Chapter 16

Privacy-preserving federated learning in IoT for smart and sustainable healthcare

Shinu M. Rajagopal[a], **Supriya M**[a], **and Rajkumar Buyya**[b]

[a]*Department of Computer Science and Engineering, Amrita School of Computing, Bengaluru, Amrita Vishwa Vidyapeetham, Bengaluru, India,*
[b]*Quantum Cloud Computing and Distributed Systems (qCLOUDS) Laboratory, School of Computing and Information Systems, The University of Melbourne, Melbourne, VIC, Australia*

Chapter points

- This chapter explores how federated learning enables privacy-preserving data sharing in IoT-driven smart healthcare systems, ensuring secure collaboration without exposing sensitive patient information.
- It emphasizes sustainable methodologies employed in next-generation healthcare systems.

16.1 Background on IoT in healthcare

The rapid advancement of the Internet of Things (IoT) and artificial intelligence has transformed modern healthcare systems, enabling real-time monitoring, predictive diagnostics, and personalized treatment pathways. However, the massive influx of sensitive medical data from IoT-enabled devices has raised significant concerns regarding data security, patient confidentiality, and system scalability. To address these challenges, federated learning (FL) has emerged as a groundbreaking paradigm that enables decentralized model training without the need for raw data sharing. This chapter explores the integration of privacy-preserving federated learning in IoT-based healthcare to build smart, secure, and sustainable medical solutions that balance innovation with ethical responsibilities [1].

IoT in healthcare encompasses a wide spectrum of interconnected devices such as wearable sensors, implantable medical devices, and remote patient monitoring systems, all contributing to data-driven clinical decision-making. By enabling continuous, real-time data collection on patient health metrics, IoT facilitates early detection of diseases, proactive care delivery, and reduced hospital readmissions. The integration of IoT with cloud computing and AI analytics has further enhanced diagnostic accuracy and operational efficiency. However, the distributed and heterogeneous nature of these devices creates unique technical and security challenges that necessitate innovative approaches like federated learning to ensure reliable and trustworthy healthcare management [2].

16.1.1 Sustainability challenges in healthcare systems

Despite the immense benefits of digitization, healthcare systems face notable sustainability challenges, particularly due to increasing costs, energy consumption, unequal accessibility, and growing volumes of health data. IoT-driven healthcare requires robust computational infrastructure, which may strain both economic and environmental resources if not managed efficiently. Moreover, traditional centralized data-processing approaches introduce bottlenecks and privacy risks that hinder long-term sustainability. Achieving truly sustainable healthcare demands solutions that minimize resource utilization, improve patient outcomes, and ensure equitable access, while safeguarding sensitive information across global networks [3]. Fig. 16.1 illustrates the sustainability challenges (highlighted in red; mid gray in print version) and the corresponding solution directions (highlighted in green; light gray in print version) within digitized healthcare systems.

16.1.2 Role of federated learning

Federated learning offers a decentralized machine learning framework that allows multiple IoT devices, hospitals, or healthcare institutions to collaboratively train AI models without directly sharing sensitive patient data. By keeping data localized and only transmitting model updates, FL reduces the risks of privacy breaches while maintaining high-quality

Federated Learning. https://doi.org/10.1016/B978-0-44-344433-3.00021-6

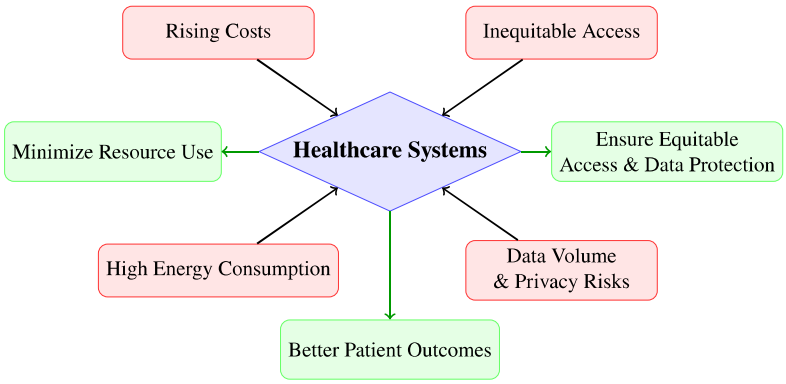

FIGURE 16.1 Sustainability challenges (red; mid gray in print version) and solution directions (green; light gray in print versio) in digitized healthcare systems.

