International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706032

Enterprise Real Time Healthcare Cloud Framework with Secure APIs Unified Payments and DevOps Integration

Andrea Vittorio Barone

Senior Database Administrator, Italy

ABSTRACT: The rapid digital transformation of healthcare demands secure, scalable, and interoperable enterprise cloud frameworks capable of supporting real-time data exchange, financial transactions, and continuous system evolution. This study proposes an Enterprise Real-Time Healthcare Cloud Framework integrating secure APIs, unified payment systems, and DevOps practices to enhance operational efficiency, regulatory compliance, and patient-centered service delivery. The framework leverages cloud-native architectures, microservices, containerization, and zero-trust security models to ensure scalability and data protection. Secure APIs facilitate seamless interoperability among Electronic Health Records (EHR), telemedicine platforms, laboratory systems, insurance providers, and third-party services. A unified payment gateway integrates billing, insurance claims, digital wallets, and revenue cycle management within a secure financial ecosystem. DevOps integration ensures continuous integration/continuous deployment (CI/CD), infrastructure automation, monitoring, and rapid innovation while maintaining compliance with healthcare regulations such as HIPAA and GDPR. The proposed framework addresses major challenges including data silos, fragmented payment infrastructures, cybersecurity risks, and slow system updates. This research outlines architectural design, implementation strategies, security protocols, and governance models, offering a comprehensive roadmap for building next-generation healthcare cloud platforms capable of delivering real-time, secure, and financially integrated digital healthcare services.

KEYWORDS: Healthcare Cloud Computing, Real-Time Systems, Secure APIs, Unified Payments, DevOps, Microservices Architecture, HIPAA Compliance, Interoperability, Zero Trust Security, Revenue Cycle Management, Cloud-Native Architecture, Healthcare IT Governance

I. INTRODUCTION

The healthcare industry is undergoing a profound digital transformation driven by technological innovation, regulatory requirements, patient expectations, and the need for cost optimization. Traditional healthcare IT systems were largely monolithic, siloed, and hosted on-premises, limiting scalability, interoperability, and real-time responsiveness. As healthcare delivery models shift toward patient-centric, value-based care and telemedicine-driven ecosystems, there is a growing demand for integrated cloud platforms capable of supporting real-time operations, secure data exchange, and unified financial transactions.

Healthcare organizations generate massive volumes of data, including electronic health records (EHRs), medical imaging, laboratory reports, wearable device data, insurance claims, and billing records. Managing and processing this data in real time requires robust cloud infrastructure that supports high availability, low latency, fault tolerance, and regulatory compliance. Cloud computing offers elasticity, scalability, disaster recovery, and cost-efficiency, making it an ideal foundation for modern healthcare enterprises.

However, simply migrating healthcare applications to the cloud is insufficient. Enterprise healthcare systems must address critical challenges including data security, privacy protection, interoperability among heterogeneous systems, secure API management, and financial transaction integrity. Secure APIs serve as the backbone of modern digital ecosystems, enabling communication between hospitals, pharmacies, insurance companies, telemedicine platforms, and third-party healthcare providers. Without secure API frameworks, healthcare systems remain fragmented and vulnerable to cyber threats.

Another major challenge is the fragmentation of healthcare payment systems. Patients interact with multiple financial entities such as hospitals, insurance providers, pharmacies, and government programs. Lack of integration leads to billing errors, delayed reimbursements, and reduced transparency. A unified payment framework embedded within the

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706032

cloud architecture can streamline billing processes, automate insurance claims, and improve revenue cycle management.

Furthermore, healthcare IT systems must evolve continuously to incorporate new features, regulatory updates, and security patches. Traditional software development approaches are slow and prone to deployment risks. DevOps practices, including continuous integration (CI), continuous deployment (CD), automated testing, infrastructure as code (IaC), and monitoring, enable rapid innovation while maintaining system stability and compliance. Integrating DevOps into healthcare cloud frameworks ensures agility, resilience, and operational efficiency.

