating new

techniques. The ten most serious web application security concerns have been determined by the Open Web Application Security Project (OWASP).

3.3 Multi-tenancy

Scalability, configurability via metadata, and multi-tenancy are all qualities that can be used to categorize SaaS systems into maturity models. Each customer has his or her own customized instance of the software in the first maturity model. This model contains flaws, although security concerns aren't as serious as they are with other models. The vendor delivers separate instances of the apps for each client in the second model, but all instances use the same application code. Customers can customize several configuration options in this model to match their own demands. Multi-tenancy is added to the third maturity model, allowing a single instance to service all clients.

3.4 Data security

Data security is a key worry for any technology, but it gets even more difficult when SaaS users must rely on their providers to keep their data safe. Organizational data is frequently processed in plaintext and saved in the cloud while using SaaS. The SaaS provider is in charge of the data's security while it's being processed and stored. Data backup is also important in order to assist recovery in the event of a disaster, but it raises security risks. Furthermore, cloud companies can subcontract other services, such as backup, to third-party service providers, raising problems. Furthermore, most compliance standards do not consider how to comply with legislation in the cloud computing era. Because data is stored in the provider's datacenters, the process of compliance is complicated in the SaaS environment. This can lead to regulatory compliance issues such data privacy, segregation, and security, which must be enforced by the provider.

3.5 Accessibility

Using a web browser to access apps over the internet makes accessing them from any network device, including public computers and mobile devices, much easier. However, this adds to the service's security threats. The Cloud Security Alliance has released a document describing the current state of mobile computing and the top threats in this area, including data-stealing mobile malware, insecure networks (Wi-Fi), vulnerabilities found in the device OS and official applications, insecure marketplaces, and proximity-based hacking.

3.6 Platform-as-a-service (PaaS) security issues

PaaS allows cloud-based applications to be deployed without the need to purchase and maintain the underlying hardware and software layers. PaaS, like SaaS and IaaS, requires a secure and dependable network as well as a secure web browser. PaaS application security is divided into two layers: PaaS platform security (i.e., runtime engine) and PaaS platform security (i.e., client apps installed on a PaaS platform). The platform software stack, which includes the runtime engine that runs the customer apps, is the responsibility of PaaS providers. PaaS, like SaaS, introduces data security concerns and other challenges, which are listed below:

3.6.1 Third-party relationships

PaaS also includes third-party web services components such as mashups, in addition to standard programming languages. Mashups are a type of mashup that combines multiple source elements into a single integrated unit. As a result, PaaS models inherit mashup security vulnerabilities such as data and network security. PaaS users must also rely on the security of web-hosted development tools as well as third-party services.

3.6.2 Development life cycle

Developers face the challenge of creating secure applications that can be hosted in the cloud from the standpoint of application development. The System Development Life Cycle (SDLC) and security will be affected by the rate at which cloud applications evolve. Developers must bear in mind that PaaS apps are constantly modified, thus they must ensure that their application development procedures are adaptable enough to keep up with changes. Developers must be aware, however, that any changes to PaaS components may jeopardize the security of their apps. Developers must be trained on data legal issues in addition to secure development methodologies, so that data is not stored in insecure locations. Data may be stored in a variety of locations with varying legal regimes, putting its privacy and security at risk.

3.6.3 Underlying infrastructure security

Because developers rarely have access to the underlying layers in PaaS, suppliers must secure both the underlying infrastructure and the application services. Even though developers have complete control over the security of their apps, they cannot be certain that the development tools offered by a PaaS provider are secure. Finally, there is a scarcity of information in the literature on PaaS security issues. PaaS provides development tools to create SaaS applications, while SaaS delivers software distributed over the web. Both of them, however, may employ multi-tenant architecture, which allows numerous users to access the same software at the same time. PaaS apps and user data are also stored on cloud servers, which, as mentioned in the preceding section, might be a security risk. Data is linked to a cloud-based application in both SaaS and PaaS scenarios. The provider is responsible for the security of this data as it is processed, transferred, and stored.

