Advances in Anomaly Detection in Healthcare Using Federated Machine Learning

Shivangi Valand[1]* · Umesh Kumar[2] · Yatin Shukla[3]

[1,2,3] Department of Computer Science, Faculty of Engineering and Technology
Parul University, Waghodia, Vadodara, Gujarat, India
*shivangi.valand35391@paruluniversity.ac.in,
yatinkumar.shukla18611@paruluniversity.ac.in

Abstract. In the field of healthcare, anomaly detection is essential in identifying the abnormal tendencies of patient records, function and/or medical procedures of a device. Electronic health records (EHRs), wearable sensors, and Internet of Medical Things (IoMT) devices are big and have created certain challenges in ensuring data privacy and regulatory compliance. The traditional centralized systems of learning are limited by the data sharing restriction and the data security issues. The Federated Machine Learning (FML) eliminates all these drawbacks by allowing model training in the presence of distributed sources, yet without a direct exchange of patient data. In this review, FML-based systems of detection of anomalies in healthcare are thoroughly analyzed in terms of their architecture, mechanisms of privacy protection, and use scenarios. The uniqueness of the given work is in the combination of the experience of two spheres federated learning and healthcare anomaly detection, where privacy-sensitive, distributed analytics is seen as a single unit. Moreover, the main issues of heterogeneity of data, the efficiency of communication and security of the model are addressed with the prospects of the future research. The goal is to influence the creation of secure and scalable healthcare solutions that have the ability to identify anomalies in an efficient manner without compromising the privacy of data.

Keywords: Anomaly Detection, Cyber Security, Edge Intelligence, Federated Learning, Internet of Medical Things (IoMT) Healthcare, Privacy Preservation.

1 Introduction

The healthcare industry produces large volumes of disseminated data in the form of hospitals, wearable, and intelligent sensors [1], [2]. Such heterogeneous data analysis and treatment is critical in detecting abnormalities, which may signify medical errors, computer breach or disease progression. This is the biggest drawback of the conventional centralized machine learning models, however. They are likely to undermine privacy needs, contribute to the latency, and disrupt the regulatory guidelines such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) [3].

S. Bhalerao et al. (eds.), *Proceedings of the 2nd International Conference on Recent Advancement and Modernization in Sustainable Intelligent Technologies & Applications (RAMSITA-2026)*, Advances in Intelligent Systems Research 207,
https://doi.org/10.2991/978-94-6239-678-4_8

The federated learning (FL) has been a topical paradigm that enables various healthcare organizations to learn models cooperatively without necessarily leaving information centrally dispersed [4]. This decentralization platform enhances privacy, reduces the cost of data transfer and in addition, makes sure that data regulations are not breached [5]. The general architecture of the anomaly detection in healthcare systems is illustrated in Fig. 1 that reveals that the data collected by the sensors, hospital databases, and sensors are processed in question with the assistance of the anomaly detection modules and decision-making layers which allow the clinical insights to be tracked [6].

FML has been demonstrated to be helpful in enhancing distributed anomaly detection, particularly in interconnected medical devices, Internet of things (IoT) networks, and electronic health record (EHR) [7][8]. These efforts illustrate how FML can balance privacy data and its capacity to analyze the data in an analytical manner in developing the foundation of higher privacy-sensitive healthcare analytics [9][10]. The principal purpose of this review is to summarize the already existing literature, describe the potential drawbacks of the current methodology, and demonstrate the future perspectives of the further development of the idea of anomaly detection with the assistance of federated machine learning in the healthcare environment.

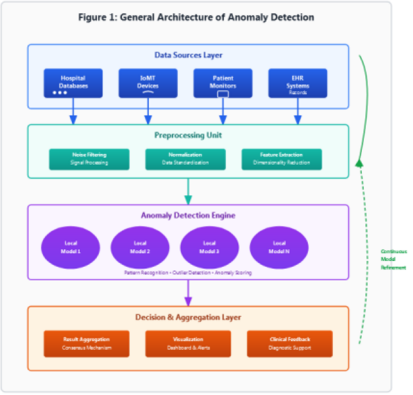

Fig.1 General architecture of anomaly detection in healthcare systems

The figure 1 represents data collection from multiple sources, preprocessing for quality enhancement, distributed anomaly detection modules at the edge, and centralized aggregation for decision support in clinical environments.

