IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

DATA SECURITY AND PRIVACY IN CLOUD COMPUTING

Km Komal[1] , Dr Puspneel Verma[2] ,Ajay Singh[3],Pawan Kumar Goel[4]
Research Scholar, Bhagwant Institute of Technology, Muzaffarnagar, UP, India

Abstract:-

Cloud Computing is a popular buzzword in today's computing world.The cloud is a global platform that enables digital information to be stored and distributed at a low cost and in a very short amount of time. Many consumers are interested in storing their valuable data in the cloud these days because data is so large.In cloud computing, application software and databases are relocated to centralized massive data centers, where data and service management may not be completely trustworthy.Cloud computing is a technology platform for IT enabled services delivered over the internet that is scalable, rapid, flexible, and cost-effective.There are numerous benefits to cloud computing, but in the end, cloud service users must send their data to third-party servers that are not directly controlled by the data owner. In the eyes of users, data security has always been a big issue in information technology, particularly in cloud computing. This is especially true in government, industry, and business. In the cloud architecture, data security and privacy protection concerns both hardware and software.Cloud security is quickly establishing itself as a major difference and competitive advantage among cloud providers.Despite the numerous advantages that cloud computing services bring, cloud computing service consumers are concerned about the security of their data.So, this article focuses on a variety of topics related to cloud computing, data security, and how the cloud ensures data integrity, confidentiality, and availability for users. How will data saved on cloud storage systems be kept safe from hackers?Another problem is risk management for data stored in the cloud.It is necessary to understand the dangers that a company will face when storing data and services in the cloud.We describe in this paper the obstacles that are keeping individuals from adopting the cloud and how to mitigate them.

Keywords: Cloud Computing, Integrity, Confidentiality, Availability.

INTRODUCTION

Although there are various alternative definitions of cloud computing, they all agree on how to provide services to network users. Cloud computing is a type of technology development that is based on the Internet. It refers to the use of computing resources, hardware, and software that are offered as a web service on demand. It provides a number of services to network users, including applications, storage, various processes, and remote printing, among other things. [1]. It usually entails the provision of dynamically scaled and occasionally virtualized resources over the internet [2].Businesses use the cloud to operate a variety of apps. Cloud computing is frequently thought of as a system that stores data, may be used in a variety of applications, and can be operated remotely without the need to download specific software onto machines.

The following are a few of the potential advantages of cloud computing that apply to most types of cloud computing.

1. Cost savings: Companies can increase their computing capacity by utilizing operational expenses and reducing capital expenses.
2. Flexibility: Cloud computing's pliability enables businesses to use more resources during peak times to meet customer requests.
3. Reliability: Multi-redundant site services can aid in business continuity and disaster recovery.
4. Lower Maintenance: Cloud service providers handle system maintenance, which does not necessitate the installation of applications on PCs.
5. Mobile Accessible: Mobile workers have boosted productivity thanks to solutions that are accessible from anywhere in the infrastructure.
6. Transparency: Additional servers can be added to the supplied service without disrupting it or requiring the appliance delivery solution to be reconfigured.
7. Transparency is also provided by automated resource provisioning and de-provisioning if the appliance delivery solution is integrated via a management API.

The National Institute of Standards and Technology (NIST) [2] defines "cloud computing" as "a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing, according to the explanation, allows on-demand network access to a shared pool of programmable computing resources.Computing applications, network resources, platforms, software services, virtual servers, and computing infrastructure are among the resources requested. Cloud computing is frequently regarded as a replacement computing model that will give on-demand services at a low cost.Within the cloud paradigm, there are three well-known and widely utilized service models: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) .

In SaaS, a cloud service provider deploys software along with accompanying data, which consumers can access via online browsers.

In PaaS, a service provider provides users with services via a suite of software programmes that fulfil specific tasks.

In IaaS, the cloud service provider provides virtual machines and storage to users to help them expand their business capabilities.

Data is distributed across multiple computers and storage devices, such as servers, PCs, and other mobile devices such as wireless sensor networks and smart phones, data security becomes more important in the cloud computing environment.The security of data in cloud computing is more sophisticated than that of traditional information systems.However, data protection mechanisms must be improved further.

Cloud computing services are available across the entire computing spectrum. Organizations are now shifting and expanding their businesses by utilizing cloud computing to reduce costs.This can help free up additional manpower to focus on strategic differentiation and make the corporate division of labour more obvious.The cloud is becoming more popular as it offers high-performance computing at a lower cost.Cloud services have been supplied on the Internet by well-known IT businesses like as Amazon, Microsoft Azure, Google, and Rock Space.

