International Journal of Core Engineering & Management
Volume-7, Issue-11, 2024 ISSN No: 2348-9510

ENHANCING PERFORMANCE AND SECURITY IN MULTI-CLOUD AND HYBRID-CLOUD ENVIRONMENTS

Venkata Baladari
Senior Software Developer, CGI Inc.
vrssp.baladari@gmail.com
Newark, Delaware

Abstract

Cloud computing is becoming more sophisticated, with companies increasingly adopting multi-cloud and hybrid cloud systems to improve flexibility, scalability, and disaster recovery capabilities. The shift in this direction poses new security, interoperability, and management challenges that need to be resolved to guarantee a secure and efficient functioning of cloud environments.

This study delves into the future of cloud computing by investigating significant trends, obstacles, and resolutions connected to multi-cloud and hybrid cloud implementations. Key areas of focus examine effective methods for effortless cloud integration, encompassing multi-cloud orchestration, secure application relocation, and cloud-specific security measures. It incorporates real-world examples and comparisons of key cloud service providers (AWS, Microsoft Azure, and Google Cloud) to demonstrate best practices and valuable insights. Findings from this research adds to the expanding domain of cloud security and infrastructure management by suggesting a strategic framework for the future of multi-cloud and hybrid cloud settings. The study's results are designed to assist companies, cloud designers, and cybersecurity specialists in navigating the changing cloud environment while ensuring security, compliance, and operational effectiveness.

Index Terms – Multi-Cloud, Hybrid Cloud, Cloud Security, Cloud Environments, Zero Trust Architecture, Cloud Adoption

I. INTRODUCTION

The adoption of Cloud computing has significantly altered the manner in which businesses and organizations oversee their IT infrastructure, providing unmatched scalability, adaptability, and cost-effectiveness. Cloud adoption is increasing, causing enterprises to transition from conventional single-cloud models to more intricate multi-cloud and hybrid cloud systems. These models facilitate organizations in utilizing multiple cloud service providers (AWS, Microsoft Azure, Google Cloud, etc.) alongside maintaining on-site infrastructure, thereby enhancing performance, redundancy, and regulatory adherence [1],[2].

This transition also brings forth substantial difficulties in the realms of security, interoperability, governance, and workload management. Organizations operating in multi-cloud environments must contend with disparities in security protocols, application programming interfaces, and regulatory compliance across various cloud services. Hybrid cloud setups that combine in-house infrastructure with public and private cloud services create extra challenges for data synchronization, secure network connections, and workload management. As a consequence, businesses need to implement strategic frameworks, automated security controls, and cloud-based solutions in order to efficiently manage these environments.

This study seeks to examine the future of cloud computing, focusing on the major trends, issues, and developments influencing the adoption of multi-cloud and hybrid cloud environments additionally explores these significant areas in-depth.

- Security concerns encompass issues such as data fragmentation, cloud misconfigurations, and the vulnerabilities associated with shared responsibility models.
- Ensuring seamless workload portability across various cloud environments through effective interoperability and integration.
- The emphasis is on cloud automation and AI-driven management, where artificial intelligence and machine learning (AI/ML) are shown to improve cloud operations and security [1],[2].
- Issues with compliance and regulation are prevalent in sectors that handle sensitive information and conduct cross-border cloud services.

This paper offers a strategic plan for businesses, cloud designers, and cybersecurity experts to guide them through the changing environment of cloud computing. The objective is to pinpoint top-performing strategies, forward-thinking solutions, and emerging trends that will boost the efficiency, security, and sustainability of both multi-cloud and hybrid cloud implementations.

II. OVERVIEW OF MULTI-CLOUD AND HYBRID CLOUD ENVIRONMENTS

Cloud computing has transformed the landscape of IT infrastructure by offering organizations on-demand access to resources, the ability to scale as needed, and reduced costs. As companies aim to maximize their cloud plans, a significant number are moving from a single-cloud approach to multi-cloud and hybrid cloud systems to boost resilience, flexibility, and adherence to regulations. This section offers a detailed summary of multi-cloud and hybrid cloud settings, including their differences, advantages, difficulties, and practical applications.