2 Literature Review

2.1 Traditional Learning using Machines

Federated and deep learning paradigms did not exist before other conventional machine learning techniques were employed to perform anomaly detection in

healthcare. Some of the techniques, which are employed to detect anomalies in medical signals, EHR data, and IoMT outputs, include SVMs, isolation forest, K-means clustering, and principal component analysis (PCA) [17] [18]. Most of the models are often centered on centralized data collection in as far as training is concerned although the models can achieve a fairly good level of detection accuracy. This type of centralization is not only a factor in the threat of data breaches, but also leads to inability to scale in situations where it is applied in different healthcare institutions [19].

Table 1. Summary of existing anomaly detection techniques in healthcare

Dataset/Domain	Methodology	Key Findings	Limitations
Healthcare IoT sensor data	Random forest and SVM models	Achieved early anomaly detection in real-time medical monitoring	Dependent on centralized data storage
IoT-based patient monitoring	Hybrid CNN–LSTM model	Improved detection accuracy for temporal anomalies	High computational cost at the server
Medical device logs	Auto encoder-based anomaly detection	Effective in identifying abnormal device behavior	Limited generalization to unseen devices
Mobile Edge healthcare network	Hybrid deep learning with privacy modules	Enhanced security and anomaly detection accuracy	Privacy risk during data aggregation

Traditional anomaly detection techniques used in healthcare are summarized in **Table 1**.

These traditional methods imply the importance of anomaly detection in the sphere of healthcare and reflect the implicit limitations of this method with data centralization, privacy, and interoperability. Such concerns prompt the necessity to integrate federated learning models to share and identify anomalies in the modern healthcare systems in a safe way. I. Federated principles of learning. A. Federated Learning Architecture. Federated learning (FL) is a decentralized machine learning framework, where numerous clients (e.g., hospitals or edge devices) collaboratively train a global model, although retaining raw data in a localized (e.g. hospital) setting [24][25]. Each client trains a local model using its own data and after every few steps, the model is updated (to a central server) with weights, or gradients. All these updates are added on the server, typically through federated learning methods like Federated Averaging (FedAvg), to form a fined tuned global model, and re-distilled back to all clients to proceed with training. Then, this process is repeated until the model converges, and federated learning on distributed datasets can be performed without any information sharing, as different institutions with dissimilar data (EHRs, wearable, and so forth) are given to them and trained separately. Fig. 2 shows the federated learning model applied to healthcare, where various institutions with different sources of data (EHRs and wearable, and so on) are linked and trained individually. These models are communicating their updates to a central server that amalgamates them in order to store a shared global model. Arrows depict how the

communication process is iterated and the framework accentuates how the concept of privacy is assumed since raw data are never transmitted outside the local institutions [26].

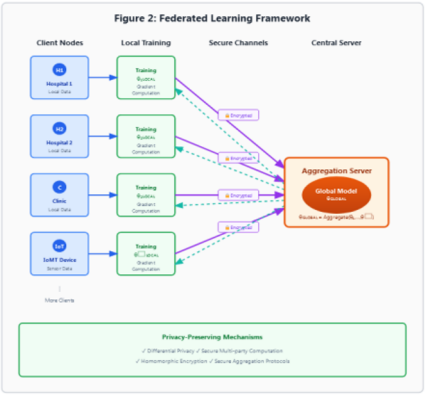

Fig.2 Federated learning framework for healthcare data across multiple institutions

The figure 2 contains four components arranged horizontally representing federated learning framework.

2.2 Privacy and Security Mechanisms

Data privacy in FL is also a priority especially in the health sector where the information of the patients is very sensitive. There are techniques, such as differential privacy, and others, which add noise to model updates so that it is no longer possible to reconstruct the original data [27]. Homomorphism encryption enables the computation on encrypted information such that the aggregation of the server does not demonstrate client information [28]. One can ensure that the individual model updates are aggregated without any personal information being exposed with the help of secure aggregation protocols. In addition, the updates of the models are recorded in a verifiably cryptographic manner with block chain-based verification systems, and client information can be inferred using gradients obfuscation to perform inference attacks [29][30]. All this enhances the degree of trust and confidence to federated anomaly detection systems.

