Matthew Fernandes, 2020, 8:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

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

Salesforce AI-Powered Service Cloud for Hybrid Unix Disaster Recovery with Commvault and Veritas Cluster Server

Matthew Fernandes
St. Augustine's Global University

Abstract - The rising dependence on Salesforce Service Cloud for mission-critical customer service operations has made disaster recovery a strategic priority for modern enterprises. Hybrid Unix environments—spanning AIX, Solaris, and Linux—introduce both opportunities and challenges for ensuring continuous availability of CRM workloads. This review explores how AI-driven automation, integrated with Commvault's intelligent backup and recovery features and Veritas Cluster Server's high availability capabilities, can deliver resilient disaster recovery strategies for Salesforce Service Cloud. It begins by examining the evolution of hybrid disaster recovery frameworks and the expanding role of Salesforce Service Cloud in enterprise continuity. Core features of Commvault, including policy-driven recovery and anomaly detection, are assessed alongside VCS's clustering and automated failover mechanisms. The review also highlights integration strategies that unify Service Cloud workflows with DR tools to enable proactive, AI-enhanced orchestration across hybrid infrastructures. Security, compliance, and governance considerations are evaluated in the context of GDPR, HIPAA, and SOX, emphasizing the importance of intelligent monitoring and auditability. Challenges such as integration complexity, performance bottlenecks, and organizational silos are analyzed, followed by future directions including autonomous AI-powered pipelines, cloud-native DR, and emerging trends such as DevSecOps adoption and low-code/no-code orchestration. The article concludes that integrating Salesforce Service Cloud with Commvault and Veritas Cluster Server establishes a robust foundation for AI-powered disaster recovery in hybrid Unix ecosystems, positioning enterprises to achieve long-term resilience and regulatory compliance.

Keywords - Salesforce Service Cloud, Commvault, Veritas Cluster Server, AI-powered disaster recovery, Hybrid Unix infrastructures, AIX, Solaris, Linux, Intelligent CRM resilience, High availability, Backup and recovery, Compliance and governance, DevSecOps, Cloud-native DR.

I. INTRODUCTION

Context of Salesforce Service Cloud in Modern Enterprise CRM Ecosystems

Salesforce Service Cloud has established itself as a cornerstone in enterprise CRM strategies, providing omni-channel case management, workflow automation, and AI-powered analytics that enhance customer engagement. For industries such as healthcare, financial services, and government, Service Cloud supports mission-critical operations where downtime is directly linked to customer dissatisfaction, revenue loss, and regulatory risks. Its scalability and adaptability make it a natural fit for enterprises transitioning toward hybrid IT models.

Importance of AI-Driven Disaster Recovery Strategies for Mission-Critical Workloads

The increasing reliance on digital services has amplified the importance of disaster recovery (DR) frameworks that go beyond traditional backup and restore methods. AI introduces predictive capabilities that can detect anomalies, forecast potential system failures, and initiate proactive countermeasures. For Salesforce Service Cloud, AI-driven DR ensures continuity of customer service processes, enabling enterprises to maintain service-

level agreements and protect brand trust even during disruptions.

Growing Role of Hybrid Unix/Linux Infrastructures

Hybrid Unix infrastructures—spanning AIX, Solaris, and Linux systems—remain a backbone of enterprise computing. They combine the reliability of on-premises environments with the flexibility of cloud services, creating an ecosystem well-suited for mission-critical workloads. However, the heterogeneity of these systems presents unique challenges for disaster recovery. Ensuring seamless integration of Salesforce Service Cloud with backup and clustering tools across these environments requires intelligent orchestration that balances resilience, performance, and compliance.

Scope and Objectives of the Review

This review aims to evaluate how Salesforce Service Cloud, when combined with Commvault and Veritas Cluster Server, can enable intelligent, AI-driven disaster recovery within hybrid Unix ecosystems. It discusses the evolution of DR strategies, examines the architecture and features of each component, and analyzes security, compliance, and governance considerations. The review also highlights challenges, emerging trends, and future directions, offering enterprises a roadmap to resilient CRM continuity in increasingly complex IT landscapes.