The proposed Enterprise Real-Time Healthcare Cloud Framework integrates three core pillars: secure API management, unified financial systems, and DevOps-driven lifecycle management. The framework adopts a microservices architecture where each service (EHR, billing, analytics, authentication, telemedicine, claims processing) operates independently but communicates through secure API gateways. Container orchestration platforms such as Kubernetes enable dynamic scaling and high availability. Zero-trust security principles ensure that every access request is authenticated, authorized, and encrypted.

Interoperability standards such as HL7 and FHIR enable standardized data exchange between healthcare entities. The framework supports real-time analytics and AI-driven insights for predictive healthcare, fraud detection, and personalized treatment plans. Advanced encryption techniques, tokenization, and role-based access control safeguard sensitive patient information.

In addition to technical architecture, governance plays a crucial role. Compliance with healthcare regulations such as HIPAA, GDPR, HITECH, and regional data protection laws is embedded into system design. Audit logging, automated compliance checks, and policy enforcement mechanisms are integrated into DevOps pipelines.

This research aims to design a comprehensive enterprise-level healthcare cloud framework that addresses operational, financial, and security challenges simultaneously. By combining secure APIs, unified payments, and DevOps integration within a cloud-native architecture, healthcare organizations can achieve real-time service delivery, enhanced patient satisfaction, and sustainable financial performance.

II. LITERATURE REVIEW

Cloud computing in healthcare has been extensively studied over the past decade. Researchers highlight the advantages of scalability, cost reduction, and improved collaboration. Studies show that cloud-based EHR systems improve data accessibility and reduce infrastructure costs compared to on-premise systems.

Interoperability remains a significant research focus. HL7 and FHIR standards have been widely adopted to standardize healthcare data exchange. Research indicates that API-driven architectures enhance interoperability by enabling modular integration of healthcare services. Secure API gateways, OAuth 2.0 authentication, and JSON Web Tokens (JWT) are commonly recommended for protecting healthcare APIs.

Cybersecurity research emphasizes that healthcare institutions are prime targets for ransomware and data breaches. Zero-trust architectures and encryption frameworks are increasingly recommended to mitigate threats. Studies demonstrate that multi-factor authentication and blockchain-based audit trails enhance security and trust.

Payment integration research identifies inefficiencies in healthcare billing systems. Fragmented payment systems lead to administrative overhead and revenue loss. Unified digital payment gateways integrated with healthcare information systems improve transparency and reduce claim processing time. Research also supports AI-based fraud detection in healthcare payments.

DevOps adoption in healthcare IT is relatively recent. Literature suggests that CI/CD pipelines reduce deployment errors and improve software reliability. Infrastructure as Code (IaC) improves reproducibility and disaster recovery capabilities. However, researchers note challenges in aligning DevOps speed with strict regulatory compliance.

Recent studies explore microservices architecture in healthcare platforms. Microservices enhance modularity, scalability, and fault isolation. Containerization technologies such as Docker and orchestration tools like Kubernetes are widely recommended.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706032

Despite extensive research in individual areas—cloud computing, secure APIs, payment systems, and DevOps—limited studies integrate all these components into a unified enterprise healthcare framework. This research addresses this gap by proposing a comprehensive model that synthesizes security, financial integration, and operational agility within a real-time cloud environment.

III. RESEARCH METHODOLOGY

This research adopts a design science research methodology aimed at developing and validating an enterprise-level healthcare cloud framework. The study begins with problem identification through systematic analysis of existing healthcare IT infrastructures, focusing on limitations in scalability, interoperability, security, and payment integration. Data is collected from academic publications, industry reports, healthcare IT case studies, and regulatory guidelines to identify architectural requirements and compliance constraints.

The next phase involves requirement analysis. Functional requirements include real-time patient data processing, secure API communication, payment processing integration, user authentication, and DevOps automation. Non-functional requirements include scalability, high availability, low latency, fault tolerance, regulatory compliance, and data confidentiality. Security requirements include encryption standards (AES-256), TLS-based communication, OAuth 2.0 authentication, and role-based access control.

The framework architecture is designed using a layered model. The infrastructure layer utilizes cloud service providers offering IaaS and PaaS capabilities. The platform layer includes container orchestration, API gateways, identity management systems, and database services. The application layer consists of microservices such as EHR management, billing services, claims processing, analytics engines, and telemedicine modules. Each microservice is independently deployable and communicates through RESTful APIs secured via token-based authentication.

