e-ISSN:2582-7219

# INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 5, May 2024

Impact Factor: 7.521

6381 907 438 6381 907 438 ijmrset@gmail.com www.ijmrset.com

# Securing SaaS: Key Challenges and Effective Mitigation Strategies

**Sai Shreya R, Kavitha R**

Department of Computer Science and IT, JAIN (Deemed-to-be University), Bangalore, India

Department of Computer Science and IT, JAIN (Deemed-to-be University), Bangalore, India

**ABSTRACT:** Cloud computing has fundamentally changed the research environment by offering unmatched scalability, collaboration tools, and immediate access to resources, significantly improving the efficiency and productivity of research endeavors. This transformation has led to a substantial enhancement in the conduct of research activities The study focused on conducting a detailed review to investigate the specific security vulnerabilities that Software as a Service (SaaS) providers encounter in the context of cloud computing. The advantages of cloud computing are vast for scholars and educational institutions, yet it is crucial for them to recognize these security risks and adhere to the suggested security protocols. By adopting a methodology that prioritizes security, researchers can ensure the confidentiality and integrity of their research data, thereby nurturing a secure and thriving environment for cloud-based research initiatives. Upholding a security-centric approach is critical in protecting sensitive research information from potential threats and vulnerabilities. Researchers must stay abreast of the evolving security landscape in cloud computing and consistently enhance their security frameworks to mitigate any potential risks effectively. In essence, the incorporation of robust security measures is indispensable for the enduring success and advancement of cloud-based research endeavors.

**KEYWORDS:** Cloud Computing; Security Vulnerabilities; Security Protocols; Mitigation strategies; Security Measures; Data Protection; Security Challenges.

## I.INTRODUCTION

Among the resources that can be shared over the internet is cloud computing. Commonly referred to as “the cloud,” cloud computing makes it possible for application software to work on internet-enabled devices seamlessly. Its functions are many through the internet, and storage stands out as one of its major roles. By ensuring that resources are utilized efficiently, there is uniformity while at the same time attaining economies of scale which makes it efficient and useful in equal measure.

Cloud computing has become a significant area in IT research. It is considered among the most critical features in terms of data storage, security, accessibility and cost-reliability. With increased technological advancement there has been wider use of internet services and an increase in hardware prices as well as software costs. Within a short span though, cloud- computing has proved very successful and gained popularity fast since its idea was to provide services whenever they are needed via the web thus reducing hardware/software expenses.[17],[18]

In today’s digital age, there are companies relying on cloud computing more and more to store, process, and even retrieve their business’ information. Scalability, flexibility and cost efficiency are some of the benefits that come with switching to a cloud environment but so does new security challenges. As organizations move their activities into the cloud, they need to protect their data and applications from threats.

The reason why security is important in cloud computing is because of the amount and sensitivity of stored or processed data. Different types of valuable data like personal information, intellectual property or trade secrets are entrusted by modern businesses to cloud service providers. This information can be exposed to many risks if not properly secured for example; cyber threats such as malware attacks unauthorized access among others. These breaches may have severe impacts including financial loss legal obligations reputation damage etcetera for an organization.

An administrator for a system could offer a different definition of cloud computing than that of a software developer, in fact so too can the database administrator. When we talk about ‘the cloud’ it refers to a broad range of on-demand services delivered over the Internet that enable users to access and utilize IT resources such as servers, storage and application software on an as-needed basis from any location. For instance, Microsoft, Amazon, Google among others offer various cloud-based services which can be consumed by subscribing to them whenever required. Included in this wide array are Identity Management Services; Storage Services; Messaging Services; Social Computing Services etc.

Different types of cloud computing can be classified using two models: deployment models and service models. Moreover, being a file backup system also allows sharing of common documents for different purposes by users at diverse locations simultaneously. This facilitates ease-of-use while at the same time enabling bypassing many restrictions often associated with traditional computers. Furthermore, quicker availability of resources is facilitated by agility through cloud computing.

