Secure Healthcare Data Analytics for Early Disease Detection: Cybersecurity and Big Data Solutions

Dipanshi Verma, Mamta Ashwar, Aman Padariya, Shradha Shinde, Ramachandra P
Parul University, Vadodara, Gujarat, India
E-mail: 2405112110133@paruluniversity.ac.in, 240511070009@paruluniversity.ac.in, 2405112130023@paruluniversity.ac.in, 2405102070005@paruluniversity.ac.in, ramchandran.p34251@paruluniversity.ac.in

Keywords: Healthcare analytics, big data, cybersecurity, encryption, early disease detection, patient privacy, federated learning, blockchain

Received: April 22, 2026

The fusion of big data analytics and Cybersecurity has transformed the healthcare industry through technology-enabled methods to detect diseases early and achieve clinical improvement. The exponential growth of electronic health records (EHRs), wearable sensors, and Internet of Things (IoT)-based medical devices has created vast amounts of patient data available for analytics. This data can be used to identify early symptoms of a disease and inform evidence-based clinical decisions. However, increased dependence on digital technologies creates new challenges including data privacy risk; cyberattacks; and unpermitted access to data. This article looks at secure methods for healthcare data analytics leveraging big data technologies in conjunction with advanced cybersecurity methods, including encryption, blockchain, federated learning, and artificial intelligence (AI) models which help ensure patient data remain protected while providing predictive information. The findings outline the vital importance of ensuring innovation with protection of privacy and presents a broadly applicable framework for secure, scalable, and ethical analytics for healthcare.

Povzetek: Povezovanje analitike velikih podatkov in kibernetske varnosti omogoča varnejšo uporabo zdravstvenih podatkov za zgodnje odkrivanje bolezni in boljše klinično odločanje.

1 Introduction

The growing availability of digital data is reshaping the healthcare industry. Hospitals, labs, and wearables are producing large amounts of health- related data on an ongoing basis. If managed properly, this data can help improve patient care, allow for personalized treatment, and support the identification of diseases at an early stage. However, with increasing inter connectivity among healthcare systems, they are also more prone to cyberattacks. Healthcare systems are more prone to cyberattacks with, inter connectivity. In fact, hackers often target sensitive medical records, which can lead to data breaches and violation of privacy rights. In addition, being able to ensure compliance with various healthcare regulations such as HIPAA and GDPR adds another level of complexity. This paper explores opportunities for healthcare organizations to use big data analytics in a secure manner to assist in the early detection of disease. This paper discusses the combination of Cybersecurity tools such as encryption, blockchain, and access control practices together with analytic which are driven by AI in order to help providers.

1.2 The value of early detection of disease

Early detection can improve treatment options and help clinicians intervene before a condition becomes severe. This is particularly relevant to cancer, cardiovascular disease, diabetes, and neurological secure patient information and provide critical information that can be lifesaving.

1.1 Digital transformation in healthcare

Healthcare has changed quickly as hospitals have adopted EHRs, medical imaging, wearable devices, genomics, telemedicine, and IoMT systems. These sources produce data in different formats and at very different rates. When combined carefully, they can support risk prediction, continuous monitoring, and earlier clinical intervention.

Cloud platforms now make it possible to store and process large volumes of health data, while AI and machine learning can identify patterns in images, physiological signals, and patient records. Wearables and connected devices add another useful feature: they can capture changes over time rather than only during a clinical visit.

The value of these technologies depends on how the data are collected, shared, and protected. A model trained on inconsistent data may not generalize well, and moving sensitive records between organizations increases exposure. Secure analytics therefore has to address data quality and data movement as well as model performance.

disorders, where changes may appear before serious complications develop.

Machine-learning models can use imaging, EHR data, and physiological signals to identify patterns associated with disease risk. For example, CNN-based systems have been studied for lung-nodule and retinal-abnormality detection, while continuous ECG and wearable measurements can support cardiovascular monitoring.

These systems should still be treated as decision-support tools. A useful early-warning model needs more than a high accuracy score; calibration, false-alert rates, subgroup performance, and clinical interpretability also affect whether clinicians can use its output safely.

1.3 Cybersecurity challenges in digital health

The same connectivity that makes healthcare analytics useful also expands the attack surface. EHRs contain highly sensitive information, while cloud services, APIs, IoMT devices, remote access, and third-party software create additional points of exposure.

