International Journal of Digital Twin Systems and Computing (IJDTSC) ISSN: 3108–0790
DOI: https://doi.org/10.XXXXX/IJDTSC.2025.V2I103

Privacy-Preserving Digital Twin Models for Smart Healthcare Applications

[1]Chaithanya Virupaksha
[1]Student, Advance Computer Science, Newcastle University, UK
Email id: c5060796@newcaslte.ac.uk

Abstract ***The integration of Digital Twin technology into Cyber-Physical Healthcare Systems signals a paradigm shift towards a new generation of personalized and predictive medicine. Through the continuous synchronization of physical biological states with dynamic virtual models using the Internet of Medical Things (IoMT) technology, it is now possible for medical professionals to transition from reactive medicine to proactive medicine. Nevertheless, the continuous transmission and aggregation of extremely sensitive physiological data pose a series of critical security challenges that include false data injection, massive data breaches, and the total compromise of data sovereignty for patients. In this paper, we present a comprehensive review of the latest privacy-preserving mechanisms for smart healthcare digital twins. We systematically examine the underlying multi-tier architecture of DTs and their underlying threat models. Moreover, we synthesize the latest results from three key technology pillars for digital twin technology that include Federated Learning (FL) for privacy-preserving machine learning, blockchain technology for establishing data ownership using Non-Fungible Tokens (NFTs), and edge computing for encrypted refreshment services. We then discuss key challenges for the technology that include consensus latency, algorithmic optimization on constrained devices, and regulatory compliance.***

Keywords Digital Twin, Healthcare, Privacy-Preserving, Federated Learning, Blockchain, Internet of Medical Things (IoMT), Edge Computing, Data Sovereignty, Cyber-Physical Systems, Unscented Kalman Filter.

I. Introduction

With the rapid advancement of electronic devices and communication systems, the conventional healthcare system has been revolutionized to a smart, ubiquitous service system with the Internet of Medical Things (IoMT) as the underlying technology. The wide-scale digital revolution, with the subsequent exponential growth of health data, has enabled the integration of the concept of Digital Twin (DT) technology into the Cyber-Physical Healthcare Systems (CPHS). In the aforementioned context, the concept of DT represents a virtual, dynamic entity that can replicate the complex physical, biological, and physiological states of a patient in a real-time environment [1][2]. With the integration of the constant flow of health data from wearable devices, DTs can empower the healthcare system to move from a reactive system to a highly proactive system.[3]

This is despite the immense transformative capabilities of these DTSs in the healthcare sector. The reliance of these DTSs on the constant flow of very sensitive physiological information makes them extremely vulnerable to security risks. Current intelligent healthcare systems are mostly based on centralized servers or cloud infrastructures for data storage and AI model training.[4][5][6] This makes them extremely vulnerable, given that confidential patient information is constantly exposed to adversaries through malicious attacks. The constant flow of sensitive patient information from consumer IoT devices to centralized hospital networks also compromises data sovereignty, where users are denied control over their data access, audit, or utilization.[6][7]

To fully realize the benefits of DTs while not compromising patient safety, there is an urgent need to move towards decentralized DTs while preserving patient privacy. The emerging paradigms of Distributed AI, such as Federated Learning (FL), have been shown to be promising solutions to train predictive models collaboratively on IoMT networks without the need to share raw confidential data with a central server.[8]-[12] At the same time, cryptographic techniques need to be introduced to implement secure user-centric access controls to reinstate data sovereignty for the healthcare user.[14]-[17]

In this review, recent state-of-the-art developments in privacy-preserving Digital Twin models for smart healthcare applications are discussed. In addition, the review will discuss the important intersection of distributed machine learning, blockchain-based cryptographic authentication, and edge computing as a basis for ensuring patient digital avatar security.[13]

The rest of this paper is structured as follows: Section II describes the underlying architecture for the development of cyber-physical healthcare Digital Twins. Section III describes the underlying privacy challenges and threat models for IoMT networks. Section IV describes the advancements in privacy-preserving machine learning techniques and methodologies, specifically focusing on Federated Learning. Section V describes blockchain technology and decentralized authentication techniques for data sovereignty. Section VI describes the underlying edge computing techniques for real-time refreshment of DT accuracy. Finally, Section VII describes the challenges and future directions for this topic, and Section VIII concludes the paper.

