Order No.: .....

The People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

UNIVERSITY OF MOHAMED BOUDIAF - M'SILA

FACULTY OF MATHEMATICS AND COMPUTER SCIENCES

COMPUTER SCIENCES DEPARTMENT

THESIS

Presented with a view to obtaining the degree of

LMD Ph.D

Field : Computer Science

Speciality : Computer Systems

Presented By :

Wafa Bouras

Supervisor :

Benouis Mohamed

ENTITLED

IoMT-Enabled 5G for Patient Identification

A Resilient Blockchain-Based Federated Learning Framework for Optimized and Secure Participant Selection

Defended on : 04 / 11 / 2025

Before the jury composed of:

Said Gadri	MCA	University of M'sila	**President**
Mohamed Benouis	MCA	University of M'sila	**Supervisor**
Nasser Eddine Mouhoub	MCA	University of M'sila	**Examiner**
Abdelouahab ATTIA	professor	University of Bordj Bou Arreridj	**Examiner**
Farid Nouioua	professor	University of Bordj Bou Arreridj	**Examiner**
Samir Akhrouf	professor	University of M'sila	**Guest**

Academic year : 2024-2025

ACKNOWLEDGMENT

First and foremost, I express my deepest gratitude to **Allah Almighty**, whose infinite mercy and guidance have sustained me throughout this journey.

I would like to thank my supervisor, **Dr. Benouis Mohamed**, for his guidance and support during the course of this thesis.

I am also deeply thankful to **Professor Samir Akhrouf** and **Professor heraguemi kamel eddine**, whose insightful advice, consistent support, and mentorship throughout the years have greatly contributed to both my academic progress and personal development.

My gratitude extends to **all the professors and staff of this esteemed institution**, whose dedication to teaching and research has enriched my academic experience.

I would also like to sincerely thank the members of the examination committee for dedicating their time to reviewing my thesis and for providing valuable feedback.

Finally, I would like to express my heartfelt appreciation to my family. Special thanks to my beloved parents, for their unconditional love, prayers, and unwavering belief in me. I am equally grateful to my siblings, **Amine**, **Imene**, and **Aymen Salim**, for their constant encouragement and support.

ABSTRACT

The Internet of Medical Things (IoMT) has revolutionized modern healthcare by enabling continuous monitoring and real-time data exchange among medical devices. However, the heterogeneity of data sources, limited computational resources, and increasing security threats pose significant challenges to the deployment of intelligent and privacy-preserving solutions.

This thesis proposes an enhanced framework that integrates Federated Learning (FL) with lightweight blockchain consensus mechanisms to address key issues in participant selection and system robustness. A comparative study of existing participant selection methods is presented, followed by the design of a refined probabilistic model that balances optimization and privacy. Furthermore, we introduce a blockchain-assisted role assignment mechanism to improve transparency and trust among distributed participants.

The proposed framework, BlockGuard-RD, is evaluated against various threat scenarios such as data poisoning, impersonation, and denial-of-service (DoS) attacks. Experimental results demonstrate the framework's ability to enhance model accuracy, improve resource efficiency, and maintain high security standards within IoMT environments.

Ultimately, this work contributes a robust and adaptive solution for secure, scalable, and privacy-aware machine learning in medical cyber-physical systems.

Key Words: Federated learning, Internet of Medical Things, participant selection, Privacy levels, optimization levels

RÉSUMÉ

L'Internet des objets médicaux (Internet of Medical Things, IoMT) a profondément transformé le domaine de la santé moderne en permettant la surveillance continue et l'échange de données en temps réel entre dispositifs médicaux. Toutefois, l'hétérogénéité des sources de données, les ressources de calcul limitées et la multiplication des menaces de sécurité constituent des défis majeurs pour le déploiement de solutions intelligentes et respectueuses de la confidentialité.

Cette thèse propose une plateforme améliorée intégrant l'apprentissage fédéré (Federated Learning, FL) à des mécanismes de consensus blockchain allégés, afin de résoudre les principaux problèmes liés à la sélection des participants et à la robustesse du système. Une étude comparative des méthodes existantes de sélection des participants est présentée, suivie de la conception d'un modèle probabiliste affiné conciliant optimisation et préservation de la vie privée. De plus, un mécanisme d'attribution de rôles assisté par blockchain est introduit pour renforcer la transparence et la confiance entre les participants distribués.

La plateforme proposée, nommée BlockGuard-RD, est évaluée dans divers scénarios de menace tels que l'empoisonnement des données, l'usurpation d'identité et les attaques par déni de service (DoS). Les résultats expérimentaux démontrent la capacité de cette structure à améliorer la précision des modèles, à optimiser l'utilisation des ressources et à maintenir des standards de sécurité élevés dans les environnements IoMT.

En définitive, cette thèse contribue à la conception d'une structure robuste et adaptative pour un apprentissage automatique sécurisé, évolutif et respectueux de la confidentialité au sein des systèmes cyber-physiques médicaux.

Mots-clés : Apprentissage fédéré, Internet des objets médicaux, sélection des participants, confidentialité, optimisation

ملخص

لقد غيَّرت إنترنت الأشياء الطبية مجال الرعاية الصحية الحديثة من خلال تمكين المراقبة المستمرة وتبادل البيانات في الوقت الحقيقي بين الأجهزة الطبية. ومع ذلك، فإن تباين مصادر البيانات، وقيود الموارد الحاسوبية، والتهديدات الأمنية المتزايدة تطرح تحديات كبيرة أمام تنفيذ حلول ذكية تحافظ على الخصوصية.

تقترح هذه الأطروحة هيكلًا مُحسَّنًا يدمج التعلم الفيدرالي مع آليات توافق خفيفة تعتمد على سلسلة الكتل لمعالجة المشكلات الرئيسية في اختيار المشاركين وصلابة النظام. يتم تقديم دراسة مقارنة لأساليب اختيار المشاركين الحالية، تليها تصميم نموذج احتمالي محسَّن يوازن بين التحسين وحماية الخصوصية. علاوة على ذلك، نقترح آلية لتوزيع الأدوار بمساعدة سلسلة الكتل من أجل تعزيز الشفافية والثقة بين المشاركين الموزعين.

تم تقييم الهيكل المقترح في مواجهة تهديدات مثل تسميم البيانات، والانتحال، والهجمات الحرمانية من الخدمة. وتُظهر النتائج التجريبية قدرته على تحسين دقة النماذج، وكفاءة استخدام الموارد، مع الحفاظ على معايير أمان عالية في بيئات إنترنت الأشياء الطبية.

في الختام، تساهم هذه الأطروحة في تقديم حل قوي وقابل للتكيف من أجل تعلم آلي آمن وقابل للتوسع ويراعي الخصوصية في الأنظمة السيبرانية-الفيزيائية الطبية.

الكلمات المفتاحية: التعلم الفيدرالي، إنترنت الأشياء الطبية، اختيار المشاركين، مستويات الخصوصية، مستويات التحسين.

LIST OF FIGURES

LIST OF TABLES

List of Publications

Journal Articles

- – *Title:* **Optimizing Security and Performance in Blockchain-Enhanced Federated Learning Through Participant Selection with Role Determination.**
  – *Authors:* Wafa Bouras, Kamel Eddine Heraguemi, Mohamed Benouis, Brahim Bouderah, and Samir Akhrouf.
  – *Journal: Computing and Informatics*, **44**(3), 682–716.
  – *Publisher:* Slovak Academy of Sciences.
  – *DOI:* `https://doi.org/10.31577/cai_2025_3_682`
  – *Year:* 2025.

Conference Papers

- – *Title:* **Analysis Study of Participant Selection Methods in Federated Learning.**
  – *Authors:* Wafa Bouras, Mohamed Benouis, Kamel Eddine Heraguemi, Brahim Bouderah, and Samir Akhrouf.
  – *Conference:* 2024 2nd International Conference on Electrical Engineering and Automatic Control (ICEEAC).
  – *Location:* Setif, Algeria.
  – *Publisher:* IEEE.
  – *Pages:* 1–6.
  – *DOI:* `https://doi.org/10.1109/ICEEAC61226.2024.10576424`
  – *Keywords:* Performance evaluation, Electrical engineering, Correlation, Federated learning, Hardware, Servers, Faces, Security, Participant selection, Machine learning.
  – *Year:* 2024.

List of Abbreviations

Abbreviation	Full Form
2FA	Two-Factor Authentication
5G	Fifth Generation
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
ACLF	Assistive Care Loop Framework
AFL	Active Federated Learning
AI	Artificial Intelligence
BAN	Body Area Network
BlockGuard-RD	Blockchain-enabled Guard with Role Determination
Biometrics	Biometric Verification
BVP	Blood Volume Pulse
CPU	Central Processing Unit
COVID-19	Coronavirus Disease 2019
DDOS	Distributed Denial-of-Service
DGRU	Deep Gated Recurrent Units
DICOM	Digital Imaging and Communications in Medicine
Diffie-Hellman	Diffie-Hellman Key Exchange
DP	Differential Privacy
EDA	Electrodermal Activity
ECG	Electrocardiogram
EHR	Electronic Health Record
FedAvg	Federated Averaging
FedMeta	Federated Meta-Learning
FedNova	Federated Nova
FedProx	Federated Proximal
FedShare	Federated Sharing

FL	Federated Learning
GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
HFL	Horizontal Federated Learning
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level 7
Huffman Encoding	Huffman Encoding Algorithm
IaaS	Infrastructure as a Service
IID	Independently and Identically Distributed
IoMT	Internet of Medical Things
IoT	Internet of Things
LPWAN	Low-Power Wide-Area Network
MEC	Mobile Edge Computing
Non-IID	Non-Independently and Identically Distributed
Oort	Optimized Synchronous Participant Selection Framework
OpenEHR	Open Electronic Health Record
PaaS	Platform as a Service
PoS	Proof of Stake
PoW	Proof of Work
RAM	Random Access Memory
RDM	Role Determination Module
RNN	Recurrent Neural Network
SaaS	Software as a Service
SGD	Stochastic Gradient Descent
VFL	Vertical Federated Learning
WESAD	Wearable Stress and Affect Detection
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
ZigBee	ZigBee Wireless Communication Protocol
ZKP	Zero-Knowledge Proof

TABLE OF CONTENTS

General Introduction

Introduction

The Internet of Medical Things (IoMT) signifies a profound intersection between healthcare and advanced digital technologies, resulting in a sophisticated network of interconnected medical devices, sensors, and applications. These systems are designed to collect, process, and transmit health-related data in real time, thereby enabling continuous patient monitoring, personalized diagnostics, and the provision of remote medical services. This integration not only enhances the quality and accessibility of healthcare delivery but also contributes to cost reduction and operational efficiency.

However, the realization of IoMT's full potential is contingent upon the secure, efficient, and privacy-preserving management of vast quantities of sensitive data. Several challenges impede this goal, including data heterogeneity, limited computational resources of edge devices, strict privacy requirements, and significant communication overheads. To address these obstacles, the combined application of Federated Learning (FL) a decentralized machine learning paradigm and blockchain technology has emerged as a promising solution. FL enables collaborative model training without the need to centralize raw data, while blockchain provides transparency, immutability, and trust among participating entities.

Motivation and Gap Identification

Despite considerable advancements, existing FL-based IoMT frameworks frequently exhibit shortcomings in their participant selection methodologies. Specifically, reliance on arbitrary or static client selection can result in suboptimal learning outcomes, inefficient resource utilization, and heightened susceptibility to adversarial attacks. Furthermore, many current approaches inadequately address the dynamic and heterogeneous characteristics of IoMT environments, where devices differ significantly in terms of availability, reliability, and data quality.

Although blockchain technology has been widely adopted to enhance data integrity and trust in FL systems, its potential to directly improve participant selection processes

remains insufficiently explored. This observation highlights a critical research gap: the necessity for a secure, adaptive, and intelligent participant selection mechanism that is both privacy-aware and resilient to the unique threats prevalent in IoMT contexts.

Key Research Gap

A principal limitation of current Federated Learning implementations within IoMT is the inefficiency associated with random or uniform participant selection strategies. Empirical evidence suggests that judicious selection of participating clients can substantially enhance model convergence rates, system stability, and overall performance.

To address this gap, the present thesis is guided by the following central research questions:

- **Optimal Participant Selection:** What strategies can be employed to develop an intelligent, resource-aware participant selection algorithm that optimizes training efficiency and model accuracy?
- **Blockchain Integration:** In what ways can the participant selection process be seamlessly integrated into a blockchain-based infrastructure to ensure decentralization, trust, and tamper resistance?
- **Security and Resilience:** How can the proposed selection mechanism be designed to strengthen robustness against prevalent attacks such as data poisoning, impersonation, and denial-of-service (DoS) within IoMT networks?

By systematically addressing these questions, this research aspires to establish a comprehensive framework for the secure, privacy-preserving, and performance-optimized deployment of FL in healthcare environments.

Thesis Structure

The thesis is organized into four chapters, each focusing on a key aspect of the proposed research:

- **Chapter 1: Introduction to IoMT** — Provides an overview of the IoMT paradigm, detailing its architecture and the principal challenges related to data privacy, system scalability, and the integration of FL and blockchain technologies in healthcare. The chapter also delineates the research problem and objectives.

- **Chapter 2: Comparative Study of Participant Selection Methods** — Describes the experimental framework and offers an in-depth analysis of existing FL participant selection strategies, highlighting their limitations and establishing the rationale for a novel approach.
- **Chapter 3: Proposed Participant Selection Method** — Introduces a novel probabilistic algorithm for participant selection that balances optimization objectives with privacy considerations. This chapter also presents a block-chain -assisted role assignment mechanism to reinforce transparency and security.
- **Chapter 4: Enhanced Framework with Attack Resistance** — Details the Block-Guard-RD framework, which incorporates dynamic, role-based access control and robust defense mechanisms against major IoMT-specific threats. The chapter concludes with a comprehensive evaluation of the framework's performance, privacy, and security attributes.

In conclusion, this thesis seeks to advance the state of the art by proposing a robust and adaptive framework for secure and efficient participant selection in FL-enabled IoMT systems, thereby facilitating the trustworthy deployment of such technologies in real-world healthcare settings.

Chapter 1: Introduction to IoMT

1.1 Introduction

The COVID-19 pandemic has significantly increased the demand for remote patient monitoring, leading to the widespread adoption of the Internet of Medical Things (IoMT). While IoMT improves healthcare by enabling real-time data collection and analysis, it also introduces critical challenges related to security, privacy, and system resilience.

To address these concerns, Federated Learning (FL) offers a decentralized approach to model training, ensuring that sensitive patient data remains protected. However, the effectiveness of FL relies on the selection of appropriate participants, a process that becomes even more complex when incorporating blockchain technology for enhanced security and trust management.

This chapter provides an overview of IoMT systems and their associated challenges while examining the role of FL and blockchain in strengthening security. Additionally, it highlights the importance of optimized participant selection in healthcare applications to ensure efficient and trustworthy model training.

1.2 Overview of IoMT Systems and Their Challenges

1.2.1 Definition of IoMT Systems

The Internet of Medical Things (IoMT) is a specialized domain within the broader Internet of Things (IoT) that focuses on healthcare, a critical aspect of human well-being. It encompasses various components, including:

- **Medical Sensors and Devices** – These range from basic body sensors to advanced surgical tools, collecting and transmitting biomedical data. [1]
- **Communication Networks and Secure Channels** – These facilitate secure interactions between patients, medical staff, and healthcare facilities. [2]

- **Distributed Information Technology Systems** – These enable the creation, access, and management of electronic health records. [3]
- **Healthcare-Oriented Services and Applications** – These support patient care through interactive digital tools and healthcare services. [4]

1.2.2 IoMT System Architecture

IoMT is a specialized subset of IoT, designed to meet the stringent requirements of healthcare environments. While general IoT architectures range from the traditional three-layer model (perception, network, application) to more complex five- and seven-layer frameworks, IoMT typically adopts a streamlined four-layer architecture. This model is widely recognized for its ability to balance efficient data acquisition, secure communication, intelligent processing, and user-centric delivery [5, 6, 7, 8, 9, 10].

This four-layer structure enables seamless end-to-end integration facilitating real-time data collection, secure transmission, advanced analytics, and clinical usability. It also supports interoperability and scalability, both of which are essential for modern healthcare systems. The layers are defined as follows:

- **Perception Layer (Sensing Layer):** This foundational layer comprises medical sensors, wearable devices, and smart implants that continuously collect physiological and biometric data from patients. Typical parameters monitored include heart rate, blood pressure, glucose levels, and body temperature. Advanced imaging tools and remote monitoring systems are also included, enabling comprehensive and real-time healthcare diagnostics [6].
- **Network Layer:** This layer is responsible for the reliable and secure transmission of medical data. It connects IoMT devices to healthcare networks using diverse communication technologies such as Bluetooth, Wi-Fi, 5G, and Low-Power Wide-Area Networks (LPWAN). Protocols like 6LoWPAN facilitate efficient IPv6-based communication over low-power wireless networks, ensuring seamless data flow between devices and healthcare infrastructure [5].
- **Processing Layer (Edge/Fog/Cloud Computing Layer):** Critical for real-time analytics and decision-making, this layer consists of:
  - **Edge Computing:** Local data processing on devices or nearby nodes, minimizing latency and reducing bandwidth usage.
  - **Fog Computing:** Acts as an intermediary, performing localized processing before forwarding data to the cloud, thereby enhancing security and efficiency.

  - **Cloud Computing:** Offers scalable storage, advanced analytics, machine learning, and remote access for healthcare providers [7].

- **Application Layer:** The topmost layer delivers user interfaces and applications for healthcare professionals and patients. It encompasses electronic health record (EHR) systems, telemedicine platforms, AI-driven diagnostic tools, and mobile health apps. This layer ensures intuitive access to processed data, supporting informed clinical decision-making and improved patient care [8].

