



PRIVACY-AWARE REQUIREMENTS TRACEABILITY AND RISK INTELLIGENCE FOR INTEROPERABLE DIGITAL HEALTH INFORMATION SYSTEMS

Ashraful Alom Munna ^{1, *}, Adiluzzaman ², Aarsal Arif ³ and Syeda Nazia Huq ⁴

¹ M.S. in Project Management, Oklahoma Christian University.

² MBA in Management Information, International American University, Los Angeles, California, USA.

³ MS in Business Analytics Management, Avila University, United States.

⁴ MBA in Project Management, Central Michigan University.

* Corresponding Author

ORCID Details

Ashraful Alom Munna: <https://orcid.org/0009-0005-6874-5302>

Adiluzzaman: <https://orcid.org/0009-0009-1231-3657>

Aarsal Arif: <https://orcid.org/0009-0007-8443-6854>

Syeda Nazia Huq: <https://orcid.org/0009-0005-3354-5546>

International Journal of Science and Research Archive, 2026, 21(01), 276–287

Publication history: Received on 31 August 2026; revised on 08 October 2026; accepted on 10 October 2026

Article DOI: <https://doi.org/10.30574/ijrsra.2026.21.1.1860>

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Interoperable digital health systems connect electronic health records, patient portals, clinical services, administrative platforms, and third-party applications, creating dependencies that can propagate requirement changes across workflows, data exchanges, privacy constraints, and security controls. This study develops a privacy-aware requirements traceability and risk intelligence framework to identify such dependencies and assess associated risks. The framework represents requirements, components, workflows, data elements, privacy constraints, security controls, and organizational responsibilities in a typed multi-relational graph. Analytical risk scoring is combined with explainable machine learning to detect high-risk states and identify contributing factors. Evaluation uses 10 synthetic healthcare architectures, 15 public standards and implementation documents, and 120 simulated requirement change scenarios. The proposed graph detected conflicts in 112 of 120 simulated requirement change scenarios, corresponding to a 93.3% detection rate. The combined analytical and ML model achieved 86.3% precision, 84.1% recall, and 85.2% F1 score. These findings show that integrated traceability can support change impact analysis, privacy assessment, and interpretable risk review. Future work should test the framework with real healthcare systems and organizational incident data.

Keywords: Requirements Traceability; Digital Health Interoperability; Privacy-Aware Analytics; Graph-Based Dependency Modeling; Risk Intelligence; Explainable Machine Learning; Conflict Detection; Healthcare Information Systems.

1 INTRODUCTION

Interoperable digital health systems connect EHRs, patient portals, administrative platforms, clinical decision support, and third-party services. These connections create dependencies among requirements, workflows, data exchange, privacy constraints, and security controls. A change in one requirement can therefore affect multiple connected artifacts and create operational, privacy, or compliance risks. Existing research addresses these areas largely separately, with limited integration between traceability, privacy analysis, and explainable risk assessment.

2 BACKGROUND AND MOTIVATION

Requirements traceability supports change impact analysis, while healthcare interoperability research addresses integration and semantic issues across heterogeneous systems. Privacy and security studies show the risks associated with sensitive health data moving across connected services. Explainable analytics can identify factors behind predicted risk, but existing work mainly focuses on healthcare prediction rather than risks caused by requirement, workflow, interface, and access changes.

2.1 Problem Statement

Conventional traceability methods provide limited support for multi-hop dependencies involving requirements, components, workflows, data elements, privacy constraints, and security controls. They also provide limited support for combining operational impact, privacy impact, conflict detection, and interpretable risk analysis. This creates a need for a unified model that can trace requirement changes across interconnected healthcare artifacts and identify their potential risk factors.

2.2 Proposed Solution

This paper proposes a privacy-aware requirements traceability and risk intelligence framework based on a directed, labeled, multi relational graph. The model links requirements, components, workflows, data, privacy constraints, security controls, and organizational responsibilities through typed dependencies. It combines analytical risk scoring with explainable machine learning to identify high risk states and their contributing factors. The framework is evaluated using synthetic healthcare architectures, public standards, and simulated requirement change scenarios, and is compared with matrix based tracing and simple dependency graphs.

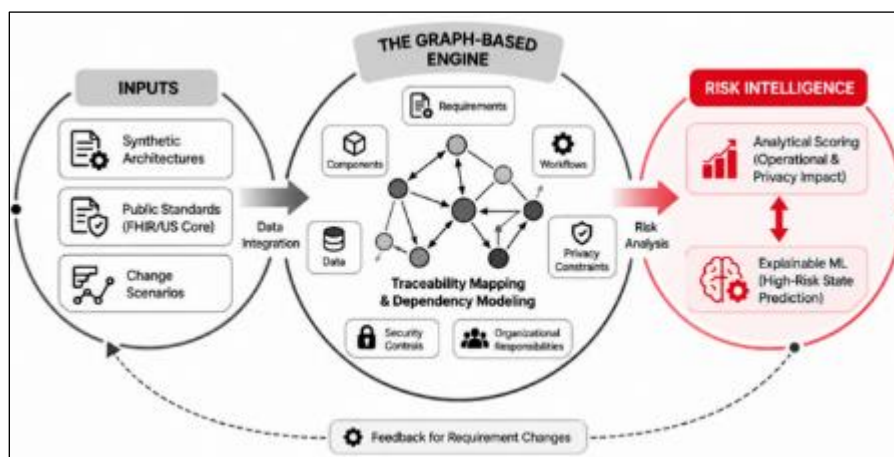


Figure 1: Proposed framework for privacy-aware requirements traceability and risk intelligence

2.3 Contributions

The main contributions of this study are a privacy-aware graph model for multi artifact requirements traceability, an integrated risk scoring method that combines operational and privacy impact, and an explainable machine learning layer for high risk state prediction. The framework is further evaluated against conventional approaches using conflict detection, precision, recall, F1 score, and feature contribution analysis.

