Nikhil Varma, 2021, 9:6
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Secure and Automated Enterprise Platforms in Multi-Cloud Environments

Nikhil Varma
Sri Venkateswara University

Abstract - The accelerated adoption of cloud computing has fundamentally reshaped modern enterprise IT infrastructures, driving organizations toward increasingly sophisticated multi-cloud strategies in which workloads are distributed across multiple cloud service providers to achieve enhanced scalability, operational resilience, and service optimization. By leveraging diverse platforms such as public, private, and hybrid cloud environments, enterprises seek to improve cost efficiency, avoid vendor lock-in, and access best-in-class technological capabilities. However, while multi-cloud ecosystems promote architectural flexibility and business continuity, they simultaneously introduce substantial complexity in areas including security governance, configuration management, automation orchestration, regulatory compliance, and cross-platform interoperability. This review systematically examines the architectural foundations of secure and automated enterprise platforms operating within multi-cloud environments. It critically analyzes core security challenges, including identity and access management (IAM) fragmentation, inconsistent authentication and authorization models, data protection and encryption management disparities, configuration drift, and expanded network attack surfaces arising from inter-cloud connectivity. Particular attention is given to the risks associated with misconfigurations, privilege escalation, insecure APIs, and insufficient visibility across distributed infrastructures. The study further explores the central role of automation as an enabler of security and operational consistency. Technologies such as Infrastructure as Code (IaC), DevSecOps pipelines, container orchestration, and policy-as-code frameworks are evaluated as mechanisms for embedding security controls directly into infrastructure provisioning and application deployment workflows. By integrating automated compliance validation and continuous monitoring, enterprises can mitigate human error and enforce standardized security baselines across heterogeneous cloud platforms. In addition, the review assesses governance models including centralized security hub architectures, federated governance frameworks, and cloud-agnostic abstraction layers implemented through platform engineering and internal developer platforms. Emerging paradigms such as Zero Trust Architecture, artificial intelligence-driven security analytics, cloud security posture management (CSPM), and automated threat detection are examined for their capacity to enhance real-time risk mitigation and policy enforcement. The analysis also highlights persistent limitations inherent in multi-cloud adoption, including operational complexity, integration challenges, latency constraints, cost escalation, and shortages in specialized cloud security expertise. Finally, future trajectories are explored, encompassing autonomous security orchestration, confidential computing, secure multi-party computation, and advanced platform engineering practices that embed governance into self-service enterprise ecosystems. The findings suggest that sustainable multi-cloud success depends not merely on distributed cloud utilization, but on deeply integrated security automation, standardized identity governance, continuous compliance enforcement, and policy-driven infrastructure management. Enterprises that strategically align automation, governance, and architectural design will be better positioned to transform multi-cloud complexity into a secure and scalable competitive advantage.

Keywords - Multi-Cloud Architecture, Cloud Security Governance, Infrastructure as Code (IaC), DevSecOps, Zero Trust Architecture, Cloud Security Posture Management (CSPM), Policy as Code, Enterprise Platform Engineering, AI-Driven Threat Detection, Compliance Automation.

I. INTRODUCTION

In the past decade, enterprise computing has undergone a fundamental transformation driven by cloud technologies. Organizations that once relied heavily on on-premises data centers now distribute workloads across multiple cloud providers to gain scalability, agility, and competitive advantage. Rather than committing to a single vendor, enterprises increasingly adopt multi-cloud environments, leveraging platforms such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform to optimize cost structures, enhance resilience, and access specialized services.

This approach enables organizations to select the most suitable services for analytics, machine learning, storage, compute, or geographic distribution without being constrained by a single ecosystem (Khan et al., 2019).

However, while multi-cloud strategies reduce vendor lock-in and improve operational flexibility, they simultaneously introduce significant complexity. Each provider offers unique identity systems, networking models, configuration standards, and compliance mechanisms.

As enterprises expand across heterogeneous environments, maintaining consistent security governance becomes increasingly difficult. Configuration management, automation consistency, compliance monitoring, and interoperability challenges escalate with every additional cloud platform integrated into the architecture (Mishra et al., 2015).