II. BACKGROUND AND FOUNDATIONS

Evolution of Disaster Recovery in Hybrid Infrastructures

Disaster recovery has evolved dramatically over the past two decades. In the early days, enterprises relied on tape-based backup systems that were often slow, labor-intensive, and prone to data loss. These traditional methods provided basic recovery but lacked the flexibility and speed required by modern digital businesses. The shift toward virtualization and cloud computing introduced new paradigms for disaster recovery, including cloud replication, continuous data protection, and near-instantaneous failover. In hybrid Unix/Linux environments, disaster recovery has become even more critical as organizations continue to operate mission-critical workloads on platforms like AIX and Solaris while simultaneously adopting cloud-native services. Modern DR frameworks in these contexts must integrate on-premises resilience with cloud-enabled recovery, balancing cost, performance, and compliance requirements.

Role of Salesforce Service Cloud in Enterprise Continuity

Salesforce Service Cloud has become a central platform for enterprise customer service, managing omni-channel communications, case resolution, and knowledge management. For organizations in sectors like banking, healthcare, and telecommunications, uninterrupted service delivery is essential to maintaining customer trust and operational efficiency. When disruptions occur—whether due to infrastructure failures, cyberattacks, or natural disasters—the Service Cloud is often the first system affected, directly impacting the customer experience. Service disruptions can cascade into reputational harm, regulatory penalties, and financial losses. As a result, ensuring continuity of Salesforce Service Cloud operations has become a top priority for enterprises. Disaster recovery solutions must therefore extend beyond infrastructure-level protections to integrate with CRM workflows, ensuring that customer-facing services remain functional even during crisis events.

Disaster Recovery Tools in Focus: Commvault and Veritas Cluster Server

Two key tools stand out in modern DR strategies for hybrid Unix environments: Commvault and Veritas Cluster Server (VCS). Commvault offers comprehensive enterprise backup, recovery, and replication, enabling organizations to protect data across heterogeneous systems and cloud platforms. Its integration with AI allows anomaly detection in backup datasets, which reduces the risk of corrupted recoveries. Veritas Cluster Server, on the other hand, provides clustering and high-availability mechanisms that automate failover between nodes, minimizing downtime during outages. Together, Commvault and VCS complement Salesforce Service Cloud by providing data protection, workload availability, and seamless recovery orchestration. Their synergy with AI-enabled features in Service

Cloud creates a resilient, intelligent framework for CRM continuity.

Salesforce Service Cloud: Architecture and AI Capabilities

Core Features of Service Cloud

Salesforce Service Cloud is designed as an enterprise-grade customer service platform that enables organizations to manage end-to-end customer interactions efficiently. Its architecture is built on Salesforce's multi-tenant cloud infrastructure, providing scalability, security, and reliability. At its core, Service Cloud supports omni-channel engagement, enabling agents to handle interactions across phone, email, chat, messaging apps, and social media from a unified interface. Case management is central to the platform, automating the tracking, escalation, and resolution of customer issues. Workflow automation streamlines repetitive tasks, while integrated analytics provide managers with real-time visibility into customer service performance. The platform also leverages a knowledge base for self-service and guided resolution, helping organizations reduce case volumes while improving customer satisfaction. Real-time dashboards, customizable reports, and integrated collaboration tools ensure that customer service teams can operate with both speed and precision.

