WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Investigation of Data Security Issues and Challenges in Cloud Computing Environment

***Neha Khandelwal*[1]**

Department of Information Technology, Swami Vivekanand College of Engineering, Indore M.P

ABSTRACT:

Another term for cloud security is cloud computing security. For virtual infrastructure, which consists of hardware, software, and applications, it is the policy, technology, application, and control set. This field encompasses database security, web security, network security, and other related areas. To put it another way, there are significant similarities between cloud, computer, and information security. Because IT infrastructure is becoming a daily requirement for every individual and organization, security is a big concern. Several components, including obstacle control, preventive control, analyst control, and aggregate control, limit the security of distributed computing. This essay explores various aspects of safety in a basic way and is reasonable in nature. Cloud-related security concerns are also covered in the paper.

KEYWORDS: - Cloud Computing, IT Security, Cloud Security, Security policy, Cloud Computing Challenges, Security Risks & Solutions.

1. INTRODUCTION

A contemporary technology that has completely changed how people and businesses conduct business is cloud computing. A cloud is an internet-based model for the on-demand delivery of computer resources, such as servers, storage, and applications. As long as they have an internet connection, businesses and individuals can now store, process, and access their data from almost anywhere. Despite all of the technology's advantages, there are security concerns with cloud computing. Because of the possible security risks associated with cloud computing, both individuals and organizations are reluctant to adopt it. This research paper will look at the various security issues related to cloud computing The method, methods, and procedure for protecting data and contents from online systems is referred to as cloud computing security, or simply cloud security. Most of the time, cloud security is a way to prevent data leaks and deletions. Among the most common ways to keep cloud systems or online systems safe are the following:

- Use of firewall
- Penetration testing
- Use VPN only in real need
- Tokenization

II. CLOUD SECURITY: THE ROOT

In addition to being closely related to organization security, data set security, web security, and other security concepts, cloud security is also referred to as distributed computing security. Furthermore, it bears a striking resemblance to information technology security [8, 10]. Cloud security is important because it primarily concerns the safe and secure data and objects stored in cloud infrastructures. Moreover, security is necessary for distributed computing in all modes and stages. Distributed computing is the IT Framework's virtualization, encompassing products, gear, businesses, websites, and more. The following models can be used, or they can be designed and developed using:

1. **Public Cloud Computing**
2. **Private Cloud Computing**
3. **Hybrid Cloud Computing**

Public Cloud Computing— It is the development and implementation of IT infrastructure virtually from distant locations using relevant internet-based technologies. Private clouds are the most widely used type of cloud. Resources specific to each client are dynamically provided for parties by a third-party vendor. This third-party supplier provides all security upkeep, hosts the cloud for multiple clients across multiple data centers, and provides the

required hardware and infrastructure necessary for the cloud's operation. The client has no access to, control over, or knowledge of the infrastructure that is available or how the cloud is managed.

Private Cloud Computing— It is the independent design and development of their own cloud-based infrastructure within their borders. Private clouds replicate the concept of cloud computing on a private network. They let users benefit from cloud computing's advantages while avoiding some of its disadvantages. Total control over data management and the applied security measures is provided by private clouds.

Hybrid Cloud Computing—It is the blending of public and private cloud computing, with applications determined by need. Hybrid clouds integrate the two clouds into a single network. It permits the organizations to profit from both deployment options.

Hybrid Cloud=Public Cloud Private Cloud

III. SECURITY POLICY: THE WAY

It is possible to stay up to date with cloud security using modern methods, so agreements may vary from specialist co-ops to specialist co-ops or even client to client. It is also possible to compare security strategies based on the assistance model. The nuances are shown in Table 1 and generally speaking, cloud security approaches may vary depending on your types and organization models.

Table 1: Security Policies in Cloud

Security Policies respect of Deployment Models	Different Types of Cloud and Policies
Security Policies in Software-as-a-Service Security Policies in Security-as-a-Service Security Policies in Storage-as-a-Service Security Policies in Platform-as-a-Service Security Policies in Infrastructure-as-a-Service etc.	Public Cloud Computing Policies Private Cloud Computing Policies Hybrid Cloud Computing Policies

Cloud security demands a lot of capacity, so legitimate security should be ready to advance as well as strong administrations. Reviews of a cloud provider's security frameworks by outside parties are also important in certain situations. Moreover, Cloud Clients should protect access from unauthorized users, log-ins, accreditations, and other entities. Furthermore, data stored on cloud-based services hosted in different countries may be subject to different privacy policies and guidelines.