Secure and automated enterprise platforms have therefore emerged as a critical architectural paradigm. These platforms aim to harmonize security, automation, governance, and operational processes across diverse cloud ecosystems.

This review examines the foundational architecture of multi-cloud enterprise platforms, the security challenges inherent to such environments, the role of automation in mitigating risk, governance and compliance mechanisms, and emerging technologies shaping the next generation of secure enterprise infrastructure (Rho & Vasilakos, 2018).

II. UNDERSTANDING MULTI-CLOUD ENTERPRISE PLATFORMS

A multi-cloud enterprise platform is more than a collection of independent cloud accounts. It represents a strategically designed ecosystem in which services from multiple cloud providers are integrated under a unified governance, operational, and security framework. The objective is not merely workload distribution but centralized visibility, standardized policy enforcement, and automated lifecycle management across environments (Sousa et al., 2016).

One of the primary drivers behind multi-cloud adoption is the desire to avoid vendor lock-in. When enterprises rely exclusively on a single cloud provider, they become dependent on that provider's pricing structures, service evolution, and architectural constraints. A multi-cloud strategy mitigates this dependency, allowing organizations to negotiate better pricing and pivot services as technological demands evolve (Raj & Raman, 2018). Regulatory compliance requirements also encourage multi-cloud adoption. Data residency laws in various jurisdictions require sensitive data to remain within specific geographic boundaries. By leveraging multiple cloud providers with region-specific data centers, enterprises can align operations with national and international regulations. This flexibility is especially critical for industries such as finance, healthcare, and government (Lal, 2016).

High availability and disaster recovery further justify multi-cloud architectures. If a regional outage affects one provider, workloads can failover to another cloud environment, ensuring business continuity. Multi-cloud resilience is particularly important for mission-critical systems where downtime translates directly into financial loss and reputational damage (Yang & Cheng, 2015).

Additionally, different cloud providers often excel in specific service domains. One platform may offer superior artificial intelligence services, while another may provide more advanced data warehousing solutions. Multi-cloud architectures allow enterprises

to access best-in-class technologies across ecosystems (Obiuto et al., 2020).

Security Challenges in Multi-Cloud Architectures

Security in multi-cloud environments extends beyond traditional perimeter defense. It requires maintaining consistent policy enforcement across heterogeneous infrastructures. Each cloud provider introduces unique security configurations, identity models, and logging standards. Ensuring uniform protection across these diverse systems is a central challenge (Mitrovic et al., 2016).

Identity and Access Management (IAM)

Identity and Access Management is arguably the most critical component of multi-cloud security. Each provider offers distinct IAM frameworks with different role structures, policy definitions, and federation mechanisms. Inconsistent identity federation across platforms increases the risk of privilege escalation, orphaned accounts, and misconfigured access controls (Chondamrongkul & Temdee, 2013).

Without centralized identity governance, administrators may create redundant accounts or assign excessive permissions across environments. Such mismanagement creates opportunities for attackers to exploit lateral movement pathways. A unified identity federation strategy, often integrated with enterprise directory services, becomes essential for minimizing access sprawl (Sabharwal & Shankar, 2013).

Zero-trust security models have gained prominence in addressing these challenges. Zero trust assumes no implicit trust within the network; every request for access must be authenticated, authorized, and continuously verified. Implementing zero-trust principles across multiple cloud providers demands centralized policy orchestration and identity verification mechanisms (Li et al., 2019).

Data Protection

Data protection in multi-cloud ecosystems involves encryption, classification, and lifecycle management. Cross-cloud encryption standards may vary, leading to inconsistencies in cryptographic implementation. Additionally, encryption key management becomes fragmented when each provider operates separate key management services (Hirai et al., 2020).

Centralized key management strategies reduce this fragmentation. Enterprises increasingly adopt unified key management platforms that integrate across cloud environments to ensure consistent encryption policies. Data classification systems further enhance protection by categorizing information based on sensitivity and regulatory requirements, thereby enabling automated enforcement of encryption and access controls (Chondamrongkul, 2016).