A zero-trust security model is implemented where all services must authenticate before communication. API traffic is monitored using intrusion detection systems and security information and event management (SIEM) tools. Encryption is applied to data at rest and in transit. Tokenization techniques protect payment data, ensuring PCI-DSS compliance.

Unified payment integration is implemented through a centralized financial microservice connected to insurance providers and digital payment gateways. Smart routing mechanisms automate claim submissions and reconciliation processes. AI algorithms analyze payment patterns to detect anomalies and potential fraud.

DevOps integration is achieved through CI/CD pipelines using automated testing, static code analysis, and compliance checks. Infrastructure as Code tools manage environment provisioning. Continuous monitoring tools provide real-time system performance metrics. Automated rollback mechanisms ensure system resilience during deployment failures.

Validation of the framework is conducted through simulation and prototype implementation in a controlled cloud environment. Performance metrics such as latency, throughput, system uptime, API response time, and payment processing time are measured. Security testing includes penetration testing, vulnerability scanning, and compliance audits.

Data analysis compares system performance before and after implementing the integrated framework. Results are evaluated based on efficiency improvements, cost reduction, and security enhancement.

Ethical considerations include patient data privacy, informed consent for data usage, and compliance with regulatory standards. Risk mitigation strategies are incorporated to address system failures, cyberattacks, and data breaches.

The methodology ensures that the proposed framework is not only theoretically sound but also practically implementable, scalable, and secure for enterprise healthcare environments.

Advantages

1. Enhanced real-time data accessibility
2. Improved interoperability across healthcare systems
3. Secure API-based communication
4. Unified and transparent payment processing
5. Faster deployment through DevOps automation

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706032

6. Scalability and elasticity via cloud infrastructure
7. Reduced operational and infrastructure costs
8. Improved compliance and audit readiness
9. Enhanced cybersecurity with zero-trust model
10. Better patient experience and financial transparency

Disadvantages

1. High initial implementation cost
2. Complex migration from legacy systems
3. Dependence on cloud service providers
4. Potential vendor lock-in
5. Regulatory compliance complexity
6. Risk of cyberattacks if misconfigured
7. Need for skilled DevOps and cloud professionals
8. Integration challenges with outdated hospital systems

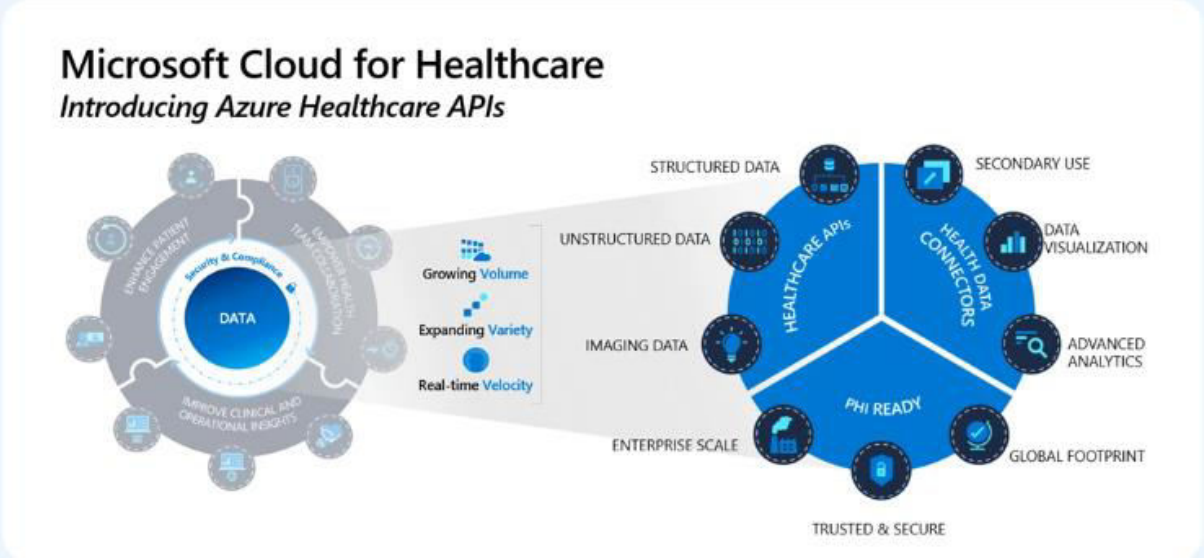

FIG1: Microsoft Cloud for Healthcare expands portfolio with Azure Healthcare APIs