IV. RESEARCH CHALLENGES IN CLOUD COMPUTING

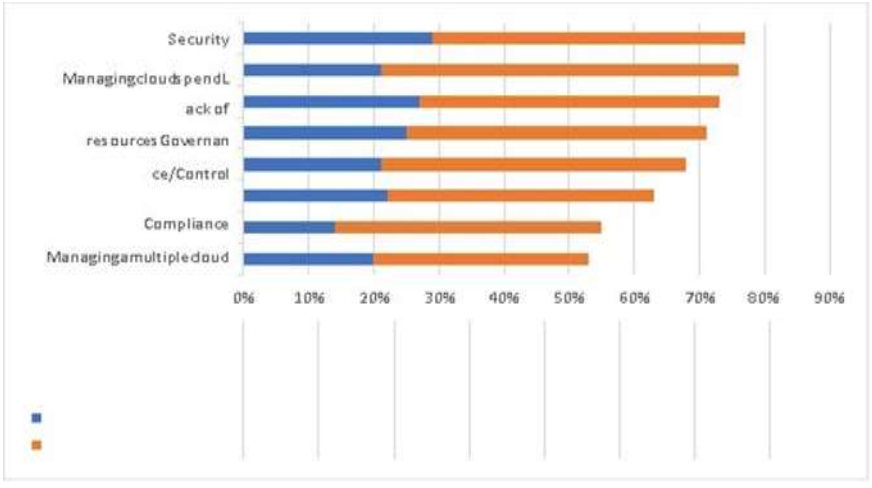

Figure 1:- Cloud Challenges

Despite the quick rise in popularity of cloud computing. Research on cloud computing is still in its infancy. Many problems are still unsolved, and new challenges are always appearing for every industry. There aren't many exam challenges in cloud computing up next.

1. Service level agreement (SLA)
2. Cloud data management and security
3. Data Encryption

4. Virtual machines migration
5. Access controls
6. Multi-tenancy
7. Reliability and availability of services

1. **Data Encryption:** In terms of information security, it is a crucial innovation. Remember that based on the problem or expense, security can be low, medium, or high. In this instance, APIs can be used as an example. When an object gets to the cloud, the data is decrypted and stored.
2. **Access Control :** To ensure the security and reliability of their cloud-based systems, associations need to address a few challenges related to access control in distributed computing. Scalability, shared responsibility, identity & authentication, and shared responsibility are the main challenges.
3. **Multi-tenancy:** What distinguishes multi-tenancy in cloud computing is that both the attacker and the victim use the same server, also referred to as a physical machine (PM). Due to its limited network layer monitoring and lack of server penetration, traditional security measures are unable to mitigate this setup. We have determined that the Multi- Tenancy effect cannot be eliminated due to its substantial benefits, based on prior research.