Secure data migration between clouds presents additional challenges. During transit, data must be protected against interception and unauthorized access. Secure transfer protocols, encrypted tunnels, and integrity verification mechanisms are essential for maintaining confidentiality (Mishra et al., 2015).

Misconfiguration Risks

Misconfigurations remain one of the leading causes of cloud security breaches. Publicly exposed storage buckets, improperly configured firewalls, and overly permissive access policies can create significant vulnerabilities. In multi-cloud environments, the risk is amplified because administrators must manage multiple configuration models simultaneously (Khan et al., 2019).

Automated configuration scanning tools play a crucial role in mitigating these risks. Cloud Security Posture Management systems continuously monitor configurations against predefined security baselines and compliance frameworks. Automated remediation workflows can correct deviations before they are exploited (Raj & Raman, 2018).

Network Security

Multi-cloud networking increases the attack surface significantly. Inter-cloud traffic, API endpoints, hybrid connections to on-premises infrastructure, and distributed workloads create complex network topologies. Ensuring secure communication across these environments requires robust network segmentation and encryption (Mitrovic et al., 2016).

Software-defined networking (SDN) technologies enable centralized network policy control across environments. Micro-segmentation strategies isolate workloads, limiting lateral movement opportunities for attackers. Secure Virtual Private Networks (VPNs) and encrypted communication channels further protect data in transit between cloud platforms (Li et al., 2019).

Automation in Multi-Cloud Enterprise Platforms

Automation is the backbone of secure multi-cloud management. Human-driven processes are prone to error, especially in complex, distributed environments. Automated provisioning, configuration, and compliance enforcement reduce operational risk and enhance scalability (Sousa et al., 2016).

Infrastructure as Code (IaC)

Infrastructure as Code enables enterprises to define cloud resources using declarative configuration files rather than manual setup. Tools provided by HashiCorp (Terraform) and Red Hat (Ansible) support consistent infrastructure provisioning across multiple cloud providers (Yang & Cheng, 2015).

Version-controlled infrastructure definitions ensure reproducibility and traceability. Changes to infrastructure can be audited, reviewed, and rolled back if necessary. Automated compliance validation can be integrated into IaC pipelines, ensuring that deployments adhere to security standards from inception (Obiuto et al., 2020).

CI/CD Pipelines and DevSecOps

Continuous Integration and Continuous Deployment pipelines streamline application delivery while embedding security into development workflows. Security testing tools, including Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and container image scanning, are integrated directly into pipelines (Rho & Vasilakos, 2018).

Containerization and Orchestration

Containerization abstracts applications from underlying infrastructure, enabling portability across cloud environments. Platforms such as Kubernetes orchestrate containerized workloads, offering self-healing capabilities, automated scaling, and rolling updates (Hirai et al., 2020).

Governance and Compliance Frameworks

Governance in multi-cloud environments serves as the structural backbone that aligns technological operations with regulatory mandates, internal security policies, and strategic business objectives. As enterprises distribute workloads across multiple cloud providers, maintaining consistent oversight becomes increasingly complex. Governance frameworks ensure that security controls, access policies, and operational procedures are not fragmented across platforms but instead operate within a coherent, standardized model. Without strong governance, multi-cloud adoption can quickly lead to policy drift, compliance gaps, and inconsistent risk management practices (Chondamrongkul & Temdee, 2013).

Regulatory compliance represents one of the most significant drivers of structured governance. Frameworks such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and ISO/IEC 27001 impose strict requirements on data handling, privacy protection, access control, and auditability. In a multi-cloud context, ensuring compliance is not a one-time certification exercise; it requires continuous verification that configurations, encryption standards, and access permissions remain aligned with regulatory expectations across all cloud environments. The distributed nature of multi-cloud infrastructures makes manual compliance monitoring impractical, thereby necessitating automated compliance enforcement mechanisms (Lal, 2016).

