RESEARCH ARTICLE

International Journal of Applied Machine Learning and Computational Intelligence

Evaluating the Effectiveness of Access Control Models and Identity Management Systems in Multi-Tenant Cloud Infrastructures

Prajwal Khadka Siti[1] and **Sujata Adhikari** [2]

Department of Computer Science, Sagarmatha Institute of Technology, 89 Kalimati Road, Kathmandu, 44601, Nepal.

Department of Computer Science, Lumbini University of Applied Sciences, Buddha Path, Butwal, Rupandehi, 32907, Nepal.

Published: 2023-01-04

Full list of author information is available at the end of the article

Abstract

Multi-tenant cloud infrastructures provide significant advantages in terms of scalability, flexibility, and cost-efficiency by allowing multiple tenants to share the same physical and virtual resources. However, this shared model introduces complex security challenges, particularly in terms of access control and identity management. Effective access control is essential for ensuring that tenants' data remains isolated, and unauthorized access is prevented, while identity management systems play a critical role in securely managing user authentication and authorization across different services. This paper evaluates the effectiveness of various access control models and identity management systems within the context of multi-tenant cloud infrastructures. Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are examined, with RBAC providing simplicity and ease of administration, while ABAC offers greater flexibility through the use of contextual attributes. Both models have strengths and weaknesses when applied to cloud environments, especially concerning the need to balance security with performance and scalability. ABAC's dynamic nature makes it better suited for environments requiring fine-grained access controls, but its complexity can pose challenges in policy management and enforcement. Conversely, RBAC's static nature may lead to overly simplistic access controls in dynamic scenarios but excels in environments with relatively stable access requirements. Similarly, SSO simplifies access to multiple services but presents risks if not properly secured, especially in the case of compromised login sessions. Identity Governance and Administration (IGA) is discussed as a critical element for ensuring compliance, enforcing policies, and managing identities across multiple cloud environments.Tenant isolation remains a critical requirement to prevent unauthorized access between tenants. Cross-tenant attacks, often facilitated by vulnerabilities in the shared cloud infrastructure, highlight the importance of robust access controls and continuous monitoring. Insider threats, including those from administrators and privileged users, also present a significant risk and underscore the need for least-privilege access models and zero-trust security frameworks.

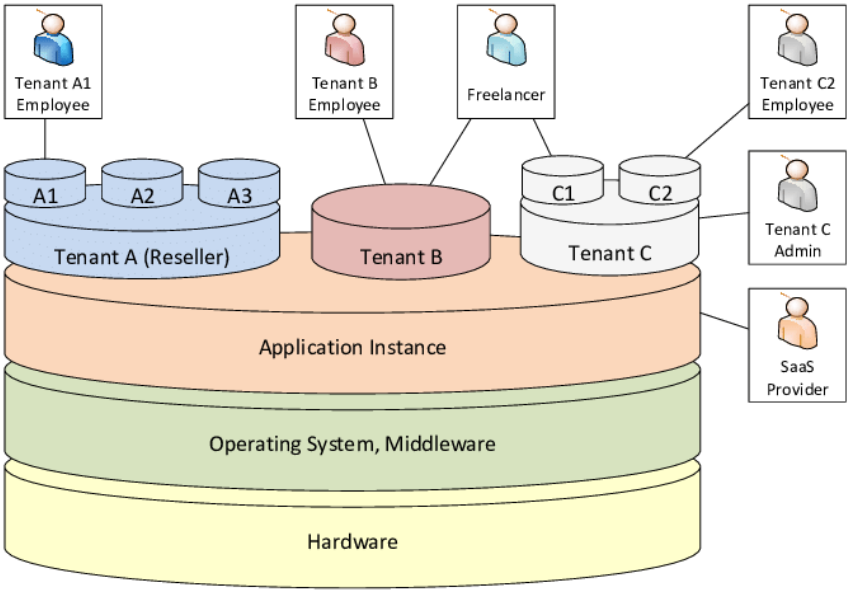

Figure 1 Multi-Tenant Clouds

1 Introduction

Cloud computing has revolutionized the IT landscape by enabling organizations to outsource their data storage, applications, and computing resources to cloud service providers (CSPs). In multi-tenant cloud infrastructures, multiple customers or tenants share the same physical and virtualized resources. While cloud infrastructures provide numerous benefits such as cost efficiency, scalability, and flexibility, they also introduce significant security challenges. One of the most critical challenges is ensuring proper access control and identity management to safeguard data and prevent unauthorized access across tenants.

