Research Article

Zero-Downtime Cloud Migration in Healthcare: Ensuring Uninterrupted Patient Care and Data Security

Raja Venkata Sandeep Reddy Davu

Senior Systems Engineer -Virtualization and cloud solutions, Texas
Rajavenkata.davu@gmail.com

_____

ABSTRACT

Cloud computing is replacing on-premises IT infrastructure in the healthcare business due to scalability issues and rising data volumes. This study discusses zero-downtime cloud migration in healthcare and how to secure data while maintaining patient care. Zero-downtime migration prevents clinical workflow and patient outcomes interruptions. This comprehensive healthcare cloud migration guide highlights improved disaster recovery, economic efficiency, and flexibility. In the planning phase, the study focuses on assessment, preparedness, strategic planning, and risk assessment. These migration methods include lift-and-shift, replatforming, and refactoring. Zero-downtime options like blue-green deployments, canary releases, and rolling updates are emphasised. A detailed healthcare case study describes zero-downtime migration methodologies and results. Moving data to the cloud creates severe security risks. The study mentions data breaches and GDPR and HIPAA compliance as security concerns. Encrypted data transfers, persistent monitoring, incident response, and best practices for protecting sensitive data are recommended. It also shows a secure data migration workflow to protect sensitive data. Application availability, real-time data synchronisation, redundancy, and failover protocols are crucial to maintaining patient care during the transfer. The study emphasises user training and assistance to minimise clinical operational disturbances. It also provides a high availability cloud migration architecture diagram to visualise service continuity infrastructure. This study will examine the most important cloud migration tools and technologies, compare the most popular platforms and solutions, and stress how automation and orchestration may reduce downtime. Optimisation and monitoring following relocation, resource management, and performance improvement are covered. The study predicts cloud migration trends, issues, and solutions, including AI, ML, and edge computing. The conclusion summarises the main aspects and provides methods healthcare businesses might shift to the cloud more efficiently, taking into account future technological advances and ongoing improvement.

Key words: Zero-downtime migration, Healthcare, cloud migration, data security, patient care, virtualization, AI, edge computing, HIPAA compliance, cloud solutions.

_____

INTRODUCTION

A. Background on Cloud Migration in Healthcare

Cloud migration in healthcare involves migrating data, software, and other business components to the cloud [1]. On-premises infrastructure is unrestrained.

Big data analytics, AI, and ML are needed to improve operational efficiency and scalability, driving this change. Cloud solutions are being used by a sector that historically relied on physical servers and data centres to meet these expectations and respond to rapid technological advances in healthcare.

Cloud computing is popular in healthcare. Due to its flexibility, cost-effectiveness, and data management benefits, healthcare companies are migrating their IT infrastructure and apps to the cloud. Growing healthcare data, enhanced data analytics, and unified patient treatment regardless of location are driving this trend. Cloud technology lets healthcare firms store and analyse massive data volumes. Deployed 24/7/365 Electronic Hospital Records (EHR), telemedicine platforms, and patient management systems can be widely used [2]. Cloud computing improves patient care by enabling safer data interchange and real-time healthcare provider communication.

_____

B. Importance of Maintaining Uninterrupted Patient Care and Data Security During Migration

Healthcare organisations are concerned about maintaining patient care during cloud migration. Any interruption might cause treatment delays, misconceptions, and poor patient outcomes, therefore ongoing patient care is crucial. Therefore, healthcare providers should take great precautions to ensure clinical app and data access throughout relocation. Many methods are utilised to minimise downtime, including phased migration, blue-green deployment, and real-time data syncing. Cloud migration requires strict data protection. Healthcare data is sensitive since it includes patients' identities, residences, birthdates, medical records, and finances. The migration procedure requires protecting this data from breaches, illegal access, and loss. This requires advanced encryption methods, secure data transfer protocols, and comprehensive access controls. Healthcare standards must be followed to protect patient data and confidence. Cloud technologies in healthcare promote efficiency, scalability, and data management. A well-planned and executed cloud migration is necessary to maintain patient care and data protection.

