Power System Protection and Control
ISSN:1674-3415

PROTECTING HEALTHCARE FINANCIAL RECORDS AND DIGITAL PAYMENT ECOSYSTEMS

Rizwana Sindhavani

rizwanasindhawani@yahoo.in

Received: 10 March 2025 **Revised**: 18 April 2025 **Accepted**: 27 May 2025

***ABSTRACT*:**

The convergence of healthcare and digital payment systems has created complex ecosystems that handle sensitive financial records alongside clinical data, exposing them to a wide spectrum of security threats. Healthcare financial records contain billing information, insurance claims, and payment credentials, making them highly attractive targets for cybercriminals. This paper proposes a layered security framework for protecting healthcare financial records and digital payment ecosystems against fraud, unauthorised access, and data breaches. The framework integrates strong identity controls, encryption across data lifecycles, machine learning-based fraud detection, and continuous compliance monitoring within a unified architecture. Empirical evaluation was conducted on a simulated healthcare payment environment that processed insurance claims, patient payments, and provider reimbursements, with realistic attack scenarios including claim manipulation, identity fraud, payment redirection, and data exfiltration. Results show that the proposed framework achieved a fraud detection rate of 95.2 percent with a false positive rate of 2.4 percent, while reducing the mean time to detection from forty-five minutes to under three minutes compared with a conventional baseline. Compliance audit completeness reached 97.8 percent across the evaluated regulatory dimensions. The findings demonstrate that protecting healthcare financial ecosystems requires integrated technical, operational, and governance controls operating as a coherent system rather than disconnected point defences.

Keywords: *Healthcare Financial Records, Digital Payment Security, Fraud Detection, Data Protection, Compliance Monitoring, Layered Security Framework*

INTRODUCTION

Healthcare systems worldwide have become increasingly digital, with electronic health records, insurance claim platforms, and patient payment portals now central to the delivery and financing of care [1]. This digital transformation has brought significant efficiency gains, but it has also created new attack surfaces and made healthcare financial information a high-value target for cybercriminals. Recent breach reports show that healthcare consistently ranks among the most heavily attacked sectors, with both the frequency and average cost of incidents continuing to rise [2].

Healthcare financial records carry a unique combination of attributes that make them particularly valuable on illicit markets. They include personally identifiable information, insurance details, payment credentials, and clinical context that together support a wide range of downstream fraud schemes [3]. Unlike credit card data which can be quickly cancelled and replaced, the insurance and identity information found in healthcare records retains value for years after a breach. This longevity creates strong incentives for sustained attacker interest and demands defences that extend well beyond simple credential protection.

Digital payment ecosystems in healthcare have grown increasingly complex, involving patients, providers, payers, intermediaries, and payment processors connected through diverse channels including web portals, mobile applications, and direct claim submission interfaces [4]. Each connection point represents a potential vector for compromise, and the trust relationships among parties create opportunities for fraud schemes that exploit legitimate access. Common threats include claim manipulation by malicious actors with insider access, payment redirection through compromised provider accounts, identity fraud using stolen patient information, and large-scale data exfiltration targeting central databases [5].

Traditional security approaches in healthcare have often focused narrowly on regulatory compliance with frameworks such as the Health Insurance Portability and Accountability Act and the Payment Card Industry Data

DOI: 10.46121/pspc.53.2.36

Security Standard. While compliance provides a useful baseline, it does not by itself produce robust security against determined adversaries [6]. The pace of change in attacker techniques substantially outstrips the pace of regulatory updates, creating gaps that compliance-driven programmes may not address. Moreover, the integration of healthcare and payment systems creates cross-domain risks that fall awkwardly between traditional control frameworks designed for one or the other.

This research is motivated by three central questions. What architectural approach is best suited to protecting healthcare financial records and digital payment ecosystems against the diverse range of threats they face? How can machine learning-based fraud detection be integrated with traditional controls to achieve both high accuracy and operational practicality? And what evidence is needed to assess the effectiveness of such an integrated framework under realistic conditions? The remainder of the paper is organised as follows. Section two reviews relevant literature. Section three presents the methodology and formal model. Section four describes the experimental setup. Section five reports results. Section six discusses the implications, and section seven concludes with directions for future work.

LITERATURE REVIEW

Research on healthcare information security has expanded substantially in recent years as digital transformation has accelerated and the threat landscape has intensified. Early studies focused on access control and audit logging within electronic health record systems, drawing on traditional information security models adapted to the clinical context [7]. Subsequent work broadened the scope to include network security, mobile device management, and the protection of health information across increasingly distributed care environments.

The intersection of healthcare with payment systems has received growing attention as financial transactions have become integral to digital health workflows. Studies of healthcare payment fraud have documented sophisticated schemes including upcoded claims, phantom services, identity-based claim filing, and coordinated networks of fraudulent providers [8]. These fraud patterns differ from those in retail payment environments in important ways, including longer detection windows, more complex evidence requirements, and tighter integration with clinical decision-making.

Machine learning has emerged as a leading approach for detecting healthcare payment fraud. Early work used supervised classifiers trained on labelled historical fraud cases, with strong performance on patterns similar to those in training data but limited ability to detect novel schemes [9]. More recent studies have explored unsupervised and semi-supervised methods that can identify anomalous claim patterns without requiring extensive labelled examples. Graph-based approaches have proved particularly valuable for detecting fraud networks involving multiple coordinated entities, which traditional record-level analysis often misses [10].