3.7 Infrastructure-as-a-service (IaaS) security issues

It provides a virtualized system that contains a pool of resources such as servers, storage, networks, and other computing resources that can be accessed through the Internet. Users have complete control and administration over the resources allotted to them, allowing them to run whatever software they want. As long as there are no security holes in the virtual machine monitor, cloud users have more control over security with IaaS than with previous models. They oversee the software operating in their virtual machines and of correctly configuring security settings. Cloud providers, on the other hand, are in charge of the underlying compute, network, and storage infrastructure. To limit the vulnerabilities posed by creation, communication, monitoring, modification, and mobility, IaaS providers must make a significant effort to safeguard their systems. Here are a few of the security concerns with IaaS.

3.8 Virtualization

Users can utilize virtualization to create, clone, share, move, and roll back virtual machines, allowing them to run a wide range of applications.

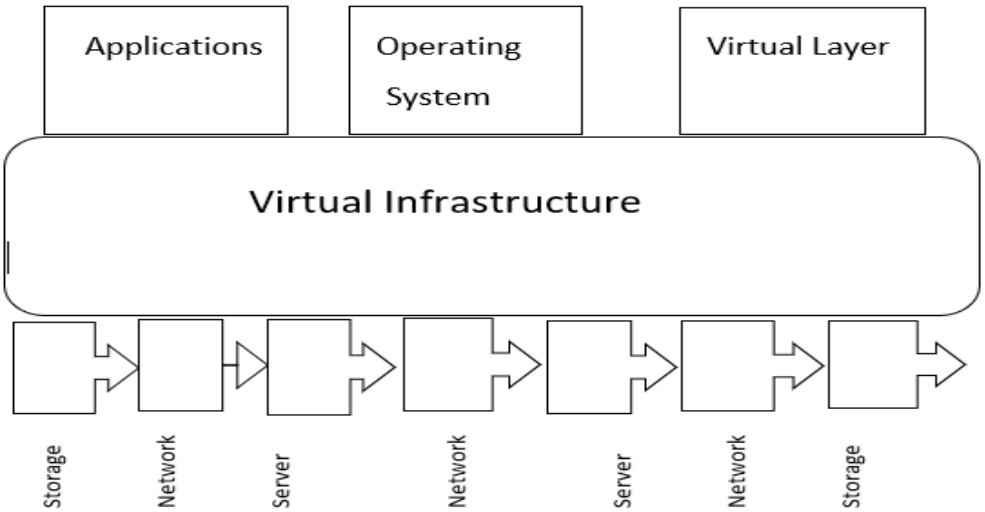

Figure 1. How virtualization works

However, because of the additional layer that must be guarded, it opens new options for attackers. Virtual machine security has surpassed physical machine security, and any defect in one can harm the other. For regular infrastructures, virtualized systems are vulnerable to all forms of assaults; however, security is a harder problem since virtualization introduces more points of entry and interconnection complexity. Virtual machines, unlike actual servers, have two distinct boundaries: physical and virtual.

3.9 Virtual machine monitor

The Virtual Machine Monitor or hypervisor is liable for virtual machines separation; along these lines, if the VMM is compromised, its virtual machines may conceivably be compromised too. The VMM is a low-level programming that controls and screens its virtual machines, so as any conventional programming it involves security imperfections. Keeping the VMM as straightforward and little as conceivable decreases the danger of safety weaknesses, since it will be simpler to discover and fix any weakness.

In addition, virtualization acquaints the capacity with move virtual machines between actual workers for adaptation to non-critical failure, load adjusting or support. This valuable component can likewise raise security issues. An assailant can think twice about movement module in the VMM and move a casualty virtual machine to a malevolent worker. Likewise, obviously VM movement uncovered the substance of the VM to the organization, which can think twice about information respectability and classification. A noxious virtual machine can be moved to another host (with another VMM) compromising it.

3.10 Shared resources

VMs on the same server can share resources such as CPU, memory, and I/O. Sharing resources between VMs may compromise each VM's security. A malicious VM can, for example, use shared memory or other shared resources to infer information about other VMs without compromising the hypervisor. Two VMs can communicate using covert channels, bypassing all the rules

provided by the VMM's security module. As a result, a malicious Virtual Machine can monitor shared resources without attracting the attention of its VMM, allowing the attacker to deduce information about other virtual machines.

3.11 Virtual networks

Organization parts are shared by various occupants because of asset pooling. As referenced previously, sharing assets permits aggressors to dispatch cross-occupant assaults. Virtual Networks increment the VMs interconnectivity, a significant security challenge in Cloud Computing. The most solid way is to snare each VM with its host by utilizing committed actual channels. Be that as it may, most hypervisors utilize virtual organizations to connect VMs to convey even more straightforwardly and proficiently. For example, most virtualization stages, for example, Xen give two different ways to arrange virtual organizations: connected and steered, however these strategies increment the likelihood to play out certain assaults, for example, sniffing and ridiculing virtual organization.