II. Architecture of Healthcare Digital Twins

For effective implementation of privacy-preserving mechanisms in CPHS, it is first important to identify and comprehend the underlying architecture of Digital Twins in CPHS. A healthcare DT is not a single entity; rather, it is a sophisticated and multi-layered environment that synchronizes physical biological states and virtual computing environments.[18] According to recent literature, the underlying architecture of a smart healthcare DT can be broadly delineated into four interdependent layers: Physical Layer (Device Layer), Data Management Layer, Modeling Layer, and Application Layer.

A. Physical and Device Layer

The foundation of the DT stack is the physical layer. This layer comprises the human patient under monitoring as well as the array of Internet of Medical Things (IoMT) devices. This includes wearable devices such as smartwatches used to measure the patient's heart rate and blood oxygen levels. This layer's primary role is the acquisition of physiological and environmental data in real-time. This layer provides the empirical foundation for the creation of the digital avatar.[19][20]

B. Data Management and Networking Layer

Acting as a bridge between the physical and virtual worlds, the data management layer has the critical responsibility of ensuring the safe transmission, aggregation, and preprocessing of raw data pertaining to health. This is particularly true since most IoMT devices are known for their limited computing capabilities; hence, edge computing nodes are often used for filtering data before transmission. It is at this point that data is most prone to being intercepted; thus, cryptographic techniques are a key focus in this layer.[21]-[23]

C. Modeling and Computation Layer

The modeling layer is the brain of the Digital Twin. This is where the aggregated data is used to feed complex machine learning algorithms to create a high-fidelity dynamic replica of the patient. This layer not only provides a replica of the current state of the patient but also provides a model of the future state of the patient. Advanced CPHS architectures, such as the DTS-CPHS model, require the intrinsic integration of security and privacy mechanisms within the middleware layer.[22]

D. Application and Service Layer

The highest layer is responsible for translating the insights obtained from the computation carried out by the DT into practical clinical services. The applications that can be performed at this layer include intelligent disease diagnosis, remote monitoring of patients, personalized therapeutic planning, and dynamic optimization of hospital resources. The healthcare professionals and patients use this layer to interact with the DT. Hence, access control mechanisms need to be in place to ensure that only authorized entities can access and interact with the digital avatar.[23]

III. Privacy Challenges and Threat Model in IoMT

The integration of the Internet of Medical Things (IoMT) and Digital Twin technology greatly increases the attack surface for a traditional healthcare network. The reason for this is that a patient's digital avatar requires continuous real-time physiological synchronization. Any disruption in the data pipeline can have catastrophic and deadly clinical outcomes. The threat model for healthcare DT can be defined by the following three vulnerabilities in the CPHS architecture: data acquisition, communication latency, and storage.

A. Physical Layer and False Data Injection

In the device layer, IoMT devices such as sensors and wearables are highly resource-constrained and do not possess the computing power to perform strong cryptographic techniques. Hence, these devices are highly vulnerable to Eavesdropping Attacks, Physical Attacks, and False Data Injection Attacks. In an FDIA attack, an adversary manipulates the physiological data being transmitted from the sensor to the digital twin.[24] The DT makes use of sophisticated state estimation techniques to autonomously predict health conditions and can perform closed-loop medical interventions such as insulin injections and drug therapies. False data can be injected in such a way that the DT's state is compromised in a way that can perform therapeutic actions without the system being able to raise an alarm.