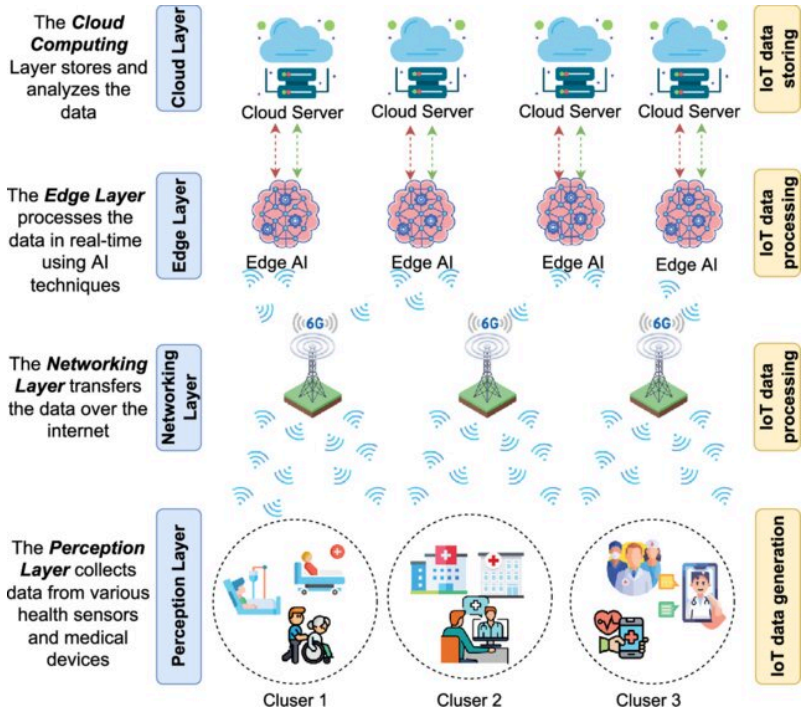

Figure 1.1 The four-layer IoMT system architecture [11]

This structured architecture, as represented in Figure 1.1, ensures that IoMT systems are scalable, secure, and capable of supporting diverse healthcare applications such as remote patient monitoring and AI-driven diagnostics. Nevertheless, challenges remain particularly in the areas of data privacy, security, and interoperability which necessitate ongoing advancements and innovations in IoMT technologies [9].

1.2.3 Introduction to Advanced Technologies in IoMT Systems

Given the critical role of IoMT systems in modern healthcare enabling remote monitoring, diagnosis, and continuous patient care the integration of advanced technologies is indispensable. These technologies enhance system efficiency, promote equitable healthcare access, and improve overall reliability. By leveraging such innovations, IoMT can deliver more secure, intelligent, and adaptive healthcare solutions [12].

A fundamental aspect of IoMT systems is the nature of IoMT devices themselves as it appears on Figure 1.2, which serve as essential components within the broader healthcare infrastructure [13]. These devices are responsible for the real-time collection, processing, and transmission of patient data [14]. Structurally, an IoMT device comprises both hardware and software elements: the hardware includes sensors, and communication modules, while the software manages data processing, security enforcement, and interoperability within healthcare networks [15, 12, 13]. The seamless integration of these components ensures effective system operation, enabling continuous monitoring and intelligent decision-making [15].

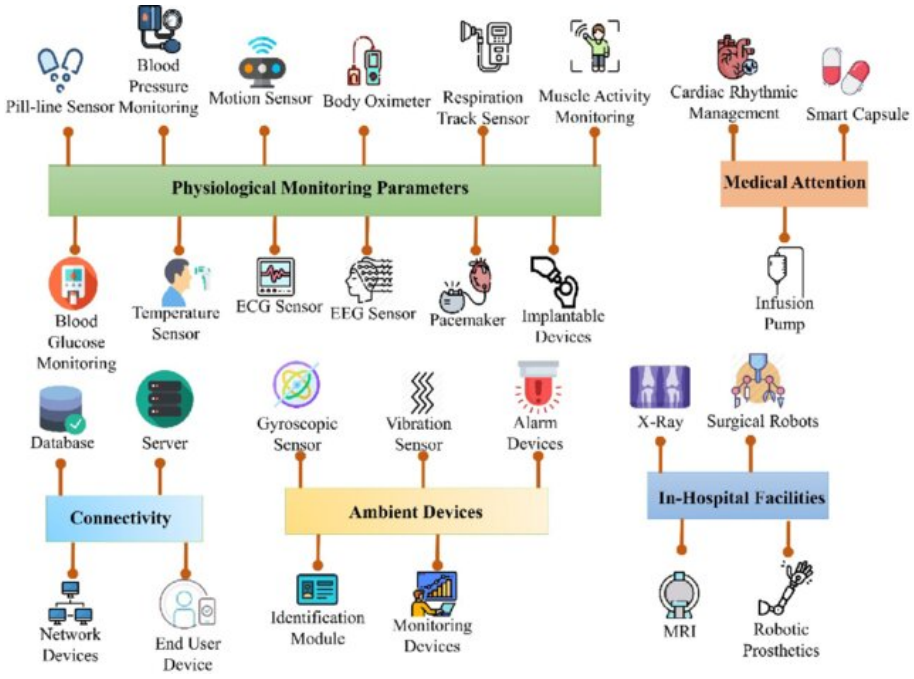

Figure 1.2 Categories of IoMT devices according to [14]

However, IoMT devices exhibit significant heterogeneity in hardware and software configurations, arising from differences in manufacturers, operating systems, communication protocols, and functional capabilities [16]. This heterogeneity means that only subsets of devices within a network share common characteristics, necessitating selective integration strategies. Effectively addressing this heterogeneity is vital for ensuring interoperability, optimizing data flow, and enhancing the efficacy of advanced technologies within IoMT ecosystems.

Federated Learning

Among the advanced technologies recently integrated into IoMT systems, *federated learning (FL)* has emerged as a foundational approach to address privacy, data locality, and

real-time intelligence. It represents one of the first privacy-preserving machine learning techniques adopted in healthcare-oriented IoMT infrastructures, enabling collaborative model training without the need to share sensitive patient data.

Originally introduced in [17], FL allows multiple edge devices to train local models on-device and share only the resulting updates. These updates are then aggregated to form a global model, as illustrated in Figure 1.3, significantly reducing the risks associated with data transmission and centralized storage. To implement FL effectively, two primary

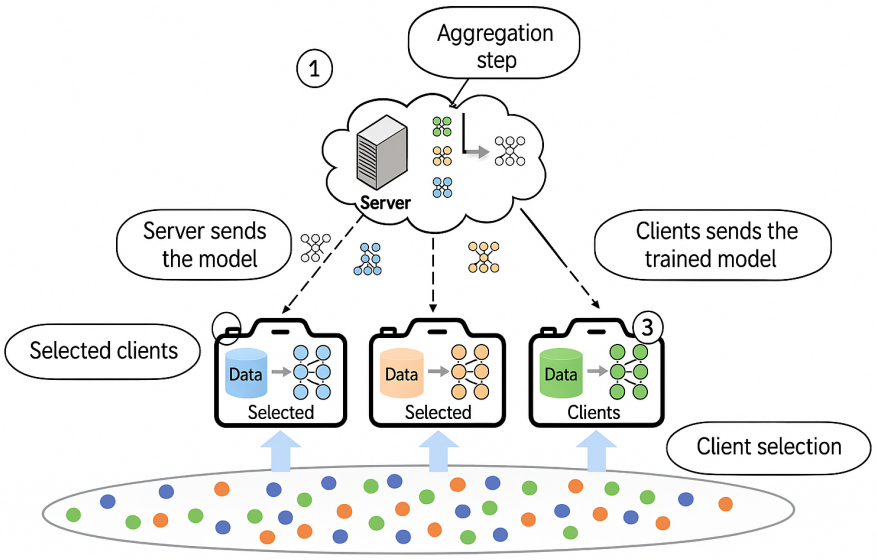

Figure 1.3 Overview of the FL Workflow

architectural approaches have emerged, as illustrated in Figure 1.4:

- **Centralized Method:** A central server acts as an intermediary, collecting model updates from clients and aggregating them using various algorithms. This approach ensures that raw data remains on client devices, with only model parameters exchanged [17].
- **Decentralized Method:** In this approach, training and decision-making occur collaboratively among peer nodes rather than being coordinated by a central server. This decentralized coordination is often achieved through integration with blockchain technologies, which provide a secure infrastructure based on distributed ledgers and consensus mechanisms. Such integration not only eliminates the reliance on a single point of control but also enhances system transparency, resilience, and data integrity [18, 19].

Both approaches are applicable in IoMT contexts, where preserving data privacy while maintaining model quality is paramount. However, the unique characteristics of IoMT

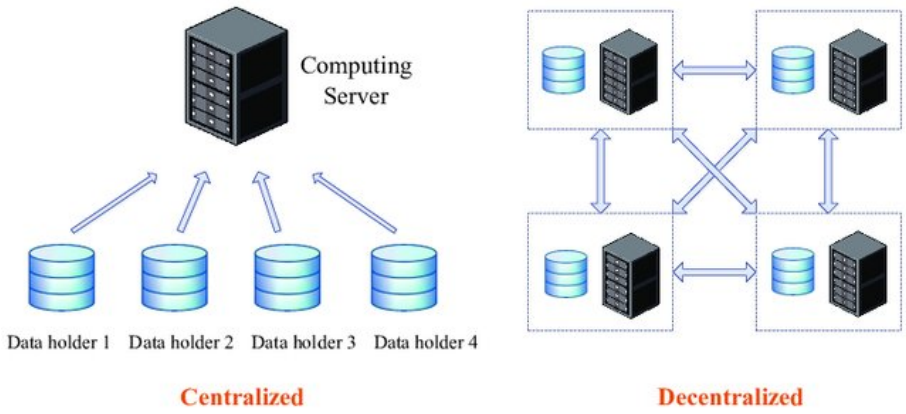

Figure 1.4 Basic differences between centralized and decentralized FL [20]

environments such as device heterogeneity and dynamic connectivity require more than architectural design. In particular, the process of *client selection* becomes a central challenge.

Before training can begin in FL approaches, a crucial preliminary step called *client selection* is typically performed as the figure1.3 shows. This process determines which devices will participate in each training round and directly influences both training efficiency and overall model performance. Selection strategies can be random as in the widely adopted FedAvg algorithm [17] or pattern-based, as explored in [21, 22]. In IoMT scenarios, effective selection prioritizes devices with strong computational capabilities, reliable battery life, and robust network connectivity, while excluding resource-constrained or unreliable nodes.

Building on this, recent research has sought to improve training efficiency by addressing limitations such as gradient bias and inconsistent objective distributions. For instance, [23] proposed mathematical refinements to the FedAvg algorithm to overcome these challenges. Comparative experiments demonstrated that algorithms like FedMeta outperform traditional approaches such as FedShare, FedProx, and FedAvg in terms of accuracy. Notably, FedProx [18] introduces mechanisms to handle system and network heterogeneity, thereby increasing robustness across diverse IoMT deployments.

Another fundamental component in FL is the *aggregation* step as on figure 1.3, where model updates from selected clients are combined to generate the next global model iteration. The quality and accuracy of the final model heavily depend on the effectiveness of this process. In centralized settings, aggregation is typically performed using algorithms like FedAvg [24], FedNova [25], and FedProx [18]. In decentralized systems, alternative methods such as gossip-based protocols [18], cyclical weight transfer [19], and proxy model sharing [26] are explored to support aggregation without relying on a central entity. These methods are crucial for ensuring model consistency and convergence in distributed

IoMT environments.

Finally, as FL matures, *fairness* has emerged as a critical concern particularly in IoMT systems where data distribution is inherently non-uniform and client participation can be highly variable. This heterogeneity often leads to biased global models that disproportionately favor dominant data sources or frequently participating clients, while marginalizing those with smaller datasets or limited connectivity [27]. Addressing fairness requires not only algorithmic strategies such as cross-stability modeling and utility-based optimization frameworks that balance client contributions while respecting privacy constraints [28] but also systemic approaches that incentivize equitable participation and mitigate resource disparities [29]. Ensuring fairness is especially vital in healthcare contexts, where unbiased, inclusive models directly impact patient outcomes and ethical standards. In the following sections, we will explore how the nature of IoMT data and advanced security technologies further influence FL's effectiveness and trustworthiness.

Nature of Patient Data

Patient data in healthcare is inherently sensitive, heterogeneous, and distributed across multiple institutions, often subject to strict privacy regulations such as HIPAA and GDPR. These characteristics pose significant challenges for collaborative machine learning, motivating the adoption of FL paradigms that enable joint model training without sharing raw data.

Within FL, three primary strategies address different data-sharing and privacy-preservation scenarios:

- **Vertical Federated Learning (VFL):** Applicable when datasets from different parties contain complementary but non-overlapping feature sets for the same individuals (e.g., clinical records vs. genomic data). Each party retains control over its unique features, collaboratively training models to extract insights without exposing raw data. VFL is particularly valuable in multi-institutional medical research where data confidentiality is critical.

- **Horizontal Federated Learning (HFL):** Suitable when multiple entities hold datasets with similar features but distinct patient populations (i.e., different data instances). Each party trains local models on its data subset, and model updates are aggregated to enhance the global model's generalization across diverse populations. HFL is relevant for applications like distributed disease prediction across hospitals.

- **Hybrid Federated Learning:** This approach combines vertical and horizontal FL to handle complex data distributions exhibiting both feature and sample partitioning.

For example, healthcare analytics involving multiple institutions with overlapping and institution-specific patient data can leverage hybrid FL to jointly model global trends and local nuances while preserving privacy.

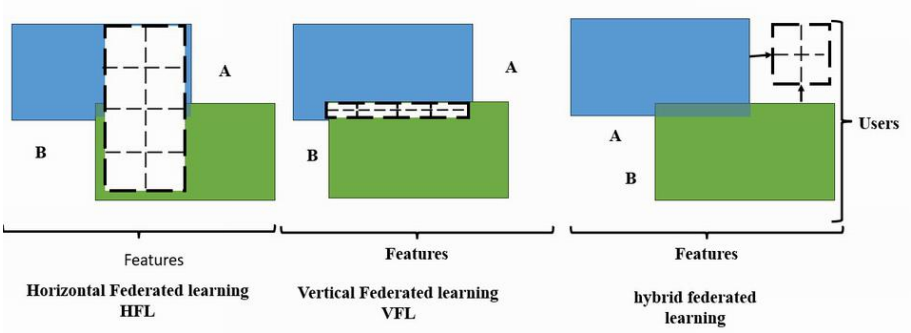

Figure 1.5 Illustration of vertical, horizontal, and hybrid FL

Security in IoMT

IoMT comprises a diverse network of medical devices, wearables, sensors, and applications that continuously collect and transmit sensitive patient data. This interconnectedness, while enabling advanced healthcare services, also introduces numerous potential entry points for cyberattacks. Such attacks threaten patient privacy, disrupt healthcare operations, and, in severe cases, can endanger lives. Effective security measures including encryption [30], two-factor authentication [31], and biometric verification [32] are essential for protecting data across the IoMT ecosystem. However, the diversity of devices, rapid technological evolution, and prevalence of legacy systems can lead to compatibility issues and expose vulnerabilities, particularly in older devices with outdated security protocols [33]. Privacy protection, enforced by regulations such as HIPAA [34], must complement these technical measures to ensure data confidentiality and integrity at all layers of IoMT.

Cryptographic Systems Robust cryptographic methods are fundamental to IoMT security. Lightweight encryption algorithms [35] are particularly important for resource-constrained devices. Protocols such as Diffie-Hellman key exchange [36], Huffman encoding [37], and homomorphic encryption [38] protect sensitive data during transmission and storage. In FL, secure aggregation methods [39] encrypt model updates, safeguarding them from interception or tampering during server-side processing.

Differential Privacy Differential privacy is integral to FL, adding controlled noise to model updates to protect individual data contributions. The privacy-utility trade-off is gov-

erned by the privacy parameter ϵ and failure probability δ:

$$\Pr[M(x) \in S] \leq \exp(\epsilon) \cdot \Pr[M(y) \in S] + \delta$$

where M is the randomized mechanism, and x and y are neighboring datasets [40, 41, 42]. This approach helps prevent information leakage, even if model parameters are exposed.

Blockchain Blockchain technology enhances IoMT security by decentralizing data management and providing tamper-resistant ledgers [43]. In IoMT, blockchain supports secure sharing of medical records, real-time monitoring, and pandemic tracking [44]. When integrated with FL, blockchain mitigates data sparsity and trust issues by enabling transparent, auditable participant selection and model update validation [45]. However, blockchain introduces computational and latency overheads that must be balanced against security gains.

Zero-Knowledge Proofs (ZKPs) ZKPs allow one party to prove the validity of information to another without revealing the underlying data. In FL, ZKPs enhance security by enabling participants to verify compliance with protocol rules while preserving privacy [46, 47, 48].

Digital Twins A digital twin is a dynamic, virtual representation of a physical IoMT device or system, updated in real-time with operational data. While primarily used for system optimization and predictive maintenance, digital twins can also contribute to security by enabling early detection of anomalies or cyber threats [49].

5G Communication

Short- and long-range communication methods are critical for smart healthcare devices. Common short-range technologies, such as Body Area Network (BAN), Wi-Fi, ZigBee, and Bluetooth, enable seamless data exchange between devices [50].

5G has transformed healthcare by enabling resource pooling, virtualization, high-performance telemedicine, and tactile internet with haptic feedback. Its higher bandwidth, ultra-low latency, and ubiquitous access expand healthcare reach, supporting applications such as remote surgery, real-time diagnostics, and continuous patient monitoring [50].

The integration of 5G with short-range wireless technologies enhances data exchange and patient experience, enabling robust, low-latency communication in IoMT environments [50].

Network Configuration Efficient network configuration is essential for IoMT devices. Frameworks like FallDeF5 leverage 5G to connect medical organizations and patients, achieving higher accuracy in fall detection using deep gated recurrent units (DGRU) and mobile edge computing (MEC) [51].

In FL, multiple communication rounds and large model updates can increase costs and delays. Improving communication efficiency through techniques such as model compression and asynchronous updates is essential to address these challenges [52].