3 LITERATURE REVIEW

Interoperable digital health systems create dependencies among requirements, workflows, data exchange, privacy controls, and system components. Existing research largely addresses these areas separately, leaving limited integration between requirements traceability, privacy analysis, and explainable risk assessment.

3.1 Requirements Traceability

Requirements traceability links requirements with related software artifacts and supports impact analysis when systems change. Demi et al. [1], Mucha et al. [2], and Koboyatshwene and Ayalew [3] identify persistent challenges in automated and early stage traceability. However, interoperable healthcare systems require tracing across requirements, workflows, data exchange, access rules, and system components.

3.2 Healthcare Interoperability

Healthcare interoperability connects heterogeneous systems, data structures, and applications. Torab Miandoab et al. [4] and Amar et al. [5] identify integration and semantic challenges, including those associated with FHIR. Existing work does not fully connect interface and data exchange changes with privacy, security, and workflow consequences.

3.3 Privacy and Security

Healthcare information systems require privacy and security controls because sensitive data can move across multiple applications and services. Keshta and Odeh [6] highlight security and privacy challenges in electronic health records, while changes to access, authentication, or information sharing can affect both system behavior and information exposure.

3.4 Explainable Risk Analytics

Explainable AI supports interpretation of analytical results in healthcare. Loh et al. [7] and Niu et al. [8] examine explainable healthcare applications and risk prediction. Similar techniques can support information system risk analysis by identifying the requirements, interfaces, workflows, and privacy conditions associated with high risk states.

3.5 Integrated Traceability and Risk Intelligence

The literature shows separate development of requirements traceability [1]-[3], healthcare interoperability [4], [5], privacy and security [6], and explainable healthcare analytics [7], [8].

The proposed framework connects these areas through a multidimensional model involving functional requirements, system components, healthcare workflows, data exchange, privacy constraints, security controls, and organizational responsibilities.

3.6 Research Gaps

Three gaps are evident. First, requirements traceability provides limited support for privacy sensitive dependencies in interconnected healthcare systems. Second, interoperability research does not fully connect information exchange with requirement changes and privacy consequences. Third, explainable healthcare analytics focuses mainly on clinical prediction rather than risks caused by changes in requirements, workflows, access rules, and interfaces. The proposed framework addresses these gaps through graph-based dependency modeling, risk scoring, and explainable machine learning.

4 METHODOLOGY

This section presents the process for constructing and evaluating the privacy-aware requirements traceability and risk intelligence framework. The methodology comprises six stages: system scoping, data curation, graph-based modeling, risk scoring and explainable analytics, experimental simulation, and comparative validation.

4.1 System Architecture

The study considers interoperable digital health systems comprising EHRs, patient portals, administrative platforms, clinical decision support modules, and third-party services. The system boundary includes functional requirements, privacy constraints, security controls, data exchange interfaces, and organizational responsibilities. A reference architecture incorporates HL7/FHIR APIs, message brokers, identity providers, and consent management services to define the artifacts used for traceability and risk analysis.

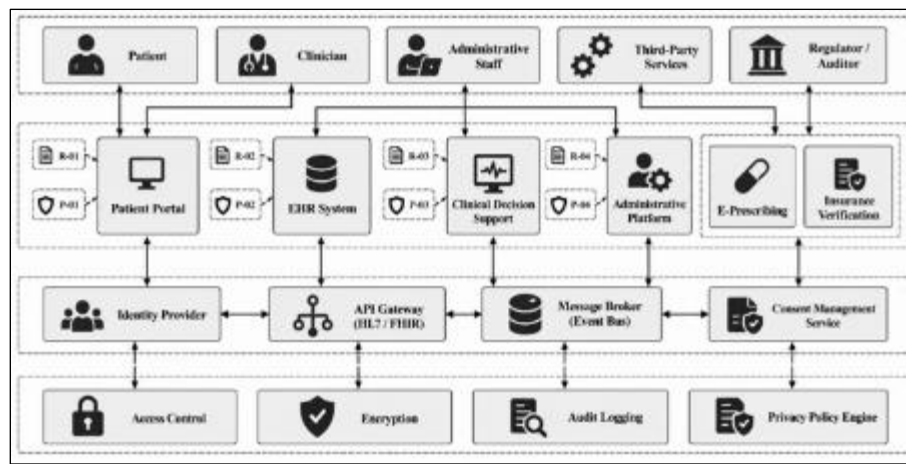


Figure 2: System architecture of the interoperable digital health information system.

The architecture links major applications, integration services, actors, and privacy and security controls, providing the structural basis for subsequent traceability and risk analysis.

4.2 Data Collection and Curation

Artifacts are collected from three sources: synthetic healthcare architectures representing multi vendor EHRs, cross organization data sharing, and patient mediated access; public interoperability standards and implementation guides, including HL7 FHIR and US Core; and simulated requirement change scenarios covering patient access, data sharing, authentication, and interface updates.

Table 1: Data sources used for constructing and evaluating the privacy-aware requirements traceability and risk-intelligence framework.

Source type	Description	Example artifacts	Volume / count	Role in methodology
Synthetic architectures	Modeled multi-system hospital networks with realistic interoperability patterns	Component inventories, interface specifications, workflow diagrams, data dictionaries	10	Basis for graph construction and scenario simulation
Public standards	Interoperability, privacy, and security specifications from open healthcare initiatives	HL7 FHIR resources, US Core profiles, consent models, access control policies	15	Reference basis for dependency definitions and privacy constraints
Change scenarios	Simulated requirement and workflow modifications reflecting real-world updates	Modified patient-access rules, new data-sharing permissions, API version changes, updated authentication flows	120	Input for impact analysis, risk scoring, and evaluation

The dataset comprises 10 synthetic healthcare architectures, 15 public standards and implementation documents, and 120 simulated requirement change scenarios. All artifacts are normalized into a common schema. Requirements, components, workflows, data exchanges, privacy constraints, security controls, and organizational responsibilities are assigned stable identifiers and linked attributes for graph construction. Ambiguities are resolved through predefined rule-based heuristics applied consistently across the simulated artifacts.