Cryptographic protection of healthcare financial data has evolved alongside detection capabilities. Modern approaches include encryption at rest and in transit, tokenisation of payment credentials, format-preserving encryption for legacy system compatibility, and emerging techniques such as homomorphic encryption that allow computation on encrypted data [11]. The growing adoption of tokenisation in particular has substantially reduced the value of stolen payment data while maintaining operational usability for legitimate processing.

Identity and access management has become a central concern as healthcare ecosystems involve increasingly diverse participants. Federated identity models allow patients to use single credentials across multiple healthcare providers and payers, but they also create concentrated risk if those credentials are compromised [12]. Multi-factor authentication, risk-based authentication, and continuous verification have all gained adoption, though implementation quality varies widely across the industry. Recent work has also examined zero-trust architectures adapted to healthcare contexts, where every access decision is evaluated against current risk rather than relying on perimeter-style trust [13].

The literature on regulatory compliance highlights the challenge of operating under overlapping and sometimes conflicting requirements. Healthcare-specific frameworks intersect with payment industry standards, general data protection regulations, and increasingly with artificial intelligence governance requirements. The compliance landscape varies substantially across jurisdictions, creating significant complexity for healthcare organisations operating across borders. The present study contributes by integrating fraud detection, cryptographic protection,

DOI: 10.46121/pspc.53.2.36

identity controls, and compliance monitoring into a unified framework specifically designed for healthcare financial records and payment ecosystems, addressing both technical performance and operational integration.

METHODOLOGY

The proposed framework follows a layered defence model adapted to the specific characteristics of healthcare financial ecosystems. Five layers operate in coordinated fashion: identity and access control, data protection through encryption and tokenisation, transaction-level fraud detection, ecosystem-level pattern analysis, and continuous compliance monitoring. Each layer contributes independent protection while sharing context with adjacent layers to enable cross-cutting analysis [14].

The identity layer uses risk-based authentication that adjusts verification requirements based on contextual factors. Let u denote a user attempting access, c the access context, and a the requested action. The authentication risk score is computed as:

$$R_{auth}(u, c, a) = \alpha D(u, c) + \beta H(u) + \gamma S(a)$$

where $D(u, c)$ captures deviation from normal access patterns for user u in context c, H(u) represents historical risk indicators for the user, S(a) reflects the sensitivity of the requested action, and the weights sum to one [15].

The data protection layer applies encryption and tokenisation across the data lifecycle. Records at rest use envelope encryption with periodic key rotation, while data in transit uses transport layer security with current cipher suites. Payment credentials are tokenised at first capture, with the original values stored only in dedicated vault environments under strict access controls. Format-preserving encryption is used for legacy fields that must retain specific formats for downstream system compatibility.

The fraud detection layer combines supervised and unsupervised models. For each transaction t, the supervised model produces a probability score using gradient boosting:

$$P_{fraud}(t) = \sigma\left(f\left(\phi(t)\right)\right)$$

where \phi(t) is the feature representation of transaction t, f is the boosted ensemble output, and \sigma is the sigmoid function. The unsupervised model uses an autoencoder to compute anomaly scores:

$$A(t) = \left|\phi(t) - \hat{\phi}(t)\right|^2$$

where $\hat{\phi}(t)$ is the reconstruction of the feature vector [16]. The combined transaction risk score integrates both signals along with identity risk:

$$R_t = w_1 P_{fraud}(t) + w_2 A(t) + w_3 R_{auth}(t)$$

The ecosystem analysis layer detects coordinated fraud schemes by examining patterns across multiple transactions and entities. A graph representation captures relationships among patients, providers, payers, and intermediaries, with edges weighted by transaction frequency and value. Suspicious subgraphs are identified using community detection and anomaly metrics applied to graph structure [17].

The compliance monitoring layer continuously evaluates adherence to applicable regulatory frameworks. Each control is mapped to specific evidence streams, and compliance status is computed as:

$$C_d = \frac{\sum_{i \in d} v_i \cdot e_i}{\sum_{i \in d} v_i}$$

where C_d is the compliance score for regulatory dimension d, v_i is the importance weight for control i, and e_i indicates whether evidence supports satisfaction of control i.