Three main categories usually include the hosted services provided by cloud computing providers: SaaS, consisting of a provision of software; PaaS, a service of development platforms; and IaaS, infrastructures on-demand. The use of cloud services by customers becomes possible at any time when they need it. They can do it often with an hourly subscription. The path-with-usage model completely redefined the cloud computing market by allowing users customized services for diverse needs any time they want. It is significant to keep in mind, however, the provider of the cloud services, has a full command over them, thus in a nutshell offering a great online platform.[1],[2]

In addition to that, the pay-as-you-go philosophy, implemented by cloud computing where companies and organizations are given access to virtually limitless amount of IT resources only by making hourly or monthly payments, is another core feature that contributes to the aesthetic makeup of this technology. offered by the cloud computing are flexibility and scalability due to which it is recommended to those who have high demand on processing power. This particular model offers the significant capacity of scalability that permits users to have the flexibility of modifying the capacity to their other way by keeping the cost more or less consistent to the operation.

Though you may agree or disagree, cloud computing turns out to be far more beneficial for enterprises than having an on- premises infrastructure. Indeed, cloud computing can also be debilitated by any attackers from either the side of insider or from side of outside. Examining some of the threats faced by the cloud by depending on the measures spelled out in that will enhance the standard of an application in the cloud.

## II.LITERATURE REVIEW

Researchers' community changed to instant access to huge resources and a collaboration among them became real in the cloud computing technology. There is no universal pathway from warlordism to peace, but rather sundry difficulties that must be deeply researched. Lack of information is just everywhere, irrespective of its origin as a result of power outage, machine failure or external cyberattacks or forgetfulness. Yet, the results of such cataclysmic events can be detrimental: they can prevent development through the reduction in inquiry, they can be a source of deception for many, and they can create more morally challenging tasks. A multiple way to extinguish the dangers is by using different techniques such as reinforcement downloading, encryption methods, monitoring systems, selecting for reliable cloud providers, and providing data management plans. Vendors' lock-in reliance is also an aspect that need examination as the analysts may excessively depend on the basis or the system of the particular provider which is ineffective and a matter which does not allow innovation in technology handling.[14],[15]

On the contrary to the specific viewpoint of the Secure confirmation and section control systems, the matter is very serious as it affects the integrity of the information. Examples of common login tasks include the use of weak username-password combinations which can be used to crack passwords, while the lax controls on information can also lead to unauthorized access and alterations. General settings for blueprints, problems with keeping to the thumb rule of minimum energy consumption, reliance on default settings, and lack of user training all make these configurations difficult. The remedies that look into these shortcomings include the use of multi-factor affirmation warnings, strong password approaches, adherence to the principle of least privileges, standard audits of access points, data fragmentation and awareness programs of the user through educative programs. Moreover, another risk factor is account grabbing, which is when bad-willing people use other people’s access keys, similar to registered users. In addition, insufficient employees' engagement and careless operators or those who are dealing with sensitive data is a risk factor too.

However, for eliminating the data breach threats, the technical solutions like multi-factor verification, authentic and strong practice of authentication processes, continuous movement monitoring, minimum limit of privileges as well as an encryption of data, informational security training sessions and a complete assessment of the IT infrastructure are implied. In order to completely master that of cloud protection solutions, analysts should not be discouraged to enjoy the benefits of being in the open cloud same time, they should contribute to the findings security and of course to digging data.

## III.CLOUD COMPUTING SERVICE MODELS

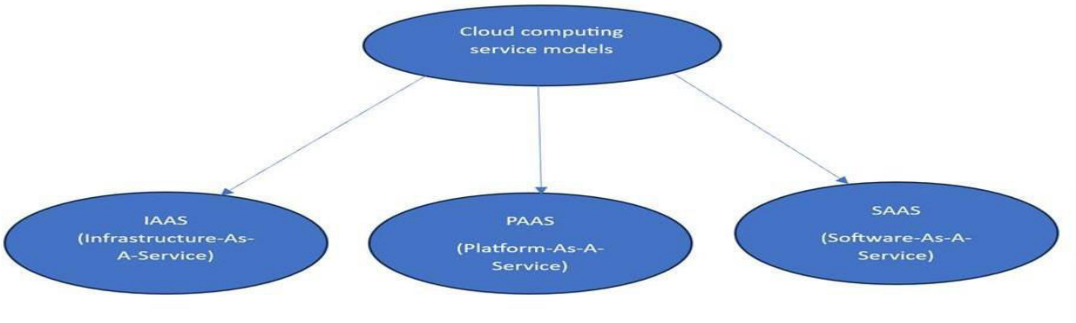
Cloud computing service models
IAAS (Infrastructure-As-A-Service)
PAAS (Platform-As-A-Service)
SAAS (Software-As-A-Service)