Healthcare organizations face ransomware, phishing, data manipulation, denial-of-service attacks, weak authentication, unpatched systems, insider misuse, and supply-chain vulnerabilities. Machine-learning systems add risks such as model inversion, membership inference, and data poisoning. A compromised device or corrupted data source can affect both privacy and the reliability of a clinical prediction.

The security problem is also tied to governance. HIPAA, GDPR, and related frameworks place requirements on access, privacy, accountability, and handling of health information. In practice, these requirements have to be reflected in identity management, data minimization, audit trails, consent controls, monitoring, and incident response.

Table 1: Cybersecurity challenges in digital health

Risk Category	Specific Threat	Impact on Healthcare Systems
Technical Vulnerabilities	Medical IoT Firmware Attacks	Can alter device functionality, making them unsafe for patients .
	API Exploitation Risks	Allows unauthorized gathering or modification of sensitive health data across linked systems .
	Misconfigured Cloud Storage	Exposes massive amounts of unencrypted patient records to the public internet .
Adversarial Tactics	AI Model Inversion Attacks	Attackers recreate sensitive patient data by exploiting vulnerabilities in diagnostic AI models .
	Data Poisoning Attacks	Destroys the trustworthiness of AI-informed predictions or medical research findings .
Human & Operational	Shadow IT Usage	Creates uncontrolled data flows and increases the risk of regulatory non-compliance .
	Insider Privilege Escalation	Employees can abuse legitimate access to modify data beyond their authorized scope .

1.4 Research objectives

This study examines how healthcare analytics and cybersecurity can be combined to support early disease detection without treating patient privacy as a separate concern.

The objectives are to:

1. Examine the use of big-data analytics and AI for early disease detection;
2. identify cybersecurity threats affecting healthcare data and analytics systems;
3. Compare privacy and security approaches, including federated learning, homomorphic encryption, blockchain, secure multi-party computation, and anomaly detection; and
4. Develop a reference framework that connects analytics with privacy, security, clinical oversight, and governance.

The paper is a structured technical review and framework proposal. It does not claim to introduce a new prediction algorithm or report a new clinical experiment.

2 Literature review and methodology

The review uses a structured technical search and evidence-synthesis approach. It is not presented as a PRISMA systematic review or meta-analysis because the selected studies use different diseases, datasets, models, privacy definitions, and evaluation procedures. Instead, the review applies consistent selection and extraction criteria so that the approaches can be compared on common technical dimensions.

The search covered four areas: healthcare analytics and early detection; privacy-preserving machine learning; healthcare cybersecurity and IoMT; and governance and regulation. Search terms combined concepts such as healthcare, federated learning, privacy-preserving AI, homomorphic encryption, blockchain, IoMT security, model inversion, and explainable AI. Recent peer-reviewed work, especially from 2021–2026, was prioritized. Older sources were retained where they provided foundational methods.

Sources were included when they directly addressed healthcare analytics, clinical AI, privacy-preserving

computation, cybersecurity, or health-data governance and provided technical, empirical, or regulatory evidence. General consumer-privacy, smart-home, or unrelated IoT papers were excluded when they did not contribute directly to secure healthcare analytics.

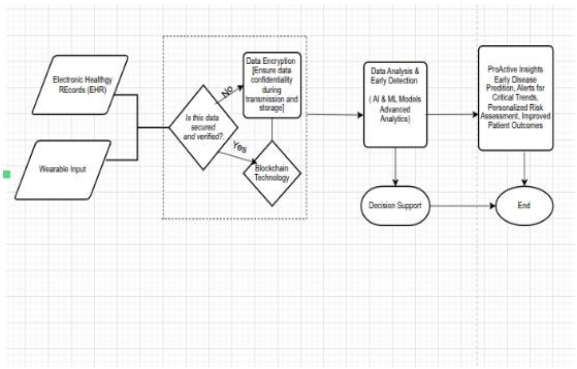

Figure 1: Secure healthcare analytics workflow integrating healthcare data, security controls, and predictive analysis.

For each source, the review recorded the application area, data type, dataset or setting, analytical method, security mechanism, threat addressed, evaluation measures, reported results, and limitations. The evidence was then grouped into six comparison dimensions: predictive utility, privacy, security, efficiency, clinical usability, and governance.