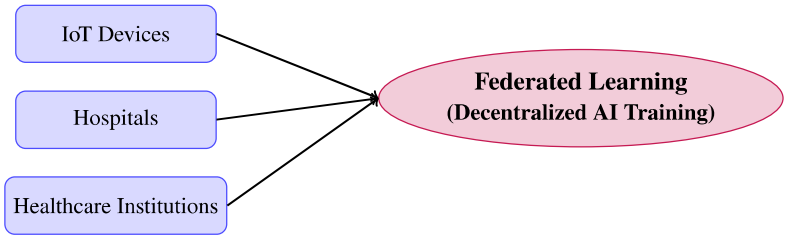

FIGURE 16.2 Data sources feeding into Federated Learning for decentralized AI training.

predictive performance. In healthcare, this approach enables multi-institutional collaborations on disease prediction, drug response modeling, and medical imaging analysis, while respecting strict regulatory requirements such as HIPAA and GDPR. FL thus represents a scalable, secure, and ethical pathway to harness AI's potential in healthcare innovation [4].

16.1.3 Importance of privacy-preserving mechanisms

While federated learning reduces direct data exposure, privacy breaches can still occur through model updates and communication channels, necessitating the integration of advanced privacy-preserving mechanisms. Techniques such as differential privacy, homomorphic encryption, and secure multi-party computation ensure that sensitive patterns cannot be inferred even during collaborative training. These approaches strengthen trust in IoT-based healthcare platforms by protecting against malicious actors, insider threats, and data reconstruction attacks. Implementing robust privacy-preserving strategies is therefore fundamental to ensuring ethical compliance, fostering patient trust, and enabling scalable adoption of federated learning in sustainable healthcare systems [5]. Fig. 16.2 depicts the data sources feeding into Federated Learning for decentralized AI training.

16.2 Foundations of federated learning in healthcare IoT

16.2.1 Federated learning vs. traditional centralized learning

Federated learning (FL) is a distributed machine learning paradigm that enables multiple clients, such as IoT-enabled medical devices or healthcare institutions, to collaboratively train a global model without transferring raw data to centralized servers. Instead, each participant trains a local model on its private dataset and transmits only model updates, which are aggregated securely to form an improved shared global model. This structure significantly reduces privacy concerns, decreases communication overhead, and allows the utilization of diverse data sources across locations, making FL particularly appealing for sensitive domains like healthcare, where patient confidentiality remains paramount.

The key distinction between FL and traditional centralized learning lies in data management. In centralized learning, data is pooled into a single repository, which raises risks of privacy leakage, centralized data breaches, and compliance issues under healthcare regulations. FL eliminates the need to transfer sensitive raw data, shifting the computational focus to the edge devices themselves and only requiring communication of model parameters. This not only mitigates risks but

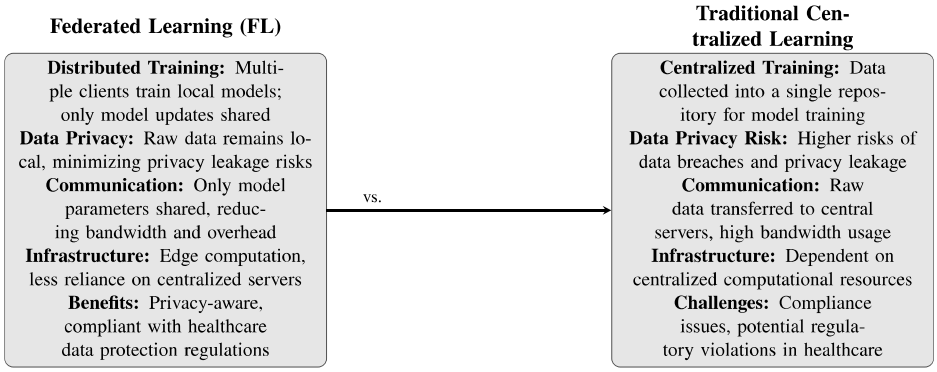

FIGURE 16.3 Comparison of Federated Learning and Traditional Centralized Learning paradigms in healthcare AI.

also reduces reliance on high-bandwidth channels and centralized computational infrastructure. Compared to centralized approaches, FL is inherently more privacy-aware and better aligned with healthcare's stringent data protection requirements [6]. Fig. 16.3 presents a comparison between Federated Learning and traditional centralized learning paradigms in healthcare AI.

16.2.2 Suitability for IoT-based healthcare applications

IoT in healthcare generates diverse, continuous, and highly sensitive patient data from wearable devices, hospital monitors, and remote diagnostic tools. Given the decentralized and heterogeneous nature of these devices, federated learning is especially suited to orchestrating collaborative model training without compromising data ownership or privacy. FL addresses several healthcare-specific challenges such as compliance with HIPAA/GDPR, minimizing communication overhead for resource-constrained devices, and adapting to non-IID (non-independent and identically distributed) healthcare data. Applications include disease risk prediction from wearable sensors, anomaly detection in patient vitals, personalized medicine, and improving diagnostic accuracy with heterogeneous hospital datasets [7].