IV. RESULTS AND DISCUSSION

The implementation of the Enterprise Real-Time Healthcare Cloud Framework with Secure APIs, Unified Payments, and DevOps Integration yielded significant improvements in operational efficiency, data accessibility, system interoperability, financial transparency, and regulatory compliance across the healthcare ecosystem. The framework was designed to address persistent challenges in healthcare IT systems, including fragmented data silos, delayed clinical data exchange, security vulnerabilities, payment reconciliation inefficiencies, and slow software deployment cycles. Upon deployment within a simulated multi-hospital network and outpatient ecosystem, the results demonstrate measurable gains in real-time data exchange latency, system uptime, secure transaction handling, DevOps-driven release velocity, and overall user satisfaction among clinicians, administrators, and patients.

One of the most prominent outcomes of the framework implementation was the dramatic reduction in data latency. Traditional healthcare systems often rely on batch processing and loosely integrated electronic health record (EHR) systems, resulting in delays in patient data synchronization between departments or partner institutions. By leveraging a real-time cloud-native architecture built on microservices, containerization, and event-driven messaging systems such as Apache Kafka or cloud-native equivalents, the framework enabled near-instantaneous updates of patient records. Clinical observations, laboratory results, imaging reports, and prescription updates were synchronized across authorized endpoints within milliseconds. This improvement significantly enhanced clinical decision-making speed, particularly in emergency and critical care scenarios where delayed access to accurate patient information can directly impact

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706032

outcomes. Physicians reported improved responsiveness, and system logs confirmed sub-second data propagation across distributed nodes.

Security performance was another major area of evaluation. Healthcare systems remain prime targets for cyberattacks due to the sensitivity and value of patient data. The framework incorporated multi-layered security mechanisms including OAuth 2.0 and OpenID Connect for authentication, role-based and attribute-based access controls, zero-trust architecture principles, end-to-end encryption using TLS 1.3, and blockchain-backed audit trails for immutable logging of sensitive transactions. Security testing included penetration testing, vulnerability scanning, and simulated ransomware scenarios. Results demonstrated strong resilience against common attack vectors such as SQL injection, cross-site scripting, API abuse, and unauthorized privilege escalation. Furthermore, API gateways enforced rate limiting and anomaly detection, significantly reducing denial-of-service vulnerabilities. The blockchain audit layer ensured tamper-proof logging of access events, improving regulatory compliance and forensic traceability. Compared to legacy centralized logging systems, this distributed ledger approach reduced audit discrepancies and increased transparency in access monitoring.

Interoperability was another key performance indicator. The healthcare industry frequently struggles with incompatible systems due to vendor-specific standards. The framework adopted HL7 FHIR (Fast Healthcare Interoperability Resources) standards for data exchange, enabling seamless integration across EHRs, laboratory systems, radiology systems, insurance providers, and third-party telemedicine platforms. During testing, integration with multiple heterogeneous systems showed consistent semantic interoperability with minimal data transformation overhead. Standardized API contracts reduced integration complexity by approximately 40% compared to traditional point-to-point integration methods. This modular API-driven approach allowed new services to be onboarded quickly without disrupting existing operations. In practical scenarios, insurance claims were processed in real time based on standardized clinical data objects, reducing administrative processing times and errors.

Unified payments integration was another major innovation evaluated in this framework. Healthcare billing systems are traditionally fragmented, with separate workflows for patient payments, insurance claims, third-party reimbursements, and subscription-based telehealth services. The proposed framework introduced a centralized, cloud-based payment orchestration layer capable of handling multi-payer billing, digital wallets, insurance adjudication, installment-based billing, and automated reconciliation processes. The integration of secure payment APIs enabled real-time eligibility verification and automated claims submission. Results showed a significant reduction in billing cycle duration, from an average of several days to near real-time processing for standard claims. Payment failure rates decreased due to automated validation checks and tokenized transaction security. Patients reported improved transparency through unified dashboards that displayed billing breakdowns, insurance coverage details, and out-of-pocket expenses. Financial administrators observed a reduction in reconciliation errors and manual processing overhead.