Access control models define how users can access specific resources within the cloud environment, while identity management (IdM) systems provide the necessary framework to authenticate and authorize users. Given the shared nature of cloud resources in multi-tenant environments, access control and identity management become particularly important to ensure isolation between tenants and to protect sensitive information. Several models and systems have been developed to address these concerns, such as Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and the use of federated identity management systems.

This paper evaluates the effectiveness of various access control models and identity management systems in multi-tenant cloud infrastructures. The goal is to explore how these systems ensure security, scalability, and performance while minimizing the risk of security breaches and unauthorized access. This evaluation is essential to identify best practices and potential improvements that could enhance the security posture of multi-tenant cloud environments.

2 Access Control Models in Multi-Tenant Clouds

Access control models play a crucial role in maintaining security within multi-tenant cloud infrastructures. These models determine how users, applications, and services are granted access to resources while ensuring compliance with security policies. In cloud environments, where multiple tenants share physical and virtual resources, access control models must be carefully chosen and configured to provide the appropriate level of isolation and security between tenants while maintaining ease of management. The two most commonly adopted access control models in cloud computing are Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). Other models, such as Mandatory Access Control (MAC) and Discretionary Access Control (DAC), are less commonly applied in cloud environments but provide foundational insights into access management and serve as theoretical baselines that have influenced more modern models.

2.1 Role-Based Access Control (RBAC)

RBAC is one of the most widely used access control models in cloud infrastructures due to its simplicity, scalability, and manageability. In RBAC, access permissions are assigned to roles rather than to individual users, and users are granted roles based on their responsibilities within an organization. This model simplifies the management of access control policies by reducing the number of individual permissions that need to be managed, thus making it particularly useful in large, multi-tenant environments where managing individual user permissions could quickly become unmanageable. By assigning permissions to roles, cloud administrators can more easily enforce consistent access policies across different users within the same role, ensuring that all users with similar responsibilities have uniform access rights.

In multi-tenant cloud environments, RBAC allows organizations to define roles such as tenant administrators, service users, and auditors, each with specific permissions to access resources. For instance, a tenant administrator might have broad access to manage the tenant's resources, while a service user may only have limited access to perform specific tasks within their assigned scope. The main advantage of RBAC is its ease of implementation and low management overhead. Once roles are defined, administrators can easily assign users to these roles without needing to adjust permissions on a per-user basis, which is especially beneficial in dynamic environments where users are frequently added or removed. Furthermore, RBAC aligns well with the principle of least privilege, which ensures that users are only granted the minimum level of access required to perform their tasks, thereby reducing the risk of unauthorized access or accidental data exposure.

Despite its advantages, RBAC has limitations, especially when dealing with complex access control requirements that demand dynamic and context-dependent access decisions. In a cloud environment, users may require access based on factors that go beyond static role definitions, such as location, time of day, or workload sensitivity. For example, an employee might need elevated access privileges only during a specific project phase or when working from a secure location. In such cases, the static nature of RBAC can become a hindrance, as it lacks the flexibility to accommodate these dynamic requirements without introducing an excessive number of roles, which can complicate policy management and lead to "role explosion." This

limitation has led to the development of more flexible models, such as ABAC, that can handle complex and conditional access scenarios.

