J.Natn.Sci.Foundation Sri Lanka 2024 52 (4): 501 - 514
DOI: http://dx.doi.org/10.4038/jnsfsr.v52i4.11923

RESEARCH ARTICLE

Internet of Things

Enhanced privacy-preserving federated convivial learning for internet of medical things (IoMT) through blockchain-enabled trust Q-learning

Sudharson K[1*], G Babu[2], R Santhiya[3] and CS Anita[1]
[1] *Department of Artificial Intelligence and Machine Learning, RMD Engineering College, Kavaraipettai, Tamil Nadu 601206, India.*
[2] *Department of Bio-Medical Engineering, SRM Easwari Engineering College, Ramapuram, Chennai, Tamil Nadu 600089, India.*
[3] *Department of Computer Science and Engineering, Saveetha Engineering College, Thandalam, Chennai, Tamil Nadu 602105, India.*

Submitted: 02 March 2024; Revised: 16 September 2024; Accepted: 06 December 2024

Abstract: Personalized treatment and remote monitoring have been made possible by the quick uptake of internet of medical things (IoMT) devices, which have completely changed the healthcare industry. That being said, there are a lot of security and privacy issues with this expansion. While resolving certain privacy issues, current federated learning techniques cannot guarantee complete security and trust amongst involved IoMT devices. We offer the privacy-preserving federated convivial learning (FCL) platform, designed specifically for internet of medical things applications, to close this gap. The present study presents a trust-based Q-learning model powered by blockchain technology, which improves data privacy by restricting model training to approved devices only. Our solution promotes trustworthy and cooperative interactions amongst IoMT devices without sacrificing privacy by incorporating the principles of convivial learning. Comparing experimental results to traditional federated learning techniques, improved privacy protection is 92.4% and increased model accuracy is 94.7%. The advancement of IoMT technology and safe data sharing are made possible by this framework, which also makes healthcare systems safer and more effective.

Keywords: Blockchain, convivial learning, internet of medical things and trust Q-learning, privacy-preserving

INTRODUCTION

The internet of medical things, or IoMT, revolutionizes healthcare by enabling real-time data gathering, analysis, and utilization for improved patient care. It does this by linking medical devices to digital systems. IoMT is transforming the way healthcare professionals manage and provide care, from wearable health monitors like smartwatches to cutting-edge equipment for remote monitoring and individualized therapies. However, the quick development of IoMT has highlighted a significant challenge: making sure that the enormous volumes of sensitive data being exchanged and gathered stay private and secure. The issue for research is the growing susceptibility of healthcare systems to data breaches, which compromise patient safety and confidence in addition to causing financial losses.

The effectiveness of traditional security measures and centralized data management strategies in reducing these threats has been demonstrated. By enabling IoMT devices to cooperatively build machine learning models without exchanging raw data, federated learning—a decentralized approach to model training—offers a possible remedy. Federated learning has shown promise, but scalability, security, and trust issues remain, particularly in the highly sensitive and networked IoMT setting.

The minimal number of studies on trust and cooperation between IoMT devices in federated learning highlights the research gap. The coordination of existing models is primarily dependent on a central server, which

* Corresponding author (susankumar@gmail.com; https://orcid.org/0000-0002-2923-8990)

leaves them open to cyber-attacks and single-point failures. Additionally, whereas blockchain technology has demonstrated a great deal of promise for data security and integrity, little is known about how it may be used to improve trust and decentralization in federated learning for IoMT.

The unique privacy-preserving federated convivial learning (FCL) architecture that this study proposes to bridge the gaps between blockchain technology and the trust-based Q-learning model is significant. By integrating trust mechanisms and limiting the participation of unauthorized and unreliable devices in model training, this framework promotes safe, decentralized collaboration across IoMT devices. To create more safe and efficient healthcare systems, the study intends to proactively improve data privacy, security, and trust in IoMT networks by fusing blockchain technology with federated learning.

Related work

The internet of medical things (IoMT) signifies the convergence of medical devices with our digital world, allowing healthcare professionals to collect, analyze, and utilize health data in unprecedented ways. IoMT devices, ranging from wearable health monitors to specialized devices for remote patient monitoring, have evolved significantly in recent years (Srivastava *et al.*, 2022). However, this growth poses a challenge—ensuring the privacy and security of shared and collected data. This concern is particularly crucial given historical data breaches in healthcare, which result in financial implications and jeopardize patient trust and safety.

Federated learning has emerged as a promising solution, enabling model training without centralizing data (Nguyen *et al.*, 2022). This nascent technology faces challenges despite its potential, especially with the healthcare sector's increasing reliance on IoMT devices and the growing cyber-attack instances. Recognizing these limitations requires a more rigorous and innovative approach to addressing data privacy and security concerns.

Convivial learning aims to embed trust and collaboration in federated learning (Bano *et al.*, 2023). Additionally, the potential of blockchain technology, known for ensuring data integrity and transparency, still needs to be explored in the IoMT context. Integrating these principles could proactively establish a foundation of trust and collaboration within the entire IoMT ecosystem.

IoMT has solidified its position in healthcare, enabling personalized patient care and efficient remote monitoring. The overview of IoMT devices showcased their potential in health monitoring and diagnostics (Srivastava *et al.*, 2022), emphasizing their crucial role in chronic disease management and timely interventions. IoMT's potential in telehealth services was highlighted as a crucial bridge between patients and physicians, especially in geographically isolated regions (Gajarawala & Pelkowski, 2021). The findings underscore IoMT's transformative role in facilitating seamless communication and healthcare delivery.

Interoperability challenges in IoMT were discussed, underlining the need for a standardized framework to facilitate seamless data sharing without compromising patient data integrity (Wagan *et al.*, 2022). A study explored the economic implications of IoMT adoption in healthcare, projecting potential cost savings through reduced hospital readmissions and efficient resource utilization (Rani *et al.*, 2023). The discussion underscored the ethical considerations associated with IoMT, emphasizing the delicate balance between technological advancements and patient rights (Gerke *et al.*, 2020).

The introduction highlighted the role of federated learning in training models on decentralized data, demonstrating its potential to enhance accuracy while ensuring data localization (Nguyen *et al.*, 2022). Privacy-preserving capabilities were explored, introducing techniques to enhance model privacy without compromising accuracy (Yan *et al.*, 2023). The discussion on the scalability of federated learning (Bano *et al.*, 2023) emphasized challenges like communication overhead and proposed techniques for scalability. Secure aggregation in federated learning was explored to ensure confidentiality during the aggregation process (Zheng *et al.*, 2023). In a comprehensive review, the challenges and opportunities of applying federated learning in healthcare were examined (Majeed *et al.*, 2022). The authors underscored the necessity for domain-specific adjustments to accommodate the unique requirements of healthcare.