Transmission FL transmission occurs under diverse network conditions, often with slower upload speeds and unreliable channels, leading to delays and potential model staleness [53]. 5G, with its reduced latency and high transmission speeds, enables advanced applications such as remote surgeries and fast data access in remote areas, ensuring continuous and reliable patient monitoring [54, 55].

Unreliable Channel IoMT networks face challenges from bandwidth limitations, channel noise, and transmission delays, which can impact the timeliness and accuracy of FL model updates [52]. Dynamic network architectures, especially those with mobile nodes, require adaptive strategies to manage communication bottlenecks and maintain system performance [55].

Heterogeneity in Systems The heterogeneity of medical hardware and software in IoMT necessitates frameworks that accommodate asynchronous communication and diverse data formats. FL frameworks can improve overall system performance by effectively distributing workloads across heterogeneous devices [56]. The adoption of 5G in IoMT systems is expected to address these challenges, supporting secure and optimized participant selection in FL.

Cloud Computing

Cloud computing provides scalable services such as databases, servers, and analytics over the internet. In IoMT, cloud platforms store and process medical data, supporting applications in disease prediction and technological innovation. However, challenges such as data integrity risks, energy consumption, and operational costs persist [57].

Edge Computing Edge computing brings computation closer to data sources, reducing latency and bandwidth usage. In FL, edge architectures must address heterogeneity, energy efficiency, and job offloading. Large-scale networks avoid star topologies to prevent central server overload, instead offloading tasks to capable nearby devices [58].

Fog Computing Fog computing, a decentralized extension of cloud computing, brings processing even closer to data sources, improving responsiveness and efficiency. It shares similarities with edge computing and is increasingly applied in IoMT architectures to optimize cloud benefits [59].

Scalable Environment Scalability is vital for IoMT systems, addressing both hardware and software demands. Cloud services such as IaaS, SaaS, and PaaS face unique challenges in healthcare, but scalable frameworks like the Assistive Care Loop Framework (ACLF) demonstrate promise in supporting real-time monitoring and adaptive resource management [60].

1.3 Different Challenges in Advanced Technologies

Despite the integration of advanced technologies, IoMT systems face persistent challenges particularly in healthcare, where reliability, security, and efficiency are paramount. These obstacles not only hinder the practical deployment of IoMT but also directly impact the performance and trustworthiness of FL frameworks that rely on secure, optimized participant selection [61].

1.3.1 Interoperability and Data Integration

Healthcare professionals including doctors, radiologists, pharmacists, and technicians exchange vast amounts of medical data daily. However, the lack of interoperability among IoMT systems creates significant challenges, impacting patient care and operational efficiency [61].

- **Standardization Issues:** Many systems fail to comply with standards like HL7, OpenEHR, and DICOM, leading to compatibility issues. Inconsistent data formats between hospitals and vendors can result in medical errors and delays in treatment.
- **Terminology and Ontology Differences:** Without standardized terminologies, crucial clinical information may be misinterpreted, affecting decision-making.
- **Legacy Systems:** Older proprietary healthcare systems lack integration capabilities, making it difficult to merge them with advanced IoMT and FL technologies.
- **Manual Data Management:** Paper-based records introduce inefficiencies and risks of data loss. Transitioning to cloud-based EHRs can facilitate FL but requires secure, cost-effective implementation.

- **Infrastructure and Device Optimization:** Outdated or poorly designed devices can lead to system failures, incorrect diagnostics, and compromised patient care.

To fully harness IoMT's potential, healthcare systems need standardized, well-integrated, and high-performance devices that ensure secure, accurate, and efficient data exchange across platforms.

1.3.2 Computational and Communication Constraints

The effectiveness of IoMT systems depends on their ability to process and transmit large volumes of medical data efficiently. However, computational limitations and communication bottlenecks significantly impact real-time healthcare applications [62, 63].

- **Processing Limitations:** Many IoMT devices operate on resource-constrained hardware, limiting their ability to run complex algorithms for real-time decision-making.
- **Energy Constraints:** Battery-operated sensors must balance power consumption and performance. Energy-efficient computing methods, such as edge computing, are crucial.
- **Latency and Network Reliability:** Healthcare applications demand low-latency communication to support real-time monitoring and emergency response.
- **Data Overload and Bottlenecks:** The continuous generation of high-frequency medical sensor data creates network congestion, leading to packet loss and increased delays.
- **Optimized Device Performance:** Efficient data compression and adaptive communication protocols are needed for reliable medical services.

These constraints directly affect the scalability and reliability of FL participant selection, as only devices with sufficient resources and connectivity can be trusted to participate effectively.

1.3.3 Security and Privacy Challenges

The increasing adoption of IoMT introduces significant security and privacy concerns. IoMT networks are highly vulnerable to cyber threats, including data breaches, ransomware attacks, and unauthorized access [64]. Decentralized architectures such as FL and Blockchain, while enhancing privacy, introduce new attack vectors including poisoning attacks and

model inversion threats [65]. Ensuring secure model aggregation and verifying participant authenticity are critical to maintaining system integrity. Our proposed framework addresses these issues by integrating blockchain-based participant verification and secure aggregation protocols.

1.3.4 Scalability Issues

Large-scale IoMT deployments must efficiently manage millions of connected devices while ensuring real-time data processing [66]. Distributed learning models require optimized communication protocols to handle increasing numbers of participants. Efficient resource allocation and edge computing integration are essential for minimizing latency and improving responsiveness [67]. As device counts grow, participant selection strategies must adapt to maintain performance and security.

1.3.5 Energy Efficiency and Sustainability

IoMT devices often operate under strict energy constraints due to their reliance on battery-powered systems. High computational demands, continuous data transmission, and encryption processes significantly impact power consumption [68]. Energy-efficient algorithms, optimized protocols, and low-power hardware are essential. Our framework incorporates energy-aware participant selection to balance security and computational overhead with battery life [69, 70].

These challenges ranging from limited computational capacity and energy constraints to security threats and system scalability underscore the critical importance of strategic decision-making in FL for IoMT. Among the various factors, the selection of participants for training rounds emerges as one of the most decisive. Effective participant selection not only improves model accuracy and training efficiency, but also enhances security, fairness, trust, and system resilience especially in sensitive healthcare environments.

1.4 Introduction to Participant Selection Methods

In IoMT systems utilizing FL to preserve patient data privacy, the model training process typically involves several key steps [71]:

1. **Global Model Initialization**: The central server initializes a global model and distributes it to client devices.

2. **Participant Selection**: The server selects a subset of clients to participate in each training round. While traditional selection is random, optimizing this step can significantly impact performance and security.

3. **Local Model Training**: Selected clients train the model on their local data without sharing raw patient information, ensuring privacy.

4. **Model Aggregation and Update**: Clients send their trained model updates to the central server, which aggregates them (e.g., using Federated Averaging) and updates the global model.

To support the context of our research, the following section reviews a selection of related works that have directly contributed to the conceptual and technical foundation of our study. These references highlight the current landscape of blockchain-assisted FL, particularly within IoMT environments, and outline the limitations in existing frameworks that our proposed BlockGuard-RD framework aims to address.

1.5 Related Works

This section reviews the current state of research relevant to enhancing security, privacy, and efficiency in FL systems, with particular emphasis on client selection strategies, blockchain integration, and challenges in IoMT environments. The survey highlights existing approaches, their limitations, and the motivation for the proposed BlockGuard-RD framework.

1.5.1 Client Selection Strategies in FL

Client selection significantly impacts the performance, convergence, and resource utilization of FL systems. Various approaches have been proposed to address heterogeneity, energy constraints, and security concerns.

- **Reputation and Heterogeneity-Aware Methods** Reputation-based frameworks such as PIRATE [72] employ consortium blockchains to decentralize trust management, improving client reliability in FL. Centralized approaches like Oort [21] optimize participant selection based on processing speed and accuracy, while PISCES [73] extends this with asynchronous updates to mitigate straggler effects, albeit with limited privacy guarantees. AFL [74] incorporates differential privacy to balance data utility and communication efficiency. Hermes [75] focuses on structured pruning

and communication-aware grouping to enhance FL personalization on mobile devices. Other works [76, 77] adapt client selection frequency and reputation scoring to accommodate low-capacity and non-IID data clients, respectively.

- **Blockchain-Enabled Participant Selection** Blockchain technology has been leveraged to enhance transparency and trust in client selection. For example, [78] uses blockchain consensus to evaluate client trustworthiness, while Lotto [79] combines random and informed selection mechanisms secured by blockchain. Additional works [80, 81] utilize smart contracts and zero-knowledge proofs to enforce privacy-preserving and auditable selection processes.

- **Energy-Aware and Security-Focused Methods** Energy efficiency is addressed in methods like REWAFL [82], which considers residual energy and wireless conditions for participant optimization in decentralized FL. Security enhancements include VerifyNet [83], which verifies server outputs under dropout scenarios, and FedRank [84], employing imitation learning to rank clients by contribution, improving convergence and reducing energy consumption.

- **Adaptive Resource Management** Techniques such as SAM [85] and FLOAT [86] apply selective model uploads and multi-objective reinforcement learning to mitigate communication bottlenecks and reduce client dropouts in heterogeneous FL environments.

- **Reputation and Privacy Enhancements** Frameworks like FedCure [87] and PI-RATE [72] integrate blockchain-based reputation scoring and edge computing to improve latency and privacy in IoMT FL applications.

- **Defense Against Adversarial Behavior** Lotto [79] secures FL against adversarial clients by combining blockchain-facilitated selection with informed randomness, enhancing robustness.

1.5.2 Security and Privacy Mechanisms in FL

Ensuring privacy and robustness remains a critical challenge in FL.

- **Dynamic Client Selection and Privacy** SLMFed [88] introduces stage-based learning for dynamic client selection, while FLIPS [89] enhances efficiency through intelligent participant choice. Differential privacy is integrated in IIoT-FL scenarios with blockchain-based aggregation in dp_homm [90]. Taxonomies assessing FL trustworthiness by privacy, fairness, and accountability are proposed in [91].

- **Advanced Privacy-Preserving Techniques** Methods employing homomorphic encryption and secure multiparty computation [92, 90] enable secure model aggregation. Blockchain-based privacy preservation in medical FL is explored in [78, 80], with comprehensive surveys on blockchain and differential privacy integration available in [93].

1.5.3 Security Challenges in IoMT

While IoMT facilitates advanced healthcare services, it is vulnerable to attacks such as Distributed Denial of Service (DDoS), data poisoning, and impersonation. Existing defenses include encryption [94], anomaly detection [95], and device authentication [96], though comprehensive solutions addressing all threat vectors remain limited.

1.5.4 FL Applications in IoMT

FL offers privacy-preserving model training in IoMT but faces challenges from malicious updates and dynamic network conditions. Studies [97, 14] demonstrate FL's potential, while trust-based defenses [98] highlight the need for adaptable mechanisms in heterogeneous IoMT settings.

1.5.5 Blockchain-Assisted FL in IoMT

Integrating blockchain with FL addresses trust and transparency but introduces scalability and role assignment challenges.

Recent works include alliance chain-based secure IoT data sharing with anonymous interaction [99], Bayesian trust evaluation for IoV sensor data with hybrid consensus [100], and dynamic trust assessment frameworks in vehicular networks [101, 102]. FL-BETS [103] combines FL and blockchain for fraud detection in IoMT but lacks advanced privacy and heterogeneity support.

Multi-tier blockchain solutions like BigchainDB [104, 105] filter malicious IoMT data and support latency-aware FL. ChainFL [106] and FedChain [107] integrate edge computing, cross-chain token transfer, and novel consensus protocols for secure and scalable FL. HealthChain [108] leverages permissioned blockchain and IPFS for secure electronic health record management, emphasizing patient data control. Blockchain's decentralized ledger properties immutability, transparency, and tamper resistance offer significant advantages for FL systems, particularly in trust management and compliance. Despite these advances, gaps remain in dynamic, trust-aware role assignment and comprehensive threat

resistance in IoMT FL, motivating the development of the BlockGuard-RD framework presented in this thesis.

1.6 Participant Selection Definition

Participant selection is a foundational element in the FL paradigm, systematically identifying which devices (often called workers or users) will participate in each training round. This process may be random or, more effectively, based on specific device and data characteristics to enhance training efficiency, accuracy, and security. In advanced FL frameworks, participant selection is not merely a technical necessity but a strategic process that directly influences the overall success of distributed learning. Recent research [109] highlights the use of coordinators or specialized algorithms to optimize selection, ensuring scalability, efficiency, and robustness in federated environments. These insights motivate the design of advanced frameworks.

1.6.1 Characteristics Considered in Participant Selection

Several key attributes are evaluated during participant selection to optimize FL outcomes. These factors are often interdependent and include:

- **Device Heterogeneity**: Devices differ in hardware capabilities such as battery life, storage, processing power, and network bandwidth. For example, a smartwatch with low battery may be excluded to prevent training interruptions. Algorithms often prioritize devices with sufficient resources, while adaptive mechanisms dynamically adjust participation based on real-time metrics.
- **Data Heterogeneity**: The data stored on each device may vary in both quality and distribution:
  - *IID Data*: Ideally, each device's data is independently and identically distributed, but this is rarely the case in real-world IoMT.
  - *Non-IID Data*: More commonly, data distributions differ, potentially biasing model updates. Techniques such as differential privacy, data augmentation, and specialized algorithms are used to mitigate these effects and promote fairness.
- **Dynamic Behavior**: Devices may join or leave the network at any time, or be replaced due to failures or mobility. Robust FL systems must adapt to these changes, ensuring resilience and scalability.

- **Security and Privacy**: The risk of malicious or compromised devices participating in FL is significant. Secure participant selection algorithms, cryptographic techniques, and secure aggregation protocols are essential to protect model integrity and prevent adversarial attacks.
- **Fairness**: Ensuring equitable participation opportunities prevents unjust exclusion and distributes computational burdens and rewards fairly. Strategies such as random sampling and active learning-based selection support this principle, fostering trust and collaboration.

Understanding and addressing these characteristics is crucial for designing participant selection methods that are secure, efficient, and fair especially in heterogeneous and sensitive IoMT environments.

The Objective of Participant Selection

The primary goal of participant selection in FL is to devise an optimal framework that maximizes model accuracy while minimizing training time and resource consumption. This strategic process seeks to achieve several key objectives:

1. Increasing the number of participants per round to enrich data diversity and improve model generalization.
2. Prioritizing reliable devices to maintain training integrity and consistent model quality.
3. Reducing training duration for faster convergence and lower computational overhead.
4. Balancing privacy preservation with learning precision to meet regulatory and user requirements.
5. Mitigating the adverse effects of non-IID data through targeted selection and data-handling strategies.
6. Enhancing overall system dependability to support deployment in diverse, real-world conditions.

Effective participant selection is crucial for achieving these objectives, ensuring the success of FL while preserving data confidentiality and model fidelity. Achieving these goals often involves trade-offs for example, between speed and accuracy or privacy and utility which underscores the complexity of designing robust selection strategies.

1.6.2 Participant Selection Categories

Participant selection strategies in FL can be classified according to their methodologies and objectives [109]:

- **Random Selection**: Participants are chosen randomly each round. This simple approach is computationally inexpensive but may repeatedly select underperforming devices ("stragglers"), reducing accuracy and prolonging training. Random selection serves as a baseline for comparison with more advanced methods.
- **Performance-Based Selection**: Participants are selected based on historical performance metrics, such as task completion time or reliability. Reputation-driven algorithms and predictive models help prioritize devices likely to contribute effectively to training.
- **Data-Based Selection**: This strategy addresses data heterogeneity by selecting participants to balance or diversify the training data. Techniques such as clustering or re-weighting may be used to mitigate non-IID effects, though fairness may not always be prioritized.
- **Security-Based Selection**: Focuses on excluding potentially malicious participants to prevent attacks or model manipulation. Reputation systems and anomaly detection are often used to reinforce trust and integrity in the FL process.
- **Group-Based Selection**: Participants are grouped by attributes such as geographic location, device type, or data characteristics, and selection is based on group-specific traits. This approach can optimize local performance and scalability.
- **Characteristics-Based Selection**: Selection is based on specific features influencing training outcomes, such as weight divergence, loss gradients, or probabilistic allocation. This method fine-tunes the process to achieve better convergence and model quality.

Alternative classification frameworks include:

- **Synchronous Selection**: Participants are selected and train simultaneously, ensuring uniformity in timing and resource use.
- **Asynchronous Selection**: Participants are selected and train at different times, offering flexibility but potentially increasing coordination overhead.
- **Hybrid Selection**: Combines synchronous and asynchronous elements to balance efficiency and adaptability.

These categories highlight the multifaceted and adaptive nature of participant selection in FL. The diversity of strategies reflects the need to tailor selection methods to specific operational constraints and objectives a challenge addressed by the advanced frameworks discussed in this thesis.

1.7 Blockchain for IoMT Security

Distributed ledger technology, widely recognized as blockchain, emerged in 2008 as an innovative paradigm integrating consensus protocols, cryptographic methods, and decentralized systems [110]. Its distinctive sequential architecture guarantees immutability and auditability, positioning it as a fortified, tamper-resistant framework that maintains data confidentiality without reliance on intermediaries. Blockchain technology is increasingly recognized for its transformative capacity to address pressing challenges in the management and security of IoMT ecosystems [111]. In healthcare, blockchain establishes a secure infrastructure for managing personal records, archiving health-related data, and enabling precise access control conferring substantial benefits to patients, researchers, and healthcare professionals [112].

Applications in Healthcare: Blockchain facilitates secure data exchange in several domains, including:

- Secure medical record management and patient data sharing.
- Oversight of pharmaceutical supply chains to ensure traceability [113].
- Safeguarding sensitive personal health data against unauthorized access [114, 115, 116].