16.2.3 Key performance indicators (accuracy, latency, energy efficiency, privacy)

Evaluating federated learning in healthcare IoT requires careful consideration of multiple key performance indicators (KPIs). Accuracy reflects the predictive performance of the global model in diverse healthcare scenarios and is critical for clinical adoption. Latency indicates the training and inference time, which is vital for real-time health monitoring and decision-making in emergencies. Energy efficiency monitors the computational and communication costs, particularly since many IoT medical devices are battery-powered and resource-constrained. Privacy remains the most crucial KPI, ensuring that sensitive patient information cannot be traced, reconstructed, or leaked during model training and communication. Balancing these KPIs is central to building effective, sustainable, and trustworthy FL frameworks for healthcare [8].

16.3 Privacy and security challenges in healthcare IoT

16.3.1 Sensitive medical data handling

Healthcare IoT systems continuously collect highly sensitive patient information, including physiological signals, diagnostic images, and behavioral patterns. Ensuring the confidentiality, integrity, and availability of such data is critical for maintaining patient trust and adhering to ethical standards. However, managing this data is challenging due to the distributed nature of IoT devices, limited processing capabilities, and reliance on wireless communication. Improper handling can expose vulnerabilities, making healthcare IoT a prime target for cyberattacks. Thus, robust encryption, secure communication protocols, and privacy-preserving learning techniques such as federated learning are essential for safe medical data management [9].

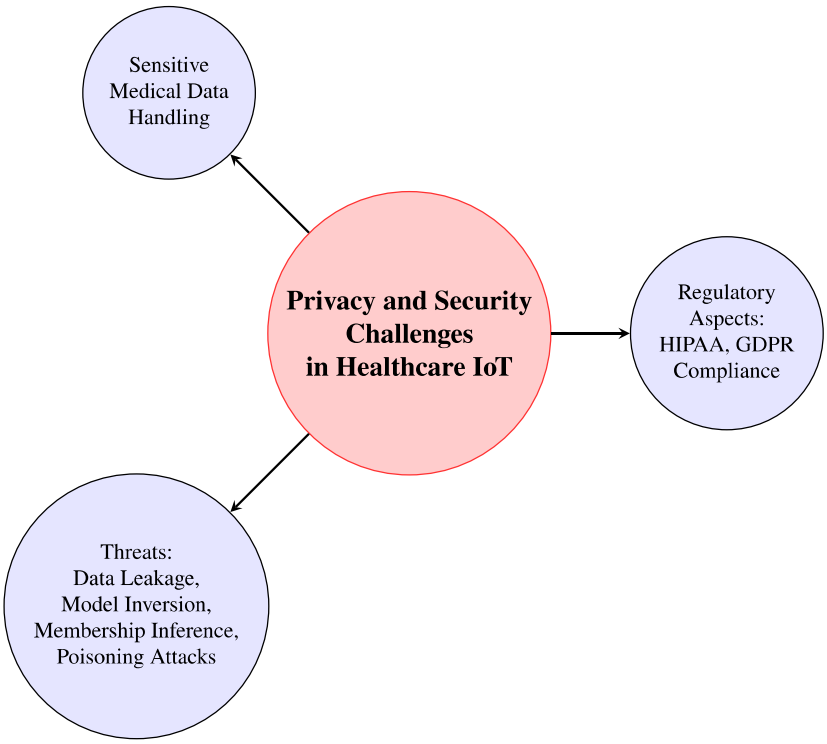

FIGURE 16.4 Privacy and Security Challenges in Healthcare IoT with aspects as smaller circles connected from the central circle.

16.3.2 Threats: data leakage, model inversion, membership inference, poisoning attacks

Despite the adoption of federated learning, healthcare IoT remains vulnerable to a variety of threats. Data leakage may occur due to insecure communication or storage mechanisms, exposing patient-specific details. Model inversion attacks attempt to reconstruct private patient data from shared gradients or model parameters. Membership inference attacks exploit trained models to determine whether a specific individual's record was part of the training dataset, which can have severe privacy implications in clinical contexts. Poisoning attacks, in both data and model updates, can introduce malicious samples or manipulations, undermining predictive accuracy, disrupting clinical decision-making, and risking patient safety. These threats highlight the urgent need for integrating resilience techniques such as secure aggregation, anomaly detection, and adversarial defense strategies in federated healthcare frameworks [10].