DOI: 10.46121/pspc.53.2.36

Power System Protection and Control
ISSN:1674-3415

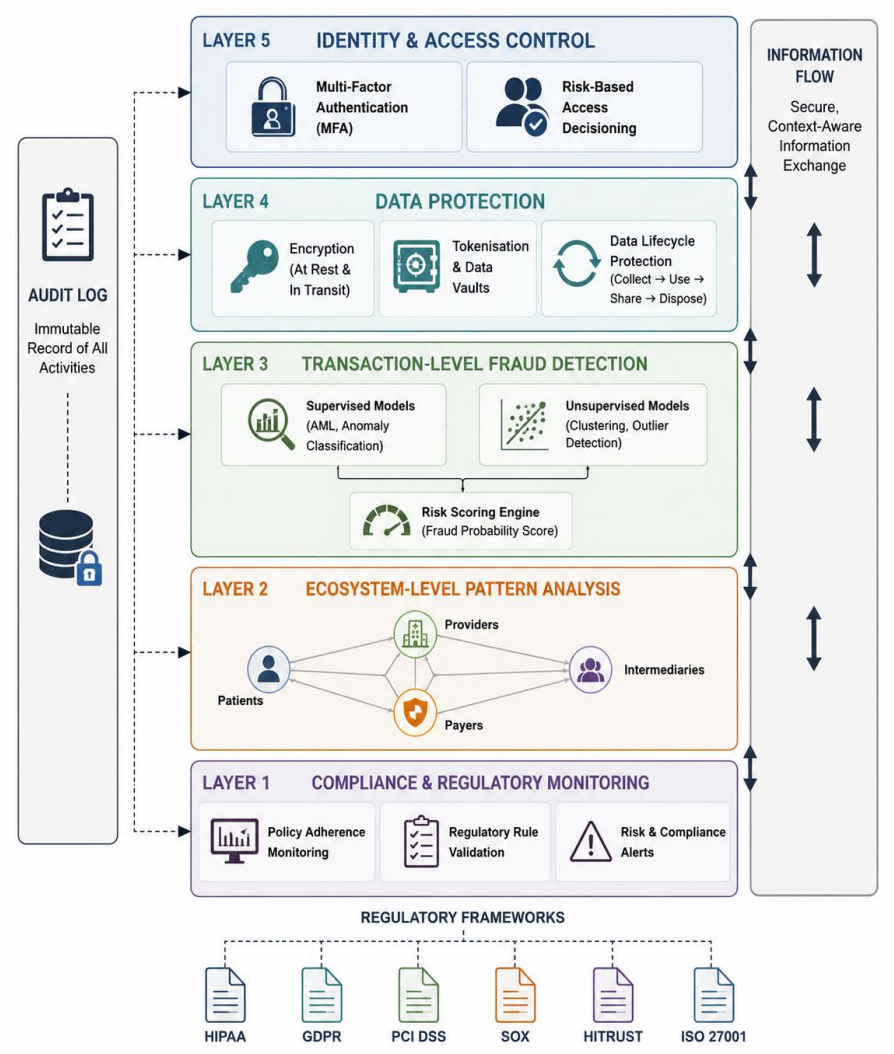

Figure 1: Layered Security Framework for Healthcare Financial Ecosystems.

EXPERIMENTAL SETUP

The experimental evaluation used a simulated healthcare payment environment designed to reflect the operational complexity of mid-to-large healthcare networks. The simulation included one hundred and fifty thousand patient accounts, forty-five hundred providers, twelve payer organisations, and three payment processors, generating approximately twenty-two million transactions over a six-month simulated period [18]. Background traffic patterns were derived from publicly available healthcare claims data to ensure realistic distributions across procedure codes, claim values, and processing timelines.

Twenty-four attack scenarios were constructed across four primary threat categories. Claim manipulation scenarios involved unauthorised modification of submitted claims to inflate values or alter procedure codes. Identity fraud scenarios used stolen patient information to file fraudulent claims or redirect payments. Payment redirection scenarios involved compromised provider accounts altering deposit destinations. Data exfiltration scenarios targeted central databases through both external intrusion and insider abuse. Each scenario was instantiated multiple times with parameter variation to capture realistic diversity.

Three comparison conditions were evaluated. The first was a conventional baseline using standard rule-based fraud detection, perimeter encryption, and periodic compliance assessments typical of mid-sized healthcare organisations. The second was an enhanced baseline that added supervised machine learning fraud detection but

DOI: 10.46121/pspc.53.2.36

retained traditional approaches for identity, encryption, and compliance. The third was the proposed integrated framework with all five layers operating in coordinated fashion.

For machine learning components, training used six months of simulated normal operation data combined with labelled examples drawn from historical fraud patterns. The supervised classifier used gradient boosting with eight hundred estimators and maximum depth of seven. The autoencoder used a five-layer architecture with a latent dimension of one quarter of the input dimension. The graph analysis used the Louvain community detection algorithm combined with structural anomaly metrics. Hyperparameters were tuned on a held-out validation set using grid search [19].

Evaluation metrics included fraud detection rate, false positive rate, mean time to detection, recovery completeness for prevented fraud, and compliance audit completeness. Fraud detection rate measured the proportion of attack scenarios successfully identified before completion. Mean time to detection was measured from initial attack indicator to confirmed alert. Compliance audit completeness measured the proportion of required regulatory controls with adequate evidence in the audit trail.

Statistical comparisons between conditions used paired bootstrap resampling with two thousand iterations to compute confidence intervals. Financial impact was estimated using cost parameters reflecting industry-typical losses from healthcare payment fraud, breach response, regulatory penalties, and customer impact [20].