The COVID-19 pandemic underscored the urgent need for seamless and secure data interchange among healthcare stakeholders. While the aggregation of clinical data accelerated research, it also highlighted the critical importance of upholding patient confidentiality and adhering to standards such as HIPAA. Monitoring data interactions and ensuring secure, auditable dissemination remain formidable challenges [117, 118, 119, 120, 121]. This necessitates mechanisms that balance accessibility with rigorous privacy safeguards a gap addressed by integrating blockchain into FL frameworks.

1.7.1 IoT-Enhanced Health Surveillance Systems

The rapid advancement of IoT technology makes it ideally suited for patient health surveillance, enabling real-time monitoring of vital physiological indicators. Integrating blockchain

with IoT enhances patient autonomy by decentralizing authority over data, strengthening privacy protections, and providing tamper-evident audit trails. This synergy revolutionizes the secure collection, sharing, and retention of medical data, transforming healthcare administration and delivery.

1.7.2 Attributes of Blockchain Technology

Key characteristics of blockchain include:

- **Decentralization:** Distributed validation eliminates the need for centralized oversight, enhancing system resilience and mitigating single points of failure [122].
- **Transparency:** Immutable record-keeping ensures universal visibility of transaction histories, promoting accountability and enabling meticulous audit trails [123].
- **Security:** The architecture's resistance to tampering and data breaches provides robust defenses, especially in healthcare applications [124, 125, 126].

1.7.3 Categories of Blockchain Systems

Blockchain systems are generally classified as:

- **Public Blockchain:** Fully decentralized, open to all participants, and validated through collective consensus. While highly transparent, public blockchains may not meet the privacy and efficiency needs of healthcare [127].
- **Private Blockchain:** Access is restricted and managed by a governing entity, offering enhanced confidentiality and scalability often preferred for organizational healthcare applications [114].
- **Consortium Blockchain:** Managed by a coalition of organizations, this model balances decentralization with controlled access, making it suitable for regulated environments like healthcare consortia [115].
- **Hybrid Blockchain:** Combines private and public features, allowing selective confidentiality and public validation well-suited for complex, multi-stakeholder healthcare platforms [128].

1.8 Conclusion

IoMT has emerged as a transformative force in modern healthcare, enabling real-time patient monitoring, remote diagnostics, and data-driven medical decision-making. However, the integration of IoMT technologies presents significant challenges particularly in the realms of security, privacy, interoperability, and computational efficiency. This chapter provided a comprehensive overview of IoMT system architecture, highlighting its multi-layered structure and the advanced technologies required to enhance its functionality.

FL has been identified as a promising approach for privacy-preserving model training, allowing medical institutions to collaborate without exposing sensitive patient data. Yet, the effectiveness of FL in heterogeneous IoMT environments hinges on the adoption of optimized participant selection methods. Strategies such as reputation-based selection, energy-aware optimization, and adaptive learning mechanisms have been proposed to ensure reliable and efficient model convergence.

Security remains a critical concern in IoMT ecosystems, with blockchain technology playing a pivotal role in enhancing trust, data integrity, and decentralized authentication. Additional advancements, such as differential privacy and digital twin technology, further strengthen the resilience of IoMT-based FL frameworks.

Despite these advancements, numerous challenges persist including adversarial threats, unreliable communication networks, and the need for scalable computing solutions. Addressing these limitations requires innovative frameworks that can simultaneously optimize participant selection, enhance security, and ensure system scalability. In this context. In the next chapter, we delve deeper into the complexities of participant selection methods, examining the impact of device heterogeneity, threat resistance frameworks, and blockchain integration in optimizing FL for medical applications.

CHAPTER 2: COMPARATIVE STUDY OF PARTICIPANT SELECTION METHODS

2.1 Introduction

Participant selection is a fundamental component in the design and implementation of FL systems. As FL relies on decentralized data and collaborative training, the choice of which clients participate in each training round can have a profound impact on the model's convergence speed, accuracy, communication efficiency, and overall robustness. Given the diversity in client capabilities, data distributions, and availability, participant selection has become a rich area of study, with numerous strategies proposed to address the associated challenges.

These strategies are commonly categorized based on their selection criteria, such as availability-based, performance-based, resource-aware, or fairness-oriented approaches. Each category offers different trade-offs and is suited to specific use cases, particularly in sensitive domains like IoMT, where data privacy, device heterogeneity, and communication constraints are significant concerns.

In this chapter, we present a comprehensive set of experiments that explore and compare these alternative participant selection categories. Through practical implementation and evaluation, we aim to highlight the performance differences between methods and identify which strategies are most effective under the constraints typical of IoMT environments. This analysis provides valuable insights into the design of secure and efficient FL frameworks tailored to real-world healthcare applications.

2.2 Software Environment

To conduct the experimental evaluation of participant selection methods in FL for IoMT, a robust and flexible software environment was established. The following tools were selected for their widespread adoption in machine learning research and their compatibility

with FL frameworks:

2.2.1 Anaconda

Anaconda is a free and open-source distribution of the Python and R programming languages designed for scientific computing. It simplifies package management and deployment, providing a stable environment for machine learning and data science workflows [129]. In this work, Anaconda was used to manage dependencies and ensure reproducibility of experiments.

2.2.2 Python

Python is a high-level, interpreted language known for its simplicity and readability. It serves as the primary programming language for implementing machine learning algorithms, data preprocessing, and experimental scripts [130].

2.2.3 PyTorch

PyTorch is an open-source machine learning library developed by Facebook's AI Research lab. It offers dynamic computation graphs and is particularly well-suited for deep learning research [131]. PyTorch was used as the core framework for building and training neural network models in this thesis.

2.2.4 Plato

Plato is a research framework for FL built on top of PyTorch. It enables customization of client and server behaviors and supports a variety of FL scenarios [132]. In this study, Plato facilitated the implementation and evaluation of different participant selection algorithms in FL experiments.

2.3 Theoretical and Experimental Comparison of Participant Selection Categories

As outlined in Section 1.4 of Chapter One, participant selection methods in FL are classified into several categories, including random, performance-based, data-based, security-based, group-based, and characteristics-based selection. These categories reflect diverse

strategic focuses ranging from computational efficiency to trust management and fairness, particularly relevant in IoMT environments with stringent latency and privacy requirements.

In this section, we present a comparative analysis of these participant selection strategies, grounded in empirical observations and supported by experimental insights. The objective is to evaluate how each category performs in terms of critical FL criteria such as accuracy, robustness, scalability, privacy preservation, and latency tolerance under 5G-enabled IoMT scenarios.

2.3.1 Comparison Between Selection Categories

Table 2.1 summarizes the core characteristics of each selection category. The comparison includes quantitative or semi-quantitative metrics where available, and highlights specific mechanisms relevant to healthcare IoMT applications.

Table 2.1 Theoretical Comparative Overview of Participant Selection Categories in FL

Selection Category	**Primary Objective**	**Non-IID Data Handling**	**Security Mechanisms**	**Scalability (Clients)**	**5G Latency Tolerance**
Random Selection	Simplicity, baseline performance	No explicit handling	None	$> 10^4$	High (minimal overhead)
Performance-Based	Resource efficiency, fast convergence	Limited (no explicit mitigation)	Reputation-based filtering	$\sim 10^3$	Medium (dependent on client response times)
Data-Based	Fairness, data diversity enforcement	Yes (diversity-aware sampling)	None	$\sim 10^3$	Medium (may induce delays due to data profiling)
Security-Based	Trust and anomaly detection	No	High (e.g., homomorphic encryption, anomaly detection)	$\sim 10^3$	Low (encryption overhead impacts latency)
Group-Based	Localized optimization, domain-specific clusters	Possibly (group-level aggregation)	Indirect (group validation)	$> 10^4$	High (parallel group updates)
Characteristics-Based	Model optimization via client metrics	Yes (loss-based client filtering)	Moderate (differential privacy filters)	$\sim 10^3$	Medium

2.3.2 Alternative Selection Modes: Synchronous vs Asynchronous vs Hybrid

Beyond strategic categories, timing-based selection modes impact FL performance, especially under heterogeneous IoMT device constraints. Table 2.2 provides a qualitative and quantitative comparison.

Table 2.2 Comparison of Timing Modes in FL Client Selection

Mode	Advantages	Limitations	Suitability
Synchronous Selection	Uniform update timing simplifies aggregation; predictable convergence; latency bounded by slowest client	Stragglers slow down rounds; less flexible for heterogeneous IoMT devices	Homogeneous device clusters with stable connectivity
Asynchronous Selection	Flexibility to incorporate fast clients; reduces waiting time; better adapts to device heterogeneity	Coordination complexity; model version staleness can degrade accuracy; requires advanced aggregation	Dynamic IoMT environments with mixed device capabilities
Hybrid Selection	Balances stability and adaptability; e.g., weighted synchronous with asynchronous updates; mitigates straggler effects	Increased design and implementation complexity; requires adaptive scheduling algorithms	Large-scale, dynamic IoMT systems needing both latency control and responsiveness

2.3.3 Limitations of Cross-Category Comparisons

While this chapter provides a comparative overview of various participant selection categories, it is crucial to acknowledge that direct comparisons across these categories can be misleading. Each category has a distinct primary objective some focus on improving convergence speed or fairness, others prioritize security or device-level efficiency. Consequently, the evaluation metrics and contextual assumptions often vary significantly between them.

For example, security-based selection methods may only demonstrate their strengths when facing adversarial conditions, such as data poisoning or impersonation attacks, which do not affect performance-based methods in the same way. Similarly, performance-optimized strategies may favor computational efficiency without addressing fairness or robustness. Therefore, empirical comparisons based on a unified metric (e.g., accuracy or latency) risk oversimplifying the nuanced trade-offs involved.

This analysis underscores that no single participant selection method is universally superior. Instead, their applicability must be interpreted within the context of specific deployment goals and environmental constraints. The experimental results and comparisons presented in this chapter are thus intended to inform understanding rather than declare definitive rankings across categories.

2.3.4 Discussion

Theoretical analysis of participant selection strategies reveals inherent trade-offs across categories. Random and performance-based methods prioritize simplicity and computational efficiency, making them attractive for resource-constrained environments. However, these methods often fail to adequately address challenges such as adversarial manipulation or non-IID data distributions. On the other hand, security-based and group-based strategies significantly enhance trustworthiness and robustness but introduce additional coordination overhead and potential latency challenges, limiting their applicability in real-time IoMT deployments.

Hybrid strategies, which attempt to balance these trade-offs by combining features from multiple categories, can provide a more nuanced solution. However, they often increase system complexity, which can be a significant drawback in large-scale IoMT environments where simplicity and efficiency are paramount.

2.4 Participant Selection Methods in FL: A Comparative Overview

Participant selection is a critical determinant of FL performance, influencing model accuracy, communication efficiency, and adaptability to data heterogeneity. This section presents a comparative analysis of three prominent participant selection strategies: the synchronous **Oort** method, the asynchronous **Pisces** method, and the hybrid **Active Federated Learning (AFL)** approach. Each method is evaluated using the WESAD dataset within the Plato FL simulation framework, focusing on metrics such as model accuracy,

communication efficiency, and scalability under both IID and non-IID settings. This analysis is particularly relevant for IoMT applications, where device heterogeneity and real-time constraints are paramount.

2.4.1 Experimental Motivation and Design Rationale

While the previous sections provided a conceptual comparison of participant selection categories, this section introduces empirical validation by focusing on representative algorithms. Given the diversity of goals among selection categories such as performance optimization, trustworthiness, or data diversity it would be methodologically inappropriate to compare the categories as a whole without contextual alignment. Therefore, in the experimental phase, we select specific algorithms that fall under alternative categories but share a similar goal namely, optimizing performance under realistic IoMT constraints. This ensures a fair and coherent comparison by aligning objectives across methods. The selected algorithms reflect key approaches from categories such as performance-based, group-based, and characteristics-based selection, each tuned to enhance federated learning efficiency in the presence of non-IID data and edge-device heterogeneity.

This targeted approach allows us to evaluate the comparative effectiveness of different participant selection strategies under equivalent operational goals, while acknowledging the broader diversity of objectives that each category may serve in other contexts.

2.4.2 Synchronous Strategy: Oort

Oort is a centralized, synchronous participant selection framework designed to optimize training time and model accuracy in federated settings [21]. It employs a scoring mechanism based on system availability and data utility to select participants for each round. While Oort provides a predictable workflow, its synchronous nature makes it susceptible to the straggler problem, where slow clients delay the entire round. This limitation is especially pronounced in large-scale or heterogeneous environments with non-IID data distributions.

2.4.3 Asynchronous Strategy: Pisces

Pisces is an asynchronous selection framework that maximizes participation, including contributions from less reliable or low-resource clients [22]. It enables concurrent communication and computation, reducing idle time and mitigating the impact of slow participants. Pisces demonstrates rapid early-phase accuracy improvements, but its convergence rate aligns with synchronous methods over extended training. Its flexibility makes

it suitable for dynamic IoMT environments, though it may introduce challenges in model consistency and aggregation.

2.4.4 Hybrid Strategy: Active Federated Learning (AFL)

AFL adopts a hybrid, dynamic approach, leveraging active learning principles to prioritize participants with underrepresented or unreliable data distributions [74]. AFL dynamically adapts participant selection based on the evolving state of the global model and observed data quality, enhancing model robustness and generalization. This approach is particularly effective in non-IID settings and heterogeneous systems.

2.4.5 Experimental Setup

Dataset and Preprocessing

The WESAD dataset [133], designed for affective state recognition, was used for evaluation. It contains multimodal physiological signals (BVP, EDA, ECG) for binary stress classification. Signals were segmented into 700-sample windows with 50% overlap, extracting statistical and nonlinear features, resulting in 121,813 instances. This preprocessing ensures a balanced testbed for both IID and non-IID configurations.

Model Architecture and Training Configuration

A recurrent neural network (RNN) with 70 memory cells, dropout regularization, and a flattened output layer was used. Training employed cross-entropy loss and SGD (learning rate $\beta = 0.005$, momentum 0.9, batch size 32). Experiments were run in the Plato framework with varied participant counts and communication rounds. Table 2.3 summarizes the training parameters.

Table 2.3 Training parameters for participant selection experiments

Model	RNN
Optimizer	SGD
Batch Size	32
Learning Rate	0.005
Momentum	0.9
Epochs per Round	1

2.4.6 Comparative Analysis and Results

Accuracy Across Communication Rounds

Figure 4.2 shows model accuracy over communication rounds under IID conditions. All methods converge to approximately 77.2% accuracy, but Pisces achieves faster early improvements. Oort exhibits unstable trends due to sensitivity to participant heterogeneity, while AFL maintains steady, balanced progress, highlighting its adaptive selection advantage.

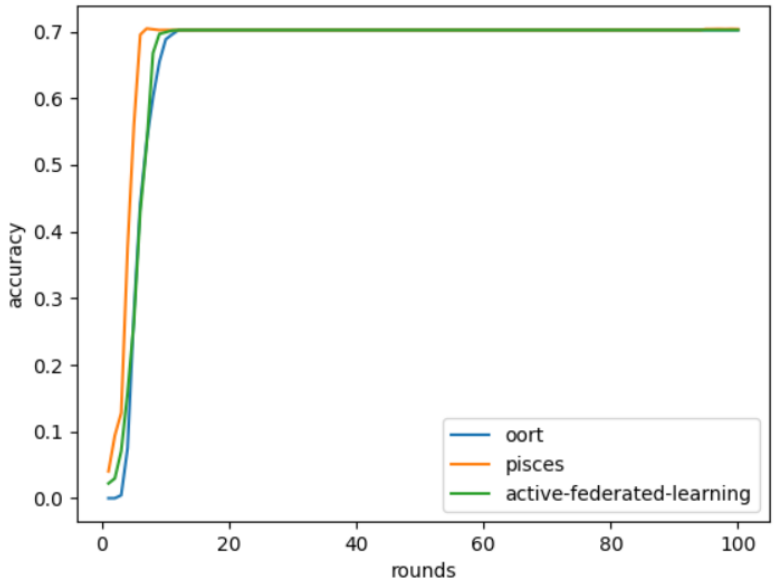

Figure 2.1 Model accuracy over communication rounds under IID conditions.

Temporal Efficiency

Figure 2.2 compares selection time for each method. AFL achieves the lowest latency (∼X seconds per round), followed by Pisces, while Oort incurs the highest selection time due to synchronous overhead. Asynchronous and hybrid approaches are preferable for latency-sensitive applications such as real-time health monitoring.

Scalability with Participant Count

Figure 2.3 illustrates accuracy as a function of participant count. AFL maintains consistent accuracy (∼70.2%) as participant numbers increase, demonstrating robust scalability. Pisces shows mild fluctuations, while Oort's accuracy drops to 55% under non-IID conditions, underscoring AFL's suitability for real-world, heterogeneous deployments.

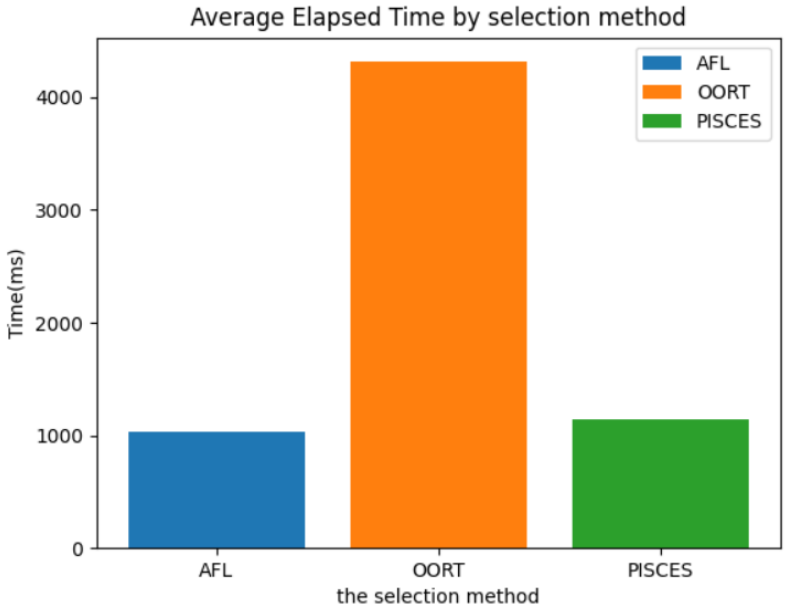

Figure 2.2 Temporal efficiency (selection time) of participant selection strategies.