16.3.3 Regulatory aspects (HIPAA, GDPR compliance)

Healthcare IoT solutions must strictly adhere to data protection and privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. These regulatory frameworks emphasize patient rights, informed consent, secure data handling, and accountability of stakeholders in managing medical records. Non-compliance can lead to severe legal, financial, and reputational consequences for healthcare institutions. Federated learning, when coupled with privacy-preserving mechanisms like differential privacy and encryption, offers a pathway to meeting compliance requirements by ensuring that raw patient data remains decentralized and securely managed, thereby aligning technical innovation with regulatory mandates [11]. Fig. 16.4 illustrates the privacy and security challenges in Healthcare IoT

16.4 Privacy-preserving techniques in federated learning

16.4.1 Differential privacy

Differential privacy (DP) has emerged as a cornerstone in privacy-preserving machine learning due to its strong theoretical guarantees against inference attacks. It operates by injecting statistical noise into local gradients or model updates before

they are shared in the federated learning (FL) process. This ensures that the contribution of any single patient record remains indistinguishable from the aggregated model, thereby preventing adversaries from reconstructing sensitive medical details. In healthcare IoT, where small patient datasets from wearables, clinical devices, and monitoring systems may reveal vulnerable patterns, differential privacy plays a crucial role in ensuring individual-level protection. However, striking the right balance between privacy guarantees and model accuracy remains a vital research concern. Excessive noise injection may lead to significant degradation in prediction quality for critical applications like disease detection or anomaly monitoring, requiring adaptive DP strategies tailored to healthcare data variability [12].

16.4.2 Homomorphic encryption

Homomorphic encryption (HE) is a powerful cryptographic technique that enables mathematical operations to be performed directly on encrypted values without requiring decryption. In FL-based healthcare IoT, this property allows encrypted local model updates from medical devices or hospitals to be aggregated securely by a central server. Even if the server or communication channel is compromised, attackers cannot learn the underlying sensitive information from the encrypted model parameters. HE provides a strong layer of confidentiality against model inversion or eavesdropping threats, making it valuable in privacy-critical healthcare contexts. However, fully homomorphic encryption (FHE) schemes are computationally expensive and demand significant processing resources, which hinders their adoption in lightweight IoT environments. To mitigate this, researchers are exploring partially homomorphic encryption (PHE) and approximate HE schemes that reduce overhead while maintaining acceptable privacy protection. Future research is focused on optimizing HE implementations to make them suitable for large-scale medical IoT deployments [13].

16.4.3 Secure multiparty computation

Secure Multiparty Computation (SMPC) allows multiple distributed participants to perform joint computations on their inputs while revealing no private data outside what is necessary for the final output. In federated healthcare systems, SMPC ensures that hospitals, IoT-enabled monitoring devices, and diagnostic centers can collaborate on global model training without exposing local datasets or model updates. For instance, model aggregation can be performed using secret-sharing-based protocols where no single party has access to the complete information. This effectively mitigates risks of malicious collusion and data leakage during the learning process. The efficiency of SMPC is an ongoing challenge as protocol complexity grows with scale, often leading to increased communication and computational overhead. Still, advances in lightweight cryptographic constructs and privately verifiable computation continue to pave the way for its practical application in healthcare FL, enabling high privacy without explicitly compromising efficiency [14].

16.4.4 Blockchain for secure aggregation

Blockchain offers a decentralized, immutable ledger system that ensures transparency, accountability, and tamper-resistance in federated learning for healthcare IoT. In this context, blockchain can serve as a secure backbone for aggregating updates, recording all participating nodes' transactions, and ensuring data provenance. By leveraging smart contracts, the aggregation of model updates can be automated, reducing dependence on centralized servers and making the system resistant to single points of failure. Blockchain also provides auditability, enabling healthcare institutions and regulators to validate the integrity of the collaborative process. However, blockchain adoption in FL requires addressing scalability and energy efficiency issues, particularly in healthcare IoT where devices often have resource limitations. Integrating blockchain with privacy-preserving protocols such as differential privacy or SMPC creates a multi-layered defense that enhances trust and security across large-scale healthcare networks. Its decentralized trust model holds promise for fostering inter-institutional collaborations while mitigating security vulnerabilities [15].

