Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2022, 9(5):106-114

Research Article ISSN: 2394 - 658X

Developing a Unified Security Framework for the Establishment of Secure and Resilient Multi-Cloud Infrastructures

Arun Pandiyan Perumal

Graduate Student, Illinois Institute of Technology, USA
arun4pap@gmail.com

ABSTRACT

The advent of cloud computing has revolutionized the landscape of information technology infrastructure, offering unprecedented scalable, efficient, and flexible infrastructure resources. Multi-cloud infrastructures, involving the orchestrated use of services from multiple cloud providers, have emerged in response to diverse organizational needs, including enhanced resilience, risk management, and access to specific capabilities. However, the complexity and heterogeneity of multi-cloud environments pose significant security challenges, necessitating robust and resilient security mechanisms to protect sensitive data and maintain system integrity. This study aims to address these challenges through the development of a unified security framework designed to enhance the security and resilience of multi-cloud environments, motivated by the growing reliance on multi-cloud setups and the surge in targeted security threats. To develop the proposed unified security framework, the methodology encompasses the identification of key security principles, analysis of existing security solutions, standards, and protocols, and the integration of best practices in cloud security. The proposed security framework comprises critical components such as a unified security control plane, identity and access management, data protection and privacy, network security and segmentation, threat detection and response, and compliance and audit. The study's findings highlight the framework's significant impact in addressing the challenges faced by multi-cloud infrastructures, demonstrating its interoperability and efficacy in improving security measures, reducing vulnerabilities, and enhancing overall resilience. The practical implications of this study are profound, offering a pathway to more secure and efficient operations for organizations seeking to secure their multi- cloud infrastructures. The development and implementation of this unified security framework represents a major stride towards securing multi-cloud infrastructures, reinforcing the need for continuous innovation in cloud security practices.

Key words: Multi-cloud infrastructures, Cloud Security, Security Framework, Data Protection, System Integrity, Compliance and Governance, Cloud Service Providers (CSP).

INTRODUCTION

In the ever-evolving landscape of digital transformation, cloud computing has emerged as a cornerstone, enabling organizations to harness the power of scalable computing resources, storage, and applications over the internet. It facilitates on-demand access to a shared pool of configurable computing resources, which can be rapidly provisioned with minimal management effort or service- provider interaction [1][2]. As businesses strive to remain competitive and agile, the adoption of cloud technologies continues to accelerate, fundamentally transforming the way organizations operate and deliver services. Amidst this cloud-centric transformation, a significant shift has been observed from single-cloud deployments to sophisticated multi-cloud environments. With multi-cloud infrastructures, organizations aim to mitigate risks, enhance operational performance, and achieve cost efficiency through strategic deployment across multiple cloud service providers (CSP) [16].

Securing multi-cloud environments presents a complex challenge, exacerbated by their distributed nature, the diversity of technologies and architectures involved, and the varying security policies and practices across

different CSPs [3]. This complexity is compounded by the absence of a standardized approach to security in multi-cloud infrastructures, leading to potential inconsistencies and gaps in security postures and an increased vulnerability to cyber-attacks. Common challenges and vulnerabilities in these environments include misconfigurations, inadequate identity and access management, data breaches, and advanced persistent threats, necessitating the critical need for enhanced security measures.

Ensuring the protection of data, applications, and infrastructures from cyber threats while maintaining operational continuity is essential for maintaining business operations and safeguarding sensitive information. The primary objective of this study is to propose a comprehensive and unified security framework encompassing core components, best security practices, and technologies that are explicitly tailored for multi-cloud infrastructures. The framework focuses on interoperability, scalability, and adaptability, aiming to enhance the security posture and resilience of multi-cloud environments against emerging threats.

The development of the unified security framework involves a meticulous methodology, incorporating the identification of key security principles and analysis of existing security solutions, standards, and protocols. By integrating established best practices in cloud security, the study delineates critical components of the proposed security framework, including a unified security control plane, identity and access management, data protection and privacy, network security and segmentation, threat detection and response, and compliance and audit. This study holds significant implications for the field of cloud security, providing a systematic and cohesive approach to managing security risks in multi-cloud environments. This proposed framework intends to offer improved security visibility, streamlined compliance with regulatory requirements, enhanced incident response capabilities, and a robust security posture.

