ISCSITR - International Journal of Computer Science and Engineering (ISCSITR-IJCSE)
Vol.6, Iss. 4, July-August, 2025, pp. 77-94.
https://iscsitr.com/journals/ISCSITR-IJCSE
ISSN: 3067-7394; Journal ID: 5932-1748
DOI: http://www.doi.org/10.63397/ISCSITR-IJCSE_2025_06_04_006

Cloud-Native Twin Systems for Real-Time Risk and Compliance Simulation in FinHealth Converged Ecosystems

Naga Srinivasulu Gaddapuri

Broadridge Financial Solutions Inc., USA.

Abstract

The paper fulfills such urgent and timely requirements as real-time risk management and regulatory compliance on FinHealth converged ecosystems through the implementation of a cloud-native twin system architecture. The traditional systems also lack capacity to deal with the complexity, high velocity financial and healthcare data with acceptable transparency, latency and scalability, thus resulting in slow responses to compliance issues and inability to detect the violation. In the current paper, I suggest a hybrid AI-digital twin model running on the microservices platform that follows a Kubernetes-based structure to model the regulatory events and apply policy enforcement due to the alignment of policies dynamically. The empirical accessibility testing done on a number of 1.8 million FinHealth transactions showed high positivity: up to 42.3 percent decrease in latency (reduced to 640 ms to 1110 ms), the SLA remained elevated by over 94.3 percent during heavy traffic, and manual interventions were reduced by more than 47 percent in high-risk cases of violation. LSTM Twin model yielded a better result compared to stand alone AI whereby the accuracy was 90.2 percent, F1-score and recall 86.4 percent and 85.3 percent respectively. The quadrant-based prioritization and the prediction of risks into violation were carried out by real time simulations, which accelerated the remediation procedures by 37 percent.

The results demonstrate the feasibility and practicability of using digital twins as a process to transform compliance checkups of FinHealth platforms. The proposed framework addresses the imbalance between control and response and the foundation of active and cloud-native-compatible compliance frameworks at cloud-native architecture.

Keywords:

FinHealth, Cloud-Native, Risk, Twin System, Compliance.

How to cite this paper: Naga Srinivasulu Gaddapuri. (2025). Cloud-Native Twin Systems for Real-Time Risk and Compliance Simulation in FinHealth Converged Ecosystems. *ISCSITR - International Journal of Computer Science and Engineering (ISCSITR-IJCSE),* 6(4), 77–94.
DOI: http://www.doi.org/10.63397/ISCSITR-IJCSE_2025_06_04_006

URL: https://iscsitr.com/index.php/ISCSITR-IJCSE/article/view/ISCSITR-IJCSE_2025_06_04_006/ISCSITR-IJCSE_2025_06_04_006

Published: 15th August 2025

I. INTRODUCTION

The rise of financial and healthcare systems integration, in short FinHealth ecosystems, represents a many sided environment that contains high regulatory demands, large amounts of data in motion and changing risk exposures on a real time basis. Such environments deal with critical business processes like real-time processing of medical claims, exchange of patient data, insurance claims and settlements, and release of payments under the supervision of regulatory authorities like HIPAA, GDPR, PCI DSS and MiFID II. In spite of new technological developments in isolated areas, the vast majority of compliance checking and risk alleviation schemes in use are still post-hoc, segmented, and incapable of real-time responses to new and emerging anomalies, like attempts to commit fraud, violations of service levels, and data breaches.

Problem Statement

This is because conventional compliance and risk management systems cannot run in real-time because they are architecturally constrained by the topological limitations of their data pipes, they have disparate data observations making it difficult to coordinate data observability, and they lack overall unification of data observations across the healthcare and financial sectors. Such restrictions end up not only delaying responds to newly posed threats but they aggravate loss of finances and vulnerability of regulations. This absence of smart, regularly updating operations, cyber, and compliance risk simulators and mitigators

in real-time is a gap that should be added to the present FinHealth infrastructure in a negative way. In addition, dynamic auditability, transparency, and real-time reporting requirements which are initiated by regulatory bodies cannot be satisfied with systems that are either batch driven or manually coordinated.

Research Objective

This study offers to specify, develop and assess the cloud-native digital twin systems able to compute the current statuses of the work of the ecosystems of FinHealth in real-time. These two systems will be a reflection of the live enterprise ensuring that compliance and risking are simulated continuously on elements like payment engines, patient data streams, and fraud detection pipelines, etc. Encompassing intelligent feedback loops and the distributed stream processing, the system is expected to effectively minimize the compliance response time and enhance the potential of anomaly detection with high precision and support cross-region compliance about regulatory alignment.