2.3 Healthcare Federated Learning Problems

FL is not simple to implement in the healthcare. In various institutions, the data are heterogeneous whereby the data formats, the sampling rate, and the measurement units are varied resulting to the problem of convergence of models [31]. Unless treated accordingly, there are possibilities of bias in global models because of non-IID (non-independent and identically distributed) data between clients. Communication bottlenecks may delay the model aggregation, especially in resource-constrained networks of IoMT. Besides that, equality among institutions is

necessary and in this sense the models ought to apply equally to all clients regardless of size and quality of their data [32] -[34].

Table 2. Overview of federated learning algorithms applied in healthcare domains

Algorithm	Key Features	Advantages	Limitations
FedAvg	Standard aggregation of client updates	Simple and efficient, widely adopted	Sensitive to non-IID data
FedProx	Modifies local objective to improve robustness	Handles client heterogeneity better	Slower convergence than FedAvg
Hierarchical FL	Aggregation at multiple levels (local, regional, global)	Scalable for large networks	Complex communication management
Block chain-Enhanced FL	Records model updates securely on a block chain	Tamper-proof, improves trust	Increased computational and storage overhead

Table 2. provides a summary of comparative overview of federated learning algorithms in healthcare with a focus on their methodology, benefits, and limitations.

These algorithms demonstrate the ways of adaptation of FL strategies to various healthcare applications. Although all the approaches have their advantages in privacy, scalability or robustness, they also have trade-offs like higher complexity or reduced convergence that need to be well considered to be used in practice. The design of architecture, privacy mechanisms and the choice of algorithms are what make the federated anomaly detection an effective technique in healthcare systems. Although existing research show that federated learning is helpful for detecting anomalies in healthcare, there are some drawbacks. Most techniques have issues with non-IID data distribution, communication overhead, limited scalability, and explainability in therapeutic settings. Furthermore, a coherent approach that integrates architectures, privacy measures, anomaly detection models, and open research problems is still lacking. This highlights the necessity for a thorough examination of federated anomaly detection strategies in healthcare systems.

3 Anomaly Detection in Healthcare

3.1 Definition and Importance

The detection of anomalies in healthcare is the process of identifying the abnormalities in data that are not common patterns of physiological, clinical or operational behavior. Such anomalies may give the first signs of disease, device failure, damaging data or even cybernetic attacks in the medical networks [11][12]. Anomaly detection in clinical practices finds use to detect abnormal heart rates, irregular glucose readings and unexpected imaging results that could indicate a serious health problem. Its operation wise gives stability in hospital systems, which does not interfere with medical processes. Therefore, the appropriate detection of anomalies is the contributor to patient safety and the integrity of the healthcare system, which is the foundation of intelligent and proactive healthcare management.

3.2 Types of Anomalies

There are three groups of healthcare abnormalities. The clinical anomalies may be those that entail a change in the vital signs, radiographic scans or laboratory tests that are much differentiated with the usual medical baselines [13]. As an example, any acute worsening of health may be noted by uncharacteristic alterations of ECG waves or blood oxygen level. The problem of operational anomalies arises due to the presence of anomalies in the hospital information systems due to equipment failures, problems of data transmission, or workflow problems [14]. Identification of these abnormalities may be helpful in the effectiveness of the system and ensuring the accuracy of patient information. Finally, the aberrant behaviors are detected in the patient-generated or wearable device data where strange movement or sleep or medication patterns may serve as evidence of health risks or non-adherence of the patient [15][16].

4 Anomaly Detection Using Federated Learning

4.1 Integration of FL with Anomaly Detection Models

Federated learning (FL) is compatible with other models of anomaly detection to study distributed healthcare data without patient privacy invasion. Convolutional neural networks (CNNs), recurrent neural networks (RNNs), auto encoders, and generative adversarial networks (GANs) are deep learning models that have found extensive application [37][38]. CNNs can be useful in identifying spatial abnormalities of medical data, but RNNs and LSTMs are applicable to sequential data, including vital signs and time-series sensor measurements. Auto encoders are utilized to detect anomalies without any supervision through learning compact representations and detecting anomalies in the reconstruction error. More recent hybrid frameworks, including CNN-LSTM and transformer-based models, have been shown to be more accurate in learning more complex temporal and spatial patterns in heterogeneous healthcare data [39][40][41].