LITERATURE REVIEW

The adoption of multi-cloud environments has grown exponentially, driven by the need for businesses to leverage the unique offerings of different cloud providers, achieve cost efficiency, enhance performance, and ensure business continuity through geographical diversity. The strategic deployment of multi-cloud infrastructures leverages the strengths of various cloud services, optimizing business operations and fostering innovation. Security and resilience are paramount in multi-cloud infrastructures due to the increased attack surface and the complexity of managing disparate systems with potentially inconsistent security controls [4]. The importance of vigorous security measures is underscored by the critical need to protect sensitive data, maintain service availability, and ensure regulatory compliance across jurisdictions [9]. Multi-cloud environments face several unique security challenges and threats, including:

A. Data Security and Privacy:

The dispersion of data across multiple jurisdictions complicates compliance with data protection regulations, posing significant risks to data privacy and sovereignty.

B. Intricate Identity and Access Management (IAM):

Ensuring secure and efficient access management across disparate cloud platforms is a formidable challenge, as compromised credentials can lead to unauthorized access.

C. Interoperability and Compatibility Issues:

The seamless integration of services and platforms from multiple cloud service providers introduces compatibility and interoperability issues, posing risks to data integrity and potentially creating security vulnerabilities [5].

D. Advanced Persistent Threats (APTs) and Multi-Vector Attacks:

Multi-cloud environments can be targeted by advanced persistent threats (APTs) and multi-vector attacks that use sophisticated techniques to infiltrate systems and remain undetected for extended periods.

E. Misconfigurations:

The complexity and diversity of multi-cloud environments increase the risk of misconfigurations, which are a leading cause of cloud security breaches. Misconfigured cloud storage permissions, improper management of encryption keys, and inadequate network access controls are common known vulnerabilities.

F. Visibility and Monitoring:

Achieving comprehensive visibility and monitoring across all cloud environments is complex, making it challenging to detect and respond to security incidents promptly.

Several security frameworks and strategies have been developed to enhance the security and resilience of cloud environments. The Cloud Security Alliance (CSA) provides comprehensive guidance on cloud security best practices, while the National Institute of Standards and Technology (NIST) offers a detailed cloud computing security reference architecture [9]. However, these frameworks often lack the specificity required to address the unique challenges of multi-cloud environments, resulting in gaps in security coverage. Current security frameworks and models exhibit significant limitations in addressing the complexities of multi-cloud infrastructures [6]. Many frameworks operate in isolation, failing to provide an integrated approach that encompasses the entirety of the multi-cloud ecosystem. The variability in the adoption and enforcement of security controls across different cloud providers leads to inconsistencies and potential security gaps [10]. Organizations often face challenges in gaining complete visibility into the security posture and controls implemented by cloud providers, complicating effective risk management and incident response. Several security incidents involving multi-cloud environments emphasize critical vulnerabilities and the need for enhanced security approaches.

The identified gaps and challenges underscore the necessity of developing a unified security framework specifically adapted to multi-cloud infrastructures. Such a framework should integrate existing best practices while addressing the unique needs of multi-cloud environments, offering a comprehensive, adaptable, and scalable solution to secure multi-cloud ecosystems against a wide range of threats. Implementing a unified security framework could improve consistency in security policy enforcement, enhance visibility and management of security threats, and ensure more efficient compliance with regulatory requirements [11]. By addressing the heterogeneity and complexity of multi-cloud environments, a unified framework can significantly reduce the attack surface and mitigate the risk of breaches, thereby enhancing the overall security and resilience of multi-cloud infrastructures.

DEVELOPMENT OF THE UNIFIED SECURITY FRAMEWORK

Framework build approach

The development of a unified security framework for multi-cloud infrastructures involves a systematic and comprehensive approach that integrates various security measures, methodologies, and technologies to safeguard resources across diverse cloud platforms [6][7]. The process involves several crucial steps, each contributing to the framework's overall effectiveness.