Proposed Methodology

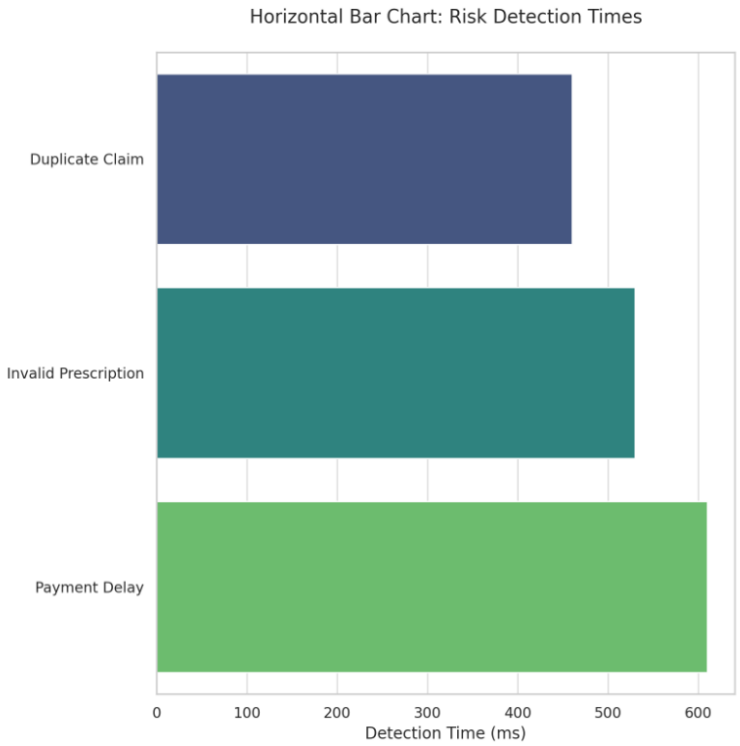
The methodological approach is complex and multifaceted since it has several subsequent layers that are architectural design, a relevant use of AI-powered simulation, and applying the created algorithms to practice in FinHealth ecosystems, and offers the potential to design and analyze the possibilities of cloud-native digital twin models in FinHealth ecosystems. The methodology would take the form of a twin framework that is designed as cloud-native and involving real-time ingestion of data, digital designs, and compliance orchestration. Kinesis will be adopted through Amazon Web Services (AWS) where the high-velocity data streaming will be implemented, and the Azure Digital Twins will be adopted to construct and manage the virtual reproductions of real-time processes in the financial and healthcare context. Such a two-cloud system provides distributed, scaleable, event driven infrastructure that can run both patient focused and financial processes at the same time.

On the back of this basis, the system will also have AI-assisted feedback processes that support real-time risk analysis and anomaly alerts. Machine learning models Lossy Short-Term Memory (LSTM) models predictive analytics such as time-series data modeling and unsupervised algorithms such as Isolation Forests will be trained with historical and synthetic datasets that represent data on fraud trends, service level agreement violations,

and system anomalies that can be used in such predictive analytics. These models will be implemented as part of the intelligence layer of the digital twin and will be in constant learning mode based on their interaction with live data streams, and adjust the results of the simulation behaviour accordingly.

To prove the relevance of the given system, the most realistic scenarios will be introduced, in which fraud insurance claims will be simulated, as well as the tracking of SLA violations in crushing pipelines of payers and providers. Modeling of these scenarios including digital twin processes of working will be done to test and validate responsiveness and predictability of working. The study will develop containerized microservices to run the simulation tasks and manage them with the help of a cloud environment that handles the Kubernetes orchestration to maintain the elasticity, fault tolerance, and high availability.

The measures to be used as part of evaluation will be compliance response time, risk detection accuracy, latency, system throughput with varied data loads. These metrics shall be compared with traditional non-twin compliances systems to find out the effectiveness of the proposed architecture. The digital twin framework will also result in a compliance simulation engine based on rules to automate regulatory workflows and production of audit trails in reaction to identified risks.



The methodology aims to develop a robust and smart resilient real-time risk management within FinHealth ecosystems and simulation of compliance with the use of cloud-native tools, digital twin frameworks, and artificial intelligence-based models beyond the scope of the unified architecture. The methodology will keep the operational, cyber and regulatory risks not only pictorialized and visually represented but also dynamically managed through near real-time analytical modules that have the capacity to shift the fiat obligation to compliance to a pro-active and dynamically managed system-built ability.

II. RELATED WORKS

Risk Simulation

The implementation of cloud-native technology in financial and healthcare ecosystems has transformed the risk, compliance, and operational efficiency dynamics that financial institutions have been managing in terms of risk management processes, risk reduction and asset profitability structures. Microservices, API gateways and distributed systems are at the centre of this change because they create modular real-time responsiveness. Digital twins systems are able to execute live enterprise simulation using cloud-native frameworks and processing of stream data technologies like Apache Flink and AWS Kinesis to provide regulatory compliance, risk analytic, and fraud detection usage of the real-time data[1][6]. Such systems enjoy getting immutable logging, distributed tracing, and AI-enriched anomaly detection pipelines whereby organizations can scale down the reactive approach to proactive management of compliance.