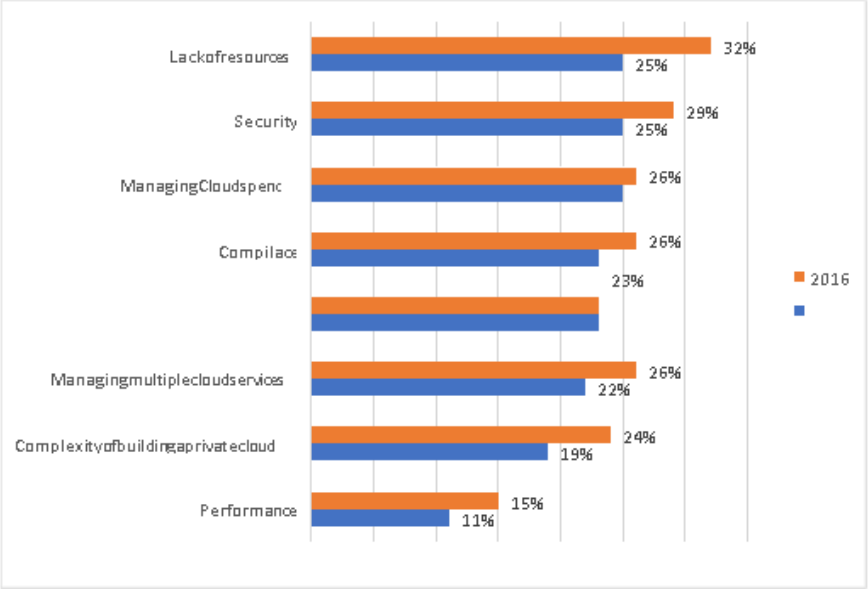

Figure 2 :- Cloud Challenges 2016 vs 2017

V. CLOUD COMPUTING SECURITY RISKS:

Figure 3 :- Seven Security Risks of Cloud Computing

1. **Data Breaches:**

A common threat to distributed computing is data breaches. Information breaches occur when attackers obtain unauthorized access to sensitive data stored on cloud servers. This might occur if the security protocols of the cloud provider are breached or if a client who has been approved for service by mistake shares their login credentials with a third party.

2. **Malware Attacks:**

Another significant security concern for distributed computing is malware attacks. Malware is used by cybercriminals to infiltrate cloud infrastructure and steal data. Malware can propagate via email merges, infected files, or by exploiting flaws in the cloud provider's product.

3. **Distributed Denial of Service (DDoS) Attacks :**

DDoS attacks are a type of cyberattack that aims to overwhelm a website or cloud administration system by sending an excessive amount of traffic to it. A botnet can be used to launch DDoS attacks, which aregrouping of malware-infected computers. Once a botnet is established, the attacker can use it to overload the cloud foundation with traffic, causing it to crash or stop working.

4. **Insecure APIs :**

APIs, or application programming interfaces, are used to facilitate communication between different programming applications. APIs are typically used in cloud computing scenarios to allow information sharing between different applications.

5. **Vendor Lock-in :**

Vendor lock-in is one of the main security risks associated with cloud computing. Shifting a company's services from one vendor to another may present difficulties. Switching between clouds can be difficult because different vendors provide different platforms.

6. **Loss of Control:**

By outsourcing infrastructure and services to the cloud, organizations relinquish some control over the physical security of their data. This loss of control can be unsettling for some organizations.

7. **Resource hijacking :**

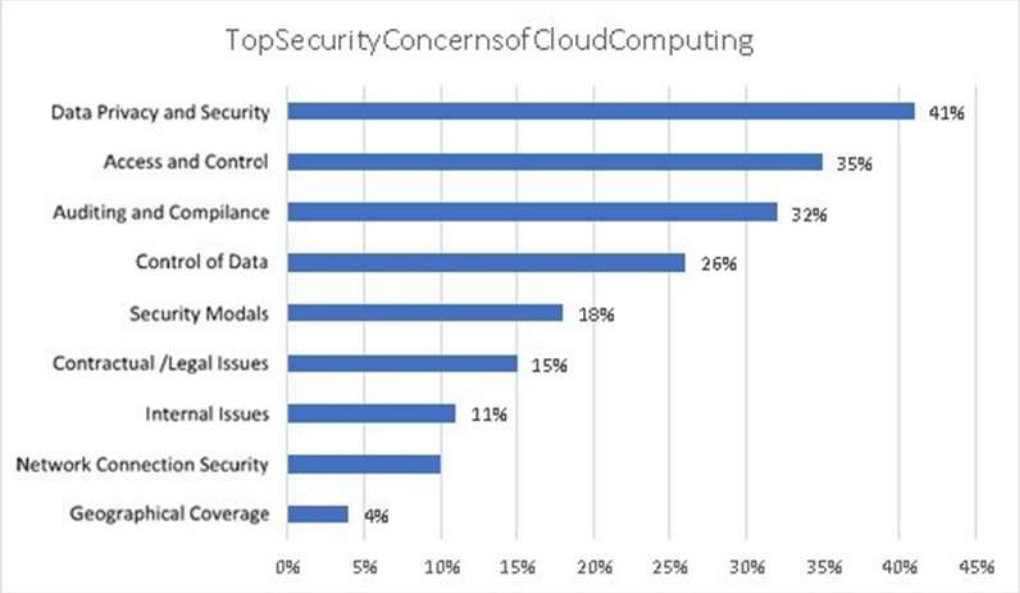

Figure 4:-Security concern swith cloud computing

VI. SOLUTIONS OF CLOUD COMPUTING SECURITY RISKS:

1. Data Encryption:

Data encryption is a foundational and multifaceted security solution critical to securing data in cloud computing. It addresses a spectrum of security risks by rendering data unintelligible to unauthorized users at rest, in transit, and during processing. Data at rest encryption ensures that stored information remains protected from physical or digital breaches, requiring encryption keys for access. Data in transit encryption safeguards data as it traverses the internet, thwarting interception and eavesdropping. Encryption during processing, with techniques like homomorphic encryption and secure enclaves, shields data even while it's being used or manipulated in cloud applications. This comprehensive approach protects against data breaches, unauthorized access, and complies with data protection regulations. Whether data is stored in cloud servers, transmitted through APIs, or analyzed within cloud services, encryption remains the cornerstone of security, bolstering data privacy, integrity, and availability in the cloud.