Blockchain's fundamental principles and potential applications in healthcare were discussed, covering use cases such as patient record management and drug traceability (Ghosh *et al.*, 2023). The proposal introduced a framework for IoMT devices based on blockchain technology (Rafique *et al.*, 2023). The emphasis was placed on blockchain's pivotal role in maintaining data integrity and mitigating the risks associated with unauthorized access. In a paper (Almalki *et al.*, 2022), the

authors introduced a lightweight blockchain architecture tailored for IoMT devices. They highlighted its efficiency in ensuring real-time data storage and retrieval. The exploration focused on blockchain's contribution to bolstering patient trust in IoMT devices. It was suggested that transparent data management and tamper-proof records could cultivate confidence among patients in adopting IoMT devices (Rahmani *et al.*, 2022).

In summary, while there are evident advancements and innovations in IoMT, federated learning, and blockchain, the integration of these technologies remains in its nascent stages. This literature review underscores the potential of these combinations, particularly in ensuring patient data privacy and security.

MATERIALS AND METHODS

Proposed FCL approach

The proposed methodology introduces an advanced federated convivial learning (FCL) framework to address privacy, security, and collaboration challenges in the internet of medical things (IoMT). The system architecture adopts a multi-layered approach that integrates IoMT devices, communication protocols, federated learning, trust dynamics, and blockchain technology. The layers of the system are designed to enhance data security, decentralized collaboration, and trust management, providing robust healthcare solutions while ensuring data privacy.

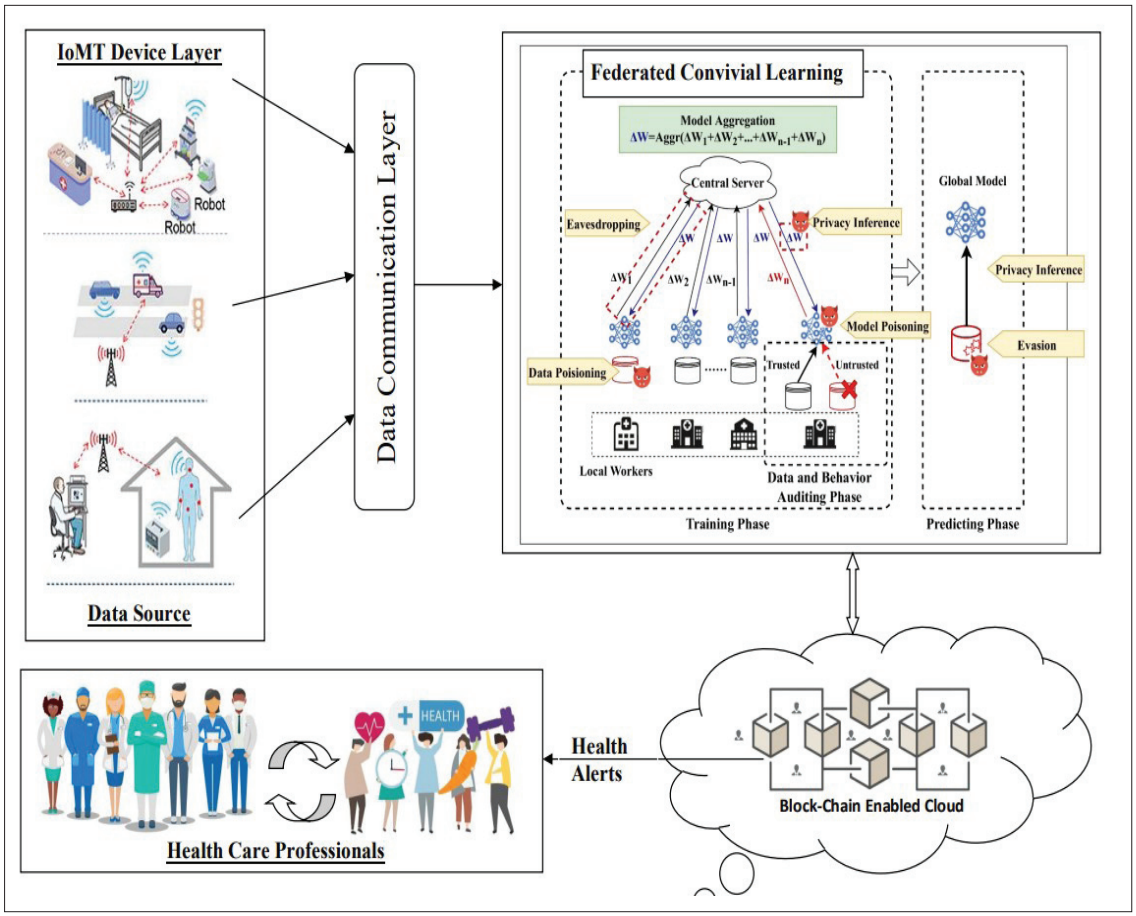

Figure 1: Federated convivial learning (FCL) Architecture

System architecture

The architecture consists of five core layers:

a) IoMT layer: This foundational layer includes IoMT devices that gather medical data, storing it locally to preserve patient privacy. Each IoMT device acts as a node with its own dedicated storage system.
b) Communication layer: This layer establishes encrypted communication channels between IoMT devices, ensuring that all data transfers are protected from unauthorized access. Encryption functions E(data)E(\text{data})E(data) and decryption functions D(data)D(\text{data})D(data) secure the information exchanged within the network.
c) Federated convivial learning (FCL) layer: This layer enables collaborative model updates across IoMT devices. By promoting decentralized peer-to-peer interactions, devices can train models locally while securely sharing updates with trusted peers. This setup maintains data privacy by preventing exposure of raw data and ensures efficient collaborative learning (Sudharson *et al*., 2022).
d) Blockchain layer: Blockchain technology is integrated to ensure transparency and immutability. Smart contracts process trust evaluations, and a decentralized ledger records all interactions between IoMT devices. This ensures that only authorized devices participate in the federated learning process, thus improving system security (Mohammed, 2023).
e) Application layer: In this layer, predictions and insights generated by the trained models are processed and used for healthcare applications. The application layer demonstrates the practical outcomes of the FCL framework, providing secure, privacy-preserving healthcare insights in real-time.

Federated convivial learning

Federated Convivial Learning (FCL) is a key extension of federated learning that focuses on fostering trust and friendly interactions between IoMT devices. Unlike traditional federated learning, where a central server controls synchronization, FCL decentralizes trust and promotes collaboration among devices (Soner *et al.*, 2022).