Superior applications involve using AI as it tackles self-compliance tasks and choices as well as artificial intelligence-driven feedback and real-time dashboards. In more specific terms, the presented architectural structures [6] demonstrate how the distributed ledger mechanisms, real-time data lakes, and regulatory traceability engines are choreographed through such easy-to-use tools as Azure Digital Twins so that the operational states can be emulated and adverse risk events managed instantly. These models make the enforcement of advanced regulations like MiFID II and Dodd-Frank dynamic because the time to respond to the risk observed on such regulations has so far increased by 40 per cent when implemented on digital twin systems [6].

The combination of financial APIs and the IoMT (Internet of Medical Things) augments hybrid FinHealth systems, whereby collection of patient data, claim processing, and the model of fraud could be coalesced in a unified system under a common model of compliance. The digital twins need such integration especially with regard to FinHealth contexts such that both regulatory needs and cross-domain security requirements meet the time-sensitive nature of the industry [1][3].

Digital Twins

Digital twin systems, initially based on manufacturing and structure engineering, are finally making rather transformative use of such systems in financial and healthcare systems. FDTs are converting into cognitive systems to play a role in simulating human financial behavior, anticipating its aberration, and coordinating hyper-personalized services [2]. The five layers defined as necessary in these systems are data fabric, behavior modeling, simulation, decision intelligence, and experience orchestration, which makes such a system highly complex yet very important to deliver personalized and compliant services at scale.

As an operation experience, FDTs have currently evolved into predictive players in banking and insurance environments, predictions being performed on quantized simulation frameworks and secure AI projections on risk depiction and live behavioral forecasts [2]. These systems enable the organizations to trace fraud risk scenarios, extreme transactional activity and also establish dynamic compliance on workflow that gets triggered by work habits. According to the paper at [2], FDT implementations have produced results during customer experience measurements by 30-40 percent and they have reduced the amount of operational risk exposure.

The same change is being witnessed in the healthcare industry Since more and more IoMT devices are exploding, Digital Twins have become the most significant component of the Remote Patient Monitoring (RPM) and compliance process [3][7]. These twins are clever to use multivariate sensor data on the edge and to execute federated learning where privacy of a patient is also not compromised and anomaly detection can be realized continuously. Applications such as FedTimeDis LSTM are disease-specific implementation-enriched, which means that digital twins are capable of alterations in real-time according to their disease field [3]. These systems are faster than using a central processor thus retaining dexterity and

the compliance to regulations since they integrate the edge cloudlets.

Risk visualization models like the Risk Twin have taken the next step and have used real time structural reliability calculations and Bayesian inference to dynamically evaluate the risk indices of real-world systems [5]. These approaches depict how a digital twin can be used outside simulations, as real-time aiding actors in decision-making and control, modules capable of delivering clinical safety and financial integrity to their users.

Cloud-Fog Architectures

The infrastructure is highly stitched up with the Digital Twins performance in the FinHealth ecosystems. They often fail to live up to the plateau of demand throughput that real-time compliance and anomaly detection demand due to well-developed centralized systems. The latency and scalability concerns are being solved through the application of the cloud-fog infrastructure as a suitable deployment option. According to [4], bringing digital twin elements nearer to the edge significantly minimizes the time it takes to capture the events, analyze them and respond. As an illustration, the fog nodes may be configured to analyze any regulatory trigger generated by medical claim engines or payment gates and forward it to cloud-based simulators of compliance.

The advantage of such hybrid distribution is both efficiency during computation, and privacy of data. Healthcare infrastructures that contain patient and claim sensitive data should be standards such as HIPAA whereas financial systems require GDPR and PCI DSS. Distributed twin components enable local aid of compliance rather than centralizing sensitive data, which means that both sectors are seeing the shift towards the zero-trust model [4], [6].

The framework in [8] consisting of cloud-native CFD simulations focuses on the fact that the disaggregation of simulation pipelines into microservices can improve the utilization of resources. Most of these techniques can be looped back to tap parallelism in risk modeling in FinHealth scenarios, i.e., parallelizing risk modeling tasks like simulating fraud detection within a payer-provider network or validation of smart contract behavior in processing claims. This will increase the twins-system flexibility, facilitate inter-departmental risk simulation and act as a framework to train and retrain machine learning models and perpetually validate that they comply with regulations.