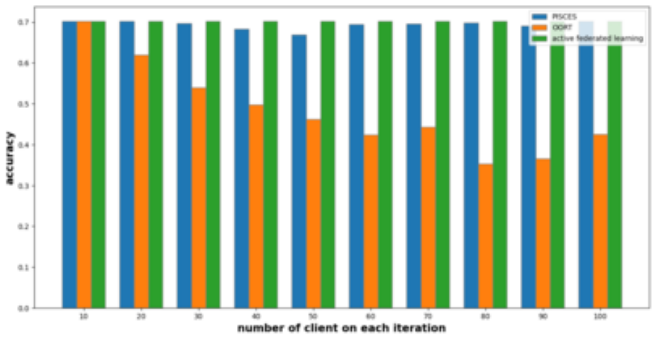

Figure 2.3 Model accuracy as a function of participant count.

Summary of Comparative Findings

Table 2.4 summarizes the key attributes and performance outcomes of the evaluated methods. Notably, none of the methods explicitly integrate privacy or security mechanisms, which remains a critical area for future research, especially in sensitive domains like healthcare.

2.4.7 Discussion

The empirical results highlight the strengths and limitations of the three strategies. AFL is the most robust, maintaining high accuracy and efficiency across scenarios, especially with non-IID data. Pisces offers rapid early-stage improvements but converges similarly to

Table 2.4 Summary of participant selection strategies in FL

Attribute	Oort	Pisces	AFL
Approach	Centralized	Centralized	Dynamic/Hybrid
Heterogeneity Awareness	Yes	Yes	Yes
Dynamic Selection	No	No	Yes
Communication Efficiency	Moderate	High	High
Accuracy (IID)	77%	77%	77%
Accuracy (Non-IID)	55%	71%	77%
Privacy/Security	No	No	No

Oort over time. Oort, while simple, is hindered by synchronization delays and non-IID sensitivity. For IoMT and other real-world applications, dynamic and context-aware selection strategies like AFL are preferable, though privacy and security remain open challenges.

2.4.8 Conclusion

This chapter provided a comparative evaluation of Oort, Pisces, and AFL for participant selection in FL. Using the WESAD dataset and the Plato framework, we demonstrated that dynamic selection methods like AFL deliver superior performance, particularly in heterogeneous, non-IID environments. Future work should focus on integrating privacy and security mechanisms to further enhance FL's applicability in sensitive domains such as healthcare.

CHAPTER 3: PROPOSED PARTICIPANT SELECTION METHOD

3.1 Introduction

As we concluded from the previous chapters, participant selection is a critical factor influencing the efficiency, security, and overall performance of FL, particularly in resource-constrained and heterogeneous environments such as IoMT. The success of FL in these contexts hinges on the ability to judiciously select clients for training, while effectively addressing challenges including data heterogeneity, energy limitations, and diverse communication capabilities.

In this chapter, we present a dynamic participant selection mechanism tailored for both centralized and decentralized FL architectures. This mechanism not only identifies the most suitable participants based on optimized selection criteria but also assigns roles that reflect each participant's computational capabilities and trustworthiness. In centralized FL settings, the approach facilitates efficient coordination and accelerates model convergence. In decentralized, blockchain-enhanced environments, it further ensures robustness and resilience against common security threats by integrating consensus-based validation within the selection process.

The chapter proceeds with a detailed exposition of the proposed mechanism, covering its core components, decision-making logic, and practical implementation in both centralized and decentralized FL frameworks. We also demonstrate how this mechanism aligns with the unique requirements of IoMT systems, thereby advancing the development of secure, scalable, and performance-optimized FL infrastructures.

3.2 Overview of the Proposed Mechanism

Building upon insights drawn from previous works, it becomes evident that the selection of the most efficient clients (also referred to as participants) is often based on specific

characteristics inherent to the devices themselves. In our approach, we categorize these characteristics into two main dimensions: *optimization* and *privacy*. Each device is evaluated and assigned levels corresponding to these two categories. In order to underscore the novelty and effectiveness of our proposed mechanism for dynamic participant selection in Federated Learning (FL), we compare it with several state-of-the-art methods in the literature. As shown in Table 3.1, existing methods tend to focus on either optimization (e.g., model accuracy, communication efficiency, or energy consumption) or privacy/security (e.g., resilience to malicious clients or privacy-preserving techniques), often sacrificing one for the other. However, few methods offer a balanced, integrated solution that performs well across optimization, privacy, decentralization, and security dimensions simultaneously. Our approach addresses this critical gap by incorporating blockchain-assisted role determination and differential privacy, while supporting both centralized and decentralized architectures. This integrated framework ensures robust, privacy-aware, and efficient client selection, even in heterogeneous environments.

The following comparison table systematically evaluates existing methods against several key criteria, and clearly demonstrates the comprehensive nature and advantages of our solution.

Table 3.1 Comparison of Existing Client Selection Methods in Federated Learning (FL)

Method	**Selection Criteria**	**Key Features and Findings**	**Optimization**	**Privacy**	**Centralized/ Decentralized**	**Against Malicious Clients**
PIRATE [72]	Reputation-based, Blockchain	Efficient reputation system, decentralized	✗	✓	Decentralized	✓
Oort [21]	Processing time, Accuracy	Optimizes participant selection, integrates with FL coordinator	✓	✗	Centralized	✗
Control Mechanism [76]	Selection frequency	Enhances participation of weaker clients, tested on FEMNIST datasets	✓	✗	Centralized	✗

Continued on next page

Method	Selection Criteria	Key Features and Findings	Optimization	Privacy	Centralized/ Decentralized	Against Malicious Clients
VerifyNet [83]	Verification of server results	Robust under honest-but-curious security setting, supports dropout handling	✗	✓	Centralized	✓
SAM [85]	Selective Aggregation of Models	Efficient model aggregation, reduces communication overhead	✓	✗	Centralized	✗
REWAFL [82]	Residual energy, Wireless conditions	Optimizes energy consumption, suitable for mobile devices	✓	✓	Decentralized	✗
Ranking-based Client Selection [84]	Imitation learning, Efficiency	Improves efficiency through learning-based ranking	✓	✗	Centralized	✓
FLOAT [86]	Automated Tuning	Optimizes FL parameters automatically	✓	✗	Centralized	✗
Lotto [79]	Adversarial server resistance	Secure participant selection	✗	✓	Centralized	✓
Long-Term Client Selection [134]	Emulates full client participation	Long-term strategy for client selection	✓	✗	Centralized	✗

Continued on next page

Method	Selection Criteria	Key Features and Findings	Optimization	Privacy	Centralized/ Decentralized	Against Malicious Clients
FedCure [87]	Heterogeneity-Aware, Blockchain	Personalized FL, intelligent healthcare applications	✗	✓	Decentralized	✓
Pisces [73]	Processing time, Accuracy	Optimizes participant selection, take advantage of struglers by adding asynchronous method	✓	✗	Centralized	✗
afl [74]	Calculate probabilities depending on utilities	Probability-based client selection	✓	✗	Centralized	✗
novel-reputation [135]	Calculate the reputation score for allowing participation	Trustscore for client selection	✓	✗	Centralized	✗

Continued on next page

Method	Selection Criteria	Key Features and Findings	Optimization	Privacy	Centralized/ Decentralized	Against Malicious Clients
hermes [75]	Communication overhead and improving inference efficiency	Group participant selection depending on communication	✓	✗	centralized	✗
This proposed method	Data quality, Resource availability	Combines dynamic client selection with adaptive learning rates, proven on Mnist, privacy-preserving mechanisms	✓	✓	**Centralized/ Decentralized**	✓

These levels serve as indicators of the device's overall efficiency and reliability, which in turn guide its inclusion in the training process or the role it assumes within the decentralized system particularly when integrated with blockchain technologies that enable role differentiation. Importantly, the criteria used to determine these levels are based on fundamental attributes that are critical to the performance and trustworthiness of each device. By incorporating this structured evaluation, our mechanism facilitates a more secure and performance-aware participant selection process.

The metrics summarized in Tables 3.2 and 3.3 were derived from an extensive review of related work, emphasizing the impact of device capabilities on FL performance [21, 22, 135, 74]. Commonly referenced criteria include connectivity, computational resources, and security protocols, which we incorporate into our selection logic.

3.2.1 Optimization Metrics

The optimization metrics reflect the device's ability to contribute effectively to model training. These include the quality of connectivity, battery status, storage availability, and processing capacity (RAM and CPU). These factors are used to prioritize devices that can

manage the computational demands of training. Table 3.2 outlines the specific optimization metrics applied in our approach.

Table 3.2 Optimization metrics for participant selection.

Metric	**Description**
Connectivity Level	The type and strength of the device's network connection.
Battery Life	Battery level, with a threshold of 70% as a key indicator.
Storage Capacity	Availability of sufficient storage space for the training process.
RAM	Adequacy of random-access memory for training tasks.
CPU	Suitability of the central processing unit for training requirements.
Priority	Preference given to devices based on proximity or other factors.

3.2.2 Privacy Metrics

To preserve data confidentiality and model integrity, privacy metrics are equally emphasized. Devices are evaluated on their use of encryption, robustness of security protocols, firewall effectiveness, and overall vulnerability. These factors help gauge the risk level associated with each participant. The detailed metrics used for assessing privacy levels are provided in Table 3.3.

Table 3.3 Privacy metrics for participant selection.

Metric	Description
Encryption Algorithms	The effectiveness and strength of the encryption methods used.
Security Protocols	The security level provided by device and network protocols.
Firewall Robustness	The firewall's capability to control access and protect resources.
Vulnerability	The presence of known security weaknesses in the device.
Last Update Time	Recency of the last security update, indicating the currency of protective measures.

3.3 Participant Selection Process in Centralized FL

In the context of centralized FL, participant selection is managed by a central server that serves as the global coordinator. The server is responsible for balancing two core objectives: maximizing training efficiency and preserving data privacy.

To make informed decisions, the server evaluates candidate devices using a defined set of optimization and privacy metrics, as previously discussed. Devices are scored and ranked based on their level in each dimension. Only those that meet the established thresholds for both optimization and privacy are selected to participate in the current training round.

The overall workflow of the centralized participant selection process is summarized in Figure 3.1. As shown, the mechanism consists of metric evaluation, level computation, threshold comparison, and role assignment (if applicable). This structured approach ensures that only capable and trustworthy participants are admitted, thereby maintaining the integrity and effectiveness of the FL system.

3.3.1 Refined Probabilistic Participant Selection Model

To enhance the basic participant selection strategy, we propose a refined probabilistic model that enables a more nuanced evaluation of each device. Rather than using hard thresholds alone, this model computes the likelihood that a client will be selected based

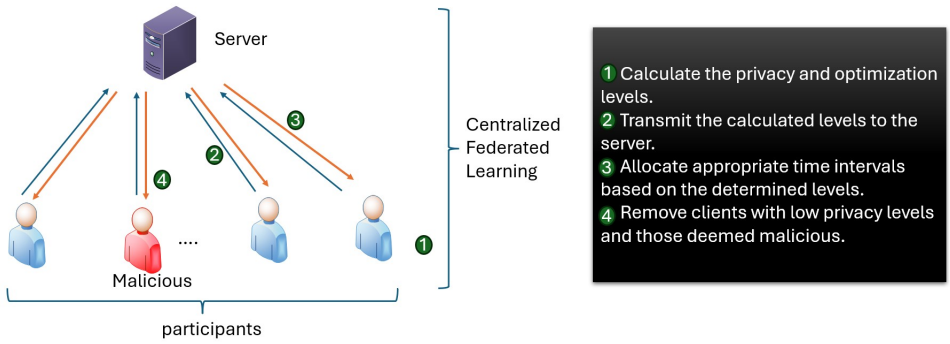

Figure 3.1 Graphical overview of the main steps of the proposed participant selection method in centralized FL.

on its assessed optimization and privacy levels. The selection probability is given by the following equation:

$$P(\text{selected}) = \frac{1}{2}\left(\frac{1}{1+\exp(-(\text{privacyLevel}-8))} + \frac{1}{1+\exp(-(\text{optimizationLevel}-8))}\right) \tag{3.1}$$

This formula incorporates several key design components:

- **Sigmoid Function:** A sigmoid function is applied to both the optimization and privacy levels to model the probability of selection. This provides a smooth, non-linear transition, where the likelihood of being selected increases steadily as the levels surpass a predefined threshold.
- **Thresholds:** The model uses thresholds of $\theta_1 = 8$ and $\theta_2 = 8$, which serve as central points of reference. These values define where the selection probability begins to rise significantly.
- **Normalization:** The expression is averaged with a factor of $\frac{1}{2}$ to ensure the resulting probability stays within the range $[0, 1]$, giving equal weight to both privacy and optimization levels.

3.3.2 Clarification of Threshold Basis ($\theta_1 = 8$ and $\theta_2 = 8$)

The selection thresholds θ_1 and θ_2 were set to 8 based on both theoretical reasoning and empirical observations. Below, we explain the basis for this choice:

1. Normalized Evaluation Scale All metrics used to compute the optimization and privacy levels are evaluated on a normalized scale from 0 to 10. A threshold of 8 corresponds to an 80% score, which represents a strong but achievable standard. This allows high-performing devices to participate while still accommodating minor imperfections.

2. Empirical Validation During experimental trials, devices with levels greater than or equal to 8 showed consistent performance in terms of computational capacity and adherence to privacy standards. Specifically:

- Devices with high **Optimization Levels** contributed efficiently to training tasks.
- Devices with high **Privacy Levels** ensured better protection of sensitive data.

In contrast, lower-scoring devices were frequently associated with system bottlenecks or increased security risks.

3. Balancing Inclusiveness and Reliability Choosing a threshold of 8 helps strike a balance:

- Lower thresholds could increase participation but allow underperforming or vulnerable devices.
- Higher thresholds could excessively reduce the participant pool, limiting overall system performance.

4. Role of the Sigmoid Transition The sigmoid function ensures that scores near the threshold exhibit a moderate selection probability. At a level of 8, the selection probability equals 0.5. Scores above this value increase the likelihood of participation, while those below it rapidly decrease, ensuring only reliable devices are prioritized.

5. Metric Aggregation Formulas Each device's optimization and privacy levels are computed by averaging the scores of five key sub-metrics:

$$\begin{aligned} \text{Optimization Level} &= \frac{\text{Battery} + \text{Storage} + \text{RAM} + \text{CPU} + \text{Priority}}{5}, \\ \text{Privacy Level} &= \frac{\text{Encryption} + \text{Security Protocols} + \text{Firewall} + \text{Vulnerability} + \text{Update Time}}{5}. \end{aligned} \tag{3.2}$$

6. Example Calculation Consider a device with the following metric values:

- **Optimization Metrics:** Battery = 8.0, Storage = 9.0, RAM = 7.0, CPU = 6.5, Priority = 8.5
- **Privacy Metrics:** Encryption = 7.0, Security Protocols = 7.5, Firewall = 8.0, Vulnerability = 9.0, Update Time = 8.5

The computed levels are:

$$\text{Optimization Level} = \frac{8.0 + 9.0 + 7.0 + 6.5 + 8.5}{5} = 7.8$$
$$\text{Privacy Level} = \frac{7.0 + 7.5 + 8.0 + 9.0 + 8.5}{5} = 8.0$$

The corresponding selection probability becomes:

$$P(\text{selected}) = \frac{1}{2}\left(\frac{1}{1+\exp(-(7.8-8))} + \frac{1}{1+\exp(-(8.0-8))}\right)$$
$$\approx 0.4636$$

This result demonstrates how falling slightly below the threshold reduces the probability of selection, reinforcing the importance of maintaining high performance across both dimensions.

3.4 Simulation of This Method

Algorithmic Integration: The proposed model reflects a dynamic participant selection strategy by prioritizing clients based on their `privacyLevel` and `optimizationLevel`. Clients with values exceeding 8 are granted higher selection probabilities. Those with intermediate values (between 4 and 8) have moderate chances, while those below this range are typically excluded. This probabilistic model enhances the flexibility and resilience of the selection process.

As shown in Algorithm 1, the server selects clients based on optimization and privacy metrics informed by the probabilistic model. Each client is evaluated and assigned to a category that determines the selection timing. This strategy improves overall system performance by allocating earlier participation to high-scoring clients, thereby enhancing efficiency and effectiveness in the FL process.

Table 3.4 Participant Selection Based on Optimization and Privacy Levels

Optimization Level	**Privacy Level > 8**	**$4 <$ Privacy Level < 8**	**Privacy Level < 4**
Level > 8	Selected (time = 0)	Selected (time = 0)	Eliminated
$4 <$ Level < 8	Selected (time = +1)	Selected (time = +1)	Eliminated
Level < 4	Selected (time = +2)	Selected (time = +2)	Eliminated

Algorithm 1 Participant Selection in FL

function SELECTPARTICIPANTS($clients$)
  $selectedClients \leftarrow []$
  for $client$ **in** $clients$ **do**
    $privacyLevel \leftarrow$ GETPRIVACYLEVEL($client$)
    $optimizationLevel \leftarrow$ GETOPTIMIZATIONLEVEL($client$)
    if $privacyLevel > 8$ **then**
      $selectedClients$.append(($client$, $t1$)) ▷ Worker with requested time
    else if $4 < privacyLevel \leq 8$ **then**
      $selectedClients$.append(($client$, $t2$)) ▷ Worker with requested time + 1
    else ▷ Eliminated
    end if
    if $optimizationLevel > 8$ **then**
      $selectedClients$.append(($client$, $t1$)) ▷ Worker with requested time
    else if $4 < optimizationLevel \leq 8$ **then**
      $selectedClients$.append(($client$, $t2$)) ▷ Worker with requested time + 1
    else ▷ Eliminated
    end if
  end for
  return $selectedClients$
end function

3.5 Experimental Scenarios and Results

3.5.1 Experimental Design

To comprehensively evaluate the proposed participant selection mechanism, we designed four experimental scenarios involving 100 clients over 20 training rounds:

- **Scenario 1:** Traditional centralized Federated Learning (FL), where all clients collaboratively train a global model in a fully coordinated manner.
- **Scenario 2:** Centralized FL with the presence of malicious clients aiming to disrupt training or manipulate model updates.
- **Scenario 3:** Centralized FL enhanced with differential privacy (DP) techniques to mitigate privacy risks by injecting controlled noise into model updates.

