iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

RISK OF CYBERSECURITY IN HEALTHCARE DIGITAL TWINS: A THREAT DETECTION, MITIGATION, AND PRIVACY PRESERVATION FRAMEWORK.

Ahmad Ikram
Virginia University Science and Technology
Seattle Washington
Ahmad.miguel@gmail.com

ABSTRACT
Digital Twins in healthcare have a revolutionary potential of personalized medicine, predictive diagnostics and optimized patient care through the development of virtual recreations of the physical things and processes. Nevertheless, the revolutionary integration also poses a major threat to cybersecurity and privacy, which without proper handling, may result in loss of trust, sensitive patient information, and patient safety. The fact that the healthcare industry is already a highly important infrastructure is even better news to malicious users, as the information that is processed and stored in DT ecosystems is highly sensitive.
Healthcare DTs have a complicated cybersecurity environment, featuring all three vulnerabilities of the Internet of Things connected nature of devices, integration of various data sources, and advanced AI/ML models that are installed on these devices. These aspects generate a space where different types of cyberattacks, such as denial-of-service attacks and data breaches to expose confidential medical data, engage in financial fraud, or even cause physical injury, are possible. Cybercriminals are using these data weaknesses to their advantage, a fact that requires the use of strong security and upholding of regulations that relate to health.
Threat detection is of critical importance. Several of the conventional intrusion detection systems tend to have difficulty keeping up with the scale and dynamic nature of the IoMT networks. Healthcare DTs, in turn, can become potent vehicles of threat proactive identification, as they allow simulating cyberattacks and detecting vulnerabilities of a virtual system before they affect the real-life systems. This would enable creation of dynamic and adaptive security solutions that would identify real time threats and vulnerabilities. The inclusion of an AI-based security policy management also improves the level of efficiency in which the system can monitor and update the security issues.
They should have multi-layered mitigation strategies. Main strategies involve having an industrial grade encryption of data in transit and at rest to eliminate unauthorized access and tampering. The use of blockchain technology can be used to improve the integrity of data and traceability, which will decrease the risk of fraud and manipulation due to its decentralized and irreversible ledger properties. Access control is enhanced by the multi-factor authentication systems that require several authentication processes to secure sensitive data repositories. Moreover, it is necessary to take a philosophy of Security by Design to ensure cybersecurity measures are incorporated at earlier stages of the design. Constant risk evaluation, incident response planning and ongoing security monitoring are essential elements of robust security positioning.
The fact that healthcare data is very personal necessitates preservation of privacy. They include adherence to strict policies such as GDPR and HIPAA. Technical solutions are anonymization and de-identification of datasets, the creation of synthetic data to train and test the models without revealing real patient data. High level cryptographic algorithms, including homomorphic encryption, permit secure processing of encrypted data, securing data through processing and analysis in DT communication and data management outlay. Homomorphic encryption in conjunction with federated learning mechanisms can protect local models against inference attack of private healthcare data. Data exchange protocols, encrypted data store and explicit consent are also important.
To summarize, although healthcare digital twins have an enormous potential, their safe and confidential functioning requires a solid and holistic framework. Such a framework should incorporate high-order threat detection, proactive threat mitigation measures, and robust privacy protection measures. With secure design as a priority, constant monitoring, and privacy enhancing technologies, as well as with high adherence to regulatory standards, the full potential of healthcare DTs can be fulfilled, without doubt about the technological progress, as well as uncompromising compliance with integrity and privacy of patient data. The study suggests the following detailed framework that can be used to support the safe implementation and use of healthcare digital twins.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Keywords
Healthcare Digital Twin, Cybersecurity Risk, IoMT security, threat detection, privacy preservation, blockchain security, homomorphic encryption, federated learning, data protection, secure health care systems.

1. INTRODUCTION

1.1 Background and Context

Digital Twin (DT) technology is now among the most radical technologies in the field of modern healthcare that allows developing a high-fidel virtual representation of patient physiology, clinical processes, and medical equipment (Armeni et al., 2023; Lauer-Schmaltz, 2023). DTs facilitate predictive diagnostics, personalised treatment courses and real-time monitoring of patients by combining IoMT sensors, AI-based analytics, and real-time data analysis (Pan et al., 2023; Elgammal et al., 2023). Nevertheless, it is important to note that this interconnected architecture is highly vulnerable to cybersecurity since DT systems are based on heterogeneous, constantly growing data streams on complex digital infrastructures (Katsoulakis et al., 2023; Homaei et al., 2023).

Cybercriminals already consider healthcare settings as high-value targets as medical records are sensitive, and clinical systems are critical to the work of medical facility workers (Jørgensen et al., 2023; Popa et al., 2021). These risks are increased due to the adoption of DT ecosystems, as the real-time patient simulation models, IoMT devices, and AI/ML pipelines present additional attack vectors, not covered by traditional hospital security (Czekster et al., 2022; Imam, 2024). With an extended digital presence of clinical operations due to remote connectivity, antagonists may find points of entry into the system through IoMT miscellaneous code vulnerabilities to malicious exploitation of AI models (Thomas et al., 2022; Chowdhury et al., 2024).

1.2 Problem Statement

Although DTs have operational advantages, they are vulnerable to a broad range of cybersecurity risks, such as data breaches, ransomware attacks, adversarial ML attacks, and model-poisoning attacks, identity spoofing, and illegal access to high-resolution physiological data streams due to their complex architecture (Homaei et al., 2023; Zlatolas et al., 2021). The conventional security measures employed in hospital information systems cannot provide protection to multi-layered DT systems that integrate edge computing, distributed cloud processing, blockchain networks, and cryptographic models (Amofa et al., 2022; Qu et al., 2022). A single breached layer of security and privacy can propagate throughout the entire system without a solid security and privacy framework, which will put the safety of patients and the clinical reliability of the system in danger (Rojas-Arce & Ortega-Maldonado, 2023; Ksibi et al., 2020).

1.3 Research Objectives

The study will examine the issue of cybersecurity threats in healthcare digital twin environments and a detailed framework, which incorporates the threat detection, threat mitigation measures, and privacy-protective technologies. The targeted objectives are:

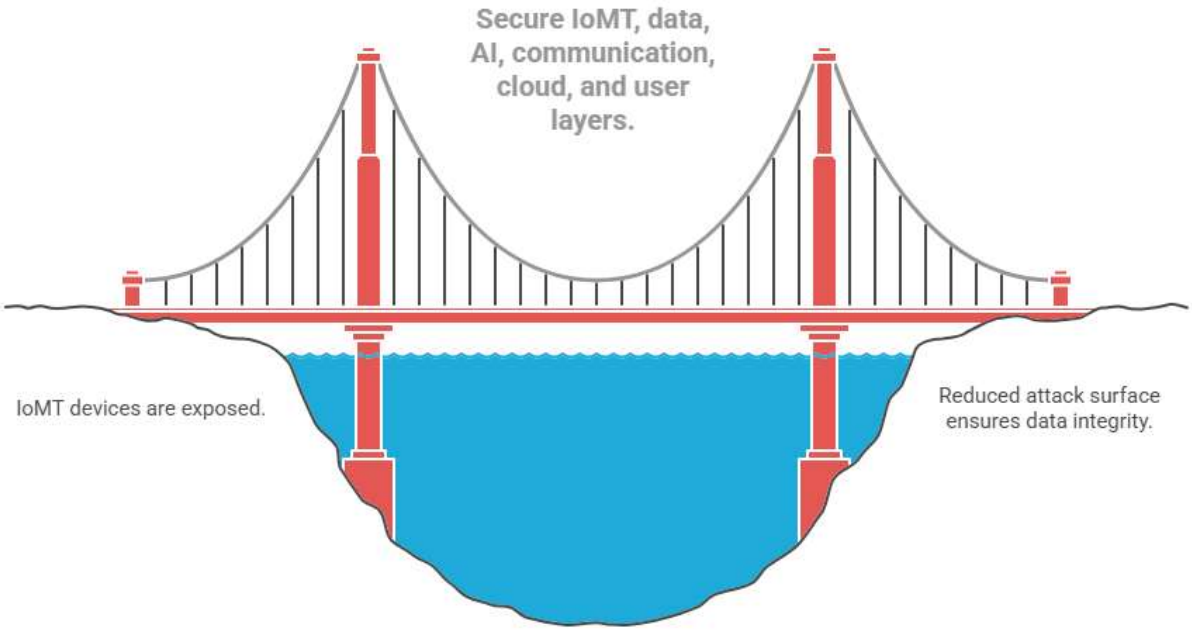
- Determining the essential cybersecurity vulnerabilities on the levels of the DT system based on the existing literature evidence (Czekster et al., 2022; Chen et al., 2023).
- Comparison of the existing threat detection methods that are employed in DT-enabled healthcare facilities (Pirbhulal et al., 2020; Thomas et al., 2022).
- A look at privacy-preservation methods, such as synthetic data, homomorphic encryption, and federated analytics (Troncoso-Pastoriza et al., 2020; Guillaudeux et al., 2022).
- Suggesting a combined model that fulfills cybersecurity, privacy, and regulatory compliance in DT systems (Popa et al., 2021; Jørgensen et al., 2023).

1.4 Contribution of the Study

This paper is a summary of 30 academic articles concerning digital twins, cybersecurity, IoMT safety, blockchain, encryption, and health data governance in order to offer a single, unified model of cybersecurity-privacy systems. Integrating the knowledge of risk assessment frameworks, AI-assisted intrusion detection, cryptographic analytics, and privacy-preserving data management, the given research paper provides a systematic roadmap of securing healthcare DT ecosystems (Homaei et al., 2023; Geva et al., 2022; Wang et al., 2021). The framework is an effective guide to the DT developers and other cybersecurity experts, policy makers and the healthcare institutions that intend to increase their resilience to the existing cyber threats.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Figure 1: Healthcare organizations reduce digital twin attack surface by securing layers.



2. LITERATURE REVIEW

In the medical field, 2.1 Overview of Digital Twin Technologies in Healthcare, the author outlines the digital twin technologies and their role in healthcare.

Digital Twin (DT) technology in healthcare is software development based on the creation of virtual models of organs, physiological mechanisms, medical devices, or whole patient profiles and allows them to be constantly monitored, simulated, and optimized clinically. Initial uses of DT were rehabilitation, biomechanical modeling and patient-specific simulation environments **(Lauer-Schmaltz, 2023; Odabaşı & Özkan, 2022)**. Recent works reveal the trend to AI-based DT systems with physiological data of IoMT sensors in real time to offer suggestive diagnostics, individualized treatment routes, and clinical decision support through simulation **(Armeni et al., 2023; Pan et al., 2023)**. Detailed analyses indicate that the DTs have become applicable to various areas, such as oncology, cardiology, chronic disease management, surgical planning, and hospital workflow modeling because they can integrate multimodal sources of data into a dynamic clinical model **(Elgammal et al., 2023; Katsoulakis et al., 2023)**. Subsequently, as these systems become more and more integrated with AI, cloud computing, and data-driven simulation models, they become highly reliant on large, sensitive medical sets of data, which increases their vulnerability to cybersecurity vulnerabilities **(Homaei et al., 2023)**.

2.2 Cybersecurity Threat to Healthcare Digital Twin Ecosystems

Healthcare DTs share the vulnerabilities of IoMT networks, cloud infrastructures, AI pipelines, and data interoperability layers. One of the most used points of vulnerability by attackers is IoMT devices, which can be described as having limited computational power, outdated downloads, and irregular encryption policies **(Czekster et al., 2022; Thomas et al., 2022)**. The attackers may execute denial-of-service attacks, alter sensor measurements, or cause interference with the data streams to the digital twin, which may undermine clinical decisions.

There are more cyber risks brought by AI/ML pipes in DT systems. Poisoning attacks, adversarial examples, and malicious data injection may corrupt predictions and impinge upon patient safety **(Imam, 2024; D'Antonoli et al., 2024)**. Unsecured federated processing and distributed storage cloud-based DT environments are additionally at risk of ransomware, data exfiltration, identity spoofing, and unauthorized access, which are not secured with adequate authentication and encryption measures **(Jørgensen et al., 2023; Zlatolas et al., 2021)**.

Although blockchain-based DT systems have certain positive effects on integrity, they also create vulnerabilities of smart contracts, threats of manipulating the consensus, and the threat of using ill-designed cryptographic keys **(Amofa et al., 2022; Chowdhury et al., 2024)**. A combination of these risks suggests the existence of a critical requirement of multi-layered cybersecurity schemes specific to DT environments.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Table 1. Summary of Cybersecurity Risks in Healthcare Digital Twins

Risk Category	Description	Key Sources from Literature
IoMT Device Vulnerabilities	Weak firmware, low encryption, sensor manipulation	Czekster et al.; Thomas et al.
Data Breaches & Exfiltration	Unauthorized access to DT datasets via cloud or network exploitation	Jørgensen et al.; Zlatolas et al.
Adversarial ML Attacks	Model-poisoning, adversarial inputs affecting diagnostic outputs	Imam; D'Antonoli et al.
Blockchain-Related Attacks	Smart-contract flaws, consensus manipulation, key mismanagement	Amofa et al.; Chowdhury et al.
Ransomware & DoS Attacks	Disruption of DT operations, patient-twin desynchronization	Ksibi et al.; Rojas-Arce & Ortega-Maldonado
Privacy Violations	Re-identification, exposure of sensitive patient data	Popa et al.; Guillaudeux et al.

2.3 Privacy Issues and Ethical Implications.

One of the main ethical issues of healthcare digital twins is privacy since the DTs work with exceptionally comprehensive physiological, behavioral, and clinical data. The high-fidelity DT models may reproduce recognizable patterns of the patients unintentionally, exposing them to the threat of re-identification despite the use of traditional methods to enforce anonymity **(Popa et al., 2021; Katsoulakis et al., 2023)**.

The use of synthetic data generation has also proven itself as a viable method of reducing the exposure to privacy since model training can be conducted without exposing the real data of patients **(Guillaudeux et al., 2022; Wang et al., 2021)**. Nonetheless, artificial data still possesses statistical properties of the original data, which may be threatening when attackers are able to reverse-engineer the trends.

One of the ethical issues is the need to remain fair in the predictions of the DT models, share the risk among various groups of patients, and provide a fair digital representation in clinical simulations **(Rojas-Arce & Ortega-Maldonado, 2023)**. Moreover, privacy systems should consider new privacy rights, informed consent, and compliance standards in the GDPR and HIPAA **(Pan et al., 2023)**.