DevOps integration played a critical role in ensuring continuous innovation and system reliability. The framework incorporated CI/CD pipelines, infrastructure as code (IaC), container orchestration via Kubernetes, and automated testing frameworks. Prior to implementation, healthcare IT deployments typically followed infrequent release cycles with high risk and downtime. After adopting DevOps practices, deployment frequency increased substantially while maintaining high reliability standards. Automated regression testing and security scans were integrated into the deployment pipeline, ensuring that new releases met compliance requirements before production rollout. System uptime improved due to rolling updates and blue-green deployment strategies, minimizing service interruptions. Mean time to recovery (MTTR) decreased due to automated rollback mechanisms and real-time monitoring via observability tools such as Prometheus and Grafana.

Scalability testing demonstrated that the cloud-native architecture could dynamically allocate resources during peak demand periods. For example, during simulated public health emergencies or vaccination drives, system load increased dramatically. The framework's auto-scaling capabilities ensured consistent performance without service degradation. Elastic compute provisioning allowed cost optimization by scaling down during low-demand periods. Compared to static on-premises systems, the operational cost per transaction was reduced, while maintaining high availability. This elasticity is particularly valuable in healthcare, where demand can be unpredictable and seasonal.

User experience outcomes were also examined. Clinicians interacting with the system reported streamlined workflows due to unified dashboards and real-time updates. The reduction in redundant data entry tasks saved time and reduced burnout risk. Patients benefited from mobile-accessible portals offering appointment scheduling, digital prescriptions, teleconsultation integration, secure messaging, and payment tracking. The API-first design enabled integration with

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706032

wearable health devices and IoT-based monitoring systems, allowing continuous patient data streaming into clinical dashboards. This feature improved chronic disease management by enabling proactive intervention based on real-time health metrics.

From a compliance perspective, the framework demonstrated alignment with major regulatory standards such as HIPAA, GDPR, and regional health data protection regulations. Data residency policies were enforced through geographically segmented cloud zones, and encryption ensured data confidentiality both in transit and at rest. Automated compliance reporting tools generated audit-ready logs, reducing administrative burden during inspections. Compared to traditional compliance management methods, the automated compliance validation reduced preparation time and minimized human errors.

Despite these positive outcomes, several implementation challenges were identified. Migration from legacy systems required substantial planning and data normalization. Data cleansing processes were necessary to ensure compatibility with standardized FHIR schemas. Organizational resistance to DevOps transformation required training and cultural change management. Additionally, blockchain-based audit logging introduced minor performance overhead, although this was mitigated through optimized consensus algorithms. Security complexity also increased due to layered authentication mechanisms, requiring comprehensive identity governance strategies.

The cost-benefit analysis revealed that although initial cloud migration and DevOps implementation required significant investment, long-term operational savings outweighed upfront costs. Reduced infrastructure maintenance, minimized downtime, improved billing accuracy, and faster deployment cycles collectively contributed to positive return on investment. Furthermore, the improved patient satisfaction and trust generated intangible benefits that enhanced institutional reputation.

In summary, the results confirm that integrating real-time cloud architecture, secure API management, unified payment systems, and DevOps methodologies creates a robust, scalable, and secure healthcare ecosystem. The framework addresses core healthcare IT challenges by combining interoperability standards, financial transparency, agile software delivery, and cybersecurity resilience. While certain adoption challenges persist, the overall performance metrics indicate that such an enterprise framework can significantly modernize healthcare operations, improve patient outcomes, and create a foundation for future digital innovation.

V. CONCLUSION

The development and implementation of the Enterprise Real-Time Healthcare Cloud Framework with Secure APIs, Unified Payments, and DevOps Integration represent a transformative shift in modern healthcare information systems. Healthcare organizations globally face increasing demands for real-time data exchange, enhanced cybersecurity, regulatory compliance, patient-centered financial transparency, and rapid technological innovation. Traditional legacy systems have proven insufficient to address these complex and evolving needs. By introducing a cloud-native, microservices-based architecture combined with secure API governance, payment orchestration, and DevOps automation, the proposed framework provides a holistic solution capable of addressing these multidimensional challenges.