- **Scenario 4:** An advanced setup combining DP with our proposed participant selection strategy based on privacy and optimization metrics.

This experimental framework enables a thorough comparative analysis of performance, security, and privacy preservation across diverse FL configurations.

3.5.2 Experimental Setup and Evaluation Metrics

Experiments were executed on an Intel Core i7 CPU, 16 GB RAM, and an NVIDIA RTX 3070 GPU running Windows 11. FL models were implemented in Python 3.9 using PyTorch. DP was integrated via the Opacus library.

Key hyperparameters were set as follows:

- Learning rate: 0.01
- Batch size: 64
- Number of epochs per round: 10

The evaluation focused on the following metrics:

- **Model accuracy:** The predictive performance of the global model.
- **Robustness to adversarial attacks:** The system's ability to withstand malicious client behavior.
- **Privacy protection effectiveness:** The degree to which sensitive information is safeguarded.

3.5.3 Results Analysis

Figures 3.2 and 3.3 illustrate the impact of intelligent client selection under both IID and non-IID data distributions. Incorporating optimization and privacy metrics significantly improves participant choice, effectively balancing model performance with data confidentiality.

Compared to standard FL, our participant selection mechanism accelerates convergence and enhances model accuracy throughout training. These results underscore the benefits of optimized client selection in achieving efficient and secure federated learning.

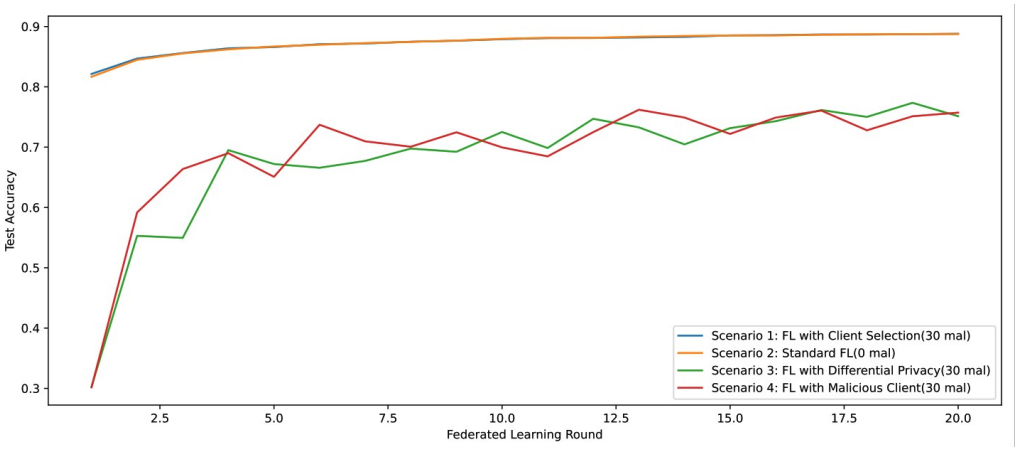

Figure 3.2 Performance of centralized participant selection under IID data distribution

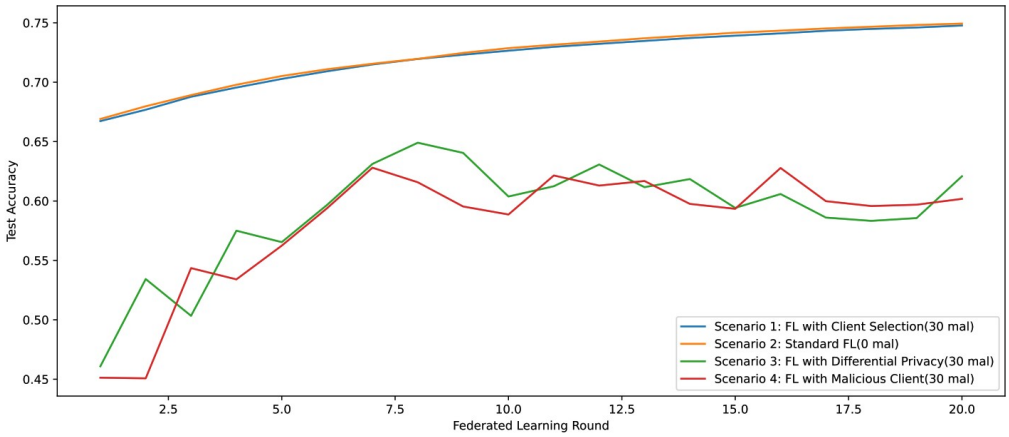

Figure 3.3 Performance of centralized participant selection under non-IID data distribution

3.6 Comparison with Existing Methods

Our proposed method uniquely balances both security and optimization objectives, in contrast to prior approaches that predominantly focus on optimization alone. The experiments utilized the MNIST dataset and a SimpleNN architecture comprising two hidden layers.

Table 3.5 presents a comparative evaluation against state-of-the-art FL participant selection strategies. Notably, competing methods such as Oort, Pisces, and Hermes prioritize optimization but neglect privacy considerations, resulting in substantially degraded performance in adversarial environments.

Our approach significantly outperforms these methods, achieving an accuracy of **90.39%** even in the presence of malicious clients, demonstrating its robustness and efficacy.

Table 3.5 Comparison of Our Centralized Participant Selection Method with Existing Approaches

Experiments Conducted in the Presence of Malicious Clients		
Algorithm	**Objective**	**Accuracy**
Random Selection [17]	Optimization	68.9%
Oort [21]	Optimization	16.7%
Pisces [22]	Optimization	28.2%
Hermes [75]	Optimization	23.8%
Our Proposed Method	**Security + Optimization**	**90.39%**

3.7 Role Determination in Blockchain-Enabled Federated Learning

3.7.1 Overview of the Role Determination Mechanism

Building upon the Blockchain-Assisted Federated Learning (FL) framework introduced earlier, this section presents a dynamic role determination mechanism that classifies participating nodes based on their optimization and privacy levels. This stratified role assignment significantly enhances both the efficiency and security of the FL process, as illustrated in Figure 3.4. The mechanism is integrated within a private permissioned blockchain environment, selected for its robust capabilities in enforcing controlled access, governance, and data integrity across the network.

The deliberate use of a private blockchain ensures restricted participation, strengthened privacy controls, and robust protection against unauthorized access or tampering. Empirical evaluations indicate that the choice of consensus algorithm has negligible effect on the effectiveness of the role determination strategy. The overall workflow of this process is depicted in Figure 3.1.

3.7.2 Node Classification Based on Privacy and Optimization Metrics

Role assignment is guided by two pivotal attributes for each node: optimization level and privacy level. Optimization metrics encompass hardware and connectivity characteristics such as CPU performance, RAM capacity, battery status, storage availability, and network reliability. Privacy metrics evaluate the robustness of security mechanisms deployed on the node, including encryption strength, firewall integrity, authentication protocols, and vulnerability resistance.

This comprehensive evaluation enables the systematic classification of nodes into distinct roles within the decentralized FL ecosystem, ensuring that each participant con-

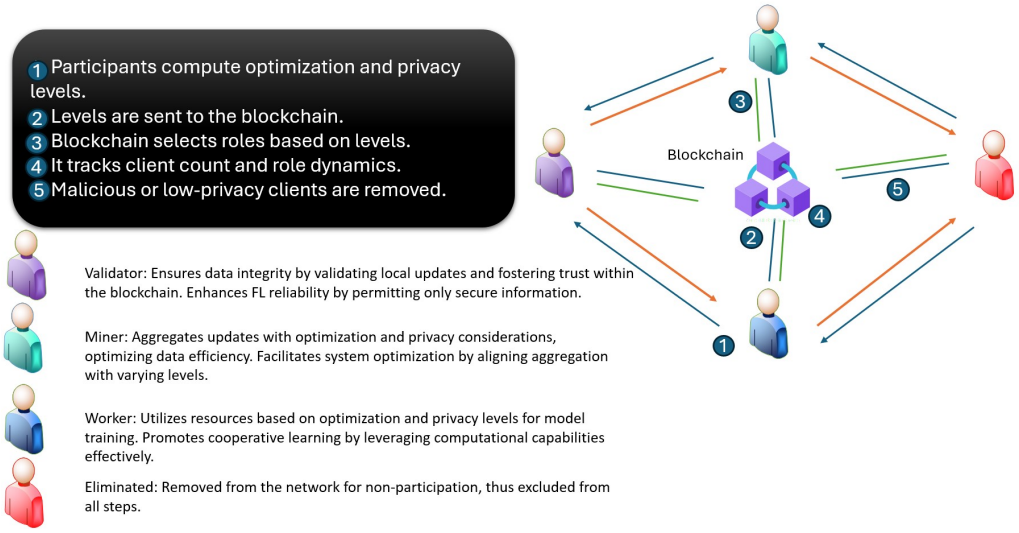

Figure 3.4 Graphical overview of the main steps of the proposed Role Determination method in Blockchain-Enabled FL.

tributes in accordance with its capabilities and trustworthiness.

3.7.3 Blockchain-Based Role Allocation Strategy

The role determination strategy is operationalized within the private blockchain infrastructure, ensuring secure, transparent, and auditable role assignments. Based on the assessed optimization and privacy levels, nodes are dynamically assigned one of the following roles:

- **Worker**: Nodes exhibiting high optimization and privacy levels undertake the primary responsibility of model training.
- **Miner**: Nodes with moderate optimization but high privacy levels participate in block creation and transaction validation.
- **Validator**: Nodes with lower optimization but strong privacy assist in verifying transactions and model updates.
- **Eliminated**: Nodes failing to meet minimum privacy thresholds are excluded to preserve system integrity and security.

Table 3.6 summarizes the criteria for role assignment. By dynamically allocating roles through a privacy- and optimization-aware mechanism, the system ensures secure, efficient, and trustworthy operation of the FL process while safeguarding sensitive client data.

Table 3.6 Role Assignment Criteria Based on Optimization and Privacy Levels in Blockchain-Enabled Decentralized FL

Optimization Level	**Privacy Level > 8**	**$4 <$ Privacy Level ≤ 8**	**Privacy Level ≤ 3**
Level > 8	Worker	Worker	Worker
$4 <$ Level ≤ 8	Miner	Worker	Worker
Level ≤ 3	Validator	Worker	Eliminated

3.7.4 Probabilistic Role Assignment: Concept and Formula

To provide a more flexible and adaptive method for assigning roles in the Blockchain-Assisted Federated Learning (BAFL) system, we propose a probabilistic approach. Instead of using fixed threshold-based decisions, we introduce a formula that assigns roles based on the likelihood derived from each node's `privacyLevel` and `optimizationLevel`. This probabilistic method allows the system to make more nuanced decisions, especially in cases where node metrics fall near threshold boundaries.

Threshold Parameters

The formula uses the following threshold values:

- $\theta_{\text{privacy}} = 8$: Threshold for acceptable privacy level
- $\theta_{\text{optimization}} = 8$: Threshold for high optimization level
- $\alpha = 4$: Lower bound for both privacy and optimization

Role Probabilities

We define the probability $P(R)$ of assigning a node to a specific role R based on its `privacyLevel` and `optimizationLevel`. These probabilities are calculated using logistic sigmoid functions to reflect the soft boundaries between different role levels.

1. Worker Role

$$P(\text{worker}) = \frac{1}{2}\left(\frac{1}{1+\exp(-(\text{privacyLevel} - \theta_{\text{privacy}}))} + \frac{1}{1+\exp(-(\text{optimizationLevel} - \theta_{\text{optimization}}))}\right) \tag{3.3}$$

Nodes with high values in both privacy and optimization are more likely to be assigned as workers responsible for model training.

2. Miner Role

$$P(\text{miner}) = \frac{1}{2}\left(\frac{1}{1+\exp(-(\text{privacyLevel} - \theta_{\text{privacy}}))} \cdot \frac{1}{1+\exp(-(\text{optimizationLevel} - \alpha_1))}\right) \tag{3.4}$$

Miners require strong privacy and at least moderate optimization capabilities. Their role is primarily focused on data aggregation and participation in consensus mechanisms.

3. Validator Role

$$P(\text{validator}) = \frac{1}{2}\left(\frac{1}{1+\exp(-(\text{privacyLevel} - \theta_{\text{privacy}}))} \cdot \frac{1}{1+\exp(-(\text{optimizationLevel} - \alpha_2))}\right) \tag{3.5}$$

Similar to miners, validators require good privacy. However, they can operate with lower optimization, focusing instead on verifying data and ensuring integrity.

4. Eliminated (Non-participant)

$$P(\text{eliminated}) = 1 - (P(\text{worker}) + P(\text{miner}) + P(\text{validator})) \tag{3.6}$$

Nodes with poor optimization and privacy scores are excluded from participation to protect the integrity and efficiency of the system.

3.7.5 Rule-Based Algorithm for Role Assignment

To complement the probabilistic model, we also define a deterministic rule-based algorithm for role assignment. This decision tree ensures reliable fallback logic and aligns with the probabilistic framework.

3.7.6 Functional Roles and System Integration

This subsection describes the functionality and responsibility of each role and explains how they interact in the blockchain-based FL environment.

Validator: Privacy Assurance and Trust Enforcement

Validators are responsible for verifying model updates received from worker nodes. Their key task is to ensure the data adheres to privacy and integrity standards. Validators act as a decentralized trust layer, preventing malicious or corrupted updates from entering the system.

Algorithm 2 Role Assignment in Blockchain-Assisted FL

```
function assignRole(optimizationLevel, privacyLevel)
    if optimizationLevel > 8 then
        return "worker"
    else if 4 < optimizationLevel < 8 then
        if privacyLevel > 8 then
            return "miner"
        else
            return "worker"
        end if
    else
        if privacyLevel > 8 then
            return "validator"
        else if 4 < privacyLevel < 8 then
            return "worker"
        else
            return "eliminated"
        end if
    end if
end function
```

Miner: Efficient Aggregation and Consensus Support

Miners handle aggregation tasks and participate in the blockchain's consensus process. They must balance computational efficiency and data security, ensuring that aggregated updates reflect accurate contributions without compromising sensitive information.

Worker: Decentralized Model Training

Worker nodes are the primary contributors to model training. They locally train the model using their private data and submit updates to the system. Their assignment is based on their strong performance (optimization) and privacy capabilities, allowing them to contribute securely and efficiently.

System Synergy: Election-Based Coordination

The roles of validators and miners are coordinated through an election mechanism. This mechanism considers both device characteristics and current network conditions, ensuring that role assignments remain optimal over time. This creates a synergistic environment where resources are used effectively and securely.

Adaptability: Resilience through Dynamic Role Updates

As network conditions and device metrics evolve, roles are dynamically reassigned. This adaptability ensures continued performance and compliance with privacy standards, even as devices join or leave the FL system or their capabilities change.

Governance and Trust via Blockchain

The use of blockchain ensures transparent and decentralized governance. Every role decision and update is recorded on-chain, providing verifiability and fostering trust among participants. The immutable ledger ensures that malicious behavior can be tracked and traced.

Secure Communication and Monitoring

To protect data in transit, the system uses encrypted channels and strict authentication protocols. Continuous monitoring helps identify underperforming or risky nodes, allowing for proactive intervention and optimization.

3.7.7 Experiments

To evaluate the proposed framework, we designed four experimental scenarios, each involving 100 clients over 20 communication rounds. These scenarios simulate real-world challenges in decentralized FL, particularly in the presence of adversaries and privacy constraints.

- **Scenario 1: Standard Decentralized FL (Baseline)**
  A conventional setup where clients collaboratively train a global model assuming all participants are honest.
- **Scenario 2: Decentralized FL with Malicious Clients**
  Approximately 20% of the clients act maliciously, injecting poisoned data or manipulating gradients.
- **Scenario 3: DP-Enhanced FL with Malicious Clients**
  Extends Scenario 2 with differential privacy (DP) mechanisms to mitigate malicious impact while preserving privacy.
- **Scenario 4: Blockchain-Based Role Determination with DP**
  Incorporates DP and a private blockchain-based role assignment to dynamically exclude or downgrade malicious clients.

Experimental Setup and Evaluation Metrics

We conducted this experiment using the same laptop described in Section 3.5.2, ensuring consistency in the computational environment.

Key parameters:

- Learning rate: 0.01
- Batch size: 64
- Epochs per round: 10

Metrics:

- **Accuracy:** Final and per-round classification accuracy.
- **Robustness:** Resistance to adversarial manipulation.
- **Privacy Preservation:** DP effectiveness in confidentiality.