AI-Driven Enhancements

The integration of artificial intelligence has significantly expanded the capabilities of Service Cloud. Salesforce Einstein, the AI engine within the platform, empowers organizations with predictive and proactive service intelligence. Einstein AI assists agents by recommending next best actions, predicting case resolution times, and identifying high-priority incidents before they escalate. In disaster recovery contexts, these AI features become particularly valuable. For example, during a system outage or failover event, AI-driven escalation rules ensure that critical cases are prioritized and routed to the most capable agents. Predictive analytics help organizations anticipate surges in customer inquiries following disruptions, allowing them to allocate resources proactively. Moreover, Einstein AI integrates with monitoring and disaster recovery tools, creating intelligent workflows where infrastructure failures trigger automated alerts, CRM case creation, and guided recovery steps. These AI-driven enhancements transform Service Cloud from a reactive service management platform into an intelligent orchestration hub capable of sustaining business continuity during crises.

Commvault for Intelligent Backup and Recovery

Commvault Overview

Commvault has long been recognized as a leader in enterprise data protection, offering an extensive suite of solutions for backup, recovery, archiving, and replication. Its architecture is designed to address the needs of hybrid environments, spanning on-premises Unix/Linux systems, private data centers, and multi-cloud platforms. Unlike traditional backup systems that rely on rigid scheduling, Commvault enables continuous and incremental data capture, ensuring minimal recovery point objectives (RPOs). Its policy-driven architecture allows organizations to tailor protection schemes based on workload criticality, data sensitivity, and compliance requirements. By integrating with diverse infrastructures—including AIX and Solaris—Commvault provides consistent and reliable data protection across heterogeneous enterprise landscapes.

Intelligent Features for Salesforce DR

Commvault's intelligence-driven features make it particularly effective for supporting disaster recovery in Salesforce Service Cloud ecosystems. Automated policy enforcement ensures that customer data and case records are consistently protected without manual oversight. Its AI-driven anomaly detection identifies irregularities in backup datasets, which may signal ransomware attacks, data corruption, or incomplete recovery points. This proactive approach prevents faulty recoveries that could compromise Service Cloud operations. Furthermore, Commvault enables rapid recovery at scale, restoring critical Salesforce data across distributed environments while minimizing downtime. Integration with Salesforce APIs allows seamless protection of metadata and configurations, ensuring that both data and platform settings can be restored in a disaster scenario.

Integration With Hybrid Unix Environments

One of Commvault's greatest strengths lies in its ability to protect data across hybrid Unix/Linux infrastructures. For organizations running mission-critical applications on AIX or Solaris, Commvault ensures that both structured and unstructured data are backed up and recoverable in near real time. In multi-cloud deployments, it provides unified visibility and orchestration across backup repositories, making it easier for IT teams to maintain resilience. By integrating Commvault's backup intelligence with Salesforce Service Cloud, enterprises gain a holistic disaster recovery framework where infrastructure-level data protection aligns with CRM continuity, ensuring uninterrupted service delivery.

Veritas Cluster Server for High Availability

Overview of Veritas Cluster Server (VCS)

Veritas Cluster Server (VCS) is a proven enterprise solution for clustering and high availability, widely used in mission-critical environments where downtime is unacceptable. At its core, VCS provides a mechanism to monitor applications, services, and infrastructure components across multiple nodes and initiate automated failover when a failure is detected. Unlike simple redundancy solutions, VCS offers sophisticated dependency management, ensuring that interconnected services restart in the correct sequence during recovery. Its flexibility supports a wide range of workloads, including databases, middleware, and CRM platforms, across diverse Unix/Linux systems. By offering centralized management, fault detection, and failover automation, VCS reduces the complexity of maintaining business continuity in hybrid infrastructures.

VCS in Hybrid Unix Disaster Recovery

In hybrid Unix environments where AIX and Solaris coexist with modern Linux and cloud platforms, VCS plays a pivotal role in orchestrating disaster recovery. It ensures continuous availability of mission-critical applications by enabling failover across both on-premises and cloud-based nodes. For Salesforce Service Cloud, this means that supporting infrastructure—such as middleware, APIs, and integration services—can remain operational even during outages. VCS clustering allows organizations to create geographically distributed failover clusters, enhancing resilience against regional disasters. Its ability to integrate with multi-cloud ecosystems also extends Service Cloud reliability, ensuring consistent customer engagement regardless of infrastructure disruptions.