THE NEED FOR CLOUD MIGRATION IN HEALTHCARE

A. Current Challenges in Healthcare IT Infrastructure

Healthcare IT infrastructure's on-premises systems have long severe challenges. The current healthcare systems are unable to expand due to the increasing demands they face. EHRs, medical imaging, and personalized treatment are driving healthcare data growth, making on-premises solutions unsuitable [3]. Maintaining and updating physical infrastructure requires large initial and continuing investments.

Scalability difficulties degenerate on-premises weaknesses. Healthcare organisations should assess IT traffic before a public health emergency or seasonal patient rush. On-premises solutions are too stiff to swiftly adjust capacity to meet changing demands. Rigidity may cause performance constraints that reduce the quality of patient care.

B. Benefits of Cloud Migration

Cloud migration is appealing due to its versatility, scalability, and cost. Dynamic resource scaling is a major benefit of cloud migration. Cloud technologies that allow on-demand computing capacity can help healthcare institutions handle variable workloads [4]. EHRs, medical imaging, and other essential patient data may be simply connected and processed due to its scalability, which is especially helpful when dealing with huge healthcare data volumes. Cloud migration improves business continuity and catastrophe recovery. Cloud providers offer advanced backup and recovery options to protect and restore data after a system failure or data loss. The healthcare business relies on patient data availability for effective and continuing treatment; therefore robustness is crucial. Cloud systems typically store data in several datacentres across regions. This ensures that data is accessible in the event of a datacenter failure.

Cloud migration reduces costs and operations. Moving to the cloud reduces the need for large on-premises equipment, saving capital expenditures. Healthcare organisations can use pay-as-you-go to avoid overprovisioning and match pricing to consumption. Thus, they will only pay for used resources. Software upgrades, security patches, and system maintenance are automated by cloud services, simplifying IT processes. Automation improves operational efficiency and frees IT staff to work on key projects. On-premises systems have limits and scalability difficulties, which is why healthcare businesses need to transition to the cloud. Disaster recovery, business continuity, flexibility, scalability, and cost effectiveness improve with cloud migration. Cloud technology can improve IT infrastructure management, handle expanding data volumes, and ensure high-quality patient care in healthcare.

PLANNING FOR ZERO-DOWNTIME CLOUD MIGRATION

A. Assessment and Readiness Evaluation

Ensure that IT infrastructure is ready for a zero-downtime cloud migration. Before migration begins, infrastructure must be assessed and locations needing repair. Analysis requires a thorough assessment of the IT infrastructure's hardware, software, network settings, and data storage systems. This analysis can identify legacy systems that are incompatible with cloud settings and estimate the cost of upgrading or replacing them. The most critical applications and data must be identified at this point. These components are essential to the healthcare organization's daily operations and cannot be done. By prioritising these key components, healthcare IT teams may relocate them without disrupting patient care. This stage classifies data by sensitivity and compliance to ensure transfer security.

B. Strategic Planning

After assessment and readiness evaluation, a migration strategy will be devised. Clear targets and timelines should be set in this plan to keep the migration on track. Before moving to the cloud, companies must set goals to improve scalability, data security, and operating costs. SMART (Specific, Measurable, Achievable, Relevant, Time-bound) goals specific, measurable, attainable, relevant, and time-bound are easier to track and manage. Timelines help organise migration activities and ensure each phase is completed on time. As a result, healthcare procedures are less likely to be stopped and better coordinated. Strategic planning requires stakeholder

participation. Get the IT department, healthcare providers, administrators, and third-party vendors engaged in the move to ensure everyone understands their roles. Regular updates and feedback loops are needed to stay open and handle any issues during the move.