FIGURE 1. CLOUD COMPUTING SERVICE MODELS

### 3.1. IAAS(INFRASTRUCTURE-AS-A-SERVICE)

For the Infrastructure as a Service (IaaS) model, the providers give out the internet by which the virtualized computing resources can be accessed. They, in turn, involve the existence of virtual machines, networking, and storage infrastructure, among other resources. Now consumers can draw down resources as and when needed at the pay-as-you-go rate, as the consumption replaces the investment or installed and maintained appliances. The high degree of scalability of IaaS provides users with the convenience to adapt their resource allocation to their corresponding requirements, thus making it ideal for enterprises with variable loads or those are looking for ways to keep their infrastructure costs down. Although they mainly differ in their target user, the most known IaaS providers can be classified under Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).[3]

### 3.2. PAAS(PLATFORM-AS-A-SERVICE)

Building on the Infrastructure as a Service platform model, PaaS establishes a foundation for developers, allowing them to focus on their applications development, deployment, and supervision. In PaaS solutions the most typical bundles are IDE tools, complemented by middleware, databases, and runtime environments. However, with PaaS, infrastructural features are generalized and the technical details underlying the whole system are abstracted, leaving a range of development to coders with no need for thinking about server administration or the scalability issues. PaaS is in most use case of the application development and deployment, and so it is accelerating the time-to-market and can be easily changed to meet the market or customer's need.[4]

### 3.3. SAAS (SOFTWARE-AS-A-SERVICE)

The Software as a Service (SaaS) model first delivers software applications through the internet and simultaneously enables them to be used by a subscription-based model. Contrary to the traditional installing and configuring the software on physical devices, users can access and run the application in their browsers or through an app. The cloud provider who is in charge of the software regularly updates the system for task such as software updates, patching security holes and backup the data. SaaS solutions, which are designed to provide a variety of functions, like productivity systems, CRM, ERP and collaboration software, can be found in abundance. SaaS with its benefit package of convenience, scalability, and low cost improves the user's ability to operate apps from any device connected to the internet. To note, the SaaS products carrying Microsoft Office 365, Salesforce and Google Workspace (formerly known as G Suite) are recognized examples.[5]

## IV. CLOUD SECURITY SERVICES CHALLENGES

Cloud computing allows accessibility and dynamic scaling through network resources. The rapid expansion in usage of the cloud has led to higher risks of data breaches and the leakage of private information.