When it comes to trusting the system, cloud computing introduces certain characteristics that require specific consideration. The information security and prevention strategies used in the system determine the system's overall trustworthiness. Researchers have tested and introduced a variety of tools and approaches for data security and prevention in order to realise and remove the trust barrier, but there are still gaps that need to be filled by making these techniques more better and effective.

Resource security, resource management, and resource monitoring are all key concerns in cloud computing.

2. CLOUD COMPUTING COMPONENTS AND MODELS

Cloud computing is often regarded as the next generation of IT enterprise design.Cloud computing is a sort of network in which there is no central controller, making security a primary concern for the network.Many new security challenges arise as a result of this new paradigm.

The platforms, such as front end, back end, and cloud-based delivery, as well as the network employed in the cloud are referred to as components.In a simple topology, the main components of cloud computing are split into three parts: clients, datacenters, and distributed servers.

Clients in a cloud computing architecture are claimed to be the same as those in traditional local area networks (LANs).The majority of them are desktop computers.Laptops, tablet computers, mobile phones, and PDAs, for example, are all key drivers for cloud computing due to their mobility.Clients connect with in order to manage their data in the cloud.

A datacenter is a collection of servers; it may be a large space in the basement of your building packed with servers on the other side of the world that you connect to via the internet.Virtualizing servers is a growing trend in the IT sector.That is, software is frequently deployed to enable the operation of numerous instances of virtual servers.You'll have a half-dozen virtual servers running on one real server this way.

Distributed Servers refers to the placement of a server in a separate location.The servers, on the other hand, do not have to be housed in the same location.Servers are frequently located in different parts of the world.Several components are necessary for cloud computing services, including [3].

Cloud Clients are computers or software that are specifically built to use cloud computing services.

Example :Mobile - Windows Mobile, Symbian
Thin Client - Windows Terminal Service, Cherry Pal
Thick Client - Internet Explorer, Firefox, and Chrome

B. Cloud Services: Cloud services relate to products and solutions that are offered over the internet.

Identity (Open ID, OAuth, etc.) is an example. Amazon Simple Queue Service integration. PayPal and Google Checkout are two options for making payments. Google Maps and Yahoo! Maps are two mapping services.

C. Cloud Applications: Cloud applications are software applications that leverage Cloud Computing in their architecture so that customers don't have to install anything but can use the appliance with a computer.

Example: BitTorrent, SETI, and other peer-to-peer networks are examples of peer-to-peer networks. Facebook is a web application. Google Apps, SalesForce.com, and others are examples of SaaS.

D. Cloud Platform, a service that consists of hardware and infrastructure software and is part of a computer platform. This service could be part of a computing platform that includes hardware and software for infrastructure. Web Application Frameworks - Python Django, for example.NET Framework, Ruby on RailsForce.com is a private web hosting company.

E. Cloud storage is a type of data storage that is provided as a service. Example:Google Big Table and Amazon Simple DB are two databases to consider. NirvanixCloud NAS, NirvanixCloudNAS, NirvanixCloudNAS, NirvanixCloudNAS, NirvanixCloudNAS,iDisk for MobileMe.

F. Cloud Infrastructure is a service that provides access to the internet.Infrastructure as a Service (IaaS) is a term that refers toExample:Sun Grid is a grid computing platform.,GoGrid and Skytap provide full virtualization.,Amazon Elastic Compute Cloud – Compute

III. SERVICE MODELS OF CLOUD COMPUTING

SAAS (Storage-as-a-service) - This refers to the disc space we use once we lack a storage platform and thus request it as a service.

Database-as-a-service - This component works as a database that is accessed directly from a remote server, with the same capability and features as if the database were physically present on the local machine.

Information-as-a-service (IaaS) is a term used to describe information that can be accessed remotely from anywhere.Emphasize the ease with which information can be accessed from a distance. Process-as-a-service - This component, unlike others, brings together a variety of resources such as data and services.This is primarily used for business processes that incorporate several critical services and knowledge to form a process.

Application-as-a-service (AaaS) - as the name implies, this is frequently a complete package for obtaining and using apps.This is designed to connect people to the internet, and consumers often access this service using browsers and hence the internet.This component serves as the user's primary interface.

