ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun154

Landscape of Cloud Infrastructure: Security Concerns, Mitigation Strategies, and Research Opportunitieser

Hasaan Bin Mohamad[1]; Shreyansh Singh Katiyar[2]; Aditya Kumar[3]; Nikesh Choudhary[4]; Sheveta Vashist[5]

[1,2,3,4,5]School of Computer Science and Engineering, Lovely Professional University, Jalandhar, Punjab, India

Publication Date: 2025/07/14

Abstract: The objective of this review is to analyze the possible security concerns within a cloud infrastructure and check the validity of current solutions in mitigating the alarming security issues that this technological advancement brings. As more and more organizations embrace the cloud, the need to assess and control security threats to safeguard confidential information and system integrity becomes imperative. This review analyzes the existing and anticipated security challenges, as well as the existing solutions for overcoming them, such as encryption, access control, and incident management systems. The deductive components of this research select best practices forecast future extensions and combines them as an extensive inventory of major issues and areas that require research. Despite the huge array of tactics for prevention and remedy rapidly advancing technology provides a constant challenge. It brings the question of how any system can be regarded as secure in the long run because of the constant technology change one is forced to adapt with. This paper, therefore, calls for the implementation of security measures that are proactive and forward thinking and the critical need for further studies to develop strategies that will suit the ever-changing cloud-based system of today.

Keywords: *Cloud Computing, Cyber Security, Cloud Infrastructure, Cloud Security, Data Security*.

How to Cite: Hasaan Bin Mohamad; Shreyansh Singh Katiyar; Aditya Kumar; Nikesh Choudhary; Sheveta Vashist (2025), Landscape of Cloud Infrastructure: Security Concerns, Mitigation Strategies, and Research Opportunitieser. *International Journal of Innovative Science and Research Technology*, (RISEM–2025), 7-16.
https://doi.org/10.38124/ijisrt/25jun154

I. INTRODUCTION

Cloud computing has evolved through several implementations, such as Software as a Service (SaaS), grid and utility computing, and application service provision (ASP). Setting the foundation for ARPANET in 1969, the fundamental idea began in the 1960s when J.C.R. Licklider pondered the concept of a "intergalactic computer network" that would allow for global communication and access to data and programs. [1]

Because cloud computing offers processing, storage, and software-based services, it has become widely accepted by both individuals and organisations. By offering its clients on demand pay-per-use services, it helps them deal with their resource scarcity problems [2]. Since the rising quantity of fresh advancements in cloud computing platforms, security issues become a major concern in relation to this technology [3]. Clearly more people and companies are using cloud services, software, and infrastructure following the epidemic as they can be accessed anywhere and at any moment.

In response to the growing number of security threats, security systems have advanced over the past years. Various countermeasures can detect and fix attacks emerging due to networks such as botnets and stepping-stone attacks. Cryptographic methods help to reduce the possibility of data protection attack violaations. Using authentication systems, the vulnerabilities based on VM and hypervisor are addressed. In a same vein, intrusion detection systems help to control assaults employing denial or theft-of- service. Privacy laws like ECPA and HIPAA have been applied for the risks leading to the information disclosure to third parties [8–10].

While at the same time stressing the elements of security that are crucial when deploying computing systems that are cloud-based, this work intends to investigate and evaluate the perspective towards cloud computing. Moreover, the study addresses some of the technical features and normative approaches towards the idea of cloud computing together with an architectural perspective taken in line with this. Following this, the study looks at the numerous security issues the emergence of cloud computing presents.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun154

Understanding the technology challenges and grasping the security concerns helps the research study to show an all inclusive study of cloud computing throughout the course. Various strategies for managing the security concerns of cloud computing are discussed; it is underlined that no one mechanism Cloud Computing Structure and Terminologies can completely eradicate these threats.

II. OVERVIEW OF CLOUD SERVICES

Cloud storage allows users to store and retrieve data online. Being a storage service means users can retrieve data from the space. The cloud stores consumer-created files and apps. The competitive nature of today's environment forces most people to use additional storage systems for personal or organizational files, driving up demand. Cloud systems' more substantial benefits, such as the ability to access superior storage services at lower rates and faster times, have raised demand for cloud and outsourced services [11].

Cloud computing, commonly known as "the cloud," provides servers, databases, networking, analytics, and more over the internet, accelerating development and optimizing resources. Cloud computing is defined by NIST as a concept for providing on-demand access to a shared pool of programmable computer resources that can be quickly assigned with minimal supervision. Future cloud computing will include AI, IoT, and edge computing, causing even more changes in all sectors. Finally, prediction models show that cloud services will continue to grow and that hybrid and multi-cloud infrastructures will be prioritized.

➢ *Cloud Computing: Stakeholders):*

In cloud computing, stakeholders are a wide spectrum of entities that interact in its ecosystem:

- *Cloud Service Providers (CSPs):*

Businesses like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) offering cloud-based services (CSPs) [12]

- *Consumers:*

Companies and personal consumers using cloud services for storage, computation, and other purposes [12].

- *Developers:*

Professionals making use of cloud environments to create, implement, and manage applications [12].

- *Regulators:*

Authorities and institutions verifying cloud services fulfil security and compliance requirements [12].

- *Third-Party Vendors:*

Entities providing supplementary tools and services, such as monitoring and security solutions [12].

➢ *Cloud Computing Delivery Frameworks:*

Delivery models for cloud computing are critical. The three main delivery models with differing degrees of responsibility sharing are:

- *Software as a Service (SaaS):*

SaaS is a cloud service provider's whole software suite that you pay for by usage. SaaS | Microsoft Azure, n.d.). You rent an app for your company, and users access it via a web browser. The service provider's data center houses all infrastructure, middleware, app software, and app data. The service provider controls hardware and software and ensures app and data availability and security with the right service agreement. SaaS lets your company launch an app rapidly and cheaply [13].