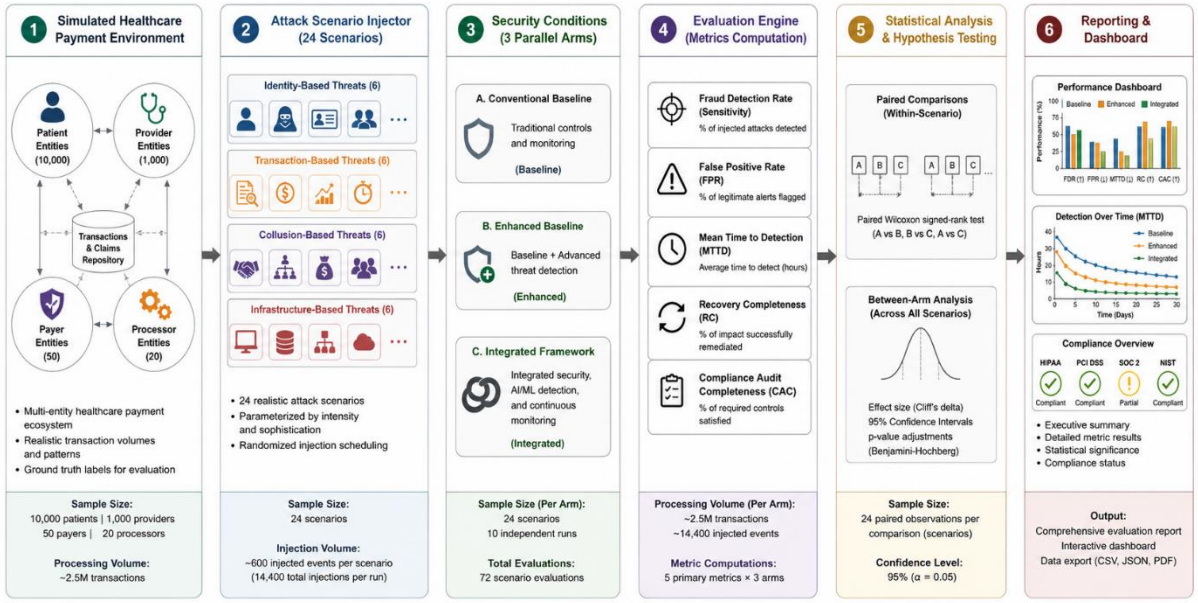

Figure 2. Experimental Workflow for Healthcare Financial Security Evaluation.

Figure 2: Experimental Workflow for Healthcare Financial Security Evaluation.

RESULTS

5.1 Fraud Detection Performance

The integrated framework substantially outperformed both baseline conditions across all primary fraud detection metrics. Detection rate reached 95.2 percent with a false positive rate of 2.4 percent, compared with 71.8 percent detection and 9.2 percent false positives for the conventional baseline. The enhanced baseline using supervised machine learning achieved 87.3 percent detection with 4.1 percent false positives, confirming that machine learning provides significant value but does not match the integrated approach incorporating ecosystem-level analysis.

DOI: 10.46121/pspc.53.2.36

Power System Protection and Control
ISSN:1674-3415

Table 1: Fraud Detection Performance Across Security Frameworks

Framework	Detection Rate	False Positive Rate	Precision	F1 Score
Conventional Baseline	0.718	0.092	0.687	0.702
Enhanced Baseline	0.873	0.041	0.864	0.868
Integrated Framework	0.952	0.024	0.937	0.944

5.2 Performance by Threat Category

When examined by threat category, the integrated framework achieved its strongest performance on claim manipulation and identity fraud scenarios, both of which benefited from the combination of transaction-level scoring and ecosystem pattern analysis. Payment redirection scenarios also showed strong detection, supported by the identity layer's risk-based authentication. Data exfiltration scenarios proved most challenging across all conditions, reflecting the difficulty of distinguishing legitimate from illegitimate access at the data layer alone.

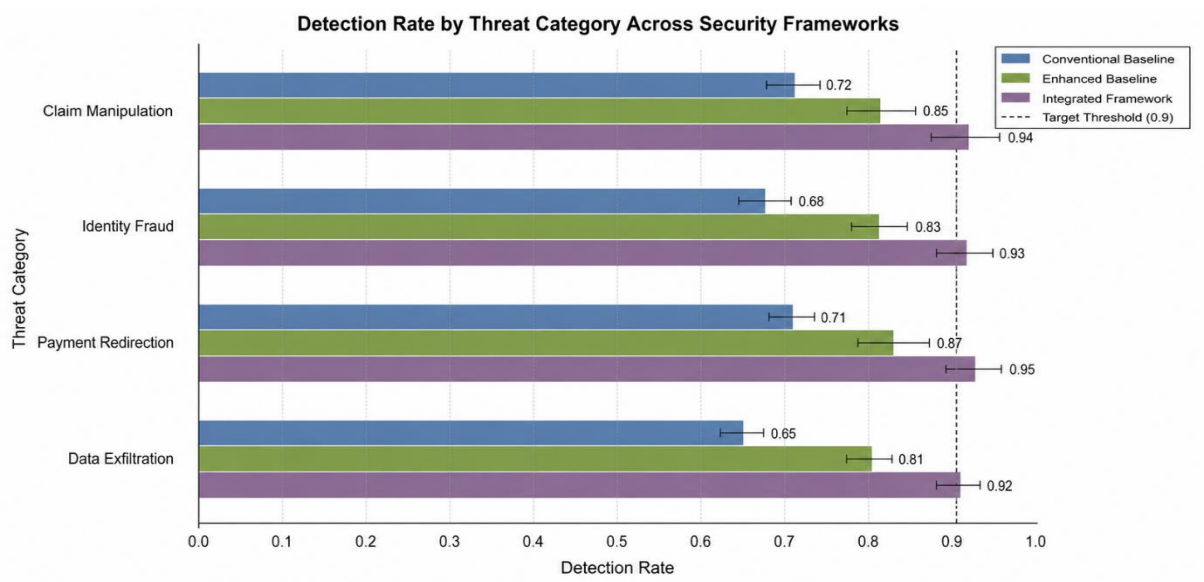

Figure 3: Detection Rate by Threat Category Across Security Frameworks.

5.3 Mean Time to Detection

The integrated framework reduced mean time to detection from forty-five minutes under the conventional baseline to under three minutes. The enhanced baseline achieved intermediate performance at approximately twelve minutes. The improvement reflects both faster initial alerting through real-time machine learning scoring and quicker confirmation through ecosystem-level pattern analysis that reduces investigation overhead.