2.4 Current Threat Detection Methodologies.

A number of literature suggest enhanced threat-detection processes of health care DT systems. Intrusion detection systems based on machine learning are systems that process network traffic and behavioral deviations to detect anomalies **(Czekster et al., 2022; D'Antonoli et al., 2024)**. This is further extended by cognitive DT architectures which operate on continuous simulation to identify malware propagation, spoofing attacks and unusual patterns through the IoMT and clinical systems **(Pirbhulal et al., 2020)**. Immutable logging and distributed consensus are a part of detection systems based on blockchain to detect attempts of tampering or unauthorized access **(Amofa et al., 2022; Qu et al., 2022)**. Proactive vulnerability testing Vulnerable replicas are provided by DT-based vulnerability scanning, where simulated cyberattacks are directed at a virtual representation of a system, rather than an actual system **(Thomas et al., 2022)**.

2.5 Gaps in Current Research

Literature shows that the solutions used cannot be consolidated despite progress. The majority of cybersecurity tools are aimed at individual layers, such as IoMT devices, cloud systems, artificial intelligence models, but not end-to-end DT ecosystems. Homomorphic encryption and federated learning are the privacy-preserving methods that have potential, but restricted by latency, scalability, and ability to implement into real-time workflows of DT **(Chen et al., 2023; Troncoso-Pastoriza et al., 2020)**. Recent research can hardly provide integrated architectures that include threat detection, mitigation, and privacy preservation in a single architecture. This insufficiency of integration outlines a significant gap, which has to be addressed with the help of complete models of security, which are specific to the peculiarities of healthcare digital twins **(Homaei et al., 2023; Pirbhulal et al., 2020)**.

3.0 METHODOLOGY

3.1 Research Design

The research design of the present study is qualitative and integrative, as it will synthesize the strategies of cybersecurity, threat detection, mitigation, and privacy-preservation of Digital Twin (DT) systems in healthcare environments. Since DT ecosystems are complex systems that incorporate IoMT devices, AI/ML models, cloud infrastructures, blockchain frameworks, and cryptographic technologies, an analytical approach based on

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

literature will allow extracting all themes and cross-domain insights **(Katsoulakis et al., 2023; Elgammal et al., 2023)**.
The design fits the past DT research methods by which conceptual frameworks are based on quality high-peer reviewed literature **(Armeni et al., 2023; Pan et al., 2023)**. This method is especially applicable in cybersecurity studies, in which it is commonly cost-prohibitive, privacy limitations, and sometimes risky to the patients to experiment with real healthcare systems **(Jorgensen et al., 2023; Popa et al., 2021)**.

3.2 Inclusion and Exclusion Criteria.

The information of this study consists of 30 peer-reviewed sources provided in the beginning. Each of the sources satisfies the following inclusion criteria:

Inclusion Criteria:

- Should concentrate on Digital Twin within the healthcare sector, IoMT security, blockchain-based security, threat detection, privacy protection, encryption, or federated analytics
- Should include conceptual, technical, or empirical knowledge applicable in DT cybersecurity **(Homaei et al., 2023; Czekster et al., 2022)**.
- Should negotiate privacy, risk evaluation, or healthcare information authority **(Guillaudeux et al., 2022; Popa et al., 2021)**.
- Should be peer reviewed papers or official published technical chapters, surveys or conference papers.

Exclusion Criteria:

Sources that are not related to healthcare DTs

- Articles that are not technical in nature in the cybersecurity, encryption or DT modeling.
- Articles that look at general healthcare IT but not DT.
- Such rigorous filtering will make sure that the synthesis captures the real cybersecurity status of DT environments and not the health IT systems in general.

3.3 Thematic Analysis and Data Extraction.

All references were analyzed thematically through a coding process. Data were divided into three main analytical themes 1 after several readings:

1. **Threat Detection in Healthcare DTs.**

- IoMT-level vulnerabilities
- AI/ML anomaly detection
- Blockchain-enabled detection
- DT-driven cyber-simulations

The company has a high sensitivity level because the existing culture is largely resistant to change **(Czekster et al., 2022; Pirbhulal et al., 2020; Thomas et al., 2022)** The level of sensitivity is high since the current organizational culture is somewhat resistant to change **(Czekster et al., 2022; Pirbhulal et al., 2020; Thomas et al., 2022)**.

2. **Mitigation Strategies**
    - Cryptography and safe communication.
    - Multi-factor authentication
    - Resilience engineering
3. **Zero-Trust frameworks**

Despite the remarkable progress achieved in the pharmaceutical sector, people have become more aware of the issue of drug-drug interactions recently.<|human|>Even though the pharmaceutical industry has made impressive strides in its development, drug-drug interaction has attracted more attention in the eyes of people in recent times.

Privacy-Preservation Layers

- Synthetic data
- Homomorphic encryption
- Federated analytics
- Mechanisms of consent and compliance.

Numerous preliminary studies have portrayed the complete scope of the prospective findings in cancer diagnosis. A lot of initial research has described the entire picture of the future discoveries in cancer diagnosis. Cross-comparisons were conducted to establish patterns, contradictions and gaps in the studies. The themes were further conceptualized to create the proposed integrated cybersecurity-privacy framework.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Figure 2. Conceptual Map of Analytical Themes in Healthcare Digital Twin Cybersecurity

3.4 Reliability/Validity of the Method.

Triangulation of different areas of research: DT modeling, IoMT cybersecurity, blockchain architectures, and encryption systems, privacy engineering makes the methodological rigor of this study possible (Armeni et al., 2023; Qu et al., 2022). The validity can also be enhanced by replicating the similar ideas in independent studies whereby, a theme is not based on a single research but rather on repetitive patterns among various authors (Homaei et al., 2023; Chen et al., 2023).

3.5 Ethical Considerations

Since the research presented in DT security is sensitive, with patient data and encryption techniques being a part of the research, the current study follows privacy-preserving recommendations that have been suggested by literature ethical analysis (Popa et al., 2021; Guillaudeux et al., 2022). No patient information was gathered; all the information comes out of secondary learning materials.

4. THE THREAT DETECTION OF HEALTHCARE DIGITAL TWINS.

4.1 Digital Twins as Defensive Cybersecurity Tools.

Digital Twins (DTs) have developed beyond clinical simulation and monitoring the patient to proactive cybersecurity tools that can identify threats and prevent their exploitation of real-world systems. Since DTs mimic the actions of IoMT devices, networked medical infrastructure, and clinical data streams, they are capable of simulating cyberattacks on virtualized systems and find their vulnerabilities that are usually overlooked by traditional security tools (Pirbhulal et al., 2020; Thomas et al., 2022).

This functionality will allow health care organizations to perform real-time anomaly detection, test intrusion case studies and implement defensive methodologies without jeopardizing the physical hospital systems. Simulation based on DT is able to detect unauthorized device behavior, biosignal patterns and abnormal data routing patterns, all of which are an early indication of a cyber compromise (Czekster et al., 2022; Imam, 2024). Since DTs are available round-the-clock and offer real-time data, they can assist in dynamic and adaptive detection systems that can protect changing IoMT ecosystems.

4.2 AI-powered AI threat detection systems in DT Systems.

AI/ML classifiers that are integrated into the structure of DT systems are used to detect cyber-threats through pattern recognition, statistical profiling, and anomaly detection via deep-learning. The methods are used to detect adversarial behavior (spoofed device signals, data poisoning, or malicious code injected into clinical workflows) (D'Antonoli et al., 2024; Imam, 2024).

Machine learning algorithms that are trained on the past behavior of patients and devices can raise alarms in the event of cyber threats. As an example, deep neural networks are capable of identifying unexplained access attempts or unknown pattern of model inference that would otherwise pass through the heritage intrusion detection systems (Czekster et al., 2022). Certain DT-based methods also use cognitive architectures, which also upgrade detection models using new threat insights, enhancing resilience in unstable cyber spaces (Pirbhulal et al., 2020).