Centralized governance models have emerged as a practical solution to this challenge. These models consolidate monitoring, policy enforcement, and audit tracking into unified management platforms. Cloud Security Posture Management (CSPM) solutions continuously evaluate cloud configurations against predefined compliance baselines, identifying misconfigurations and policy violations in real time. Cloud Workload Protection Platforms (CWPP) extend

this oversight to runtime environments, monitoring workloads for vulnerabilities and suspicious activity. Security Information and Event Management (SIEM) systems aggregate logs and telemetry data from multiple clouds, enabling centralized visibility and correlation of security events (Mitrovic et al., 2016).
The shift from periodic audits to continuous compliance monitoring marks a critical advancement in governance practices. Traditional compliance models often relied on scheduled assessments conducted quarterly or annually. However, in dynamic multi-cloud environments where infrastructure is provisioned and decommissioned rapidly through automation, static audit cycles are insufficient. Continuous monitoring ensures that compliance status is evaluated in real time, and deviations from policy are immediately flagged. This proactive approach significantly reduces the window of vulnerability between misconfiguration and remediation (Raj & Raman, 2018).

Automation further enhances governance by embedding security controls directly into infrastructure provisioning workflows. Real-time alerting systems notify security teams of anomalies or policy violations as they occur, enabling rapid incident response. More advanced systems implement automated remediation, where predefined corrective actions are executed without human intervention. For example, if a storage resource is deployed without encryption enabled, an automated workflow can enforce encryption or revoke public access immediately (Sabharwal & Shankar, 2013).

Emerging Technologies Enhancing Security and Automation

The evolution of multi-cloud environments has catalyzed the integration of advanced technologies designed to enhance both security and automation. As infrastructures grow more complex and dynamic, traditional rule-based monitoring approaches struggle to keep pace with the scale and velocity of cloud operations. Emerging technologies—particularly artificial intelligence, machine learning, zero-trust architectures, and policy-driven automation—are reshaping how enterprises secure and manage distributed systems (Li et al., 2019).

Artificial Intelligence (AI) and Machine Learning (ML) are increasingly embedded within cloud security platforms to process vast volumes of logs, telemetry data, and behavioral signals generated across multiple cloud environments. Multi-cloud infrastructures produce enormous amounts of operational data, including API activity logs, network flow records, user authentication events, and workload performance metrics. Human analysts cannot realistically evaluate this data at scale. AI-driven security systems address this limitation by identifying anomalous behavior patterns, correlating disparate signals, and prioritizing high-risk events (Khan et al., 2019).

Machine learning models can detect subtle deviations from normal operational baselines, such as unusual login patterns, unexpected lateral network movement, or abnormal resource consumption. Predictive analytics extends this capability by identifying indicators of compromise before exploitation occurs. For example, abnormal privilege escalation attempts combined with suspicious API calls may trigger automated containment actions. By shifting from reactive alerting to predictive defense, AI-enhanced systems enable more proactive security postures (Obiuto et al., 2020).

Zero Trust Architecture (ZTA) has simultaneously emerged as a foundational principle for securing distributed cloud infrastructures. Traditional perimeter-based security models assumed trust within internal networks, but multi-cloud environments dissolve clear network boundaries. Zero trust operates under the assumption that no user, device, or workload should be implicitly trusted, regardless of its location. Every access request must be continuously authenticated, authorized, and validated based on contextual risk factors (Chondamrongkul, 2016).

In multi-cloud ecosystems, zero trust minimizes lateral movement opportunities for attackers. Micro-segmentation isolates workloads, while continuous identity verification ensures that access permissions are dynamically adjusted according to risk signals. Integration of zero trust principles with identity

federation systems strengthens consistency across diverse cloud platforms. This approach reduces reliance on network-based trust and shifts security focus toward identity-centric controls (Yang & Cheng, 2015).

Policy as Code further enhances governance and automation integration. By formalizing security policies in declarative code, organizations eliminate ambiguity in enforcement. Policy engines evaluate infrastructure configurations, access requests, and deployment artifacts against predefined compliance rules in real time. Unlike manual policy review processes, which may introduce inconsistency or delay, policy-driven automation ensures uniform enforcement across environments (Rho & Vasilakos, 2018).