C. Risk Assessment and Mitigation

A zero-downtime cloud migration plan should analyse and mitigate risks. Technical risks include network outages and data corruption. Organisational issues include change aversion and technical illiteracy. Healthcare IT teams should monitor risks early on to ensure a smooth transition. Risk mitigation and contingency measures are essential. Backup, recovery, transport encryption, and application failover mitigate risks. If a disruption occurs, activate backup systems, return to on-premises infrastructure, or notify management. Validate these plans in practice. Risk assessment, IT infrastructure evaluation, and strategic migration strategy are needed for a zero-downtime healthcare cloud migration. Assessing infrastructure, identifying important apps and data, setting concrete targets and timelines, consulting stakeholders, and creating solid mitigation plans can help healthcare organisations shift to the cloud without sacrificing patient care or data security.

MIGRATION STRATEGIES AND APPROACHES

A. Types of Cloud Migrations

Healthcare businesses must consider their goals when choosing a cloud migration plan. Main cloud migration types are replat forming, lift-and-shift, and refactoring.

Lift-and-Shift

The lift-and-shift technique moves data and programmes to the cloud with little architectural changes [5]. This is frequently the fastest and easiest cloud migration. Healthcare companies may prefer this method since it reduces complexity and early investment while optimising cloud scalability and cost. However, non-cloud-optimized software may lack cloud-native capabilities and cost more.

Replat forming

Replat forming, or "lift, tinker, and shift," optimises data and software during migration. These changes aim to increase cloud infrastructure usage without redesigning. A healthcare company may migrate to a managed cloud database provider or application components to save money and enhance efficiency [6]. Many companies use this fast, optimised technique.

Refactoring

Refactoring is the hardest cloud migration approach. Redesigning programmes for cloud-native capabilities and services is important. The application may need a complete redesign to be more robust, maintainable, and scalable. This technique takes time and money but improves performance, lowers operational expenses, and increases flexibility. Reorganising healthcare organisations requires consideration of resources, expertise, and advantages and downsides.

B. Zero-Downtime Techniques

During cloud migration, healthcare providers must prioritise patient care and data availability. Blue-green deployment, canary releases, and rolling updates help.

Blue-Green Deployment

Blue-green deployment has two complementary production environments, active and inactive. The green environment changes first during migrations or updates. Traffic changes from blue to green without delay after approval. If issues emerge, the previous setting can be restored, lowering risk. Blue-green deployment allows healthcare providers to update mission-critical apps and systems without disrupting care.

Canary Releases

A canary release is a gradual upgrade that commences with a small number of users or servers. This method allows health systems to test new ideas securely. A successful canary release steadily improves all users or servers. This proactive approach finds and resolves issues early, guaranteeing a smooth move. Canary releases are ideal for modernising EHRs and patient management systems that need uninterrupted access.

Rolling Updates

Rolling upgrades update servers or instances incrementally without downtime. Some instances are updated, others run. This allows certain instances to process requests, assuring continued service. Large healthcare applications and systems retain performance and availability throughout migration using rolling updates.

C. Case Study Example: Successful Zero-Downtime Migration in a Healthcare Setting

Major healthcare provider MedCare implemented zero-downtime migration. MedCare wanted to cloud-base its patient management system for scalability and security [7]. Blue-green deployment and replatforming were MedCare's migration plans. First, they examined its IT architecture and identified mission-critical apps and data that needed security. They set targets and timeframes after involving IT, healthcare, and third-party vendors in the planning process. MedCare built two identical environments: blue on-premises and green cloud during the transfer. They migrated and improved the patient management system in the green environment to meet performance and security standards. They moved traffic from blue to green when it was fully working and tested.

_____

This solution allowed MedCare to transfer data and services without downtime, ensuring patient access. Due to its improved disaster recovery and scalability, the new cloud-based system managed more patient data and reduced data loss [8]. To ensure a smooth cloud migration without downtime, healthcare businesses must choose the correct approach. Rolling upgrades, blue-green deployment, and canary releases provide robust data security and continuous service frameworks. These strategies improve patient care and operations, as shown by MedCare's migration.