A. Key Characteristics of Multi-Cloud and Hybrid Cloud

- **Multi-Cloud Environment**
  Implementing a multi-cloud approach involves leveraging two or more cloud computing platforms (such as AWS, Microsoft Azure, Google Cloud, IBM Cloud) to spread workloads, ensure higher system uptime, and decrease reliance on a single cloud vendor[1],[2][3]. This method allows companies to utilize top-tier services from various suppliers, while simultaneously reducing costs and improving efficiency.
- **Hybrid Cloud Environment**
  A hybrid cloud setup combines on-site data centres (private cloud) with one or more external public cloud services. This architecture allows businesses to run critical workloads securely on internal systems, while also taking advantage of the scalability and cost benefits of the public cloud for non-core operations [2][3].

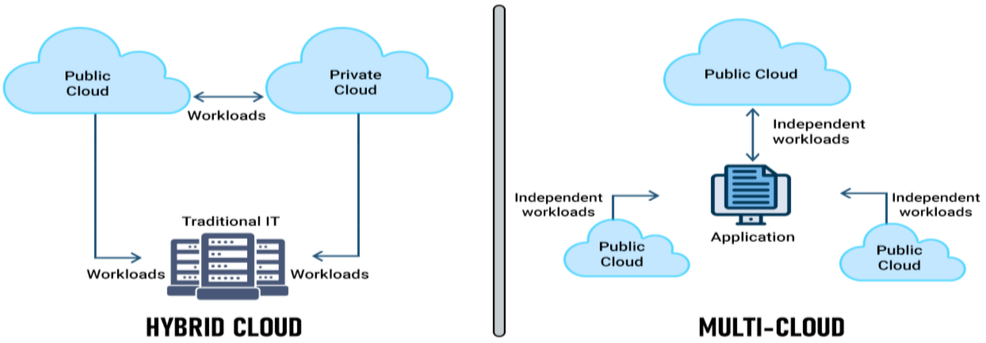

Fig. 1. Hybrid cloud and multi-cloud

B. Advantages of Multi-Cloud and Hybrid Cloud Adoption

1. **Flexibility**
   Selecting multiple cloud service providers enables companies to minimize reliance on a single supplier, thereby permitting them to pick the most suitable services for their particular requirements.
2. **Reliability**
   Distributing workloads across multiple cloud environments through multi-cloud and hybrid cloud strategies improves resilience by minimizing the risk of downtime caused by provider outages.
3. **Cost Optimization**
   Businesses can select cost-efficient cloud solutions based on their workload requirements, thereby controlling expenses and adjusting the level of performance across both public and private cloud platforms.
4. **Security**
   Private data can be stored in a private cloud or on-site infrastructure while utilizing public clouds for scalability purposes, thereby ensuring adherence to regulatory standards such as GDPR, HIPAA, and SOC 2 [4].
5. **Scalability**
   Companies can adaptively adjust the amount of work their systems handle by moving it between various cloud platforms, selecting the cloud environment that is most suitable for each task based on considerations such as response time, data protection, and expenses.

C. Disadvantages of Multi-Cloud and Hybrid Cloud Adoption

1. **Increased Complexity**
   Maintaining multiple cloud providers or combining private and public clouds necessitates additional expertise, tools, and procedures. Streamlining communication across various platforms can be a complicated and labour-intensive process.
2. **Security Risks**
   Cloud providers have distinct security policies, controls, and compliance regulations. Managing security across numerous environments heightens the risk of misconfigurations, weaknesses, and possible non-compliance breaches.
3. **Higher Costs**
   Using cloud services can be an economical option, but running applications across multiple

cloud platforms may result in increased expenditures due to data transfer charges, licensing fees, and the extra tools needed for overseeing and managing the infrastructure.