3.7.8 Results Analysis

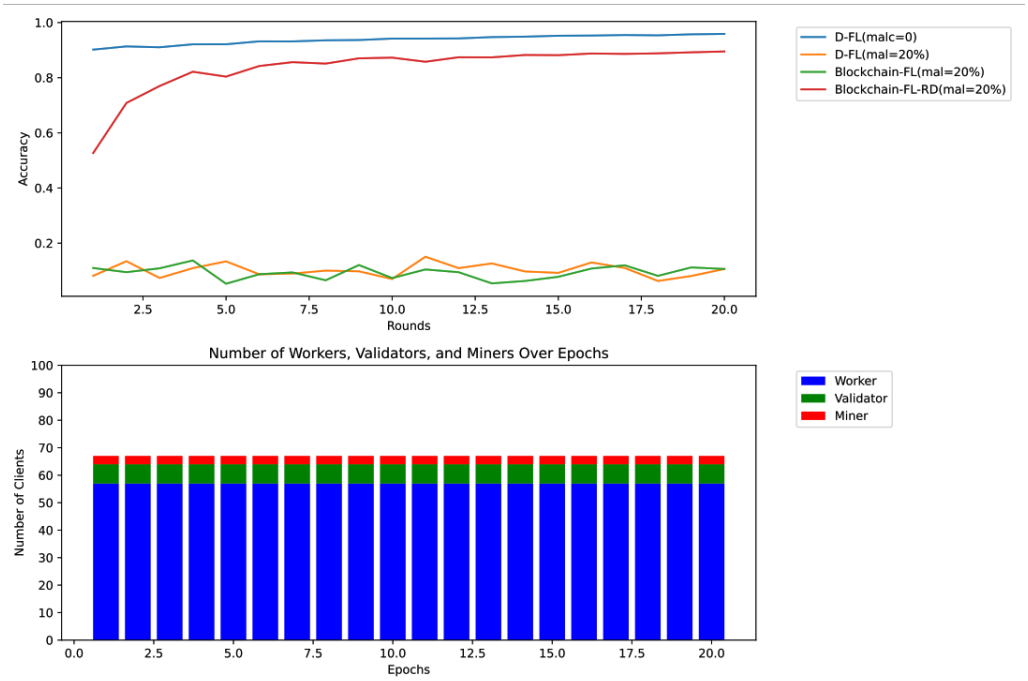

Figure 3.5 Performance comparison across scenarios on IID data

Key observations:

- Baseline (no adversaries) peaks at 97% accuracy.

- Malicious clients reduce performance to 10–17%.
- Blockchain-based role determination recovers up to 87% accuracy.

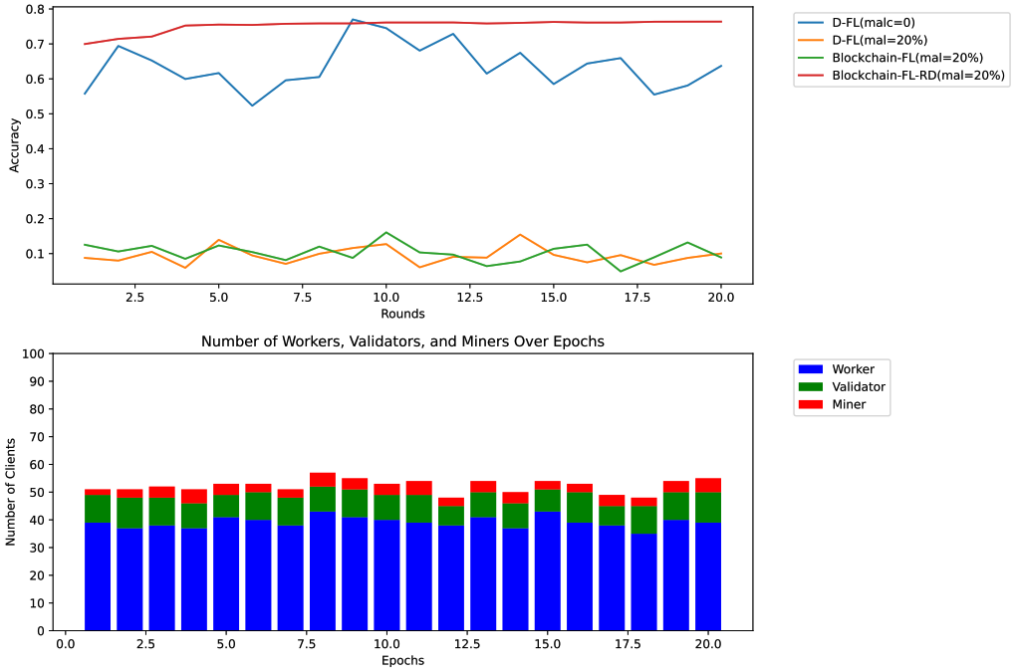

Figure 3.6 Performance comparison across scenarios on non-IID data

In non-IID conditions, the blockchain-enhanced method maintains performance by filtering outliers.

Table 3.7 Comparative Results of Previous Works and the Proposed Method

Algorithm	**Objective**	**Accuracy**
Random Selection	Optimization	18.9%
Oort	Optimization	16.4%
Active Federated Learning	Optimization	18.4%
Novel-Reputation	Security	67.7%
Proposed Method	**Security + Optimization**	**87.39%**

3.8 Role Determination Performance on Different Models

Table 3.8 Results of Experiments on Different Case Scenarios

Datasets and Models	SimpleNN	MLP	CNN	Net0
Best Case				
MNIST	83.12%	85.9%	82.29%	87.39%
FASHION MNIST	72.55%	72.38%	72.54%	77.02%
CIFAR-10	29.26%	29.14%	30.24%	37.61%
Average Case				
MNIST	78.28%	79.59%	77.6%	86.77%
FASHION MNIST	71.43%	70.88%	71.11%	76.6%
CIFAR-10	29.61%	29.05%	25.83%	37.19%
Worst Case				
MNIST	52.61%	60.96%	57.28%	79.92%
FASHION MNIST	52.04%	55.34%	57.49%	73.07%
CIFAR-10	28.65%	21.99%	15.63%	37.17%

3.9 Conclusion

This chapter presented a comprehensive exploration of dynamic participant selection mechanisms within FL, particularly in IoMT environments. We introduced a novel approach that leverages blockchain-assisted role determination and differential privacy to enhance the security, efficiency, and scalability of both centralized and decentralized FL systems.

Through rigorous experimentation across various scenarios ranging from standard FL to adversarial environments with up to 20% malicious clients we demonstrated that the proposed method significantly improves model accuracy, robustness, and privacy preservation. Notably, the integration of a private blockchain framework facilitated transparent and secure role assignment, while dynamic rule adaptation enabled continuous optimization even in challenging or static system conditions.

Evaluation across multiple neural network models and datasets confirmed the method's adaptability and resilience, particularly under non-IID data distributions and adverse op-

erating scenarios. Compared to existing optimization- or security-focused methods, our approach consistently outperformed in balancing both objectives.

Future research will aim to extend this methodology to more complex, large-scale, and fully decentralized FL ecosystems. This includes refining probabilistic role assignment formulas, incorporating advanced cryptographic techniques such as homomorphic encryption and secure multi-party computation, and applying the framework in high-stakes domains like healthcare and finance.

Overall, this proposed work lays a solid foundation for trust-aware, privacy-preserving, and performance-optimized federated learning systems in sensitive and dynamic environments.

CHAPTER 4: ENHANCED FRAMEWORK WITH ATTACK RESISTANCE

4.1 Introduction

Building upon the participant selection mechanism proposed in Chapter 3 — which is adaptable to both centralized and decentralized FL — this chapter presents an enhanced framework that addresses security vulnerabilities still present in IoMT environments. While the original mechanism improves efficiency and fairness in participant selection, it does not fully address certain advanced threats such as impersonation attacks, poisoning attacks, and post-consensus manipulation.

To overcome these challenges, we introduce a role determination mechanism as a critical extension of our initial approach. This method enhances the selection process by dynamically assigning functional roles to participants based on optimization and privacy metrics, thereby enabling more intelligent and secure collaboration within the FL ecosystem.

The enhanced framework, termed **BlockGuard-RD**, incorporates this role determination logic into a multi-layered blockchain-assisted architecture. It leverages dynamic access control, secure consensus mechanisms, and real-time threat evaluation to provide strong resilience against a range of security threats in IoMT scenarios. Through this layered design, BlockGuard-RD not only improves the robustness of the participant selection strategy but also establishes a higher degree of immunity against attacks that traditional FL setups fail to mitigate.

4.2 BlockGuard-RD Framework

The BlockGuard-RD framework is designed to address the critical need for security and privacy in IoMT environments by combining the strengths of blockchain technology and FL. Its novel feature is a **dynamic role determination mechanism** that assigns roles—such as workers, validators, and miners—based on real-time assessments of device trustworthiness, privacy scores, and performance efficiency. This ensures a secure, adaptive system resilient to various IoMT-specific attacks and operational challenges.

To contextualize the novelty of our approach, Table 4.1 provides a comparative analysis of BlockGuard-RD with existing blockchain-based and FL frameworks. It highlights key architectural differences and showcases how BlockGuard-RD addresses the current limitations in IoMT environments through its integrated role determination strategy and IoMT-specific optimizations.

Table 4.1 Comparison of BlockGuard-RD with Related Frameworks

Framework	**Blockchain Integration**	**FL Support**	**Role Determination Strategy**	**IoMT-Specific Optimization**
[99] Alliance Chain Scheme	Yes (anonymity, partial key management)	No	Not considered	Limited (IoT-cloud data sharing)
[100] IoV Trust System	Yes (trust-aware blockchain updates)	No	Not considered	No (focus on vehicular networks)
[103] FL-BETS	Yes (secure aggregation and fraud detection)	Yes	Not considered	Yes (healthcare-specific task scheduling)
[104] Multi-Level Blockchain	Yes (BigchainDB with filtering)	Yes	Not considered	Yes (EHR protection, patient privacy)
[106] ChainFL	Yes (secure offloading using blockchain)	Yes	Not considered	Partially (IIoT and edge computing)
[107] FedChain	Yes (cross-chain PoS consensus)	No	Partial (Stackelberg game model)	No
[108] Hyperledger EHR	Yes (Fabric/Composer with IPFS)	No	Not considered	Yes (EHR access control, privacy)
BlockGuard-RD (Proposed)	**Yes (multi-role blockchain)**	**Yes (secure FL training)**	**Yes (trust-performance adaptive)**	**Yes (role-aware, IoMT-optimized)**

As evident from the comparison, BlockGuard-RD is the only framework that fully integrates federated learning, blockchain, and dynamic role determination tailored to IoMT environments.

The BlockGuard-RD framework is structured around three core layers—Federated Learning, Blockchain, and Role Determination—designed to address key challenges in trust, privacy, and resource optimization. Figure 4.1 provides an overview of its architecture.

4.2.1 Architecture Overview

BlockGuard-RD adopts a multilayer architecture composed of four interdependent layers, as illustrated in Figure 4.1.

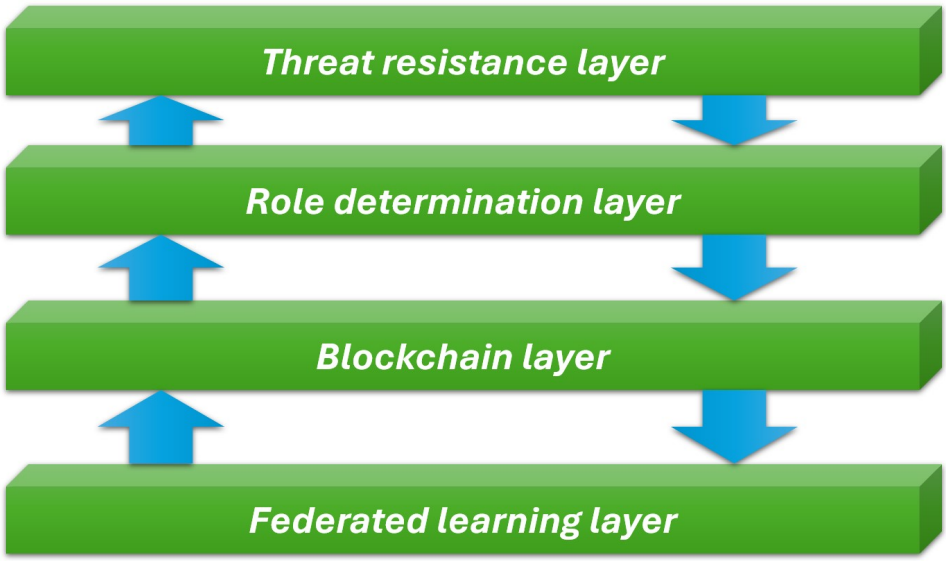

Figure 4.1 **BlockGuard-RD Layered Architecture:** A multi-layered structure integrating Federated Learning, Blockchain, Role Determination, and Threat Resistance to enhance security, privacy, and adaptability in IoMT environments.

- **Federated Learning (FL) Layer:**
  - Performs decentralized model training while preserving data confidentiality.
  - Employs lightweight differential privacy (DP) to obscure local gradients before aggregation.
  - Quantifies each participant's privacy level according to the applied noise and update frequency.

- **Blockchain Layer:**
  - A permissioned blockchain securely stores model-related metadata such as hashes, trust values, and assigned roles.
  - Smart contracts regulate access control and verify the integrity of role assignments and model updates.
  - Consensus mechanisms (e.g., PoS and PoW) ensure transparency and fault tolerance across the network.
- **Role Determination Layer:**
  - Dynamically evaluates each device based on three main criteria: trust, privacy, and optimization efficiency.
  - Assigns operational roles accordingly:
    - **Workers:** High trust and strong computational resources; perform local updates.
    - **Validators:** Moderate optimization and high privacy; verify model integrity.
    - **Miners:** High optimization and blockchain capability; finalize validated blocks.
  - Generates *trust scores* and *post-consensus indicators* that are reused by the upper layer to assess network reliability.
- **Threat Resistance Layer:**
  - Operates as a monitoring and defensive layer built on the trust and consensus outputs from the Role Determination Layer.
  - Detects and mitigates malicious or inconsistent behavior using adaptive trust decay and anomaly detection strategies.
  - Ensures robustness against poisoning, Sybil, and inference attacks while maintaining system stability and model quality.

4.2.2 Metric-Driven Role Assignment Logic

The following metrics and thresholds are combined to assign roles efficiently and securely:

- **Trust Score (T_i):** Updated after each round using a decay-reward model:

$$T_i^{(t+1)} = \gamma T_i^{(t)} + \alpha(r_i - p_i)$$

where r_i is reliability (e.g., timely update), p_i is penalty for misbehavior, γ is a decay factor, and α is learning rate.

- **Privacy Score (P_i):** Scaled from 0–10 based on differential privacy usage, e.g.,

$$P_i = 10 \cdot (1 - e^{-\epsilon_i})$$

where ϵ_i is the privacy budget used by device i.

- **Optimization Score (O_i):** Aggregates resource availability and efficiency:

$$O_i = w_1 \cdot \text{CPU}_i + w_2 \cdot \text{Bandwidth}_i + w_3 \cdot \text{Latency}_i^{-1}$$

where weights w_j reflect resource priority.

- **Fibonacci-Golden Ratio Scheduling:** Periodic reassignment uses Fibonacci indices and golden ratio $\phi = 1.618$ to rebalance roles fairly and avoid stagnation.

4.2.3 Dynamic Role-Based Access Control

1. **Trust Score Calculation:** Reflects device behavior consistency, anomaly resistance, and update integrity.
2. **Performance Assessment:** Devices are benchmarked for resource efficiency, ensuring miners can handle ledger tasks reliably.
3. **Adaptive Role Reassignment:** Fibonacci intervals and golden-ratio indexing ensure fresh reassignment while avoiding redundant computation and stale trust states.

4.2.4 Role Assignment Algorithm

To operationalize the dynamic role allocation mechanism, we introduce an algorithm that leverages Fibonacci indexing and the golden ratio $\phi = 1.618$ to ensure balanced, trust-aware, and adaptive role selection among IoMT participants.

4.2.5 Fibonacci-based Role Assignment Justification

In the proposed framework, we introduce a novel **Fibonacci-based Role Assignment Algorithm** for participant selection and role distribution in blockchain-assisted FL environments. The choice of the Fibonacci sequence is motivated by its *self-organizing and*

naturally distributed characteristics, which align well with the needs of dynamic, decentralized systems such as FL networks.

Why Fibonacci?

The Fibonacci sequence offers several key advantages:

- **Non-uniform but deterministic selection**: Fibonacci indices provide a sparse yet predictable selection pattern, enabling efficient and fair participant distribution while avoiding centralized clustering.
- **Golden ratio heuristic**: By incorporating the golden ratio $\phi \approx 1.618$, we determine top-performing or "central" clients in a mathematically principled way, inspired by optimal resource distribution observed in natural systems.
- **Scalability**: The use of Fibonacci-indexed client selection naturally adapts to varying network sizes without requiring exhaustive search or manual tuning.
- **Trust-weighted selection**: When combined with dynamic trust scores and varying privacy/optimization levels, the algorithm supports robust and resilient role assignment even under adversarial conditions.

Role Assignment with Consensus Overrides

To enhance flexibility, the algorithm incorporates *consensus-aware role overrides*, tailored to specific blockchain consensus protocols:

- **PoW and PoS**: Default all roles to `worker` with a single `validator`, reducing complexity and computational load.
- **DPoS**: Select top trusted clients as `validators`, simulating delegate-based validation mechanisms.
- **PBFT**: Assign clients as `replicas`, promoting fault-tolerant execution with a fixed validator subset.
- **PoA**: Prioritize participants with high trust scores, assigning a small subset as `validators` and the rest as `workers`.

This dual-layer strategy—Fibonacci-based initial role selection followed by consensus-driven adjustments—ensures improved **resilience, scalability, and adaptability** in FL systems, particularly in IoMT environments where trust, privacy, and performance constraints are critical.