2.2 Attribute-Based Access Control (ABAC)

ABAC offers a more dynamic and flexible approach to access control compared to RBAC. In ABAC, access decisions are based on a set of attributes associated with users, resources, actions, and the environment. These attributes can include user roles, resource classifications, access times, network locations, and more. This flexibility allows ABAC policies to be more granular and adaptable to a wider range of scenarios than is possible with RBAC, making ABAC a suitable choice for environments with complex or context-sensitive access requirements.

In multi-tenant cloud environments, ABAC is particularly beneficial because it enables cloud service providers (CSPs) and tenants to define access policies based on a wide array of factors, including tenant-specific attributes. For example, an organization may use ABAC to enforce access policies that restrict data access to users within a specific geographic region, limit access to sensitive resources based on the time of day, or apply additional security controls to high-sensitivity resources. This level of granularity allows for more robust security measures, which can significantly reduce the risk of unauthorized access in environments where data protection and regulatory compliance are paramount. ABAC's ability to evaluate multiple attributes in real-time enables organizations to implement fine-grained policies that adapt to changing conditions, which is particularly useful for ensuring secure access in multi-tenant clouds where tenant-specific requirements must be met.

However, ABAC's flexibility comes with higher complexity in policy management and enforcement. Defining and maintaining policies based on multiple attributes can be challenging, particularly as the number of attributes and the complexity of conditions grow. This complexity can also introduce performance bottlenecks in large-scale cloud environments, where real-time policy evaluation is required for each access request. Moreover, ensuring consistency in attribute definitions and policy interpretation across different tenants and services can be difficult, especially when multiple CSPs are involved. This challenge may necessitate investment in sophisticated policy management tools and monitoring systems to ensure that ABAC policies are implemented correctly and efficiently.

2.3 Comparison of RBAC and ABAC

RBAC and ABAC each have distinct advantages and disadvantages when applied to multi-tenant cloud infrastructures. RBAC's strength lies in its simplicity and ease of administration, making it suitable for organizations with relatively static access control requirements and clear role definitions. The model is particularly useful in scenarios where the principle of least privilege can be achieved through well-defined roles, as it allows for straightforward management of access rights and ensures consistency across users with similar job functions. ABAC, on the other hand, provides greater flexibility and granularity, making it a better choice for organizations with dynamic and context-sensitive access needs. In ABAC, access decisions can be tailored based on real-time conditions, enabling organizations to implement more nuanced and adaptable access policies.

Despite its flexibility, ABAC's increased complexity can lead to challenges in policy management and performance. The need to evaluate multiple attributes for each access decision can be computationally intensive, potentially affecting system responsiveness in high-demand environments. In contrast, RBAC's simpler role-based approach is less prone to performance issues, as access control decisions do not require complex, real-time evaluations of multiple attributes. However, RBAC's limitations in handling dynamic access scenarios can make it inadequate for certain cloud environments where access needs to be highly adaptable. In many cases, organizations may opt for a hybrid approach that combines elements of both RBAC and ABAC. By implementing role-based controls for common access patterns and attribute-based controls for more complex scenarios, a hybrid model can provide a balance between simplicity and flexibility, particularly in large multi-tenant environments.

2.4 Hybrid Access Control Models

Given the unique demands of multi-tenant cloud environments, hybrid access control models that combine elements of both RBAC and ABAC are becoming increasingly popular. A hybrid model seeks to leverage the strengths of both approaches while mitigating their respective weaknesses. In a hybrid model, RBAC can be used to define core access permissions based on user roles, while ABAC can be applied to enforce additional access conditions based on attributes. This approach allows organizations to implement a baseline level of access control through roles, thereby simplifying policy management for common access patterns, while also enabling attribute-based controls to handle more dynamic and situational requirements.

For example, a hybrid model could assign users to general roles that grant basic permissions, while ABAC policies provide additional restrictions based on location, device type, or time of access. This combination allows for efficient policy management without compromising on flexibility. In scenarios where a user's access rights need to change dynamically based on context, ABAC's attribute-based evaluations can override or refine RBAC-based permissions, providing a more adaptive and secure approach to access control.