4. **Performance**
   Applications requiring communication between various cloud environments may experience elevated latency, resulting in decreased performance. Maintaining seamless communication and data transfer across multiple cloud systems can be a complex task.
5. **Integration Challenges**
   Cloud providers deliver distinctive services, application programming interfaces, and pricing structures. Integrating various platforms seamlessly and preventing reliance on a single vendor while ensuring data sharing capabilities can be complex and necessitate advanced technical knowledge.

III. EMERGING THREATS IN MULTI-CLOUD AND HYBRID CLOUD SECURITY

A. Misconfigurations and Inconsistent Security Policies

1. **Threat Explanation**
   a) Configuring cloud environments such as multi-cloud and hybrid cloud necessitates setting security parameters across various platforms, each with its own distinct tools and protocols.
   b) Misconfigurations such as open storage buckets, weak authentication methods, exposed public databases, and default security settings not altered are commonly encountered issues.
   c) Organizations experience security inconsistencies when they do not implement uniform security policies across multiple cloud providers, resulting in policy drift and expanded vulnerabilities to cyber attacks.
2. **Example Attack Scenario**
   a) Sensitive customer data stored in a cloud storage bucket is inadvertently exposed to the public due to incorrect configuration settings.
   b) Exploitation of this vulnerability results in a data breach impacting a substantial number of users, reportedly in the thousands.
3. **Mitigation Strategies**
   a) Put in place Cloud Security Posture Management (CSPM) solutions to consistently monitor and rectify system misconfigurations [5].
   b) Implement automated security protocols and utilize infrastructure-as-code (IaC) to ensure uniform settings across multiple cloud platforms [6].
   c) It is essential to conduct routine security audits and penetration testing in order to discover and rectify vulnerabilities prior to their being exploited by attackers.

B. Identity and Access Management (IAM) Complexities

1. **Threat Explanation**
   a) Controlling multiple user identities, roles, and access permissions within a combination of cloud environments is often a challenging and error-sensitive task.
   b) Organizations frequently fail to implement the principle of least privilege access, resulting in excessive permissions that attackers can take advantage of.
   c) Cloud environments are vulnerable to issues such as insufficient session timeouts, the

absence of multi-factor authentication (MFA), and the implementation of weak password policies [7].

2. **Example Attack Scenario**

a) An individual with extensive privileges to critical cloud systems is the victim of a phishing attack.

b) The attacker uses the compromised account to steal sensitive information and carry out additional malicious activities.

3. **Mitigation Strategies**

a) Implement a Zero Trust Architecture (ZTA) that necessitates ongoing identity authentication prior to granting access[8].

b) Implement two-factor authentication (2FA) or multi-factor authentication(MFA) across all cloud-based services [7].

c) It is essential to conduct periodic reviews of user permissions and remove any privileges that are not required.