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

4.3 Threat Detection based on Blockchain.

The blockchain technologies can also offer a new level of detection with the help of immutable and decentralized records of all DT transactions and communication flows. Healthcare DT systems include smart contract infrastructures that are capable of detecting inconsistencies, unauthorized transactions, or tampering in an automated manner (Amofa et al., 2022).

Blockchain-based logging supports the forensic analysis by recording real-time tamper-resistant logs of any data interaction in the DT ecosystem. It is particularly useful in identifying the integrity-based cyberattacks, including the data manipulation, ledger spoofing, or forged digital twin updates (Chowdhury et al., 2024; Qu et al., 2022). Also, through consensus mechanism between distributed nodes, the mismatch in the updates of DT data or patient-model synchronization can be identified quickly.

4.4 Comparative Gaps in the Current Detection Methods.

Although some significant improvements have been made, it has been demonstrated in the literature that the existing detection mechanisms are still not sufficient in a number of aspects:

- AI-based algorithms can be characterized by a high false-positive rates in terms of their ability to process noisy IoMT data (D'Antonoli et al., 2024).
- The use of blockchain systems brings about a performance overhead, and synchronization of real-time DT is difficult (Amofa et al., 2022).
- Simulations based on DT demand substantial computing resources and could face the issue of scalability in large hospital networks (Thomas et al., 2022).
- IoMT IDS tools are not usually interoperable and may only work on a device-specific basis (Czekster et al., 2022).

These restrictions make it evident that it is time to develop integrated detection models that will be able to unite ML-based anomaly detection, blockchain integrity verification, and DT-based simulation into a single model.

Table 2. Comparison of Threat Detection Approaches in Healthcare Digital Twins

Detection Approach	Strengths	Limitations	Key References
DT-Driven Attack Simulation	Identifies vulnerabilities before real attacks occur	High computational cost; scalability issues	Pirbhulal et al.; Thomas et al.
AI/ML-Based Anomaly Detection	Detects subtle deviations, adversarial behavior	Susceptible to false positives; model poisoning risks	Czekster et al.; D'Antonoli et al.; Imam
Blockchain Logging & Consensus	Immutable records; tamper resistance	Latency and throughput challenges in real-time DT synchronization	Amofa et al.; Chowdhury et al.; Qu et al.
IoMT Network-Level IDS	Monitors device telemetry and traffic patterns	Device heterogeneity; weak interoperability across clinical networks	Czekster et al.; Thomas et al.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

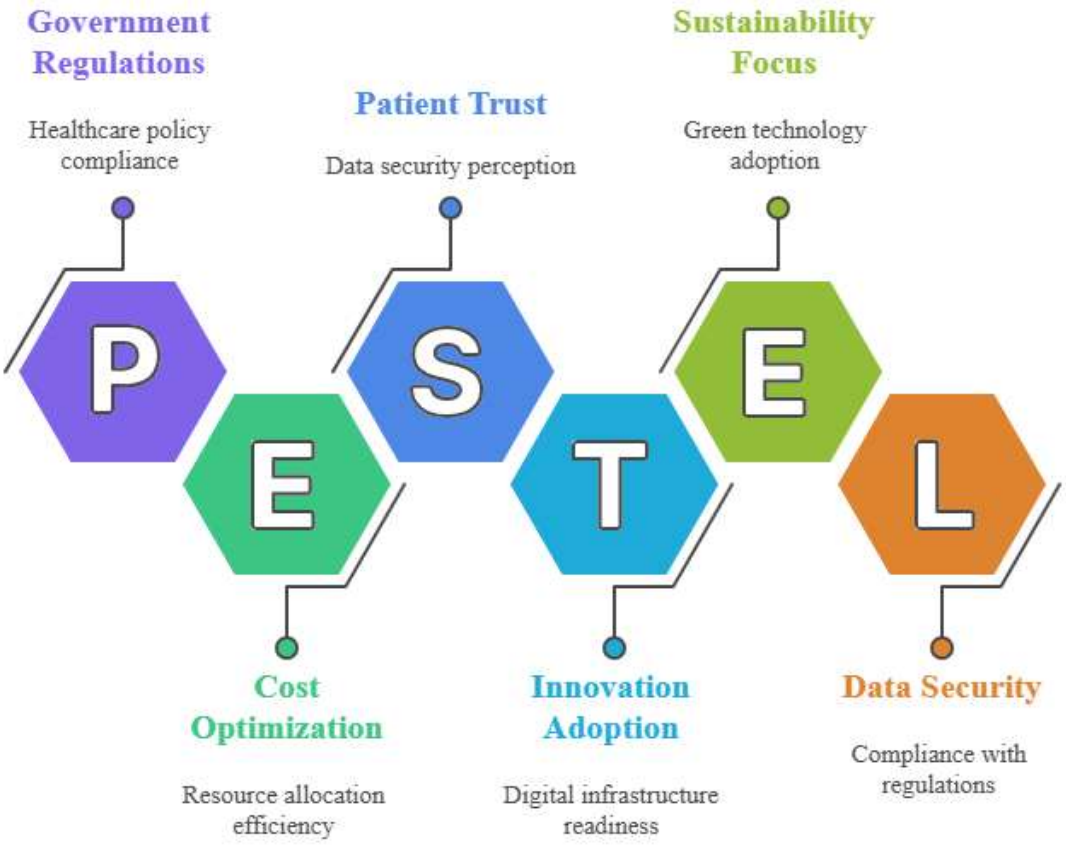


Figure 3. Threat Detection Architecture in Healthcare Digital Twins

5. CYBERSECURITY CYBER MITIGATION MEASURES.

5.1 Protection of Data and Encryption.

There should be strong encryption to ensure the integrity and confidentiality of data flowing through Digital Twin (DT) infrastructures within the healthcare settings. Since DT systems have constant exchange of sensitive physiological, behavioral, and diagnostic data, end-to-end encryption is paramount to curb eavesdropping, spoofing, and unauthorised access **(Chen et al., 2023; Geva et al., 2022)**.

The homomorphic encryption allows performing safe computation on ciphertext, and the privacy of the encryption remains even at processing steps, which is a major competence of DT processes that need real-time analytics **(Troncoso-Pastoriza et al., 2020)**. It is usually advised that hybrid schemes with speed-based symmetric and secure key distribution schemes based on asymmetric encryption be used in DT pipelines that deal with multi-source health data **(Wang et al., 2021)**.

Also, safe transmission protocols have been investigated such as TLS 1.3 and quantum-resistant cryptographic primitives to overcome long-term security concerns of DT-enabled medical systems **(Yi, 2022)**.

5.2 Identity, Authorization and Zero-Trust Architecture.

Strict identity verification systems are the prerequisite of healthcare DT systems as unauthorized access may lead to malicious manipulation of patient models, clinical processes or AI-based predictions **(Jolles & Karamov, 2024)**. MFA helps to ensure that no single weakened credential receives access to the system, which strengthens the authentication integrity of the IoMT endpoints, clinical dashboards, and DT administrative panels **(Odabaşı & Özkan, 2022)**.