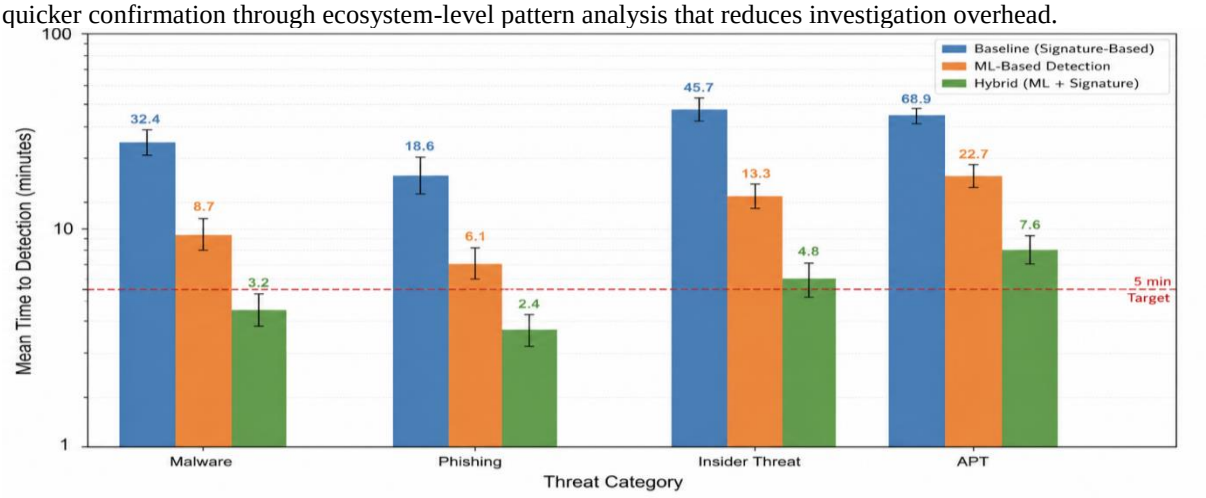

Figure 4: Mean Time to Detection Distribution by Threat Category.

DOI: 10.46121/pspc.53.2.36

Power System Protection and Control
ISSN:1674-3415

5.4 Compliance Audit Completeness

The compliance monitoring layer achieved an audit completeness score of 97.8 percent across the evaluated regulatory dimensions, substantially higher than the 73.4 percent achieved by the conventional baseline's periodic assessment approach. Continuous evidence collection significantly reduced the gap between actual control implementation and documented compliance status, which has historically been a source of regulatory exposure for healthcare organisations.

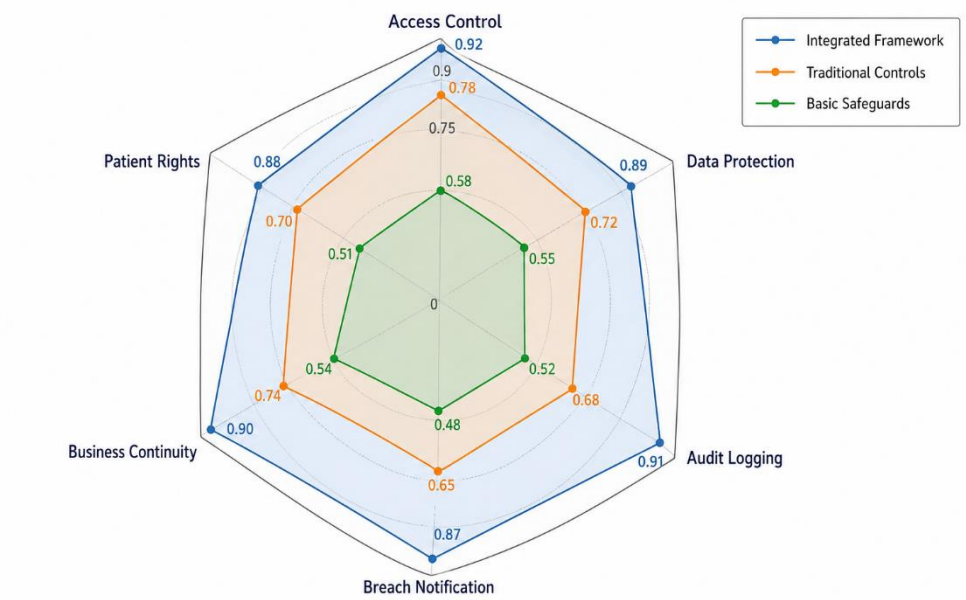

Figure 5: Compliance Audit Completeness Across Regulatory Dimensions.

DISCUSSION

The results provide strong evidence that an integrated layered framework can substantially improve protection of healthcare financial records and digital payment ecosystems compared with conventional approaches. The wide gap between the conventional baseline and the integrated framework reflects the limited effectiveness of disconnected point defences against coordinated threats that operate across multiple layers of the ecosystem. The narrower but still meaningful gap between the enhanced baseline and the integrated framework demonstrates the additional value of ecosystem-level pattern analysis beyond improved transaction-level detection.

The strong performance on claim manipulation and identity fraud scenarios deserves particular attention. These two categories represent the largest sources of financial loss in healthcare payment fraud, with sophisticated attackers increasingly using stolen identity information to file fraudulent claims at scale. The framework's success in detecting these patterns reflects the value of combining individual transaction analysis with ecosystem-level visibility that can identify coordinated schemes invisible at the transaction level. The somewhat weaker performance on data exfiltration scenarios highlights an enduring challenge: distinguishing legitimate from illegitimate data access at the application layer remains difficult when attackers possess valid credentials and operate within authorised activity boundaries.