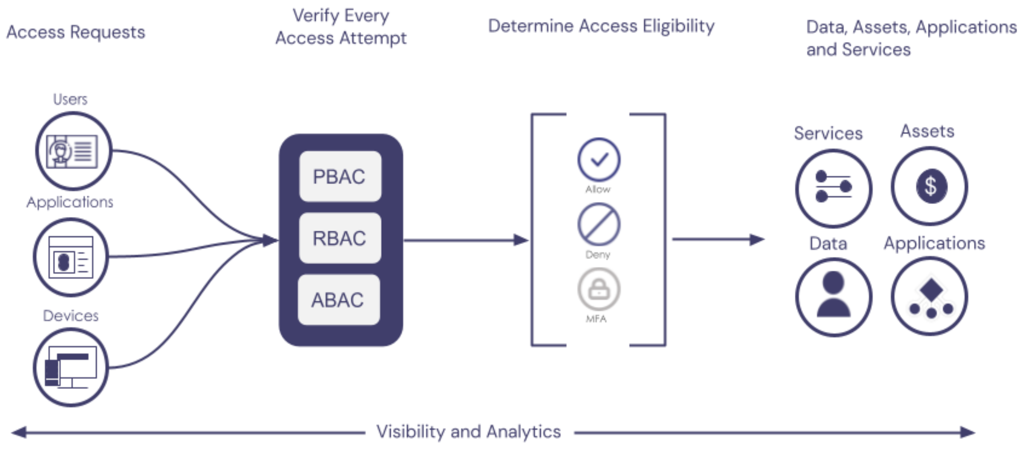

Fig. 2. Zero-Trust Architecture

C. Third-Party Vulnerabilities

1. **Threat Explanation**

a) Cloud environments frequently depend on third-party integrations, managed services, and application programming interfaces, which can bring about supply chain vulnerabilities.

b) A compromised third-party supplier can serve as an entry point for hackers to breach numerous companies using the same service.

c) Cyber attackers often focus on infiltrating the software supply chains of cloud-based applications, by embedding malicious code into the dependencies these programs utilize.

2. **Example Attack Scenario**

a) A cloud service provider utilized by several corporations was breached via an unpatched zero-day flaw.

b) Attackers exploit a single vulnerable entry point to breach secure systems and conduct large-scale cyber assaults.

3. **Mitigation Strategies**

a) On an ongoing basis, evaluate and authenticate third-party service providers to ensure adherence to the most secure practices.

b) Implement a Software Bill of Materials (SBOM) to monitor dependencies and counteract potential risks in the software supply chain.

c) Implement least privilege access controls for third-party integrations and continuously monitor their actions.

d) It is essential to keep third-party services and software dependencies up-to-date and patched regularly.

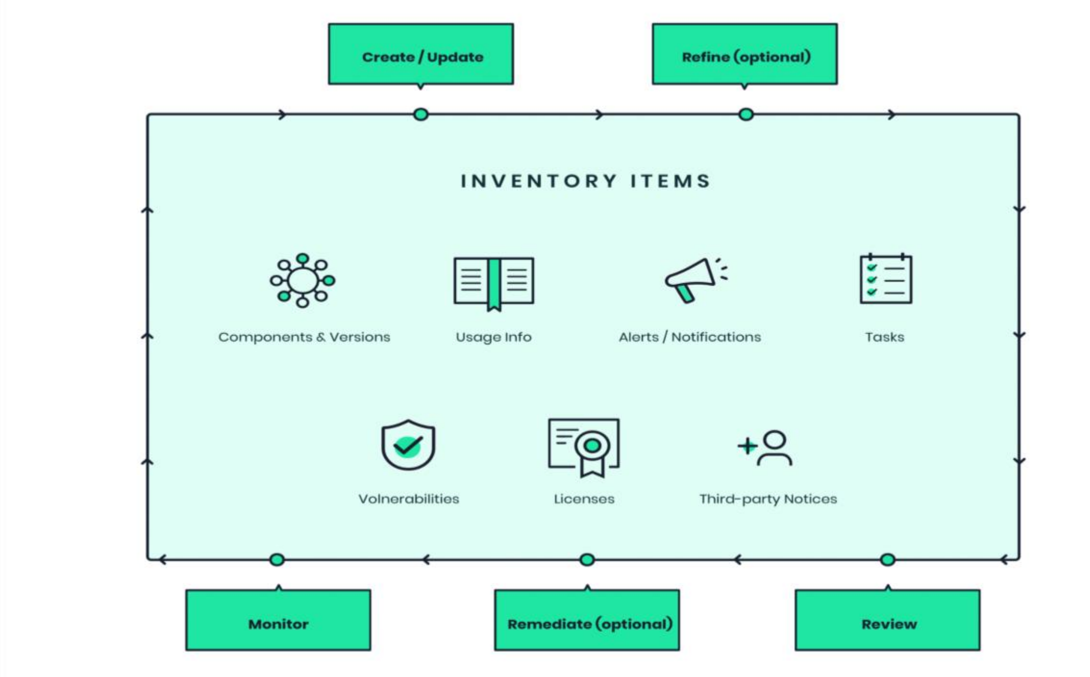

Fig. 3. Software Bill of Materials Lifecycle

D. Compliance Risks and Data Fragmentation

1. **Threat Explanation**

a) Data is frequently dispersed across various cloud providers and on-site systems, rendering it challenging to implement uniform security protocols and adhere to regulatory requirements.