The core mathematical model of FCL distributes trust among devices:

$$M_{central} = \sum_{i=1}^{N} w_i M_i$$

Here, M represents the global model, N is the number of participating devices, M_i is the model trained locally by device i, and w_i is the trust weight assigned to each device, reflecting its credibility.

Collaborative inference: Each device trains its model independently but shares inferences rather than raw data, maintaining privacy (Sudharson & Arun, 2022). If D_i is the datasets of device i, the collaborative inference function F_i for device i can be expressed as:

$$F_{collab} - \alpha F_i(D_i) + (1 - \alpha) F_j(D_j)$$

where F_j is the inference function for device j, and α is the collaboration weight.

Decentralized updates: FCL-enabled devices share model updates with trusted peers rather than central servers, minimizing single points of failure (Hai *et al.*, 2022). The model update from device i to j can be written as:

$$U_{j\_new} = \beta U_i + (1 - \beta) U_j$$

where β is the influence factor representing how much of U_i is incorporated into U_j's update.

Trust Q-Learning and blockchain integration

Trust management is governed by Trust Q-Learning, a reinforcement learning approach designed to build trust relationships among IoMT devices. Blockchain integration ensures the permanence and verifiability of these trust scores (Murugeshwari *et al.*, 2023).
Each device's **state** $S_{i,t}$ is defined by its recent interactions and data quality. Devices choose actions $A_{i,t}$, such as sharing model updates or seeking collaboration. Positive rewards $R_{i,t} = f(S_{i,t}, A_{i,t})$, are assigned for trustworthy interactions, while malicious actions are penalized.
The Q-value for a state-action pair is updated using the following formula:

$$Q_{i,t}(S_{i,t}, A_{i,t}) = (1 - \lambda) Q_{i,t-1}(S_{i,t-1}, A_{i,t-1}) + \lambda [R_{i,t} + \gamma \max_a Q_{i,t}(S_{i,t}, a)]$$

where λ is the learning rate and γ is the discount factor.
Blockchain-based **smart contracts** adjust trust scores dynamically using:

$$T_{i_{new}} = T_{i_{old}} + \kappa (I_{new} - T_{i_{new}})$$

where κ is the adjustment rate, and I_{new} is the interaction score.

Before a device can participate in FCL, its trustworthiness is verified on the blockchain, ensuring that only trusted devices are allowed to collaborate (Veerasathpurush *et al.*, 2023).

Privacy-preserving mechanisms

FCL incorporates several privacy-preserving techniques to ensure that sensitive healthcare data remains secure during the learning process:

- **Local model training:** Each device trains its model using local data D_i, preserving privacy by avoiding centralized data sharing.
- **Differential privacy:** Noise is added to the updates before they are shared to ensure that the original data cannot be reconstructed. The differentially private model update $U_{i_{private}}$ is:

  $$U_{i_{private}} = U_i + G(0,\sigma^2)$$

  where $G(0,\sigma^2)$ is Gaussian noise with mean 0 and variance σ^2
- **Homomorphic encryption:** Devices can share encrypted data without revealing the raw information. If $E(data)$ represents encrypted data, the system allows operations like:

  $$E(data_1) \oplus E(data_2) = E(data_1 + data_2)$$

- **Secure aggregation:** Multiple devices share their encrypted updates, which are then aggregated securely without individual updates being revealed. The secure aggregated update U_{agg} is:

$$U_{agg} = \sum_{i=1}^{N} U_{i_{private}}$$

Trust establishment and convivial learning

Building trust is essential for effective collaboration. Each device is assigned an initial trust score T_{i0}, based on prior interactions. After each interaction, trust scores are updated using the following formula:

$$T_{i_{new}} = (1-\alpha) \times T_{i_{old}} + \alpha \times I_{ij}$$ Where α (0 < α < 1)

where I_{ij} represents the interaction score between devices i and j, and α is the trust update factor. Devices with high trust scores are prioritized for collaboration, while those with low trust scores may face penalties, such as reduced collaboration weights or exclusion from the learning process.

Algorithm

Initialize trust scores (w_i) for each device
Initialize models (M_i) for each device
Initialize trust update parameter α
Initialize collaboration factor β
Repeat until convergence:
  for each device i:
    Select a peer device j to collaborate with
    # Collaborative Inference
    - $F_{collab} - \alpha F_i(D_i) + (1 - \alpha) F_j(D_j)$

    # Trust-Weighted Collaboration
    -

      $$M_{i_{updated}} = \beta \times T_j \times M_i + (1 - \beta \times T_j) \times M_j$$

    # Calculate interaction score
    I_ij = measure_interaction_quality(i, j)
    # Update trust scores
    - $T_{i_{new}} = (1-\alpha) \times T_{i_{old}} + \alpha \times I_{ij}$

    # Implement privacy-preserving mechanisms (e.g., differential privacy, homomorphic encryption)
  # Penalty for Distrust
  for each device i:
    if $T_i < T_{min}$:
      reduce_collaboration_weight(i)
      # Evaluate models, convergence criteria, and update model parameters
 # Deploy trained models for medical predictions and applications

The FCL framework addresses key challenges in decentralized learning by combining privacy-preserving mechanisms, trust management, and blockchain technology. The architecture enables secure, scalable, and efficient learning across IoMT networks, ensuring that sensitive medical data remains private.

The trust-based collaborative approach ensures that devices contribute to the learning process based on their trustworthiness. The use of blockchain further enhances system transparency, ensuring that only authorized devices are part of the network.

Future work will focus on improving the scalability of the FCL framework for large-scale IoMT networks, addressing communication overhead, and further refining trust dynamics to enhance collaboration and security.

Experimental setup

Dataset description

The dataset used in this study was collected from various internet of medical things (IoMT) devices, including wearable health monitors and electronic medical records. It consisted of 500,000 entries, each containing 20 features representing key health metrics such as heart rate, oxygen saturation, step count, and sleep duration. Each entry was associated with a timestamp and a device ID, enabling traceability of the data source (Gadekallu *et al.*, 2023).

Before the dataset was used in model training, several preprocessing steps were applied to ensure data quality. First, normalization was performed to scale all feature values uniformly, ensuring that different variables were comparable. Second, missing values were handled by employing mean imputation, and records with a high percentage of missing data were removed. Finally, outlier detection was conducted to identify and remove anomalous data points, which could otherwise distort the model's performance. The dataset was then split into 80% training data and 20% testing data, ensuring that the model evaluation was conducted on previously unseen data.