The literature shows that no single technology solves the security problem. Federated learning reduces the need to move raw data, but model updates can still leak information. Differential privacy offers a formal privacy guarantee but can reduce utility. Homomorphic encryption and secure multi-party computation protect computations at higher computational cost. Blockchain can improve provenance and auditability, while zero-trust access and anomaly detection address operational threats.

Recent healthcare analytics research also shows the importance of multimodal data. EHR variables, imaging, laboratory results, genomics, and wearable signals can provide complementary information, but differences in data quality and site-specific populations can affect model performance. External validation and calibration are therefore important when models are moved between institutions.

The state of the art can be organized into seven practical layers: data locality, privacy mechanisms, security controls, integrity and provenance, analytics, clinical trust, and governance. This classification makes it easier to identify what a method actually protects instead of treating all secure-analytics technologies as interchangeable.

A comparison of the reviewed work shows that many studies optimize one part of the system—usually accuracy, privacy, or security—without evaluating the complete pipeline. This is the main gap addressed by the framework proposed in this paper.

Table 2: Comparison of secure healthcare analytics approaches

Approach	Healthcare application / data	Security or privacy mechanism	Typical evaluation measures	Main advantage	Main limitation
Federated Learning (FL)	EHRs, medical imaging, ECG, wearable data	Raw data remain at participating institutions; model updates are exchanged	AUROC, AUPRC, accuracy, communication cost	Enables multi-institution learning without centralizing raw records	Model updates can still leak information; affected by data heterogeneity
Differential Privacy (DP)	EHR prediction, medical imaging, statistical analysis	Noise is added to model updates or outputs	Accuracy, F1-score, AUROC, privacy budget (ε, δ)	Provides a formal privacy guarantee	Stronger privacy can reduce model utility
Homomorphic Encryption (HE)	Encrypted clinical data and privacy-preserving inference	Computation is performed on encrypted data	Accuracy, inference/training time, computational overhead	Sensitive data remain encrypted during computation	High computational and latency overhead
Secure Multi-Party Computation (SMPC)	Multi-hospital collaborative analytics	Joint computation without revealing individual inputs	Accuracy, communication rounds, computation time	Allows joint analysis without exposing raw inputs	Communication and computation can become expensive
Blockchain	EHR sharing, consent, audit logs, data provenance	Tamper-evident distributed ledger and smart contracts	Transaction latency, throughput, storage, interoperability	Improves traceability and auditability	Scalability and integration with existing healthcare systems remain difficult
IoMT security / anomaly detection	ECG, wearable sensors, medical devices	Device authentication, network monitoring, anomaly detection	Detection rate, precision, recall, false-positive rate, latency	Supports continuous monitoring and attack detection	False alarms and device/resource constraints
Zero-Trust Architecture	Hospital networks, APIs, cloud and IoMT systems	Continuous authentication, authorization, least privilege	Unauthorized-access rate, detection time, policy violations	Reduces implicit trust between users and devices	Requires significant identity and infrastructure management
Explainable AI	Clinical decision support,	Explanation of model	Accuracy, calibratio	Helps clinicians understan	Explanations may not

(XAI)	imaging, diagnosis	features or predictions	n, explanation fidelity, clinician assessment	d model outputs	always be clinically reliable or validated

The framework connects data preparation, privacy-preserving learning, cybersecurity monitoring, audit controls, clinical decision support, and governance in one workflow.

3 Challenges in secure healthcare analytics

The main challenges are not limited to data security. Healthcare analytics also has to deal with inconsistent data formats, fragmented records, limited computing resources, regulatory differences, model attacks, interoperability problems, human error, and the difficulty of integrating modern tools with legacy hospital systems.

Data inconsistencies arise because EHRs, clinical notes, imaging, genomics, and wearable streams use different formats and have different levels of completeness. Fragmentation makes it difficult to build a reliable model across hospitals, while encryption and federated learning can increase computation and communication requirements.

Compliance adds another layer of work because privacy and data-sharing rules differ between jurisdictions. At the same time, poisoned data and adversarial inputs can affect model reliability, while black-box predictions can make clinical accountability harder.