4.3 Graph-Based Dependency Modeling

We represent the system as a directed, labeled, multi-relational graph $\{ G = (V, E) \}$; where (V) represents requirements, system components, workflows, data elements, privacy constraints, security controls, and organizational responsibilities. The edge set (E) represents typed dependencies among these artifacts, including “implements,” “depends on,” “exchanges data with,” “constrained by,” and “enforced by.”

Let (T) denote the set of dependency types. For each $(t \in T)$, the corresponding relationship is represented as $Rt \subseteq V \times V$, $t \in T$. The complete edge set is defined as:

$$E = \bigcup_{t \in \tau} R_t$$

This structure supports multi-hop reasoning, for example from a requirement to a component, then to a data element, and finally to a privacy constraint.

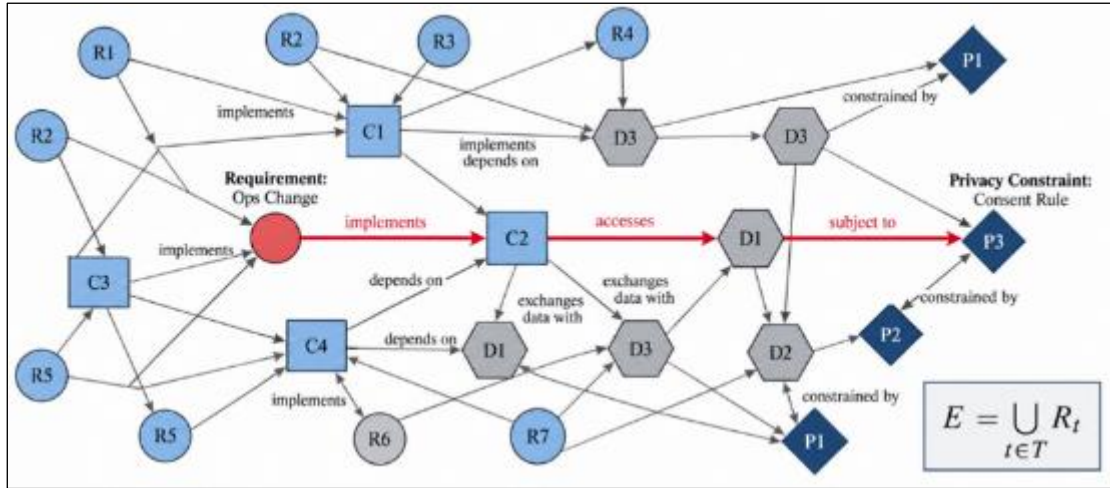


Figure 3: Requirements traceability graph with privacy aware risk path.

This figure shows dependencies among requirements, workflows, components, data elements, and constraints. The highlighted path shows how a privacy-related requirement can propagate across connected system artifacts.

4.4 Risk Scoring and Explainable Analytics

For each requirement change or conflicting state, we compute a risk score R as a weighted combination of operational and privacy impact:

$$R = w_o \cdot I_o + w_p \cdot I_p$$

Where, I_o is the operational impact score (for example number of affected components, workflows, and interfaces), I_p is the privacy impact score (for example sensitivity of exposed data, number of patients affected, and regulatory severity), and w_o, w_p are weights reflecting organizational priorities with $w_o + w_p = 1$. Operational impact I_o is derived from graph traversal counts and criticality labels, where core clinical services are weighted higher. Privacy impact I_p combines data sensitivity levels, consent coverage, and jurisdictional rules.

We further define a conflict severity metric C for detected requirement conflicts:

$$C = \sum_{k=1}^n \alpha_k \cdot s_k$$

Where, s_k is the severity of conflict type k (for example contradictory access rules or inconsistent data retention policies) and α_k is its relative importance.

To complement analytical scoring, the high-risk prediction model uses graph-derived features including affected node count, affected edge count, dependency density, privacy constraint density, conflict indicators, and criticality-related features. The model produces risk probabilities and feature importance scores to identify the requirements, interfaces, data elements, and privacy constraints associated with high-risk predictions. The model was trained and evaluated using the simulated requirement-change scenarios, with the same model configuration, data partitioning procedure, and validation settings applied consistently across the experimental runs.

4.5 Experimental Design and Simulation

The framework is evaluated through controlled experiments using synthetic healthcare architectures and standards-derived models. The evaluation includes 10 synthetic healthcare architectures, 15 public standards and implementation documents, and 120 simulated requirement change scenarios. The simulated scenarios represent five major change categories: patient access rule changes, data sharing permission changes, authentication requirement changes, API or

data schema changes, and administrative workflow changes. Each scenario specifies the affected artifacts, expected dependency propagation paths, and predefined evaluation labels used for conflict and risk analysis. For each scenario, the framework updates the corresponding graph nodes and edges, performs dependency traversal, computes operational and privacy impact, calculates conflict severity, and generates risk predictions. Detected conflicts and risk classifications are then aggregated across the simulated scenarios and synthetic architectures. The simulation is intended to evaluate the internal behavior of the proposed framework rather than to represent observed healthcare incidents. Therefore, the reported results should be interpreted as simulation-based evidence, and not as direct evidence of performance in production healthcare environments.