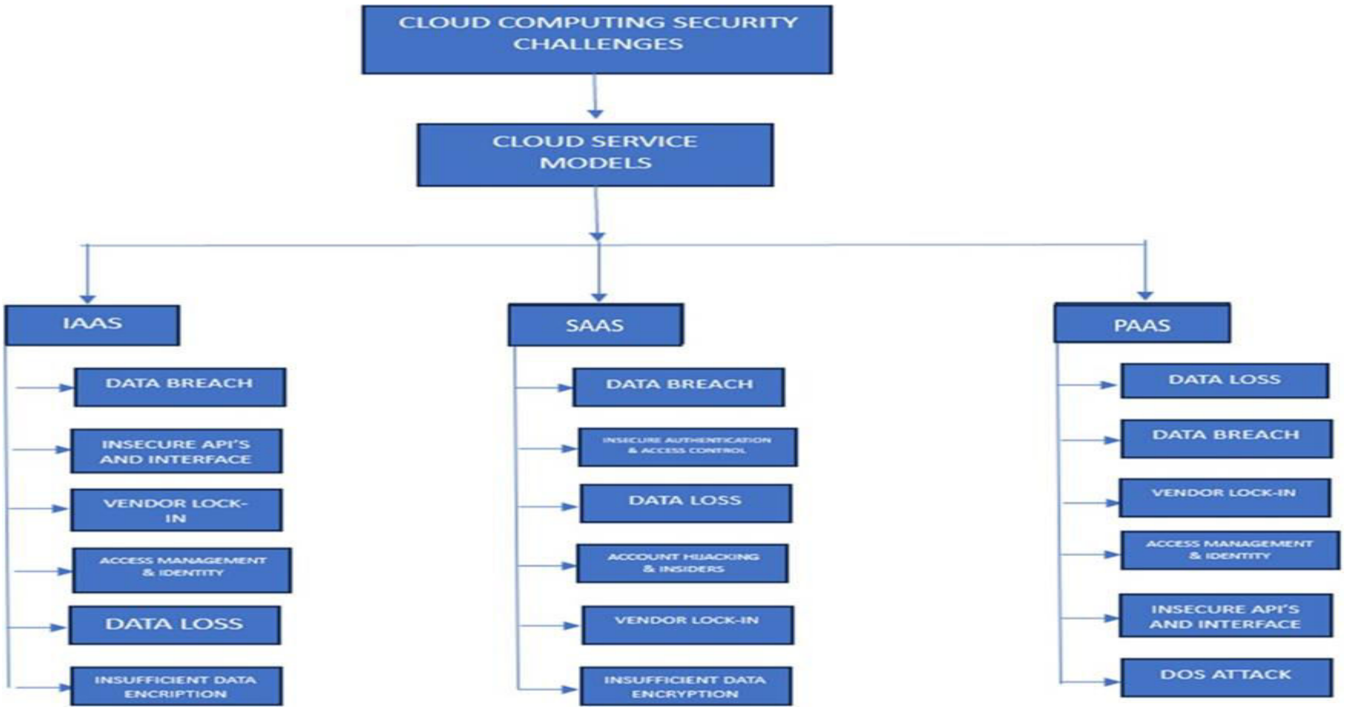
CLOUD COMPUTING SECURITY CHALLENGES
CLOUD SERVICE MODELS
IAAS
DATA BREACH
INSECURE API'S AND INTERFACE
VENDOR LOCK-IN
ACCESS MANAGEMENT & IDENTITY
DATA LOSS
INSUFFICIENT DATA ENCRIPTION
SAAS
DATA BREACH
INSECURE AUTHENTICATION & ACCESS CONTROL
DATA LOSS
ACCOUNT HIJACKING & INSIDERS
VENDOR LOCK-IN
INSUFFICIENT DATA ENCRYPTION
PAAS
DATA LOSS
DATA BREACH
VENDOR LOCK-IN
ACCESS MANAGEMENT & IDENTITY
INSECURE API'S AND INTERFACE
DOS ATTACK

FIGURE 2. CLOUD SECURITY SERVICES CHALLENGES

## V.SECURITY ISSUES IN SAAS IN CLOUD COMPUTING

SaaS Apps often have to control massive information volumes, including secret data such as personal data, financial reports and intellectual property. Consequently, they are seeking to be spread and, consequently, the objectives of cyber assaults, like data breaches, malware infiltrations, become more appealing. The wide use of SaaS applications makes them more vulnerable because of their online accessibility to security threats like unlawful entrances, eavesdropping on wireless connections, or an account takeover.

Furthermore, the distinct security challenges in SaaS are due to their nature of being multi-tenant while the fact that they act as a centralized point of reliance also poses a threat. In these situations, many users share one single infrastructure and resources as a SaaS application, in general, and in addition, data leakage and cross username attacks may be escalated especially if there are no isolation measurements put in place. An incident striking one user means the stolen passwords may be usable across all other users with the same service.