ENSURING DATA SECURITY DURING MIGRATION
A. Data Security Challenges in Cloud Migration
Data breaches and loss are the biggest concerns when shifting healthcare data to the cloud. Healthcare data is highly vulnerable to breaches that could harm persons and organisations due to its sensitive personal and medical information. Data transported between contexts is vulnerable to risks. Unauthorised access, transfer interception, and misuse by internal and external parties must be prevented to maintain patient trust. Meeting healthcare laws like the EU's General Data Protection Regulation (GDPR) and the US's Health Insurance Portability and Accountability Act is another challenge [9]. These standards require strict PHI security. When transitioning to the cloud, healthcare companies must ensure that their security, documentation, and audit capabilities follow requirements. Failure to comply could cost the company fines and reputation.

B. Best Practices for Data Security
Encryption is a key cloud migration recommended practice. Data encryption at rest and in transit prevents unauthorized parties from reading intercepted data. SSL and AES are used to send sensitive data. HTTPS, SFTP, and VPNs can encrypt data travelling from on-premises to the cloud [10]. Data migration must be monitored to identify and resolve security risks. Strong monitoring tools and systems can detect unusual activity, attempted unauthorised access, and other security irregularities. Setting up an incident response plan is equally important. This approach should cover contacting affected parties, security breaches, and problem resolution. The healthcare company regularly practises incident response and updates its incident response plan to prepare for security issues. Careful planning and administration are required to ensure healthcare compliance during and after migration. Companies should document the migration process and audit their data security. Maintain data access, transfer, and security protocol records carefully. Engaging with regulators and pre-migration compliance evaluations helps identify gaps and improvement possibilities. After the migration, audits should confirm the new cloud environment meets regulations.
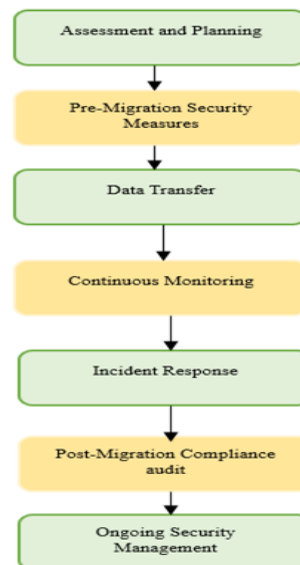

Figure 1: Secure Data Migration Workflow (Source: Self-Created)

MAINTAINING UNINTERRUPTED PATIENT CARE
A. Critical Factors for Uninterrupted Care
One of the most crucial aspects of cloud migration for healthcare is app availability and performance. Healthcare providers use many apps for patient data, diagnostics, treatment plans, and more [11]. These applications' downtime or performance degradation could delay diagnosis and treatment. Thus, programme dependencies and performance standards must be assessed before migration. These programmes must continue during the move to ensure patient care. Medical procedures are often interconnected. Any interruption can affect patient care and operational efficiency. Cloud migration must be carefully planned and executed to avoid

_____

disrupting vital processes. Migrations should be scheduled during off-peak hours, stakeholders should be informed of brief interruptions, and critical functions should have backup plans. Clinical staff must be involved in planning to identify their needs and potential pain areas during relocation.

B. Techniques for Maintaining Service Continuity

Synchronising data in real time is crucial to cloud service continuity. With this process, on-premises data changes are promptly reflected in the cloud. By synchronising the two settings, healthcare professionals may prevent data loss and ensure patients have the latest information. Database replication, distributed file systems, and real-time data streaming can help synchronise. Strong data synchronisation systems ensure reliable and consistent data for clinical decision-making and patient care [12]. Cloud migration strategies should include redundancy and failover to avoid service interruptions. Redundancy involves producing multiple copies of important data and programmes and storing them in different locations or cloud regions.

