The American Journal of Engineering and Technology
ISSN 2689-0984 Volume 08 - 2026

A Scalable AWS-Native Architecture for Modernizing Legacy Healthcare Information Systems Through Secure Microservices and Automated DevOps Pipelines

Dr. Rizky Pratama Wijaya
Department of Cloud Computing and Distributed Systems
Nusantara Institute of Technology, Jakarta, Indonesia,

Received: 01 May 2026 | Received Revised Version: 15 May 2026 | Accepted: 24 May 2026 | Published: 01 Jun 2026

Volume 08 Issue 06 2026 |

Abstract

Legacy healthcare information systems often operate through fragmented data models, monolithic applications, limited interoperability, and manually governed deployment practices that restrict scalability, security, and clinical responsiveness. This technical paper proposes an AWS-native modernization architecture that transforms legacy healthcare platforms into secure, interoperable, microservices-based systems supported by automated DevOps pipelines. The paper synthesizes research on electronic health record interoperability, FHIR-based integration, blockchain-enabled health data exchange, semantic data mapping, cloud-native systems, cybersecurity, healthcare analytics, and artificial intelligence to develop a structured modernization framework. The proposed model combines domain-oriented microservices, API-driven interoperability, container orchestration, automated CI/CD workflows, identity and access management, observability, and compliance-aware data governance. The analysis indicates that healthcare modernization should not be treated merely as infrastructure migration but as a socio-technical redesign of data, workflow, security, and operational governance. Findings suggest that AWS-native services can improve deployment reliability, horizontal scalability, auditability, and system resilience when combined with standardized clinical terminologies and secure interoperability layers. However, modernization also introduces risks related to vendor dependency, migration complexity, data quality, regulatory accountability, and organizational readiness. The paper concludes that a phased, security-by-design, interoperability-first architecture provides a practical pathway for healthcare institutions seeking to modernize legacy systems without disrupting clinical continuity.

Keywords: AWS-native architecture; healthcare information systems; legacy modernization; microservices; DevOps pipelines; electronic health records; FHIR interoperability; cloud security; healthcare data governance; automated deployment.

Cite This Article: Dr. Rizky Pratama Wijaya. (2026). A Scalable AWS-Native Architecture for Modernizing Legacy Healthcare Information Systems Through Secure Microservices and Automated DevOps Pipelines. The American Journal of Engineering and Technology, 8(06), 13–20. Retrieved from https://www.theamericanjournals.com/index.php/tajet/article/view/8035

1. Introduction

Healthcare information systems have become central to clinical decision-making, administrative efficiency, public health surveillance, patient engagement, and data-driven medical innovation. However, many hospitals and healthcare organizations continue to rely on legacy electronic health record systems, fragmented departmental applications, and tightly coupled software architectures that were not designed for contemporary interoperability, cloud scalability, real-time analytics, or

continuous software delivery. These systems often contain valuable longitudinal clinical data, yet their technical rigidity limits integration with mobile healthcare, artificial intelligence, recommender systems, blockchain-based data exchange, and advanced analytics platforms (Awad et al., 2021; Benuzillo et al., 2019; Fihn et al., 2014).

The core problem is not only technological obsolescence but architectural misalignment. Legacy healthcare systems commonly depend on centralized databases, proprietary interfaces, batch-based data exchange, manual release cycles, and weak observability. Such characteristics create barriers to secure health data sharing, clinical terminology standardization, patient-centered digital services, and rapid deployment of new functionality. Research on electronic health record interoperability shows that technical integration must address semantic, structural, and organizational dimensions rather than simple data transfer alone (Jardim, 2013; Huang et al., 2020; Amar et al., 2024). Similarly, studies on FHIR, SNOMED CT, blockchain, and ontology mapping demonstrate that healthcare modernization requires common data representations, trusted exchange mechanisms, and governance frameworks (Anand and Sadhna, 2023; Sung et al., 2023; Haw et al., 2023).