### 5.1. DATA LOSS

Researching SaaS involves working under a very unsafe methodology and data loss being the ultimate catastrophic event in cloud computing is a fact. The piece refers to the vital sources of data race in the cloud and which could potentially lead to the outcome of good and bad research results**.**

### 5.1.1. CAUSES OF DATA LOSS

•Accidental Deletion: Contrasting with conventional storage where scientists experience remote access to their data and results; in the cloud, they also acquire escalated computational power but the main disadvantage of it could be human error which may lead to loss of information or forgetting the stored scientific data.

•Technical Failures: If the hardware or software was malfunctioning on the cloud services' provider side the service would be down and the data would not be available.

•Security Breaches: The occurrence of cyberspace attack and data privacy can bring the loss or disorganization of data in an organization.

### 5.1.2. MITIGATION STRATERGIES OF DATA LOSS

•Data Backups: Automation mechanize the procedure leading to faster response for data recovery, the backup can be performed more often to on-site external storage beyond cloud infrastructure. But, on the other hand, being able to rely on data backup lace makes the data vulnerable from information loss and safeguard the purity of data too.

•Encryption: Having the peaceful security embedded specially in the non-basic essential features, the intruder would have hard time to go elsewhere. Data integrity and confidentiality are stumped on the strong encryption tactics and thus you will notice an inward change towards publicized data security systems.[13]

•Version Control Systems: The review process version control systems with work is to give researchers a chance to look into the data and track their every moves while changing the changes made. The process being needed to be much simpler and now possesses primary attraction in situation of mistaken overwriting even considering the fact of this doing.

### 5.2. DATA BREACH

The cloud computing ensures research with lot of benefits, however, data vulnerability to hackers are some another security threat. Further, the section will explore specific instances in which cloud systems expose themselves to data breaches and provide a brief description of risks of research integrity.

### 5.2.1. CAUSES OF DATA BREACHES

•Misconfigured Cloud Storage: Misconfigured cloud storage buckets and databases which is vulnerable to unauthorized access by malicious users can pose a great chance of data exposure.

•Phishing Attacks: Data stored in the cloud is most susceptible to phishing attempts by researchers, thus granting people with the unauthorized access into such data.

•Weak Authentication Protocols: A patchy password policy and the use of single-factor authentication could weaken the defenses of the cloud systems, hence, allowing the attackers to have easy access to the cloud accounts.

### 5.2.2. MITIGATION STRATEGIES OF DATA BREACHES

•Data Minimization: Scientists ought to upload the crucial information to the Cloud thus doing this will diminish the probable effect of an attack.

•Strong access controls: Format of authentication with use of several factors can reduce the risk of unauthorized access, and so through enforcing a tight access control policy based on the principle of the minimum rights.

•Regular Security Audits: Compliance with regular assessments of cloud environment is one common practice that assures identification of vulnerabilities before they may be exploited.

### 5.3. VENDOR LOCK-IN

We observe vendor lock-in when such a client becomes a loyal user of a unique supplier's goods or services. This happens when a company announces their own proprietary solution for technology which hampers the user from switching to another supplier.[14],[15]

### 5.3.1. CAUSES OF VENDOR LOCK-IN

•Limited Control: While they may enjoy the convenience and flexibility that a specific service of a cloud vendor would bring, the organization may have limited control when it comes to designating the security risks configuration and implementation. The inability to have full control over platform restrictions can give birth to weaknesses that are inherent to cloud platform providers.

•Data migration risks: Moving from one cloud service provider to another is likewise a task that is very arduous and might take you through dangerous paths, particularly if the new provider does not support the file formats, APIs that determine the communication between technologies, or even proprietary technologies. Migration of data could happen across some online path networks and could, as a result, expose the data to threats of security or vulnerabilities.

•Dependency on Vendor's Security Measures: Some of the platforms that cloud providers apply to secure their platforms and services include. Though reliance on the vendor's security measures might be deceptive without full understanding and incomplete domino effect, it is one of the safest approaches. It works better when following it with other securities. In case the supplier does not respond to security threats or suffer from outage, the customer can face loss of data or apps.

### 5.3.2. MITIGATION STATERGIES OF VENDORS LOCK-IN

•Adopting Multi-Cloud Strategies: Differentiation of the workloads on several cloud vendors instead of one allows to diversify and prevent such restrictions as vendor lock-in. In the multi-cloud set-up, enterprises can maximize availability that’s not cloud provider specific and still leverage the benefits of diverse providers.