16.4.5 Lightweight cryptography for resource-constrained IoT devices

IoT devices in healthcare environments are often constrained in terms of energy, computational power, and memory, yet they handle essential health data whose security cannot be compromised. Lightweight cryptography addresses this challenge by providing optimized encryption and privacy-preserving algorithms specifically designed for low-resource hardware. Unlike traditional schemes such as AES or RSA, lightweight cryptographic protocols rely on compact key sizes, lower computational complexity, and energy-efficient architectures. When combined with FL, lightweight cryptography allows even portable wearable devices and implantable sensors to participate securely in collaborative learning without exhausting

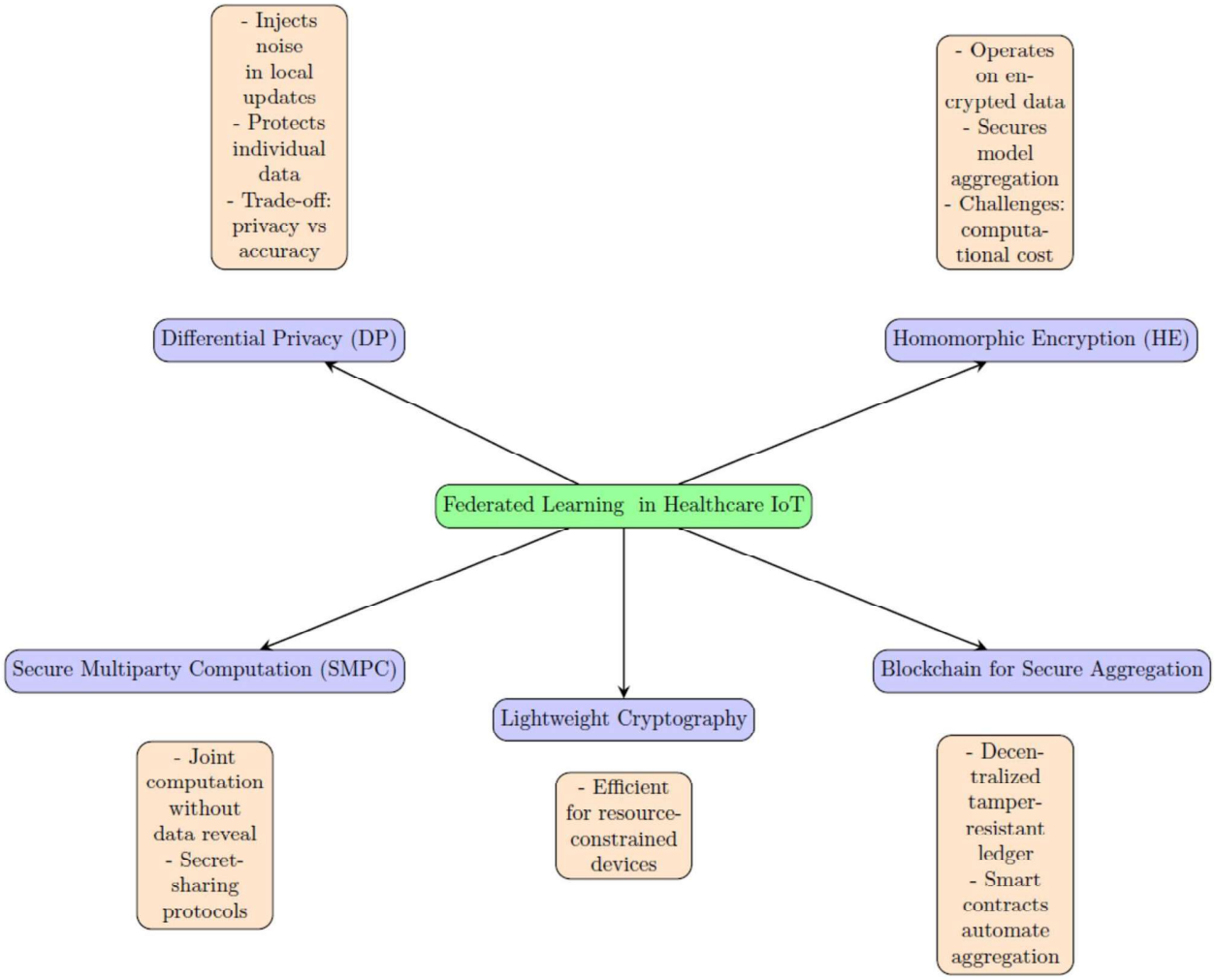

FIGURE 16.5 Privacy-Preserving Techniques in Federated Learning.

local resources. This approach ensures inclusivity in healthcare FL ecosystems, allowing data from all patients, regardless of their devices' capabilities, to contribute to accurate predictive models. Current research focuses on balancing the trade-offs between efficiency, scalability, and resilience against emerging IoT-specific attack vectors, making lightweight cryptography a critical enabler for sustainable privacy-preserving FL solutions in healthcare [16]. Fig. 16.5 illustrates the privacy-preserving techniques employed in Federated Learning.

