International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN(Online): 2347-5552, Volume-12, Issue-3, May 2024
https://doi.org/10.55524/ijircst.2024.12.3.14
Article ID IRP-1518, Pages 87-95
www.ijircst.org

# Securing the Skies- A Critical Analysis of Cloud Infrastructure Vulnerabilities

**Vaishnavi Chaudhari[1], Poonam Dhake[2], Snehal Salunkhe[3], and Mahendra Suryavanshi[4]**

[1 2 3] Student, Department of Computer Science and Application, Dr Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India
[4]Assistant Professor, Department of Computer Science and Application, Dr Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India

Correspondence should be addressed to Vaishnavi Chaudhari; vaishnavichaudhari2002@gmail.com

Received: 16 April 2024 Revised: 30 April 2024 Accepted: 14 May 2024



**ABSTRACT-** Cloud computing offers storage, infrastructure, computing, networking, databases, platform, software, and analytics services over the Internet. It provides numerous benefits including scalability, cost management, broad access to resources, elasticity, resource pooling. Though cloud computing is mature and widely adopted computing model in software as well as non-software industries, it has several issues regarding security as it provides most of the cloud services over the public infrastructure. Denial of service (DOS), malware injection, insecure APIs, data loss, data breaches, hypervisor vulnerabilities, VM escape are a few major issues in cloud computing. In this paper, authors tried to provide comprehensive analysis of critical security issues in cloud computing. Furthermore, this paper critically analyses the existing solutions to the various security issues in cloud computing model.

**KEYWORDS-** Cloud Security, Authentication, Access Control, Hypervisor, Data Breaches.

## I. INTRODUCTION

A technology known as "cloud computing" makes it possible to provide computer services such as servers, storage, databases, networking, software, and analytics over the internet. Without the use of local servers or desktop computers, it enables users to access, store, and execute apps remotely. Numerous benefits, including scalability, flexibility, cost savings, and simpler management, come with cloud computing. On the other hand, cloud computing has several issues such as Incast, load balancing, resource allocation, vendor lock-in, interoperability, data lock-in and security [1][2].

Latest Facts and Details of Cloud Computing-

- Handling security issues, especially those pertaining to compliance and data protection[3].
- Integration of blockchain improving data management and security[4].
- Green cloud computing lowers carbon emissions and energy use[5].
- Resource management for cloud infrastructure is made easier with Software-Defined Cloud Computing[6].
- Improved administrative support and corresponding focal points have an impact on the appropriation of cloud computing[7].

These most recent trends and advancements in cloud computing show the continuous attempts to solve issues and enhance the system for enhanced usability, security, and performance.

Three primary deployment strategies and three service delivery models are included in the cloud computing model. Three deployment methods are offered: Public cloud, which is open to the public for registration and usage; Private cloud, which is exclusive to a single organization; and Hybrid cloud, which combines elements of both public and private clouds. Conversely, the models of service delivery include Infrastructure as a Service (IaaS): Providers offer network, storage, and computational resources as internet-based services; one well-known IaaS provider is Amazon EC2.

Platform-as-a-service (PaaS): With Google Apps and Microsoft Windows Azure as well-known examples, providers offer platforms, tools, and business services for users to develop, deploy, and manage applications without the need for local installations.

Software-as-a-service (SaaS): Providers offer cloud-hosted software to end customers as internet-based services, removing the requirement for [8][9].

Three primary deployment models are included in the cloud computing model: private, public, and hybrid clouds.

*Private cloud*: With this deployment strategy, sensitive data and operations are housed in a highly regulated and secure environment on a cloud platform that is exclusive to an organization.

*Public cloud:* On the other hand, anybody may sign up and utilize a public cloud, which provides accessibility and scalability but may also give rise to security issues because of its openness.

*Hybrid cloud*: By extending private cloud resources to use public cloud services as needed, hybrid clouds enable enterprises to take use of the advantages of both private and public cloud models.

These deployment patterns are essential in determining how businesses organize their cloud infrastructure to satisfy their unique [8][9].

There are many advantages and benefits of service model and deployment model are as follows:

*Efficient Resource Utilisation:* In order to satisfy customer demands for scalable resources based on demand, cloud providers strive to increase resource utilisation while cutting costs.

*Multiple Tenancy and Elasticity*: The cloud model provides both multi-tenancy, which permits resource sharing across tenants, and elasticity, which permits resource scaling up or down in response to demand. Although these characteristics increase flexibility and resource efficiency, strong security measures are needed to preserve data confidentiality.

*Isolation and Location Transparency:* To stop planned attacks that take use of data co-location vulnerabilities, secure multi-tenancy necessitates location transparency and data isolation between tenants.

Identity & Access Management: For safe cloud operations, strong identity management systems with capabilities like identity provisioning, federation, single sign-on, and authentication is essential.

Key Management: Data secrecy requires encryption, and efficient key.