Legacy systems and limited staff training remain practical barriers. Strong technical controls cannot compensate for weak credentials, phishing susceptibility, poor device maintenance, or unclear operational responsibilities. These issues need to be considered when evaluating any secure analytics architecture.

Table 3: Mapping of healthcare cybersecurity threats to technical controls

Threat	Affected component	Potential consequence	Recommended control
Ransomware	EHR, hospital servers, cloud infrastructure	Loss of access to clinical systems and disruption of care	Network segmentation, MFA, backups, endpoint monitoring, incident response
Medical IoMT compromise	Wearables, sensors, medical devices	Manipulated measurements or unauthorized access	Device authentication, secure firmware updates, network isolation, anomaly detection
API exploitation	EHR APIs, cloud services, third-party integrations	Unauthorized data access or modification	API authentication, authorization, rate limiting, encryption, logging
Model inversion	AI/ML models	Reconstruction of sensitive patient information	Differential privacy, secure model access, output restrictions
Membership inference	Trained AI models	Disclosure of whether a patient contributed to training data	Differential privacy, regularization, privacy testing
Data poisoning	Training datasets / federated updates	Reduced model reliability or manipulated predictions	Data validation, robust aggregation, anomaly detection
Insider privilege escalation	Hospital staff and administrators	Unauthorized modification or disclosure of records	RBAC, least privilege, MFA, audit logs
Cloud misconfiguration	Cloud storage and analytics platforms	Exposure of large volumes of patient data	Encryption, configuration monitoring, access policies, security audits
Phishing / credential theft	Users and administrators	Unauthorized account access	MFA, security training, phishing detection
Weak interoperability controls	EHR and external systems	Data leakage, inconsistent records, integration failures	Standardized APIs, access policies, provenance tracking

4 Cases and frameworks

4.1 Healthcare data analytics

Healthcare analytics combines structured EHR variables with imaging, laboratory results, clinical notes, genomic information, and wearable measurements. The main benefit for early detection is the ability to identify patterns across several data types. The main limitation is that performance can change when the model is applied to another hospital or patient population.

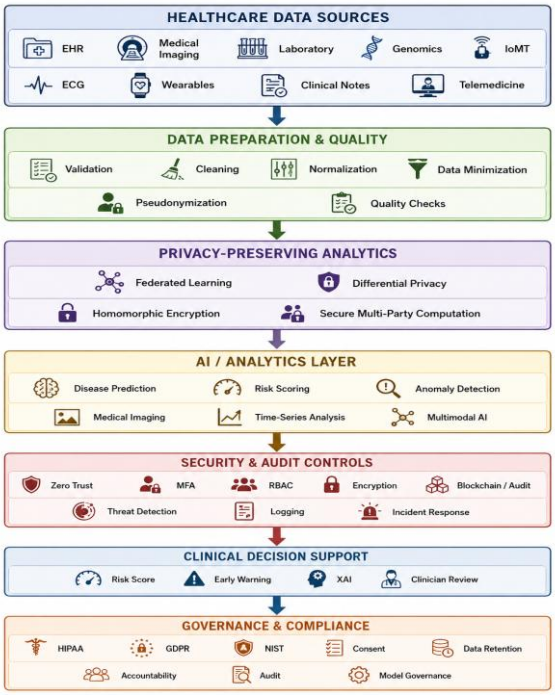

Figure 2: Proposed secure healthcare analytics architecture for early disease detection.

4.2 Federated deep learning for cancer Detection

A consortium of hospitals worked together in a federated deep learning project to identify lung cancer from CT images while maintaining decentralized datasets. Each site trained its respective model and shared only encrypted model parameters.While the collaboration among hospital sites provided evidence that federated deep learning could identify lung cancer from CT images without the need for centralized data. Each of the hospitals obtained a model for lung cancer detection, sharing only encrypted model weights while maintaining privacy. The model, developed in a federated learning approach, achieved diagnostic accuracy similar to using an AI that required centralizing medical data for analysis, demonstrating feasibility for doing health informatics research that prioritized privacy.

4.3 Remote cardiovascular monitoring

IoMT devices can stream ECG and other physiological measurements to analytics services for continuous monitoring. Anomaly detection can flag unusual patterns such as arrhythmias, while encryption protects data during transfer. Homomorphic encryption can provide additional confidentiality during selected computations, although its computational cost may limit real-time use. A practical deployment would also require device authentication, secure updates, access control, and monitoring.