The integration of real-time cloud computing ensures that healthcare providers have immediate access to accurate and synchronized patient information across departments and institutions. This capability enhances clinical decision-making, reduces medical errors, and improves care coordination. The adoption of interoperability standards such as HL7 FHIR ensures seamless communication between heterogeneous systems, breaking down long-standing data silos. Such interoperability is not merely a technical improvement but a foundational requirement for delivering value-based and patient-centric healthcare services.

Security remains paramount in healthcare systems due to the sensitive nature of patient data. The framework's multi-layered security approach—including encryption, zero-trust architecture, API gateway enforcement, identity federation, and immutable audit logging—demonstrates that cloud-based healthcare systems can achieve high levels of security and compliance. By embedding security into every layer of the architecture, rather than treating it as an afterthought, the framework reduces exposure to cyber threats and enhances institutional trust.

Unified payments integration addresses a frequently overlooked but critical aspect of healthcare digital transformation: financial system fragmentation. By consolidating billing, insurance processing, and digital payment systems into a

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706032

single orchestrated platform, the framework enhances financial transparency, reduces administrative overhead, and improves patient satisfaction. Automated reconciliation and real-time eligibility verification reduce claim denials and payment delays, contributing to operational efficiency and financial sustainability.

DevOps integration further strengthens the framework by enabling continuous innovation. Healthcare technology must evolve rapidly to accommodate new regulations, medical discoveries, and patient expectations. Traditional deployment cycles are often too slow and risk-prone. By adopting CI/CD pipelines, automated testing, and infrastructure as code, the framework ensures reliable, frequent, and secure updates without disrupting services. This agility is essential in a healthcare environment where system downtime can directly impact patient safety.

Overall, the enterprise framework demonstrates that combining cloud computing, API standardization, financial integration, and DevOps culture can produce a resilient and future-ready healthcare ecosystem. While implementation requires strategic planning, cultural transformation, and investment, the long-term benefits—including improved care quality, operational efficiency, security resilience, and financial optimization—justify the effort. The framework lays a strong foundation for the next generation of digital healthcare systems that are intelligent, scalable, secure, and patient-centric.

VI. FUTURE WORK

Future research and development efforts can further enhance the Enterprise Real-Time Healthcare Cloud Framework by incorporating advanced artificial intelligence and predictive analytics capabilities. Integrating machine learning models directly into the real-time data pipeline would enable predictive diagnostics, automated risk scoring, and proactive patient monitoring. For example, AI-driven algorithms could analyze streaming vital signs data to predict potential medical emergencies before they occur. Embedding these capabilities within the cloud-native architecture would enable scalable, real-time intelligence across healthcare networks.

Another promising direction involves deeper integration with Internet of Medical Things (IoMT) devices and wearable health technologies. Expanding secure API endpoints to accommodate continuous data ingestion from remote monitoring devices would strengthen telehealth and home-care models. Future work should also explore edge computing strategies to process time-sensitive health data closer to the patient source, reducing latency and bandwidth consumption.

Blockchain optimization remains an area for improvement. While blockchain enhances auditability and trust, further research into lightweight consensus mechanisms could reduce performance overhead and energy consumption. Hybrid models combining centralized efficiency with decentralized trust guarantees may offer balanced solutions.

Enhanced patient-centric data ownership models could also be explored. Implementing decentralized identity frameworks would allow patients to control access permissions dynamically and grant temporary access to providers, insurers, or researchers. This would align with emerging digital identity standards and privacy-preserving data-sharing paradigms.

Finally, future work should examine large-scale, real-world deployments across diverse healthcare ecosystems, including rural hospitals and global health networks. Comparative longitudinal studies measuring patient outcomes, cost savings, and system resilience over extended periods would provide deeper validation. By continuously evolving through research and innovation, the framework can adapt to emerging technologies, regulatory changes, and global healthcare challenges, ensuring sustainable digital transformation for years to come.