AI-Enhanced Monitoring and Automation

While VCS has traditionally been rule-based, modern deployments increasingly leverage AI-driven enhancements. Predictive analytics can detect early warning signs of node degradation, disk failures, or network bottlenecks before they trigger outages. AI-based resource balancing ensures workloads are distributed optimally during failover, preventing performance degradation when systems operate in degraded modes. For Salesforce Service Cloud, this intelligent monitoring ensures that customer-facing workflows remain stable, even in the event of large-scale infrastructure disruption. By integrating AI insights with automated clustering, VCS creates a more adaptive and self-healing disaster recovery framework, aligning closely with enterprise goals for resilience and uptime.

Integration of Salesforce Service Cloud, Commvault, and VCS

End-to-End Disaster Recovery Architecture

The integration of Salesforce Service Cloud with Commvault and Veritas Cluster Server (VCS) forms a cohesive disaster recovery (DR) framework designed for hybrid Unix infrastructures. At the architectural level, Commvault manages intelligent data protection and recovery, while VCS ensures high availability through clustering and failover automation. Salesforce Service Cloud acts as the orchestrating CRM layer, where customer-facing processes continue with minimal disruption. During an incident, monitoring tools trigger alerts that flow into Service Cloud, initiating predefined recovery workflows. Commvault restores critical data, while VCS shifts application workloads to standby nodes, ensuring uptime. This end-to-end architecture leverages AI-driven orchestration to shorten recovery time objectives (RTO) and recovery point objectives (RPO), safeguarding business continuity.

Workflow Automation in Hybrid Environments

One of the most valuable aspects of this integration is workflow automation across heterogeneous Unix and cloud systems. Service Cloud's case management and AI-powered routing can automatically generate tickets when anomalies are detected, linking them directly to recovery actions. For example, if Commvault identifies corrupted backup data, Service Cloud can escalate the issue to the appropriate IT team while simultaneously initiating corrective workflows. Similarly, when VCS executes a failover, Service Cloud can log the event as a case, ensuring transparency and traceability. This automation bridges the gap between infrastructure recovery and CRM continuity, enabling IT and business units to work from a unified platform.

Case Study Scenarios

In financial services, downtime during a trading session can result in significant financial losses. With this integrated framework, Commvault ensures rapid restoration of transaction data, VCS provides seamless application failover, and Service Cloud maintains uninterrupted customer communication. In healthcare, patient record availability is critical. The combined solution allows medical staff to access records even during infrastructure outages, with AI-driven Service Cloud workflows escalating recovery events in real time. These scenarios demonstrate how the integration not only minimizes downtime but also protects trust, compliance, and customer satisfaction in sectors where service continuity is paramount.

Security, Compliance, and Governance

Security Challenges in Hybrid DR

Hybrid disaster recovery introduces unique security challenges as data flows between on-premises Unix environments, public clouds, and Salesforce Service Cloud. During replication and failover, sensitive customer information may be exposed to unauthorized access if not properly encrypted. Authentication and authorization become more complex across multi-cloud pipelines, requiring integration of identity management solutions such as LDAP, Active Directory, or modern IAM platforms. Misconfigurations can also create vulnerabilities that attackers may exploit during recovery operations. Moreover, insider threats remain a concern when administrators have broad access privileges across backup, clustering, and CRM layers. To mitigate these risks, organizations must adopt zero-trust principles, enforce least-privilege access, and apply continuous monitoring to detect anomalies during disaster recovery events.