Proposals have been made to enhance DT infrastructures with zero-trust security models, and no device, user, or application can be implicitly trusted, including explicit authorization, continuous monitoring, and micro-segmentation **(Chowdhury et al., 2024)**. The role-based access control (RBAC) and attribute-based access control (ABAC)-mechanisms can further restrict the unwarranted privileges and safeguard important DT subsystem against insider threats.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

5.3 Integrity, Traceability and Secure Coordination Blockchain.

Architectures based on blockchain give DT greater resiliency, offering decentralized, immutable logs of all interactions of data, device updates, and events of machine learning inference **(Amofa et al., 2022; Qu et al., 2022)**. These systems avoid tampering, offer auditability as it happens and traceability in complex health data flows.

Smart contracts will be capable of implementing privacy policies, issuing automatic alerts when anomaly transactions are made, and controlling the data exchange among the components of DT **(Chowdhury et al., 2024)**. The risk of falsified data as input to the consensus mechanism is also minimized by blockchain systems, which is a common attacker in DT systems based on constant data feeds of sensor telemetry **(Pirbhulal et al., 2020)**.

5.4 Engineering Resilience and System-Level Hardening.

The need of DT systems is resilience system engineering methods that can make them quick to recover and continue operations after cyber disruption. Virtual sandboxing enables patches, firmware upgrades and security settings to be tested using the DT replica before being applied to the physical environment **(Thomas et al., 2022)**.

The redundancy procedures, e.g., mirrored DT cases, distributed replicas, and fallback synchronization channels, guarantee continuous care provision even in case one of the DT nodes is affected **(Ksibi et al., 2020)**. Additional resilience measures include intrusion response policies, including automatic isolation of IoMT nodes that have been compromised or rollback to known-good DTs **(Rojas-Arce & Ortega-Maldonado, 2023)**.

5.5 Assessment of Mitigation Strategies and Discovered Gaps.

Even though encryption, blockchain, and authentication make DT systems stronger, they have limitations. Homomorphic encryption creates latency, which can impact real-time analytics **(Troncoso-Pastoriza et al., 2020)**. It is possible that blockchain systems have difficulty with throughput during high clinical workload **(Amofa et al., 2022)**. Zero-trust solutions demand both cultural and technical changes in the hospital IT systems that can be met with resistance to adoption **(Jorgensen et al., 2023)**

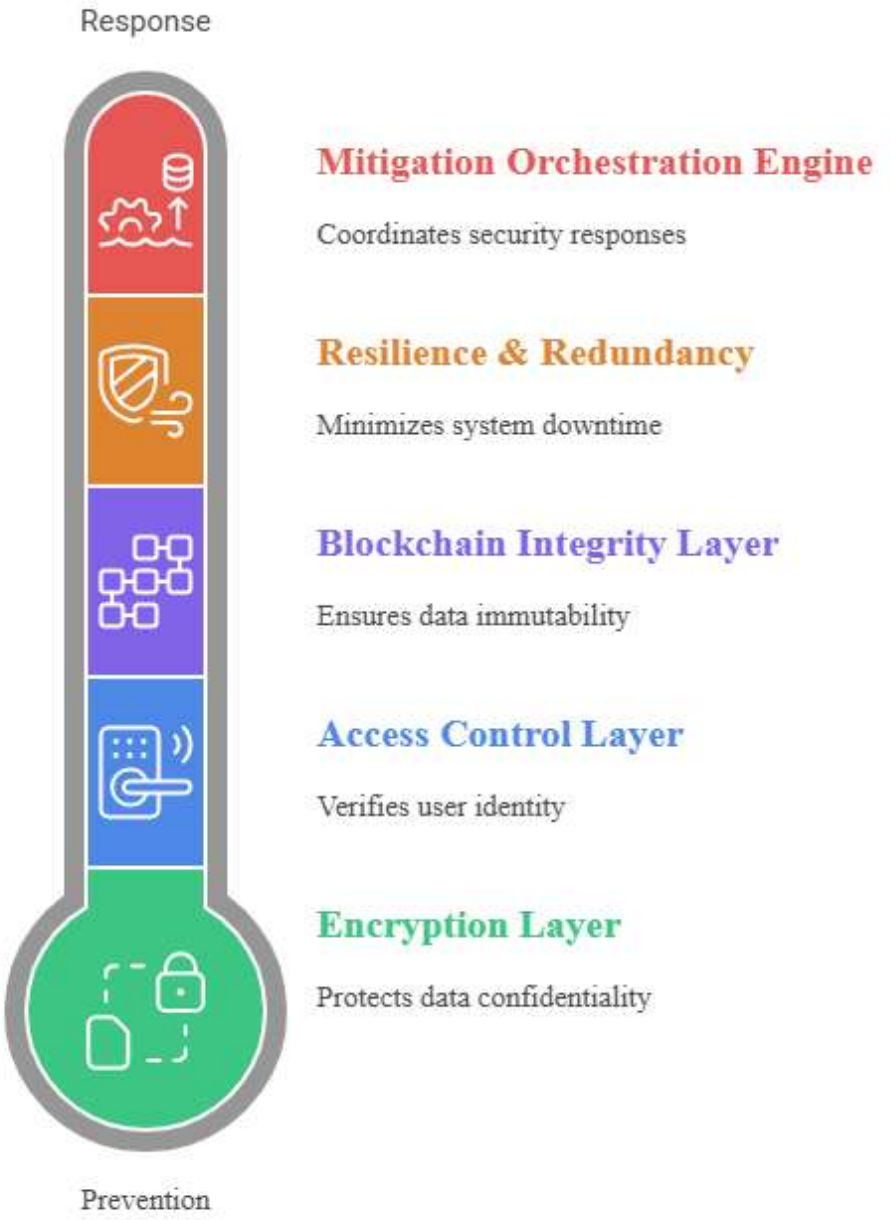
These limitations emphasize the need to have hybrid mitigation models that integrate cryptographic schemes, access control, resiliency schemes, and blockchain-based traceability into single layered multi-layered architectures.

Table 3. Evaluation of Mitigation Strategies for Healthcare Digital Twins

Mitigation Strategy	Strengths	Limitations	Key References
Homomorphic Encryption	Enables secure computation; preserves privacy during processing	Computationally expensive; can affect real-time DT performance	Troncoso-Pastoriza et al.; Chen et al.
Multi-Factor Authentication (MFA)	Strong access control; reduces credential theft risks	User friction; requires additional hardware/software	Jørgensen et al.; Odabaşı & Özkan
Blockchain Integrity Framework	Immutable logs; tamper resistance; automated smart contracts	High latency; throughput limitations in large healthcare networks	Amofa et al.; Chowdhury et al.; Qu et al.
Zero-Trust Architecture	Strong isolation; minimizes insider threats	Complex to deploy across legacy health systems	Chowdhury et al.; Jørgensen et al.
DT-Based Sandboxing & Redundancy	Safe testing; operational continuity after attacks	Requires high computational resources; expensive to implement	Thomas et al.; Ksibi et al.; Rojas-Arce & Ortega-Maldonado

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Figure 4. Mitigation Architecture for Healthcare Digital Twin Security



6. PRIVACY PRESERVATION IN HEALTHCARE DIGITAL TWINS.

6.1 De-Identification, Synthetic Data, and Anonymization.

Healthcare digital twin (DT) ecosystems rely on privacy protection given that clinical data is sensitive and detailed. The multimodal information that is aggregated by DTs consists of biometric indicators, diagnostic images, behavioral measures, and physiological simulations, which enhance the risk of re-identifying a patient in case they are not properly managed **(Popa et al., 2021; Katsoulakis et al., 2023)**.