Fig. 3 shows how anomaly models can be integrated into a federated learning model. The local anomaly detection models are trained by each client node on its own data. Model updates are sent to a central server on a regular basis, where they are aggregated. The server creates a model of the whole world to be re-dispersed to the clients. The observed anomalies are notified in either local node or global aggregation, allowing real-time messages without transmitting raw data [42].

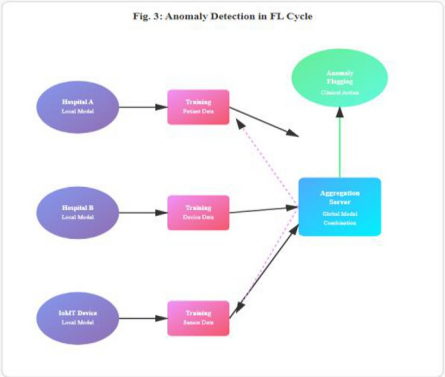

Fig.3. Integration of anomaly detection models within the federated learning cycle

4.2 Applications in Healthcare Domains

Various healthcare fields of data have been subject to federated anomaly detection. FML is used in medical imaging to facilitate cooperative training of models in different hospitals without any exposure of sensitive scans of patients, [43]. The wearable monitoring devices take advantage of FL because they can be used to identify abnormal physiological indicators, e.g. irregular heart rate or activity, in real-time whilst maintaining user privacy [44]. FML can also be used to analyze electronic health records (EHRs) to identify inconsistency, unusual disease patterns, or unusual events including treatment across institutions. IoMT and edge computing devices that operate in real-time use FL to offer low-latency anomaly detection and stay within privacy requirements [45] [46].

A comparative description of the various ways of anomaly detection is presented in Table III under the federated learning configurations. Such metrics as detection accuracy, precision, recall, communication cost, and scalability are taken into account. The table shows that the hybrid and deep learning models with FL are more accurate, robust, and privacy-preserving than the traditional ones.

Table 3. Comparative analysis of anomaly detection methods under federated learning setups

Method	Data Type	FL Integration	Accuracy	Precision	Communication Cost	Important points
CNN	Medical images	FedAvg	High	Moderate	Low	Effective for Spatial Anomalies
LSTM	Vital signs, time-series	FedProx	Moderate	High	Moderate	Captures temporal dependencies

Auto encoder	EHR and IoMT signals	Hierarchical FL	High	High	Low	Unsupervised detection
CNN–LSTM	Medical imaging + time-series	FedAvg + edge aggregation	Very High	Very High	Moderate	Captures complex spatiotemporal patterns
Transformer-based	Multi-modal healthcare data	FedAvg	Very High	Very High	Moderate-High	Handles heterogeneous distributed datasets

Performance comparisons of federated anomaly detection methods are shown in Table 3**.**

4.3 Performance and Evaluation Metrics

The metrics of the evaluation of anomaly detection during federated learning imply a variety of metrics that allow balancing the predictive accuracy and efficiency of the system. The first standard performance measures are F1-score, area under the curve (AUC), recall, and precision that assess the capability of the model to detect anomalies correctly [10][11]. Convergence rate is also taken into consideration to measure the rate at which the federated model is stabilized over distributed clients.

FL-based anomaly detection has a trade-off between accuracy and communication efficiency. Although the frequent aggregation enhances the performance of the models, it introduces overhead in the process of communication among client nodes. Less frequent updates on the other hand minimize bandwidth consumption at the expense of slightly reducing detection performance [12] [13].

Fig. 4 is a comparison of centralized and federated performance of anomaly detection. The centralized systems tend to be a little more accurate as they have access to all the raw data; however, they are associated with privacy and high communication cost. Federated systems have high privacy, mediocre latency, and competitive detection, and they represent a viable trade-off to large-scale healthcare deployments [14].

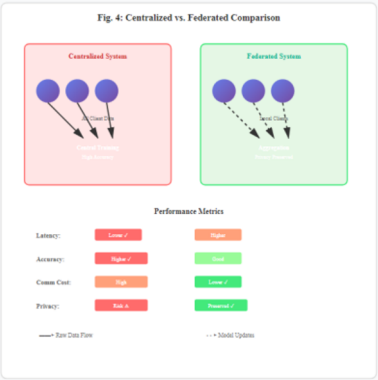

Fig.4 Comparison of centralized vs. federated anomaly detection performance

5 Challenges and Open Research Issues

Even though federated learning (FL) can transform into a useful tool in detecting anomalies in healthcare, several challenges that should be addressed to enable robust and scalable implementation should be addressed. The problem of data heterogeneity and non-IID distribution is great. Patient data in different institutions, device, and monitoring systems is usually of dissimilar format, range and sampling frequency. This variability can cause unpredictable convergence of models, generalization and biased global models [15][16].