4.6 Validation and Comparative Evaluation

The proposed framework is compared with two reference approaches: matrix-based traceability and a simple dependency graph without privacy or risk layers. The matrix-based approach represents direct requirement-to-artifact relationships, while the simple dependency graph represents dependency relationships without explicit privacy and risk attributes. The comparison focuses on conflict detection across the simulated requirement-change scenarios. Performance is reported using detection rate for conflict identification and precision, recall, and F1 score for high-risk state identification. Results are aggregated across the simulated scenarios and synthetic healthcare architectures. Because all three approaches are evaluated using the same simulated scenario set, the comparison provides a controlled assessment of their behavior within the constructed evaluation environment. It does not represent a comparison using production healthcare data.

5 RESULTS

This section reports findings from the simulated evaluation of the privacy aware requirements traceability and risk intelligence framework. We present conflict detection and risk identification results, then interpret their meaning for interoperable digital health systems. Finally, we outline limitations and future work. Reported values are aggregated over the simulated requirement-change scenarios and synthetic architectures described in Section III.

Table 2 summarizes conflict-detection performance for the proposed framework and the two reference approaches. The proposed privacy-aware graph identifies conflicts in 112 of the 120 simulated requirement-change scenarios, corresponding to a 93.3% detection rate. The simple dependency graph identifies 95 scenarios, while matrix-based traceability identifies 78 scenarios. Figure 4 presents the corresponding detection rates. The results indicate that the graph representation with explicit privacy and risk relationships captures more simulated conflict cases than the two reference approaches within the constructed evaluation environment.

Table 2: Conflict-detection capability across approaches

Approach	Scenarios with detected conflicts	Detection rate
Matrix based	78	65.0%
Simple dependency graph	95	79.2%
Proposed	112	93.3%

The privacy-aware graph detects most conflicts from contradictory access rules, inconsistent data-retention policies, and mismatched consent coverage. Matrix-based tracing misses conflicts that emerge through multi-hop dependencies.

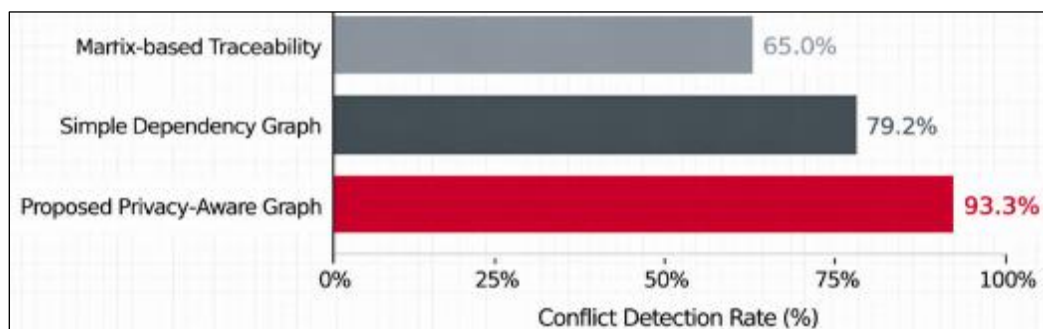


Figure 4: Conflict detection rate across different requirement change scenarios.

Figure 4 compares conflict detection rates across the three approaches. The proposed privacy-aware graph detects conflicts in 93.3% of the simulated requirement-change scenarios, compared with 79.2% for the simple dependency graph and 65.0% for matrix-based traceability.

Table 3 reports risk-identification performance for analytical scoring, ML prediction, and their combined use. The combined analytical and ML configuration achieved 86.3% precision, 84.1% recall, and 85.2% F1 score on the simulated evaluation set. These values describe performance within the constructed simulation and should not be interpreted as validated performance on real healthcare incident data.

Table 3: Risk-identification performance for high-risk state prediction

Model variant	Precision (%)	Recall (%)	F1 score (%)
Analytical scoring only	76.4	71.2	73.7
ML prediction only	81.5	78.9	80.2
Combined (analytical + ML)	86.3	84.1	85.2

The combined model produced the highest precision, recall, and F1 values among the three evaluated variants. Analytical scoring provides a strong baseline rooted in domain logic, while ML adds sensitivity to complex dependency patterns that are hard to encode manually.

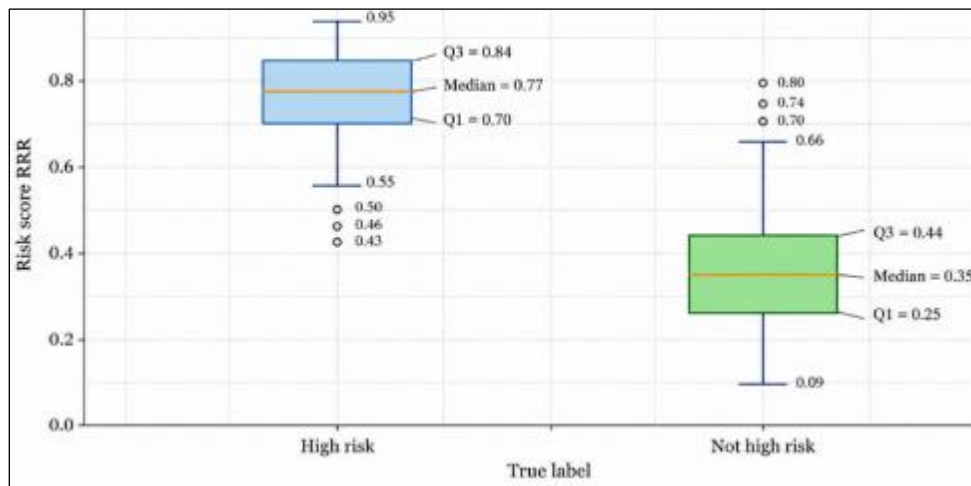


Figure 5: Distribution of predicted risk scores for high-risk and non-high-risk requirement changes.