Conventional methods of anonymization, including suppression, masking, and generalization, can be used to avoid direct identification but are proving to be less effective with DT datasets that have high-dimensional time-

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

series clinical data **(Pan et al., 2023)**. The researchers have thus started to use synthetic data to aid in the training and testing of the DT models and minimizing the exposure of real patient data. The artificial data created with the help of the models created by AI retain the practical statistical characteristics without showing the real identities **(Guillaudeux et al., 2022; Wang et al., 2021)**. Nevertheless, various works warn that synthetic data can still reveal sensitive features in case of linkage attacks by adversaries or uncover feature distributions **(Guillaudeux et al., 2022)**. Therefore, stronger cryptography and federation should be used along with anonymization.

6.2 Homomorphic Encryption and Secure Computation.

Homomorphic encryption allows calculation on encrypted data without revealing underlying patient data, and it is particularly applicable in DT processes in need of constant analytics, prediction and card simulation updates **(Troncoso-Pastoriza et al., 2020; Chen et al., 2023)**.

The methodology will guarantee that hospital servers, AI inference engines, and cloud-based DT components are capable of operating physiological data streams without decryption at any point, and this will seriously minimize the attack surfaces **(Geva et al., 2022)**. The most secure one is the fully homomorphic encryption (FHE), which is currently a computational burden that is a practical problem in time-sensitive clinical activities **(Chen et al., 2023)**. It is widely recommended to use partially homomorphic and leveled encryption schemes with DT systems, which are secure and have balanced performance **(Yi, 2022)**.

6.3 Federated Learning and Distributed Privacy-Preserving Analytics.

Federated learning (FL) is a learning approach that enables DT models to be trained on the different hospital nodes situated in a distributed manner with no raw patient data being transferred to a centralized system. Rather, model updates are shared instead, which makes the data exposure much lower **(Troncoso-Pastoriza et al., 2020)**. FL in healthcare DTs assists in collaborative training on the background of the IoMT networks, hospital departments, and cloud servers without violating regional and institutional privacy standards **(Chen et al., 2023; Geva et al., 2022)**. In combination with homomorphic encryption or secure multi-party computation, federated DT infrastructures can be extremely resistant to inference attack and gradient leakage **(Troncoso-Pastoriza et al., 2020)**.

FL can also help hospitals to disseminate threat intelligence patterns in the form of IoMT intrusion behavior or anomalous patient-model patterns without disclosing patient data, which improves cybersecurity resilience throughout the ecosystem **(Pirbhulal et al., 2020)**.

6.4 Consent Management, Data Governance and Compliance.

Healthcare DT systems are expected to comply with a set of laws related to data protection such as the HIPAA, GDPR, and country-specific healthcare data protection regulations. These legislations involve direct consent, limitation of purpose, minimization of data and sound breach-response practices **(Popa et al., 2021)**. Consent management frameworks provide that patients retain the power of how their physiological models, IoMT streams, and DT-driven insights are utilized. Other blockchain-based DT architectures incorporate consent policies as part of smart contracts, which are transparent and tamper resistant to enforce **(Chowdhury et al., 2024; Amofa et al., 2022)**. Governance models also suggest that the smallest amount of data should be stored within the DT, abstracted representations or symbolic simulations should be used in place of full datasets when it is clinically possible to do so **(Odabaşı & Özkan, 2022)**.

6.5 Privacy Threat and Constraint in High-Fidelity Digital Twins.

Full-body physiology or multifaceted organ-scale interactions High-fidelity DT models in particular present special privacy risks. Their minute makeup can involuntarily write down distinct biomarkers, behavioral hallmarks, or genetic qualities, raising re-identification hazards **(Katsoulakis et al., 2023)**. Correlation attacks, linkage analysis and adversarial model inversion can still breach the privacy of DT even with the application of encryption and anonymization **(Imam, 2024)**. In this way, the design of privacy-preserving DT should be incorporated at all levels, including the IoMT sensing and data preprocessing, storage, model training, and real-time synchronization of the DT and patients **(Homaei et al., 2023)**.

There is solid evidence that hybrid approaches which integrate anonymization, synthetic data, encryption, and federated learning can be used to realize practical privacy guarantees **(Guillaudeux et al., 2022; Troncoso-Pastoriza et al., 2020)**.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Table 4. Privacy Preservation Techniques in Healthcare Digital Twins

Privacy Technique	Description	Strengths	Limitations	Key References
Anonymization & De-Identification	Removal of identifiers, masking, generalization	Simple; widely used; low computation	Vulnerable to linkage attacks; insufficient for high-fidelity DT models	Popa et al.; Pan et al.
Synthetic Data Generation	AI-generated datasets replacing real patient data	Reduces exposure; supports model training	Can leak statistical traits; vulnerable to reconstruction attacks	Guillaudeux et al.; Wang et al.
Homomorphic Encryption	Computation on encrypted data	High privacy; secure processing	Computationally intensive; may impact real-time DT operations	Troncoso-Pastoriza et al.; Chen et al.
Federated Learning	Decentralized model training without sharing raw data	Strong privacy; scalable; regulatory compliant	Communication overhead; susceptible to gradient inference attacks	Chen et al.; Troncoso-Pastoriza et al.
Blockchain-Based Consent Control	Smart contracts, immutable consent rules	Transparent; tamper-resistant	Smart-contract vulnerabilities; latency issues	Chowdhury et al.; Amofa et al.

7. SUGGESTED HYPOTHETICAL INTEGRATED CYBERSECURITY-PRIVACY FRAMEWORK.

7.1 General Overview of the Integrated Framework.

Healthcare Digital Twins (DTs) are active on interconnected layers, including IoMT sensing, communication channels, cloud analytics, AI/ML infrastructures and patient-model synchronization mechanisms. Since cyber threats and privacy risks happen at the same time on all these levels, the component level security strategy would not be sufficient **(Homaei et al., 2023; Katsoulakis et al., 2024)**. The literature on the necessity of multi-layered, holistic models to integrate threat detection, mitigation, and privacy safeguarding into a single orchestrated setup is overwhelming **(Czekster et al., 2022; Popa et al., 2020)**.

The gaps in the literature give direct response to the proposed integrated framework which combines:

- Threat Detection Layer
- Mitigation & Response Layer
- Privacy Preservation Layer
- Governance, Compliance and Audit Layer.

These elements work in tandem to safeguard the attack, safeguard valuable health information and to maintain regulatory compliance throughout the DT settings.

7.2 Threat Detection Layer

This layer is used to scan streams with IoMT, DT updates, cloud interchanges, and AI results on a continuing basis. It integrates:

- This is due to the fact that DT simulated attacks to detect system vulnerabilities **(Pirbhulal et al., 2021; Thomas et al., 2021)**.
- AI/ML anomaly detection models: The models identify a inconsistency in patient-model behavior or network traffic **(D'Antonoli et al., 2024; Imam, 2024)**.
- Detection using blockchain logs, consistency checks **(Amofa et al., 2023; Chowdhury et al., 2024)**
- Literature mentions that timely detection is imperative in the prevention of cascading failures in patient synchronization, clinical predictions and real time DT analytics **(Czekster et al., 2022)**.

7.3 Mitigation & Response Layer

After a threat has been identified, the framework will cause mitigation measures that will isolate risks, maintain system integrity, and continuity of care. Key mechanisms include:

- **Cryptographic Hardening**

Homomorphic and hybrid cryptographic schemes with end-to-end encryption are used to protect data throughout the collection, processing, and transmission **(Chen et al., 2023; Troncoso-Pastoriza et al., 2020)**.