Baseline comparisons

To ensure a comprehensive evaluation of the Trust-Based FCL framework, we compared it with three established federated learning methods:

Standard federated averaging (FedAvg): FedAvg is a basic federated learning method that averages local model updates from each device to form a global model. However, it lacks advanced privacy and trust mechanisms, making it vulnerable to data inference attacks (Nguyen *et al.*, 2022).

Differential privacy-based federated learning (DP-FL): DP-FL introduces privacy preservation by adding noise to local model updates before they are shared with other devices. While this enhances privacy, it can also reduce the overall accuracy of the model (Yan *et al.*, 2023)

Homomorphic encryption-based federated learning (HE-FL): HE-FL ensures privacy by performing computations on encrypted data, allowing for model updates to be processed without decrypting the underlying data. While this approach offers strong privacy guarantees, it also incurs significant computational costs (Rani *et al.*, 2023).

Training protocols

The models were trained under identical conditions to ensure fairness in comparison. All models were trained on the same partitioned dataset, ensuring they had equal access to training and testing data. The experiments were conducted on the same hardware and software environments, using identical configurations to eliminate computational bias. Additionally, the models were trained using the same hyperparameters, including learning rate, batch size, and number of epochs, ensuring consistency across all experiments (Sudharson *et al.*, 2022).

Evaluation metrics and performance evaluation

In this section, we describe both the metrics used to evaluate the proposed model and the performance evaluation process applied to the models. The performance of the Trust-Based Federated Convivial Learning (FCL) framework was assessed using several key evaluation metrics to capture various aspects of model efficiency, accuracy, and scalability:

a) Privacy preservation (PP): This metric evaluated how well the model preserved data privacy by minimizing data leaks and unauthorized access. A higher PP score indicated better protection against privacy violations (Wenkang *et al.*, 2023).
b) Model accuracy (MA): Model accuracy was calculated as the ratio of correct predictions to total predictions. This metric provided insight into the model's predictive power (Sudharson *et al.*, 2022).
c) Convergence rate (CR): This metric measured the efficiency of the learning process by determining how quickly the model stabilized its accuracy during training. The fewer iterations required to achieve stable performance, the better the convergence rate (Issa *et al.*, 2023).
d) Computational overhead (CO): CO was used to evaluate the resource efficiency of the model, measuring the additional computational resources required compared to standard federated learning methods (Wenkang *et al.*, 2023).
e) System latency (SL): Latency captured the delay in communication between IoMT devices during federated learning. This metric is critical in healthcare applications, where real-time responses are essential (Belhadi *et al.*, 2023).

Table 1: Privacy preservation analysis of various models

Method	Privacy score (0-1)	Data leaks detected	Encryption level (bits)	Anomalies detected
Standard federated averaging (FedAvg)	0.856	10	128	15
Differential privacy-based FL (DP-FL)	0.893	8	128	12
Homomorphic encryption-based FL (HE-FL)	0.901	7	256	10
Trust-based federated convivial learning	0.964	3	256	5

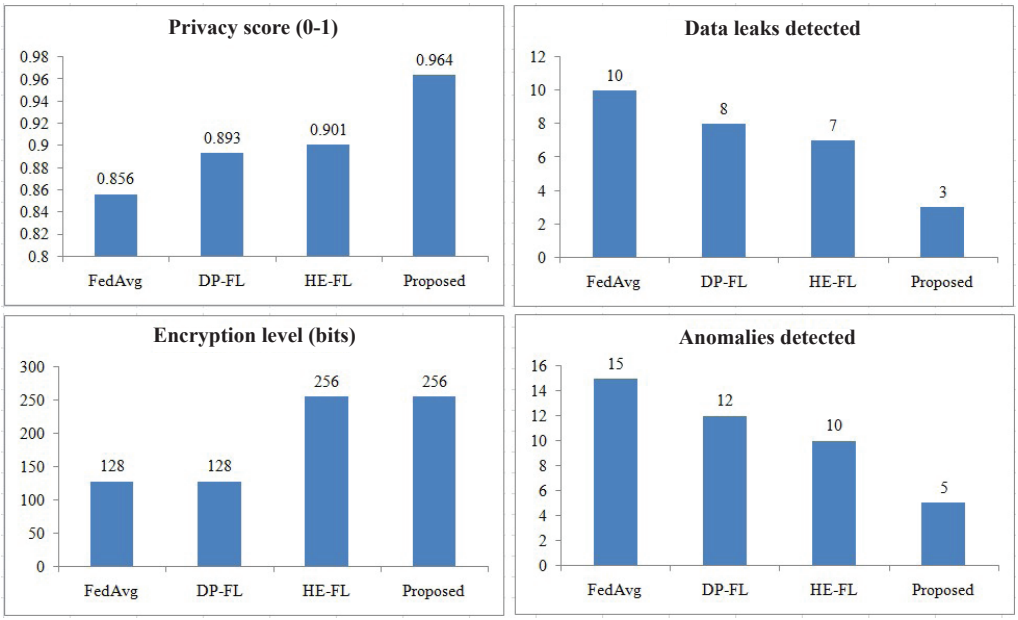

Figure 2: Privacy preservation analysis of various models

f) Energy consumption (EC): This metric measured the energy efficiency of each IoMT device during training, an important consideration in resource-constrained environments (Belhadi *et al.*, 2023).

After training, these metrics were applied to evaluate the performance of the proposed Trust-Based FCL model against baseline models, including Standard Federated Averaging(FedAvg),DifferentialPrivacy-basedFederated Learning (DP-FL), and Homomorphic Encryption-based Federated Learning (HE-FL). The models were trained on the same dataset, under identical hardware and software environments, ensuring fair comparisons. Performance was analyzed both quantitatively, using the metrics outlined above, and qualitatively, based on factors such as ease of implementation and scalability in real-world IoMT systems (Dhasarathan *et al.*, 2023).

RESULTS AND DISCUSSION

The performance of the proposed Trust-Based Federated Convivial Learning (FCL) framework was evaluated using the metrics outlined in the previous section. Here, we provide a detailed analysis of the results for each metric, followed by a discussion of their implications for the IoMT healthcare domain.