A. Requirements Analysis:

This initial phase involves identifying specific security requirements unique to multi-cloud environments, including data sovereignty, identity and access management, compliance with regulatory standards, etc.

B. Security Policy Development:

Based on the requirements analysis, comprehensive security policies that address identified risks and compliance obligations must be developed. These policies should cover areas such as access control, data encryption, incident response, identity management, etc.

C. Risk Assessment:

A thorough risk assessment is critical to identify potential security threats and vulnerabilities within the multi-cloud infrastructure. This involves understanding the diverse nature of services and resources deployed across multiple cloud platforms and recognizing the unique security challenges each presents.

D. Framework Design Principles:

Establishing a set of design principles is crucial for guiding the development of the security framework. These principles should embrace scalability, flexibility, interoperability, and automation, ensuring the framework can adapt to evolving threats and integrate with emerging technologies [11][12].

E. Integration and Automation Layer:

Developing an integration and automation layer is vital for ensuring seamless interoperability between different cloud platforms and automating repetitive security tasks.

F. Implementation Strategy:

Defining an implementation strategy for phased implementation of the security framework, including a selection of the right tools and techniques, pilot testing, and full-scale deployment in multi-cloud environments.

G. Continuous Monitoring and Improvement:

Enable continuous monitoring of the security framework to identify and respond to new threats and vulnerabilities. This includes regular security assessments, the refinement of security policies, and the incorporation of feedback from security incidents into future framework iterations.

Core Components of the Security Framework

The architecture of the unified security framework is conceptualized as layers of security controls and services with the following core components that adopt imperative security principles to achieve scalability, flexibility, and interoperability in multi-cloud environments [8][14].

A. Unified Security Control Plane:

The Unified Security Control Plane serves as the cornerstone of the security framework, providing centralized visibility and management across multi-cloud environments [13].

- **Cloud Access Security Brokers (CASBs)** – Providing a centralized platform using solutions like McAfee MVISION Cloud for comprehensive visibility and policy enforcement across multi-cloud environments, facilitating risk assessment and threat protection.
- **Security Orchestration, Automation, and Response (SOAR)** – Streamlining security operations with tools like Palo Alto Networks Cortex XSOAR or Siemplify SOAR by automating response actions and orchestrating security processes, reducing manual workloads and improving response times.
- **Cloud Security Posture Management (CSPM)** – Utilize solutions such as Palo Alto Networks Prisma Cloud or Check Point CloudGuard to identify misconfigurations and compliance risks, ensuring a consistent security posture across cloud platforms.
- **API-based Integration with CSPs' Native Security Tools** – Leveraging APIs for seamless integration with Cloud Service Providers (CSPs) native security tools such as AWS Security Hub, Azure Security Center, and Google Cloud Security Command Center enables real-time data exchange and interoperability.

B. Identity and Access Management (IAM):

IAM plays a crucial role in controlling who has access to what resources in the cloud. It involves authentication, authorization, and the management of roles and permissions [15].

- **Centralized Identity Governance** – Establishing a single source of truth for identity management across all cloud environments. Solutions like SailPoint IdentityIQ and Okta provide centralized identity governance, ensuring access rights are granted based on users' roles and responsibilities in an organization.
- **Multi-Factor Authentication (MFA) and Single Sign- On (SSO)** – Enhance security by requiring multiple forms of verification and simplifying access with a single set of credentials. MFA can be implemented using Duo Security or Microsoft Authenticator, and SSO capabilities can be used with tools like Okta or Microsoft Azure Active Directory.
- **Role-Based Access Control (RBAC) and Least Privilege Access** – Ensuring that users have only the permissions necessary for their role, minimizing the potential impact of compromised accounts. Enforcing RBAC and least privilege can be achieved through cloud service providers' IAM services.
- **IAM Policy Management and Best Practices** – Develop and enforce IAM policies that are consistent across multi-cloud environments, incorporating best practices for secure and efficient access management.