Cloud-native architectures offer a practical route for addressing these limitations. Microservices, containerized deployment, managed databases, API gateways, event-driven integration, and automated DevOps pipelines enable modular transformation of legacy functions into scalable, maintainable, and observable services. In the AWS context, this modernization can involve services such as container orchestration, managed relational and NoSQL databases, identity and access management, monitoring, encryption, serverless functions, CI/CD automation, and secure network segmentation. Yet healthcare cloud adoption requires a stricter architectural discipline than ordinary enterprise migration because clinical data is sensitive, system downtime can affect patient safety, and compliance obligations must be embedded throughout the lifecycle.

The objective of this paper is to propose and analyze a scalable AWS-native technical architecture for modernizing legacy healthcare information systems through secure microservices and automated DevOps pipelines. The paper focuses on how legacy healthcare capabilities can be decomposed into domain-aligned services, how interoperability can be implemented through standardized APIs and semantic mapping, how automated pipelines can reduce deployment risk, and how security controls can be integrated across infrastructure, application, and data layers. The scope is conceptual and technical rather than empirical; it develops an architecture grounded in the provided literature and evaluates expected outcomes, limitations, and implementation implications.

The significance of this research lies in positioning modernization as a structured transformation of healthcare infrastructure, software engineering, and data governance. Rather than treating cloud migration as a hosting decision, the paper argues that sustainable modernization depends on secure modularity, interoperability, automated operations, and continuous compliance.

2. Literature Review

The literature on healthcare information system modernization emphasizes interoperability as a central challenge. Jardim (2013) identifies the electronic health record as a key mechanism for healthcare information systems interoperability, but also highlights that interoperability depends on the ability of systems to exchange, interpret, and reuse data meaningfully. Huang et al. (2020) further show that transitions from one electronic health record system to another are complex because technical migration interacts with workflow redesign, user adaptation, data integrity, and institutional risk. These insights suggest that legacy modernization cannot be reduced to platform replacement; it must preserve clinical continuity while improving technical adaptability.

FHIR-based interoperability has received significant attention as a pathway for modern health data exchange. Amar et al. (2024) discuss semantic issues related to electronic health records and Fast Healthcare Interoperability Resources, indicating that standards are necessary but insufficient unless semantic alignment is also achieved. Haw et al. (2023) similarly examine XML-to-ontology representation for effective data integration, while Rajput et al. (2023) and Sung et al. (2023) focus on SNOMED CT terminology mapping. Together, these studies demonstrate that modernization architectures must include terminology services, mapping layers, metadata governance, and validation mechanisms. Without semantic consistency, cloud-native APIs may only accelerate the movement of inconsistent

data.

Blockchain-oriented studies contribute another perspective on trust, auditability, and decentralized exchange. Anand and Sadhna (2023), Mauricio et al. (2024), Samala and Rawas (2024), Tariq (2024), and Aljaloud and Razzaq (2023) emphasize blockchain's potential for secure EHR interoperability and decentralized health data platforms. While blockchain is not always required for every modernization scenario, the literature is valuable because it frames health data exchange around immutability, traceability, patient control, and distributed trust. These principles are relevant to AWS-native architecture through audit logging, encryption, access control, and immutable infrastructure practices.

Cloud-native architecture and cybersecurity studies provide the technical foundation for scalable and secure modernization. Ammi et al. (2022) demonstrate how cloud-native architecture can enable semantic interconnectedness of data in cyber threat intelligence, suggesting that modular services and semantic integration can operate together. Xiong et al. (2025) propose deep learning-based anomaly detection in container environments, while Carter et al. (2025), Chettier et al. (2025), Masunda, and Xing et al. (2010) collectively highlight threats, anomaly detection, explainable AI, and countermeasures in distributed or networked systems. These works show that microservices and containers increase flexibility but also expand attack surfaces, making runtime monitoring, intrusion detection, access governance, and automated security testing essential.