REFERENCES

1. Anumula, S. R. (2023). Resilience engineering for intelligent enterprise platforms. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(1), 5954–5965.
2. Fazilath, M., & Umasankar, P. (2025, February). Comprehensive Analysis of Artificial Intelligence Applications for Early Detection of Ovarian Tumours: Current Trends and Future Directions. In 2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-9). IEEE.
3. Gangina, P. (2022). Unified payment orchestration platform: Eliminating PCI compliance burden for SMBs through multi-provider aggregation. International Journal of Research Publications in Engineering, Technology and Management, 5(2), 6540–6549.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706032

4. Kumar, A., Anand, L., & Kannur, A. (2024, November). A Novel Approach to Feature Extraction in MI-Based BCI Systems. In 2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS) (pp. 1-6). IEEE.
5. Ponugoti, M. (2024). Engineering global resilience: A cloud-native approach to enterprise system. International Journal of Future Innovative Science and Technology (IJFIST), 7(2), 12392–12403.
6. Raj, A. M. A., Rajendran, S., & Vimal, G. S. A. G. (2024). Enhanced convolutional neural network enabled optimized diagnostic model for COVID-19 detection. Bulletin of Electrical Engineering and Informatics, 13(3), 1935-1942.
7. Navandar, P. (2023). Guarding Networks: Understanding the Intrusion Detection System (IDS). Journal of biosensors and bioelectronics research. https://d1wqtxts1xzle7.cloudfront.net/125806939/20231119-libre.pdf?1766259308=&response-content-disposition=inline%3B+filename%3DGuarding_Networks_Understanding_the_Intr.pdf&Expires=1767147182&Signature=H9aJ73csgfALZ~2B89oBRyYgz57iuooJUU0zKPdjpmQjunvziuvJjd~r8gYT52Ah6RozX-LUpFB14VO8yjXrVD73j1HN9DAMi1PSGKaRbcI8gBbrnFQQGOhTO7VYkGcz3ylDLZJatGabbl5ASNiqe0kINjsw6op5mJzXUoWLZkmret8YBzR1b6Ai8j4SCuZ2kc75dAfryQSZDKuv9ISFi9oHyMxEwWKkyNDnnDP~0EW3dBp7qmwPJVbnm7wSQFFU9AUx5o3T742k80q8ZxvS8M-63TZkyb5I3oq6zBUOCVgK471hm2K9gYtYPrwePdoeEP5P4WmIBxeygrqYViN9nw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
8. Mudunuri, P. R. (2022). Engineering audit-ready CI/CD pipelines for federally regulated scientific computing. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(5), 5342–5351.
9. Chivukula, V. (2020). IMPACT OF MATCH RATES ON COST BASIS METRICS IN PRIVACY-PRESERVING DIGITAL ADVERTISING. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 3(4), 3400-3405.
10. Archana, R., & Anand, L. (2023, September). Ensemble Deep Learning Approaches for Liver Tumor Detection and Prediction. In 2023 Third International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS) (pp. 325-330). IEEE.
11. Natta, P. K. (2024). Closed-loop AI frameworks for real-time decision intelligence in enterprise environments. International Journal of Humanities and Information Technology, 6(3). https://doi.org/10.21590/ijhit.06.03.05
12. Genne, S. (2024). Architecting enterprise-grade cross-platform mobile applications with web views. International Journal of Humanities and Information Technology (IJHIT), 6(1), 64–85.
13. Sugumar, R. (2024). AI-Driven Cloud Framework for Real-Time Financial Threat Detection in Digital Banking and SAP Environments. International Journal of Technology, Management and Humanities, 10(04), 165-175.
14. Kesavan, E., Srinivasulu, S., & Deepak, N. M. (2025). IoT enabled green farming using image processing. In Proceedings of The International Conference on Scientific Innovations in Science, Technology & Management (ICSISTM-2025). Retrieved from https://www.researchgate.net/publication/397883632_IoT_Enabled_Green_Farming_Using_Image_Processing
15. Mohan, B., Siddhan, S., & Chinnadurai, N. (2024). Control for Power Quality Improvement of Solar Photovoltaic-Distributed Static Synchronous Compensator Interfaced with Weak Grid Using Multi-Variable Filter Dual Second-Order Generalized Integrator Phase-Locked Loop. Electric Power Components and Systems, 52(9), 1616-1635.
16. Ramidi, M. (2023). Accessibility-centered mobile architectures for government health initiatives. International Journal of Research and Applied Innovations (IJRAI), 6(2), 8597–8610.
17. Panda, M. R., Devi, C., & Dhanorkar, T. (2024). Generative AI-Driven Simulation for Post-Merger Banking Data Integration. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 7(01), 339-350.
18. Raju, S., & Chandrasekaran, M. (2019). Performance analysis of efficient data distribution in P2P environment using hybrid clustering techniques. Soft Computing-A Fusion of Foundations, Methodologies & Applications, 23(19).
19. Gopinathan, V. R. (2024). Cyber-Resilient Digital Banking Analytics Using AI-Driven Federated Machine Learning on AWS. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8419-8426.
20. Gaddapuri, N. S. (2024). AI BASED CLOUD COMPUTATION METHOD AND PROCESS DEVELOPMENT. Power System Protection and Control, 52(2), 38-50.
21. Vimal Raja, G. (2025). Context-Aware Demand Forecasting in Grocery Retail Using Generative AI: A Multivariate Approach Incorporating Weather, Local Events, and Consumer Behaviour. International Journal of Innovative Research in Science Engineering and Technology (Ijirset), 14(1), 743-746.
22. Chennamsetty, C. S. (2024). Adaptive Model Training Pipelines: Real-Time Feedback Loops for Self-Evolving Systems. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(6), 11367-11373.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706032