Implementing a hybrid access control model requires careful integration to ensure compatibility between RBAC and ABAC components. Organizations need to establish clear rules on how role-based and attribute-based policies interact, particularly in cases where conflicting policies may arise. Additionally, hybrid models may benefit from advanced policy management tools that provide centralized control and visibility over both RBAC and ABAC policies, thus ensuring coherent policy enforcement across the multi-tenant cloud infrastructure.

3 Identity Management Systems in Cloud Environments

Identity management (IdM) systems are essential in multi-tenant cloud environments to ensure secure authentication and authorization of users. Effective IdM solutions help organizations manage user identities, enforce access control policies, and maintain accountability. In the context of cloud computing, IdM systems must also address issues such as identity federation, single sign-on (SSO), and cross-tenant access control. These systems are increasingly complex due to the distributed nature

of cloud services, where identity data and access rights often span multiple cloud providers. Consequently, identity management in cloud settings must address a variety of operational and security challenges to safeguard sensitive data and maintain regulatory compliance.

3.1 Federated Identity Management

Federated identity management allows users to authenticate across multiple cloud environments using a single set of credentials. This approach is particularly valuable in multi-tenant cloud environments where users often need to access resources and services provided by different cloud service providers (CSPs). Federated identity systems enable users to authenticate once and gain access to multiple services without the need to maintain separate credentials for each service, which simplifies identity management and reduces the security risks associated with password reuse and proliferation. Federated identity management is thus an enabler of cross-organization collaboration and interoperability in cloud ecosystems.

At the technical level, federated identity management typically relies on standardized protocols such as Security Assertion Markup Language (SAML), OpenID Connect, and OAuth. These protocols facilitate secure identity exchange and authentication across disparate systems by providing mechanisms for token issuance and assertion-based trust. SAML, for example, allows for secure exchange of authentication and authorization data between an identity provider (IdP) and a service provider (SP), using XML-based messages to carry identity assertions. OpenID Connect, which is an identity layer on top of the OAuth 2.0 protocol, provides a more lightweight and JSON-based approach suitable for modern web and mobile applications. By adopting these protocols, organizations can create a federated identity environment that promotes seamless access to resources across multiple cloud services while ensuring that user identity information is managed securely.

Despite the benefits, federated identity management introduces new security challenges. One significant risk is the potential for identity federation attacks, where attackers exploit weaknesses in the federation process to gain unauthorized access to resources. For instance, attackers could intercept or manipulate identity tokens during transmission, a vulnerability that might be exploited in man-in-the-middle (MITM) attacks. Additionally, trust relationships between identity providers and service providers can be targeted, especially if attackers compromise one of the trusted entities. To mitigate these risks, CSPs and tenants must implement strong security measures, including multi-factor authentication (MFA), secure token exchange practices, and rigorous auditing of identity federation processes. These measures, combined with robust encryption and proper certificate management, help ensure the integrity and security of federated identity systems.

3.2 Single Sign-On (SSO)

Single sign-on (SSO) is another critical component of identity management in multi-tenant cloud environments. SSO enables users to authenticate once and gain access to multiple applications and services without needing to re-enter credentials, thereby reducing the friction associated with multiple logins and enhancing the user experience. In an enterprise setting, SSO is especially valuable as it allows employees to

move seamlessly between different internal and external systems without interrupting their workflow to re-authenticate.

In a multi-tenant cloud infrastructure, SSO can streamline access across various tenant services and applications. For example, a user from Tenant A who authenticates through an SSO portal can seamlessly access Tenant A's services without needing to log in separately to each individual service. This functionality is particularly useful in scenarios where tenants use a combination of cloud services or applications from different providers, as it allows for centralized identity verification and reduces the administrative complexity of managing multiple login credentials across services.