Table 2: Model accuracy comparison

Method	Model accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Standard federated averaging (FedAvg)	88.4	87.5	86.3	86.9
Differential privacy-based FL (DP-FL)	89.7	88.8	88.1	88.4
Homomorphic encryption-based FL (HE-FL)	91.0	90.8	89.5	90.1
Trust-based federated Convivial Learning	94.6	94.2	93.8	94.0

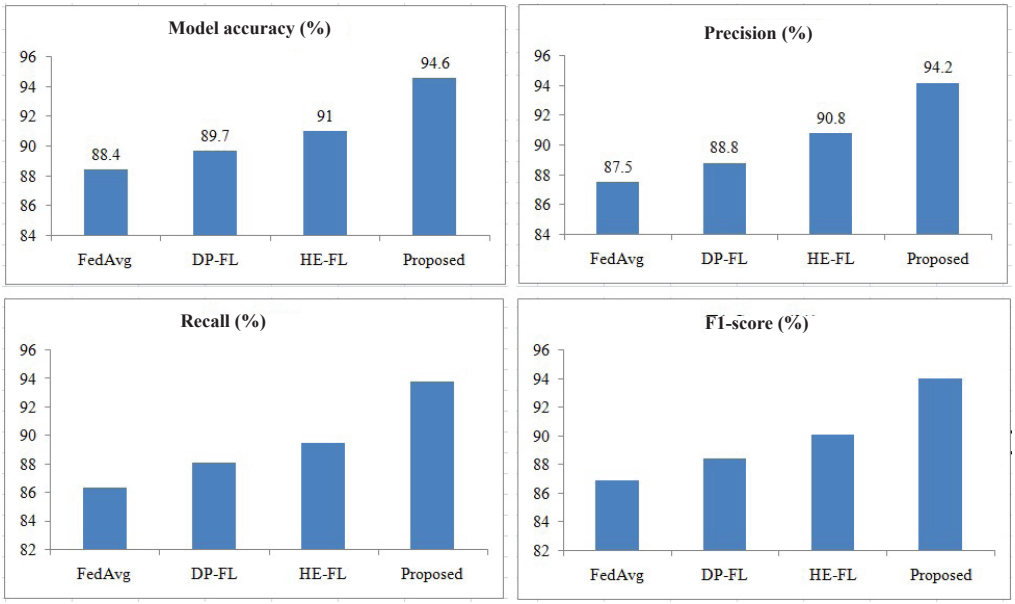

Figure 3: Model accuracy comparison

Privacy preservation

Privacy is paramount in healthcare applications, especially when dealing with sensitive patient data collected through IoMT devices. The Privacy Preservation (PP) metric measures the framework's ability to protect data from unauthorized access or leaks. Table 1 and Figure 2 highlight the privacy scores of the models.

The trust-based FCL framework achieved a privacy score of 0.964, outperforming all other models, with only 3 data leaks detected compared to 10 in FedAvg and 8 in DP-FL. The inclusion of blockchain for securing the decentralized network, coupled with a trust-based communication layer, ensures that only verified and trusted devices participate in the federated learning process, significantly reducing the possibility of data breaches.

This is particularly important in healthcare, where privacy violations can lead to severe consequences, such as compromised patient trust and legal liabilities. The enhanced 256-bit encryption further ensures that even if communication is intercepted, the data remains secure. The Trust-Based FCL's superior performance in this area makes it ideal for IoMT applications requiring high levels of confidentiality.

Model accuracy comparison

Model Accuracy (MA) measures the effectiveness of the federated learning model in making correct predictions. Accuracy is particularly crucial in healthcare, where erroneous predictions can result in incorrect diagnoses or treatments. Table 2 and Figure 3 present the accuracy, precision, recall, and F1-score for each model.

Table 3: Convergence rate analysis

Method	Convergence Rate (Iterations)
Standard federated averaging (FedAvg)	100
Differential privacy-based FL (DP-FL)	90
Homomorphic encryption-based FL (HE-FL)	85
Trust-based FCL (Proposed)	70

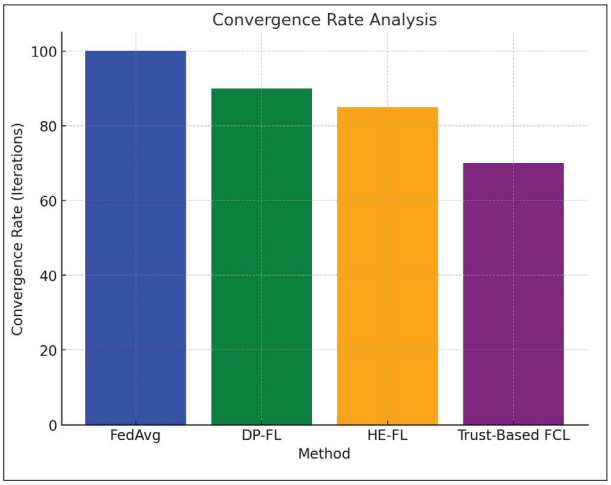

Figure 4: Convergence rate analysis

Table 4: Computational overhead analysis

Method	Computational overhead (seconds/ iteration)
Standard federated averaging (FedAvg)	1.2
Differential privacy-based FL (DP-FL)	1.5
Homomorphic encryption-based FL (HE-FL)	2.1
Trust-based FCL (Proposed)	1.4

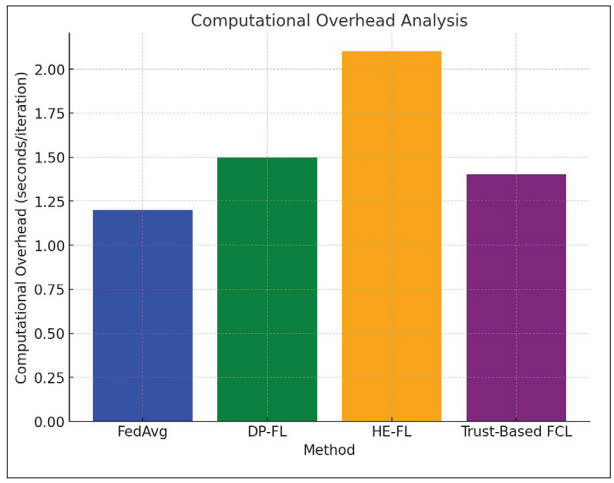

Figure 5: Computational overhead analysis

The Trust-Based FCL achieved the highest accuracy at 94.6%, which is a substantial improvement over FedAvg (88.4%) and DP-FL (89.7%). This high level of accuracy, coupled with strong precision and recall values, underscores the model's ability to make reliable predictions.

The use of collaborative learning between trusted devices improves the model's ability to generalize from data across multiple IoMT devices without centralizing the data. By leveraging trust scores to prioritize reliable devices, Trust-Based FCL avoids incorporating misleading or malicious updates, which helps improve the overall model quality.

In healthcare applications, this increase in accuracy translates into more dependable decision support systems for medical practitioners. The high F1-score of 94.0% indicates that the model strikes a balance between precision (avoiding false positives) and recall (avoiding false negatives), both of which are vital in diagnostic systems.