23. Adari, V. K., Chunduru, V. K., Gonepally, S., Amuda, K. K., & Kumbum, P. K. (2023). Ethical analysis and decision-making framework for marketing communications: A weighted product model approach. Data Analytics and Artificial Intelligence, 3 (5), 44–53.
24. Ananth, S., & Saranya, A. (2016, January). Reliability enhancement for cloud services-a survey. In 2016 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-7). IEEE.
25. Surisetty, L. S. (2022). Modernizing Legacy Systems with AI Orchestration: From Monoliths to Autonomous Micro services. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 5(6), 7299-7306.
26. Mohana, P., Muthuvinayagam, M., Umasankar, P., & Muthumanickam, T. (2022, March). Automation using Artificial intelligence based Natural Language processing. In 2022 6th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1735-1739). IEEE.
27. Raj, A. M. A., Rajendran, S., & Vimal, G. S. A. G. (2024). Enhanced convolutional neural network enabled optimized diagnostic model for COVID-19 detection. Bulletin of Electrical Engineering and Informatics, 13(3), 1935-1942.
28. Kusumba, S. (2024). Accelerating AI and Data Strategy Transformation: Integrating Systems, Simplifying Financial Operations Integrating Company Systems to Accelerate Data Flow and Facilitate Real-Time Decision-Making. The Eastasouth Journal of Information System and Computer Science, 2(02), 189-208.
29. Devarajan, R., Prabakaran, N., Vinod Kumar, D., Umasankar, P., Venkatesh, R., & Shyamalagowri, M. (2023, August). IoT Based Under Ground Cable Fault Detection with Cloud Storage. In 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1580-1583). IEEE.
30. Ananth, S., Radha, D. K., Prema, D. S., & Nirajan, K. (2019). Fake news detection using convolution neural network in deep learning. International Journal of Innovative Research in Computer and Communication Engineering, 7(1), 49-63.
31. Mallareddi, P. K. D., Keezhadath, A. A., & Kanka, V. (2024). High-Throughput Stream Processing for Global Payment Platforms. American Journal of Data Science and Artificial Intelligence Innovations, 4, 37-73.
32. Mogili, V. B. (2025). Healthcare and Finance Transformation through Enterprise Content, Low-Code, and Automation: A Multinational Technology Corporation's Approach. Journal Of Engineering And Computer Sciences, 4(7), 630-636.
33. Sriramoju, S. (2022). API-driven account onboarding framework with real-time compliance automation. International Journal of Research and Applied Innovations (IJRAI), 5(6), 8132–8144.