Cloud computing presents several security issues and challenges. One major concern is the lack of control and awareness over the location of data stored in the cloud, which raises questions about data security and privacy [10]. Additionally, there are risks of unauthorized access, breaches of security measures, and disruptions to service availability [11]. The virtualization environment used in cloud computing is also vulnerable to attacks, such as information leakage during VM migration and uploading malicious VMs [12]. Other challenges include auditing, data migration between clouds, and ensuring the permanent deletion of user data [13]. The complexity of the cloud architecture makes achieving end-to-end security difficult, requiring the development of new security techniques and the adaptation of existing ones [14]. Overall, addressing these security challenges requires a holistic understanding of cloud security attributes, security requirements, and the roles of different parties involved.

## II. SECURITY ISSUE IN CLOUD COMPUTING

Issues with cloud security include denial of service (DOS), malware injection, insecure APIs, account or service traffic hijacking, data breaches, cloud abuse, and data loss. Privilege access, regulatory compliance, recovery, data location, data segregation, support for investigations, and data availability are additional issues [15]. In addition, there are application problems, shared vulnerabilities, lack of support for investigations, and malicious insider attackers when it comes to cloud computing security [16]. Aside from that, crucial factors to consider are security policy, legal, regulatory, and compliance, privacy, trust, control, data ownership, data location, audits and reviews, business continuity and disaster recovery, and emerging security threats and attacks. Concerns about privacy and security are brought up by the paradigm shift that cloud computing brings about with its deperimeterized organizational infrastructure, particularly in public cloud computing [17].
Some of the major security issues are as follows-

### *A. Data Breaches*

Sensitive information kept in cloud environments is at risk from data breaches, a serious cloud security concern. The following points shed light on data breaches as a potential threat to cloud security:

- Challenges and Issues with Cloud Computing Security: The study emphasizes that despite cloud computing's advantages, businesses are reluctant to use it because of security concerns. Transferring sensitive information to a different organization increases the risk of data breaches, underscoring the importance of being aware of the dangers of cloud environments [18].
- Cloud Computing and Security Concern: The author highlights how crucial security is in cloud computing settings. It talks about how weak and inconsistent security measures can leave sensitive data on remote servers vulnerable to unauthorized access, potentially undermining the legitimacy of cloud computing's benefits [19].
- Enhanced Cloud Computing End-to-End Data Security Method: This paper addresses cloud computing security breaches by proposing an end-to-end data security approach. The suggested approach seeks to improve data security and prevent breaches by implementing additional security measures like padding sequences, randomized salting, hashing, and encryption techniques, making it more difficult for unauthorized access to occur [20].

### *B. Insecure APIs*

- Vulnerabilities in API Security: Although many users are unaware of their insecurity, APIs are recognized as potential points of attack in cloud applications. Instead of securing individual APIs, organizations frequently rely on network security because they lack the tools and training necessary to inform users about API security [21].
- Role-Based Access Control for API Security: A strong API access control mechanism is required because cloud computing security greatly depends on API security. To improve security in cloud environments, the Role-Based Access Control Model is suggested as a two-stage access control mechanism at the API level [22].
- Emphasis on Secure APIs: The literature review highlights the significance of securing APIs to improve business enterprises in the United States of America, particularly in the context of improving cloud security. One of the vulnerabilities affecting cloud services is identified as insecure APIs, highlighting the necessity of addressing this problem to reduce security risks in cloud computing [23].

### *C. Data Loss*

The article discusses security concerns related to data loss, specifically pertaining to cloud resources and insider attacks. The report emphasizes that data loss is a serious security risk in cloud computing [24]. In order to avoid breaches and guarantee data integrity, cloud computing security concerns related to data loss are handled by encryption techniques and fine-grained authorization [25].
The study discusses data loss security challenges, especially in light of insider attacks and cloud vulnerabilities. The study

emphasizes that a significant security risk associated with cloud computing is data loss [26]. Because several people can access and alter data in the cloud, which raises security concerns, data loss is a frequent issue. The paper discusses data loss security challenges, especially as they pertain to cloud data storage [8].

### *D. Account Hijacking*

There is no mention of account hijacking security vulnerabilities in the material that is provided. Weak authentication procedures, unsecured API interfaces, data loss, and leakage are some of the security challenges [25][27].

Data theft results from the compromise of confidentiality and integrity caused by account or service traffic hijacking. Policies for fraud detection and anti-phishing are advised for mitigation [20]. Hackers can obtain personal information, such as bank account credentials, through account or service traffic hijacking, which compromises confidentiality and integrity. Weak authentication procedures, unsecured API interfaces, and vulnerabilities related to data loss and leakage are some of the security flaws that lead to account hijacking. account or service Traffic hijacking compromises integrity and confidentiality by giving hackers access to users' private information, such as bank account credentials [8].