4. Analysis of security issues in cloud computing

We examine the current security weaknesses and threats to Cloud Computing in a systematic manner. We determine which cloud service models are affected by these security issues for each vulnerability and threat. This work provides a brief summary of the vulnerabilities as well as a list of cloud service models (SPI) that may be impacted. We primarily focus on technology-based vulnerabilities in this research; however, there are other vulnerabilities that are common to any business and must be considered since they might compromise the security of the cloud and its underlying platform. The following are a few examples of these flaws. Poor hiring methods and a lack of personnel screening - Some cloud service providers may not conduct background checks on their personnel or vendors. Cloud administrators and other privileged users typically have unrestricted access to the data in the cloud.

Customer background checks aren't done - Most cloud providers do not conduct background checks on their customers, and nearly anyone with a valid credit card and email address can open an account. Attackers can use fictitious accounts to carry out any nefarious action without being detected. Lack of security education - Information security continues to be hampered by individuals. This is true in any form of organization; but because there are more people who engage with the cloud: cloud providers, third-party providers, suppliers, organizational customers, and end-users, it has a greater impact in the cloud. Many current technologies, such as web services, web browsers, and virtualization, are used in cloud computing, which adds to the advancement of cloud environments. As a result, any vulnerability linked with these technologies has an impact on the cloud, and it can be considerable.

5. Countermeasures

5.1 Account or service hijacking

Identity and access management guidance – The Cloud Security Alliance (CSA) is a non-profit organization dedicated to promoting the implementation of best practices in cloud security. The CSA has published Identity and Access Management Guidance, which includes a list of best practices for ensuring identities and secure access management. Access management, identity management, role-based access control, user access certifications, privileged user and access management, division of roles, and identity and access reporting are all covered in this study. **Dynamic credentials -** Proposes a method for generating dynamic credentials for cloud computing systems on mobile devices. When a user changes their location or exchanges a particular number of data packets, the dynamic credential's value changes.

5.2 Data leakage

Fragmentation redundancy scattering (FRS) technique – Intrusion tolerance and, as a result, secure storage are the goals of this technique. This method entails breaking down sensitive material into negligible fragments, each of which has no relevant information on its own. The fragments are then dispersed across the distributed system's several sites in a redundant manner. Digital signature - Recommends employing a digital signature with the RSA method to safeguard data while it is being sent over the Internet. According to them, RSA is the most well-known technique and can be used to secure data in cloud environments.

5.3 Encryption

For a long time, encryption techniques have been employed to protect sensitive data. Data security is ensured by sending or keeping encrypted data on the cloud. It is true, though, if the encryption algorithms are strong. AES, for example, is a well-known encryption technique (Advanced Encryption Standard). SSL technology can also be used to secure data while it is being transmitted.

5.4 Customer data manipulation

Web application scanners - Because web apps are open to the public, including prospective attackers, they can be an easy target. Web application scanners are programs that scan web applications using the web front-end in order to detect security flaws. Other online application security tools, such as a web application firewall, are also available. The web application firewall inspects all web traffic and routes it through the web application firewall.

5.5 Virtual machine escape

Hyper safe - It's a method for ensuring hypervisor control-flow integrity. Hyper Safe uses two strategies to protect type I hypervisors: non-by passable memory lockdown, which prevents write-protected memory pages from being updated, and restricted pointed indexing, which converts control data into pointer indexes. They executed four sorts of assaults to test the effectiveness of this approach: alter the hypervisor code, run the injected code, modify the page table, and tamper from a return table. They concluded that Hyper Safe had successfully stopped all the assaults and that the performance overhead was minimal. Trustworthy cloud computing platforms - TCCP empowers suppliers to offer shut box execution conditions and permits clients to decide whether the climate is secure prior to dispatching their VMs. The TCCP adds two major components: a believed virtual machine screen (TVMM) and a confided in facilitator (TC). The TC takes an interest during the time spent dispatching or moving a VM, which confirms that a VM is running in a confided in stage. The creators guaranteed that TCCP has a critical drawback because of the way that every one of the exchanges need to check with the TC which makes an overburden. They proposed to utilize Direct Anonymous Attestation (DAA) and Privacy CA plan to handle this issue.