•Embracing Open Standards and APIs: Putting solutions which respects open standards and different APIs that are widely accepted should be the priority option for facilitating that cloud platforms interoperates and there is portability. Open teamwork with local community and open-source software most of the time leads to more freedom and eliminates lock-in in which all the systems are of one vendor.

•Application containerization and orchestration: Through the abstraction layers that come with orchestration platforms like Kubernetes, and container technologies such as Docker enable application consistency across various compute/virtualization settings. Containers facilitate being easily transported and cut dependence on system layer thus migrating between different providers of cloud services may become much easier.

### 5.4. INSECURE AUTHENTICATION AND ACCESS MANAGEMENT

The Sensitive user data and apps primarily used in SaaS platforms when it comes to cloud computing are rising the security problems related to the widespread use of in cloud environments. In a SaaS context, strong authentication mechanisms have become necessary because cloud users largely rely on external servers for data storage, management, or app accessing**.** Having said that, it does not mean that data cannot be compromised, because it still will be possibly in case of unauthorized use of passwords that are cracked or if authentication is not multifactorial.[11]

### 5.4.1. CAUSES OF INSECURE AUTHENTICATION AND ACCESS MANAGEMENT

•Misconfigured Cloud Environments: The thy density of clouds means that, as a result of erroneous access permissions set, rows may be opened that the attacker can in turn use.

•Neglecting Least Privilege: It has become a standard practice to grant users only the privileges that they absolutely need throughout their job functions. Any more than that would broaden the attack surface and the liability from a compromised account as well.

•Reliance on Default Settings: Research platform in the cloud very if often comes with pre-installed security settings that do not match the unique security needs of the research project better. The existence of such personalized settings being excluded leads to hazards.

### 5.4.2. MITIGATION STRATERGIES OF INSECURE AUTHENTICATION AND ACCESS MANAGEMENT

•Multifactor Authentication: The next safety procedure is Multifactor Authentication (MFA), which requires more than a single method of authentication for a user to log in. It comprises two different types of verification factors: the first option is the password-sign-in, and the other one requires more unique things that are harder to predict like a fingerprint.[12]

•Strong Password Policies: Firing up a strong password policy that part of its requirements simple passwords and obligatory periodical change of passwords is driving out an opposing intrusion attempt.

•The principle of minimum privilege: stopping us at a minimal level possible, users would only acquire permissions needed to complete their tasks makes for a more secure option.

•Regular Access Reviews: Periodical access privileges examination allows rights remain suitable to actual positions and tasks.

### 5.5. HIJACKING ACCOUNTS AND INSIDERS THREAT

A situation when unlawfully people are granted access to the authenticated user account through obtaining valid user credentials is known as account hijacking. A convincing number of procedures, like setting up poorly secured passwords or launching the virus attacks or even those of phishing, are just a piece of cake. Malicious insider acts aren't seen as a problem only within perimeter protection, they are a serious and growing threat, even in the presence of strong perimeter protection. Insiders are persons who obtain authorization to access a system or information channels but use them for destructive, illegal or self-serving purposes. They may consist of individuals of research, collaborators, or even personnel of cumulus providers of service.

### 5.5.1. CAUSES OF HIJACKING ACCOUNTS AND INSIDERS THREAT

•Phishing attacks: The activities within the category of phishing activities typically involve e-mailing malicious emails in which attackers will stealthily ask for their login credentials.

•Credential stuffing: Compromising SaaS accounts is a major consequence of data breaches. Cyber scoundrels perform credential stuffing by using login credentials from identified sources to break into SaaS accounts.

•Malicious insiders: The malicious insider is an individual such as a staff theoretically knew to the company or a contractor who has legitimate access rights but may abuse them for bad purposes.

### 5.5.2. MITIGATION STRATERGIES OF HIJACKING ACCOUNTS AND INSIDERS THREAT

•User Authentication and Authorization: Authentication methods such as Multifactor Authentication that is focused on granting each role users specific permissions is going to be a very important tool. This will be a part of authorization that emphasizes the principle of Additional restrictions through limiting users access to the minimal required resources.