4.4 Blockchain for data integrity

Blockchain is most useful here as an audit and provenance mechanism. Patient data can remain in conventional clinical storage while hashes, access events, consent changes, or record updates are written to a permissioned ledger. This makes later changes easier to detect and provides a shared audit trail across participating organizations. It does not, by itself, solve data-quality, interoperability, or scalability problems.

4.5 Secure multi-modal data analytics

Combining EHRs, imaging, genomics, and wearable data can improve the information available to an early-detection model. The security challenge is that these sources have different sensitivity levels and often remain at different institutions. Privacy-preserving learning can allow collaboration without moving all raw data, while encryption and access controls protect the data that must be exchanged. The literature supports the value of multimodal analysis, but the exact benefit depends on data quality and external validation.

4.6 Cloud-based secure analytics framework

To conduct disease prediction and population health assessment, healthcare organizations employed encrypted cloud analytics while maintaining compliance with GDPR and HIPAA.Hospitals are using cloud platforms with end-to-end encryption to meet the demand for scalable storage and analysis of data. Homomorphic encryption allows computations to be executed on encrypted data without revealing information. Role-based access control permits only authorized personnel to query or modify the data and/or the records. Real-time analytics dashboards assist clinicians in monitoring patient health virtually. Cloud compliance features allow the cloud to meet GDPR and HIPAA requirements. Multi-factor authentication helps prevent unauthorized access and enhances the overall cloud security posture.

4.7 Pandemic data collaboration

Large-scale public-health collaboration requires rapid data exchange while preserving patient privacy. Blockchain can provide a shared audit trail for verified events and permissions, while IoT and spatial-temporal data can support outbreak monitoring. The main design question is not whether the ledger is immutable, but how data quality, consent, access rights, and cross-border governance are handled during a fast-moving public-health event.

4.8 Remote rehabilitation framework

IoMT devices can collect mobility, heart-rate, and exercise data after surgery and transmit them to clinicians through encrypted channels. Analytics can help identify recovery problems and support remote therapy adjustments. For deployment, device authentication, secure communication, consent, and alert management are as important as the predictive model because false or excessive alerts can affect patient adherence and clinical workload.

4.9 AI-based sepsis detection and alert system

Sepsis models can use continuously updated vital signs and EHR information to generate risk scores before severe deterioration occurs. Encryption protects data in transit, while access controls restrict who can view or act on the alerts. Clinical validation remains essential because a high false-alert rate can overwhelm staff, and model performance may change across hospitals. The system should therefore be evaluated using calibration, sensitivity, specificity, alert burden, and external validation rather than accuracy alone.

4.10 Secure telemedicine and virtual Care-framework

The rise of telehealth calls for an advanced digital infrastructure to secure patient consultations, diagnostic results, and live video communications. When well built, telehealth infrastructure guarantees encryption, authentication and aligns with global privacy regulations so medical services are delivered remotely safely and securely for patients and providers. End-to-end encryption secures audio, video, and data exchanged between clinician and patient when participating in a teleconsultation. Multi-factor authentication (MFA) assures that only validated users can access virtual appointments and associated records. AI chatbots may assist with scheduling appointments and provide encrypted communications logs. Cohesion with EHR systems provides for seamless transfer of data pertaining to new prescriptions, test results, and clinical notes. Cloud-based servers with encryption that adheres to HIPAA regulations protect patient data from external threats. Intrusion detection tools monitor network activity unauthorized access. Continuously and restrict All of these are essential to provide trust, reliability, and anonymity for medical transactions in a digital environment during public health emergencies or in rural health systems.