B. Edge-Layer Refreshment Timeouts

In order for a high-fidelity digital avatar to be maintained, continuous "service refreshment" must be provided by the nearby edge computing services. Nevertheless, edge servers that are deployed in a distributed fabric metaverse are exposed to harmful hijacking and resource depletion attacks.

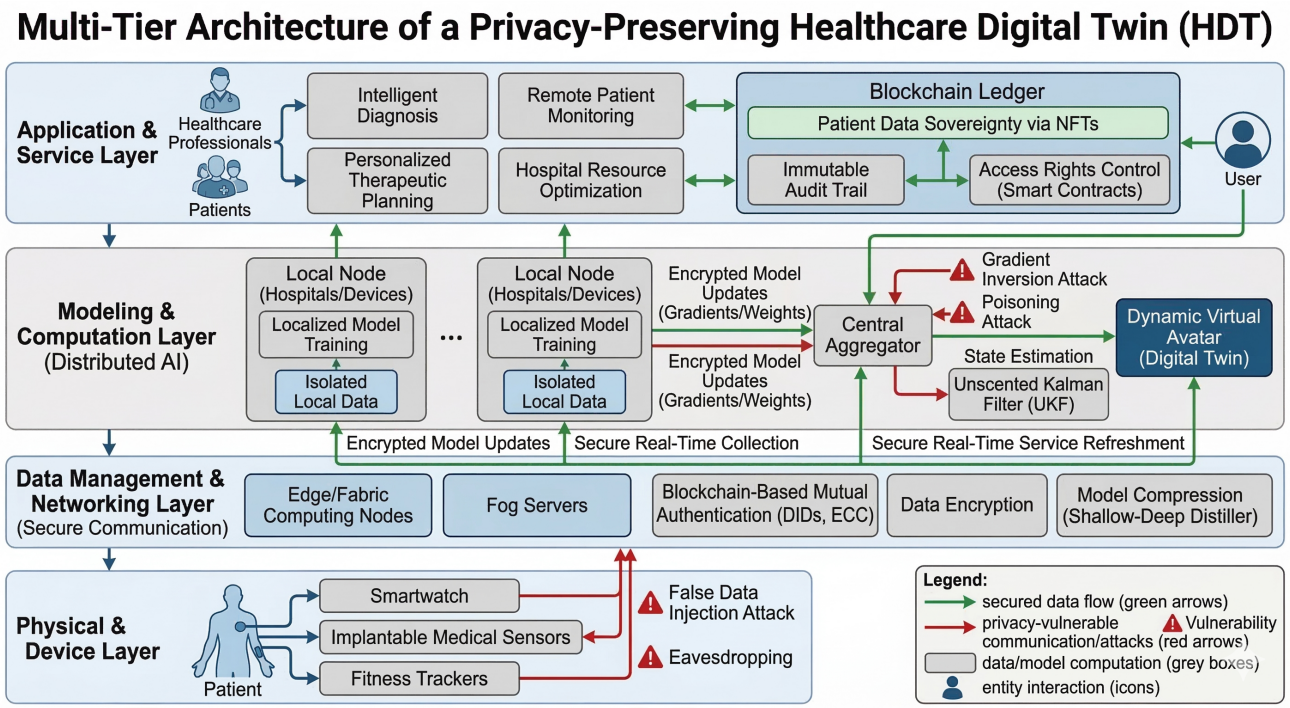

Figure 1: Proposed multi-tier architecture of a Healthcare Digital Twin, illustrating the bidirectional flow of data from physical IoMT sensors through edge-computing data layers, into the virtual modeling environment, and ultimately delivering personalized medical applications.

In the event that a cyber attacker gains access to the edge server, they may intentionally induce refreshment timeouts that halt the synchronization between the physical patient and the digital avatar in real-time.[25] Moreover, processing unencrypted continuous monitoring data from the edge servers results in a major privacy leak, especially for a patient's intimate biological routines.