2. Multi-Factor Authentication (MFA) :

One essential cloud security solution that strengthens the protection of private information and resources online is multi-factor authentication (MFA). Multi-factor authentication (MFA) effectively reduces the growing risks associated with unauthorized access, data breaches, and compromised credentials by requiring users to submit multiple forms of verification before granting access. This strong security strategy includes elements like something you have (like a hardware token or smartphone), something you know (like a password), and something you are (like biometric traits). Because of this multi-layered authentication strategy, malicious actors will have a difficult time breaking security even if one factor is compromised. This makes multi-factor authentication (MFA) an invaluable defense against credential theft and unauthorized access, as well as a critical compliance enabler for data protection standards

3. Regular Security Audits

Regular security audits are a fundamental cloud security solution that ensures the ongoing integrity and resilience of an organization's digital infrastructure. By systematically evaluating the security measures, configurations, and policies within a cloud environment, security audits help identify vulnerabilities, compliance gaps, and potential threats. These assessments encompass network architecture, access controls, encryption, data management, and user permissions, among other critical elements. By conducting security audits on a routine basis, organizations can proactively address vulnerabilities, fine-tune their security posture, and align with best practices, ultimately fortifying their defenses against evolving cyber threats and maintaining the trust and compliance standards crucial for secure cloud operations.

VII. CONCLUSION:

These days, people are very concerned about security, and security is one of the most important things to remember. The great majority of associations use data innovation these days, and distributed computing is one of the most prominent emerging technologies. The cloud model is applicable to many associations and organizations, including bodies and associations in government. Additionally, there are a lot of benefits to cloud computing, such as cost-effectiveness, flexibility, and increased availability. However, it is impossible to ignore the security risks associated with distributed computing. Organizations and individuals should take proactive steps to store their data on cloud servers. Additionally, cloud providers should make sure that their

security protocols are strong and effective. By carryingout safety efforts like information encryption, MFA, and normal security reviews, the dangers related with distributed computing can be limited, and the advantages can be completely understood.

VIII. REFERENCES:

1. Shin S., Gu G., and Yoon J. (2014). "A Survey of Security Threats on Cloud Computing." Journal of Information Processing Systems, 10(1): 120-135.

2. Subashini S, Kavitha V: A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 2011.

3. National Institute of Standards and Technology, NIST Definition of Cloud Computing, Sept 2011.

4. Kyriakos Kritikos, Kostas Magoutis, Manos Papoutsakis, Sotiris Ioannidis, "A survey on vulnerability assessment tools and databases for cloud-based web applications," Array, Volumes 3–4, 2019, 100011, ISSN 2590-0056, https://doi.org/10.1016/j.array.2019.100011

5.Ananthi Claral Mary.T, Dr.Arul Leena Rose.P.J., Implications, Risks And Challenges Of Cloud Computing In Academic Field – A State-Of-Art, International Journal of Scientific & Technology Research (2019) Volume 8 Issue 12 ISSN 2277- 8616

6. Rittinghouse JW, Ransome JF: Security in the Cloud. In Cloud Computing. Implementation, Management, andSecurity, CRC Press; 2009.

7. H. Takabi, J.B.D. Joshi, and G.-J. Ahn, "Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," Proc. 1st IEEE Int'l Workshop Emerging Applications for Cloud Computing (CloudApp 2010), IEEE CS Press, 2010, pp. 393– 398.

8. Wang S., Zhao J., Zhang Z., and Jia L. (2018). "A Survey on Cloud Computing Security." Journal of Cloud Computing, 7(1): 1-24.

9.Bohn, R. & Messina, John & Liu, Fang & Tong, Jin & Mao, Jian. (2011). NIST Cloud ComputingReference Architecture. 594-596. https://doi.org/10.1109/SERVICES.2011.105