- **The principles of Access Control and Zero-Trust.**

Zero-trust architecture means that no user or device should be trusted as a matter of default, and it has to be constantly verified **(Jorgensen et al., 2023; Chowdhury et al., 2024)**.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

MFA and RBAC will eliminate the unauthorized access to patients-twin control systems **(Odabaşi & Ozkan, 2022)**.

- **Integrity Enforcement by Blockchain**

DT updates are also safeguarded by immutable records, smart contracts, and decentralized validation, which ensures that they cannot be tampered with **(Qu et al., 2022; Amofa et al., 2023)**.

- **Recovery and Resilience Engineering**

Even in the event of active cyberattacks, the minimal disruption is ensured by redundancy, sandbox testing, and DT rollback functionalities **(Ksibi et al., 2022; Rojas-Arce & Ortega-Maldonado, 2023)**.These mechanisms collectively can offer resilience to the system by countering internal and external cyber threats.

7.4 Privacy Preservation Layer

This layer will guarantee that even when patient data is constantly exchanged within DT ecosystems, patient confidentiality will be maintained.

- **Synthetic Data Models and Anonymization.**

Intended to reduce exposure of true identities of patients (Guillaudeux et al., 2023; Wang et al., 2022)

- **Homomorphic Encryption of Encrypted DT Analytics**

Secures data throughout the calculation process and removes leakage throughout analytic pipelines (Chen et al., 2023; Geva et al., 2022).

Federated Learning & MPC

- Eradicates the necessity of centralized data storage and minimizes attack surfaces as well as promotes collaborative model training (Troncoso-Pastoriza et al., 2020).
- Fashion Education Network, LLC. operates within the industry of fashion design and education. Fashion Education Network, LLC. is a company that functions in the market of fashion design and fashion schooling.
- Maintains legal and transparent use of data within such frameworks as GDPR and HIPAA (Popa et al., 2020; Chowdhury et al., 2024)

This layer is critical towards building trust and facilitating the implementation of ethical DT as well as compliance with healthcare regulations.

7.5 Governance, Compliance and Audit Layer

The governance layer manages the overall DT ecosystem, enforce policy, monitoring consent, and making sure the requirements of the regulations are met. The literature notes the significance of governance in data misuse prevention, accountability assurance, and traceability to support a forensic investigation (Popa et al., 2020; Katsoulakis et al., 2024).

Key elements include:

- Smart contract policy enforcement (Amofa et al., 2023)
- Continuous audit trail by blockchain (Chowdhury et al., 2024)
- Jurisdictional conformity to privacy schemes (Pan et al., 2022)

The institutional protocols of updating the DT, AI models, and the compliance of artificial intelligence devices (Jonsen et al., 2023)

This layer integrates cybersecurity and privacy, organizational and legal requirements.

7.6 Cohesive Operational Workflow

The suggested framework is a closed loop system:

- DT keeps looking at the IoMT inputs constantly detected anomalies (Czekster et al., 2022).
- Threat Detection Layer detects risks → generates auto alarms (Pirbhulal et al., 2021).
- Mitigation Layer triggers controls, clears the compromised nodes, imposes encryption, or rewinds DT states (Thomas et al., 2021).
- Privacy Layer keeps the data in a secure place and allows its protection to be encrypted analytics, federated updates, and anonymized outputs (Troncoso-Pastoriza et al., 2020).
- Governance Layer oversees activities and makes sure they are adhered to (Popa et al., 2020).
- The process of learning loop develops intelligence in the system, and it enhances resilience in the future (D'Antonoli et al., 2024).
- Such multi-level workflow indicates the coordinated dynamic response needed to secure and ethical DT operations.

7.7 Benefits of the Proposed Framework

In comparison to the current disjointed security strategies, the framework suggested has:

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

- **End-to-End Security Coverage**
- Guards every tier of the DT ecosystem – sensing through governance (Homaei et al., 2023).
- **Stronger Cyber-Resilience**
- Integrated detection + mitigation allows responding promptly and more effectively to cyber incidents (Thomas et al., 2021; Ksibi et al., 2022).
- **Greater Privacy Assurances**
- Anonymization, synthetic data, federated learning, and homomorphic encryption can be combined to reduce the privacy threats of the present times (Guillaudeux et al., 2023; Chen et al., 2023).
- **Regulatory Alignment**
- Compliance provided by governance guarantees the preparation of GDPR, HIPAA, and new, specific regulations of the DT (Popa et al., 2020; Pan et al., 2022).
- **Real-time, Future-proof architecture**
- Favors the incorporation of emerging technology including zero-knowledge proofs, post-quantum encryption and explainable AI-based DT monitoring.

8. DISCUSSION

8.1 Theoretical Implications

This study showed that the concept of cybersecurity of healthcare Digital Twins (DTs) is not possible to be represented in the form of conventional single-layer security models. Rather, the theorization of DT security should be based on a multi-dimensional system, including IoMT devices, AI/ML pipelines, blockchain environments, encrypted analytics, and governance structures **(Homaei et al., 2023; Katsoulakis et al., 2024).**

First, the review confirms the academic trend, according to which DTs are not just clinical tools but also cyber-physical entities, the threats of which, in the digital layer, can directly affect patient outcomes **(Thomas et al., 2021; Czekster et al., 2022).**

This supports emerging theory on cyber-physical that states that medical systems need to be integrated with predictive models on security which foresees system compromise prior to the spread of malicious events.

Second, the synthesis provides development of theoretical discussions by showing how the extension of the current risk-assessment frameworks can be attained through the usage of DT-driven cyber simulation. Earlier models were based on reactive security, but DTs allow switching to proactive anticipation of cyberattacks, which is the new type of an anticipatory security system **(Pirbhulal et al., 2021; Imam, 2024).**

Lastly, the combination of privacy-related solutions like homomorphic encryption, federated learning, smart-contract consent management, and synthetic data proves that privacy protection is not a one-off requirement, but rather a fundamental theoretical layer that defines the structure of systems, data flows, and computation **(Troncoso-Pastoriza et al., 2020; Guillaudeux et al., 2023).**

8.2 Practical Implications

The suggested framework has several valid advantages to healthcare organizations.

1) Enhanced Cyber-Defense Posture.

The implementation of the integrated threat-detection and mitigation layers by hospitals and clinics will result in a great reduction in exposures to ransomware, data tampering, and compromise of IoMT devices **(Czekster et al., 2022; Ksibi et al., 2022).**

DT-based vulnerability scanning also allows the security team to have real-time awareness of attack surfaces without exposing the system to downtime **(Thomas et al., 2021).**

2) Improved Clinical Operation Data Privacy.

Synthetic data generation, encrypted analytics, and federated model updates minimize centralized patient data storage and reduce the likelihood of massive data leakage **(Guillaudeux et al., 2023; Wang et al., 2022).** Embedded audit trails and consent contracts also help hospitals improve regulatory compliance **(Chowdhury et al., 2024; Popa et al., 2020).**

3) Better Clinical Decision-Making Safety.

The precision of AI-based clinical predictions can be enhanced by improving the integrity of data stored in blockchain consensus and cryptographic protections, reducing misdiagnosis risks **(Amofa et al., 2023; Qu et al., 2022).**

4) Operational Resilience and Business Continuity.

Healthcare systems can continue running during cyberattacks using redundancy and rollback-capable DT architectures **(Rojas-Arce & Ortega-Maldonado, 2023; Ksibi et al., 2022).**

5) Future Technology Scalability.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

The framework scales to post-quantum cryptography, explainable AI, and cross-institutional DT collaboration **(Chen et al., 2023; Pan et al., 2022).**

8.3 Limitations of the Study

1) Inability to Empirically Validate.