IV. CLOUD COMPUTING DEPLOYMENT MODELS

We may have a variety of deployment methods from which consumers can choose based on their requirements and availability [4].

A. Private Cloud: A cloud that is exclusively used by one company. The cloud may be managed by the company or by a third party. The private cloud has minimised possible security risks when properly installed and administered.

B. Public Cloud: a cloud that the general public can use (for a price), and which involves an organisation employing a cloud infrastructure that is shared via the Internet with many other organisations and members of the public;

Microsoft, Google, and Amazon, for example [14]. The security hazards associated with the public cloud must be examined.

C. Community Cloud: is a cloud that is shared by several companies and is typically set up for their similar security requirements and the need to store or process data of similar sensitivity, such as multiple government agencies [14].

D. Hybrid Cloud is a hybrid cloud deployment model that combines several cloud deployment models. Each cloud will be administered individually, but apps and data will be able to flow across them. Private cloud resources can be migrated to public cloud if more are needed. (14) Hybrids are designed with specific business and technological requirements in mind, which helps to maximize security and privacy while lowering IT costs.

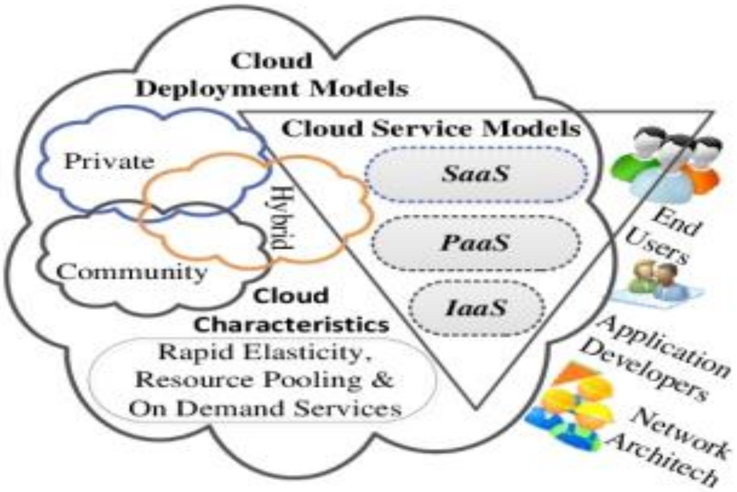

Fig -1 cloud computing models

V) Threats to the security of cloud computing

Cloud computing offers customers and companies money savings and operational benefits, but it also creates new security concerns and uncertainties.The larger attack surface in a cloud environment makes it possible to exploit additional vulnerabilities, raising the risk to the enterprise.The term "risk" refers to a threat that can harm an organisation by taking advantage of a weakness in one or more assets.The danger to the organisation rises as a result of the increased attacks in the cloud environment, which make use of virtual switches and hypervisor that are absent from traditional data centres.

The following dangers are listed as the most significant: [5], [6]

A. **Data Breaches:** Preventing any data violations is of utmost importance. Because "solutions you put in place to improve one can aggravate the other," tackling the threats of data loss and data leaking is difficult. In order to lessen the severity of a violation, data is encrypted; but, if the encryption key is lost, the data will also be lost. Offline knowledge backups, on the other hand, enhance vulnerability to data breaches if they are chosen to reduce data loss.

B. **Data loss or leakage:** Without adequate authentication, authorization, and audit (AAA) measures, it is possible to lose or change records without a copy of the original data. An encoding key can be effectively destroyed if lost. Sensitive information may be accessed by unauthorised individuals. The data of a target could be deleted by an evil hacker.

C. **Account or Service Hijacking:** A variety of hijacking techniques, including phishing, fraud, and the exploitation of software flaws, continue to be effective. If an attacker is able to access user credentials, he can monitor user behaviour and transactions, altering the data, including bogus information, and directing user clients to malicious websites.

D. **Application Programming Interfaces** (APIs) that aren't secure These interfaces need to be built to defend the user against both innocent and malevolent attempts. Examples of this kind of risks include attacks involving anonymous access, reusable tokens or passwords, clear-text content transmission or authentication, rigid access rules or erroneous authorizations, and inadequate monitoring and recording capabilities.

E. **Insider Threats**: A provider might withhold information about how it monitors, analyses, and grants access to employees to physical and virtual assets. The business is not required to understand the specific technicalities of how the services are supplied with cloud computing. In some circumstances, the risk is high. Your company could be in risk if you don't have complete awareness and control. In some circumstances, the risk is high. Your company could be in risk if you don't have complete awareness and control.