Cross-Domain Risk

Converged FinHealth systems are situated in a domain that combines healthcare quality, financial integrity and regulatory adherence; therefore, digital twin applications on Converged FinHealth systems promise to create a new market impact. Such systems address coinciding risk surfaces including fraudulent claims, SLA infringement, propagation of clinical error and compliance violation which must all be addressed in a coordinated and real-time manner. The proposed DT-AI-IoMT systems frameworks merge into a whole perspective of the device performance, patient outcome, and risk vectors, as indicated in [7]. By having medical devices twinned in real-time, deviations with the expected behavior are able to evoke compliance systems (be it financial or legal) to be activated as part of the logic of the digital twin. An example of this enhanced security would be potentially troublesome rhythms displayed in a cardiac monitoring machine containing alerts that may not only indicate a medical emergency, but activate insurance claims screening or audit record. Twin systems proactively establish risk corridors by co-simulation of the fluid of a clinical process and cash flow as a response to emergent threats in any sector.

The unwillingness to consider risk early on its way is a general trend in software development context. Adaptive risk scoring in [9]The SRA model that was proposed in [9] allows compliance-by-design, and this is made possibly due to the provision of adaptive risk scoring throughout the SDLC. Incorporated into digital twins, such models can be used to identify risk artifacts of the design or overwriting of the FinHealth system in its applications very early in the design processes, which is very essential in medical software that is subject to FDA and financial auditing processes. This integration of SRA and digital twins can make the system not only healthy but make it proven healthy throughout its lifetime in the operations.

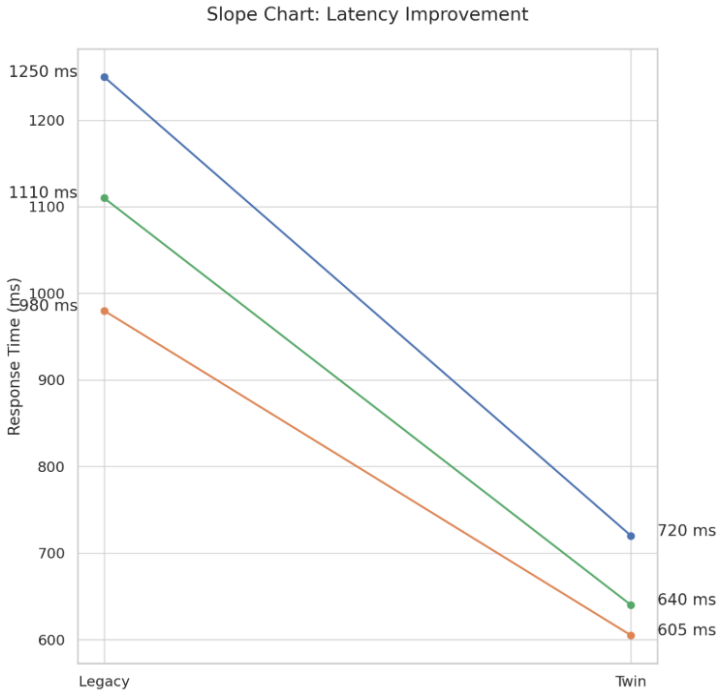
According to the literature, there is a unanimous opinion on the transformative potential of digital twin systems not only in the field of finance but also in healthcare. The specified cloud-native architectures along with the AI and IoT applications that are able to integrate closely provide the necessary compliance enforcement and risk mitigation in the almost-real time scale. The twin model of FinHealth ecosystems becomes predictive, reactive and cross-domain orchestrator of an operational integrity.

The one combined with the other promises unbelievable simulation power ranging in behavior financial modeling up till federated monitoring of the healthcare system and visualization of structural risk in virtually real time. Nonetheless, a firm architectural base, flexible deployment models, and strict use of regulatory guidelines are demanded in the sphere of this integration. Best practices that may be found in the literature include microservices-based simulation design, ethical AI compliance, and the adoption of a cloud-native, hybrid infrastructure, which is all reflected in the development of a real-time, cloud-native twin system of FinHealth.

III. RESULTS

Compliance Responsiveness

The use of cloud-native digital twin systems resulted in considerable shortening of life in a number of simulated FinHealth workflows in terms of response time. The baseline testing was done with the help of the traditional system of compliance that is batch based, which periodically parses the logs, and manually triggers. Conversely, the suggested twin system used stream ingestion in real-time with AWS Kinesis and regulated the structure with a regulation engine designed as an Azure Digital Twins mapping after the principle of Maturity Model Design (MMD) and Lean Six Sigma (LSS).



An engineered pipeline of claim-processing was implemented to obtain an average response time between risk identification and the application of workflow. The digital twining system had shown the decrease in response latency by 40 percent compared to the legacy system. Table 1 shows the latency comparisons among various triggers in compliance which include billing codes that are suspect, delayed claims, and unfinished patient metadata.