C. Data Protection and Privacy:

Protecting data across multiple clouds requires a comprehensive approach that ensures data confidentiality and integrity [13].

- **Data Classification and Discovery** – Identify and classify data stored across cloud environments, facilitating adequate protection and compliance measures. Tools like Varonis and Spirion help organizations discover and classify sensitive data across their environments, which is critical for effective data protection strategies.
- **Encryption Strategies for Data-at-Rest and Data-in- Transit** – Implement encryption at rest and in transit to protect data integrity and confidentiality. Various cloud-native services such as AWS KMS, Azure Key Vault, and Google Cloud KMS can be used to encrypt and protect sensitive data.

- **Data Loss Prevention (DLP)** – Monitor and control data movement to prevent unauthorized access or exfiltration. Solutions like Zscaler Cloud DLP and Digital Guardian Cloud Data Protection safeguard against data breaches by monitoring and controlling data movement.
- **Data Privacy Regulations and Compliance** – Ensuring adherence to global data protection regulations such as GDPR and CCPA to maintain privacy and regulatory compliance. Tools like Palo Alto Networks Prisma Cloud and TrustArc assist in compliance management and reporting.

D. Network Security and Segmentation:

Network security in a multi-cloud environment involves securing the data in transit and segmenting the network to contain threats.

- **Zero Trust Network Architecture** – Incorporating a zero trust approach, where trust is never assumed, and verification is required from everyone trying to access resources, significantly enhancing network security. Implementing Zero Trust models can be facilitated by solutions like Duo Security and Palo Alto Networks Prisma Access.
- **Firewalls and Intrusion Detection and Prevention Systems (IDPS)** – Protect cloud environments against external threats and monitor network traffic for suspicious activity. Cloud firewalls and IDPS, such as Barracuda CloudGen Firewall, AWS Network Firewall, and Azure Firewall, provide robust perimeter defense and threat detection capabilities.
- **Secure Cloud Connectivity** – Implement secure cloud connectivity solutions such as VPNs and Direct Connect, ensuring a secure communication path between the cloud and on-premises environments. Solutions like Palo Alto GlobalProtect for VPN, AWS Direct Connect, and Azure Express Route for secure direct connectivity can be integrated.
- **Micro-segmentation** – Isolating workloads from one another to minimize the lateral movement of threats and reduce the attack surface. Tools like VMware NSX and Cisco Tetration enable micro-segmentation, isolating workloads and minimizing the lateral movement of threats.

E. Threat Detection and Response:

Effective threat detection and response mechanisms are vital for identifying and mitigating security incidents in real-time [17].

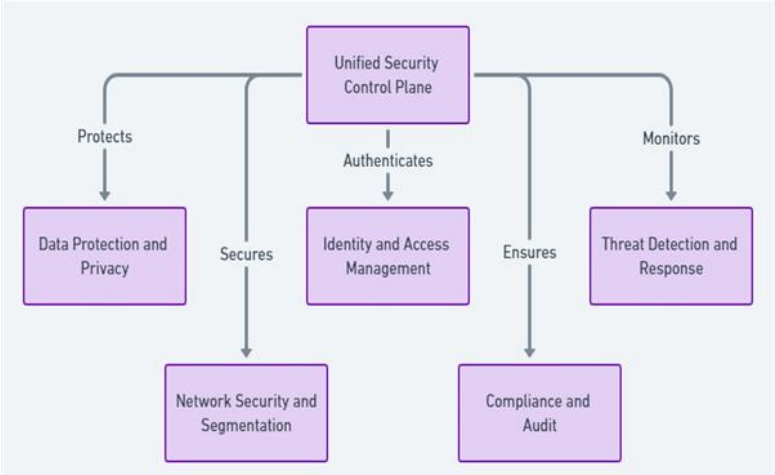
- **Security Information and Event Management (SIEM) Integration** – Aggregate and analyze security data from logs across cloud environments, facilitating timely detection of potential threats. Tools such as Splunk Enterprise Security and IBM QRadar Cloud collect and analyze security data from various sources.
- **Anomaly Detection and Behavioral Analytics** – Optimize security solutions such as Darktrace or Exabeam to identify unusual patterns or behaviors in cloud systems that may indicate a security threat.
- **Threat Intelligence** – Leveraging threat intelligence tools like Anomali ThreatStream or CrowdStrike Falcon to enhance the detection of sophisticated threats and inform security strategies.
- **Automated Incident Response** – Orchestrate and automate the response to security incidents through SOAR tools like Palo Alto Networks Cortex XSOAR, minimizing remediation time and potential damage.