Compliance With Regulations

Enterprises in regulated industries must align their disaster recovery strategies with strict compliance requirements. Regulations such as GDPR in Europe, HIPAA in healthcare, and SOX in financial services mandate secure handling of customer and operational data. Commvault supports compliance by offering encryption, immutable backups, and automated retention policies, ensuring that recovery operations preserve data integrity and privacy. Veritas Cluster Server complements this by maintaining uptime for critical workloads, reducing regulatory risks associated with downtime. Salesforce Service Cloud further strengthens compliance by providing auditable case histories, automated escalation logs, and secure communication channels. Together, these tools create a framework that not only enables resilience but also demonstrates adherence to industry standards during audits.

Intelligent Monitoring and Auditability

AI-driven monitoring introduces a higher level of intelligence in security and governance. By analyzing backup patterns, Commvault can detect anomalies such as sudden spikes in data changes, which may indicate ransomware attacks. VCS integrates predictive monitoring to identify potential node failures before they occur, while Salesforce Service Cloud captures every recovery-related event as an auditable record. These audit trails provide transparency for internal governance and external compliance audits. Intelligent dashboards consolidate insights across CRM, backup, and clustering layers, enabling executives to track security posture and recovery readiness in real time. This holistic approach ensures that disaster recovery not only restores services but also strengthens the enterprise's governance framework.

Challenges and Limitations

Integration Complexity

One of the major challenges enterprises face in deploying Salesforce Service Cloud disaster recovery with Commvault and Veritas Cluster Server is integration complexity. Each tool has its own architecture, configuration requirements, and dependencies, which must be carefully aligned to achieve seamless recovery. For example, Salesforce's cloud-native CRM workflows need to synchronize with Commvault's backup policies and VCS's clustering logic, often requiring custom connectors and middleware. In hybrid Unix environments, such as AIX, Solaris, and Linux, interoperability issues may arise due to OS-specific drivers, security modules, and networking layers. This complexity increases the likelihood of misconfigurations, leading to failed backups, incomplete failovers, or prolonged recovery times. Skilled cross-domain expertise is essential, yet difficult to maintain in many organizations.

Performance Bottlenecks

Performance limitations also emerge in large-scale deployments where CRM workloads span multiple data centers and cloud providers. Latency in data replication is a common bottleneck, particularly when recovery involves geographically distributed infrastructures. Commvault's AI-driven optimizations help reduce backup overhead, but real-time synchronization of Salesforce Service Cloud data still places significant strain on network bandwidth. Similarly, Veritas Cluster Server must continuously monitor system health, manage heartbeat signals, and orchestrate failovers, all of which require processing resources that can impact application performance. During peak disaster recovery scenarios, such bottlenecks may delay service restoration, undermining the promise of near-zero downtime. Enterprises need to strategically allocate resources, adopt containerized workloads, and use intelligent caching to minimize these performance issues.

Organizational Barriers

Beyond technical challenges, organizational barriers often limit the effectiveness of disaster recovery strategies. Many enterprises operate with siloed IT teams where Unix administrators, CRM specialists, and backup operators rarely collaborate closely. This lack of alignment leads to gaps in disaster planning, delayed response times, and inconsistencies in recovery testing. Furthermore, training requirements are substantial—administrators must master Salesforce workflows, Commvault backup policies, and VCS clustering strategies simultaneously. Resistance to change can also hinder adoption, particularly in industries with deeply entrenched legacy practices. Overcoming these barriers requires fostering a culture of shared responsibility, conducting regular cross-team drills, and aligning IT operations with business continuity priorities.

Future Directions

AI-Powered Autonomous DR Pipelines

The next evolution of Salesforce Service Cloud disaster recovery will likely focus on AI-powered autonomous pipelines capable of executing recovery processes with minimal human intervention. Emerging AI models can predict failure points based on telemetry data, initiate backups before disruptions occur, and trigger automated failovers using orchestration rules defined across Commvault and Veritas Cluster Server. Instead of relying on predefined runbooks, future pipelines will dynamically adapt to context, selecting the optimal recovery path based on workload priority, regulatory constraints, and infrastructure health. This shift toward self-healing systems reduces reliance on manual oversight while improving speed, accuracy, and resilience in hybrid Unix environments.