- *Platform as a Service (PaaS)*:

PaaS is a large cloud-based development and deployment environment that lets you build everything from simple cloud apps to advanced cloud-enabled commercial apps. You pay-as-you-go for cloud infrastructure and customize it online. In addition to servers, storage, and networking, PaaS offers middleware, development tools, business intelligence (BI) services, database management systems, and more. What's PaaS? PaaS | Microsoft Azure, n.d.). PaaS supports web application development, testing, deployment, management, and updates. PaaS saves you money and time on software licenses, application infrastructure, middleware, container orchestrators like Kubernetes, development tools, and other resources. Developers manage apps and services, while cloud service providers handle everything else [14].

- *Infrastructure as a Service (IaaS):*

As a cloud computing service, infrastructure as a service (IaaS) offers basic compute, storage, and networking functions on demand. Cloud computing services include SaaS, PaaS, serverless, and IaaS. Moving to an IaaS solution reduces data center maintenance, hardware expenses, and provides real-time business information. With IaaS, you may scale IT resources up and down as needed. IaaS | Microsoft Azure, n.d. They also speed up application provisioning and improve infrastructure dependability. IaaS eliminates the cost and hassle of owning and operating physical servers and data center equipment. Each resource is an independent service component, and you only pay for what you use. Azure maintains infrastructure while you buy, install, configure, and manage software including operating systems, middleware, and apps [15].

➢ *The Five Types of Cloud Deployment Models:*

A cloud deployment methodology configures a cloud computing solution for end-user access and resource utilization. It describes cloud resource ownership, solution operating level, and user access to end components.

- *Public Cloud:*

The public cloud is the most common sort of cloud-based technology implementation. Third-party public clouds offer infrastructure and software on a pay-as-you-go basis. Large data centers feed these clouds by allocating resources to clients according to agreements or automatically based on traffic and demand [17-18].

These arrangements are easier to maintain than others since users have limited administrative obligations. A wide community of specialists and internet tools aid troubleshooting and problem-solving. Public clouds are cost-

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun154

effective because users only pay for the resources they utilize [12,17-18].

Security, data retention, and privacy remain major concerns. Customers, usually end users, subscribe to ready-to-use applications using the SaaS model (Bokhari et al., 2018). We can assume that something public is less secure than something private. Public cloud environments are less secure than private setups, security breaches can be devastating due to delayed response times, and companies can rarely guarantee the following due to the distributed nature of the cloud [17-18].

- *Private Cloud:*

Private cloud computing infrastructures are unlike public clouds and more like on-premises setups. A private cloud arrangement involves the client owning infrastructure (an internal cloud) or leasing dedicated hardware (a virtual private cloud). [17-18].

Both clients have direct access to the underlying infrastructure and can control it more since it's not being utilized to run and maintain other cloud-based services [12].

Because they are private and less apparent to malevolent parties, private clouds can improve security. Keeping this level of protection is difficult, expensive, and time-consuming. An already sophisticated system is hampered by private cloud scalability costs and complexity. [17-18].

- *Hybrid Cloud:*

A hybrid cloud combines public and private clouds. Clients may utilise a private cloud for certain data, workflows, or procedures necessitating enhanced security or compliance, while leveraging the scalability and cost-efficiency of public clouds for less sensitive operations. This architecture is popular for balancing security, performance, and efficiency. AWS, Google Cloud, and Microsoft Azure facilitate hybrid cloud integration, making data management easier. [16-17].

- *Community Cloud:*

Community cloud is the least popular of the four National Institute of Standards models. It works like a private cloud but is shared by numerous companies with similar needs. This notion benefits collectives who want to share resources and expenses but can't manage a cloud solution [16-19].

Governments and nonprofits who need to work together in trust use community clouds.

Community clouds work like private clouds except from sharing resources and expenses across multiple enterprises. The participating organizations may own the infrastructure and cloud solution, or a cloud provider may provide exclusive access to certain clients [16-19].

A provider may jointly own or manage infrastructure and provide exclusive access to participating firms. Community clouds are rarely used but could develop as cloud adoption rises worldwide [16-19].

- *Multi Cloud:*

Unlike the others, NIST does not accept the multi-cloud model. It uses middleware to connect many public or private clouds [16].

Integration of services from diverse providers has gotten easier as cloud computing technologies have matured, allowing enterprises to leverage a mix of solutions and avoid vendor dependence. Many providers enable multi-cloud integration, although specialized middleware solutions are also available. [16].

Maintaining access to several systems in a multi-cloud deployment architecture is costly and risky for business and finances. Administrators must master numerous platforms and workflows, complicating company operations [16-17].

III. SECURITY CONCERNS IN CLOUD COMPUTING

Threats must be mitigated at four fundamental levels in the design and implementation of cloud infrastructure security: data, application, network, and host [19]. Prior to cloud computing being considered a reliable option in corporate computing, several difficulties must be addressed. Businesses are really concerned about relinquishing physical control over their cloud-stored data. Until date, service providers have struggled to ensure that a business's data is consistently stored on designated servers in specific areas [20].

Cloud computing presents a transformative potential for developing nations, allowing them to leverage advanced information technology without the substantial initial expenditures that have historically created obstacles. Nonetheless, this opportunity is accompanied with considerable concerns. Data security, physical control, and privacy continue to pose significant issues, as data is frequently housed on remote servers whose precise location and access cannot always be assured by service providers, rendering organisations susceptible to possible security and privacy threats. The strategic strategies enacted by cloud providers are essential for safeguarding customers' personal or corporate data, as technical solutions alone are unable to comprehensively resolve the issue (Joint & Baker, 2011).