Failover systems seamlessly redirect traffic to redundant instances without harming end users. These methods can be implemented using load balancers, clustering, and automatic failover scripts. By having backup systems ready, healthcare institutions can ensure service availability and reliability. User training and assistance, often overlooked, are essential for cloud migration patient care. The healthcare organisation must train workers on any new systems or practices throughout the migration. This training must include daily routine adjustments and how to use programmes in the new cloud environment. Help desks, technical support teams, and extensive documentation can address changeover queries and concerns. By ensuring people are familiar with new technologies, interruptions can be avoided while productivity and care quality are maintained.
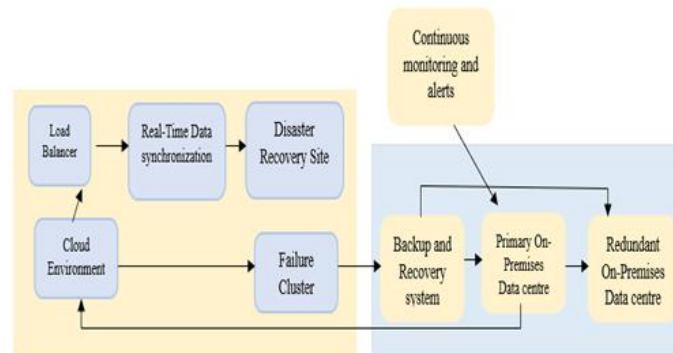

Figure 2: High Availability Architecture in Cloud Migration (Source: Self-Created)

TOOLS AND TECHNOLOGIES FOR CLOUD MIGRATION

A. Cloud Migration Tools

Cloud migration solutions make moving data, apps, and services from on-premises to cloud systems easy. Easy to track AWS and partner application migration progress. It helps businesses manage complex migrations by giving status and performance visibility. Software developed by Microsoft Azure to evaluate, plan, and execute cloud migrations. Server evaluation, database migration, and application updates are available. Google Cloud's Migrate for Compute Engine utility allows lift-and-shift migration of on-premises virtual machines to Google Cloud. Data transfer and database migration tools are included. AWS solution that replicates data and applications to the cloud continuously, enabling migrations with little downtime. It supports many source and destination settings and offers automated failover and recovery. Automatic real-time data replication to the cloud reduces migration time and downtime.

B. Selection Criteria Based on Healthcare Needs

Healthcare regulations like HIPAA must be followed for data migration safety. Access controls, encryption, and secure transfer should be accessible. Maintaining data integrity during migration is crucial. Tools should enable real-time data syncing and defect detection. The migration of many healthcare organisations' old systems requires expertise. Legacy systems should incorporate or adapt to tools.

The chosen technology should enable scalable migration to meet the company's growth and evolving cloud needs. User-friendly interfaces, adequate documentation, and competent vendor support aid migration and problem-solving.

C. Automation and Orchestration

Automation is key to minimising cloud migration downtime. Automating laborious tasks can improve migration efficiency, reduce human error, and ensure consistency. Automating configuration management, environment provisioning, and data replication reduces human involvement. This keeps services and applications functioning at high availability throughout migration, speeding things up. Orchestration tools efficiently coordinate migration procedures and operations to ensure correct sequence and integration. Migration procedures including virtual machine deployment, data synchronisation, and network configuration are automated and managed by these systems. Tools for orchestration include:

● Automates AWS service deployment and maintenance with templates for repeatable installations.
● Provides a single management layer for Azure resources, including deployment, management, and monitoring, automating deployment and configuration.
● Define and deploy Google Cloud resources using configuration files to automate infrastructure management.
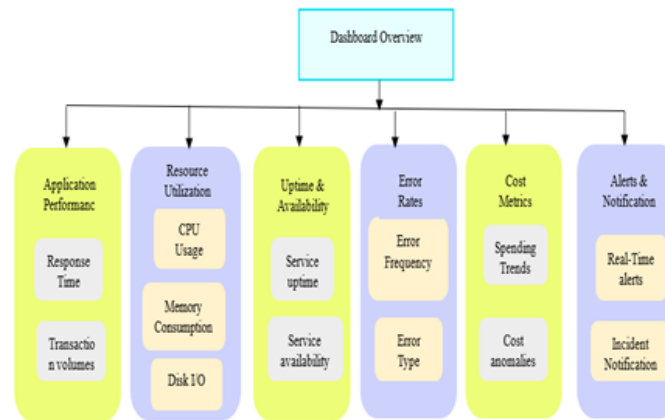

Figure 3: Comparison of Cloud Migration Tools (Source: Self-Created)

POST-MIGRATION OPTIMIZATION AND MONITORING

A. Performance Monitoring

Continuously evaluating performance once healthcare IT systems transition to the cloud is necessary to ensure operational requirements are met and patient care continues. Every major cloud provider includes monitoring solutions that operate with their systems. Stackdriver, Google Cloud Operations Suite, Azure Monitor, and AWS CloudWatch provide full cloud resource management.