C. Centralized Storage and Loss of Sovereignty

Traditionally, aggregated medical information is fed into a centralized database located in the hospital for long-term storage. This is a highly lucrative honeypot for cybercriminals to infiltrate, often causing catastrophic breaches of patient data on a large scale. Aside from the risk of external data breaches, the centralized model inherently denies the patient sovereignty over their data. Once the raw physiological data is sent from the patient environment to the centralized hospital server, the patient loses all cryptographic control over how their historical health information and digital twin models are accessed, audited, or shared with external diagnostic agencies.[26]-[28]

IV. Privacy-Preserving Machine Learning in DTs

The creation of high-fidelity Digital Twins in the healthcare industry is heavily dependent on the ingestion and analysis of huge data sets by means of powerful artificial intelligence (AI) and machine learning (ML) algorithms. Nevertheless, as discussed earlier in the threat model, traditional centralized AI systems demand the collection of raw and extremely sensitive Internet of Medical Things (IoMT) data into a single repository for the development of a model. This is against the fundamental principles of data minimization and results in a high likelihood of a huge number of privacy violations. In order to address this major bottleneck in the development of a robust smart healthcare system, Federated Learning (FL) has become the most suitable distributed ML paradigm for ensuring data privacy.

A. The Federated Learning Paradigm in Healthcare

Federated Learning is essentially the flip side of the data-to-model approach. Federated Learning is all about bringing the model to the data. In a Cyber Physical Healthcare System enabled with Federated Learning, the physiological data never needs to leave the local environment. The data may be a wearable device on the patient or a diagnostic tool in the hospital. However, the algorithmic model is sent to the local environments. The local environments then use the data to train the model. After the model has been trained on the local data, the local environments send the calculated gradients back to the central aggregator. The gradients are averaged to create an updated version of the Digital Twin

model.

This decentralized model guarantees that personal health information (PHI) remains in strict isolation and security at the edge, greatly reducing the possibility of data leaks during transmission. The adversary can only intercept the mathematical weights and not the actual biological data. FL effectively eliminates the threat of data leaks while still harnessing the power of a collective network of patients.

B. Intelligent Diagnosis Across Isolated Medical Silos

The most important challenge facing the healthcare industry today is the fragmented patient records. This is mainly due to the fact that a patient may seek medical attention from a number of medical experts working independently in different medical facilities. This leads to a lack of comprehensive patient records in any one facility. Although the integration of such information is essential in the development of precise predictive Digital Twins, the privacy policies are not encouraging the sharing of such information.

Federated Learning skillfully bypasses the ”data silo” challenge in a most elegant manner. By employing FL platforms in a consortium of medical organizations, hospitals can jointly develop smart diagnostic models without ever sharing their own exclusive or patient-specific information with each other. For example, a smart diagnostic system for predicting cardiovascular events can learn from a variety of disjointed patient histories distributed across different independent clinics. The learned global model can attain high levels of diagnostic accuracy and generality, comparable to or surpassing centralized models, solely through the sharing of encrypted model parameters.

C. Incentive Mechanisms and Tokenization in FL

However, the socio-economic challenge that the practical implementation of Federated Learning in healthcare DTs is likely to face is the participation challenge. This is because training complex machine learning models on local edge devices is computationally intensive and may drain the batteries of the edge devices. As a result, a robust Federated Learning framework for healthcare DTs should incorporate a thorough incentive mechanism to encourage participation.

Recent literature also suggests that FL can be combined with tokenized incentive structures that ensure secure incentives for participants. In this model, nodes (patients/hospitals) that provide high-quality, relevant data are rewarded through digital tokens. The incentive model considers several parameters, including data upload frequency, accuracy of local model updates, and computational resources utilized. Gamifying the collaborative training process not only ensures that high-quality training data is constantly fed into the system, which is necessary for accurate and up-to-date Digital Twins, but also ensures confidentiality of health records.