While SSO offers convenience and improved security by reducing password fatigue, it also presents risks. One primary concern is the possibility of a "single point of failure." If an attacker compromises a user's SSO credentials, they could potentially gain unauthorized access to all the services and applications associated with that user. For example, if a cybercriminal successfully executes a phishing attack to obtain an employee's SSO credentials, they may gain access to sensitive corporate applications, data, and resources. Consequently, implementing additional security layers, such as multi-factor authentication (MFA), is a critical practice for securing SSO systems in multi-tenant environments. Furthermore, continuous monitoring of login activities and implementing strict session management policies, including timeouts and IP restrictions, can help to detect and mitigate potential unauthorized access attempts.

3.3 Identity Governance and Administration (IGA)

Identity Governance and Administration (IGA) is a key aspect of identity management that focuses on ensuring compliance with regulatory requirements and internal security policies. IGA encompasses various processes, such as identity lifecycle management, access certification, and policy enforcement, to ensure that users maintain the appropriate access to resources at all times. IGA frameworks are essential for enabling organizations to not only define who has access to which resources, but also to ensure that such access aligns with corporate governance policies and regulatory requirements.

In multi-tenant cloud environments, IGA systems help organizations manage and monitor user access across multiple tenants and services, providing the tools needed to automate identity provisioning, enforce least privilege principles, and periodically review access rights. For instance, an IGA system can automate the onboarding and offboarding processes, ensuring that users are granted or revoked access to necessary resources as they join or leave an organization. Moreover, access certification campaigns can be scheduled to regularly review and validate access permissions, thus ensuring that outdated or excessive permissions are minimized, which mitigates the risk of insider threats and accidental data exposure.

One of the challenges in implementing effective IGA in cloud environments is the need for interoperability between different CSPs and IdM systems. Each cloud provider often has its own proprietary IdM solution, making it difficult to enforce consistent governance policies across different platforms. For example, managing identities across both Amazon Web Services (AWS) Identity and Access Management (IAM) and Microsoft Azure Active Directory (AAD) can present compatibility

issues. This is particularly problematic for organizations with hybrid or multi-cloud strategies, where a unified approach to identity governance is essential for maintaining visibility and control. To address this challenge, many organizations are adopting cloud-agnostic IGA solutions that integrate with multiple cloud platforms, providing a consolidated view of identity management activities. These solutions enable organizations to enforce consistent governance policies across various cloud providers, ensuring that security policies are upheld regardless of the platform.

Table 1 Comparison of Identity Governance Features in Leading Cloud Providers

Cloud Provider	Identity Governance Features	Limitations
Amazon Web Services (AWS)	Supports identity lifecycle management and role-based access control (RBAC) through IAM	Limited cross-platform integration with other CSPs, relies on third-party tools for multi-cloud environments
Microsoft Azure Active Directory (AAD)	Provides access reviews, identity lifecycle management, and Conditional Access policies	Strong within Microsoft ecosystem but integration with non-Microsoft platforms can be challenging
Google Cloud Identity	Offers user and access management, group-based policies, and access transparency	Limited features for complex IGA scenarios compared to AWS and Azure; lacks extensive governance tools for hybrid environments

The evolution of IGA in cloud environments is indicative of a broader trend towards automation and policy-driven identity management. Modern IGA solutions are increasingly incorporating artificial intelligence (AI) and machine learning (ML) capabilities to streamline access decision-making and detect anomalous behaviors. For example, AI-based IGA tools can analyze access patterns to identify deviations from usual behavior, flagging potentially suspicious activities for further review. This can enhance the organization's ability to preemptively detect and mitigate security risks associated with identity misuse. Furthermore, as regulatory requirements evolve, particularly with respect to data protection and privacy, cloud IGA systems must adapt to ensure ongoing compliance. Regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) place stringent requirements on data access controls, making effective IGA an essential component of a compliant cloud infrastructure.

identity management systems in cloud environments must be robust, adaptable, and capable of handling the unique challenges posed by multi-tenant architectures. By combining federated identity management, single sign-on, and comprehensive IGA strategies, organizations can establish a secure and user-friendly identity management framework that enhances operational efficiency and strengthens cloud security. These components work together to address the complexities of user authentication, access control, and regulatory compliance in distributed cloud ecosystems, creating a cohesive approach to identity management that meets the demands of modern cloud infrastructures.