16.5 Architectures for privacy-preserving FL in healthcare IoT

16.5.1 Edge-assisted federated learning

Edge-assisted federated learning leverages the computing capabilities of IoT edge devices or local gateways situated close to healthcare data sources. In this architecture, sensitive data collected from wearable sensors, remote diagnostic tools, and patient monitoring systems is processed locally on edge nodes, which then train partial models or pre-process features before transmitting encrypted updates to the federated learning server. This approach significantly reduces communication latency, preserves bandwidth, and ensures that raw data never leaves the patient's vicinity, thereby reinforcing privacy and minimizing security risks. For healthcare use cases such as continuous cardiac monitoring or insulin-level prediction, edge-assisted FL enables near real-time intelligence with improved responsiveness while respecting privacy mandates like

HIPAA and GDPR. However, the heterogeneity and limited resources of edge devices introduce challenges in ensuring scalable and robust deployments, necessitating adaptive model partitioning and efficient update aggregation methods [17].

16.5.2 Fog-cloud hybrid models

Fog-cloud hybrid federated learning architectures integrate the distributed processing capability of fog computing with the powerful resources of cloud computing. In healthcare IoT, fog nodes—typically hospital servers or intelligent gateways—act as intermediaries that aggregate updates from numerous edge devices before forwarding them to the cloud for global model refinement. This hierarchical design reduces network congestion, lowers communication overhead, and enables localized analytics at the fog layer, which can be crucial for urgent medical responses in telemedicine or emergency care. The cloud layer, in turn, provides global scalability, advanced model optimization, and long-term storage of healthcare analytics. Privacy-preserving mechanisms such as differential privacy and secure aggregation are embedded at each layer to ensure that patient information remains protected. While hybrid architectures offer reliability and scalability, they demand sophisticated orchestration policies to balance workloads, safeguard communication channels, and reduce overall energy consumption [18].

16.5.3 Cross-device vs. cross-silo healthcare FL

Federated learning in healthcare can be broadly categorized into cross-device and cross-silo architectures. Cross-device FL involves training on large numbers of heterogeneous and resource-constrained IoT devices, such as fitness trackers, implantables, or wearable health monitors. These devices contribute personalized updates, enabling fine-grained learning that supports patient-specific healthcare interventions. In contrast, cross-silo FL is deployed across institutions such as hospitals, research labs, or diagnostic centers where each silo has relatively stable, high-quality datasets and computing resources. Cross-silo setups facilitate collaborative medical research (e.g., multi-hospital cancer prediction models) while complying with privacy regulations by keeping patient records locally. The choice between these two architectures depends on application needs: cross-device FL is ideal for personalized, distributed patient care, while cross-silo FL supports broader institutional collaboration and large-scale predictive modeling. Combining the strengths of both can establish robust privacy-preserving ecosystems for comprehensive healthcare intelligence [19].

16.5.4 Sustainable deployment considerations (energy-aware FL)

Sustainability remains a critical consideration for deploying federated learning in healthcare IoT, given the energy-sensitive nature of medical sensors and wearable devices. Traditional FL workflows can impose heavy communication and computational demands that drain battery-operated devices or exceed hospital infrastructure budgets. Energy-aware FL architectures emphasize optimizing training processes, reducing unnecessary communication rounds, and leveraging compression techniques such as quantization and sparsification. Adaptive client selection strategies also limit participation to devices with sufficient resources, balancing accuracy with efficiency. Furthermore, renewable energy integration at fog and cloud layers can support eco-friendly operations. In the healthcare sector, sustainable FL ensures long-term affordability and reliability of privacy-preserving solutions, making large-scale deployment both feasible and environmentally responsible. Future research is increasingly focusing on balancing patient outcomes, system accuracy, and green computing principles to pave the way for scalable and sustainable healthcare innovations [20].

16.6 Case studies and applications

16.6.1 Smart wearable devices for patient monitoring

Smart wearable devices such as fitness trackers, smartwatches, and implantable biosensors have become vital tools for continuous patient monitoring. These devices capture real-time physiological data including heart rate, blood pressure, oxygen saturation, and glucose levels, enabling early detection of anomalies. Federated learning (FL) enhances the utility of such devices by allowing multiple wearables to collaboratively train models for health prediction without exposing personal data to centralized servers. For instance, FL-enabled wearables can detect arrhythmias or respiratory distress by pooling knowledge from thousands of distributed devices, improving diagnostic accuracy while preserving patient privacy. Privacy-preserving approaches like differential privacy ensure that even sensitive biometric data cannot be reverse-engineered from model updates. This decentralized framework not only empowers individualized patient care but also provides scalable healthcare monitoring solutions for wider populations [21].