Healthcare analytics and AI literature shows why modernization is strategically important beyond infrastructure improvement. Benuzillo et al. (2019) and Fihn et al. (2014) describe the operational value of advanced analytics in healthcare, while Thomas et al. (2021), An et al. (2023), Jayaram et al. (2024), Haw et al. (2024), Yong et al. (2025), Zhang and Kamel Boulos (2023), and Tang et al. (2024) indicate growing reliance on machine learning, recommender systems, generative AI, and digital health applications. These capabilities require standardized, high-quality, accessible, and secure data pipelines. Ramakrishnaiah et al. (2023) directly support this need by presenting an EHR standardization and preprocessing pipeline for clinical outcome prediction.

A key research gap emerges across these studies. Existing literature often addresses interoperability, blockchain, AI, cybersecurity, analytics, or EHR transition as separate concerns. Fewer works integrate these dimensions into a unified cloud-native modernization architecture that connects microservices decomposition, AWS-native infrastructure, secure DevOps automation, semantic interoperability, and healthcare compliance. This paper addresses that gap by proposing a technical architecture in which interoperability, security, deployment automation, and scalability are treated as mutually dependent design requirements.

3. Methodology

This paper uses a design-oriented technical methodology based on architectural synthesis. Rather than conducting a statistical experiment, it develops a conceptual AWS-native modernization framework derived from the technical problems and design principles identified in the provided literature. The methodology follows four analytical steps: legacy-system problem abstraction, domain decomposition, AWS-native architectural mapping, and operational validation through security, interoperability, and DevOps criteria.

The first step is problem abstraction. Legacy healthcare information systems are analyzed as socio-technical infrastructures composed of data repositories, clinical workflows, user roles, integration interfaces, and governance obligations. Prior studies on EHR transition and interoperability show that modernization failures often occur when institutions focus on software replacement without addressing data semantics, workflow continuity, and clinical trust (Huang et al., 2020; Jardim, 2013). Therefore, the proposed methodology begins by identifying legacy constraints such as monolithic application logic, tightly coupled databases, incomplete audit trails, manual deployment, inconsistent terminologies, and limited external integration. These constraints are then translated into modernization requirements: modularity, interoperability, security, automation, observability, and compliance.

The second step is domain decomposition. A healthcare platform can be decomposed into microservices based on functional boundaries such as patient identity, appointments, clinical encounters, laboratory results, prescriptions, billing, consent, notifications, analytics, and audit logging. This decomposition follows the principle that each service should own its business logic

and data model while communicating through secure APIs or asynchronous events. For example, a laboratory results service may expose FHIR-compatible diagnostic report endpoints, while a consent service governs which external systems can access patient records. This design reduces dependency on a single monolithic database and allows independent scaling of high-demand functions such as appointment booking or patient portal access.

The third step is AWS-native architectural mapping. In the proposed architecture, an API gateway acts as the controlled entry point for web, mobile, and partner applications. Microservices are deployed through container orchestration or serverless components depending on workload characteristics. Transactional clinical data may remain in managed relational databases, while document-based records, audit events, and analytics-ready datasets can be stored in specialized managed storage layers. Event-driven services support asynchronous operations such as notification delivery, claims processing, audit capture, and analytics ingestion. Identity and access management enforces least-privilege permissions across users, applications, services, and deployment pipelines. Encryption is applied in transit and at rest, while secrets management prevents exposure of credentials in code repositories or configuration files.

The interoperability layer is a central component of the methodology. Research on FHIR, SNOMED CT, ontology mapping, and EHR standardization indicates that technical APIs must be supported by semantic consistency (Amar et al., 2024; Sung et al., 2023; Rajput et al., 2023; Ramakrishnaiah et al., 2023). Accordingly, the proposed architecture includes a terminology service, mapping engine, validation module, and canonical data model. When a legacy system stores diagnosis codes in local formats, the mapping engine aligns them with standardized vocabularies before exposing them through interoperable APIs. This reduces ambiguity and allows downstream analytics, clinical decision support, and external exchange systems to consume normalized data.