4 Security Challenges in Multi-Tenant Environments

Despite the advantages of using access control models and identity management systems, multi-tenant cloud infrastructures face several security challenges. These challenges arise from the shared nature of cloud resources and the complexity of managing access control and identities across multiple tenants. Key security concerns include tenant isolation, cross-tenant attacks, and insider threats.

4.1 Tenant Isolation

One of the primary security concerns in multi-tenant environments is ensuring that tenants are properly isolated from each other. Without proper isolation mechanisms, an attacker who gains access to one tenant's environment could potentially access other tenants' resources. To mitigate this risk, CSPs must implement strong isolation techniques, such as virtual network segmentation, access control lists (ACLs), and hypervisor security measures.

Access control models, such as RBAC and ABAC, play a critical role in enforcing tenant isolation by ensuring that users and applications can only access resources that belong to their own tenant. Identity management systems also contribute to isolation by ensuring that user identities are properly scoped to the appropriate tenant and that cross-tenant access is only granted when explicitly authorized.

]Cross-Tenant Attacks

Cross-tenant attacks occur when a malicious actor exploits vulnerabilities in a multi-tenant environment to gain unauthorized access to another tenant's resources. These attacks can take various forms, including exploiting weak access control policies, leveraging misconfigurations, or launching side-channel attacks.

To prevent cross-tenant attacks, CSPs must enforce strict access control policies and regularly audit their systems for vulnerabilities. Additionally, implementing comprehensive logging and monitoring systems can help detect suspicious activities and mitigate potential cross-tenant threats before they escalate.

4.2 Insider Threats

Insider threats remain a significant challenge in multi-tenant cloud environments, particularly when tenants rely on external administrators or service providers to manage their infrastructure. Insider threats can arise when individuals with privileged access misuse their authority to access sensitive data or disrupt services.

Effective identity management systems can help mitigate insider threats by enforcing strict access controls, monitoring privileged activities, and ensuring that users are only granted the minimum necessary access to perform their duties. Implementing zero-trust security models, which assume that all users and devices are untrusted by default, can also reduce the risk of insider threats.

5 Conclusion

In multi-tenant cloud infrastructures, access control models and identity management systems are essential for ensuring the security and integrity of tenant data. Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) offer different approaches to managing access control, with RBAC providing simplicity and ABAC offering flexibility. Federated identity management and Single Sign-On (SSO) improve the user experience by enabling seamless access across cloud services, while Identity Governance and Administration (IGA) ensures that access policies are enforced consistently.

However, multi-tenant environments also present unique security challenges, including tenant isolation, cross-tenant attacks, and insider threats. By adopting best

practices in access control, identity management, and security monitoring, organizations can mitigate these risks and improve the overall security of their cloud infrastructures.

[1–24]

Author details
[1]Department of Computer Science, Sagarmatha Institute of Technology, 89 Kalimati Road, Kathmandu, 44601, Nepal.. [2]Department of Computer Science, Lumbini University of Applied Sciences, Buddha Path, Butwal, Rupandehi, 32907, Nepal..