F. Compliance and Audit:

Ensuring compliance with regulatory standards and conducting regular audits is crucial for maintaining trust and avoiding penalties [17].

- **Continuous Compliance Monitoring** – Implement real-time compliance monitoring with tools and processes such as Tripwire and Tenable.io to ensure organizations comply with regulations and standards.
- **Regular Security Assessments and Audits** – Perform periodic evaluations to identify vulnerabilities and assess the effectiveness of security controls. Tools such as Qualys Cloud Platform and Rapid7 can perform periodic assessments and audits.
- **Audit Trails and Log Management** – Implement log management solutions such as ELK Stack or Datadog Log Management to maintain comprehensive audit trails, support forensic analysis, and facilitate thorough investigations.

- **Compliance Reporting and Visualization** – Generate detailed compliance reports and visualization dashboards to demonstrate adherence to regulatory requirements and inform stakeholders. Platforms like Tableau and Microsoft Power BI enable the visualization of compliance data, simplifying reporting and decision-making processes.



STRATEGIES FOR IMPLEMENTING THE UNIFIED SECURITY FRAMEWORK

Adoption and implementation of the proposed security framework within organizations operating across multi-cloud infrastructures require a comprehensive, structured, and phased approach [8][12].

A. Preliminary Assessment and Planning:

This foundational step involves a comprehensive assessment of the existing security landscape and organizational requirements.

- **Cataloging Resources** – Catalog all resources deployed across cloud environments, including virtual machines, storage buckets, and network configurations. This inventory serves as the foundation for security planning and risk assessment.
- **Identifying Critical Data and Applications** – Identifying which data and applications are critical to the organization's operations is essential for prioritizing security efforts.
- **Regulatory and Compliance Requirements** – Understanding the regulatory landscape is crucial for ensuring that the security framework meets all legal and compliance obligations.
- **Current Security Posture Assessment** – A thorough assessment of the current security posture helps in identifying vulnerabilities, existing security controls, and areas for improvement.

B. Selection of Tools and Technologies:

Selecting the right tools and technologies is critical for the successful adoption of the unified security framework. Tools for cloud access security brokers (CASBs), security orchestration, automation and response (SOAR), and cloud security posture management (CSPM) should offer interoperability, scalability, and automation capabilities. The selection process should also evaluate the integration capabilities with existing tools and cloud service providers' native security features.

C. Pilot Program:

Prior to full-scale deployment, a pilot program should be conducted to test the effectiveness of the unified security framework in a controlled environment. The pilot program should involve a subset of cloud resources and aim to cover all core components of the security framework. This allows organizations to identify any issues and gaps in security coverage, understand the operational impacts of its implementation, and make necessary adjustments.

D. Full-scale Deployment:

Upon successful validation of the pilot program, the unified security framework can be deployed across the organization's multi-cloud environments. This phase involves integrating selected tools and technologies, configuring security controls, and establishing policies and procedures that adhere to the core components of the security framework. Organizations should follow best practices for secure configuration and ensure that all

components are appropriately integrated for seamless operation [16]. Regular testing and validation should be conducted during the deployment phase to ensure the effectiveness of security controls.

E. Ongoing Monitoring, Reporting, and Updating:

Establish mechanisms for continuous monitoring, reporting, and updating of the security framework to address new threats and incorporate technological advancements. This includes regular security assessments, threat intelligence gathering, and the refinement of security policies and procedures.