The DevOps component of the methodology focuses on automated delivery and controlled change. Continuous integration pipelines validate source code, run unit tests, scan dependencies, perform container image checks, and package deployable artifacts. Continuous delivery pipelines promote services through development, testing, staging, and production environments using infrastructure-as-code. Automated rollback, blue-green deployment, and canary release strategies reduce the risk of clinical disruption. In a hospital setting, this means a new patient portal feature can be deployed to a limited user group first, monitored for errors, and expanded only after stability is confirmed. This approach is consistent with the broader need for safe EHR transition and operational reliability discussed by Huang et al. (2020).

Security is embedded as a cross-cutting methodological requirement rather than a post-deployment activity. The proposed model incorporates zero-trust access assumptions, network segmentation, runtime monitoring, vulnerability scanning, audit logging, anomaly detection, and incident response automation. Studies on sensor network attacks, cloud-native anomaly detection, and AI-based intrusion detection show that distributed architectures require continuous security intelligence rather than static perimeter defense (Xing et al., 2010; Xiong et al., 2025; Carter et al., 2025). For healthcare, this is especially important because unauthorized access to patient records can produce legal, ethical, and clinical consequences.

Finally, the methodology evaluates the architecture using qualitative criteria derived from the literature: scalability, interoperability, security, maintainability, data quality, deployment reliability, and clinical continuity. The method assumes a phased migration strategy in which legacy systems are gradually wrapped, integrated, decomposed, and retired. This avoids the high risk of abrupt replacement and supports coexistence between old and new components while services are validated.

4. Findings

The architectural synthesis indicates that AWS-native modernization can produce meaningful improvements when it is implemented as a coordinated transformation of application structure, data semantics, security controls, and operational processes. The first major finding is that microservices decomposition improves scalability and maintainability only when service boundaries reflect healthcare domain logic. Decomposing a legacy system by technical layers alone may reproduce fragmentation, whereas domain-oriented services such as patient identity, encounters, laboratory results, consent, and billing enable clearer ownership and independent deployment.

The second finding is that interoperability requires a dedicated semantic layer. FHIR-compatible APIs provide structural exchange, but literature on semantic mapping and terminology systems shows that data quality depends on controlled vocabularies, validation rules, and

mapping governance (Amar et al., 2024; Haw et al., 2023; Sung et al., 2023). Therefore, the proposed architecture finds that API modernization without terminology normalization is insufficient for reliable clinical analytics or cross-institutional exchange.

The third finding is that automated DevOps pipelines reduce operational risk by making deployment repeatable, testable, and auditable. In legacy environments, manual releases often create inconsistent configurations and delayed security updates. Automated pipelines enable controlled promotion, rollback, vulnerability scanning, and infrastructure reproducibility. This is especially valuable in healthcare settings where downtime or faulty deployment can affect clinical services.

The fourth finding is that security must be distributed across the architecture. Microservices and containers increase modularity but also create more network endpoints, service identities, and runtime dependencies. As supported by cybersecurity literature, effective modernization requires encryption, identity governance, anomaly detection, container monitoring, and audit trails (Xing et al., 2010; Xiong et al., 2025; Chettier et al., 2025). Security-by-design is therefore more appropriate than perimeter-only protection.

The fifth finding is that modernization creates readiness for advanced analytics, AI, and digital health. Standardized data pipelines and cloud-native processing improve the feasibility of recommender systems, clinical prediction models, generative AI applications, and real-time operational dashboards (An et al., 2023; Benuzillo et al., 2019; Zhang and Kamel Boulos, 2023). However, these benefits depend on governance, data quality, and responsible access control.

5. Discussion

The proposed AWS-native architecture demonstrates that legacy healthcare modernization should be understood as a layered transformation rather than a simple cloud migration. The findings align with literature showing that EHR interoperability and transition projects are difficult because they combine technical, semantic, organizational, and clinical dimensions (Huang et al., 2020; Jardim, 2013). A microservices architecture can improve agility, but its value depends on whether services are designed around meaningful clinical domains and governed through stable interfaces.