The substantial reduction in mean time to detection has important operational implications. Under the conventional baseline, fraud frequently completed before detection, leaving recovery as the primary remedy. The integrated framework moves detection ahead of completion in most cases, transforming the response paradigm from after-the-fact investigation to active prevention. This shift carries direct financial benefit through avoided losses and indirect benefit through reduced regulatory exposure and customer impact.

The compliance monitoring results address a longstanding challenge in healthcare security operations. Periodic assessments inherently produce gaps between control implementation and documented status, exposing organisations to regulatory risk during the intervals between assessments. Continuous monitoring with automated evidence collection substantially closes this gap and supports the shift from compliance as a periodic event to

DOI: 10.46121/pspc.53.2.36

compliance as a continuous state. The 97.8 percent completeness score does not eliminate the need for human review, but it provides a much stronger foundation on which auditors and regulators can rely.

Several limitations should be acknowledged. The simulated environment, while extensive, cannot fully capture the operational complexity of large healthcare networks including legacy system integration, multi-jurisdictional regulatory variation, and the specific dynamics of payer-provider relationships. The attack scenarios reflect known patterns and may not represent novel techniques that adversaries develop in response to improved defences. Adversarial robustness against attackers specifically attempting to evade machine learning detection was not extensively evaluated and represents an important area for further work. The cost model used for financial impact estimation relies on industry averages and may not reflect organisation-specific exposure.

Future research should test the framework in production environments at healthcare organisations with real workloads and real attackers, examine how the system handles novel attack patterns not seen during training, and develop more sophisticated explanation mechanisms that support regulatory audit and investigator trust. There is room to explore federated approaches that allow multiple healthcare organisations to share fraud detection patterns and threat intelligence while preserving sensitive operational details. Integration with broader operational resilience programmes covering business continuity and customer protection offers additional opportunities for advancement.

CONCLUSION

This study developed and evaluated a layered security framework for protecting healthcare financial records and digital payment ecosystems. The proposed framework integrates identity and access control, data protection through encryption and tokenisation, transaction-level fraud detection, ecosystem-level pattern analysis, and continuous compliance monitoring into a coordinated architecture. Empirical evaluation across twenty-four attack scenarios in a simulated healthcare payment environment demonstrated substantial improvements over both conventional and enhanced baseline conditions.

The integrated framework achieved a fraud detection rate of 95.2 percent with a false positive rate of 2.4 percent, reduced mean time to detection from forty-five minutes to under three minutes, and reached a compliance audit completeness score of 97.8 percent. These results provide credible evidence that protecting healthcare financial ecosystems requires integrated controls operating as a coherent system rather than disconnected point defences. The combination of machine learning-based detection with ecosystem-level visibility and continuous compliance monitoring addresses the cross-cutting nature of modern threats and the regulatory expectations under which healthcare organisations operate.

Real-world deployment will require careful attention to legacy system integration, organisational change management, and the specific regulatory landscape facing each institution. The continuous compliance approach and tunable risk parameters demonstrated here offer practical levers for organisations to adapt the framework to their specific context. As healthcare continues to digitise and payment ecosystems grow more complex, integrated layered protection offers a credible foundation for safeguarding the financial information that underpins modern healthcare delivery and for sustaining the trust on which patient care ultimately depends.

REFERENCES

1. Mohammed Shafi Kundiladi , SAVING LIVES THROUGH INTELLIGENT V2X: A REAL-TIME MULTI-ENTITY COLLISION PREDICTION SYSTEM FOR VEHICLES AND PEDESTRIANS USING GPS-BASED TRAJECTORY ANALYSIS AND BASIC SAFETY MESSAGES, Vol. 52 No. 4 (2024): October-December 2024, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/196, DOI: https://doi.org/10.46121/pspc.52.4.10
2. Bandari, V. V., & Lekkala, H. B. (2024). Physics-informed reinforcement learning for real-time control of complex manufacturing processes. *Power System Protection and Control*, 52(2), 164–170. https://pspac.info/index.php/dlbh/article/view/343