Embedding security controls directly into deployment workflows prevents configuration drift and ensures that infrastructure remains aligned with organizational standards. For instance, deployment pipelines can automatically validate encryption settings, enforce network segmentation requirements, and restrict public exposure of services. This shift-left approach integrates governance into development processes, reducing the need for reactive remediation (Hirai et al., 2020). Collectively, these emerging technologies represent a transition from manual, reactive security management to intelligent, automated, and predictive governance models. AI-driven analytics enhance threat detection capabilities, zero trust redefines trust assumptions within distributed networks, and policy-as-code frameworks institutionalize consistent enforcement. As multi-cloud adoption continues to expand, the integration of these technologies will become essential for maintaining resilience, scalability, and regulatory compliance in increasingly complex enterprise ecosystems (Sousa et al., 2016).

Architectural Models for Secure Multi-Cloud

Designing secure multi-cloud enterprise platforms requires selecting an architectural governance model that balances centralized control with operational agility. As organizations expand across heterogeneous cloud ecosystems, architectural structure becomes a strategic decision rather than a technical preference. The way security policies, monitoring systems, automation pipelines, and operational responsibilities are distributed directly impacts risk exposure, scalability, compliance posture, and innovation velocity. Three dominant architectural models have emerged in practice: the centralized security hub model, the federated governance model, and the cloud-agnostic abstraction layer model. Each offers distinct advantages and trade-offs, and their effectiveness depends heavily on organizational maturity and regulatory context (Raj & Raman, 2018).

The centralized security hub model consolidates visibility, monitoring, and policy enforcement into a unified command structure. In this approach, security logs, alerts, telemetry data, and compliance metrics from multiple cloud providers—such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform—are aggregated into a centralized monitoring platform. This model emphasizes standardization and tight governance, often implemented through centralized Security Operations Centers (SOCs) and unified Security Information and Event Management systems. The primary strength of this architecture lies in its ability to provide cross-cloud visibility, rapid incident response, and consistent enforcement of security baselines. For highly regulated industries such as finance or healthcare, centralized oversight simplifies compliance auditing and risk reporting (Mitrovic et al., 2016).

However, the centralized model can introduce bottlenecks. As all policy decisions and security reviews pass through a single governance body, development velocity may slow. In large enterprises operating across multiple geographic regions, excessive centralization may also limit responsiveness to local regulatory variations or operational needs. Thus, while centralized oversight enhances control, it must be designed carefully to avoid constraining innovation (Sabharwal & Shankar, 2013).

Risks and Limitations

Despite the strategic advantages of multi-cloud adoption, significant risks and limitations persist. While automation and governance frameworks mitigate certain vulnerabilities, they cannot eliminate structural complexity inherent in managing multiple heterogeneous environments. Understanding these limitations is essential for realistic risk assessment and sustainable implementation (Lal, 2016).

One of the most prominent challenges is operational complexity. Each cloud provider offers distinct service catalogs, billing models, API interfaces, and security configurations. Managing these differences requires specialized expertise in multiple ecosystems. As organizations scale their multi-cloud presence, the demand for skilled cloud architects, DevSecOps engineers, and security analysts increases substantially. The global shortage of qualified cloud security professionals further intensifies this challenge. Without adequate expertise, misconfigurations and inconsistent governance practices become more likely (Khan et al., 2019).

Financial complexity also emerges as a limitation. While multi-cloud strategies are often justified by cost optimization, governance tooling, compliance auditing, cross-cloud monitoring systems, and data transfer charges can significantly increase operational expenditures. Organizations must invest in centralized security platforms, automation frameworks, and integration middleware to maintain consistent oversight. Furthermore, inter-cloud data movement may incur additional bandwidth and egress fees, complicating cost forecasting (Mishra et al., 2015).

Integration challenges represent another substantial risk. Interoperability between services across cloud providers is not always seamless. Differences in API structures, identity federation mechanisms, and networking architectures can complicate workload migration and data synchronization. Achieving consistent performance across distributed environments requires careful architectural planning. Latency issues may arise when workloads span geographically dispersed regions, particularly for real-time applications or data-intensive analytics systems (Yang & Cheng, 2015).

Security risks remain persistent even in highly automated environments. While Infrastructure as Code and automated compliance scanning reduce human error, architectural misjudgments cannot be fully automated away. Poor network segmentation design, weak identity federation strategies, or inadequate threat modeling can create systemic vulnerabilities. Automation enforces what is defined—but if policies are poorly designed, automation may propagate insecure configurations at scale (Chondamrongkul & Temdee, 2013).