References

1. Ali, M., Khan, R.: Cloud computing security: Issues and mitigation strategies. International Journal of Computer Science and Network Security **11**(6), 7–12 (2011)
2. Arora, N., Wang, X.: Cloud security solutions: A comparative analysis. International Journal of Cloud Applications and Computing **4**(2), 78–89 (2014)
3. Jani, Y., Jani, A., Gogri, D.: Cybersecurity in microservices architectures: Protecting distributed retail applications in cloud environments. International Journal of Science and Research (IJSR) **11**(8), 1549–1559 (2022)
4. Brown, E., Singh, M.: Cloud Computing: Security Threats and Solutions. McGraw-Hill, ??? (2013)
5. David, S., Yang, X.: Security implications of multi-tenancy in cloud computing environments. In: Proceedings of the IEEE International Symposium on Cloud and Services Computing, pp. 109–118 (2010). IEEE
6. Velayutham, A.: Ai-driven storage optimization for sustainable cloud data centers: Reducing energy consumption through predictive analytics, dynamic storage scaling, and proactive resource allocation. Sage Science Review of Applied Machine Learning **2**(2), 57–71 (2019)
7. Garcia, J., Liu, M.: Identity and access management in cloud environments: Challenges and solutions. International Journal of Cloud Computing **7**(2), 143–156 (2016)
8. Gomez, C., Walker, H.: Auditing cloud services for regulatory compliance: Challenges and strategies. In: Proceedings of the 9th IEEE International Conference on Cloud Computing (CLOUD), pp. 501–508 (2013). IEEE
9. Velayutham, A.: Architectural strategies for implementing and automating service function chaining (sfc) in multi-cloud environments. Applied Research in Artificial Intelligence and Cloud Computing **3**(1), 36–51 (2020)
10. Gupta, N., Huang, L.: Risk management in cloud computing: Challenges and strategies. Journal of Information Security and Applications **18**(3), 119–130 (2013)
11. Johnson, P., Chen, Y.: Challenges in Securing Cloud Infrastructure. Wiley, ??? (2017)
12. Velayutham, A.: Mitigating security threats in service function chaining: A study on attack vectors and solutions for enhancing nfv and sdn-based network architectures. International Journal of Information and Cybersecurity **4**(1), 19–34 (2020)
13. Jones, M., Chen, L.: Cloud Threats and Mitigation Strategies. Springer, ??? (2012)
14. Kim, S., Lin, C.: Cloud data encryption strategies and their effectiveness: A review. Journal of Cloud Computing Research **6**(1), 98–112 (2013)
15. Velayutham, A.: Methods and algorithms for optimizing network traffic in next-generation networks: Strategies for 5g, 6g, sdn, and iot systems. Journal of Intelligent Connectivity and Emerging Technologies **6**(5), 1–26 (2021)
16. Lee, K., Müller, J.: Security challenges in cloud computing environments. In: Proceedings of the 8th International Conference on Cloud Computing (CLOUD), pp. 412–419 (2014). IEEE
17. Li, H., Schmitt, K.: Encryption-based mitigation of insider threats in cloud environments. In: Proceedings of the 10th International Conference on Security and Privacy in Communication Networks (SecureComm), pp. 132–140 (2014). Springer
18. Velayutham, A.: Overcoming technical challenges and implementing best practices in large-scale data center storage migration: Minimizing downtime, ensuring data integrity, and optimizing resource allocation. International Journal of Applied Machine Learning and Computational Intelligence **11**(12), 21–55 (2021)
19. Miller, A., Zhang, J.: Cloud Forensics and Security Management. CRC Press, ??? (2011)
20. Nguyen, P., Chen, X.: Privacy and data protection in cloud computing: Challenges and mitigation techniques. In: Proceedings of the 5th IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp. 606–613 (2012). IEEE
21. Nguyen, T., Patel, A.: Data privacy in the cloud: Mitigation strategies for privacy breaches. Journal of Information Security **19**(4), 89–99 (2015)
22. Patel, R., Wang, M.: Mitigation strategies for data breaches in cloud computing. International Journal of Information Security **15**(1), 29–41 (2016)
23. Rodriguez, M., Li, J.: Security challenges in mobile cloud computing: Mitigation approaches. In: Proceedings of the 6th IEEE International Conference on Cloud Computing (CLOUD), pp. 420–428 (2011). IEEE
24. Smith, J., Zhang, W.: Cloud security issues and challenges: A survey. Journal of Cloud Computing: Advances, Systems and Applications **4**(2), 45–60 (2015)