### *E. Virtualization-Related Cloud Security Issues*

Virtualization-related cloud security problems are a major worry in cloud computing environments. Since virtualization is a key component of cloud computing, any risks or vulnerabilities affecting it could have an effect on the cloud's overall security [29]. New security issues, such as hypervisor vulnerabilities, virtual machine (VM) escape, VM sprawl, and inadequate isolation between VMs, are brought about by the use of virtualization in cloud computing [29][30].

Vulnerabilities in hypervisors can result in control compromise, data leakage, and illegal access. A security flaw known as "VM escape" allows an attacker to take over the underlying hypervisor of a compromised virtual machine (VM), which could have an impact on other VMs that are hosted on the same physical host [30]. The unchecked growth of virtual machines, or "VM sprawl," can pose security risks since it is challenging to manage and keep an eye on the security of so many VMs [30]. Security risks can also arise from inadequate isolation between virtual machines (VMs), since an attacker may be able to access resources or data in other VMs that are operating on the same physical host [29][30].

In conclusion, virtualization-related cloud security risks pose a serious threat to cloud computing environments. VM escape, VM sprawl, hypervisor vulnerabilities, and inadequate isolation between VMs are a few of the security issues that require attention. To address these security issues, a number of mitigation strategies have been put forth, including security-enhanced virtualization architectures, hypervisor hardening, and virtual machine introspection.

## III. EXISTING SOLUTIONS

### *A. Symmetric and Asymmetric Encryption*

In order to protect data privacy and ensure secure transmission, encryption techniques are frequently used to address cloud security issues. Asymmetric and symmetric encryption are the two most used kinds of encryption methods.

A pair of keys is used in asymmetric encryption, commonly referred to as public-key encryption: a private key is used for decryption and a public key is used for encryption. Because the private key is kept secret and it is computationally impossible to deduce the private key from the public key, this method offers high security. Secure email and secure web browsing are two common applications of asymmetric encryption [31][32].

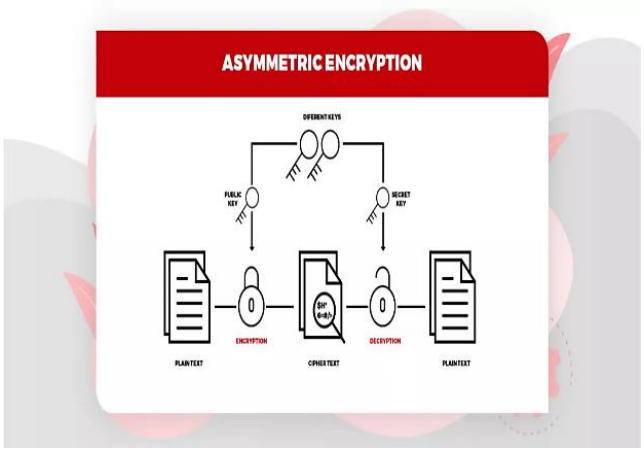


Figure 1: Asymmetric Encryption [40]

Fig. 1 illustrates the secure key-pair communication method known as asymmetric encryption. Unlike normal encryption, which employs a single key, this method uses a public key and a private key, which are coupled mathematically. The public key is freely available to anyone, allowing anyone to encrypt messages for the recipient. However, the recipient's private key, which is kept private, is required to decode the message. This creates a secure communication channel that anybody may use to send encrypted messages that are guaranteed to remain secret and can only be decrypted by the intended receiver.

In contrast, symmetric encryption employs an identical key for both encryption and decryption. Although this method requires a safe way for the communicating parties to share the key, it is faster than asymmetric encryption. For large-scale data encryption, like encrypting cloud storage data, symmetric encryption is frequently utilized [31][32].

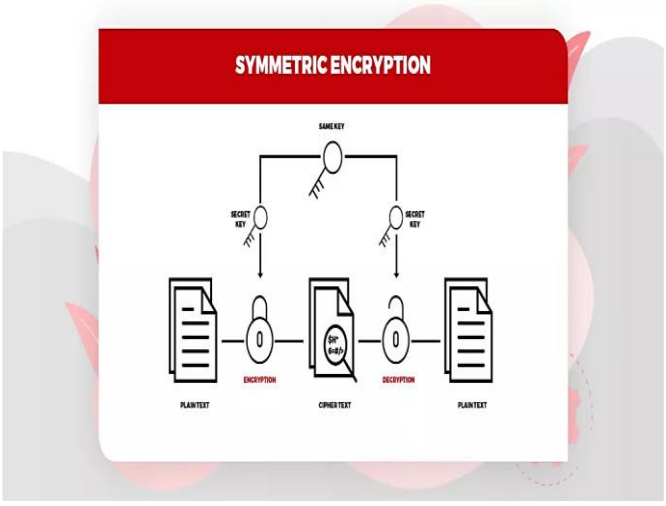


Figure 2: Symmetric Encryption [40]

As illustrated in Fig. 2, symmetric encryption secures communication by using a single, shared secret key. Unlike methods that rely on public and private keys, symmetric encryption requires that the sender and recipient share the same secret key. The procedure starts with the first plain text message that has to be sent. This message is then jumbled into illegible ciphertext using a secret key and an encryption method. This ciphertext is the secure version of the message sent across the communication channel. After getting the ciphertext, the recipient uses a decryption method and the same shared secret key to decode the message, returning it to plain text in its original, readable form. To put it another way, symmetric encryption functions like a shared secret code shared by two individuals. They both encrypt and decrypt communications using the same code, making sure that only they can decipher the private correspondence.