The other matter of concern is the effectiveness of communication. The continuous exchange of model updates between the client nodes and the central server can be a major burden to uplink and downlink traffic in particular in a large-scale IoMT architecture. The current research topic is also trade-off optimization between model performance and communication overhead [17].

Security threats are one of the main threats in the FL-based anomaly detecting. The malicious participants can introduce poisoned updates or do model inversion attacks or predict sensitive data using the gradient information. Such threats undermine the trust to the federated system and can essentialism clinical decision-making [18][19].

Explainability and transparency are also important. Combined deep learning models with FL are usually opaque and clinicians cannot understand the logic behind the anomalies posed by the models. Perhaps, this will limit its adoption into the clinical practice owing to the non-interpretability of the outputs [20].

Table.4. Challenges and potential research directions in federated anomaly detection

Challenge	Description	Potential Research Directions
Data Heterogeneity & Non-IID	Variability in data distribution across institutions and devices	Adaptive aggregation methods, personalized federated learning, domain adaptation
Communication Efficiency	High bandwidth requirements for model updates	Model compression, sparse updates, asynchronous FL

Security Threats	Vulnerabilities to poisoning, gradient, and inference attacks	Robust aggregation, secure multi-party computation, adversarial defenses
Explainability & Transparency	Lack of interpretable outputs for clinicians	Explainable AI, interpretable model architectures, visualization tools
Regulatory Compliance	Maintaining privacy and legality across regions	Privacy-preserving protocols, federated auditing, compliance-aware system design

Key challenges and future research directions are summarized in **Table 4**.

6 Future Directions

The future research directions of federated anomaly detection will enhance the scalability, privacy and the flexibility of the healthcare system. The knowledge sharing method is the federated transfer learning, which allows the models to be trained with one dataset and perform well on smaller related datasets [26]. Block chain enables FL to offer defence against model updates with resistance, enhancing security and profitability of distributed healthcare networks [27]. Another advantage is that edge-based anomaly detection provides real-time analytics with less latency to data sources that are responsive in critical care applications [28][29][30].

Integration of FL, reinforcement learning, and explainable AI has the potential to make the model more transparent and flexible in decision making. Such approaches can facilitate systems to attain the best policies of anomaly detection and clinicians explanatory output with regards to flagged events [31][32]. Personalized federated learning (also referred to as federated learning personalized to individual clients) is of interest in addressing heterogeneity and improving the model performance with regard to various groups of patients [33]. Cross-institutional partnerships can be achieved by such techniques and can be used to support rapid, large scale, privacy-preserving and effective anomaly detection systems that do not impinge on clinical endearment and regulatory acceptance [34][35].

7 Conclusion

The review has condensed the recent trends of the field of anomaly detection of federated machine learning (FML) within the health care sector. It has talked about the architectural designs, combination of the profound and hybrid learning models, privacy-protective systems, which enable collective analysis of scattered patient data. The key scenarios in the medical imaging, wearable monitoring, EHR analysis, and IoMT environment were covered, which confirms the possibility of FML to offer the appropriate anomaly detection without interfering with the data confidentiality. The review also found critical challenges including heterogeneity of data, communication limitations, security risk, explain ability, and regulatory demands and newer areas of research were identified, including federated transfer learning, block chain integration, edge-based detection, and personalized federated model. Collectively, they are capable of providing a complete illustration of the current

capabilities and assist in creating safe, effective, and clinically sound anomaly detection systems within distributed health care networks.