VI. CLOUD COMPUTING'S PROBLEM WITH DATA SECURITY

The following list of security issues is provided [7].

A. Security Issue with the VM:-The primary difference between IBM's Blue Cloud and Windows Azure is whether virtual machines run on the Linux operating system or the Microsoft Windows operating system. Virtual machine technology is used by both IBM's Blue Cloud and Microsoft's Windows Azure.

The use of virtual machines has many benefits, including the ability to run servers that are no longer connected to actual devices but rather operate on virtual servers. A phase shift or migration in a virtual machine has no impact on the services offered by the service provider. Without taking into account the hardware, the provider can meet the user's needs if they require additional services. But the logical server group's virtual server adds a tons of security issues[8][9].

Traditional data centre security measures are based on the hardware platform, but cloud computing could also be a server with multiple virtual servers. Because these servers could be members of different logical server groups, they could potentially attack one another, which poses a lot of security risks for virtual servers.

Virtual machines that extend the reach of cloud computing clouds cause the network barrier to vanish, impacting the majority of security concerns. Analysis of Data Security and Privacy for Cloud Computing.

B.Existence of Super user:-

The existence of super-users substantially simplifies the information management function for the company offering cloud computing services, but it poses a serious risk to user privacy. The company needs the right to manage and maintain data, and they need to be able to handle it. Superpowers are a two-edged blade that simultaneously provides people with convenience and puts them in danger. The fact that cloud computing platforms can provide personal services while maintaining the anonymity of private privacy on the existence of flaws is undeniable in an era where personal data should be truly secured. Both individual users and corporations could face dangers, for example, corporate users and trade secrets kept on the cloud computing platform could be taken.

C. Data Consistency:-

User’s data is transmitted from the data centre to their clients in a cloud environment. The user's data is always changing for the system, read and write information about the Difficulties with user identity authentication and permissions The data of several users may also be present in a virtual machine and need to be strictly controlled. Because the typical access control approach is built into the perimeter of computers, it is difficult to govern reading and writing across distributed computers. It is obvious that cloud computing environments do not lend themselves to traditional access control. The conventional access control technique has significant flaws in the cloud computing context.

D. Technology Innovation:-

The cloud computing idea is built on modern technology. The new architecture included a variety of cutting-edge technologies, including Hadoop and Hbase, which boost cloud system performance but also introduce hazards. In the cloud environment, users can form dynamic virtual organizations. Instead of happening on an individual level, the first cooperation typically happens during a relationship of trust between companies. Therefore, those users supported the declaration of limitations on the idea of proof technique, which is typically challenging to follow and frequently arises in numerous interacting nodes between the virtual machine. The unrestricted access to resources that a user can "purchase" in a cloud computing environment has exacerbated security issues.

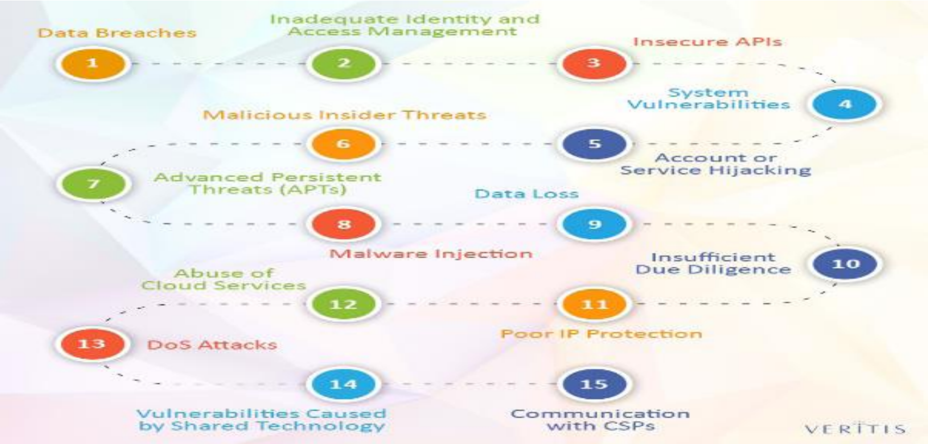
Data Breaches
1
Inadequate Identity and Access Management
2
Insecure APIs
3
System Vulnerabilities
4
Account or Service Hijacking
5
Malicious Insider Threats
6
Advanced Persistent Threats (APTs)
7
Malware Injection
8
Data Loss
9
Insufficient Due Diligence
10
Poor IP Protection
11
Abuse of Cloud Services
12
DoS Attacks
13
Vulnerabilities Caused by Shared Technology
14
Communication with CSPs
15
VERITIS

Fig. 2: Issues with cloud security

VII. CLOUD COMPUTING DATA SECURITY CONCERNS

Cloud computing security entails protecting virtualized IP, data, applications, and services utilising a wide range of rules, technologies, applications, and controls. Cloud data is subject to a variety of risks[11][12].

cloud services are misused through services like network eavesdropping, denial of service attacks, side channel attacks, and other vulnerabilities.