IT departments can use these products' real-time monitoring, alerting, and logging to monitor databases, apps, and virtual machines [13]. Datadog, New Relic, and Dynatrace provide deeper insights into application performance, user experience, and infrastructure health. Such solutions often include automated anomaly detection, detailed reporting, and customisable dashboards. SolarWinds and PRTG Network Monitor make monitoring network error rate, latency, and bandwidth easy. Network monitoring is essential to avoid connectivity issues from disrupting healthcare. APM systems like Instana and AppDynamics show reaction times, transaction volumes, and error rates. These tools help find and fix performance issues to keep applications running properly.

B. Key Performance Indicators (KPIs) to Track

To optimise and monitor cloud performance, healthcare firms should monitor following KPIs:
● Application Response Time measures how long apps take to respond to user requests. High reaction times may indicate performance issues.
● Memory, disc I/O, and CPU consumption are resource utilisation metrics. Keep an eye on these factors to optimise resource allocation and avoid over- or under-provisioning.
● Uptime and availability Notify users when apps and services are operating. For uninterrupted patient care, healthcare facilities must be available.
● Error rate tracks application and service failures. High error rates can undermine healthcare app reliability, requiring quick examination.
● Rate of Return Includes cloud, resource, and exceptional charges. Tracking these KPIs optimises budgets and cloud spending.

C. Optimization Strategies

Optimising expenses and managing resources is key to a cost-effective cloud architecture. Accurate Size Adjusting resource sizes to meet workload expectations. Storage capacities, virtual machine sizes, and demand-based service scaling change. The environment scales without user effort or cost. Reserved instances or longer-term cloud contracts save more than on-demand. Cloud expenditure can be tracked using AWS Cost Explorer, Azure Cost Management, and Google Cloud Billing.

D. Continuous Improvement Practices

● Performance indicators and resource utilisation should be examined regularly to identify issues and make improvements.
● Proactive performance management requires end-user and IT feedback loops.
● Regularly compare cloud performance to industry standards and best practices to assure functionality.
● Use the latest cloud service, app, and security configuration updates for speed and security.

_____

FUTURE TRENDS AND CONSIDERATIONS

A. Emerging Technologies in Cloud Migration

Medical businesses may adjust their cloud migration tactics due to AI and ML. These technologies forecast workload, optimise resource allocation, and anticipate issues. AI-driven predictive analytics can help healthcare companies plan relocation, reduce transfer risk, and predict downtime. The best migration paths and real-time recommendations can be determined by AI using previous data and usage trends to ensure a smooth transfer without harming patient care or data security. To keep important healthcare apps responsive, AI algorithms can predict peak use and manage cloud resource allocation. As they learn and adapt, ML models can improve cloud infrastructure efficiency and robustness. Healthcare edge computing is increasing as a cloud migration tool. Moving data processing closer to sensors and medical equipment reduces cloud server use. This method increases healthcare app latency, efficiency, and real-time data processing. Edge computing helps healthcare practitioners access patient data faster, diagnose in real time, and preserve care continuity during network outages. Switching processing from the cloud to local edge devices improves system speed and reliability. Telemedicine systems with edge computing can offer low-latency, real-time video consultations, increasing patient and doctor experiences. Edge computing safeguards medical data by processing locally and transferring only essential data to the cloud.