References

1. Ali M, Naeem F, Tariq M, Kaddoum G (2023) Federated learning for privacy preservation in smart healthcare systems: a comprehensive survey. IEEE J Biomed Health Inform 27:778–789
2. Alsulaimawi Z (2024) Federated learning with anomaly detection via gradient and reconstruction analysis. arXiv preprint arXiv:2403.10000
3. Astillo PV, Duguma DG, Park H, Kim J, Kim B, You I (2022) Federated intelligence of anomaly detection agent in IoTMD-enabled diabetes management control system. Future Gener Comput Syst 128:395–405
4. Bose ASC, Eliazer M, Maheswari BU, Sivaneshkumar A, Sumithra M, Qamar S (2025) Securing healthcare data in mobile edge computing: a hybrid deep learning framework for privacy and anomaly detection. Knowl Inf Syst 1–39
5. Chen J, Ran X (2019) Deep learning with edge computing: a review. Proc IEEE 107:1655–1674
6. Cholakoska A, Pfitzner B, Gjoreski H, Rakovic V, Arnrich B, Kalendar M (2021) Differentially private federated learning for anomaly detection in eHealth networks. In: Adjunct Proc ACM Int Joint Conf Pervasive Ubiquitous Comput, pp 514–518
7. de Carvalho Polido SI (2023) Applying federated learning to a COVID-19 anomaly detection pipeline. Doctoral dissertation, Instituto Universitário de Lisboa
8. Fu A, Zhang X, Xiong N, Gao Y, Wang H, Zhang J (2022) VFL: a verifiable federated learning with privacy-preserving for big data in industrial IoT. IEEE Trans Ind Inform 18:3316–3326
9. Gupta D, Kayode O, Bhatt S, Gupta M, Tosun AS (2021) Hierarchical federated learning based anomaly detection using digital twins for smart healthcare. In: Proc IEEE CIC, pp 16–25
10. Huong TT, Bac TP, Ha KN, Hoang NV, Hoang NX, Hung NT, Tran KP (2022) Federated learning-based explainable anomaly detection for industrial control systems. IEEE Access 10:53854–53872
11. Hussain G, Manoj G (2022) Federated learning: a survey of a new approach to machine learning. In: Proc ICEEICT, pp 1–8
12. Jithish J, Alangot B, Mahalingam N, Yeo KS (2023) Distributed anomaly detection in smart grids: a federated learning-based approach. IEEE Access 11:7157–7179
13. Khan L, Saad W, Han Z, Hossain E, Hong C (2021) Federated learning for Internet of Things: recent advances, taxonomy, and open challenges. IEEE Commun Surv Tutor 23:1759–1799
14. Khan MM, Alkhathami M (2024) Anomaly detection in IoT-based healthcare: machine learning for enhanced security. Sci Rep 14:5872
15. Lakhan A, Mohammed MA, Nedoma J, Martinek R, Tiwari P, Vidyarthi A et al (2022) Federated learning-based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. IEEE J Biomed Health Inform 27(2):664–672
16. Li T, Sahu A, Talwalkar A, Smith V (2020) Federated learning: challenges, methods, and future directions. IEEE Signal Process Mag 37:50–60