The box plot shows the distribution of predicted risk scores for high-risk and non-high-risk requirement changes. The median risk score is 0.77 for high-risk cases and 0.35 for non-high-risk cases. Some overlap between the distributions is observed, indicating that the simulated risk scores are not perfectly separated across the two groups.

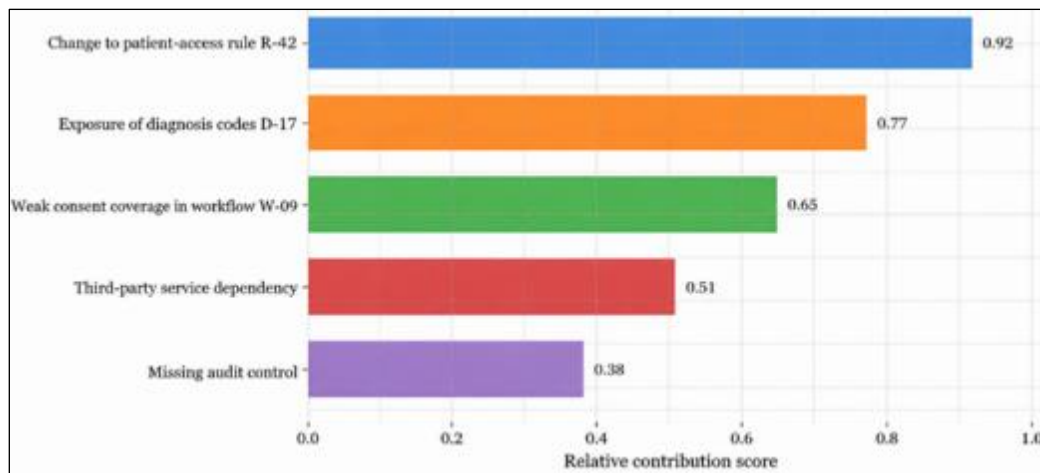


Figure 6: Relative contribution of selected factors associated with predicted requirement-change risk.

This visualization presents relative contribution scores for selected requirements, data elements, and workflow conditions associated with predicted requirement-change risk. The values are shown on a common relative scale to facilitate comparison among the displayed factors. The figure is descriptive and does not represent a causal effect or an independently validated feature-importance measure.

6 DISCUSSION

The combined analytical and ML model provides complementary information in the simulated evaluation. Analytical scoring captures operational and privacy-related factors through predefined rules, while ML identifies patterns in graph derived features. The resulting analysis provides information about requirements, interfaces, data elements, and controls associated with predicted high-risk states within the simulated evaluation. However, the evaluation uses synthetic architectures and simulated scenarios, so the results do not demonstrate effects on real security incidents or operational failures. The traceability graph also provides a structured basis for future privacy and compliance analysis.

6.1 Limitations and Future Work

The evaluation relies on synthetic healthcare architectures and simulated requirement changes rather than production healthcare systems or organizational incident data. The risk scoring and conflict severity parameters use predefined criteria and therefore do not represent empirically calibrated organizational risk preferences. Similarly, the simulated labels used for ML evaluation may not capture the variability and complexity of real healthcare incidents. The evaluation also does not provide independent validation of the framework using real operational data. The machine learning configuration and feature attribution procedure require further specification and testing before the reported metrics can be generalized beyond the simulated evaluation environment. Future work will evaluate the framework using real healthcare systems and organizational incident data, calibrate risk parameters using domain-specific evidence, and test the approach across larger and more diverse interoperability environments. Future studies may also examine time-bound consent, changing regulatory requirements, and cross-jurisdictional privacy constraints.

7 CONCLUSION

This study presented a privacy-aware requirements traceability and risk intelligence framework for interoperable digital health information systems. The framework integrates requirements, system components, workflows, data elements, privacy constraints, security controls, and organizational responsibilities within a multi-relational graph. Analytical risk scoring is combined with explainable machine learning to support high-risk state analysis. In the simulated evaluation, the proposed privacy-aware graph detected conflicts in 112 of 120 simulated requirement-change scenarios, corresponding to a 93.3% detection rate. The combined analytical and ML configuration achieved 86.3% precision, 84.1% recall, and 85.2% F1 score. These results indicate that integrated graph-based traceability can represent multi-hop dependencies and provide structured information about factors associated with simulated high-risk states. The findings are limited to synthetic architectures and simulated requirement changes. Therefore, the reported results should not be interpreted as evidence of performance in production healthcare environments. Future work should evaluate the framework with real healthcare systems and organizational incident data, calibrate risk parameters using empirical evidence, and further specify and validate the machine learning and explanation procedures.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

The authors declare no conflicts of interest regarding this manuscript.