A major implication is that DevOps automation becomes a clinical reliability mechanism, not merely a software engineering practice. Automated testing, deployment, rollback, and monitoring help reduce the uncertainty associated with frequent system changes. This is important because healthcare organizations increasingly need to add digital health functions, analytics modules, patient-facing applications, and AI-enabled features without destabilizing core clinical operations (Awad et al., 2021; Benuzillo et al., 2019).

The architecture also reveals a trade-off between flexibility and complexity. Microservices allow independent scaling and deployment, but they introduce distributed tracing challenges, service dependency management, API versioning, and stronger security requirements. Cybersecurity studies indicate that cloud-native environments require continuous anomaly detection and runtime protection because attacks may target containers, APIs, credentials, or network paths (Xiong et al., 2025; Carter et al., 2025). Thus, modernization must include observability and security engineering from the beginning.

Another critical issue is semantic governance. The literature on FHIR, SNOMED CT, and ontology mapping suggests that interoperability cannot be solved only through infrastructure (Amar et al., 2024; Rajput et al., 2023; Sung et al., 2023). If legacy records contain inconsistent local codes or incomplete metadata, cloud-native services may simply expose poor-quality data faster. Therefore, data standardization, validation, and stewardship must accompany technical migration.

The limitations of the proposed framework include its conceptual nature and dependence on institutional maturity. Smaller healthcare organizations may lack DevOps expertise, cloud governance capabilities, or resources for phased migration. Vendor dependency is another concern because AWS-native services can improve productivity but may reduce portability. Future implementations should therefore balance managed cloud benefits with open standards, portable containers, and documented exit strategies.

6. Conclusion

This paper proposed a scalable AWS-native architecture for modernizing legacy healthcare information systems through secure microservices and automated DevOps pipelines. The central contribution is an integrated framework that connects healthcare interoperability, semantic data governance, microservices decomposition,

cloud-native scalability, automated deployment, and security-by-design. The paper argues that successful modernization requires more than moving legacy applications to cloud infrastructure; it requires redesigning how healthcare systems structure services, exchange data, enforce security, and deliver software changes.

The analysis shows that domain-aligned microservices can reduce monolithic rigidity, while FHIR-oriented APIs and terminology services can improve health data interoperability. Automated DevOps pipelines strengthen deployment reliability and auditability, and AWS-native security controls support encryption, identity governance, monitoring, and incident response. These capabilities collectively prepare healthcare organizations for advanced analytics, digital health services, recommender systems, AI-assisted workflows, and more resilient patient-centered platforms.

The study also highlights important limitations. Cloud-native modernization can increase architectural complexity, require new organizational skills, introduce vendor dependency, and expose weaknesses in legacy data quality. Therefore, healthcare institutions should adopt phased migration strategies, maintain clinical continuity, invest in semantic governance, and implement security controls throughout the software lifecycle. Future research should validate the proposed architecture through case-based implementation, cost-performance analysis, compliance evaluation, and empirical measurement of deployment reliability, interoperability improvement, and clinical workflow impact.