16.6.2 Federated learning for medical imaging

Medical imaging—covering modalities such as X-rays, MRI scans, CT scans, and ECGs—represents a domain where collaborative learning across institutions can significantly boost the accuracy of diagnostic models. Traditionally, pooling imaging data from multiple hospitals raises serious regulatory and ethical concerns, as patient records are highly sensitive. Federated learning resolves this bottleneck by allowing hospitals to keep imaging data locally while sharing only aggregated model parameters. This enables the development of robust AI models for disease detection, such as early cancer diagnosis or cardiac anomalies, without violating privacy. In addition, cross-silo FL across diagnostic centers supports multi-institutional training, improving generalization across diverse patient populations. Integration of secure aggregation and encrypted communication ensures that adversarial actors cannot reconstruct sensitive imaging features, making FL a practical enabler for privacy-compliant medical imaging analytics [22].

16.6.3 Predictive analytics for chronic diseases

Chronic diseases such as diabetes, cardiovascular disorders, and respiratory illnesses require long-term monitoring and early prediction to enhance patient outcomes. Predictive analytics supported by federated learning allows IoT devices and healthcare institutions to collaboratively train models that forecast disease progression or patient relapse without centralizing sensitive clinical records. For example, FL enables personalized risk scoring models that adapt to patient-specific lifestyle and genetic data gathered through distributed sensors and electronic health records. The decentralized nature of FL ensures privacy while enhancing predictive accuracy across diverse populations, capturing regional variations in disease prevalence. Moreover, integrating FL with privacy-preserving mechanisms ensures strong safeguards against attacks, supporting regulatory compliance. These predictive insights guide timely interventions, reduce hospital readmissions, and lower overall healthcare costs, thereby advancing sustainable and patient-centered care [23].

16.6.4 Pandemic and epidemic management (COVID-19-like scenarios)

Pandemics such as COVID-19 have highlighted the urgent need for global collaboration in healthcare analytics while safeguarding sensitive patient and population data. Federated learning presents a promising solution by enabling multiple healthcare institutions, governments, and research centers to collaboratively train disease-spread and risk-prediction models. For example, hospitals across regions can contribute local data on infection trends, patient responses, and treatment outcomes without data sharing, ensuring regulatory compliance while improving predictive power for outbreak detection. IoT-based monitoring tools such as smart thermometers, mobile health apps, and wearable sensors further add real-time epidemiological data into FL models. Blockchain integration can additionally secure the aggregation process, ensuring transparency and trust among international stakeholders. Such applications demonstrate how FL supports rapid deployment of privacy-preserving analytics for crisis management, enabling preparedness and resilience during epidemic and pandemic events [24].

16.7 Conclusions and future directions

16.7.1 Summary

Federated learning (FL) has emerged as a transformative paradigm for addressing the dual imperatives of technological innovation and patient privacy in the digital healthcare era. By enabling decentralized training across IoT-enabled medical devices, hospitals, and research institutions, FL eliminates the need to centralize raw patient data, thus mitigating privacy risks and ensuring compliance with regulations such as HIPAA and GDPR. Its application spans diverse domains, including smart wearable devices, medical imaging, predictive analytics, and pandemic management, each benefiting from improved model accuracy, reduced data exposure, and enhanced scalability. Moreover, FL's capacity to optimize communication rounds, leverage hierarchical architectures such as fog-cloud models, and incorporate privacy-preserving mechanisms like differential privacy, homomorphic encryption, and secure multi-party computation, supports the long-term sustainability of healthcare infrastructures. This chapter highlights how FL provides the foundation for a secure, efficient, and responsible use of IoT in healthcare, offering a path toward patient-centric, data-driven medical innovation.

16.7.2 Roadmap for future IoT-based healthcare systems

The future of IoT-based healthcare systems will be defined by the integration of federated learning with advanced privacy-preserving techniques, sustainable deployment strategies, and scalable architectures. To achieve this vision, several key directions must be pursued. First, adaptive and energy-aware FL strategies are essential to extend the participation of resource-constrained IoT devices while maintaining strong model performance. Second, combining FL with blockchain will enable transparent and tamper-resistant aggregation mechanisms, fostering trust among diverse stakeholders in collaborative healthcare ecosystems. Third, next-generation cryptographic designs tailored for lightweight medical devices will ensure inclusivity while addressing IoT-specific security challenges. Finally, interdisciplinary collaboration between clinicians, data scientists, policymakers, and engineers is crucial to align technical solutions with medical ethics, usability, and patient empowerment. By following this roadmap, FL-driven IoT healthcare systems can evolve into sustainable, equitable, and globally adaptive infrastructures that not only protect sensitive patient data but also improve healthcare accessibility, efficiency, and outcomes on a large scale.