•Monitoring and Logging: To make the Monitoring and Logging effective, it is mandatory to keep monitoring user activities and to record all the attempts of access in a logbook because the main purpose of such activities is to identify the anomalies and find vulnerabilities.

•Data Encryption and Anonymization: Ensure the security of delicate information by encrypting it both while it is stored and when shared to prevent the access of unauthorized individuals to it. In order to make data safer, any possibility of data anonymization should to be taken into account. This will help to limit the risks of insider threats. This should comprise of using encryptions for the most key information to protect it from breaches whether it is at rest or in progress and anonymizing data whenever is possible to avoid threats from within the organization.[13]

### 5.6. INSUFFICIENT DATA ENCRYPTION

The vulnerability of any key information, including inspiration, remains a major risk to both the confidentiality and integrity of sensitive data when encryption in cloud storage is not implemented. Data received or transmitted via the cloud is subject to attacks led by eavesdropping or unauthorized access. Such attacks may be avoided by using encryption. Such kind of exposures of organizations to information leaks, rule infringements, and public relations mishaps can lead to disasters. To be able to avoid risks of this nature, users can take actions such as having reliable and achievable encryption protocols for data that are both resting and in transit so that it remains safe from unauthorized parties to access them.[13]

### 5.6.1. CAUSE OF INSUFFICIENT DATA ENCRYPTION

•Performance Impact: Because of encryption barriers, processing overhead will be added, and the researchers who are doing tasks that are very vocation-intensive, such as bioinformatics or large-sale simulations, could think that it will lower their computational efficiency.

•Vendor Lock-in Fears: Researchers might be afraid to become locked into a cloud vendor's encryption solution as this might mean that they will be forced to move elsewhere for their services. What they might find problematic is this limited choice which implies that they may switch to other cloud provider that is less good and reliable. It is preferable that on different platforms, which offers compatible encryption technologies.

•Implementation Complexity: The next step of encryption deployment, with key and other management issues being complex and making it difficult for researchers to properly implement it hence discourage them from proceeding.

### 5.6.2. MITIGATION STRATERGIES OF INSUFFICIENT DATA ENCRYPTION

•Implement Robust Encryption Protocols: Adopt appropriate risk management strategies including data at rest and transit encryption protocols based on the cloud environment. Also, acknowledge reliable encryption algorithms such as AES 256.
•End to end encryption: Make the encryption of data a one-stop shop that an eavesdropper or hacker would need to decrypt from the client side also to the storage and processing of the cloud provider. It acts as a barrier to unauthorized access and this, remarkably, prevents data transmission and storage.[13]

•Auditing and Monitoring: Implement regular monitoring and auditing techniques which should play the role of authentication encryption while detecting attacks and identifying security weaknesses. Which are the several tasks responsible for that, such as reviewing access logs, tracking the encryption key usage, data usage records and patterns of manner if it has been accessed.

## VI.CONCLUSION AND FUTURE WORK

The speed and agility of cloud computing and its unequalled capacity for collaboration and quick access to a vast repository of resources made of its a probably effective player in revolutionizing the way we do science, leading to better performance at a much faster pace than ever. This transformative experience has however drastically changed the way research initiatives train in future. Though these developments are quite significant, the migration to cloud computing has increasingly revealed new security challenges, and as a result, the need to carefully look into theses controversies and craft ways of managing them becomes more appreciated. It is an open secret that the exact cyberspace security threats SaaS vendors confront in the course of supporting cloud computing have been extensively researched in this comprehensive investigation. This sector does stand to derive great benefits from the innumerable cloud computing advantages offered; but the security issues must be recognized and addressed efficiently through due adoption of security protocols in academia and of course, educational institutes. Researchers can safeguard their research data contained in the cloud by taking a security minded approach which will lead to an environment that is secure for the development and growth of the activities that thrive on cloud computing. Putting continues vigilance in maintaining security in research data will help prevent future exploitations by malevolent actors as well as misuses of the data. In order to defend against any foreseeable risks, researchers should keep in touch with emerging cyber security trends in cloud computing and analyses their networks by updating security infrastructures. In other words, the implementation of effective security measures should be considered as vital for safeguarding research endeavors in the cloud system being a long-term project.