Additionally, trust presents a significant challenge, raising further security concerns regarding the use of cloud services. This is because trust is intrinsically linked to the credibility and reliability of cloud service providers (Ryan & Falvy,2012). One very significant issue that is common and yet not addressed as much is the human aspect.

Human negligence in the form of operational blunders like incorrect setting of configurations, password management, or simply lack of security precautions can compromise cloud systems greatly. Phishing attacks remain a major threat, as employees can be manipulated into revealing credentials, giving attackers access to critical systems.

The CIA Triad, which stands for Confidentiality, Integrity, and Availability, offers a basic foundation for cloud security to guard against these weaknesses. Only those who

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun154

are authorised can access sensitive information thanks to confidentiality. Integrity prevents data from being tampered with or changed. Availability guarantees that resources and data are consistently available when required [21]. These guidelines serve as the foundation for security concerns and have a direct impact on the tactics used to lessen cloud computing assaults, including:

- *Network Based Attacks:*

Cloud computers on a platform are linked to external systems through a network. Malicious attackers could exploit this as an entry point to capitalise on vulnerabilities, get access, and compromise the security of the cloud infrastructure. An assailant may launch an attack that diminishes cloud service performance and, in severe cases, endangers the privacy and security of sensitive data (Khan, 2016).

Several network-based assaults will be examined in this analysis; each one presents different threats to the cloud environment.

- *Host Based Attacks:*

Host-based attacks target vulnerabilities in the virtualization components of cloud environments, such as hypervisors and virtual machines (VMs) [19,23].

Since many VMs share the same physical hardware, an attacker compromising the hypervisor can gain control over all associated VMs, resulting in widespread security breaches [19,23].

Additionally, as user data is stored across distributed servers managed by Cloud Service Providers (CSPs), risks include unauthorized access to data, data corruption, and loss of confidentiality. Strict access controls for CSP employees, combined with encrypted backups and redundancy, are essential to safeguard data integrity and ensure effective recovery in case of an attack [19,24].

- *Application Based Attacks:*

Application-based attacks in a cloud environment target vulnerabilities within cloud applications and services, often exploiting weak points in authentication, access control, and resources [25]. One common attack is **insecure APIs**, where attackers exploit flaws in cloud service interfaces to gain unauthorized access or manipulate cloud resources. These vulnerabilities may stem from poor validation, improper authentication, or insufficient encryption protocols in API communication (Ryan & Falvy, 2012).

Apart from the loss of data and integrity of the cloud instances, **resource abuse** occurs when attackers exploit cloud resources for malicious purposes, such as running unauthorized applications or launching attacks from the cloud environment, impacting both the service and other users.

IV. COMMON CLOUD ATTACKS AND THEIR IMPLICATIONS

- *Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks:*

Network availability problems include DoS, DDoS, and DNS attacks, among other types of attacks. DoS and DDoS attacks overload the backend with too many repeated requests, which prevents the services or bandwidth from being provided. The major objective is to take over resources, like CPU time or network bandwidth, so that authorized users can't utilize the services. Furthermore, by imitating authentic online traffic and employing many agents to execute the DDoS assault, attackers seek to hide their identity [21]. Unlike DoS attacks, DDoS attacks are more potent, as they are launched from multiple sources and include the creation of an army of bots or zombies to launch an attack. A botnet is a collection of these zombies [26].

Cloud computing resources are seen as primary target when it comes to DoS and DDos attacks. Confidential data and essential information from various sources are stored in a centralized location, with access facilitated by the Internet. This renders Cloud data centers increasingly susceptible to attacks [26].

These attacks are performed to either block access for a specific individual, an organization or a government agency. The motives can very from extortion to various geo-political reasons.

- *Man-in-the-Middle Attack (MitM):*

Man Man-in-the-Middle (MITM) exploits may seriouslyundermine the integrity of Internet and cloud computing systems [29].The attack enables a nefarious intruder toinfiltrate and monitor the internal connection between the client and the server. This constitutes an active assault employing intricate network attack techniques, including Dynamic Host Configuration Protocol (DHCP) spoofing and Address Resolution Protocol (ARP) [27].

Some of the major issue that are from MitM attacks is data theft. As the hackers siphon private data, including identities, banking account details, and card details, as well as other confidential organizational information. Moreover, altered or modified data can cause financial losses, operational disruptions and call into question data integrity, privacy violations further leading to reputation damage.

- *Virtual Machiene (VM) Based Attacks:*

Cloud system vulnerabilities are exploited by VM based attacks to jeopardize data security and interfere with cloud services [8]. There are four stages of the virtual machines that these assaults can target.

These include Cross-VM Side Channel Attacks (Khan, 2016 b, pp. 6–7), where attackers extract sensitive information like cryptographic keys from co-located VMs by analyzing resource usage and timing data from shared resources. VM Migration and Rollback, (Khan, 2016 b, pp. 6–7) attacks data during migration or rollback processes, with protective measures including robust security policies. Lastly, VMScheduler Based Attacks (Khan, 2016 b, pp. 6–7)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun154

exploit scheduler vulnerabilities by enhanced schedulers ensuring fairness and security.

- *Hypervisor Vulnerabilities:*

Hypervisor Because hypervisors (also known as virtual machine managers, or VMMs) allow several computer instances and software programs to run concurrently on a single host while maintaining isolation between them, they present serious security issues. Hypervisors are nevertheless vulnerable to attacks even though they are made to be stable and resilient [19].

If attackers gain control over a hypervisor, they can access and manipulate all associated VMs and data. The extensive access provided at the lower layers of the virtual machine environment makes VMMs appealing targets for hackers [19].