REFERENCES

- [1] Demi, S., Sanchez Gordon, M., & Colomo Palacios, R. (2021). What have we learnt from the challenges of (semi) automated requirements traceability? A discussion on blockchain applicability. *IET Software*, 15(6), 391–411. <https://doi.org/10.1049/sfw2.12035>
- [2] Mucha, J., Kaufmann, A., & Riehle, D. (2024). A systematic literature review of pre requirements specification traceability. *Requirements Engineering*, 29, 119–141. <https://doi.org/10.1007/s00766-023-00412-z>
- [3] Koboyatshwene, T., & Ayalew, Y. (2025). Requirements traceability: A systematic literature review. In *Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing* (pp. 1509–1513). Association for Computing Machinery. <https://doi.org/10.1145/3672608.3707952>
- [4] Torab-Miandoab, A., Samad-Soltani, T., Jodati, A., & Rezaei-Hachesu, P. (2023). Interoperability of heterogeneous health information systems: A systematic literature review. *BMC Medical Informatics and Decision Making*, 23, Article 18. <https://doi.org/10.1186/s12911-023-02115-5>
- [5] 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, e45209, 2024, doi: 10.2196/45209.
- [6] Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, 22(2), 177–183. <https://doi.org/10.1016/j.eij.2020.07.003>
- [7] Loh, H. W., Ooi, C. P., Seoni, S., Barua, P. D., Molinari, F., & Acharya, U. R. (2022). Application of explainable artificial intelligence for healthcare: A systematic review of the last decade (2011–2022). *Computer Methods and Programs in Biomedicine*, 226, 107161. <https://doi.org/10.1016/j.cmpb.2022.107161>
- [8] Niu, S., Yin, Q., Ma, J., Song, Y., Xu, Y., Bai, L., Pan, W., & Yang, X. (2024). Enhancing healthcare decision support through explainable AI models for risk prediction. *Decision Support Systems*, 181, 114228. <https://doi.org/10.1016/j.dss.2024.114228>
- [9] Afrin, S. (2025). Cyber-resilient infrastructure for public internet service providers using automated threat detection. *World Journal of Advanced Engineering Technology and Sciences*, 17(02), 127–140. Article DOI: <https://doi.org/10.30574/wjaets.2025.17.2.1475>.
- [10] Farooq, H. (2025). Cross-platform backup and disaster recovery automation in hybrid clouds. *International Journal of Science and Innovation Engineering*, 2(11), 220–242. <https://doi.org/10.70849/IJSCI02112025025>
- [11] Saeed, H. N. (2025). Hybrid perovskite-CIGS solar cells with machine learning-driven performance prediction. *International Journal of Science and Innovation Engineering*, 2(11), 262–280. <https://doi.org/10.70849/IJSCI02112025027>
- [12] Zaman, M. T. (2025). Enhancing grid resilience through DMR trunking communication systems. *World Journal of Advanced Engineering Technology and Sciences*, 17(03), 197–212. <https://doi.org/10.30574/wjaets.2025.17.3.1551>
- [13] Islam, S. (2025). IPSC-derived cardiac organoids: Modeling heart disease mechanism and advancing regenerative therapies. *World Journal of Advanced Engineering Technology and Sciences*, 17(03), 227–239. <https://doi.org/10.30574/wjaets.2025.17.3.1553>
- [14] Karim, M. A. (2025). An IoT-enabled exoskeleton architecture for mobility rehabilitation derived from the ExoLimb methodological framework. *IJSRED - International Journal of Scientific Research and Engineering Development*, 8(6), 2265–2277. <https://doi.org/10.5281/zenodo.17926861>
- [15] Rahman, T. (2026). Financial Risk Intelligence: Real-Time Fraud Detection and Threat Monitoring. Zenodo. <https://doi.org/10.5281/zenodo.18176490>
- [16] Rabbi, M. S. (2026). AI-Driven SCADA Grid Intelligence for Predictive Fault Detection, Cyber Health Monitoring, and Grid Reliability Enhancement. Zenodo. <https://doi.org/10.5281/zenodo.18196487>

- [17] Zaman, S. U., Afrin, S., Zaidi, S. K. A., & Islam, K. S. A. (2026). Resilient edge computing framework for autonomous, secure, and energy-aware systems. *World Journal of Advanced Engineering Technology and Sciences*, 18(01), 105–121. <https://doi.org/10.30574/wjaets.2026.18.1.1577>
- [18] Fazle, A. B., Taimun, M. T. Y., Fareed, S. M., & Alam, M. S. (2026). Ergonomic and automation based process redesign in industrial workstations. *Global Journal of Engineering and Technology Advances*, 26(01), 091–108. <https://doi.org/10.30574/gjeta.2026.26.1.0010>
- [19] Nahar, S., Rahman, F., & Mim, M. A. (2026). AI-integrated renewable energy and data analytics platform for corporate ESG compliance. *World Journal of Advanced Engineering Technology and Sciences*, 18(01), 219–235. <https://doi.org/10.30574/wjaets.2026.18.1.0031>
- [20] Fahim, M. A. I., Farooq, H., & Sharan, S. M. M. I. (2026). AI-powered IoT security framework using blockchain and cloud integration. *Global Journal of Engineering and Technology Advances*, 26(01), 168–185. <https://doi.org/10.30574/gjeta.2026.26.1.0003>
- [21] Kamalanathan, S. (2025). Advanced damage detection and load optimization in hybrid composite structures using multi-scale simulation and machine learning. *Saudi Journal of Engineering and Technology*, 10(12), 660–673. <https://doi.org/10.36348/sjet.2025.v10i12.007>
- [22] Karim, M. A., uz Zaman, M. T. ., & Razaq, A. (2026). Integrated Renewable Energy Monitoring and Adaptive Load Optimization Using Smart Grid and Intelligent Control Algorithms. Zenodo. <https://doi.org/10.5281/zenodo.18748205>
- [23] Islam, Md A, “Native Scalable Student Information Systems and Admission Test Automation with Peak Load Architecture Database Performance Optimization and Observability Driven Reliability”. Zenodo, Mar. 12, 2026. doi: 10.5281/zenodo.18987480.
- [24] Mim, M. A. (2026). Cybersecurity risk mitigation in educational and healthcare IT environments. Zenodo. <https://doi.org/10.5281/zenodo.18988585>
- [25] Alam, M. J. (2026). Digital contract lifecycle management systems for corporate governance and regulatory oversight. Zenodo. <https://doi.org/10.5281/zenodo.19007705>
- [26] Meem, S. I. (2026). Socioeconomic determinants of oral-systemic health disparities: A public health policy perspective. Zenodo. <https://doi.org/10.5281/zenodo.19238096>
- [27] Adil, H. M. (2026). Energy-Efficient and Low-Emission Carbon Black Manufacturing through Advanced Process Optimization and Reactor Control. Zenodo. <https://doi.org/10.5281/zenodo.19339048>
- [28] Abid, A. A. (2026). AI-enhanced traffic signal optimization using microscopic simulation models for congestion and emissions reduction in mid-sized U.S. urban corridors. Zenodo. <https://doi.org/10.5281/zenodo.19349723>
- [29] Rohman, H. (2026). AI-based biosensors to detect bacterial and mold contamination, demonstrating their increasing role in ensuring food safety and quality assurance. Zenodo. <https://doi.org/10.5281/zenodo.19456417>
- [30] Asraf, M. S. (2026). Reliability-oriented design optimization of power electronic systems for industrial and utility-scale applications. *Saudi Journal of Engineering and Technology*, 11(4), 184–196. <https://doi.org/10.36348/sjet.2026.v11i04.004>
- [31] Tumpa, S. A., Sharmin, M., Rahman, M. A., & Rohman, H. (2026). Sensor-based monitoring systems for agricultural water management. *Scholars Journal of Engineering and Technology*, 14(05), 194–207. <https://doi.org/10.36347/sjet.2026.v14i05.002>
- [32] Rahat, M. K., Asraf, M. S., Junaid, A., & Islam, M. S. (2026). Communication infrastructure for secure smart meter networks in electric utilities. *Saudi Journal of Engineering and Technology*, 11(5), 450–461. <https://doi.org/10.36348/sjet.2026.v11i05.008>
- [33] Khayyam, F. (2026, April 17). Enterprise scale privacy preserving data fabric architecture for multi tenant AI driven customer relationship management platforms. SSRN <https://doi.org/10.2139/ssrn.6597358>
- [34] Siddiki, A. (n.d.). Vault-based secret management and zero-trust security model for distributed financial applications. Research Square. <https://doi.org/10.21203/rs.3.rs-9916782/v1>
- [35] Khan, M. I., Al Abid, A., Sultana, N., & Avi, S. P. (2026). Sustainable ground improvement using lime-stabilized soils and recycled construction materials: A performance-based evaluation for urban development. *International Journal of Science and Research Archive*, 20(1), 255–268. <https://doi.org/10.30574/ijrsra.2026.20.1.1213>