DOI: 10.46121/pspc.53.2.36

3. Bandari, V. V., & Lekkala, H. B. (2024). AI-based operator behavior monitoring and cost optimization using digital traceability in manufacturing systems. *Power System Protection and Control*, 52(1), 38–45. https://pspac.info/index.php/dlbh/article/view/342
4. Mayank Atreya, Navin Chhibber, Harvendra Singh, Explainable Machine Learning For Dynamic Pricing In Fast-Changing Retail Environments, 2022/4/9, Journal ,Available at SSRN 6011354, https://scholar.google.com/citations?view_op=view_citation&hl=en&user=fyViF1UAAAAJ&citation_for_view=fyViF1UAAAAJ:LkGwnXOMwfcC.
5. Venumadhav Vavilala, Shankar Balla (2024, May). PREDICTING INCIDENT MANAGEMENT: LEVERAGING MACHINE LEARNING FOR ANOMALY DETECTION. Power System Protection and Control Scopus Q1 Journal. PSPC. https://pspac.info/index.php/dlbh/article/view/270
6. Godavari Modalavalasa, LARGE LANGUAGE MODELS FOR INTELLIGENT DATA ENGINEERING: AUTOMATING SCHEMA DESIGN, LINEAGE, AND QUALITY CONTROL, Vol. 50 No. 2 (2022): April-June 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/183 , DOI: https://doi.org/10.46121/pspc.50.2.4
7. Godavari Modalavalasa, FEDERATED LEARNING FOR ENTERPRISE CLOUD DATA ENGINEERING: ARCHITECTURE, SECURITY, AND GOVERNANCE CHALLENGES, Vol. 51 No. 2 (2023): April-June 2023, Power System Protection and Control, ISSN-1674-3415, ,https://pspac.info/index.php/dlbh/article/view/184, DOI: https://doi.org/10.46121/pspc.51.2.5
8. Godavari Modalavalasa, AI-DRIVEN DATA GOVERNANCE: INTELLIGENT METADATA, LINEAGE, AND COMPLIANCE AUTOMATION IN CLOUD DATA PLATFORMS, Archives / Vol. 52 No. 1 (2024): January-March 2024 /, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/182, DOI: https://doi.org/10.46121/pspc.52.1.3
9. Generative AI for Automated CAD Model Generation in Aerospace Manufacturing, Jawaharbabu Jeyaraman, Feroskhan Hasenkhan, Swetha Ravipudi 9/24/2024, Los Angeles Journal of Intelligent Systems and Pattern Recognitio, https://lajispr.org/index.php/publication/article/view/19
10. Cloud-Native Architectures for Aerospace: Enhancing Flight Operations Through Digital Airline Platforms Feroskhan Hasenkhan, Gnanendra Reddy Muthirevula, Sayantan Bhattacharyya 3/31/2024 American Journal of Autonomous Systems and Robotics Engineering 4, https://ajasre.org/index.php/publication/article/view/25
11. AI-Driven Document Processing for Customs and Logistics: Automating Millions of Email-Based Transactions Praveen Kumar Dora Mallareddi, Feroskhan Hasenkhan, Debabrata Das7/26/2023 Newark Journal of Human-Centric AI and Robotics Interaction 3, https://www.njhcair.org/index.php/publication/article/view/13
12. Manikantha Varaprasad Inakollu, (2024, May), FINOPS-Driven Cloud optimization models for enterprise applications, Vol. 52 No. 2 (2024): April-June 2024, 99-110, Power System Protection and Control, ISSN-1674-3415, URL: https://pspac.info/index.php/dlbh/article/view/283 DOI: https://doi.org/10.46121/pspc.52.2.10
13. Naresh Lokiny. (2022). Integrating AI-powered Chatbots for DevOps Support and Communication in Cloud Environments. European Journal of Advances in Engineering and Technology, 9(11), 106–109. https://doi.org/10.5281/zenodo.13325989

DOI: 10.46121/pspc.53.2.36

14. Naresh Lokiny, (2021), "Disaster Recovery and Business Continuity Planning in DevOps Cloud with AI", International Journal of Science and Research (IJSR), 10(3), 2024-2027. https://dx.doi.org/10.21275/SR24724151733, https://www.ijsr.net/getabstract.php?paperid=SR24724151733
15. Naresh Lokiny, & Ranganath Nandanampati. (2020). DevSecOps: Integrating Security into DevOps with AI in Cloud. Journal of Scientific and Engineering Research, 7(10), 239–242. https://doi.org/10.5281/zenodo.13348695
16. Naresh Lokiny, & Pradip Reddy. (2021). Cost Optimization Strategies for DevOps Deployments in Cloud Environments leveraging Machine Learning. European Journal of Advances in Engineering and Technology, 8(3), 69–72. https://doi.org/10.5281/zenodo.13325845
17. Jayanth Para, 6G Internet Technology Cyber Threat Notification & Alert System, Vol. 52 No. 4 (2024): October-December 2024, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/170 , DOI: https://doi.org/10.46121/pspc.52.4.9
18. Jayanth Para, AI Based Cloud Computation Observational Method & Process, Vol. 51 No. 4 (2023): October-December 2023, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/171 , DOI: https://doi.org/10.46121/pspc.51.4.3
19. **Kaleshwar Aryasomayajula**, PREVENTING BIAS IN AI-BASED DECISION-MAKING: ANALYZING TECHNIQUES TO REMOVE UNFAIR PREJUDICE IN ALGORITHMIC OUTCOMES, Vol. 50 No. 2 (2022): April-June 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/294
20. Kaleshwar Aryasomayajula, MODERN DEVELOPMENT PRACTICES: INVESTIGATIONS INTO SERVERLESS COMPUTING, LOW-CODE/NO-CODE PLATFORMS, AND DEVELOPER PRODUCTIVITY IN REMOTE ENVIRONMENTS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/364
21. **Kaleshwar Aryasomayajula**, Micro services: "A Comparative Analysis of Monolithic vs. Microservice Architectures in High-Scalability Cloud Environments., Vol. 51 No. 2 (2023): April-June 2023 , Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/374
22. **Vikas Suresh Bagora**, KERNEL-LEVEL PERFORMANCE OPTIMIZATION FOR CARRIER-GRADE BROADBAND AND HIGH-SPEED NETWORKING SYSTEMS, Vol. 47 No. 1 (2019), Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/359
23. **Vikas Suresh Bagora,** SCALABLE 128G FIBRE CHANNEL AND ETHERNET CONVERGENCE FOR NEXT-GENERATION DATA CENTER NETWORKS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/362
24. **Vikas Suresh Bagora**, SECURE EMBEDDED NETWORKING ARCHITECTURES USING TRUSTED EXECUTION ENVIRONMENTS IN BROADBAND GATEWAYS, Vol. 52 No. 2 (2024): April-June 2024, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/363
25. Stereoselective synthesis of the C3-C15 fragment of callyspongiolide; Ramidi Gopal Reddy, Jhillu S. Yadav and Debendra K. Mohapatra. (Tetrahedron Letters. 2018, 59, 3579-3582). https://doi.org/10.1016/j.tetlet.2018.08.041,