Additionally, by breaching a VMM, attackers can access the hosted apps and underlying physical hardware. Well-known attacks like Bluepill and Hyperjacking use virtual machine (VM)-based rootkits to compromise or alter the hypervisor and take complete control of the system. According to Alghofaili et al. (2021a), standard security measures frequently fail to identify these breaches since hypervisors function beneath the host operating system (pp. 17–18).

- *Insecure API:*

Connecting to other systems at different infrastructure layers, such as network, host, and application services, is made possible in large part by cloud APIs. These APIs make it easier to do things like link cloud infrastructure with apps in Software as a Service (SaaS) environments, manage and control network and virtual machine (VM) resources in Infrastructure as a Service (IaaS), and access cloud-based services like storage in Platform as a Service (PaaS) [38].

But if these APIs aren't sufficiently protected, bad actors may use them to launch a range of assaults against cloud-based apps. The resilience of cloud service providers' APIs has a significant impact on their security. An API that is badly managed or built may reveal serious flaws that provide hackers access to private data and security credentials. This may result in breaches when exposed encryption keys are used to compromise encrypted client data, breaching authentication and access control protocols and jeopardizing the data's confidentiality, availability, and integrity (Alghofaili et al., 2021a, pp. 17–18).

- *Abuse of Cloud Computing:*

Significant security risks to cloud computing include inadequate due diligence and misuse of cloud services. Weak registration procedures in cloud environments, where anyone with a working credit card can register for services, create the risk of cloud service abuse by encouraging anonymity, which draws in spammers, harmful code writers, and cybercriminals who take advantage of the system [31].

On the other hand, Deficient Due Diligence represents another critical risk, as many organizations fail to thoroughly vet their cloud service providers (CSPs). Even when companies have a general awareness of cloud technology and security concerns, they often neglect essential evaluations, such as reviewing the financial stability of CSPs or verifying their operational history, which could prevent significant security vulnerabilities [32].

- *Malicious Insiders:*

Malicious Insiders are a substantial and widely recognized threat to organizations, particularly in the context of cloud computing, where a lack of transparency from cloud service providers exacerbates the issue (Aich & Sen, 2015b, pp. 155–156).

This threat arises when employees or individuals with authorized access to a company’s systems intentionally misuse their access to compromise, manipulate, or steal data, often without the awareness of clients or the enterprise itself. A significant factor contributing to this risk is the cloud providers' often opaque processes related to employee access and monitoring. Customers may not be informed about who within the provider’s organization has access to sensitive data, how employee activities are monitored, or how compliance with security policies is enforced [32].

The consequences of such attacks are severe and can include data breaches, data loss, or the falsification and manipulation of critical information. The challenge lies in identifying these threats, as insiders often have the necessary permissions to operate, blurring the lines between legitimate and malicious activity (Alghofaili et al., 2021a, pp. 17–18).

- *Account or Service Hijacking:*

In cloud context, service hijacking is a serious danger covering attacks including fraud, phishing, and software vulnerability exploitation. Often resulting from inadequate management or reuse of passwords and credentials, this risk makes it simpler for attackers to have illegal access. Once an assailant gets the account information of a client, they can interrupt and track activity, change data, provide misleading information, or send customers to dangerous websites. The stolen account then serves as a launching pad for more attacks, therefore greatly increasing the influence of the danger [32].

Some fundamental approaches help to prevent such situations by including tight limitations on account credentials shared between several services and users. Improving security mostly depends on using two-factor authentication (2FA) or another strong authentication technique. Furthermore, good monitoring mechanisms have to be in place to quickly identify illegal activity. To reduce risks and guarantee compliance, companies also have to completely comprehend cloud service provider privacy practices and Service Level Agreements (SLAs) [32].

- *Authntication and Access Control:*

Particularly with regard to illegal access and resource abuse, access control and authentication in cloud systems provide several difficulties. Driven by its elasticity characteristic, one of the main problems results from the fast changes in infrastructure configurations in IaaS, Infrastructure as a Service. These regular upgrades can make current access restrictions obsolete, so cloud apps need agile and flexible authentication systems. Furthermore crucial for

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun154

maintaining effective and current access restrictions are appropriate configuration and change management strategies [32].

The multi-tenancy feature in IaaS, which enables resource sharing among different customers, introduces complexities in access management. Authenticated users might still gain unauthorized access to shared resources, underscoring the need for conflict-resolving access control measures. Moreover, IaaS offers flexibility for users to configure virtual machines, but this can lead to significant security risks if critical security parameters are missed or misconfigured. To mitigate such vulnerabilities, role-based access control (RBAC) systems are recommended for structuring permissions appropriately (Appl. Sci., 2021, 11, 9005, p. 15) [32].

When it comes to authentication, many cloud service providers rely on simple, single-party methods or offer open access without robust multi-user interface authentication. This lack of comprehensive, multi-factor authentication platforms can expose cloud environments to unauthorized or insecure access, further emphasizing the need for improved authentication strategies (Appl. Sci., 2021, 11, 9005, p. 15).

- *Priviledge Escilation:*

Privilege When an assailant acquires unapproved higher privileges, privilege escalation results—that is, access to data or commands execution enabled by those higher privileges. Two ways this can occur are vertical privilege escalation—where a user acquires administrative or root-level access—and horizontal privilege escalation—where an assailant accesses resources or data belonging to another user with like privileges. As privilege escalation can result in illegal access to sensitive data, system configuration modification, malicious software installation, or even total system breach, its effects are rather noteworthy.

Attackers sometimes utilize social engineering techniques to fool honest users into allowing higher access permissions, and they frequently take advantage of weaknesses in software, misconfigurations, or inadequate access restrictions to escalate privileges. Organizations should apply the least privilege concept to reduce this risk, so ensuring users only have the access required for their tasks, routinely patch systems to resolve vulnerabilities, and establish role-based access control (RBAC) to restrict pointless access.