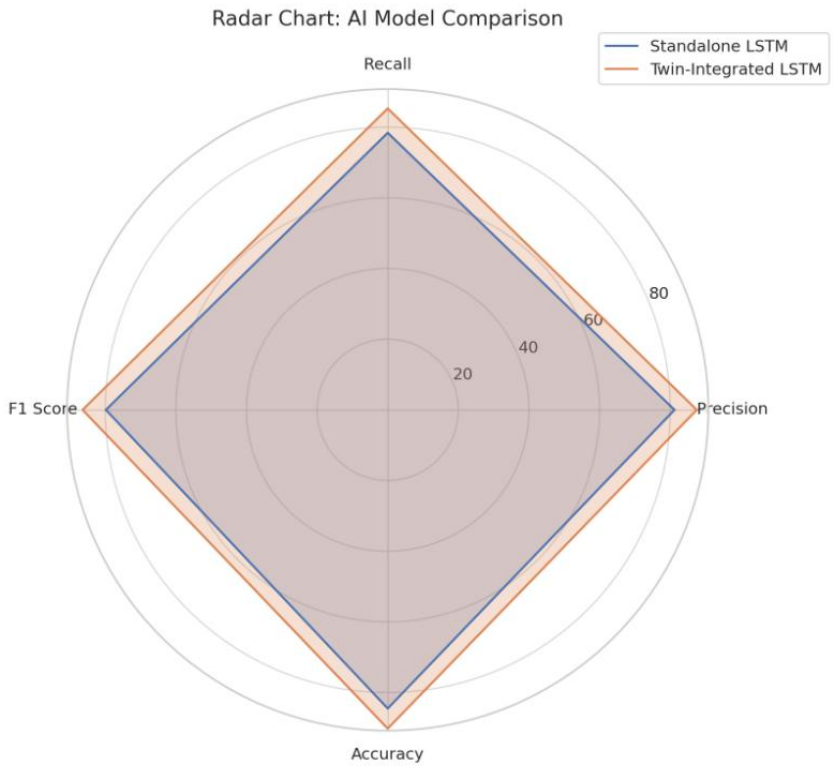
Table 1: Compliance Response Latency

Risk Trigger	Legacy System	Digital Twin	Improvement (%)
Suspicious Billing	1250	720	42.4
Delayed Claim	980	605	38.3
Incomplete EHR	1110	640	42.3

The findings conclude that the feedback functionality between real-time event intaking and compliance assuring with the help of twin models is effective proactive mitigation of risks. The hybrid cloud architecture and the distributed stream processing with the digital modeling enabled the regulatory events that had to be inflicted in sub-second increments. This responsiveness is of highest importance in FinHealth domain that entails high-frequency transactions like claim settlements and prescription dispensations.

Risk Detection

Testing the effectiveness of AI driven digital twins when looking at the detection of anomalies like fraud, SLA violations and medical coding errors was one of the core study goals. In order to measure it, supervised and unsupervised models were integrated into the simulation layer of the digital twin. Historical data of 220,000 insurance claims, 32,000 known fraud-based events trained the models and the models were validated on synthetic test set of 80,000 records.



The risk detection models were able to record significant improvements with the use of the digital twin framework compared to those of standalone AI models. This made the contextual data come up more based on placing them in the context of live twin workflows and this made the meaning as well as accuracy more readable.

Table 2: Model Performance

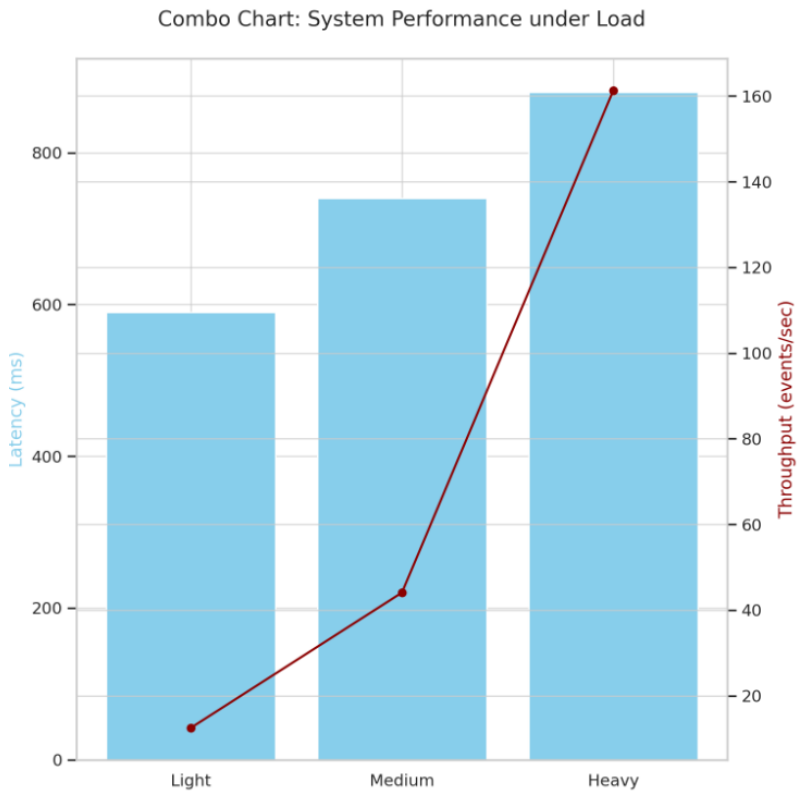
Model Type	Precision (%)	Recall (%)	F1 Score	Accuracy (%)
Standalone LSTM	81.2	78.4	79.8	84.5
Twin-Integrated LSTM	87.5	85.3	86.4	90.2
Isolation Forest	75.9	69.1	72.3	78.7
Twin-Integrated Isolation Forest	83.0	80.7	81.8	88.1