F. Training Programs and Capacity Building:

Implement training programs and capacity-building initiatives to equip personnel with the necessary skills to implement and manage the unified security framework effectively. Develop training modules focused on the specific components of the unified security framework, best practices in cloud security, and the use of selected security tools and technologies. This ensures that the organization's security team is well-prepared to address emerging security challenges.

EVALUATING THE EFFECTIVENESS AND IDENTIFYING THE CHALLENGES OF THE SECURITY FRAMEWORK

The evaluation of the proposed unified security framework's effectiveness employs a comprehensive methodology that integrates both qualitative and quantitative approaches. This includes deploying the framework in a controlled multi-cloud environment, followed by a series of simulated attack scenarios [11]. The methodology also incorporates feedback mechanisms from security experts and utilizes vital performance indicators (KPIs) to measure security posture improvements. The evaluation process is iterative, allowing for continuous refinement of the framework based on observed outcomes and expert feedback.

A. Simulated Attack Scenarios:

To rigorously test the framework's effectiveness, below range of simulated attack scenarios can be considered:

- **Credential Compromise** – Simulating an attacker gaining unauthorized access through compromised credentials to evaluate the framework's identity and access management controls.
- **Cross-Cloud Data Breach** – Introducing unauthorized data exfiltration attempts to test data protection and privacy mechanisms.
- **DDoS Attack** – Launching distributed denial-of- service attacks to assess the resilience and robustness of network security and segmentation.
- **Misconfiguration Exploit** – Simulating an attack that exploits cloud service misconfigurations to gain unauthorized access or escalate privileges.

B. Key Performance Indicators (KPIs):

Several identified KPIs critical for measuring security posture improvements in multi-cloud environments are:

- **Incident Detection Time** – The time taken to detect security incidents.
- **Incident Response Time** – Reduction in the time taken to detect and respond to security incidents.
- **Compliance Score** – The level of compliance with relevant security standards and regulations.
- **Incident Reduction Rate** – The percentage reduction in the number of security incidents.
- **Vulnerability Closure Rate** – Increase in the rate at which identified vulnerabilities are mitigated.
- **Threat Detection Accuracy** – The effectiveness of the framework in accurately identifying and mitigating threats.
- **Operational Downtime** – Reduction in downtime caused by security incidents, reflecting enhanced system resilience.

C. Feedback Loops and Continuous Improvement Mechanisms:

The framework incorporates continuous feedback mechanisms, including:

- **Automated Reporting** – Regular reports on security incidents, responses, and system performance.
- **Periodic Reviews** – Scheduled reviews of security policies, controls, and procedures to identify areas for improvement.
- **User Feedback** – Collection and analysis of feedback from users and administrators to refine the framework.

D. Potential Obstacles and Technical Hurdles:

Adopting and integrating a unified security framework may encounter specific challenges, including:

- **Complexity of Multi-Cloud Environments** – Navigating the heterogeneity and complexity of multi- cloud infrastructures can complicate the implementation of a unified framework.
- **Interoperability Issues** – Ensuring seamless integration between different cloud platforms and security tools can pose significant technical hurdles.
- **Resistance to Change** – Organizational inertia and resistance to adopting new security practices can impede the framework's implementation.
- **Intricate Configuration Management** – Managing and configuring security controls and policies consistently across multiple cloud providers can be complex.

E. Continuous Evolution of Cloud Technologies and Security Threats:

The cloud computing landscape is characterized by its rapid pace of innovation, introducing new services and architectures that offer enhanced performance, scalability, and cost-efficiency. Concurrently, security threats are becoming more sophisticated, with attackers leveraging advanced techniques to exploit vulnerabilities in multi-cloud environments. The unique needs of growing multi- cloud environments and evolving security threats necessitate the security framework to be continuously updated to address emerging threats.