V. Blockchain and Cryptographic Authentication

Although Federated Learning is capable of mitigating the risks that are present during the data aggregation phase in a centralized manner, it does not inherently address the problem of access control or data ownership. In a holistic Cyber-Physical Healthcare System (CPHS), the end user needs to have absolute control over who has access to their medical history records or device twin (DT) models. This has been addressed by the latest literature by suggesting the integration of blockchain technology along with cryptographic techniques for device authentication.

A. Data Sovereignty via Non-Fungible Tokens (NFTs)

In a traditional sense, patient data is considered a proprietary asset of the medical institution that collected it, which gives rise to a lack of patient control. Blockchain technology, in its essence, breaks away from this norm by introducing a decentralized, immutable ledger for recording transactions related to patient data access.

One of the most interesting innovations in patient data sovereignty is the concept of tokenizing medical records and DT models via a concept called Non-Fungible Tokens (NFTs). In essence, an NFT is a unique, cryptographically generated certificate of ownership for a certain part of a patient’s medical records. By employing smart contracts on a blockchain network, a marketplace is effectively created where patients can control the granting, revoking, or monetization of their historical medical records for purposes of intelligent diagnosis or research, with clear demarcations on accessibility and patient consent.

B. Decentralized Identifiers and Secure Authentication

Aside from data storage, the continuous data flow from physical IoMT devices to the virtual DT also needs to be subjected to strict authentication. If an attacker can successfully impersonate a wearable device, he/she can inject malicious data into the digital avatar and cause misdiagnosis or erroneous therapeutic actions.

To counter this potential threat, recent cryptographic techniques utilize a decentralized identifier and verifiable credential system based on blockchain technology. While the conventional Public Key Infrastructure (PKI) method relies on a centralized third-party authority to verify and authenticate data, a decentralized identifier allows consumer healthcare devices and medical servers to authenticate one another in a peer-to-peer manner. When coupled with lightweight Elliptic Curve Cryptography (ECC), a secure communication channel can be established between the consumer healthcare devices and the DT. The mutual authentication technique ensures that only authentic physiological data from the patient’s authorized devices can be synchronized with their respective DTs, effectively eliminating the possibility of impersonation and man-in-the-middle attacks

while keeping the computation overhead low for resource-constrained IoMT devices.

“‘latex “‘

VI. Edge Computing and Real-Time Service Refreshment

Although both Federated Learning and Blockchain Technologies offer robust platforms for decentralized model training, the actual utility of a Healthcare Digital Twin depends on its ability to synchronize with the patient in real-time, a concept known as ”service refreshment.” This synchronization demands tremendous computational power, far beyond what wearable Internet of Medical Things devices are capable of delivering. Hence, Healthcare Digital Twins heavily rely on Edge Computing for synchronization purposes, as it bridges the physical-virtual world divide. Yet, in doing so, it brings about a host of intricate trade-offs in terms of computational latency and data privacy.

A. Adaptive Task Offloading and Resource Management

For this purpose, raw physiological data needs to be continuously processed and mapped onto the digital avatar. This processing is done locally on nearby IoMT devices, which are resource-constrained. This is why this processing is done on nearby edge servers, which are computationally powerful. However, this also leads to a risk of interception of patient data and overloading of bottlenecks in the network.

To address these issues, recent frameworks have proposed various intelligent computational resource management strategies, including the Adaptive Cybersecurity Task Offloading (ACTO) algorithm. Instead of relying on conventional static task offloading rules, this algorithm evaluates the dynamic threat environment, network availability, and urgency of the particular healthcare task in real-time. This allows for optimizing the balance between extremely low latency requirements of digital avatars and extremely high cybersecurity requirements through intelligent task partitioning, where computationally intensive state estimation tasks are performed on secure edge nodes, whereas lightweight anomaly detection is performed locally on the device.