Vendor ecosystem fragmentation is another subtle risk. Although multi-cloud adoption aims to reduce vendor lock-in, enterprises may inadvertently create dependency on third-party integration tools or abstraction platforms. Reliance on specialized multi-cloud management solutions can introduce new forms of dependency, potentially undermining the flexibility that multi-cloud strategies seek to achieve (Obiuto et al., 2020).

Future Directions

The future of secure and automated enterprise platforms in multi-cloud environments is shaped by increasing convergence between security intelligence, automation, and platform engineering. As enterprises expand digital transformation initiatives, manual oversight becomes insufficient. Emerging technologies aim to enable adaptive, intelligent, and autonomous infrastructure management (Rho & Vasilakos, 2018).

Autonomous security orchestration is poised to become a central capability. Rather than merely generating alerts, next-generation security systems will automatically analyze threat patterns, correlate multi-cloud telemetry data, and initiate remediation actions without human intervention. Machine learning algorithms will refine anomaly detection models continuously, improving predictive accuracy over time. AI-driven compliance mapping will dynamically align cloud configurations with evolving regulatory frameworks, reducing the burden of manual audits (Li et al., 2019).

Confidential computing represents another transformative direction. By leveraging hardware-based trusted execution environments, confidential computing enables data processing while encrypted in memory. This approach minimizes exposure even within cloud provider infrastructures. As regulatory pressures intensify, confidential computing may become a standard requirement for highly sensitive workloads in multi-cloud ecosystems (Hirai et al., 2020).

Secure multi-party computation techniques are also emerging, allowing multiple entities to compute on shared data sets without exposing raw information. This technology holds promise for collaborative analytics across organizational boundaries while preserving privacy and compliance. In multi-cloud contexts, secure multi-party computation can facilitate distributed processing without centralizing sensitive data (Sousa et al., 2016).

Platform engineering is expected to evolve into a core enterprise discipline. Internal developer platforms will increasingly incorporate automated security controls, cost optimization policies, and compliance guardrails by default. Rather than treating security as an external enforcement mechanism, future platforms will embed governance directly into developer workflows. This shift represents a move from reactive security to proactive, design-driven security integration (Raj & Raman, 2018).

III. CONCLUSION

Secure and automated enterprise platforms in multi-cloud environments represent a fundamental evolution in enterprise IT architecture. The transition from single-provider reliance to distributed cloud ecosystems introduces unprecedented flexibility, scalability, and innovation potential. Organizations gain resilience against outages, access to specialized services, and improved negotiation leverage across providers. However, these benefits are accompanied by increased architectural complexity, governance challenges, and expanded attack surfaces.

Success in multi-cloud environments requires more than technological adoption; it demands strategic alignment between security architecture, automation frameworks, and organizational culture. Standardized identity governance ensures consistent access control across environments. Infrastructure as Code and DevSecOps pipelines embed security into deployment workflows. Zero-trust models redefine network trust assumptions, while centralized visibility platforms enhance cross-cloud monitoring. At the same time, organizations must acknowledge inherent risks, including operational complexity, integration difficulties, financial overhead, and skill shortages. Automation is not a substitute for sound architectural design. It amplifies defined policies—good or bad. Therefore, sustainable success depends on thoughtful governance design, continuous skill development, and adaptive risk management.

The future of enterprise computing does not merely depend on distributing workloads across multiple cloud providers. It depends on mastering secure automation, embedding policy-driven governance into every layer of infrastructure, and transforming complexity into strategic resilience. Organizations that approach multi-cloud architecture as a disciplined, security-first platform engineering initiative will convert potential vulnerability into competitive advantage.