To add even more protection, multi-factor authentication (MFA) ought to be applied—especially for administrator accounts. As it can result in major breaches if not sufficiently stopped, privilege escalation remains a major threat.

- *Cross-Site-Scriptig (XSS):*

Often targeting end users' browsers, cross-site scripting (XSS) in cloud environments is a security flaw allowing attackers to introduce harmful scripts into web apps. XSS attacks come mostly in three varieties: Reflected XSS, whereby the script is reflected off a web server and executed in the user's browser; Stored XSS, whereby the malicious script is permanently stored on the server and served to users; and DOM-based XSS, whereby the client-side script manipulates the Document Object Model (DOM) to execute malicious code [33].

XSS can be especially harmful in cloud systems since it can compromise user data, hijack sessions, propagate malware, and support phishing efforts. By means of cloud-based apps, attackers can pilfers session cookies or authentication tokens, so acquiring illegal access to private data or services (Jang-Jaccard et al., 2014; Alam et al., 2020). Particularly in cases when appropriate input validation and safe coding techniques are not followed, these weaknesses might erode confidence in cloud services, hence causing data breaches and financial losses [33].

- *Data Based Attacks:*

Data-Based In cloud systems, data-based attacks are a major security issue since they might cause sensitive data to be leaked, exposed illegally [34]. The following are some important problems pertaining to data-based attack:

✓ *Data Breach:*

Often using security flaws, inadequate access restrictions, or insider threats, a data breach is the result of an assailant gaining illegal access to private or secret data kept on the cloud. Personal, financial, or business data may all be extracted with this access [35]. A data breach exposes personal and financial information, intellectual property, and business-critical data among other serious effects. Especially with data protection rules like GDPR, this can have major legal and regulatory consequences. Customers losing faith might cause long-lasting reputation damage to the company, which would result in business losses. With companies under more inspection by both consumers and authorities, financial penalties, lawsuits, and compliance concerns might also follow [35].

✓ *Data Loss:*

Data loss occurs when data stored in the cloud is accidentally or maliciously deleted, corrupted, or rendered inaccessible. This can happen due to hardware failure, software bugs, malicious attacks, or even human error [35].

The loss of critical business data can lead to operational disruptions, with companies often facing costly recovery efforts. If the lost data is not backed up or cannot be restored, the organization may lose important business information, resulting in financial losses, operational downtime, and potential service interruptions. In some cases, a data loss incident can also lead to legal consequences, especially if the lost data includes customer or regulated data, undermining business continuity and customer trust.

✓ *Data Leaks:*

Data leakage—often resulting from poor security policies or the exploitation of vulnerabilities—is the illegal sharing or communication of private data outside of an entity. This can occur via insecure routes including email or cloud storage or through insider threats whereby staff members either purposefully or inadvertently reveal data [35].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun154

Data leaks have wide-ranging consequences include compromise of trade secrets, consumer data, or private corporate information. Should the disclosed data contravene industry standards or privacy rules, this can result in legal fines and regulatory penalties. Moreover, data leaks can seriously erode consumer confidence and trust in the company, therefore affecting loss of clients, business prospects, and reputation. Depending on the type of the disclosed material, extreme circumstances could result in business espionage or more destructive behaviour.

- *Human Error:*

Human Errors are a leading cause of security breaches in cloud environments, often resulting from carelessness or the failure to adhere to security instructions and guidelines. These incidents, known as accidental data breaches, occur when cloud users inadvertently expose or compromise sensitive information [31].

Common examples include mistakenly sending sensitive data via email or SMS to unauthorized recipients, unintentionally publishing confidential information on social media, or losing physical records, laptops, mobile devices, or storage media such as external hard drives and USB drives that lack proper security measures like password protection [31].

Additionally, failing to log out of secure websites after use or neglecting to secure access to cloud accounts can create significant vulnerabilities. These human errors can have severe consequences, as they expose organizations to data breaches that may lead to regulatory penalties, reputational damage, and financial loss.

V. VULNERABILITIES IMPACT ON CONFEDENTIALITY, INTEGRITY AND AVAILABILITY (CIA TRIAD)

Table 1 CIA Impact

Attack	CIA Impact	Effect	Link / Reference
Insecure APIs	Confidentiality, Integrity	Unauthorized access to data, data manipulation, and potential breach of secure communication	51,52,19
Data Breach	Confidentiality	Exposure of sensitive information, leading to data privacy issues and potential data loss	31,39,40,41
Misconfigured Cloud Storage	Confidentiality, Integrity and Availability	Data exposure to unauthorized users and risk of data being deleted or made inaccessible	53,54
Denial of Service (DoS)	Availability	Service disruptions, preventing legitimate users from accessing cloud applications	4,37,43
Virtualization Attacks	Integrity, Availability	Compromised virtual machines, data tampering, and possible downtime of cloud services	6,23,33,55
Insider Threats	Confidentiality, Integrity, Availability	Data theft, unauthorized data modification, and service disruptions	19,56
Data Loss	Integrity, Availability	Loss of critical data, impacting business continuity and data integrity	31,39,40,41
Account Hijacking	Confidentiality, Integrity	Data exfiltration, unauthorized actions, and compromised system security	31,39,40
Man-in-the-Middle (MITM)	Confidentiality, Integrity	Eavesdropping, data manipulation, and loss of data privacy	19,27
Weak Identity Management	Confidentiality, Integrity, Availability	Unauthorized data access, compromised integrity of transactions, and potential service outages	19,57,58

VI. EXISTING SOLUTIONS FOR THE VULNERABILITIES

- *Data Level:*

Data-level security in cloud environments has employed a variety of techniques for reducing the risk of data loss or leakage. The primary techniques include encryption mechanisms like : TLS (Transport Layer Security), AES (Advanced Encryption Standard), and SHA (Secure Hash Algorithm)-sensitive data will be stored or transmitted securely through these methods.