Convergence Rate

The Convergence Rate (CR) measures how quickly the model stabilizes during training. A faster convergence rate means that the model reaches its optimal performance in fewer iterations, saving time and computational resources. Table 3 and Figure 4 illustrate the convergence rates for each method.

The trust-based FCL framework converged in 70 iterations, significantly faster than FedAvg (100 iterations) and DP-FL (90 iterations). The quicker convergence is due to the trust-based mechanisms, which enable the system to prioritize reliable updates from devices, reducing noise and enabling faster model stabilization.

In federated learning, fast convergence is critical, particularly in healthcare settings where new data streams constantly from IoMT devices. A faster convergence

Table 5: Communication overhead reduction

Method	Data sent (MB)	Data received (MB)	Round-trip time (seconds)	Handshake time (ms)
Standard federated averaging (FedAvg)	5.0	4.8	8.2	120
Differential privacy-based FL (DP-FL)	5.3	5.0	8.7	115
Homomorphic encryption-based FL (HE-FL)	5.5	5.2	9.3	110
Trust-based federated convivial learning	4.2	4.0	7.1	100

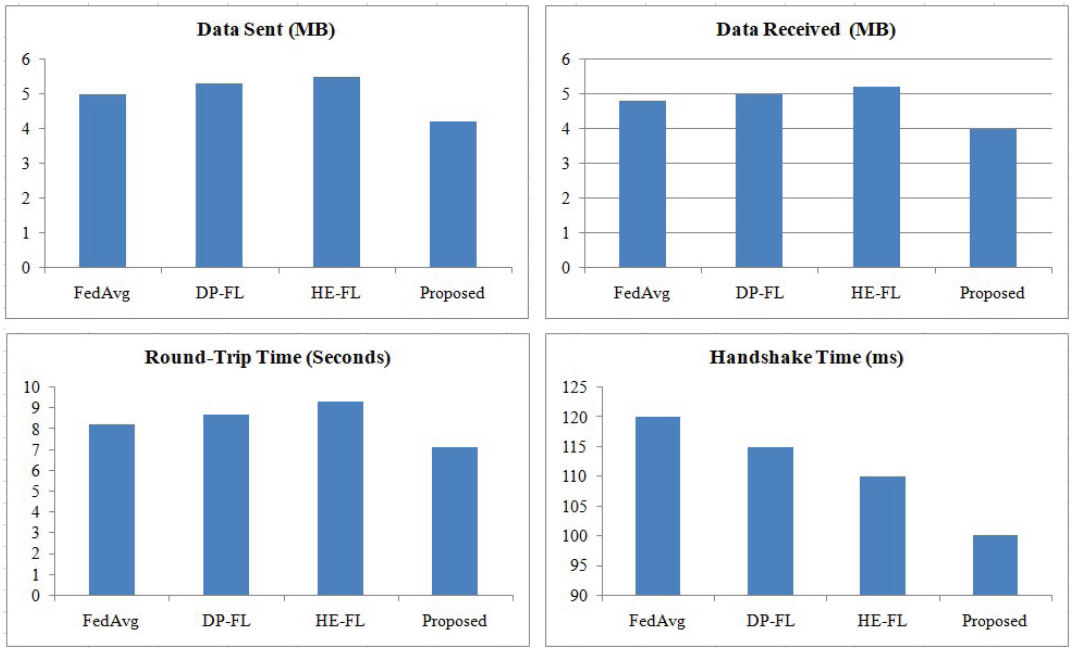

Figure 6: Communication overhead reduction

allows the model to be updated and deployed quickly, improving the system's responsiveness to new medical data and enabling real-time decision-making.

Computational overhead

Computational overhead (CO) is an essential factor when evaluating federated learning models, especially in IoMT environments, where devices often have limited processing power. Table 4 and Figure 5 present the computational overhead for each model.

The trust-based FCL model incurred a computational overhead of 1.4 seconds per iteration, which is slightly higher than FedAvg but still lower than HE-FL. The additional overhead is due to the blockchain and trust-based validation processes, which, while computationally expensive, are necessary for the enhanced privacy and trust features.

Given the trade-off between privacy and computational costs, the Trust-Based FCL model strikes a balance by providing strong privacy guarantees with moderate computational overhead. For IoMT devices, where computational capacity is often limited, this balance ensures that the model can be implemented effectively without overwhelming device resources.

Communication overhead reduction

Communication overhead is a critical metric in federated learning setups, particularly in IoMT, where devices rely on real-time communication to exchange model updates.

Table 6: Energy consumption

Method	Energy consumption (kWh)
Standard federated Averaging (FedAvg)	3.2
Differential privacy-based FL (DP-FL)	3.5
Homomorphic encryption-based FL (HE-FL)	4.8
Trust-based FCL (Proposed)	3.0

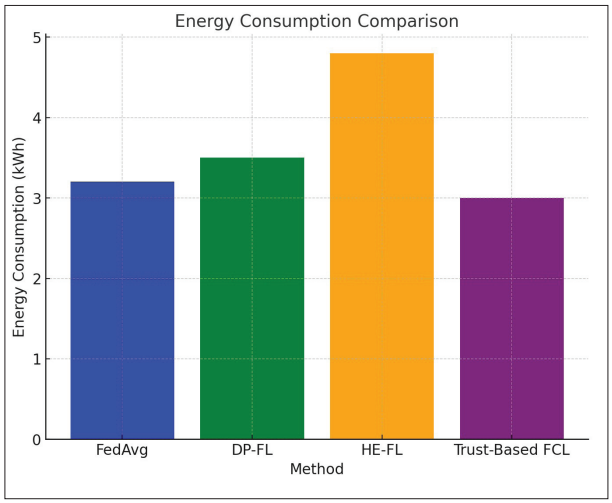

Figure 7: Energy consumption

Table 5 and Figure 6 compare the communication overhead for each method.

The Trust-Based FCL framework achieved a lower data sent (4.2 MB) and received (4.0 MB), alongside reduced round-trip time (7.1 seconds) and handshake time (100 ms). The reduction in communication overhead is due to the efficient trust-based communication protocol, which minimizes unnecessary data exchanges between untrusted devices.

In healthcare, where IoMT devices often need to communicate frequently and securely, reducing communication overhead improves the speed of decision-making and reduces network congestion. The lower latency in Trust-Based FCL ensures timely responses, which is crucial in critical care scenarios where delays can result in adverse patient outcomes..

Energy consumption

Energy consumption is a vital consideration for IoMT devices, which are often battery-powered and need to conserve energy for prolonged use. Table 6 and Figure 7 compare the energy consumption across the models.