17.Liu Y, Garg S, Nie J, Zhang Y, Xiong Z, Kang J, Hossain MS (2020) Deep anomaly detection for time-series data in industrial IoT: a communication-efficient on-device federated learning approach. IEEE Internet Things J 8(8):6348–6358
18.Mothukuri V, Khare P, Parizi RM, Pouriyeh S, Dehghantanha A, Srivastava G (2021) Federated learning-based anomaly detection for IoT security attacks. IEEE Internet Things J 9(4):2545–2554
19.Nagamani GM, Kumar CK (2024) Design of an improved graph-based model for real-time anomaly detection in healthcare using hybrid CNN–LSTM and federated learning. Heliyon 10(24)
20.Namratha M, Anusree MK, Niha P, Pooja S, Arpana MR (2023) Anomaly detection in medical IoT devices using federated learning. In: Int Conf Smart Trends Comput Commun, pp 259–270
21.Nariman GS, Hamarashid HK (2025) Hierarchical federated learning for health trend prediction and anomaly detection using pharmacy data: from zone to national scale. Int J Data Sci Anal 1–20
22.Neshenko N, Bou-Harb E, Crichigno J, Kaddoum G, Ghani N (2019) Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Commun Surv Tutor 21:2702–2733
23.Nguyen D, Pham Q, Pathirana P, Ding M, Seneviratne A, Lin Z, Dobre O, Hwang W (2022) Federated learning for smart healthcare: a survey. ACM Comput Surv 55
24.Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD et al (2021) The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ 372
25.Pavlidis N, Perifanis V, Briola E, Nikolaidis CC, Katsiri E, Efraimidis PS, Filippidou DE (2024) Federated anomaly detection for early-stage diagnosis of autism spectrum disorders using serious game data. arXiv preprint arXiv:2410.20003
26.Pekar A, Mocnej J, Seah W, Zolotova I (2020) Application domain-based overview of IoT network traffic characteristics. ACM Comput Surv 53
27.Pinto RP, Silva BM, Inácio PR (2025) Federated learning for anomaly detection on Internet of Medical Things: a survey. Internet Things 101677
28.Preuveneers D, Rimmer V, Tsingenopoulos I, Spooren J, Joosen W, Ilie-Zudor E (2018) Chained anomaly detection models for federated learning: an intrusion detection case study. Appl Sci 8(12):2663
29.Raje VV, Goel S, Patil SV, Kokate MD, Mane DA, Lavate S (2023) Real-time anomaly detection in healthcare IoT: a machine learning-driven security framework. J Electr Syst 19(3)
30.Rani S, Kataria A, Kumar S, Tiwari P (2023) Federated learning for secure IoMT applications in smart healthcare systems: a comprehensive review. Knowl Based Syst 274:110658
31.Raza A, Li S, Tran KP, Koehl L (2022) Using anomaly detection to detect poisoning attacks in federated learning applications. arXiv preprint arXiv:2207.08486
32.Raza A, Tran KP, Koehl L, Li S (2023) AnoFed: adaptive anomaly detection for digital health using transformer-based federated learning and support vector data description. Eng Appl Artif Intell 121:106051
33.Rbah Y, Mahfoudi M, Balboul Y, Fattah M, Mazer S, Elbekkali M, Bernoussi B (2022) Machine learning and deep learning methods for intrusion detection systems in IoMT: a survey. In: Proc IRASET, pp 1–9

34.Schneble W, Thamilarasu G (2019) Attack detection using federated learning in medical cyber-physical systems. In: Proc ICCCN, pp 1–8
35.Sharma B, Sharma L, Lal C (2019) Anomaly detection techniques using deep learning in IoT: a survey. In: Proc ICCIKE, pp 146–149
36.Shrestha R, Mohammadi M, Sinaei S, Salcines A, Pampliega D, Clemente R et al (2024) Anomaly detection based on LSTM and autoencoders using federated learning in smart electric grid. J Parallel Distrib Comput 193:104951
37.Simon J, Kapileswar N (2025) Federated deep learning-driven cloud-IoT framework for real-time healthcare monitoring and privacy-preserving anomaly detection. In: Proc ICSSAS, pp 1866–1871
38.Singh P, Gaba GS, Kaur A, Hedabou M, Gurtov A (2022) Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT. IEEE J Biomed Health Inform 27(2):722–731
39.Singh PK, Chowdhury A, Pal A (2025) Distributed anomaly detection using federated learning. IEEE Access
40.Taha Z, Yaw C, Koh S, Tiong S, Kadirgama K, Benedict F, Tan J, Balasubramaniam Y (2023) A survey of federated learning from data perspective in the healthcare domain: challenges, methods, and future directions. IEEE Access 11:45711–45735
41. Tahir S, Zaheer A (2024) A distributed model for IoT anomaly detection using federated learning. In: Cybersecurity Measures for Logistics Industry Framework, pp 75–91. IGI Global
42.Wang J, Liu Q, Liang H, Joshi G, Poor HV (2020) Tackling the objective inconsistency problem in heterogeneous federated optimization
43.Wang X, Garg S, Lin H, Hu J, Kaddoum G, Piran MJ, Hossain MS (2021) Toward accurate anomaly detection in industrial Internet of Things using hierarchical federated learning. IEEE Internet Things J 9(10):7110–7119
44.Wang X, Wang Y, Javaheri Z, Almutairi L, Moghadamnejad N, Younes OS (2023) Federated deep learning for anomaly detection in the Internet of Things. Comput Electr Eng 108:108651
45.Weinger B, Kim J, Sim A, Nakashima M, Moustafa N, Wu KJ (2022) Enhancing IoT anomaly detection performance for federated learning. Digit Commun Netw 8(3):314–323
46.Yogitha M, Srinivas KS (2023) Using federated learning in anomaly detection and analytics on real-time streaming data of healthcare. In: Proc ICGSP, pp 29–34