b) Varying levels of encryption, access controls, and data residency policies among different cloud providers are causing compliance issues.

c) Entities governed by regulations such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and California Consumer Privacy Act (CCPA) are required to maintain uniform data safeguarding across all relevant settings [4].

2. **Example Attack Scenario**

a) Patient data is being stored by a healthcare organization across various cloud-based systems.

b) Encryption protocols are not uniformly applied, certain data is left unsecured, thereby allowing unauthorized parties to obtain and potentially pilfer confidential data.

c) The organization is at risk of incurring substantial penalties as a result of its failure to adhere to the requirements of the HIPAA regulations.

3. Mitigation Strategies

a) Implement a consistent data security and compliance framework across all cloud-based services.

b) Provide cloud-native encryption and ensure that data is encrypted on both its journey through the internet and while it is stored.

c) Implement Data Loss Prevention (DLP) solutions to track and block unauthorized data transfers.

d) Conduct audits on a regular basis to ensure compliance and perform data classification evaluations.

E. Advanced Persistent Threats (APTs) and Ransomware

1. Threat Explanation

a) Sophisticated cybercrime groups are increasingly targeting cloud environments with advanced persistent threats (APTs) and ransomware attacks [9],[10].

b) Advanced Persistent Threats (APT) attacks involve prolonged, clandestine operations where adversaries sustain continuous access to cloud environments, gradually extracting sensitive information over a period of time.

c) Ransomware groups encrypt cloud-based storage systems and then demand payment in exchange for restoring access, resulting in significant financial and operational harm.relevant settings [9].

2. Example Attack Scenario

a) An attacker obtains unauthorized access to a company's cloud management interface through compromised login information.

b) The attacker releases ransomware, which encrypts cloud-based workloads and backup files.

c) The organization is compelled to pay a ransom to regain access to vital information.

3. Mitigation Strategies

a) Implement read-only backup systems to safeguard against ransomware encryption attacks.

b) Ensure that cloud management consoles adhere to the principle of least privilege access, and implement logging for all administrative tasks.

c) Utilize behavioral analytics to identify anomalies and potential Advanced Persistent Threat (APT) activities.

IV. REGULATORY AND COMPLIANCE CHALLENGES

A. Diverse Regulatory Frameworks

- Businesses using various cloud platforms, including both multi-cloud and hybrid cloud systems, frequently must adhere to multiple regulatory guidelines, each with specific security and confidentiality stipulations.
- In Europe, regulations like the GDPR stress the importance of safeguarding data and user confidentiality, mandating that businesses verify that their data handling practices are legitimate and that users have given their consent.
- In the United States, HIPAA necessitates rigorous security protocols for healthcare information, encompassing encryption and restricted access.
- CCPA ensures that consumers have certain data rights and mandates strict compliance with reporting regulations [11].
- The Payment Card Industry Data Security Standard (PCI-DSS) enforces strict security requirements for the handling of payment card information [12].
- Developing and implementing a comprehensive governance framework and robust cloud security protocols is essential for managing compliance across diverse regulatory environments.

B. Data Sovereignty and Residency

- Data sovereignty regulations stipulate that data must be stored and processed within predetermined geographical limits. Countries like China, Russia, Canada, and Germany have strict laws controlling data storage locations.
- Companies employing multi-cloud systems may unintentionally move data across international boundaries, resulting in possible regulatory infractions.
- Global data centers operated by cloud providers necessitate organizations to verify that their data storage locations conform to relevant regulatory standards.
- To overcome this challenge, companies need to implement geo-fencing techniques to manage where their data is stored and ensure that contracts with cloud providers outline necessary compliance specifications.