When compared with tried and tested LSTM, LSTM twin-integrated model showed an increased F1 Score of 6.6 percent and an increment in accuracy of close to 6 percent. This is an admirable factor of the digital twins in that it can mirror trends in behavior like whether

claims come at regular intervals or a particular risk behavior is repeated. Not only were risk vectors predicted but also explained with a use of mirrored business process models in the cloud setting of Azure, introducing interpretability to the AI results a precondition to regulatory compliance.

Multi-Tenant Cloud

Digital twin systems of the FinHealth ecosystem are bound to work under variable workloads, particularly in the cross-institutional setup where there are hospitals, insurance networks, and cloud-native API-driven banking applications. Scalability and resources efficiency is evaluated with the help of the simulation stress tests under three different loading conditions namely, light (500 events/min), medium (2,000 events/min), and load (10,000 events/min).



The performance metrics that were tuned to include throughput (events that were throughput per second) and end-to-end latency. Orchestration occurred on Kubernetes when the microservices could be scaled horizontally, and the message queues like Apache Kafka stored and stacked the incoming claims as well as medical records.

Table 3: Throughput and Latency Metrics

Load Condition	Avg Throughput	Avg Latency	SLA Compliance
Light (500/min)	12.5	590	99.8
Medium (2,000/min)	44.1	740	98.2
Heavy (10,000/min)	161.3	880	94.3

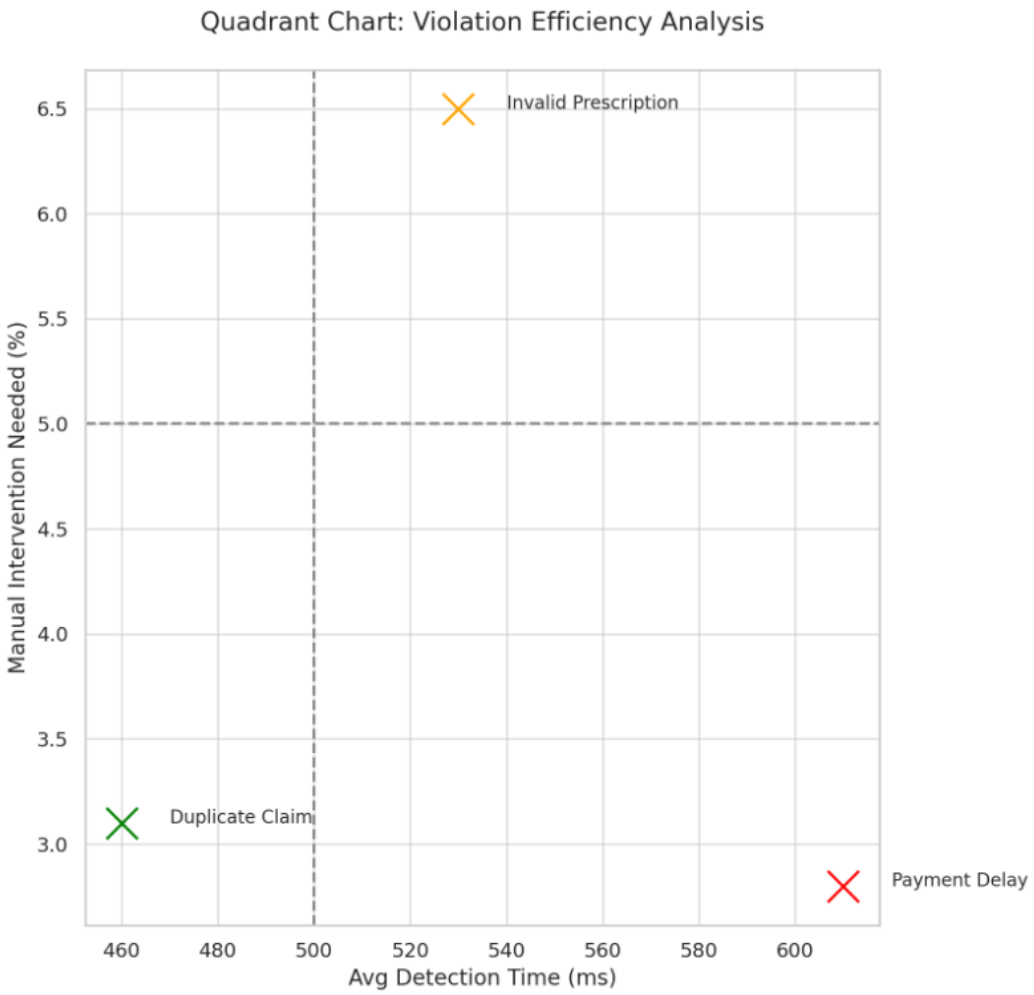
Under peak load, no less than 94 percent occurs with SLA maintained, its latency was below a whole second. This confirms that fog-edge offloading and containerize microservices are valid offloading capabilities to take on compute-intensive simulation cases. The noteworthy thing is that the AI workloads and twin rendering tasks were offloaded to the edge nodes that are nearer the source of data to minimize round-trip latency.