Data classification is the other technique which actually sets the security level according to the sensitivity of data so that suitable protection can be enforced. However, the encryption technologies are still not matured completely with many challenges like performance and implementation issues.

Also, data classification techniques tend to require a lot of resources and so reduce the efficiency of cloud operations.

- *Application Level:*

Application level security techniques like Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are quite useful with regards to mitigating Distributed Denial-of-Service (DDoS) attacks against cloud applications and services.

While these current methods are useful for simple DDoS attacks, they struggle against more sophisticated and complex attack patterns that are common within a cloud environment. This gap hence demands advancement in addressing new solutions for the detection and prevention of complex as well as unknown threats.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun154

Besides, their effectiveness is mostly limited by testing environments using little data, thus making it difficult to be implemented adequately. Conventional access control and identity management systems are also inadequate for good safeguarding. To tackle the authentication issues, techniques such as Identity Management Systems (IDMS) and mechanisms of authentication with AES (Advanced Encryption Standard) and MD5 (Message Digest Algorithm 5) are used. However, such techniques have shortcomings concerning the adaptations for the cloud's active and changing threat environment [19, 39, 42–46].

- *Network Level:*

Denial-of- Service and Distributed Denial-of- Service are common uses for existing security measures including Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) at the level of a network. They are backed by solutions addressing DNS issues, which heavily rely on dynamic firewalls and also IDS into the whole network security.

One major disadvantage of many of the DoS and DDoS mitigating strategies is that they ignore IP spoofing, a tactic often used in such attacks to destroy networks by passing for normal tainted traffic. These methods cannot distinguish between traffic, actual and dangerous. Most current solutions also overlook rather a lot of significant network vulnerabilities, including Man-in---the-middle attacks, data modification assaults, spoofed DNS IDs, and corrupted data attacks—great weaknesses in the network. [19, 26].

- *Host Level:*

Host-side mechanisms of intrusion detection and monitoring virtual machines (VMs) are common techniques to troubleshoot problems related to virtual machines and hypervisors. However, they are often specific to certain scenarios and depend on well-known attack patterns or particular software vulnerabilities.

In this sphere, more advancements could be made to tackle more complex threats, especially distributed side-channel attacks. Security measures of the future must center on designing detection and prevention mechanisms that would effectively counter these newer, more advanced types of attack, not just those that would have been effective against the more limited ones now being used. [19, 47-50].

VII. SCOPE FOR FURTHER RESEARCH

This research focuses on addressing the inadequacies limiting the existing cloud infrastructure and suggesting mitigation strategies to such concerns. The following are critical areas of impact.

- *Minimizing Human Errors in Cloud Security:*

Human errors, such as misconfigurations, weak password management, and neglecting security best practices, are significant vulnerabilities in cloud environments. Implement automated configuration management tools, use role-based access control to limit permissions, and provide extensive training programs for administrators and users to reduce human-related security risks.

- *Enhancing Intrusion Detection and Prevention Systems (IDS/IPS):*

Effective solely for established attack patterns, traditional IDS and IPS systems struggle with complex, developing threats. Particularly in distributed clouds, they are sometimes insufficient in differentiating between good and bad activity.

Create adaptive and artificial intelligence-driven IDS/IPS able to identify fresh and changing threat paths. This covers designing systems able to use real-time threat intelligence and dynamically learn from network behaviour. Studies on this approach [59] are under progress now.

- *Addressing Limitations in Current Security Measures:*

Existing defences, such as firewalls and DNS security mechanisms, are not sufficient to combat IP spoofing and advanced Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attacks.

Explore advanced techniques for identifying and mitigating IP spoofing, such as anomaly detection using machine learning algorithms. Investigate adaptive filtering and rate-limiting strategies for network traffic management.

- *Improving API Security:*

Insecure APIs remain a weak point, providing a gateway for attackers to exploit cloud services.

Emphasize secure API development practices, such as implementing strong authentication, encryption, and proper access control measures. The research can delve into methods for continuous API vulnerability assessment.

- *Hypervisor and Virtual Machine (VM) Security:*

Virtualization vulnerabilities, like hypervisor exploits and VM-based attacks, pose significant threats due to shared hardware resources in cloud environments.

Focus on developing more robust hypervisor security techniques, including monitoring systems for real-time threat detection and advanced sandboxing methods to isolate VMs securely.

- *Mitigating Data-Based Attacks:*

Especially considering the growing volume of private data kept in the cloud, data breaches, loss, and leaking remain major concerns.

Investigate advanced encryption mechanisms, efficient data backup strategies, and methods to ensure data integrity through blockchain technology or other decentralized systems.

- *Strengthening Authentication and Access Control:*

Weak identity management systems increase the risk of unauthorized access and privilege escalation.

Develop comprehensive multi-factor authentication (MFA) strategies and adaptive access control systems that can dynamically adjust based on user behaviour and context.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun154

VIII. CONCLUSION

This paper has analysed the significant risks associated with cloud computing and the advancements aimed at mitigating them. Developments in cloud technology are expected to persist. Security impacts both the institutions and the end consumers. Considering the many and ever growing cloud-related threats, the research indicates that a singular security strategy will be inadequate. A solution must be implemented in the form of a system that integrates advanced encryption protection, access control, and continuous monitoring. Moreover, due to the transitory nature of technology, proactive security research and policy implementation should consistently safeguard data confidentiality, integrity, and accessibility.

The research emphasizes the necessity of collaboration among cloud service providers, the government, and the corporation for effective security provision. Emerging security challenges stemming from the integration of advanced technologies such as artificial intelligence and the Internet of Things into the cloud necessitate a novel paradigm shift in security. Consequently, proactive measures such as investing in research and development and enhancing security awareness among many stakeholders are essential to ensure the integrity of cloud computing in the future.