- [36] Rashid, M. F. (2026, July 2). Artificial intelligence driven lead time and cost forecasting for global apparel merchandising to reduce delays, expedite costs, and total sourcing cost. SSRN. <https://doi.org/10.2139/ssrn.7040180>
- [37] Barua, P. (2026, June 23). Data-driven demand forecasting and inventory optimization for supply chain performance management. SSRN. <https://doi.org/10.2139/ssrn.6982298>
- [38] Huq, S. N. (2026, July 9). A mathematical decision framework for strategic workforce planning and resource allocation under organizational uncertainty. SSRN. <https://doi.org/10.2139/ssrn.7087041>
- [39] Hossain, M. I., Tajik, M. A., Abdullah, M. S., & Al Morshed, S. A. (2026). Lifecycle performance governance for smart buildings and critical infrastructure in sustainable urban systems. *International Journal of Science and Research Archive*, 20(2), 119–131. <https://doi.org/10.30574/ijrsra.2026.20.2.1545>
- [40] Mirza, S., Siddiqui, R., Nahian, A. E. & Bhowmick, N. (2026). Inventory resilience and demand variability modeling for multi-sector organizational operations. *Global Journal of Engineering and Technology Advances*, 28(2), 015–027. <https://doi.org/10.30574/gjeta.2026.28.2.0164>
- [41] Khalid, M. A. (2026). Structural design and optimization of industrial steel structures for process and power plant facilities. SSRN. <https://doi.org/10.2139/ssrn.7205750>
- [42] Junaid, A. (2026, July 29). Performance optimization of 5G NR networks through mobility management and carrier aggregation configuration. SSRN. <https://doi.org/10.2139/ssrn.7202280>
- [43] Al Morshed, S. A., Hossain, M. I., Tajik, M. A., & Abdullah, M. S. (2026). Risk-informed construction delivery for resilient public infrastructure under geotechnical and environmental uncertainty. *Saudi Journal of Engineering and Technology*, 11(8), 698–706. <https://doi.org/10.36348/sjet.2026.v11i08.002>
- [44] Nahar, S. (2026). Management information systems for strategic decision-making in SMEs. SSRN. <https://doi.org/10.2139/ssrn.7204998>
- [45] Islam, M. S. (2026, August 10). Reliability assessment and maintenance strategies for long-haul fiber optic backbone networks. SSRN. <https://doi.org/10.2139/ssrn.7257061>
- [46] Tumpa, S. A. (2026, August 10). Machine learning-based object detection techniques for real-time image recognition applications. SSRN. <https://doi.org/10.2139/ssrn.7257678>
- [47] Siddiqui, R. (2026, August 11). Trust and auditability in generative AI-assisted enterprise reporting systems. SSRN. <https://doi.org/10.2139/ssrn.7263879>
- [48] Ahmed, S. (2026, August 15). Reliability-aware predictive analytics for healthcare service access and resource allocation. SSRN. <https://doi.org/10.2139/ssrn.7289738>
- [49] Rahman, M. M. (2026, August 16). A multi-objective operational optimization model for lean manufacturing and industrial equipment resource allocation. SSRN. <https://doi.org/10.2139/ssrn.7292858>
- [50] Rahman, M. M. (2026). A hybrid digital twin optimization framework for predictive maintenance scheduling in smart manufacturing systems. *Zenodo*. <https://doi.org/10.5281/zenodo.22024323>
- [51] Bhowmick, N. (2026). Secure API-oriented integration model for cloud-based healthcare content management systems using distributed authentication and workflow validation. SSRN. <https://doi.org/10.2139/ssrn.7317678>
- [52] Khalil, S. (2026). Workflow optimization model for cross-functional IT project delivery. SSRN. <https://doi.org/10.2139/ssrn.7328880>
- [53] Siddiqui, R., Nahian, A. E., Bhowmick, N., & Mirza, S. (2026). Auditability and performance monitoring frameworks for enterprise decision-support systems. *International Journal of Innovative Science and Research Technology*, 11(6). <https://doi.org/10.38124/ijisrt/26jun1181>
- [54] Abdullah, M. S., Al Morshed, S. A., Hossain, M. I., & Tajik, M. A. (2026). Reliability-centered foundation and retaining system assessment for sustainable infrastructure delivery. *International Journal of Innovative Science and Research Technology*, 11(8), 425–435. <https://doi.org/10.38124/ijisrt/26aug198>
- [55] Das, N., Rokibuzzaman, M., Kashem, M. A., & Islam, M. R. (2026). Multi-objective resource allocation for resilient financial, healthcare, retail, and logistics service networks. *International Journal of Science and Research Archive*, 20(2), 803–818. <https://doi.org/10.30574/ijrsra.2026.20.2.1666>
- [56] Islam, M. R., Das, N., Nasir, F. B., & Kashem, M. A. (2026). Federated consumer and operational analytics for demand-responsive planning in digital service ecosystems. *Global Journal of Engineering and Technology Advances*, 28(2), 224–237. <https://doi.org/10.30574/gjeta.2026.28.2.0224>