B. Privacy-Enhanced Refreshment in the Fabric Metaverse

The idea of a ’Fabric Metaverse’ expands upon the concept of the HDT model by incorporating a ubiquitous and connected digital world in which digital avatars assist in the continuous remote monitoring and predictive diagnosis. In this world, refreshment of services involves the transmission of personal health data to corresponding diagnostic services running on edge servers and the receipt of predictive results for continuous refreshment of the local avatar. Nevertheless, the semi-trusted and possibly malicious nature of decentralized edge servers poses a critical threat. A refreshment timeout can occur in the event that an edge node is compromised or overwhelmed, desynchronizing the digital twin and failing to make a predictive diagnosis for a critical medical event. Furthermore, continuous execution of diagnostic inferences using unencrypted data at the edge results in a leak in user privacy. The aforementioned issues can be overcome by employing a combination of data encryption and model compression. The use of shallow and deep distiller technology allows for the execution of complex AI models for HDT updates at a high rate. The use of efficient resource schedulers ensures that data remains encrypted during the inference phase, thereby guaranteeing user privacy against malicious edge nodes.

VII. Open Challenges and Future Directions

Though the integration of Federated Learning (FL), blockchain, and secure edge computing has a strong theoretical underpinning for the implementation of privacy-preserving Healthcare Digital Twins (HDTs), there are a number of significant challenges that must be addressed to make HDTs a reality.

A. Scalability and Consensus Latency in Emergencies

However, blockchain-based frameworks and Non-Fungible Tokens (NFTs) ensure data sovereignty. There is a major drawback of blockchain-based frameworks in terms of consensus latency. Acute healthcare situations, like a cardiac arrest detected by an IoMT-based wearable device, demand an immediate response from the digital twin. The delay in the consensus mechanism of blockchain-based frameworks for refreshing the critical services may prove to be life-threatening. Therefore, the research should be directed towards the development of an ultra-low-latency consensus mechanism for emergency medical interventions.

B. Optimization of Edge-Based State Estimation

The computational cost of executing complex biological simulations and continuous encryption processes for edge nodes is also a severe issue. Additionally, while digital twins are based on continuous state estimation techniques, the use of computationally expensive pre-compiled complex simulation models (such as standard Simulink UKF blocks) is also found to incur unacceptable processing delays for edge nodes. The future architectures need to be designed to incorporate lightweight and highly customized Unscented Kalman Filter (UKF) and other predictive models that are specifically written for constrained local devices. This is to move beyond computationally expensive software blocks to highly customized code to achieve acceptable computational efficiency with continuous encrypted refreshment.

C. FL Vulnerabilities and Unbalanced Datasets

While Federated Learning protects against raw data leakage, it is not entirely safe against privacy violations. Sophisti-

Table 1: Summary of Reviewed Literature on Privacy-Preserving Healthcare Digital Twins

Ref.	Core Technology	Privacy / Security Mechanism	Target Application	Key Limitation / Challenge
[1]*	Edge AI & Digital Twins	Adaptive Cybersecurity Task Offloading (ACTO) algorithm	Dynamic computational resource management and threat mitigation	High complexity in balancing latency with robust security protocols
[2]*	Multi-Tier Architecture	DTS-CPHS architecture with embedded middleware security	Foundational cyber-physical system design and patient monitoring	Interoperability across heterogeneous hospital data formats
[3]*	Broad DT Framework	Multi-layer integration (Device, Data, Modeling, Application)	Smart personalized healthcare and operational efficiency	Lack of standardized regulatory compliance (e.g., HIPAA/GDPR) mapping
[4]*	Blockchain & IoMT	Decentralized Identifiers (DIDs) and Elliptic Curve Cryptography (ECC)	Secure mutual authentication between devices and medical servers	Scalability of blockchain transactions during real-time emergencies
[5]*	Edge Computing & Metaverse	Data encryption and shallow-deep distiller model compression	Preventing privacy leaks during real-time service refreshment	Computational overhead on malicious or resource-limited edge nodes
[6]*	Federated Learning & NFTs	Decentralized ML, smart contracts, and tokenized incentive mechanisms	Intelligent disease diagnosis across isolated hospital silos	Designing fair incentive algorithms for highly unbalanced local datasets
[7]*	Federated Learning (Survey)	Gradient-sharing and localized data processing	Broad privacy preservation in decentralized smart healthcare networks	Vulnerability to gradient-inversion attacks if aggregators are compromised