CONCLUSION

A promising and developing technology for the next wave of IT applications could be cloud computing. Data security and privacy concerns are the roadblocks and obstacles to the cloud computing industry's quick ascent. Any firm may be required to reduce data storage and processing costs, but knowledge analysis is typically one of the most crucial activities for decision-making across all enterprises. As a result, no organisations will move their data or information to the cloud unless users and cloud service providers are able to trust one another. However, like with other technologies as they develop, there will be several security risks.

These concerns revolve around protecting data from illegal access at remote locations, maintaining the data's integrity while it is held there, and making the information accessible when it is required. Additionally, it is problematic to share data in the cloud with a cloud service provider you don't trust.

These problems include ones involving the internet's earlier problems, network problems, application problems, and storage problems. A number of strategies have been put forth by researchers for data protection and to achieve the maximum level of data security in the cloud. Storing data on a remote server raises some security concerns. Numerous research have been carried out to identify the problems that affect the confidentiality, integrity, and accessibility of data in order to find a solution. These solutions will strengthen the security of cloud storage, which will increase public adoption of the cloud and boost public confidence in it. To get the support of users of cloud services, more effort must be done on cloud computing.

Security needs to be regularly examined with the expansion of cloud computing. Before interacting with the current cloud computing environment, Users should be informed of the various security issues that may arise. We have identified the main data security, data integrity, confidentiality, and availability concerns that cloud computing consumers and providers may have. In order to foster confidence between customers and cloud service providers, this article discussed many CIA concerns while concentrating on how secure data storage in cloud computing settings is.

Reference

[1] Article in the Journal of Theoretical and Applied Science entitled "Data Integrity in Cloud Computing Security."

[2] Data Integrity in Cloud Computing Security, 31st December 2013, Journal of Theoretical and Applied Information Technology. Vol. Int 2 of 58 No. 3 Brian O. et al., Cloud Computing, 2012-11-06, page 6, published in Swiss.

Components of Cloud Computing, By Cloud Storage February 14, 2019 [3] - Information about cloud news

[4] Data integrity in cloud computing security, ResearchGate article, Journal of Theoretical and Applied Information Technology, Vol. 58, No. 3, December 2013, p. 570

[5] Apponix Technologies: Cloud Security, Scribd, Apponix Technologies: Cloud Security, Cloud Computing, Public Key

[6]Top 10 Could Computing Threats (IT Blog)

[7]IJRST, 2013, Vol. 7, International Journal of Research in Science and Technology Data Security Modal for Cloud Computing, Vol. 2, No. 5, April-June

[8] Research Gate article from January 2018 published in Procedia Computer Science, "Exploring Data Security Issues and Solutions in Cloud Computing."

[9] Cloud Storage Security Standards and Best Practices for Enterprise Storage, by Samuel Greengard, published on December 5, 2018

[10] International Journal of Advanced Computer Science and Applications, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions," Vol. 7, No. 4, 2016

[11] A. In "Incremental proxy re-encryption strategy for mobile cloud computing environment," N. Khan, M. M. Kiah, S. A. Madani, M. Ali, S. Shamshirband et al., The Journal of Supercomputing, Vol. 68, No. 2, pp. 624-651,2018.

[12] P. P. Venkateswarlu, S. Kumari, and M. International Journal of Research, Vol. Afzal, "A vital aggregate framework with adaptable offering of information in cloud," 2, No. 3, pp. 5-10, 2015.

[13] C.-K. S. S. Chow, J. Zhou, W.-G. Tzeng, and R. Key-aggregate cryptosystem for scalable data sharing in cloud storage, IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, pp. 468-477, 2017.

[14] R. Enhancing data security in cloud computing by A. Sana Belguith and Abderrazak Jemai

[15] Complete information on the cloud news item Cloud Computing Components, By Cloud Storage, February 14, 2019