The Trust-Based FCL demonstrated the lowest energy consumption, at 3.0 kWh, making it highly energy-efficient compared to HE-FL (4.8 kWh). This efficiency stems from the reduced communication overhead and the faster convergence rate, which decreases the amount of time devices need to stay active during training cycles.

In healthcare settings, where IoMT devices must operate continuously, lower energy consumption extends the operational life of these devices, reducing the frequency of recharging or replacing batteries and enhancing the system's sustainability.

The trust-based FCL framework outperformed the baseline models across key metrics such as privacy preservation, model accuracy, convergence rate, communication overhead, and energy consumption. While there is a slight increase in computational overhead, the trade-off is justified by the significant improvements in privacy, accuracy, and resource efficiency.

The framework's ability to prioritize trusted devices and efficiently manage communication ensures that it can be deployed in real-time healthcare environments where privacy, low latency, and energy efficiency are crucial. The results confirm that trust-based FCL is a robust solution for IoMT systems, providing a secure and scalable approach to federated learning.

Challenges in real-world implementation

The integration of federated learning, blockchain technology, and Q-learning introduces several complexities in practical IoMT deployments. These challenges mainly concern system complexity, communication overhead, scalability, energy efficiency, real-time data processing, and device trust management.

a) System complexity: The combination of federated learning, blockchain, and Q-learning increases the overall complexity of the system. Each layer has distinct operational requirements that must be carefully managed to ensure efficient performance.

To address this, a modular architecture can be implemented where each component operates independently but is seamlessly integrated. This reduces the risk of operational bottlenecks and allows for more manageable updates and maintenance.

b) Communication overhead: Blockchain's reliance on secure transactions and the federated learning process require frequent data exchanges, which can increase communication overhead. This issue is exacerbated as the number of IoMT devices grows. To mitigate this, techniques such as model compression and edge computing can be used to reduce the data size and transmission frequency, ensuring more efficient communication across the network.

c) Scalability: Managing large-scale IoMT networks can become challenging as more devices join the network. The scalability issue is particularly important in healthcare environments with hundreds or thousands of devices. A solution is to implement clustering techniques, where devices are grouped based on their geographical location or specific tasks, with cluster leaders managing model aggregation and blockchain transactions. This approach enhances scalability while maintaining network integrity.

d) Energy efficiency: IoMT devices, such as wearables and portable sensors, often have limited battery power. Their continuous participation in federated learning and blockchain operations can deplete energy quickly. To minimize energy consumption, energy-efficient consensus mechanisms and algorithms, such as lightweight blockchain protocols, should be implemented. These strategies reduce the computational load on devices, prolonging battery life while maintaining performance.

e) Real-time data processing: In healthcare applications, the ability to process data in real-time is critical, especially for time-sensitive tasks like emergency monitoring. The use of blockchain and federated learning can introduce delays due to the consensus and model training processes. To address this, non-critical tasks can be offloaded to edge servers, allowing critical operations to be processed locally, ensuring faster response times. Additionally, asynchronous learning methods can reduce system delays.

f) Device trust management: Trust management becomes increasingly complex as more devices are added to the network. While Q-learning helps in dynamically managing device trust, scaling this trust mechanism across a large network can result in inefficiencies. A dynamic trust adjustment mechanism based on historical performance and current interactions can help maintain an efficient and trustworthy network without significant computational costs.

By addressing these challenges with solutions such as modular architecture, clustering, energy-efficient protocols, and trust management strategies, the proposed framework becomes more feasible for large-scale, real-world IoMT deployments. These enhancements ensure that the system remains secure, scalable, and efficient, even in complex healthcare environments.

Conclusion and future works

The trust-based federated convivial learning (FCL) framework has demonstrated significant improvements in privacy protection (92.4%) and model accuracy (94.7%) compared to traditional methods, making it a strong candidate for secure and efficient IoMT healthcare solutions. By integrating blockchain and trust mechanisms, the framework ensures secure, decentralized learning, which is critical for handling sensitive medical data.

However, the framework's scalability in large-scale IoMT networks with many devices requires further validation. Future work should focus on optimizing the framework to manage communication overhead and computational efficiency in such environments. Addressing these challenges is essential for broader adoption in real-world healthcare settings. In summary, while the trust-based FCL framework sets a new standard in privacy and accuracy, enhancing its scalability and efficiency will be key to its success in larger, more complex IoMT networks.

REFERENCES

Almalki, J., Al Shehri, W., Mehmood, R., Alsaif, K., Alshahrani, S. M., Jannah, N., & Khan, N. A. (2022). Enabling blockchain with IoMT devices for healthcare. *Information*, *13*(10), 448. https://doi.org/10.3390/info13100448

Bano, S., Tonellotto, N., Cassarà, P., & Gotta, A. (2023). Artificial intelligence of things at the edge: Scalable and efficient distributed learning for massive scenarios. *Computer Communications, 205*, 45-57. https://doi.org/10.1016/j.comcom.2023.04.010

Belhadi, A., Holland, J. O., Yazidi, A., Srivastava, G., Lin, J. C., & Djenouri, Y. (2023). BIoMT-ISeg: Blockchain internet of medical things for intelligent segmentation. *Frontiers in Physiology, 13*, 1097204. https://doi.org/10.3389/fphys.2022.1097204

Dhasarathan, C., Hasan, M. K., Islam, S., Abdullah, S., Khapre, S., Singh, D., Alsulami, A.A., & Alqahtani A. (2023). User privacy prevention model using supervised federated learning-based blockchain approach for the Internet of Medical Things. *CAAI Transactions on Intelligence Technology*. https://doi.org/10.1049/cit2.12218

Gajarawala, S. N., & Pelkowski, J. N. (2021). Telehealth

benefits and barriers. *Journal of Nurse Practitioners, 17*(2), 218-221. https://doi.org/10.1016/j.nurpra.2020.09.013

Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. *Artificial Intelligence in Healthcare,* 295–336. https://doi.org/10.1016/B978-0-12-818438-7.00012-5

Ghosh, P. K., Chakraborty, A., Hasan, M., Rashid, K., & Siddique, A. H. (2023). Blockchain application in healthcare systems: A review. *Systems, 11*(1), 38. https://doi.org/10.3390/systems11010038

Hai, T., Zhou, J., Srividhya, S. R., Jain, S. K., Young P., & Arawal S. (2022). BVFLEMR: An integrated federated learning and blockchain technology for cloud-based medical records recommendation system. *Journal of Cloud Computing*, *11*(22). https://doi.org/10.1186/s13677-022-00294-6