## REFERENCES

[1] Jawed MS, Sajid M. A comprehensive survey on cloud computing: architecture, tools, technologies, and open issues. International Journal of Cloud Applications and Computing (IJCAC). 2022 Jan 1, 12(1):1-33.
[2] Qi W, Sun M, Hosseini SR. Facilitating big-data management in modern business and organizations using cloud computing: a comprehensive study. Journal of Management & Organization. 2023 Jul, 29(4):697-723.
[3] Samha AK. Strategies for efficient resource management in federated cloud environments supporting Infrastructure as a Service (IaaS). Journal of Engineering Research. 2023 Oct 31.
[4] Di Orio G, Maló P. Providing the Key Ingredients of an Edge PaaS for Supporting and Facilitating the Development of Smart Energy Applications. In APCA International Conference on Automatic Control and Soft Computing 2022 Jul 2 (pp. 142-154). Cham: Springer International Publishing.
[5] Seifert M, Kuehnel S, Sackmann S. Hybrid Clouds Arising from Software as a Service Adoption: Challenges, Solutions, and Future Research Directions. ACM Computing Surveys. 2023 Feb 9, 55(11):1-35.
[6] Malallah HS, Qashi R, Abdulrahman LM, Omer MA, Yazdeen AA. Performance Analysis of Enterprise Cloud Computing: A Review. Journal of Applied Science and Technology Trends. 2023 Feb 5, 4(01):01-12.
[7] Gammelgaard B, Nowicka K. Next generation supply chain management: the impact of cloud computing. Journal of Enterprise Information Management. 2023 Mar 28.
[8] L'Esteve RC. New Horizons in Distributed Cloud Computing. InThe Cloud Leader's Handbook: Strategically Innovate, Transform, and Scale Organizations 2023 Jul 6 (pp. 123-134). Berkeley, CA: Apress.
[9] Ionescu SA, Diaconita V. Transforming Financial Decision-Making: The Interplay of AI, Cloud Computing and Advanced Data Management Technologies. International Journal of Computers Communications & Control. 2023 Oct 30, 18(6).

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 5, May 2024 |

| DOI:10.15680/IJMRSET.2024.0705096 |

[10] Yang C, Huang Q, Li Z, Liu K, Hu F. Big Data and cloud computing: innovation opportunities and challenges. International Journal of Digital Earth. 2017 Jan 2, 10(1):13-53.
[11] Mihailescu MI, Nita SL. A searchable encryption scheme with biometric authentication and authorization for cloud environments. Cryptography. 2022 Feb 14, 6(1):8.
[12] Pathan A, Ingle MD. Security Provision for Data Stored in Cloud Using Decentralized Access Control with Anonymous Authentication. International Journal of Computer Applications. 2016, 146(12).
[13] Banasode PS, Padmannavar S. Protecting and Securing Sensitive Data in a Big Data Using Encryption. EAI Endorsed Transactions on Smart Cities. 2020 Apr 17, 4(11):e5-.
[14] Kumar P, Kumar P. Vendor Lock-In Situation and Threats in Cloud Computing. International Journal of Innovative Science and Research Technology. 2022, 7(9).
[15] Opara-Martins J. Taxonomy of cloud lock-in challenges. Mobile computing-technology and applications. 2018 May 30.
[16] Ahmad W, Rasool A, Javed AR, Baker T, Jalil Z. Cyber security in IoT-based cloud computing: A comprehensive survey. Electronics. 2021 Dec 22, 11(1):16.
[17] Dittakavi RS. Evaluating the Efficiency and Limitations of Configuration Strategies in Hybrid Cloud Environments. International Journal of Intelligent Automation and Computing. 2022 Nov 17, 5(2):29-45.

INNO SPACE
SJIF Scientific Journal Impact Factor

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

# INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com