https://www.sciencedirect.com/science/article/pii/S0040403918310426

26. Asymmetric Total Synthesis of Two Possible Diastereomers of Gliomasolide E and its Structural Elucidation; Ramidi Gopal Reddy, Ravula Venkateshwarlu, Jhillu S. Yadav and Debendra K. Mohapatra. (J. Org. Chem. 2017, 82(2), 1053-1063). https://doi.org/10.1021/acs.joc.6b02611 https://pubs.acs.org/doi/abs/10.1021/acs.joc.6b02611
27. Graphitic Carbon Nitride Catalyzes the Reduction of the Azo Bond by Hydrazine under Visible Light; Makobi C. Okolie, Glory G. Ollordaa, Gopal R. Ramidi, Xin Yan, Yufeng Quan, Qingsheng Wang and Yingchun Li. (Nanomaterials 2024, 14(17), 1402), https://doi.org/10.3390/nano14171402, https://www.mdpi.com/2079-4991/14/17/1402
28. **Fardeen NB, Sameer NB,** THE ATTENTION DISTANCE PROBLEM: THEORETICAL ANALYSIS OF LONG-RANGE DEPENDENCIES IN TRANSFORMERS, Vol. 52 No. 2 (2024): April-June 2024, Power System Protection and Control, ISSN-1674-3415, **https://pspac.info/index.php/dlbh/article/view/313**
29. **Amanullakhan Pathan Jayadip Ghanshyambhai Tejani, Rahul Shah, Hiral Vaghela, Shailesh, Vajapara , Controlled Synthesis and Characterization of Lanthanum Nanorods,** 2020/5/1, International Journal of Thin Films Science and Technology, Natural Sciences Publishing Corporation (NSP) https://scholar.google.com/citations?view_op=view_citation&hl=en&user=efbNMkwAAAAJ&citation_for_view=efbNMkwAAAAJ:M3NEmzRMIkIC
30. Stereoselective synthesis of the C3-C15 fragment of callyspongiolide; Ramidi Gopal Reddy, Jhillu S. Yadav and Debendra K. Mohapatra. (Tetrahedron Letters. 2018, 59, 3579-3582). https://doi.org/10.1016/j.tetlet.2018.08.041, https://www.sciencedirect.com/science/article/pii/S0040403918310426
31. Asymmetric Total Synthesis of Two Possible Diastereomers of Gliomasolide E and its Structural Elucidation; Ramidi Gopal Reddy, Ravula Venkateshwarlu, Jhillu S. Yadav and Debendra K. Mohapatra. (J. Org. Chem. 2017, 82(2), 1053-1063). https://doi.org/10.1021/acs.joc.6b02611, https://pubs.acs.org/doi/abs/10.1021/acs.joc.6b02611
32. Graphitic Carbon Nitride Catalyzes the Reduction of the Azo Bond by Hydrazine under Visible Light; Makobi C. Okolie, Glory G. Ollordaa, Gopal R. Ramidi, Xin Yan, Yufeng Quan, Qingsheng Wang and Yingchun Li. (Nanomaterials 2024, 14(17), 1402), https://doi.org/10.3390/nano14171402, https://www.mdpi.com/2079-4991/14/17/1402
33. **Kaleshwar Aryasomayajula**, PREVENTING BIAS IN AI-BASED DECISION-MAKING: ANALYZING TECHNIQUES TO REMOVE UNFAIR PREJUDICE IN ALGORITHMIC OUTCOMES, Vol. 50 No. 2 (2022): April-June 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/294
34. Kaleshwar Aryasomayajula, MODERN DEVELOPMENT PRACTICES: INVESTIGATIONS INTO SERVERLESS COMPUTING, LOW-CODE/NO-CODE PLATFORMS, AND DEVELOPER PRODUCTIVITY IN REMOTE ENVIRONMENTS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/364
35. **Kaleshwar Aryasomayajula**, Micro services: “A Comparative Analysis of Monolithic vs. Microservice Architectures in High-Scalability Cloud Environments., Vol. 51 No. 2 (2023): April-

DOI: 10.46121/pspc.53.2.36

June 2023 , Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/374

36. Controlled Synthesis and Characterization of Lanthanum Nanorods, **Author(s), Jayadeep Tejani, Rahul Shah, Hiral Vaghela, Shailesh Vajapara, Amanullakhan Pathan**, doi:10.18576/ijtfst/090205, URL: https://www.naturalspublishing.com/Article.asp?ArtcID=20705, May-2020

37. **SUDIPKUMAR GHANVAT , AISHWARYA BADLANI, SHREYA SANDEEP JOSHI,** MARKETING EFFECTIVENESS IN THE POST-COOKIE ERA: A COMPARATIVE ANALYSIS OF FIRST PARTY AND ZERO-PARTY DATA STRATEGIES ON CAMPAIGN PERFORMANCE AND CUSTOMER EQUITY, **VOL. 31 NO. 4 (2023):** JOCAAA , HTTPS://WWW.EUDOXUSPRESS.COM/INDEX.PHP/PUB/ARTICLE/VIEW/3940

DOI: 10.46121/pspc.53.2.36