- [57] Ahmed, S. (2026). Interpretable learning for identifying digital access vulnerability in underserved communities. Zenodo. <https://doi.org/10.5281/zenodo.22236720>
- [58] Munna, A. A. (2026, September 2). Requirements traceability and KPI prioritization for agile platform delivery. SSRN. <https://doi.org/10.2139/ssrn.7396839>
- [59] Munna, A. A. (2026). Process intelligence for compliance-aware project governance in digital service organizations. Research Square. <https://doi.org/10.21203/rs.3.rs-10942588/v1>
- [60] Khalil, S. (2026). KPI-based project health assessment model for agile IT operations and service reliability. Research Square. <https://doi.org/10.21203/rs.3.rs-10941682/v1>
- [61] Rahman, M. M. (2026). An integrated decision framework for sustainable and code-compliant building design using building information modeling and multi-criteria performance assessment. Research Square. <https://doi.org/10.21203/rs.3.rs-10987415/v1>
- [62] Rahman, M. M. (2026, September 8). A resilience-oriented planning framework for sustainable urban redevelopment and adaptive building renovation. SSRN. <https://doi.org/10.2139/ssrn.7433038>
- [63] Afroj, S. (2026). Data analytics applications in banking customer service and financial operations management [Preprint]. Research Square. <https://doi.org/10.21203/rs.3.rs-11049828/v1>
- [64] Nasir, F. B., Kashem, M. A., Islam, M. R., & Das, N. (2026). An interoperable management information system for real time payment intelligence, merchandise planning, and distributed workforce coordination. Saudi Journal of Engineering and Technology, 11(9), 825–833. <https://doi.org/10.36348/sjet.2026.v11i09.007>
- [65] Rahman, M. M., Rohan, S. I., Rahman, M., & Arif, J. I. (2026). Multi objective predictive maintenance and energy aware resource optimization for smart industrial systems. International Journal of Science and Research Archive, 20(3), 569–583. <https://doi.org/10.30574/ijrsra.2026.20.3.1763>
- [66] Rohan, S. I., Rahman, M., Arif, J. I., & Rahman, M. M. (2026). Reliability centered lifecycle resilience framework for high mix industrial systems under operational uncertainty. Global Journal of Engineering and Technology Advances, 28(3), 212–225. <https://doi.org/10.30574/gjeta.2026.28.3.0246>
- [67] Mumu, T. S., Ahmed, S., Khalil, S., & Hossain, M. R. (2026). Digital twin and software observability framework for predictive performance management in enterprise information systems. International Journal of Science and Research Archive, 20(3), 584–597. <https://doi.org/10.30574/ijrsra.2026.20.3.1769>
- [68] Zaidi, S. K. A. (2025). Smart sensor integration for energy-efficient avionics maintenance operations. International Journal of Science and Innovation Engineering, 2(11), 243–261. <https://doi.org/10.70849/IJSCI02112025026>
- [69] Ahmed, S., Khalil, S., Hossain, M. R., & Mumu, T. S. (2026). Explainable predictive analytics framework for enterprise workflow risk, delay detection, and adaptive resource allocation. Global Journal of Engineering and Technology Advances, 28(3), 226–239. <https://doi.org/10.30574/gjeta.2026.28.3.0252>
- [70] Arif, A. (2026). Privacy aware and interpretable customer response forecasting for cross-channel digital marketing decision support. SSRN. <https://doi.org/10.2139/ssrn.7498603>
- [71] Arif, A. (2026). Explainable multi objective optimization of digital marketing budget allocation under uncertain consumer response [Preprint]. Preprints.org. <https://doi.org/10.20944/preprints202609.2108.v1>
- [72] Adiluzzaman, A. (2026). Multi-objective patient provider coordination and resource scheduling for integrated digital hospital networks. SSRN. <https://doi.org/10.2139/ssrn.7519498>
- [73] Rahmatullah, R. (2025). Sustainable agriculture supply chains: Engineering management approaches for reducing post-harvest loss in the U.S. International Journal of Scientific Research and Engineering Development, 8(5), 1187–1216. <https://doi.org/10.5281/zenodo.17275907>
- [74] Zaidi, S. K. A. (2025). Intelligent automation and control systems for electric vertical take-off and landing (eVTOL) drones. World Journal of Advanced Engineering Technology and Sciences, 17(2), 63–75. <https://doi.org/10.30574/wjaets.2025.17.2.1457>
- [75] Razaq, A. (2025, October 15). Design and implementation of renewable energy integration into smart grids. TechRxiv. <https://doi.org/10.36227/techrxiv.176049834.44797235/v1>