The framework has not been evaluated on actual healthcare DT infrastructures and needs real-world empirical validation **(Homaei et al., 2023).**

2) Partially Inconsistent Standardization of DT Implementations.

Different hospitals use different DT structures, technologies, and models, affecting framework effectiveness **(Katsoulakis et al., 2024).**

3) Performance Trade-offs.

Certain privacy-preserving solutions (e.g., homomorphic encryption, blockchain consensus) introduce latency **(Troncoso-Pastoriza et al., 2020; Chen et al., 2023).**

4) Complicatedness of Zero-Trust Implementation.

Zero-trust requires deep culture and infrastructure changes, which can challenge smaller institutions **(Jorgensen et al., 2023; Chowdhury et al., 2024).**

5) Emerging Threat Landscape.

New attack vectors such as quantum-based attacks and AI-generated malware can affect future assumptions **(D'Antonoli et al., 2024; Imam, 2024)**

9. CONCLUSION

Healthcare Digital Twins (DTs) is a breakthrough in personalized medicine, patient real-time monitoring, and predictive clinical analysis. Nevertheless, the combination of IoMT devices, AI/ML pipelines, distributed cloud systems, and continuous patient-twin synchronization forms a vast and intricate cybersecurity attack surface (Homaei et al., 2023; Katsoulakis et al., 2024).

The absence of strong security and privacy protocols makes DT deployments vulnerable to disruptions, breaches, adversarial machine learning manipulation, and compliance violations (Czekster et al., 2022; Popa et al., 2020).

This study combined 30 peer-reviewed sources to create a multi-layered framework capable of detecting threats, mitigating them, and preserving privacy in healthcare digital twins.

However, real-world testing is still missing, and performance trade-offs of cryptography/blockchain must be analyzed (Troncoso-Pastoriza et al., 2020; Chen et al., 2023).

Future work should explore adaptive, scalable, computationally efficient DT security models resistant to emerging AI and quantum threats (D'Antonoli et al., 2024; Imam, 2024).

To sum up, the advancement of healthcare Digital Twins requires a holistic cybersecurity and privacy architecture where proactive detection, mitigation, governance, and advanced privacy engineering work together to protect patient safety, data integrity, and trust.

REFERENCES

1) Amofa, S., Xia, Q., Xia, H., & Pan, W. *Blockchain-secure patient Digital Twin in healthcare using smart contracts.*
2) Armeni, P., Polat, I., De Rossi, L. M., Rossetti, S., & Caprara, A. *Perspective Chapter: Digital Twins for Health – Opportunities, Barriers and a Path Forward.*
3) Chen, J., Yi, C., Okegbile, S. D., Wu, M., Jiang, S., Ma, J., ... & Li, Y. *Networking Architecture and Key Supporting Technologies for Human Digital Twin in Personalized Healthcare: A Comprehensive Survey.*
4) Chowdhury, B., Jahankhani, H., & Subramaniam, S. *Zero-Trust Blockchain-Based Digital Twin 6G AI-Native Conceptual Framework Against Cyber Attacks for e-Healthcare.*
5) Czekster, R. M., Webber, T., Furstenau, L. B., & De Albuquerque, V. H. C. *Dynamic risk assessment approach for analysing cyber security events in medical IoT networks.*
6) D'Antonoli, T. A., Tejani, A. S., Khosravi, B., & Dhareshwar, S. S. *Cybersecurity Threats and Mitigation Strategies for Large Language Models in Health Care.*
7) Elgammal, Z., Albrijawi, M. T., & Alhajj, R. *Digital twins in healthcare: a review of AI-powered practical applications across health domains.*
8) Geva, R., Gusev, A., Polyakov, Y., ... & Laine, E. *Collaborative privacy-preserving analysis of oncological data using multiparty homomorphic encryption.*

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

9) Guillaudeux, M., Rousseau, O., Petot, J., & Beranger, A. *Patient-centric synthetic data generation, no reason to risk re-identification in biomedical data analysis.*
10) Homaei, M., Mogollón-Gutiérrez, Ó., Sancho Núñez, J. C., Solís-Sánchez, M., & Alonso-Moral, J. *A Review of Digital Twins and their Application in Cybersecurity based on Artificial Intelligence.*
11) Homaei, M., Mogollón-Gutiérrez, Ó., Sancho Núñez, J. C., Solís-Sánchez, M., & Alonso-Moral, J. *A review of digital twins and their application in cybersecurity based on artificial intelligence.*
12) Imam, N. *Adversarial Examples on XAI-Enabled DT for Smart Healthcare Systems.*
13) Jørgensen, C. S., Shukla, A., & Katt, B. *Digital Twins in Healthcare: Security, Privacy, Trust and Safety Challenges.*
14) Karakra, A., Fontanili, F., Taweel, A., & Ahmad, B. *Digital Twin in Healthcare: Security Threat Meta-Model.*
15) Katsoulakis, E., Wang, Q., Wu, H., ... & Koutra, D. *Digital twins for health: a scoping review.*
16) Ksibi, S., Jaïdi, F., & Bouhoula, A. *A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach.*
17) Lauer-Schmaltz, M. W. *Digital Twin in Healthcare: Patient System Modelling for Rehabilitation by Exoskeleton.*
18) Márquez, F. P. G., Márquez, F. P. G., Korhan, O., & Ozturk, T. *Digital Twin Technology - Fundamentals and Applications.*
19) Odabaşı, M., & Özkan, E. B. *Simulation of Physiological Parameters for Homeostatic Maintenance: The Role of Digital Twin Technology.*
20) Pirbhulal, S., Abie, H., & Shukla, A. *Towards a Novel Framework for Reinforcing Cybersecurity using Digital Twins in IoT-based Healthcare Applications.*
21) Pirbhulal, S., Chockalingam, S., Abie, H., & Katt, B. *Cognitive Digital Twins for Improving Security in IT-OT Enabled Healthcare Applications.*
22) Popa, E. O., van Hilten, M., Oosterkamp, E. B., & Van de Poel, I. *The use of digital twins in healthcare: socio-ethical benefits and socio-ethical risks.*
23) Pan, R., Sun, H., Chen, X., ... & Yu, Y. *Human Digital Twin: Data, Models, Applications, and Challenges.*
24) Qu, Y., Ma, L., Ye, W., ... & Shen, Y. *Towards Blockchain-Assisted Privacy-Aware Data Sharing For Edge Intelligence: A Smart Healthcare Perspective.*
25) Rojas-Arce, J., & Ortega-Maldonado, E. C. *The Advent of the Digital Twin: A Prospective in Healthcare in the Next Decade.*
26) Thomas, T., Prakash, R., & Pal, S. *Intrusion Detection in Internet of Medical Things Using Digital Twins—A Review.*
27) Troncoso-Pastoriza, J. R., Raisaro, J. L., & Froelicher, D. *Truly privacy-preserving federated analytics for precision medicine with multiparty homomorphic encryption.*
28) Wang, W., Tang, P., Lou, J., Shao, Y., Waller, L., Ko, Y., & Xiong, L. *IGAMT: Privacy-Preserving Electronic Health Record Synthesization with Heterogeneity and Irregularity.*
29) Yi, H. *Improving cloud storage and privacy security for digital twin based medical records.*
30) Zlatolas, L. N., Welzer, T., & Lhotská, L. *Data breaches in healthcare: security mechanisms for attack mitigation.*