Cloud-Native Disaster Recovery Models

Cloud-native approaches are expected to redefine how enterprises handle CRM disaster recovery. Kubernetes-native clustering, containerized workloads, and service mesh technologies will play a critical role in ensuring resilience. By decoupling workloads from physical infrastructure, organizations can achieve greater portability across AIX, Solaris, Linux, and cloud environments. Commvault is already extending capabilities for container-native backups, while Veritas is enhancing compatibility with Kubernetes clusters. Salesforce Service Cloud can integrate with these models through APIs, enabling real-time backup

orchestration, stateful service restoration, and multi-cloud scaling. Cloud-native DR not only reduces hardware dependency but also aligns recovery strategies with the elastic, distributed nature of modern enterprise workloads.

Emerging Trends

Several emerging trends promise to further transform disaster recovery in hybrid Salesforce ecosystems. Low-code and no-code platforms are being explored for recovery orchestration, allowing business teams to define workflows without deep technical expertise. DevSecOps is gaining traction as a governance model that embeds security and compliance into every stage of recovery pipelines, reducing risks of regulatory violations. Additionally, advances in edge computing could enable localized Salesforce Service Cloud instances that improve resilience for industries like healthcare and finance where latency is critical. These trends indicate a future where disaster recovery becomes not just a technical safeguard but a strategic enabler of uninterrupted digital customer engagement.

III. CONCLUSION

Salesforce Service Cloud has emerged as a cornerstone of enterprise CRM operations, supporting mission-critical workflows across industries where downtime is unacceptable. As customer expectations for availability and responsiveness continue to rise, disaster recovery has become a strategic necessity rather than a supporting function. This review has explored how AI-powered enhancements, combined with advanced backup and clustering tools like Commvault and Veritas Cluster Server, enable organizations to strengthen resilience within hybrid Unix environments such as AIX, Solaris, and Linux. The integration of Commvault provides intelligent data protection through policy-driven recovery, anomaly detection, and hybrid cloud compatibility, ensuring that backup operations are both efficient and secure. Veritas Cluster Server complements this capability by orchestrating automated failovers and maintaining high availability across complex hybrid infrastructures. When connected to Salesforce Service Cloud, these technologies collectively create a disaster recovery framework that not only restores operations rapidly but also aligns with governance, compliance, and security priorities. AI-driven automation represents the most significant shift in disaster recovery strategies. Predictive failure detection, self-healing pipelines, and intelligent orchestration promise to minimize downtime while reducing reliance on manual interventions.

REFERENCES

1. Battula, V. (2014). A new era for CRM: Salesforce automation on a scalable, cloud-native Red Hat foundation. International Journal of Science, Engineering and Technology, 2(8), 5.
2. Battula, V. (2014). Beyond legacy: Modernizing with Red Hat and the open-source stack on hybrid platforms. International Journal of Science, Engineering and Technology, 2(2), 5.
3. Illa, H. B. (2013). Optimization of data transmission in wireless sensor networks using routing algorithms. International Journal of Current Science (IJCSPUB), 3(4), 17–25.
4. Illa, H. B. (2014). Design and simulation of low-latency communication networks for sensor data transmission. International Journal of Research and Analytical Reviews (IJRAR).
5. Illa, H. B. (2015). Secure cloud connectivity using IPsec and SSL VPNs: A comparative study. TIJER – International Research Journal, 2(5), a12–a35.
6. Illa, H. B. (2016). Bridging academic learning and cloud technology: Implementing AWS labs for computer science education. International Journal of Science, Engineering and Technology, 4(3), 9.
7. Illa, H. B. (2016). Comparative study of wired vs. wireless communication protocols for industrial IoT networks. International Journal of Scientific Research & Engineering Trends, 2(6).
8. Illa, H. B. (2016). Dynamic resource allocation for cloud-based applications using machine learning. International Journal of Scientific Development and Research (IJSDR).
9. Illa, H. B. (2016). Performance analysis of routing protocols in virtualized cloud environments. International Journal of Science, Engineering and Technology, 4(5).