Table 4. Comparison of literature-derived healthcare analytics cases

Case / Application	Data type	Analytics method	Security / privacy mechanism	Evaluation focus	Main limitation
Early disease prediction	EHR, laboratory and clinical data	ML/DL risk prediction	Access control, encryption, privacy-preserving learning	AUROC, AUPRC, sensitivity, specificity, calibration	Performance may change across hospitals
Federated cancer detection	CT / medical imaging	Federated deep learning	Federated learning, encrypted model updates	Accuracy, AUROC, communication cost	Data heterogeneity and communication overhead
Remote cardiovascular monitoring	ECG, wearable and IoMT data	Time-series analysis, anomaly detection	Encryption, device authentication	Detection rate, sensitivity, false alarms, latency	Resource constraints and alert fatigue
Blockchain health-data sharing	EHR and clinical records	Data sharing / provenance	Permissioned blockchain, smart contracts	Throughput, latency, auditability	Scalability and interoperability
Multimodal analytics	EHR, imaging, genomics, wearable data	Multimodal ML	Federated learning, encryption, access control	Predictive performance and generalization	Data alignment and quality
Cloud-based analytics	EHR and population-health data	Cloud ML / analytics	Encryption, RBAC, MFA	Accuracy, latency, access-control events	Cloud dependency and configuration risk
Pandemic/public-health collaboration	Epidemiological, IoT and spatial-temporal data	Predictive and surveillance analytics	Blockchain, access control, privacy mechanisms	Timeliness, data integrity, privacy	Cross-border governance
Remote rehabilitation	Wearable / IoMT data	Monitoring and anomaly detection	Encryption, authentication, consent management	Detection accuracy, latency, alert burden	Device reliability and clinical workload
Sepsis detection	EHR and physiological data	Risk prediction / early warning	Encryption, RBAC, audit logging	Sensitivity, specificity, calibration, alert burden	False alerts and external validation
Telemedicine	Clinical records, video and consultation data	AI-assisted decision support	End-to-end encryption, MFA, intrusion detection	Security events, latency, usability	Integration with EHR and legacy systems

Note : The cases summarized in Table 4 are literature-derived application scenarios. They are not experiments conducted by the authors. Quantitative results are reported only where the cited source provides them.

Table 5: Quantitative evidence reported in selected healthcare analytics studies

Study / approach	Dataset / setting	Task	Method	Reported metric	Reported result
Federated healthcare studies	Multiple healthcare datasets	Prediction / inference	Federated learning	AUROC	Comparable to centralized models in several evaluated tasks
MIMIC-III federated prediction	MIMIC-III	In-hospital mortality	FedAvg / federated learning	AUROC	FedAvg ≈ 0.90 in one reported evaluation
Multi-site medical AI	Multi-institution clinical data	Prediction	Federated learning	AUC	Comparable to centralized approaches in several studies

Blockchain healthcare systems	EHR / clinical data sharing	Secure data exchange	Blockchain	Latency, throughput, scalability	Results vary substantially by platform and deployment
XAI healthcare studies	Imaging / diagnosis	Clinical interpretation	SHAP, LIME, Grad-CAM and related methods	Interpretability / clinician evaluation	Evidence remains heterogeneous; standardized clinical evaluation is limited

5 Future research directions

Future work in secure healthcare analytics is moving toward more distributed, privacy-aware, and continuously monitored systems. Federated learning combined with transfer learning may help institutions adapt shared models to local populations without centralizing patient records. Quantum-resistant cryptography is also becoming relevant for long-term protection of sensitive health information.

Other areas deserve practical evaluation rather than only conceptual discussion. These include explainable AI for clinical decision support, interoperability between permissioned ledgers and existing health systems, edge computing for wearable data, privacy-preserving analytics, and AI-assisted threat detection.

The direction of this work should remain evidence-based. New techniques need to be tested for their effect on accuracy, privacy, latency, energy use, security, and clinical workflow. International data-sharing standards and clearer governance will also be needed for multi-site and cross-border research.

6 Discussion and conclusion

This review examined how healthcare analytics can support early disease detection while addressing the security and privacy risks created by increasingly connected health systems. The literature does not support treating one technology as a complete solution. Federated learning can reduce raw-data movement, but model updates may still leak information. Differential privacy can provide formal protection at the cost of some utility. Homomorphic encryption and secure multi-party computation protect selected computations but increase computational overhead. Blockchain can strengthen auditability, while zero-trust access and anomaly detection address operational security.

The proposed framework brings these controls together across the healthcare data lifecycle, from data acquisition and preparation to privacy-preserving analytics, security monitoring, audit, clinical decision support, and governance. It is a reference architecture, not a clinically validated system, and the quantitative examples in this paper come from published studies.

The main limitation is the lack of a common empirical benchmark across the reviewed approaches. Future work should evaluate complete systems across multiple institutions using the same measures for predictive performance, privacy leakage, communication cost, latency, calibration, fairness, security resilience, and clinical usability.