cated attacks can use gradient inversion attacks on the central aggregator to obtain sensitive patient information by reversing the model weights. Further, the design of incentive schemes for Federated Learning faces challenges due to the highly unbalanced medical data distribution (non-IID data). Future Federated Learning architectures need to incorporate the concept of Differential Privacy (DP) into the gradient-sharing mechanism.

D. Interoperability and Regulatory Compliance

One major hindrance for the proposed multi-tier architectures is the absence of standardized data format in heterogeneous hospital systems. For the intelligent diagnosis models to effectively learn from these isolated silos, a universal ontology for HDT data needs to be proposed. Moreover, although the proposed cryptographic mechanisms have shown promising results for improving privacy, future literature needs to clearly establish the correlation between these proposed solutions and existing laws, proving strict compliance with regulations like HIPAA or GDPR.

VIII. Conclusion

The promise that the transition to Cyber Physical Healthcare Systems enabled by the power of Digital Twins holds is unprecedented. However, the need to synchronize the extremely sensitive physiological data between the physical patients and their virtual twins in real-time has created a situation that is extremely vulnerable to cyber threats. The current review has attempted to synthesize the current literature to propose a decentralized approach that will ensure the security of the HDT ecosystem. The use of Federated Learning for the training of models in a decentralized manner, blockchain with NFTs for ensuring the sovereignty of the patients' data, and optimized edge computing for the refreshment of the services in an encrypted manner will help to ensure the security of the HDT ecosystem. However, the next steps that will be crucial to ensure the scalability, optimization, and interoperability of the HDT ecosystem will be key to ensuring a future that is full of promise for medical intelligence as well as the security of the patients' data.

References

[1] A. K. Jameil and H. Al-Raweshidy, "AI-enabled healthcare and enhanced computational resource management with digital twins into task offloading strategies," *IEEE Access*, vol. 12, pp. 90356–90370, 2024.

[2] M. S. Roopa and K. R. Venugopal, "Digital twins for cyber-physical healthcare systems: Architecture, requirements, systematic analysis, and future prospects," *IEEE Access*, vol. 13, pp. 44960–44996, 2025.

[3] A. Balasubramanyam, R. Ramesh, R. Sudheer, and P. B. Honnavalli, "Revolutionizing healthcare: A review unveiling the transformative power of digital twins," *IEEE Access*, vol. 12, pp. 69650–69676, 2024.

[4] D. Kwon, A. K. Das, and Y. Park, "A blockchain-based mutual authentication scheme with data sovereignty for IoT-based healthcare digital twin environments," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 4, pp. 9401–9415, Nov. 2025.

[5] Y. Qiu, M. Chen, W. Liang, L. Ai, D. Niyato, and G. Wei, "Privacy-enhanced healthcare monitoring service refreshment in human digital twin-assisted fabric metaverse," *IEEE Transactions on Mobile Computing*, vol. 24, no. 11, pp. 11731–11745, Nov. 2025.

[6] S. Sai, V. Hassija, V. Chamola, and M. Guizani, "Federated learning and NFT-based privacy-preserving medical-data-sharing scheme for intelligent diagnosis in smart healthcare," *IEEE Internet of Things Journal*, vol. 11, no. 4, pp. 5568–5580, Feb. 2024.

[7] M. Ali, F. Naeem, M. Tariq, and G. Kaddoum, "Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 2, pp. 778–789, Feb. 2023.