References

1. G. Anand and D. Sadhna, “Electronic health record interoperability using FHIR and blockchain: A bibliometric analysis and future perspective,” Perspectives in Clinical Research, vol. 14, 2023.
2. Q. An, S. Rahman, J. Zhou, and J. J. Kang, “A Comprehensive Review on Machine Learning in Healthcare Industry: Classification, Restrictions, Opportunities and Challenges,” Sensors, vol. 23, 2023.
3. Anonymous, “Current State of Electronic Health Record Interoperability,” 2024.
4. F. Amar, A. April, and A. Abran, “Electronic Health Record and Semantic Issues Using Fast Healthcare Interoperability Resources: Systematic Mapping Review,” Journal of Medical Internet Research, vol. 26, 2024.
5. J. D. Amos, Z. Zhang, Y. Tian, G. V. Lowry, M. R. Wiesner, and C. O. Hendren, “Knowledge and Instance Mapping: Architecture for Premeditated Interoperability of Disparate Data for Materials,” Scientific Data, vol. 11, 2024.
6. M. Ammi, O. Adedugbe, F. M. Alharby, and E. Benkhelifa, “Leveraging a cloud-native architecture to enable semantic interconnectedness of data for cyber threat intelligence.” Cluster Computing, vol. 25, no. 5, pp. 3629 - 3640, 2022.
7. A. Awad, S. J. Trenfield, T. D. Pollard, J. J. Ong, M. Elbadawi, L. E. McCoubrey, A. Goyanes, S. Gaisford, and A. W. Basit, “Connected healthcare: Improving patient care using digital health technologies,” Advanced Drug Delivery Reviews, vol. 178, 2021.
8. J. Benuzillo, L. A. Savitz, and S. Evans, “Improving Health Care with Advanced Analytics: Practical Considerations,” eGEMs (Generating Evidence & Methods to Improve Patient Outcomes), vol. 7, 2019.
9. M. A. Carter, J. L. Hayes, R. J. Miller, E. K. Thompson, and C. James, “AI-based intrusion detection for multi-cloud workloads.” 2025.
10. T. M. Chettier, V. A. K. Boyina, S. Jorepalli, C. Singh, and N. Gupta, “Scalable explainable AI with a cloud-native approach for cybersecurity threat detection.” In Proc. 2025 3rd Int. Conf. Advancement in Computation & Computer Technologies (InCACCT), Apr. 2025, pp. 686–691.
11. V. Chowdhry, P. Kharat, A. Nethi, A. Arora, et al., “Secure Scalable Real-Time Machine Learning Platform for Healthcare,” United States Patent Application, no. 17..., 2021.
12. D. Mauricio, P. C. Llanos-Colchado, L. S. Cutipa-Salazar, P. Castañeda, R. Chuquimbalqui-Maslucán, L. Rojas-Mezarina, and J. L. Castillo-Sequera, “Electronic Health Record Interoperability System in Peru Using Blockchain,” International Journal of Online and Biomedical Engineering, vol. 20, 2024.
13. S. D. Fihn, J. Francis, C. Clancy, C. Nielson, K. Nelson, J. Rumsfeld, T. Cullen, J. Bates, and G. L. Graham, “Insights from advanced analytics at the Veterans Health Administration,” Health Affairs, vol. 33, 2014.
14. S.-C. Haw, J. Jayaram, E. A. Anaam, and H. A. Santoso, “Exploring Recommender Systems in the Healthcare: A Review on Methods, Applications and Evaluations,” International Journal on Robotics,