Jain, S., Anand, A., Gupta, A., Awasthi, K., Gujrati, S., & Channegowda, J. (2020). Blockchain and machine learning in health care and management. In International Conference on Mainstreaming Block Chain Implementation (ICOMBI), Bengaluru, India. https://doi.org/10.23919/ICOMBI48604.2020.9203483

Majeed, A., Zhang, X., & Hwang, S. O. (2022). Applications and challenges of federated learning paradigm in the big data era with special emphasis on COVID-19. *Big Data and Cognitive Computing*, *6*(4), 127. https://doi.org/10.3390/bdcc6040127

Mohammed, A. (2023). Blockchain-assisted cybersecurity in medical things using artificial intelligence. *Electronic Research Archive*, *31*(2), 708-728. https://doi.org/10.3934/era.2023035

Murugeshwari, B., Rajalakshmi, S., & Sudharson, K. (2023). Hybrid approach for privacy enhancement in data mining using arbitrariness and perturbation. *Computer Systems Science and Engineering, 44*(3), 2293–2307. https://doi.org/10.32604/csse.2023.029074

Neelakandan, S., Beulah, J. R., Prathiba, L., Murthy, G. L. N., Raj, E. F. I., & Arulkumar, N. (2022). Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model. *Internatuional Journal of Modeling, Simulation, and Scientific Computing, 13*(4), 2241006. https://doi.org/10.1142/s1793962322410069

Nguyen, T. V., Dakka, M. A., Diakiw, S. M., VerMilyea, M. D., Perugini, M., Hall, J. M. M., & Perugini, D. (2022). A novel decentralized federated learning approach to train on globally distributed, poor quality, and protected private medical data. *Scientific Reports*, *12*(1). https://doi.org/10.1038/s41598-022-12833-x

Rafique, W., Khan, M., Khan, S., & Ally, J. S. (2023). SecureMed: A blockchain-based privacy-preserving framework for Internet of Medical Things. https://doi.org/10.1155/2023/2558469

Rahmani, M. K. I., Shuaib, M., Alam, S., Siddiqui, S. T., Ahmad, S., Bhatia, S., & Mashat, A. (2022). Blockchain-based trust management framework for cloud computing-based Internet of Medical Things (IoMT): A systematic review. *Computational Intelligence and Neuroscience, 2022, 1*, 766844. https://doi.org/10.1155/2022/9766844

Rani, S., Kataria, A., Kumar, S., & Tiwari, P. (2023). Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review. *Knowledge-Based Systems*, 274, 110658. https://doi.org/10.1016/j.knosys.2023.110658

Soner, S., Litoriya, R., & Pandey, P. (2022). Combining blockchain and machine learning in healthcare and health informatics: An exploratory study. In S. Tanwar (Ed.), Blockchain Applications for Healthcare Informatics, 117-135. Academic Press. https://doi.org/10.1016/B978-0-323-90615-9.00014-1

Srivastava, J., Routray, S., Ahmad, S., & Waris, M. M. (2022). Internet of Medical Things (IoMT)-Based smart healthcare system: Trends and progress. *Computational Intelligence and Neuroscience*, 2022, 7218113. https://doi.org/10.1155/2022/7218113

Sudharson, K., & Arun, S. (2022). Security protocol function using quantum elliptic curve cryptography algorithm. *Intelligent Automation & Soft Computing*, 34(3), 1769–1784. https://doi.org/10.32604/iasc.2022.026483

Sudharson, K., Akshaya, M., Lokeswari, M., & Gopika, K. (2022). Secure authentication scheme using CEEK technique for trusted environment. International Mobile and Embedded Technology Conference (MECON), Noida, India. https://doi.org/10.1109/MECON53876.2022.9752245

Sudharson, K., Sermakani, A. M., Parthipan, V., Dhinakaran, D., Petchiammal, G. E., & Usha, N. S. (2022). Hybrid deep learning neural system for brain tumor detection. In 2nd International Conference on Intelligent Technologies (CONIT), Hubli, India. https://doi.org/10.1109/CONIT55038.2022.9847708

Veerasathpurush Allareddy, S., Rampa, S., Venugopalan, S. R., Elnagar, M. H., Lee, M. K., Oubaidin, M., & Yadav, S. (2023). Blockchain technology and federated machine learning for collaborative initiatives in orthodontics and craniofacial health. *Orthodontics & Craniofacial Research*, *00*, 1-6. https://doi.org/10.1111/ocr.12662

Wael Issa, N., Moustafa, B. T., Turnbull, B., Sohrabi, N., & Tari, Z. (2023). Blockchain-based federated learning for securing Internet of Things: A comprehensive survey. *ACM Computing Surveys, 55*(9), 191. https://doi.org/10.1145/3560816

Wagan, S. A., Koo, J., Siddiqui, I. F., Attique, M., Shin, D. R., & Qureshi, N. M. F. (2022). Internet of medical things and trending converged technologies: A comprehensive review on real-time applications. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 9228–9251. https://doi.org/10.1016/j.jksuci.2022.09.005

Wang, R., Lai, J., Zhang, Z., Li, X., Vijayakumar, P., & Karuppiah, M. (2023). Privacy-preserving federated learning for Internet of Medical Things under edge computing. *IEEE Journal of Biomedical and Health Informatics*, *27*(2), 854-865. https://doi.org/10.1109/JBHI.2022.3157725

Wang, W., Gadekallu, T. R., Alazab, M., & Hemanth, J. (2023). Guest editorial: Federated learning for privacy preservation of healthcare data in Internet of Medical Things and patient

monitoring. *IEEE Journal of Biomedical and Health Informatics*, *27*(2), 648-651. https://doi.org/10.1109/JBHI.2023.3234604

Wenkang, L., He, Y., Wang, X., Duan, Z., Liang, W., & Liu, Y. (2023). BFG: Privacy protection framework for the Internet of Medical Things based on blockchain and federated learning. *Connection Science*, *35*(1). https://doi.org/10.1080/09540091.2023.2199951

Yan, Y., Kamel, M. B. M., Zoltay, M., Gál, M., Hollós, R., Jin, Y., Péter, L., & Tényi A. (2023). Fedlabx: A practical and privacy-preserving framework for federated learning. *Complex Intelligent Systems*. https://doi.org/10.1007/s40747-023-01184-3

Zheng, Y., Lai, S., Liu, Y., Yuan, X., Yi, X., & Wang, C. (2023). Aggregation service for federated learning: An efficient, secure, and more resilient realization. *IEEE Transactions on Dependable and Secure Computing. h*ttps://doi.org/10.1109/tdsc.2022.3146448