F. Balancing Security Measures with Performance and User Experience:

Implementing robust security measures in multi-cloud environments is essential for protecting sensitive data and maintaining system integrity. However, these measures must be balanced with the need to ensure optimal system performance and a positive user experience. Overly stringent security controls can impede system efficiency and usability, potentially leading to reduced productivity and user dissatisfaction. Therefore, the unified security framework must strike a balance, ensuring that security measures do not adversely affect system performance or user experience.

CONCLUSION

The intricate and dynamic nature of multi-cloud environments, characterized by their diversity and complexity, necessitates a strong, cohesive, and adaptable approach to security. This study has underscored the critical need for a unified security framework tailored to multi-cloud infrastructures, aiming to address multifaceted security challenges and enhance the overall security posture of these environments. The proposed unified security framework offers a comprehensive solution designed to strengthen the security and resilience of multi-cloud infrastructures. By integrating critical core components and best practices in cloud security, the framework aims to elevate the cybersecurity posture of organizations, thereby safeguarding sensitive information and maintaining operational continuity. The novel aspects of the proposed security framework, including its focus on interoperability, scalability, and adaptability, represent significant contributions to the field of cloud security. The implications for future research and the development of security standards for multi-cloud environments are profound. It paves the way for further exploration into advanced security mechanisms, the integration of artificial intelligence and machine learning for threat detection and response, and the establishment of global standards for multi-cloud security.

REFERENCES

[1]. P. Samarati and S. De Capitani di Vimercati, Cloud Security: Issues and Concerns, Encyclopedia of Cloud Computing, pp. 205-219, May 2016.

[2]. A. Singh and K. Chatterjee, Cloud security issues and challenges: A survey, Journal of Network and Computer Applications, vol. 79, pp. 88-115, February 2017.

[3]. A. Mondal, S. Paul, R.T. Goswami, and S. Nath, Cloud computing security issues & challenges: A Review, International Conference on Computer Communication and Informatics (ICCCI), January 2020.

[4]. G. Verma and S. Adhikari, Cloud Computing Security Issues: a Stakeholder's Perspective, SN Computer Science, October 2020.

[5]. R. Kumar and R. Goyal, On cloud security requirements, threats, vulnerabilities, and countermeasures: A survey, Computer Science Review, vol. 33, pp. 1-48, August 2019.

[6]. S.A. Aljawarneh and M.O.B. Yassein, A Conceptual Security Framework for Cloud Computing Issues, International Journal of Intelligent Information Technologies, 2016.

[7]. 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, September 2017.
[8]. M. Jouini and L.B.A. Rabai, A Security Framework for Secure Cloud Computing Environments, Cloud Security, pp. 249-263, 2019.
[9]. Y. Alghofaili, A. Albattah, N. Alrajeh, M.A. Rassam, and B.A.S. Al-rimy, Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges, Applied Sciences, September 2021.
[10]. C. Di Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. H. Campbell, and M.N. Bashir, Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security, IEEE CLOUD, June 2017.
[11]. S.S. Rupra and A. Omamo, A Cloud Computing Security Assessment Framework for Small and Medium Enterprises, Journal of Information Security, 2020.
[12]. R. Patil, H. Dudeja, and C. Modi, Designing an efficient security framework for detecting intrusions in a virtual network of cloud computing, Computers & Security, August 2019.
[13]. S. Shakya, An Efficient Security Framework for Data Migration in a Cloud Computing Environment, Journal of Artificial Intelligence and Capsule Networks, 2019.
[14]. V. Casola, A. De Benedictis, M. Rak, and U. Villano, Security-by-design in multi-cloud applications: An optimization approach, Information Sciences, July 2018.
[15]. L. Megouache, A. Zitouni, and M. Djoudi, Ensuring user authentication and data integrity in a multi-cloud environment, Human-centric Computing and Information Sciences, April 2020.
[16]. C. Dotson, Practical Cloud Security: A Guide for Secure Design and Deployment: 1st Edition, O'Reilly, March 2019.
[17]. K.A. Torkura, M.I.H. Sukmana, F. Cheng, and C. Meinel, Continuous auditing and threat detection in multi- cloud infrastructure, Computers & Security, March 2021.