10. Madamanchi, S. R. (2014). Solaris to Kubernetes: A practical guide to containerizing legacy applications on Linux. International Journal of Science, Engineering and Technology, 2(2), 6.
11. Madamanchi, S. R. (2014). The UNIX-to-Linux journey: A strategic guide for enterprise IT and cloud transformation. International Journal of Science, Engineering and Technology, 2(4), 5.
12. Mulpuri, R. (2014). The Sales Cloud evolution: Salesforce and the power of hybrid infrastructure for business growth. International Journal of Science, Engineering and Technology, 2(5), 5.
13. Battula, V. (2015). Next-generation LAMP stack governance: Embedding predictive analytics and automated configuration into enterprise Unix/Linux architectures. International Journal of Research and Analytical Reviews (IJRAR), 2(3), 47.
14. Madamanchi, S. R. (2015). Adaptive Unix ecosystems: Integrating AI-driven security and automation for next-generation hybrid infrastructures. International Journal of Science, Engineering and Technology, 3(2), 47.
15. Battula, V. (2016). Adaptive hybrid infrastructures: Cross-platform automation and governance across virtual and bare metal Unix/Linux systems using modern toolchains. International Journal of Trend in Scientific Research and Development, 1(1), 47.
16. Mulpuri, R. (2016). Conversational enterprises: LLM-augmented Salesforce for dynamic decisioning. International Journal of Scientific Research & Engineering Trends, 2(1), 47.
17. Mulpuri, R. (2016). Enhancing customer experiences with AI-enhanced Salesforce bots while maintaining compliance in hybrid Unix environments. International Journal of Scientific Research & Engineering Trends, 2(5), 5.
18. Gowda, H. G. (2016). Container intelligence at scale: Harmonizing Kubernetes, Helm, and OpenShift for enterprise resilience. International Journal of Scientific Research & Engineering Trends, 2(4), 1–6.
19. Battula, V. (2017). Unified Unix/Linux operations: Automating governance with Satellite, Kickstart, and Jumpstart across enterprise infrastructures. International Journal of Creative Research Thoughts (IJCRT), 5(1), 66.
20. Madamanchi, S. R. (2017). From compliance to cognition: Reimagining enterprise governance with AI-augmented Linux and Solaris frameworks. International Journal of Scientific Research & Engineering Trends, 3(3), 49.
21. Mulpuri, R. (2017). Sustainable Salesforce CRM: Embedding ESG metrics into automation loops to enable carbon-aware, responsible, and agile business practices. International Journal of Trend in Research and Development, 4(6), 47.
22. Kota, A. K. (2017). Cross-platform BI migrations: Strategies for seamlessly transitioning dashboards between Qlik, Tableau, and Power BI. International Journal of Scientific Development and Research (IJSDR), 2(63).
23. Kota, A. K. (2018). Dimensional modeling reimagined: Enhancing performance and security with section access in enterprise BI environments. International Journal of Science, Engineering and Technology, 6(2).
24. Kota, A. K. (2018). Unifying MDM and data warehousing: Governance-driven architectures for trustworthy analytics across BI platforms. International Journal of Creative Research Thoughts (IJCRT), 6(74).
25. Sasikanth Reddy Mandat. (2019). The influence of Multi Cloud Strategy. South Asian Journal of Engineering and Technology, 9(1), 1–4. https://doi.org/10.26524/sajet.3
26. Sasikanth Reddy Mandati. (2019). The basic and fundamental concept of cloud balancing architecture. South Asian Journal of Engineering and Technology, 9(1), 1–4. https://doi.org/10.26524/sajet.2