ACKNOWLEDGMENT

Professor Sheveta's help and support throughout this review paper's development are much appreciated. I also thank Lovely Professional University for offering academic resources and an environment for this effort. Finally, AI tools like ChatGPT, Deepseek helped us grasp the research that went into this study.

REFERENCES

[1]. Roberts, L. (1988). The arpanet and computer networks. In ACM eBooks (pp. 141–172).

[2]. R. Buyya, J. Broberg, A. M. Goscinski, Cloud Computing Principles and Paradigms, Wiley Publishing, 2011.

[3]. Vulnerabilities and Countermeasures. Int. J. Comput. Appl. 2015, 119, 46–53.

[4]. Dinh, P.T.; Park, M. Dynamic Economic-Denial-of-Sustainability (EDoS) Detection in SDN-based Cloud. In Proceedings of the 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France, 20–23 April 2020.

[5]. Karajeh, H.; Maqableh, M.; Masa'deh, R. Privacy and security issues of cloud computing environment. In Proceedings of the 23rd IBIMA Conference Vision, Valencia, Spain, 13–14 May 2020.

[6]. Han, J.; Zang, W.; Chen, S.; Yu, M. Reducing Security Risks of Clouds Through Virtual Machine Placement. In Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy, Philadelphia, PA, USA, 19–21 July 2017.

[7]. Saravanan, N.; Umamakeswari, A. Lattice based access control for protecting user data in cloud environments with hybrid security. Comput. Secur. 2021, 100, 102074.

[8]. Minhaj Ahmad Khan, A survey of security issues for cloud computing, Journal of Network and Computer Applications,

[9]. 18 U.S. Code Chapter 119 - WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS. (n.d.). LII / Legal Information Institute.

[10]. Lutkevich, B. (2020, August 28). HIPAA (Health Insurance Portability and Accountability Act). Health IT and EHR.

[11]. Choo, Kim-Kwang Raymond. "Cloud computing: Challenges and future directions." Trends and Issues in Crime and Criminal justice 400 (2010): 1-6.

[12]. Marston, S.; Li, Z.; Bandyopadhyay, S.; Ghalsasi, A. Cloud Computing—The Business Perspective. Decis. Support Syst. 2011, 51, 176–189.

[13]. Microsoft, "What is SaaS? Software as a service," Microsoft Azure. [Online]. Available: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-saas

[14]. Microsoft, "What is PaaS? Platform as a service," Microsoft Azure. [Online]. Available: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-paas

[15]. Microsoft, "What is IaaS? Infrastructure as a service," Microsoft Azure.[Online].Available:https://azure.microsoft.com/enus/resources/cloud-computing-dictionary/what-is-iaas

[16]. Maha Zeedan, Gamal Attiya, Nawal El-Fishawy, Enhanced hybrid multi-objective workflow scheduling approach based artificial bee colony in cloud computing, Computing, 10.1007/s00607-022-01116-y, **105**, 1, (217-247), (2022).

[17]. V. Lakshmi Narasimhan, V. S. Jithin, M. Ananya, Jonathan Oluranti, AI-Based Enhanced Time Cost-Effective Cloud Workflow Scheduling, Artificial Intelligence for Cloud and Edge Computing, 10.1007/978-3-030-80821-1_13, (277-297), (2022).

[18]. Solanke Vikas et al, International Journal of Computer Science & Communication Networks,Vol 3(2), 79-83

[19]. Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M. A., & Al-Rimy, B. a. S. (2021). Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges. Applied Sciences, 11(19), 9005.

[20]. S.Marstonetal. /DecisionSupportSystems51 (2011) 176-189

[21]. IJCSMA. (2018). CIA Triad for Achieving Accountability in Cloud Computing Environment. In International Journal of Computer Science and Mobile Applications: Vol. Issue. 3 (pp. 38–43) [Journal-article].

[22]. Hougen, A. (2024b, July 11). What Are the 5 Cloud Deployment Models [Explained & Compared]. Cloudwards.

[23]. Tank,D.; Aggarwal, A.; Chaubey, N. Virtualization vulnerabilities, security issues, and solutions: A critical study and comparison. Int. J. Inf. Technol. 2019, 1–16.

[24]. Turab, N.M.; Abu Taleb, A.; Masadeh, S.R. Cloud Computing Challenges and Solutions. Int. J. Comput. Netw. Commun. 2013, 5, 209–216.

[25]. AlAmri,S.M.; Guan, L. Infrastructure as a service: Exploring network access control challenges. In Proceedings of the 2016 SAI Computing Conference (SAI), London, UK, 13–15 July 2016.

[26]. Gupta, B. B., & Badve, O. P. (2016). Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment. Neural Computing and Applications, 28(12), 3655–3682.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun154

[27]. C. -Y. Cheng, E. Colbert and H. Liu, "Experimental Study on the Detectability of Man-in-the-Middle Attacks for Cloud Applications," 2019 IEEE Cloud Summit, Washington, DC, USA, 2019, pp. 52-57, doi: 10.1109/CloudSummit47114.2019.00015. keywords: {Man-in-the Middle attacks;packet round-trip time analysis;machine learning},. [

[28]. Sharma, A.; Keshwani, B.; Dadheech, P. Authentication issues and techniques in cloud computing security: A review. In Proceedings of the International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Jaipur, India, 26–28 February 2019.

[29]. Kazim, M.; Zhu, S.Y. A survey on top security threats in cloud computing. Int. J. Adv. Comput. Sci. Appl. 2015, 6.

[30]. Muhammad Kazim and Shao Ying Zhu, "A survey on top security threats in cloud computing" International Journal of Advanced Computer Science and Applications(ijacsa), 6(3), 2015.