Automation and Sciences, vol. 6, pp. 6–15, 2024.
15. S.-C. Haw, L. J. Chew, D. S. Kusumo, P. Naveen, and K. W. Ng, "Mapping of extensible markup language-to-ontology representation for effective data integration," IAES International Journal of Artificial Intelligence, vol. 12, 2023.
16. C. Huang, R. Koppel, J. D. McGreevey, C. K. Craven, and R. Schreiber, "Transitions from One Electronic Health Record to Another: Challenges, Pitfalls, and Recommendations," Applied Clinical Informatics, vol. 11, 2020.
17. S. V. B. Jardim, "The Electronic Health Record and its Contribution to Healthcare Information Systems Interoperability," Procedia Technology, vol. 9, 2013.
18. J. Jayaram, Y. Kulkarni, L. V. Ganesh, P. Naveen, and E. A. Anaam, "Treatment Recommendation using BERT Personalization," Journal of Informatics and Web Engineering, vol. 3, pp. 41–62, 2024.
19. E. S. Klappe, E. Joukes, R. Cornet, and N. F. de Keizer, "Effective and feasible interventions to improve structured electronic health record data registration and exchange: A concept mapping approach and exploration of practical examples in the Netherlands," International Journal of Medical Informatics, vol. 173, 2023.
20. M. Masunda, AI-powered intrusion detection systems leveraging deep learning for anomaly detection in large-scale distributed network topologies, unpublished.
21. M. Tang, L. W. Ang, and S. Palaniappan, "Comparative Analysis of Linear and Nonlinear sEMG Methods for Detecting Muscle Fatigue During Dynamic Biceps Curls," Journal of Informatics and Web Engineering, vol. 3, pp. 121–132, 2024.
22. J. Thomas, S. McDonald, A. Noel-Storr, I. Shemilt, J. Elliott, C. Mavergames, and I. J. Marshall, "Machine learning reduced workload with minimal risk of missing studies: Development and evaluation of a randomized controlled trial classifier for Cochrane Reviews," Journal of Clinical Epidemiology, vol. 133, 2021.
23. M. U. Tariq, "Revolutionizing Health Data Management With Blockchain Technology," pp. 153–175, 2024.
24. P. S. Nikam, Customized Penetration Testing Framework for Assessing the Security of Amazon Web Services (AWS), Ph.D. dissertation, National College of Ireland, Dublin, Ireland, 2024.
25. E. Øvrelid, "Exploring adaptive mirroring in healthcare IT architectures," Health Systems, vol. 13, 2024.
26. A. M. Rajput, K. Triep, and O. Endrich, "Semi-Automated Approach to Retrieve SNOMED CT Hierarchy of Clinical Terms by Using Terminology Server," Studies in Health Technology and Informatics, vol. 301, 2023.
27. Y. Ramakrishnaiah, N. Macesic, G. I. Webb, A. Y. Peleg, and S. Tyagi, "EHR-QC: A streamlined pipeline for automated electronic health records standardisation and preprocessing to predict clinical outcomes," Journal of Biomedical Informatics, vol. 147, 2023.
28. A. D. Samala and S. Rawas, "Transforming Healthcare Data Management: A Blockchain-Based Cloud Electronic Health Record System for Enhanced Security and Interoperability," International Journal of Online and Biomedical Engineering, vol. 20, 2024.
29. M. Sharma and H. Aggarwal, "Methodologies of Legacy Clinical Decision Support System - A Review," Journal of Telecommunication, Electronic and Computer Engineering, vol. 9, 2017.
30. S. Sung, H. A. Park, H. Jung, and H. Kang, "A SNOMED CT Mapping Guideline for the Local Terms Used to Document Clinical Findings and Procedures in Electronic Medical Records in South Korea: Methodological Study," JMIR Medical Informatics, vol. 11, 2023.
31. A. Ugajin, "Automation in Hospitals and Health Care," Springer Handbooks, Part F674, 2023.
32. A. Woller, A. Daw, V. Aston, J. Lloyd, G. Snow, S. M. Stevens, S. C. Woller, P. Jones, and J. Bledsoe, "Natural Language Processing Performance for the Identification of Venous Thromboembolism in an Integrated Healthcare System," Clinical and Applied Thrombosis/Hemostasis, vol. 27, 2021.
33. K. Xing, S. S. R. Srinivasan, M. J. M. Rivera, J. Li, and X. Cheng, "Attacks and countermeasures in sensor networks: a survey." in Network Security, Boston, MA, USA : Springer US, 2010, pp. 251 - 272.
34. K. Xiong, Z. Wu, and X. Jia, "Deepcontainer: a deep learning-based framework for real-time anomaly detection in cloud-native container environments." Journal of Advanced Computing Systems, vol. 5, no. 1, pp. 1 - 17, 2025.
35. M. T.-T. Yong, S.-B. Ho, and C.-H. Tan, "Migraine Generative Artificial Intelligence based on Mobile

Personalized Healthcare," Journal of Informatics and Web Engineering, vol. 4, no. 1, pp. 275–291, 2025.

36. P. Zhang and M. N. Kamel Boulos, "Generative AI in Medicine and Healthcare: Promises, Opportunities and Challenges," Future Internet, vol. 15, 2023.