"'latex

[8] Y. Tai, B. Gao, Q. Li, Z. Yu, C. Zhu, and V. Chang, "Trustworthy and intelligent COVID-19 diagnostic IoMT through XR and deep-learning based clinic data access," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15965–15976, Nov. 2021.

[9] R. F. Mansour, A. El Amraoui, I. Nouaouri, V. G. Díaz, D. Gupta, and S. Kumar, "Artificial intelligence and Internet of Things enabled disease diagnosis model for smart healthcare systems," *IEEE Access*, vol. 9, pp. 45137–45146, 2021.

[10] M. Tariq, M. Ali, F. Naeem, and H. V. Poor, "Vulnerability assessment of 6G-enabled smart grid cyber-physical systems," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5468–5475, Apr. 2021.

[11] F. Naeem, M. Tariq, and H. V. Poor, "SDN-enabled energy-efficient routing optimization framework for industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5660–5667, Aug. 2021.

[12] B. Yuan, S. Ge, and W. Xing, "A federated learning framework for healthcare IoT devices," arXiv:2005.05083, 2020.

[13] M. J. Sheller *et al.*, "Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data," *Scientific Reports*, vol. 10, no. 1, pp. 1–12, 2020.

[14] D. C. Nguyen *et al.*, "Federated learning for industrial Internet of Things in future industries," *IEEE Wireless Communications*, vol. 28, no. 6, pp. 192–199, Dec. 2021.

[15] R. VanderMeulen, "Gartner says 8.4 billion connected 'things' will be in use in 2017, up 31 percent from 2016," Gartner, 2017.

[16] A. Zaslavsky, A. Hassani, P. D. Haghighi, A. Robles-Kelly, and P. K. Chrysanthis, "Crystal-ball and magic wand combined: Predicting situations and making them happen," in *Proc. Int. Conf. Distributed Computing and Networking*, 2020, pp. 683–697.

[17] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for Internet of Things: Recent advances, taxonomy, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1759–1799, Jul.–Sep. 2021.

[18] J. Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian, and F. Wang, "Federated learning for healthcare informatics," *Journal of Healthcare Informatics Research*, vol. 5, no. 1, pp. 1–19, 2021.

[19] Q.-V. Pham *et al.*, "Fusion of federated learning and industrial Internet of Things: A survey," arXiv:2101.00798, 2021.

[20] N. Rieke *et al.*, "The future of digital health with federated learning," *NPJ Digital Medicine*, vol. 3, no. 1, pp. 1–7, 2020.

[21] L. Tawalbeh *et al.*, "IoT privacy and security: Challenges and solutions," *Applied Sciences*, vol. 10, no. 12, Art. no. 4102, 2020.

[22] W. Aman and F. Kausar, "Towards a gateway-based context-aware and self-adaptive security management model for IoT-based eHealth systems," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, pp. 280–287, 2019.

[23] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Computer Science Review*, vol. 38, Art. no. 100312, 2020.

[24] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the Internet of Medical Things (IoMT)," in *Proc. 15th Int. Conf. Distributed Computing in Sensor Systems*, 2019, pp. 457–464.

[25] F. Alshehri and G. Muhammad, "A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare," *IEEE Access*, vol. 9, pp. 3660–3678, 2021.

[26] R. Raeside, S. R. Partridge, A. Singleton, and J. Redfern, "Cardiovascular disease prevention in adolescents: eHealth, co-creation, and advocacy," *Medical Sciences*, vol. 7, no. 2, Art. no. 34, 2019.

[27] U. Ahmad, H. Song, A. Bilal, S. Saleem, and A. Ullah, "Securing insulin pump system using deep learning and gesture recognition," in *Proc. IEEE Int. Conf. Trust, Security and Privacy in Computing and Communications*, 2018, pp. 1716–1719.

[28] K. Rannenberg, "Enabling identity management and privacy in a global context: ISO/IEC standardization in JTC 1/SC 27/WG 5," vol. 11, no. 2, pp. 9–24, 2018.