[31]. A survey on data breach challenges in cloud computing security: Issues and threats. (2017, April 1). IEEE Conference Publication | IEEE Xplore.

[32]. Aich, A., & Sen, A. (2015). Study on Cloud Security Risk and Remedy. International Journal of Grid and Distributed Computing, 8(2), 155–166

[33]. Nagar, N., & Suman, U. (2016). Analyzing Virtualization Vulnerabilities and Design a Secure Cloud Environment to Prevent from XSS Attack. International Journal of Cloud Applications and Computing, 6(1), 1–14.

[34]. Kaja, D. V. S., Fatima, Y., & Mailewa, A. B. (2022). Data Integrity Attacks in Cloud Computing: A Review of Identifying and Protecting Techniques. International Journal of Research Publication and eviews, 713–720.

[35]. Vurukonda, N., & Rao, B. T. (2016). A Study on Data Storage Security Issues in Cloud Computing. Procedia Computer Science, 92, 128–135.

[36]. Vaquero, L.M.; Rodero-Merino, L.; Caceres, J.; Lindner, M. A Break in the Clouds: Towards a Cloud Definition; ACM: New York, NY, USA, 2008.

[37]. Wani, A.R.; Rana, Q.P.; Saxena, U.; Pandey, N. Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques. In Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4–6 February 2019.

[38]. Li, P.; Li, J.; Huang, Z.; Gao, C.-Z.; Chen, W.-B.; Chen, K. Privacy-preserving outsourced classification in cloud computing. Clust. Comput. 2017, 21, 277–286.

[39]. Manogaran, G.; Thota, C.; Kumar, M.V. MetaCloudDataStorage Architecture for Big Data Security in Cloud Computing. Procedia Comput. Sci. 2016, 87, 128–133.

[40]. Sood, S.K. A combined approach to ensure data security in cloud computing. J. Netw. Comput. Appl. 2012, 35, 1831–1838.

[41]. Vurukonda, N.; Rao, B.T. A Study on Data Storage Security Issues in Cloud Computing. Procedia Comput. Sci. 2016, 92, 128–135.

[42]. AlAmri,S.M.; Guan, L. Infrastructure as a service: Exploring network access control challenges. In Proceedings of the 2016 SAI Computing Conference (SAI), London, UK, 13–15 July 2016.

[43]. Nautiyal, S.; Wadhwa, S. A Comparative Approach to Mitigate Economic Denial of Sustainability (EDoS) in a Cloud Environment. In Proceedings of the 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 21–22 November 2019.

[44]. Rehman, F.; Akram, S.; Shah, M.A. The framework for efficient passphrase-based multifactor authentication in cloud computing. In Proceedings of the 2016 22nd International Conference on Automation and Computing (ICAC), Colchester, UK, 7–8 September 2016

[45]. Rajeswari, P.; Raju, S.V.; Ashour, A.S.; Dey, N. Multi-fingerprint unimodel-based biometric authentication supporting cloud computing. In Intelligent Techniques in Signal Processing for Multimedia Security; Springer: Cham, Switzerland, 2017; pp. 469–485.

[46]. Devipriya, K.; Lingamgunta, S. Multi Factor Two-way Hash-Based Authentication in Cloud Computing. Int. J. Cloud Appl. Comput. 2020, 10, 56–76.

[47]. Deshpande, P.; Sharma, S.C.; Peddoju, S.K.; Junaid, S. HIDS: A host based intrusion detection system for cloud computing environment. Int. J. Syst. Assur. Eng. Manag. 2018, 9, 567–576.

[48]. Ramamoorthy, S.; Rajalakshmi, S. A Preventive Method for Host Level Security in Cloud Infrastructure. In Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC–16'); Springer: Cham, Switzerland, 2016; pp.3-12.

[49]. Bazm,M.-M.; Lacoste, M.; Südholt, M.; Menaud, J.-M. Isolation in cloud computing infrastructures: New security challenges. Ann. Telecommun. 2019, 74, 197–209.

[50]. Mahajan, V.; Peddoju, S.K. Deployment of Intrusion Detection System in Cloud: A Performance-Based Study. In Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, Australia, 1–4 August 2017.

[51]. Qazi, F. (2023). Application Programming Interface (API) Security in Cloud Applications. EAI Endorsed Transactions on Cloud Systems, 7(23), e1.

[52]. Multi-factor web API security for securing Mobile Cloud. (2015, August 1). IEEE Conference Publication | IEEE Xplore.

[53]. Khan, H. M., & Zaidi, S. M. H. (2024). Detecting Security System Misconfiguration Threats in Cloud Computing Environments Using AI. American Journal of Innovation in Science and Engineering, 3(3), 31–40.

[54]. Nobles, C. (2022). Investigating Cloud Computing Misconfiguration Errors using the Human Factors Analysis and Classification System. Scientific Bulletin, 27(1), 59–66.

[55]. Virtualization-level security in cloud computing. (2011, May 1). IEEE Conference Publication | IEEE Xplore.

[56]. Insider Threats to Cloud Computing: Directions for New Research Challenges. (2012, July 1). IEEE Conference Publication | IEEE Xplore.

[57]. Sharma, D.H.; Dhote, C.; Potey, M. Identity and Access Management as Security-as-a-Service from Clouds. Procedia Comput. Sci. 2016, 79, 170–174.

[58]. Khajehei, K. Preserving Privacy in Cloud Identity Management Systems Using DCM (Dual Certificate Management). Int. J. Wirel. Microw. Technol. 2018, 8, 54–65.

[59]. Khan, M. M. (2024). Developing AI-Powered Intrusion Detection System for Cloud Infrastructure. Journal of Artificial Intelligence Machine Learning and Data Science, 2(1), 1074–1080.