### *B. Access Control Measures and Multi-factor authentication*

Access control methods like multi-factor authentication and role-based access control are among the solutions currently available for cloud security problems. Using role-based access control, you can limit authorized users' access to the system [33]. It is a popular access control method that, by defining roles and giving them permissions, offers fine-grained access control. This lowers the possibility of unauthorized access and data breaches by guaranteeing that users only have access to the resources they require to perform their job duties.

Another crucial security measure that reinforces cloud security is multi-factor authentication, which confirms that only legitimate cloud users are permitted to access cloud resources, apps, data, and services [33]. Users must supply a minimum of two authentication methods, like a password and a fingerprint scan or a one-time code texted to a mobile device. This increases the difficulty of an intruder gaining access to the cloud system because they would need to know the password for the user as well as the location of their device or biometric information.

Encryption is a crucial security feature for cloud computing in addition to these access control measures. Data in transit and at rest can be safeguarded with encryption, preventing unauthorized users from accessing private data even in the event that the cloud infrastructure is compromised [33].

Implementing a secure multi-factor authentication framework that combines intrusion detection and access control with an automated authentication method selection process is crucial to bolstering cloud security further [33]. By increasing identity verification and lowering false alarms, this can make it harder for hackers to gain access to the cloud system.

To sum up, multi-factor authentication and role-based access control are crucial access control methods that, by limiting system access to authorized users and confirming their identities, can help bolster cloud security. Moreover, intrusion detection systems and encryption can be employed to improve cloud security.

### *C. Security Monitoring And Incident Response*

- ***SIEM-Based Approach for Cloud Security***

Using Security Information and Event Management (SIEM) systems to improve cloud computing environments' security is known as a SIEM-based approach to cloud security. SIEMs are frequently used to prevent data loss in computer systems and networks. Because of their capacity to instantly detect and address security incidents by monitoring logs and correlating data in real-time, they can be especially helpful in cloud environments [34].

Automating cloud resource visibility is a key advantage of adopting a SIEM-based approach to cloud security. A virtual network comprising load balancers, virtual machines, and a web application firewall (WAF) that scans incoming Internet traffic and offers centralized protection against common exploits and vulnerabilities can be used to accomplish this [34]. Organizations can proactively mitigate potential security threats in the cloud environment and continuously monitor and detect security incidents by utilizing the power of a SIEM system.

An additional benefit of employing a SIEM-based strategy for cloud security is the capacity to guarantee adherence to regulatory requirements. For instance, Microsoft Defender for Cloud can reliably evaluate how cloud resources are configured in comparison to industry norms, laws, and benchmarks to make sure compliance requirements are satisfied [34].

To summarize, a cloud security strategy based on SIEM can offer enterprises a reliable and efficient means of protecting their cloud assets, streamlining visibility and incident handling, guaranteeing adherence to regulations, and enhancing the ease of data organization and storage. Organizations can create robust and long-lasting security measures in the cloud computing environment by utilizing inexpensive cloud services and SIEMs.

- ***Cloud-Based Cyber Security Systems***

In today's interconnected digital landscape, cloud-based cyber security systems have become indispensable for organizations looking for strong protection [35]. These systems offer real-time monitoring, threat detection, and incident response while utilizing cloud computing to safeguard digital assets from online attacks. They provide scalable solutions that let companies deal with growing data volumes and respond to changing threats. Lower infrastructure costs, regular patches and updates, centralized administration, and worldwide threat intelligence are some of the main advantages. Systems for cloud-based security defend against a range of threats, such as malware, phishing, DDoS, and illegal access.

Because of the many advantages that cloud-based cyber security systems provide, they are crucial for businesses looking for strong defense in the connected digital world of today. Among these advantages are:

1. Scalability: Cloud-based systems have the ability to scale resources as needed, which enables enterprises to efficiently handle massive data volumes and analyze intricate threat patterns
2. [35]. Constant Updates and Patches: Systems based on the cloud offer constant updates and patches, guaranteeing that security precautions are current and efficient against changing online threats [35].
3. Centralized Management: With the help of these systems, businesses can more easily monitor and manage their security measures from a single platform [35].
4. Flexibility and Reliability: Cloud-based cyber security solutions provide enterprises with robust protection against a range of cyber threats, including malware, phishing, DDoS attacks, and unauthorized access, as well as ease of deployment [35].

All things considered, cloud-based cyber security solutions offer a thorough and efficient method of protecting digital assets, combining cutting-edge technology, affordability, and scalability to satisfy the security requirements of contemporary enterprises.