C. Consistency in Security Controls

- Cloud providers, such as AWS, Azure, and Google Cloud, each utilize their own individual security models, access control systems, and compliance tools, which complicates the task of implementing uniform security policies across all systems.
- In a cloud environment, a security misconfiguration can result in sensitive data being exposed and potentially trigger non-compliance issues.
- Deploying Cloud Security Posture Management (CSPM) solutions enables continuous monitoring of security configurations and ensures consistent security policy enforcement[5].
- Cloud-based companies should implement a Zero Trust Architecture (ZTA) to ensure rigorous access restrictions and ongoing surveillance across all cloud-based systems [8].
- Implementing Infrastructure as Code (IaC) and policy-as-code frameworks can facilitate consistent enforcement of security controls.

D. Audit and Monitoring Complexities

- Effective security incident response necessitates ongoing monitoring, record-keeping, and review processes to identify and address potential security breaches in a timely manner.
- In multi-cloud and hybrid settings, log data is produced across various cloud providers, hindering the ability to correlate security occurrences and verify real-time threat identification.
- Organizations are mandated by regulations like GDPR and HIPAA to keep thorough audit logs and be capable of furnishing audit trails during probes.
- Cloud providers offer various audit logging services at different levels (e.g., AWS CloudTrail, Azure Monitor, Google Cloud Logging), complicating the task of centralizing security visibility [1],[2].

E. Third-Party Risk Management

- Multi-cloud and hybrid cloud setups commonly engage the services of external companies like cloud hosting firms, software as a service applications, and managed security solution providers.
- Cloud providers must adhere to the regulations and security standards that their organizations are required to uphold.
- A security breach or non-compliance by the cloud vendor can negatively affect an organization's compliance position and result in legal repercussions.
- Establishing Service-Level Agreements (SLAs) that outline security and compliance requirements for third-party vendors can assist in reducing the risks involved with outsourcing[13].

V. SECURITY STRATEGIES AND BEST PRACTICES

A. Implement a Unified Security Framework

Multi-cloud and hybrid cloud environments having multiple cloud service providers, each with unique security controls and specific compliance requirements. In order to guarantee a secure and consistent method, enterprises should:

- Implement and enforce a single security policy across all cloud-based platforms.
- Implement cloud-agnostic security solutions to standardize and streamline threat detection, encryption, and access control protocols.
- Maintaining a robust security stance requires adherence to established industry standards, including NIST, CIS, ISO 27001, and SOC 2 guidelines [14].

B. Zero Trust Architecture (ZTA) Adoption

Under a Zero Trust Security model, all users and systems are initially deemed untrusted, necessitating ongoing verification before authorizing access to resources. Key elements of Zero Trust architecture in cloud security comprise:

- Least Privilege Access (LPA): Assign the least amount of access necessary to users and applications in order to accomplish their tasks [15].
- Multi-Factor Authentication (MFA): Implement multi-factor authentication for all high-priority cloud accounts and access to confidential data [7].
- Micro-Segmentation: Breaking down cloud networks into separate sections can help limit

the spread of potential threats.

- Continuous Monitoring and Adaptive Authentication: Employ real-time analytics and AI-driven monitoring to adapt access permissions dynamically in accordance with identified risk levels.

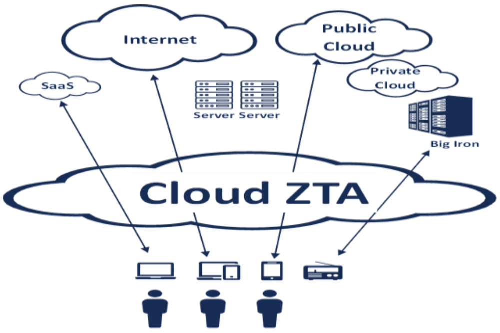

Fig. 4. ZTA Cloud

C. Robust Data Protection Measures

Protecting data is a top priority in both multi-cloud and hybrid cloud settings. In order to prevent and reduce the impact of data breaches and unauthorized access:

- Encrypt Data at Rest and in Transit: For stored data, use AES-256 encryption, and for data transmission, use TLS/SSL encryption[16].
- Implement Data Loss Prevention (DLP): To stop unauthorized access or proliferation of sensitive information.
- Backup and Disaster Recovery Planning: Keep secure backup copies of data encrypted, stored in multiple sites, and conduct regular tests of disaster recovery procedures.
- Secure Key Management: Store and manage encryption keys securely by utilizing cloud-native or third-party Key Management Systems (KMS) [4][9].

D. Continuous Security Monitoring and Threat Detection

For cloud workloads dispersed across various environments, real-time security surveillance is crucial to identify and respond to threats quickly. Industry guidelines encompass a range of standards:

- Implement and enforce a single security policy across all cloud-based platforms.
- Implement cloud-agnostic security solutions to standardize and streamline threat detection, encryption, and access control protocols.
- Maintaining a robust security stance requires adherence to established industry standards, including NIST, CIS, ISO 27001, and SOC 2 guidelines[14].

E. Implement a Unified Security Framework

Multi-cloud and hybrid cloud environments having multiple cloud service providers, each with unique security controls and specific compliance requirements. In order to guarantee a secure and consistent method, enterprises should:

- Deploy Security Information and Event Management (SIEM): Real-time threat detection is facilitated by SIEM tools, which collect logs from various cloud environments simultaneously[17].

- Implement Cloud Security Posture Management (CSPM): CSPM tools assist in detecting misconfigured settings, ensuring regulatory adherence, and immediately addressing security vulnerabilities[5].
- Use Extended Detection and Response (XDR): XDR solutions deliver comprehensive security intelligence across multiple layers, encompassing cloud-based workloads, end-point devices, and network infrastructure[18].
- Leverage AI and Machine Learning: Proactive measures can be taken to counter potential threats by using artificial intelligence to detect and prevent malicious activities before they occur.

VI. FUTURE TRENDS IN CLOUD SECURITY

A. Advanced AI-Driven Threat Detection System

Cloud security is being revolutionized by artificial intelligence (AI) and machine learning (ML) capabilities that automate threat identification and reaction processes. Artificial intelligence algorithms examine large quantities of security information to detect patterns, irregularities, and possible cyber threats in real-time.

B. Post-Quantum Cryptography for Cloud Security

Quantum computing is poised to undermine the security of existing encryption methods such as RSA and ECC, prompting the development of post-quantum cryptography - a new class of cryptographic algorithms designed to be immune to quantum-based attacks.

C. Blockchain Technology for Enhanced Cloud Security and Identity Authentication

Blockchain technology offers improved cloud security through tamper-proof identity management and data integrity protocols.

D. Implementing Secure Environments for Enhanced Data Protection.

Confidential computing uses hardware-based Trusted Execution Environments (TEE) to encrypt data throughout the processing stage. This provides robust protection against unauthorized access from cloud providers, administrators, and attackers, thereby enhancing privacy and regulatory compliance in both multi-cloud and hybrid cloud environments[19].

E. Privacy-Enhancing Technologies (PETs)

As data protection laws become more stringent, companies are turning to Privacy-Enhancing Technologies (PETs), such as homomorphic encryption, secure multi-party computation (SMPC), and differential privacy, to safeguard confidential information while allowing secure data analysis and co-operation within cloud environments [20].

VII. LIMITATIONS AND CHALLENGES

- Inconsistent resource distribution across multiple cloud providers results in latency problems, data transfer congestion, and difficulties in achieving seamless scalability.

- Unified security strategies and data privacy management are complicated by diverse security protocols, growing attack surfaces, and specific regulatory compliance demands in different regions, such as those outlined in GDPR and HIPAA.
- Platform incompatibility, inadequate centralized monitoring, and complex incident responses, coupled with unpredictable cost structures, are key challenges that undermine operational efficiency and exacerbate management complexity.