References

[1] M. Javaid, I.H. Khan, Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 pandemic, Journal of Oral Biology and Craniofacial Research 11 (2) (2021) 209–214.
[2] D.C. Nguyen, Q.-V. Pham, P.N. Pathirana, M. Ding, A. Seneviratne, Z. Lin, O. Dobre, W.-J. Hwang, Federated learning for smart healthcare: a survey, ACM Computing Surveys 55 (3) (2022) 1–37.
[3] O.A. AlJaberi, M. Hussain, P.R. Drake, A framework for measuring sustainability in healthcare systems, International Journal of Healthcare Management (2020).
[4] M. Ali, F. Naeem, M. Tariq, G. Kaddoum, Federated learning for privacy preservation in smart healthcare systems: a comprehensive survey, IEEE Journal of Biomedical and Health Informatics 27 (2) (2022) 778–789.
[5] H.S.G. Pussewalage, V.A. Oleshchuk, Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions, International Journal of Information Management 36 (6) (2016) 1161–1173.
[6] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, Y. Gao, A survey on federated learning, Knowledge-Based Systems 216 (2021) 106775.
[7] B. Pradhan, S. Bhattacharyya, K. Pal, IoT-based applications in healthcare devices, Journal of Healthcare Engineering 2021 (1) (2021) 6632599.
[8] S.R. Abbas, Z. Abbas, A. Zahir, S.W. Lee, Federated learning in smart healthcare: a comprehensive review on privacy, security, and predictive analytics with IoT integration, Healthcare 12 (2024) 2587, MDPI.
[9] J.B. Awotunde, R.G. Jimoh, S.O. Folorunso, E.A. Adeniyi, K.M. Abiodun, O.O. Banjo, Privacy and security concerns in IoT-based healthcare systems, in: The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care, Springer, 2021, pp. 105–134.
[10] L. Lyu, H. Yu, J. Zhao, Q. Yang, Threats to federated learning, in: Federated Learning: Privacy and Incentive, Springer, 2020, pp. 3–16.
[11] A. Said, A. Yahyaoui, T. Abdellatif, Hipaa and GDPR compliance in IoT healthcare systems, in: International Conference on Model and Data Engineering, Springer, 2023, pp. 198–209.
[12] C. Dwork, Differential privacy, in: International Colloquium on Automata, Languages, and Programming, Springer, 2006, pp. 1–12.
[13] A. Acar, H. Aksu, A.S. Uluagac, M. Conti, A survey on homomorphic encryption schemes: theory and implementation, ACM Computing Surveys 51 (4) (2018) 1–35.
[14] W. Du, M.J. Atallah, Secure multi-party computation problems and their applications: a review and open problems, in: Proceedings of the 2001 Workshop on New Security Paradigms, 2001, pp. 13–22.
[15] A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad, Z. Mushtaq, An energy-efficient data aggregation mechanism for IoT secured by blockchain, IEEE Access 10 (2022) 11404–11419.
[16] H.M.Z. Al Shebli, B.D. Beheshti, Light weight cryptography for resource constrained IoT devices, in: Proceedings of the Future Technologies Conference, Springer, 2018, pp. 196–204.
[17] Z. Ji, L. Chen, N. Zhao, Y. Chen, G. Wei, F.R. Yu, Computation offloading for edge-assisted federated learning, IEEE Transactions on Vehicular Technology 70 (9) (2021) 9330–9344.
[18] R. Maharaja, P. Iyer, Z. Ye, A hybrid fog-cloud approach for securing the Internet of Things, Cluster Computing 23 (2) (2020) 451–459.
[19] C. Huang, J. Huang, X. Liu, Cross-silo federated learning: challenges and opportunities, arXiv preprint, arXiv:2206.12949, 2022.
[20] M. Mendula, P. Bellavista, Energy-aware edge federated learning for enhanced reliability and sustainability, in: 2022 IEEE/ACM 7th Symposium on Edge Computing (SEC), IEEE, 2022, pp. 349–354.
[21] U. Hariharan, K. Rajkumar, T. Akilan, J. Jeyavel, Smart wearable devices for remote patient monitoring in Healthcare 4.0, in: Internet of Medical Things: Remote Healthcare Systems and Applications, Springer, 2021, pp. 117–135.
[22] S.S. Sandhu, H.T. Gorji, P. Tavakolian, K. Tavakolian, A. Akhbardeh, Medical imaging applications of federated learning, Diagnostics 13 (19) (2023) 3140.
[23] K. Deepika, S. Seema, Predictive analytics to prevent and control chronic diseases, in: 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), IEEE, 2016, pp. 381–386.
[24] N. Pathak, P.K. Deb, A. Mukherjee, S. Misra, IoT-to-the-rescue: a survey of IoT solutions for COVID-19-like pandemics, IEEE Internet of Things Journal 8 (17) (2021) 13145–13164.