- ***Container and VM Visualization***

For digital forensics and cybersecurity investigations, container and virtual machine visualization are crucial tools, especially when considering cloud computing and network softwarization. By producing two-dimensional visualizations of container contents and virtual machine disk images, these visualization techniques can aid in lowering the number of virtual machines and containers that are awaiting forensic investigation. These visualizations can be used to identify altered code, identify embedded malware instances, and fingerprint container/VM contents [36].

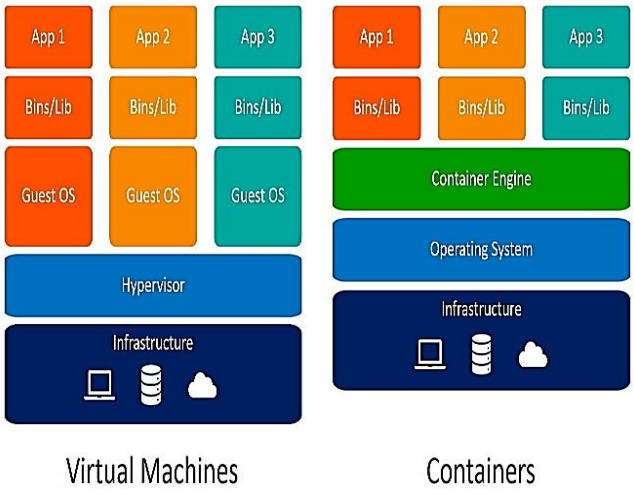


Figure 3: Container and VM Visualization [41]

A comparison diagram between virtual machines and containers is shown in Fig. 3. Self-contained systems, or virtual machines (VMs), have their own operating system (OS), libraries, apps, and binaries. The hardware of a real system powers these virtual machines (VMs), which are kept apart from one another by a software layer known as a hypervisor. With the help of this hypervisor, several virtual machines (VMs) may share the hardware resources on a single computer. On the other hand, the operating system kernel of the host machine is shared by containers. Although every container has its own segregated file system with its own libraries and apps, they are all dependent on the same host computer kernel. Because of this, containers are substantially lighter and startup faster than virtual machines. sides of containers and virtual machines. Each programmer has its own underlying operating system on the virtual machine side, while all three apps share the same underlying operating system on the container side.

- ***Defending Cloud Platforms:***

One of the most important aspects of contemporary cybersecurity is protecting cloud platforms from cyberattacks. Since cloud computing has become so popular, businesses now have more obstacles to overcome in defending their infrastructure and data against changing threats [37]. The article highlights how crucial it is to have strong security measures in place to safeguard private information, cloud-stored apps, and resources. Strong access controls, encryption, secure configurations, frequent patching, network segmentation, and logging and monitoring are important methods for protecting cloud platforms [37]. The article also emphasizes how crucial incident response planning and proactive monitoring are to spotting and averting possible security incidents [37]. It highlights how important it is for businesses, governmental organizations, and cloud service providers to work together to create all-encompassing defence plans. The article also discusses the necessity of ongoing training and skill development to keep up with new threats and effectively fend off cyberattacks [37].

- ***Cyber Incident Management System for 5G-based Critical Infrastructures***

An innovative cyber incident management system for critical infrastructures based on 5G is covered in the article [38]. A security information and event management system (SIEM) are used by this system to provide unified cyber threat monitoring. SIEM systems gather log data, analyze it in real time, identify threats, sound alarms, and provide strategy recommendations. Artificial Intelligence (AI), the Internet of Things, and cloud computing technologies augment the proposed system, greatly enhancing and optimizing threat detection. Additionally, models for distributed data bus operation are developed for fast processing of large data streams with low latency and high resilience, as well as hybrid security data storage models for quick search, scalability, and integrating with external storage.

### *D. Cloud Access Security Broker (CASB)*

A type of system software called a Cloud Access Security Broker (CASB) guards' data in cloud services against malware and regulates access to resources available to application users [39]. CASBs are a crucial component of cloud ecosystems and are employed by businesses to oversee the security of numerous cloud apps, particularly SaaS, which may handle sensitive data [39]. Since the service provider is ignorant of the data semantics, the customer is in charge of ensuring the security of the data used in these applications [39].