VIII. CONCLUSION

Adoption of multi-cloud and hybrid cloud models, businesses must take proactive measures to counter escalating security risks. Implementing comprehensive security frameworks, adopting industry-recognized standards, and utilizing cutting-edge security technologies will assist in minimizing threats and protecting cloud resources. Ongoing monitoring, strict compliance adherence, and automated security will be essential for sustaining a robust security position within a dynamic cloud environment.

REFERENCES

1. Golightly L, Chang V, Xu QA, Gao X, Liu BS. Adoption of cloud computing as innovation in the organization. International Journal of Engineering Business Management. 2022.
2. B. Liu, "Artificial Intelligence and Machine Learning Capabilities and Application Programming Interfaces at Amazon, Google, and Microsoft," M.S. thesis, Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA, USA, 2022.
3. Alonso, J., Orue-Echevarria, L., Casola, V. et al. Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review. J Cloud Comp 12, 6 (2023).
4. "SOC Reports for Cloud Security and Privacy," ISACA Journal, vol. 6, 2019.
5. M. F. Bulut and J. Hwang, "NL2Vul: Natural Language to Standard Vulnerability Score for Cloud Security Posture Management," 2021 IEEE 14th International Conference on Cloud Computing (CLOUD), Chicago, IL, USA, 2021
6. A. Rahman, R. Mahdavi-Hezaveh, and L. Williams, "A systematic mapping study of infrastructure as code research," Information and Software Technology, vol. 108, pp. 1-21, 2019.
7. Mostafa AM, Ezz M, Elbashir MK, Alruily M, Hamouda E, Alsarhani M, Said W. Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. Applied Sciences. 2023
8. Sarkar S, Choudhary G, Shandilya SK, Hussain A, Kim H. Security of Zero Trust Networks in Cloud Computing: A Comparative Review. Sustainability. 2022
9. A R, Kautish S, Juneja S, Mohiuddin K, Karim FK, Elmannai H, Ghorashi S, Hamid Y. Enhanced Cloud Storage Encryption Standard for Security in Distributed Environments. Electronics. 2023.
10. Aaron Zimba, Hongsong Chen, Zhaoshun Wang, Mumbi Chishimba, Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics, Future Generation Computer Systems, Volume 106, 2020.

11. Mishra A, Jabar TS, Alzoubi YI, Mishra KN. Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework. Concurrency Computat Pract Exper. 2023.
12. E. A. Morse and V. Raval, "PCI DSS: Payment card industry data security standards in context," Computer Law & Security Review, vol. 24, no. 6, pp. 540-554, 2008.
13. Nadeem S, Amin Nu, Zaman SKu, Khan MA, Ahmad Z, Iqbal J, Khan A, Algarni AD, Elmannai H. Runtime Management of Service Level Agreements through Proactive Resource Provisioning for a Cloud Environment. Electronics. 2023;
14. Barraza de la Paz JV, Rodríguez-Picón LA, Morales-Rocha V, Torres-Argüelles SV. A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. Systems. 2023;
15. S. Deochake, V. Channapattan, and G. Steelman, "BigBird: Big Data Storage and Analytics at Scale in Hybrid Cloud," arXiv preprint, arXiv:2203.11472, 2022.
16. P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," Internet of Things, vol. 19, 2022.
17. González-Granadillo G, González-Zarzosa S, Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors. 2021.
18. M. A. Islam, "Application of artificial intelligence and machine learning in a security operations center," Proceedings of the Information and Information Systems (IIS) Conference, 2023.
19. Y. Liu, S. Dhar, and E. Tilevich, "Only pay for what you need: Detecting and removing unnecessary TEE-based code," Journal of Systems and Software, vol. 188, 2022.
20. N. Kaaniche, M. Laurent, and S. Belguith, "Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey," Journal of Network and Computer Applications, vol. 171, 2020.