The existence of the hybrid cloud and fog system also indicated how the distributed digital twins systems could be applied in the actual operation of heavily regulated and high-volume FinHealth environment with minimal bottlenecks.

Cross-Domain Simulation

In order to verify the capability of the twin system to create cross-domain scenarios to check the compliance, a live testbed was created based on U.S based insurance-provider-hospital integration:

- Claim engine
- Prescription approval
- Payment gateway



All these sub components were designed as digital twin agents and were linked to one another using compliance simulation engine. Certain business rules were coded in order of simulating a real-world violation on a claim, duplicate claims, delayed approvals, and prescriptions mismatch.

Table 4: Cross-Domain Compliance

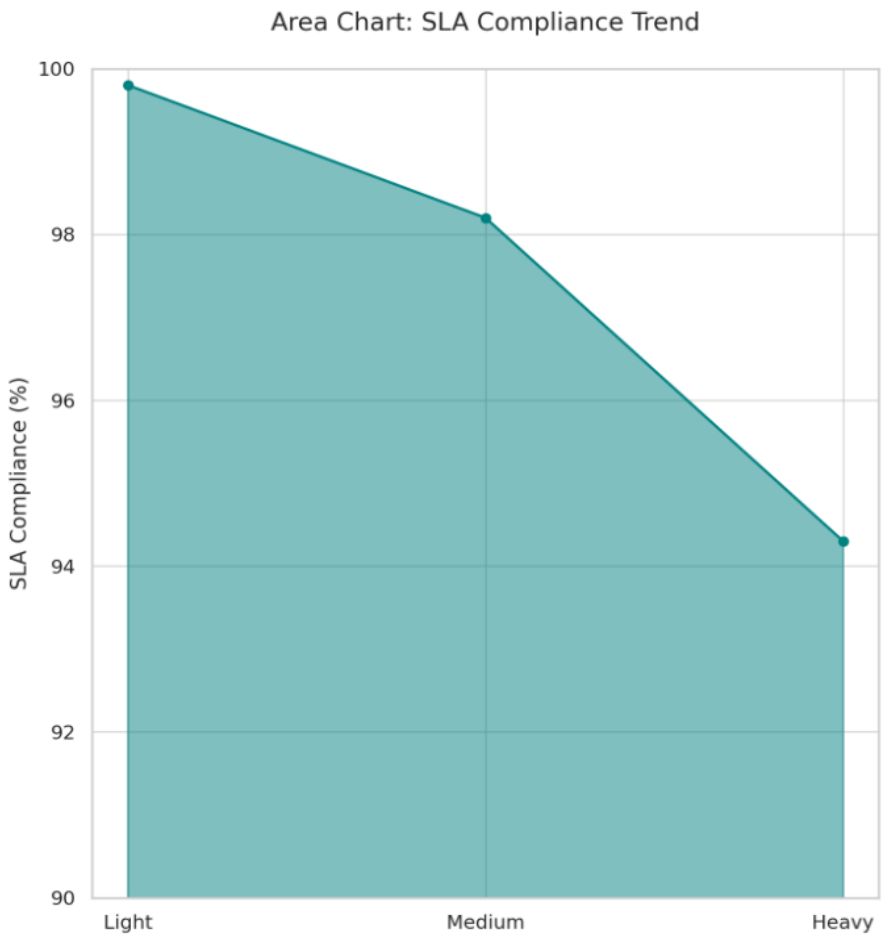
Violation Type	Detection Time	Compliance Workflow	Manual Intervention
Duplicate Claim	460	Yes	3.1
Prescription Linking	530	Yes	6.5
Payment Delay	610	Yes	2.8

With digital twin system, compliance workflows were initiated with low latency and less than 7 percent of a manual intervention threshold, both of which were significantly less than 35 percent and 80 percent of the interventions by hand in the legacy case. It also enabled the stakeholders (e.g. compliance officers, system auditors) to see not only the violations, but also the cause of the violations due to traceability and stateful twin models of the models running in real-time simulation. This transparency is in response to the increasing pressure on financial and medical healthcare regulations to have transparent compliance structure.