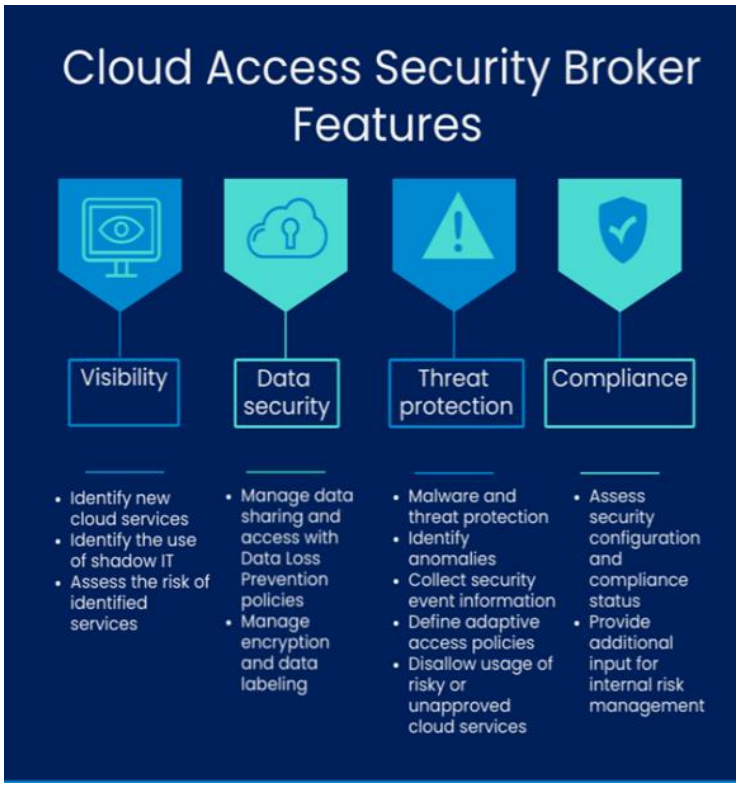


Figure 4: Cloud Access Security Broker (CASB) Features [42]

Fig. 4 depicts a Cloud Access Security Broker (CASB) diagram. Situated between an organization's IT infrastructure and a cloud service provider, a security service is known as a CASB. With capabilities like visibility, data security, threat prevention, and compliance, it aids businesses in securely utilizing cloud services. For example, shadow IT refers to employee use of unapproved cloud services, which CASBs may discover and evaluate the risks involved.

## IV. ANALYSIS ON EXISTING CLOUD SECURITY SOLUTIONS

In the below table 1, analyses existing solutions to the cloud computing security issue.

Table-1: Analysis of existing cloud security solutions

| Solution | | Key Aspects |
|---|---|---|
| Encryption Techniques | Symmetric encryption | The keys used for encryption and decryption are identical. Bulk data encryption is the most popular use case for this technique. Although asymmetric implementation is typically faster and easier to implement, it is not as secure because data can be decoded by anyone who has access to the encryption key. |
| | Asymmetric encryption | Uses a public and private authentication token as two keys to encode and decode data. Because the data cannot be accessed without both a personal token and a public, shareable key, this method offers enhanced security. |
| Access Control Measures and Multi-factor authentication | Access Control Measures | By preventing unwanted access, access controls like multi-factor authentication and strong passwords improve the security of data that is stored. Safe disposal of outdated storage devices and routine data backups are two more ways to protect data while it's not in use. |

| | | |
|---|---|---|
| | Multi-factor authentication | combines two or more authentication techniques, requiring multiple identity proofs and greatly increasing security. It guarantees that sensitive information and services are only accessible to authorized parties. |
| Security Monitoring & Incident Response | SIEM-Based Approach for Cloud Security | Security alerts produced by network hardware and applications are analysed in real time by Security Information and Event Management (SIEM) systems. They are essential for incident response, compliance reporting, and threat detection. |
| | Cloud-Based Cyber Security Systems | Advanced threat detection, network visibility, and incident response capabilities are provided by these systems. They guarantee regulatory compliance and data privacy by defending cloud infrastructure, apps, and data against cyber threats. |
| | Container and VM Visualization | It is easier to find vulnerabilities, spot threats, and handle incidents when containers and virtual machines in the cloud are monitored and visualized. It enhances operational effectiveness, security, and compliance. |
| | Defending Cloud Platforms | Strong security measures, like intrusion detection systems, firewalls, and access controls, are put in place to safeguard cloud platforms against cyberattacks and guarantee data privacy as well as regulatory compliance. |
| | Cyber Incident Management System for 5G-based Critical Infrastructures | This system ensures data protection and service continuity in 5G-based critical infrastructures by managing and responding to cyber incidents. It combines compliance reporting, incident response, and threat intelligence. |
| Cloud Access Security Broker (CASB) | | In the role of a middleman, a CASB controls access to cloud apps and enforces security regulations on behalf of cloud service providers and users. It guarantees threat protection, regulatory compliance, and data privacy. |

It is critical to consider the essential components of encryption methods, access control controls with multi-factor authentication, and security monitoring with incident response capabilities when examining current security solutions for cloud environments. Symmetric encryption is effective for encrypting large amounts of data, whereas asymmetric encryption uses public and private keys to provide increased security. Because they demand several forms of identity verification, access control methods like multi-factor authentication greatly improve security. A SIEM-based approach to cloud security, cloud-based cyber security systems, container and virtual machine visualization, and robust security measures to protect cloud platforms are critical for security monitoring and incident response. For instance, asymmetric encryption offers increased security but may be slower than symmetric encryption, which is effective for large amounts of data. SIEM systems are essential for real-time threat detection and compliance reporting, and multi-factor authentication is necessary for access to sensitive data. For a strong cloud security strategy, a combination of these methods customized to the needs of the company is advised.