B. Future Challenges and Solutions

Healthcare organisations using cloud solutions will encounter new problems that require ingenuity and proactivity. Multiple cloud providers and on-premises systems may complicate data integration, security, and management. Maintaining changing regulations is another difficulty. Healthcare providers must adapt to tightening global data protection standards to avoid fines. Cloud infrastructures will be difficult to upgrade and satisfy needs. Advanced orchestration and management solutions enable healthcare companies to manage hybrid and multi-cloud environments. These platforms simplify operations and integrate cloud and on-premises systems with unified control and visibility. Healthcare providers can follow rules via automated compliance management. For HIPAA and GDPR compliance, these technologies monitor cloud environments, give audit reports, and provide insights for addressing compliance issues. These solutions help companies comply and care for patients. Cybersecurity must be considered during cloud migration. Zero-trust architectures, constant threat monitoring, and AI-driven threat detection are essential to secure sensitive healthcare data from emerging cyber threats. Healthcare cloud migration can be transformed by AI, ML, and edge computing for efficiency, security, and patient care. To maximise cloud migration benefits, healthcare companies must anticipate and overcome challenges imaginatively. Effective cloud use, data protection, and patient care are expected.

CONCLUSION

Zero-downtime cloud migration is essential in healthcare. Migration requires patient care and data protection for confidence and efficiency.

Preparedness evaluation, strategy planning, and risk assessment and mitigation are recommended methods in this study. It also studied blue-green deployments, canary releases, and rolling updates with case studies. For data transmission security, encryption, constant monitoring, and compliance management were explored. User training, redundancy, failover, and real-time data synchronisation ensured service continuity during the migration. Following these best practices, using the right tools and technologies to monitor and optimise performance, and being flexible enough to adapt to new cloud migration trends and problems can help healthcare firms succeed. Healthcare IT system efficiency and reliability can improve with AI and edge computing development.

REFERENCE

[1]. A. Gopal and I. Garg, "Feasibility of supply chain on cloud," 2017.

[2]. J. A. Hernández, A. Hasayen, and J. Aguado, Cloud Migration Handbook Vol. 1: A Practical Guide to Successful Cloud Adoption and Migration. Lulu.com, 2019.

[3]. T. Parida, S. Pal, and A. Sarkar, "SaaS level database integration in cloud environment through database as a service," International Journal of Services Technology and Management, vol. 25, no. 3-4, pp. 236-266, 2019.

[4]. T. Laszewski and J. Williamson, Oracle Information Integration, Migration, and Consolidation. Packt Publishing Ltd, 2011.

[5]. S. Bhagavan, K. Alsultan, and P. Rao, "The case for designing data-intensive cloud-based healthcare applications," in SWH@ ISWC, 2018.

[6]. V. Medina and J. M. García, "A survey of migration mechanisms of virtual machines," ACM Computing Surveys (CSUR), vol. 46, no. 3, pp. 1-33, 2014.

[7].   R. Farmer, R. Jain, and D. Wu, Cloud Foundry for Developers: Deploy, Manage, and Orchestrate Cloud-Native Applications with Ease. Packt Publishing Ltd, 2017.

[8].   M. De Jong, A. van Deursen, and A. Cleve, "Zero-downtime SQL database schema evolution for continuous deployment," in 2017 IEEE/ACM 39th International Conference on Software Engineering: Software Engineering in Practice Track (ICSE-SEIP), pp. 143-152, IEEE, 2017.

[9].   J. Hai, C. Wang, X. Chen, T. O. Li, H. Cui, and S. Wang, "Fulva: Efficient live migration for in-memory key-value stores with zero downtime," in 2019 38th Symposium on Reliable Distributed Systems (SRDS), pp. 83-8309, IEEE, 2019.

[10].   T. Antohi, "Model for cloud migration cost," in 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 20-28, IEEE, 2019.

[11].   A. Nilsson, "Zero-downtime deployment in a high availability architecture: Controlled experiment of deployment automation in a high availability architecture," 2018.

[12].   S. B. Rathod and V. K. Reddy, "Ndynamic framework for secure VM migration over cloud computing," Journal of Information Processing Systems, vol. 13, no. 3, pp. 476-490, 2017.

[13].   A. Agarwal and S. Raina, "Live migration of virtual machines in cloud," International Journal of Scientific and Research Publications, vol. 2, no. 6, pp. 1-5, 2012.