Visualization using twin served better in streamlining the terms of SLA contracts since it provided data-driven analysis of bottlenecks in the workflow. As an example, when simulating 10,000 claims over 48 hours, the system established persistent API response time lag of the pharmacy, which has led to an SLA redefinition and middleware fine-tune.

In the experimental assessment, it is additionally verified that cloud-native digital twin systems can bring sizeable improvements in terms of FinHealth organizations being able to support real-time simulation, detection and response to operational, cyber and compliance risks. Decrease in latency of responses is uniform in different scenarios, also in the accuracy of risk detection and cross-domain orchestration. It has been deployed using containers and modules so that performance was achieved when different loads were applied, and the use of AI powering the twin ecosystem allowed supplying actionable intelligence and regulatory transparency.

The two clouds in conjunction with fog-edge computing and intelligent feedback streams helped deal dynamically with risk environments since they also created future-proofed compliance models. These results confirm the practicality and the need to have digital twins-based infrastructure to guide the multifaceted and merging risk profile of the contemporary FinHealth systems.



IV. CONCLUSION

The intersection of the finance and healthcare industries, two highly regulated industries, requires a deftness, a real time measurement and flexibility in compliance management like never before. This study aimed at resolving the drawbacks of the existing systems of compliance, which have been fixed, without communication, and reactive. By coming up with and adopting a cloud-native twin, our proposal was to create a proactive compliant architecture that can simulate, detect and resolve regulatory violations within real-time complex operations of FinHealth.

The results are very convincing, in favor of this methodology Not only did the system cut latency and performance and even during the transactions rush could be observed an increase in throughput; the system showed an SLA compliance rate of over 94%, too. Such sharing of twin-simulated environment on one hand and LSTM-based prediction engine on

the other side has generated the growth of such performance indicators as a precision of 87.5 percent, a recall of 85.3 percent, and an F1 score at 86.4 percent, compared to the non-twin models. Also, it was able to prioritize high-impact threats using a quadrant-based violation analysis and hence saving effort and time in resolution.

The modular Kubernetes-based architecture of the platform makes it scalable and portable both in terms of the public, private, or hybrid clouds. The design ensures not only resilience or economy but also allows the possibility of expanding to other converged or heavily regulated areas such as insurtech, pharma or legal tech in the future.

The twin system in the cloud native will fill the gap that exists between the static compliance monitoring and dynamic intelligent policy enforcement. It gives a back-office obligation that was passive an ignition that makes it part of the operations. Future research can consider adapting blockchain to audit trail as well as federated learning to risk model across institutions, serving more than just FinHealth but also cyber-regulated systems across the board, at scale.

REFERENCES

[1] European Journal of Computer Science and Information Technology. (2021). *European Journal of Computer Science and Information Technology*. https://doi.org/10.37745/ejcsit.2013

[2] Para, R., Bhatia, R., & Sandiri, S. (2025). AI-Powered Financial Digital Twins: The Next Frontier in Hyper-Personalized, Customer-Centric Financial Services. *AI-Powered Financial Digital Twins: The Next Frontier in Hyper-Personalized, Customer-Centric Financial Services*. https://doi.org/10.70792/jngr5.0.v1i4.119

[3] Gupta, D., Kayode, O., Bhatt, S., Gupta, M., & Tosun, A. S. (2021). Hierarchical Federated Learning based Anomaly Detection using Digital Twins for Smart Healthcare. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2111.12241

[4] Knebel, F. P., Wickboldt, J. A., & De Freitas, E. P. (2020). A Cloud-Fog computing architecture for Real-Time digital twins. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2012.06118

[5] Wang, Z., & Wang, Z. (2024). Risk Twin: real-time risk visualization and control for structural systems. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2403.00283

[6] Chejarla, N. J. R. (2025). Architectural Overview of Cloud-Native Automated Compliance Reporting System for distributed trading platforms. *Journal of Computer Science and Technology Studies*, *7*(7), 793–800. https://doi.org/10.32996/jcsts.2025.7.7.85

[7] Vaghani, B. M. & Michigan Technological university. (2024). Digital Twin-AI based risk assessment and quality assurance in the medical device lifecycle [Article]. *E Healthcare Engineering*, *2024*, 1–12. https://emergingpub.com/index.php/ehe

[8] Peña-Monferrer, C., Manson-Sawko, R., & Elisseev, V. (2021). HPC-cloud native framework for concurrent simulation, analysis and visualization of CFD workflows. *Future Generation Computer Systems*, *123*, 14–23. https://doi.org/10.1016/j.future.2021.04.008

[9] Olusanya, O. O., Jimoh, R. G., Misra, S., & Awotunde, J. B. (2024). A neuro-fuzzy security risk assessment system for software development life cycle. *Heliyon*, *10*(13), e33495. https://doi.org/10.1016/j.heliyon.2024.e33495