## V. CONCLUSION

The complexity of cloud security encompasses various threats such as data breaches, insecure APIs, data loss, account hijacking, and virtualization-related risks. Addressing these challenges requires robust measures including encryption, access controls, and API security, emphasizing the critical need for continuous vigilance and innovative mitigation strategies. Cloud security solutions encompass vital aspects including encryption techniques, access control measures with multi-factor authentication, and robust security monitoring with incident response capabilities. Symmetric encryption efficiently encrypts bulk data, while asymmetric encryption enhances security. Multi-factor authentication ensures heightened access security, while SIEM-based monitoring and incident response systems bolster overall defence against cyber threats. Customized integration of these solutions is imperative for a robust cloud security strategy.

## CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

## REFERENCES


1) M. Suryavanshi, A. Kumar, and J. Yadav, "Balanced Multipath Transport Protocol for Mitigating MPTCP Incast in Data Center Networks," International Journal of Next-Generation Computing, vol. 12, no. 3, 2021.
2) V. Roy, C. Deshpande, N. Kumar, and M. Suryavanshi, "Cloud computing security issues and existing solutions," Vidhyayana-An International Multidisciplinary Peer-Reviewed E-Journal-ISSN, vol. 8, no. si7, pp. 352-360, 2023.
3) W. Hassan, T.-S. Chou, X. Li, P. Appiah-Kubi, and O. Tamer, "Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks," International Journal of Informatics and Communication Technology (IJ-ICT), 2019.
4) Ch. V. N. U. Murthy, M. L. Shri, S. N. Kadry, and S. Lim, "Blockchain Based Cloud Computing: Architecture and Research Challenges," IEEE Access, vol. 8, pp. 205190-205205, 2020.
5) M. Masdari and M. Zangakani, "Green Cloud Computing Using Proactive Virtual Machine Placement: Challenges and Issues," Journal of Grid Computing, vol. 18, pp. 727-759, 2019.
6) A. Abbasi, A. Abbasi, S. Shamshirband, A. T. Chronopoulos, V. Persico, and A. Pescapé, "Software-Defined Cloud Computing: A Systematic Review on Latest Trends and Developments," IEEE Access, vol. 7, pp. 93294-93314, 2019.
7) Gui, Y. Fernando, M. S. Shaharudin, M. Mokhtar, I. G. M. Karmawan, and S. Suryanto, "Cloud Computing Adoption Using TOE Framework for Indonesia's Micro Small Medium Enterprises," JOIV : International Journal on Informatics Visualization, 2020.
8) S. D. S. S. Sridhar and S. Smys, "A survey on cloud security issues and challenges with possible measures," in International conference on inventive research in engineering and technology, vol. 4, 2016.
9) S. Sharma, G. Gupta, and P. R. Laxmi, "A survey on cloud security issues and techniques," arXiv preprint arXiv:1403.5627, 2014.
10) S. R. Masadeh, F. M. AlShrouf, and A. S. Kumar, "Concerns from Cloud Security Issues: Challenges and Open Problems," International Journal, vol. 12, no. 1, 2023.
11) M. Khalil, A. Khreishah, and M. Azeem, "Cloud computing security: A survey," Computers, vol. 3, no. 1, pp. 1-35, 2014.
12) R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud computing: security issues and research challenges," International Journal of Computer Science and Information Technology & Security (IJCSITS), vol. 1, no. 2, pp. 136-146, 2011.
13) A. Iqbal, "Ovarian Leiomyoma Associated with Serous Cystadenoma-A Case Report of an Uncommon Entity Ovarian Leiomyoma Associated with Serous Cystadenoma-A Case Report of an Uncommon Entity," (2023).
14) M. Abdelrazek, J. Grundy, and I. Mueller, "An analysis of the cloud computing security problem," (2010).
15) K. Surya, M. Nivedithaa, S. Uma, and C. Valliyammai, "Security issues and challenges in cloud," in 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), Chennai, India, 2013, pp. 889-893, doi: 10.1109/ICGCE.2013.6823560.
16) D. Muthu, "Security Issues and Challenges in Cloud Computing," Journal of emerging technologies and innovative research, vol. 4, no. 11, pp. 38-40, 2017.
17) P. Patil, "Cloud Security Issues," Journal of Information Engineering and Applications, vol. 5, no. 1, pp. 31-34, 2015.
18) S. O. Kuyoro, F. L. Ibikunle, and O. Awodele, "Cloud computing security issues and challenges," International Journal for Advance Research and Development, vol. 3, pp. 24-26, 2011.
19) R. Kumar, "Cloud computing and security issue," International Journal of Engineering and Computer Science, 2016.
20) S. Ghosh, S. K. Verma, U. Ghosh, and M. S. Al-Numay, "Improved End-to-End Data Security Approach for Cloud Computing," Sustainability, 2023.
21) F. Qazi, "Application Programming Interface (API) Security in Cloud Applications," EAI Endorsed Transactions on Cloud Systems, 2023.
22) A. Sirisha and G. G. Kumari, "API access control in cloud using the Role Based Access Control Model," Trendz in Information Sciences & Computing(TISC2010), pp. 135-137, 2010.
23) G. Joe-Ibekwe, "Enhancing Cloud Security By Using Secure APIs In Business Enterprises In The USA," International Journal of Scientific and Research Publications, 2024.
24) M. Ali, L. T. Jung, A. H. Sodhro, A. A. Laghari, S. B. Belhaouari, and Z. Gillani, "A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security," Alexandria Engineering Journal, vol. 64, pp. 749-760, 2023.
25) C. Surianarayanan and P. R. Chelliah, "Integration of the internet of things and cloud: Security challenges and solutions–a review," International Journal of Cloud Applications and Computing (IJCAC), vol. 13, no. 1, pp. 1-30, 2023.
26) R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud computing: security issues and research challenges," International Journal of Computer Science and Information Technology & Security (IJCSITS), vol. 1, no. 2, pp. 136-146, 2011.
27) I. M. Khalil, A. Khreishah, and M. Azeem, "Cloud computing security: A survey," Computers, vol. 3, no. 1, pp. 1-35, 2014.
28) R. Kalaiprasath, R. Elankavi, and R. Udayakumar, "Cloud security and compliance-a semantic approach in end to end security," International Journal on Smart Sensing and Intelligent Systems, vol. 10, no. 5, pp. 482-494, 2017.
29) N. M. Almutairy, K. H. A. Al-Shqeerat, and H. A. Al Hamad, "A Taxonomy of Virtualization Security Issues in Cloud Computing Environments," Indian Journal of Science and Technology, 2019.
30) N. Kumari, "A Study of Hypervisor Based Virtualization and Related Major Security Issues in Cloud Computing Architecture," International Journal for Research in Applied Science and Engineering Technology, 2023.