REFERENCE

1. Chondamrongkul, N., & Temdee, P. (2013). Multi-cloud computing platform support with model-driven application runtime framework. 2013 13th International Symposium on Communications and Information Technologies (ISCIT), 715-719.
2. Khan, G., Sengupta, S., & Sarkar, A. (2019). Dynamic service composition in enterprise cloud bus architecture. Int. J. Web Inf. Syst., 15, 550-576.
3. Mishra, D., Das, A.K., & Mukhopadhyay, S. (2015). An anonymous and secure biometric-based enterprise digital rights management system for mobile environment. Secur. Commun. Networks, 8, 3383-3404.

4. Li, Z., Guo, H., Wang, W.M., Guan, Y., Barenji, A.V., Huang, G.Q., McFall, K.S., & Chen, X. (2019). A Blockchain and AutoML Approach for Open and Automated Customer Service. IEEE Transactions on Industrial Informatics, 15, 3642-3651.
5. Obiuto, N.C., Mary, U.U., & ThankGod, O.O. (2020). Conceptual Model improving Endpoint Security across mixed Operating System Environments. International Journal of Multidisciplinary Research and Growth Evaluation.
6. Yang, S., & Cheng, I. (2015). Design Issues of Trustworthy Cloud Platform Based on IP Monitoring and File Risk. 2015 IEEE Fifth International Conference on Big Data and Cloud Computing, 110-117.
7. Mitrovic, D., Ivanović, M., Bordini, R.H., & Bădică, C. (2016). Jason Interpreter, Enterprise Edition. Informatica (Slovenia), 40.
8. Rho, S., & Vasilakos, A.V. (2018). Intelligent collaborative system and service in value network for enterprise computing. Enterprise Information Systems, 12, 1 - 3.
9. Sabharwal, N.C., & Shankar, R. (2013). Apache CloudStack Cloud Computing.
10. Hirai, S., Tojo, T., Seto, S., & Yasukawa, S. (2020). Automated Provisioning of Cloud-Native Network Functions in Multi-Cloud Environments. 2020 6th IEEE Conference on Network Softwarization (NetSoft), 1-3.
11. Sousa, G.N., Rudametkin, W., & Duchien, L. (2016). Automated Setup of Multi-cloud Environments for Microservices Applications. 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), 327-334.
12. Chondamrongkul, N. (2016). Model-driven framework to support evolution of mobile applications in multi-cloud environments. Int. J. Pervasive Comput. Commun., 12, 332-351.
13. Raj, P., & Raman, A. (2018). Automated Multi-cloud Operations and Container Orchestration.
14. Lal, K. (2016). Impact of Multi-Cloud Infrastructure on Business Organizations to Use Cloud Platforms to Fulfill Their Cloud Needs. American Journal of Trade and Policy.
15. Parimi, S. S. (2018). Exploring the role of SAP in supporting telemedicine services, including scheduling, patient data management, and billing. SSRN Electronic Journal.
16. Parimi, S. S. (2018). Optimizing financial reporting and compliance in SAP with machine learning techniques. SSRN Electronic Journal. Available at SSRN 4934911.
17. Parimi, S. S. (2019). Automated risk assessment in SAP financial modules through machine learning. SSRN Electronic Journal. Available at SSRN 4934897.
18. Parimi, S. S. (2019). Investigating how SAP solutions assist in workforce management, scheduling, and human resources in healthcare institutions. IEJRD – International Multidisciplinary Journal, 4(6).
19. Mandati, S. R. (2019). The basic and fundamental concept of cloud balancing architecture. South Asian Journal of Engineering and Technology, 9(1), 4.
20. Mandati, S. R. (2019). The influence of multi cloud strategy. South Asian Journal of Engineering and Technology, 9(1), 4.
21. Illa, H. B. (2016). Dynamic resource allocation for cloud-based applications using machine learning. International Journal of Scientific Development and Research (IJSDR).
22. Illa, H. B. (2016). Performance analysis of routing protocols in virtualized cloud environments. International Journal of Science, Engineering and Technology, 4(5).
23. Illa, H. B. (2018). Comparative study of network monitoring tools for enterprise environments (SolarWinds, HP NNMi, Wireshark). International Journal of Trend in Research and Development, 5(3), 818–826.
24. Illa, H. B. (2019). Design and implementation of high-availability networks using BGP and OSPF redundancy protocols. International Journal of Trend in Scientific Research and Development.