6. Conclusion

Cloud Computing is a relatively new concept that offers a variety of advantages to its users; nevertheless, it also raises significant security concerns that may limit its use. Understanding the vulnerabilities in Cloud Computing will assist enterprises in making the transition to the Cloud. Because Cloud Computing makes use of a variety of technologies, it also inherits their security flaws. Traditional web applications, data hosting, and virtualization have all been examined, however some of the solutions provided are either incomplete or non-existent. We've discussed security concerns for many cloud models, including

IaaS, PaaS, and IaaS, which differ based on the model. The major security risks in Cloud Computing, as discussed in this study, are storage, virtualization, and networks. One of the primary problems for cloud customers is virtualization, which allows numerous users to share a physical server. Another issue is that there are various types of virtualization technologies, each of which takes a different approach to security procedures. Some attacks target virtual networks, particularly when communicating with remote virtual machines. Some overviews have examined security issues about mists without having any effect among weaknesses and dangers. We have zeroed in on this differentiation, where we consider critical to comprehend these issues. Counting these security issues was sufficiently not; that is the reason we conveyed a connection among intimidations and weaknesses, so we can distinguish what weaknesses add to the execution of these dangers and make the framework more vigorous. Likewise, some current arrangements were recorded to moderate these dangers. Notwithstanding, new security strategies are required just as updated conventional arrangements that can work with cloud structures. Customary security instruments may not function admirably in cloud conditions since it is an intricate design that is made of a blend of various innovations.

7. Acknowledgements

The successful completion of my training would be incomplete without thanking the people who made it possible with all their hard work, dedication, and knowledge. My pleasure and gratitude to **Dr. Pawan Singh,** who inspired me with new ideas and gave me motivation to complete my project and for her guidance and constant support during the period of my work. I am very grateful to her for she has not only guided me in the right direction but also helped me in solving my problems in all possible ways and teaching me new and exciting techniques in the field of chemistry. And I finally thank to my family and my friends for their love and constant support.

References

[1]. M. K. Sasubilli and Venkateswarlu, “Cloud computing security challenges, threats and vulnerabilities,” in 6th International Conference on Inventive Computation Technologies (ICICT), 2021.
[2]. K. Hashizume, D. G. Rosado, E. F. Medina, et al, “An analysis of security issues for cloud computing,” J. Internet Serv. Appl., vol.4, no.1, pp. 5, Feb 2013.
[3]. R. Mogull, J. Arlen, F. Gilbert, et al,” Security guidance for critical areas of focus in cloud computing v4.0”, Cloud Security Analysis Research Publications. https://cloudsecurityalliance.org/download/security-guidance-v4/, July 2017.
[4]. YumpuePPER,”cloudcomputingInformationSecurityBrief-ing,01/2010CPNI,”.https://www.yumpu.com/en/document/view/35595642/cloud-computing-information-security-briefing-01-2010-cpni, Jan 2015.
[5]. Top threats,” Cloudsecurityalliance.org. [Online]. Available: https://cloudsecurityalliance.org/research/top-threats. [Accessed: 21-Jul-2022].
[6]. OWASP: The Ten most critical Web application Security risks. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[7]. IBM. (n.d.). Identity Mixer. Retrieved from www.zurich.ibm.com/security/idemix/
[8]. International Telecommunication Union, “Distributed Commuting: Utilities, Grid & Clouds”. https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000090001PDFE.pdf “March 2009.
[9]. P. Mell & T. Grance, “NIST Definition of Cloud Computing,” Retrieved from ver.15,” Computer Security Resources Center NIST” www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf ,July 2009.
[10]. S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” in Financial Cryptography and Data Security, Berlin, Heidelberg: Springer Berlin Heidelberg, LNCS, vol.6054, pp. 136–149,2010.
[11]. J. Horrigan, Use of Cloud Computing Applications and Services, Pew Research Center: Internet, Science & Tech. https://policycommons.net/artifacts/626957/use-of-cloud-computing-applications-and-services/1608265/ on 21 Jul 2022.
[12]. A. R. Lombarte “Madrid Resolution, International Standards on the Protection of Personal Data and Privacy”,” International Conference of Data Protection and Privacy Commissioners, “pp.1-36, Nov 2009.