31) M. B. Qureshi, M. S. Qureshi, S. Tahir, A. Anwar, S. Hussain, M. Uddin, and C.-L. Chen, "Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud," Symmetry, vol. 14, p. 695, 2022.
32) Dr.T. Chandrasekhar and S. Kumar, "A Novel Method for Cloud Security and Privacy Using Homomorphic Encryption Based on Facial Key Templates," Journal of Advances in Information Technology, 2022.
33) S. C. Patel, S. K. Jaiswal, R. S. Singh, and J. Chauhan, "Access Control Framework Using Multi-Factor Authentication in Cloud Computing," Int. J. Green Comput., vol. 9, pp. 1-15, 2018.
34) E. Tuyishime, T. C. Balan, P. A. Cotfas, D. T. Cotfas, and A. Rekeraho, "Enhancing Cloud Security—Proactive Threat Monitoring and Detection Using a SIEM-Based Approach," Applied Sciences, 2023.
35) A. Ravuri et al., "Evaluation of Cloud-Based Cyber Security System," International Journal on Recent and Innovation Trends in Computing and Communication, 2023.
36) J. Shropshire and R. Benton, "Container and VM Visualization for Rapid Incident Response," 2019.
37) N. Krishnamurthy et al., "Exploring the Cloud: Vulnerabilities and Cybersecurity Challenges," International Journal on Recent and Innovation Trends in Computing and Communication, 2023.
38) A. Polozhentsev, S. Gnatyuk, R. Berdibayev, V. Sydorenko, and O. Zhyharevych, "Novel Cyber Incident Management System for 5G-based Critical Infrastructures," in 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 1, pp. 1037-1041, 2023.
39) E. B. Fernández, N. Yoshioka, and H. Washizaki, "Cloud Access Security Broker (CASB): A pattern for secure access to cloud services," 2015.
40) https://peoplactive.com/blog/cryptography-in-cloud-computing/
41) https://www.bmc.com/blogs/containers-vs-virtual-machines/
42) https://secureops.com/blog/casb-and-dlp/\


## ABOUT THE AUTHORS

**Vaishnavi Chaudhari**, student, Department. of Computer science and Application, Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India

**Poonam Dhake**, Student, Department. of Computer science and Application, Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India

**Snehal Salunkhe**, student, Department. of Computer science and Application, Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India

**Dr. Mahendra Suryavanshi** completed his Ph.D in Computer Science from Savitribai Phule Pune University, Pune (Maharashtra), India in 2021. He did his master's in Computer Science from Savitribai Phule Pune University, India in 2010. He is currently working as an Assistant Professor with Dr. Vishwanath Karad MIT World Peace University, Pune (Maharashtra), India. He has more than 13 years of teaching experience. His research interest includes Cloud Computing, Data Center Networking, Data Structures and Algorithm Design.