7 Limitations and future scope

The next stage of this work should focus on empirical validation. Multi-site studies should test secure analytics on real clinical tasks and report predictive performance together with privacy, communication, latency, calibration, fairness, and security measures.

Priority areas include federated and multimodal learning, adaptive differential privacy, secure aggregation, privacy-preserving inference, IoMT threat detection, explainable clinical AI, interoperable consent and audit systems, and integration with legacy hospital infrastructure.

Pilot deployments should also examine the human side of the system. Clinician workload, alert fatigue, usability, training needs, and the handling of model errors are important parts of a secure clinical workflow. Where patient data cannot be released, researchers should provide synthetic datasets, configuration files, preprocessing steps, and evaluation scripts where possible so that results can be reproduced.

Governance should be built into these pilots from the beginning. Consent, access rights, data retention, incident response, model accountability, and cross-border data use should be defined alongside the technical architecture.

8 References

[1] S. S. Mahadik, P. M. Pawar, R. Muthalagu, N. R. Prasad,S.-K. Hawkins, and D. Stripelis (2024). Digital Privacy in Healthcare: State-of-the-Art and Future Vision. IEEE Access, vol. 12, pp. 84273– 84291

[2] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, Lorrie Faith Cranor (2022). An informative security and privacy 'nutrition' label for Internet of Things devices. IEEE Security & Privacy, vol. 20, no. 2. pp. 12–22.

[3] Duha Ibdah, Nada Lachtar, Satya Meenakshi Raparthi, Anys Bacha (2021). Why should I read the privacy policy, I just need the service: A study on attitudes and perceptions toward privacy policies.IEEE Access, vol. 9. pp. 166465–166487.

[4] Bart P. Knijnenburg (2017). Privacy? I can't even!Making a case for user-tailored privacy," IEEE Security & Privacy. vol. 15, no. 4. pp 62-67.

[5] M.A.Ahmadon, N.Napp, S.Rao, C.Silva, M. Lizar, and C. Gorog (2025).Digital privacy: Trends, challenges, and the future. IT Professional, vol. 27, no. 3.pp. 69–77.

[6] Ann Cavoukian (2020). Understanding how to implement privacy by design, one step at a time. IEEE Consumer Electronics Magazine, vol. 9,
no. 2. pp. 34–42.

[7] Argyri Pattakou, Aikaterini-Georgia Mavroeidi, Vasiliki Diamantopoulou, Christos Kalloniatis, Stefanos Gritzalis (2018). Towards the design of usable privacy by design methodologies. In Proc. 5th Int. Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE) pp. 1–8.

[8] Mahsa Keshavarz and Mohd Anwar (2018). Towards improving privacy control for smart homes: A privacy decision framework. In Proc. 16th Annual Conf. on Privacy, Security and Trust (PST). pp. 1–8.

[9] Jie Xu, Benjamin S. Glicksberg, Chang Su, Peter Walker, Jiang Bian & Fei Wang (2021). Federated Learning for Healthcare Informatics. Journal of Healthcare Informatics Research, vol. 5. pp. 1–19.

[10] H. Taherdoost (2023). "The role of blockchain in medical data sharing," Cryptography, vol. 7, no. 3, p. 36.

[11] J. Suji Priya, R. Thirumalaisamy, S. Aruna, and R. Sarulatha (2024). "Role of Big Data, AI, and Machine Learning in Decisions for Disease Diagnosis and Treatment," in Computational Approaches in Biomaterials and Biomedical Engineering Applications, 1st ed. Boca Raton, FL, USA: CRC Press.

[12] Ting et al., "Federated machine learning in healthcare: A systematic review on clinical applications and technical architecture," The Lancet Digital Health / eClinicalMedicine family, 2024, DOI: 10.1016/j.xcrm.2024.101419.

[13] "Privacy preservation for federated learning in health care," 2024, DOI: 10.1016/j.patter.2024.100974.

[14] Fonsêca et al., "Blockchain in Health Information Systems: A Systematic Review," International Journal of Environmental Research and Public Health, 2024.

[15] Svandova and Smutny, "Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review," Journal of Multidisciplinary Healthcare, 2024, pp. 2281–2301. DOI: 10.2147/JMDH.S459987.