Algorithm 3 Fibonacci-based Role Assignment with Consensus Overrides

Require: n (number of clients), $privacy\_levels$, $optimization\_levels$, $malicious\_clients$, $trust\_scores$, $consensus$
Ensure: $roles$

Initialize $roles \leftarrow$ array of n elements set to "eliminated"
Initialize Fibonacci sequence $F \leftarrow [0, 1]$
while $F[-1] < n$ **do**
    Append $F[-1] + F[-2]$ to F
end while
Remove first two elements from F
$\phi \leftarrow 1.618$
for all $idx \in F$ **do**
    if $idx < n$ and $trust\_scores[idx] > 0$ **then**
        if $privacy\_levels[idx] \geq 8$ **then**
            $roles[idx] \leftarrow$ validator if $optimization\_levels[idx] \geq 8$, else worker
        else if $privacy\_levels[idx] \geq 4$ **then**
            $roles[idx] \leftarrow$ miner if $optimization\_levels[idx] \geq 8$, else worker
        else
            $roles[idx] \leftarrow$ worker
        end if
        $trust\_scores[idx] \leftarrow trust\_scores[idx] + 0.05$
    end if
end for
$top\_idx \leftarrow \lfloor n/\phi \rfloor$
if $top\_idx < n$ and $roles[top\_idx] \neq$ eliminated **then**
    $roles[top\_idx] \leftarrow$ validator
    $trust\_scores[top\_idx] \leftarrow trust\_scores[top\_idx] + 0.1$
end if
for all $i \in malicious\_clients$ **do**
    $roles[i] \leftarrow$ eliminated
    $trust\_scores[i] \leftarrow -1$
end for
▷ Consensus-specific role overrides
if $consensus \in$ {PoW, PoS} **then**
    Set all $roles$ to worker
    $roles[top\_idx] \leftarrow$ validator
else if $consensus =$ DPoS **then**
    Select top 5 clients with highest $trust\_scores$ as validators
    Set remaining $roles$ to worker
else if $consensus =$ PBFT **then**
    Set all $roles$ to replica
    Assign first 4 roles as validator
else if $consensus =$ PoA **then**
    Select clients with $trust\_score > 1.0$
    Assign top 3 as validator, others as worker
end if
return $roles$

4.2.6 Security Features

BlockGuard-RD provides:

- **DoS Resistance:** Exclusion of low-trust devices and decentralized structure reduce vulnerability.
- **Impersonation Mitigation:** Dynamic trust scores and secure identity management prevent unauthorized access.
- **Data Poisoning Defense:** Validator-based verification of updates with cross-validation and anomaly detection.
- **Privacy Protection:** FL with differential privacy and encrypted metadata ensures patient confidentiality.

4.2.7 Workflow Illustration

1. **Initialization:** Devices register with reported trust, privacy, and performance metrics.
2. **Role Assignment:** RDM assigns roles based on real-time metric evaluation.
3. **Training Round:** Workers train and submit updates; validators verify; miners update blockchain.
4. **Reevaluation:** At each interval, trust is updated, roles reassigned using Fibonacci and ϕ logic.

This multilayered and metric-driven framework ensures robust, privacy-preserving, and attack-resistant operations in dynamic IoMT networks.

4.3 Experimental Setup and Results

4.3.1 Experiment Configuration

To evaluate the proposed BlockGuard-RD framework, a simulation-based FL environment was implemented using PyTorch. The following configuration was used:

- **Dataset**: MNIST
- **Model**: Simple Feedforward Neural Network (SimpleNN)

- **Learning Rate**: 0.005
- **Optimizer**: Stochastic Gradient Descent (SGD) with momentum 0.9
- **Scheduler**: StepLR with step size 10 and decay factor 0.5
- **Epochs per client**: 1
- **Number of Communication Rounds**: 100
- **Number of Clients**: 100
- **Malicious Clients Percentage**: 20%
- **Evaluation Metrics**: Accuracy, Precision, and Threat Resistance

The evaluation compares the following two frameworks:

- **Basic Framework**: Blockchain-assisted FL without any resistance to threats.
- **Advanced Framework (BlockGuard-RD)**: Our proposed resilient system integrating dynamic role determination, Fibonacci and golden ratio mechanisms, and trust-based filtering.

4.4 Comparative Analysis and Architectural Justification

This section presents a comprehensive evaluation of the proposed multi-layered framework in comparison to a conventional FL baseline. The evaluation is conducted with a focus on accuracy, latency, and robustness under adversarial conditions such as DDoS attacks, impersonation, and data poisoning. The advanced framework's modular design—incorporating FL, blockchain integration, role determination, and threat resistance—demonstrates significant improvements across all metrics.

4.4.1 Accuracy Evaluation

Figure 4.2 illustrates the accuracy progression over 100 training rounds for both the advanced and basic frameworks. The advanced framework achieves a rapid convergence, reaching over 95% accuracy within the first 30 rounds, while the basic framework stagnates around 29% accuracy throughout. This disparity can be attributed to the enhanced participant selection and poisoning mitigation mechanisms employed in the proposed architecture.

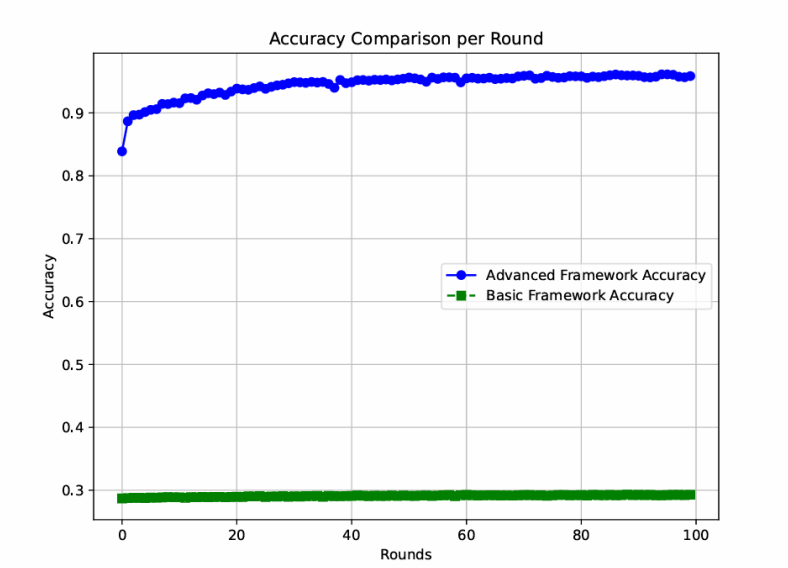

Figure 4.2 Accuracy Comparison per Round

The superior accuracy of the proposed approach stems from the use of a blockchain-backed FL environment that ensures traceable and tamper-proof model updates. More importantly, the **role determination layer** dynamically assesses participants based on two key metrics: *privacy level* and *optimization level*. These metrics are used to compute a *trust score* for each node, which directly impacts its role in the network. Nodes with insufficient trust scores are excluded from sensitive roles such as aggregation or validation, thus reducing the risk of data poisoning and enhancing the quality of model updates.

4.4.2 Latency Comparison

As depicted in Figure 4.3, the proposed framework significantly outperforms the baseline in terms of latency. The average latency per batch (10 rounds) for the advanced system remains below 1.65 seconds, whereas the basic system exhibits an average latency exceeding 4.0 seconds.

This improvement is largely due to the **role determination layer**, which minimizes communication overhead by assigning roles based on each node's computational and network capabilities. Furthermore, the use of a decentralized ledger in the **blockchain layer** eliminates the need for a centralized aggregator, allowing more efficient peer-to-peer update verification. The **threat resistance layer** also contributes by preemptively filtering out potentially malicious or unstable nodes, thereby reducing the impact of DoS attacks on latency.

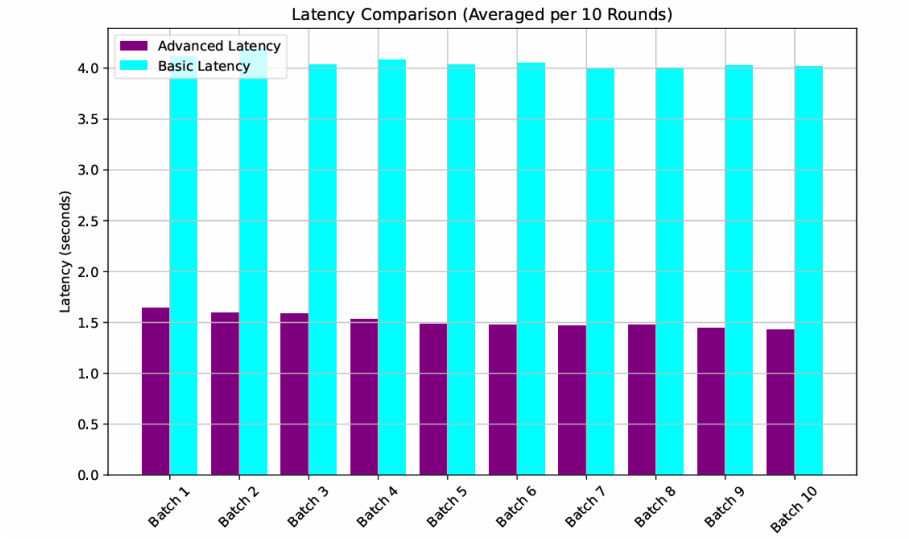

Figure 4.3 Latency Comparison Averaged per 10 Rounds

4.4.3 Threat Resistance Analysis Using Role Determination Scores

Figure 4.4 presents the relationship between the *Threat Resistance* score and the *Probability of Failure* across multiple training rounds in the presence of adversarial scenarios, such as impersonation and denial-of-service (DoS) attacks. The experimental results highlight the critical role of our Role Determination Module (RDM) in dynamically enhancing security and system reliability in blockchain-enabled FL environments.

The blue curve (right axis) illustrates the ATR score, which reflects the resilience of the system to adversarial behavior by leveraging dynamic role reconfiguration based on privacy and optimization metrics. These scores are computed using a hybrid strategy that incorporates trust scores, privacy sensitivity, utility contribution, and responsiveness—thereby ensuring that only participants with favorable behavioral and performance profiles are granted critical roles (e.g., leaders, aggregators).

Conversely, the red histogram (left axis) quantifies the empirical *Probability of Failure*, representing the fraction of consensus or aggregation failures during each round, often triggered by malicious participation or communication dropouts. Initially, the failure rate remains low, suggesting that most participants are behaving benignly or have not yet been targeted. However, as the system progresses beyond 60 rounds, the threat landscape intensifies—possibly due to accumulated targeted attacks or strategic poisoning attempts.

Notably, the *Threat Resistance* score exhibits a positive trajectory precisely when the probability of failure begins to rise. This inverse correlation suggests that the RDM effectively adapts to changing threat conditions by recalibrating the role assignments. Participants with high-risk signals are either excluded from critical pathways or demoted to low-impact roles. This adaptability plays a pivotal role in countering impersonation attacks—

where adversaries attempt to hijack high-trust identities—and in mitigating DoS attempts that rely on overwhelming leader nodes or central aggregators.

In essence, the integration of the Role Determination Module introduces a resilient behavioral layer to the system architecture. It dynamically preserves security and efficiency by:

- Preventing high-impact roles from being assigned to unreliable or compromised clients.
- Prioritizing privacy-aware clients with high utility for participation, ensuring robustness even under heterogeneous data distributions.
- Lowering attack surface exposure through distributed trust and score-based privilege management.

Therefore, the correlation observed in Figure 4.4 empirically validates the hypothesis that score-based adaptive role assignment is a crucial architectural enhancement for resisting advanced attacks in federated IoMT systems, especially in post-consensus blockchain layers.

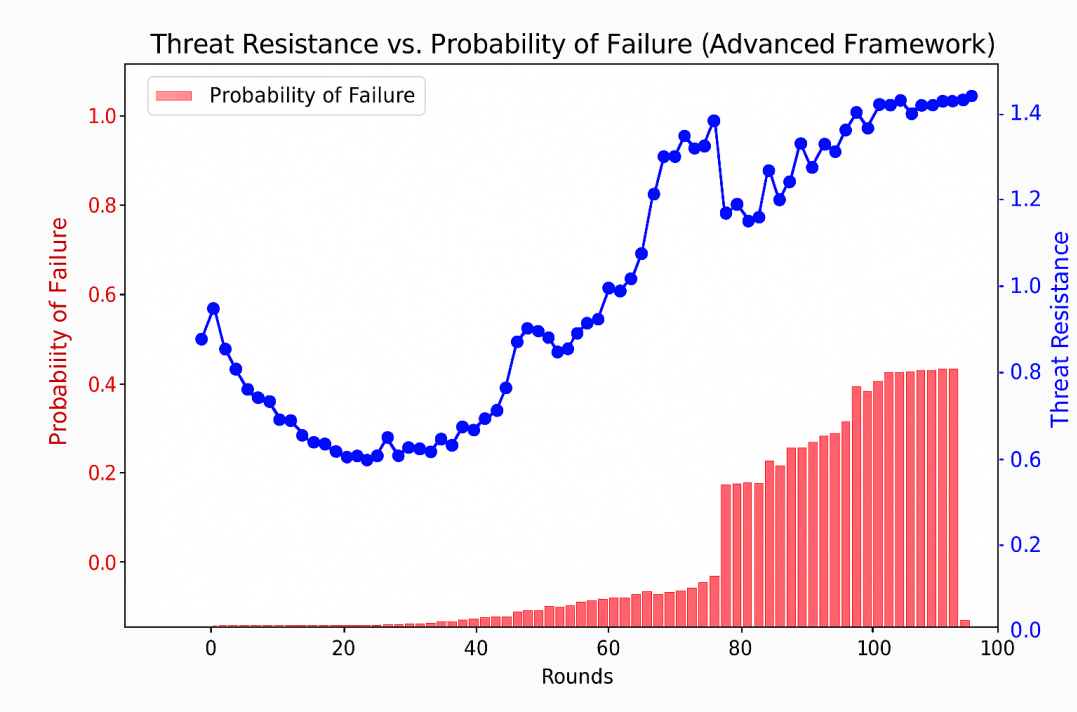

Figure 4.4 Threat Resistance vs. Probability of Failure across training rounds. Blue: *Threat Resistance* score; Red: Empirical failure rate due to impersonation and DoS attacks.

4.4.4 Consensus-wise Threat Resistance Evaluation

Figure 4.5 provides a visual comparison of threat resistance levels across five widely adopted blockchain consensus mechanisms—Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Authority (PoA)—using needle gauges for three primary threat classes: data poisoning, impersonation, and denial-of-service (DoS). Each needle indicates a resistance score normalized on a scale from 0 (low resilience) to 1 (high resilience), allowing for direct cross-consensus interpretation.

Proof of Work (PoW). PoW demonstrates high resistance to impersonation (0.82) and DoS attacks (0.83), benefiting from its inherently decentralized and compute-intensive validation process. However, its data poisoning resistance score is moderate (0.74), suggesting some vulnerability in participant vetting due to its open-access mining model. This indicates that while PoW is robust against systemic service disruption and identity spoofing, it requires auxiliary mechanisms—such as the Role Determination Module (RDM)—to harden against malicious model updates.

Proof of Stake (PoS). PoS exhibits moderate resilience across all threat classes, with scores of 0.72 for data poisoning, 0.76 for impersonation, and 0.78 for DoS. These values reflect its stake-weighted consensus model, which can provide accountability but may still allow entry to malicious actors if stake thresholds are low. The uniformity in its threat profile implies that PoS benefits significantly from additional scoring mechanisms like trust-based role allocation to elevate its defense capabilities.

Delegated Proof of Stake (DPoS). DPoS shows slightly lower resistance than PoS across all metrics—0.70 (data poisoning), 0.78 (impersonation), and 0.77 (DoS). Its reliance on a small set of elected validators introduces centralization risks, making it somewhat more susceptible to targeted attacks on trusted nodes. While efficient in performance, DPoS may require enhanced trust filtering and dynamic role rotation to reduce its security exposure.

Practical Byzantine Fault Tolerance (PBFT). PBFT consistently achieves the highest resistance scores—0.80 for data poisoning, 0.82 for impersonation, and 0.82 for DoS. This superior performance stems from its quorum-based consensus approach, which ensures that only a supermajority of vetted participants can influence state changes. When integrated with the RDM's adaptive scoring and role reassignment strategies, PBFT forms a robust foundation for secure FL in sensitive IoMT environments.

Proof of Authority (PoA). PoA presents a mixed profile, with strong data poisoning resistance (0.76) but slightly lower impersonation (0.77) and DoS (0.75) scores. While its authority-based node validation improves consistency and speed, the centralized nature of node approval introduces fixed points of failure. Thus, PoA benefits significantly from decentralized role scoring and fallback mechanisms under adversarial pressure.

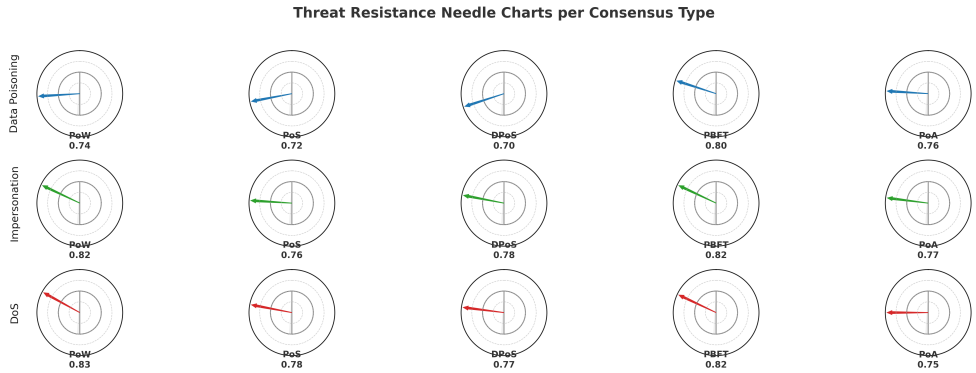

Figure 4.5 Needle chart illustrating threat resistance scores for Data Poisoning, Impersonation, and DoS attacks across five consensus protocols. Higher needle positions indicate greater resilience.

This consensus-wise breakdown confirms that the combination of adaptive role assignment and blockchain consensus choice significantly influences the threat resilience of federated IoMT systems. Notably, consensus algorithms like PBFT and PoW—when enhanced with score-based RDM integration—offer the most secure operational profile against modern federated attacks.

4.5 Conclusion

The results presented in this chapter affirm the architectural and functional superiority of the proposed BlockGuard-RD framework over conventional FL baselines. By systematically integrating FL with blockchain technology and augmenting it with a dynamic Role Determination Module (RDM), the system achieves rapid convergence, low latency, and robust resistance to advanced adversarial threats.

Empirical analyses demonstrate that BlockGuard-RD accelerates model convergence (over 95% accuracy in early rounds), reduces system latency through intelligent role allocation, and significantly improves resilience to data poisoning, impersonation, and DoS attacks. The framework's dynamic, metric-driven role assignment ensures that only trusted and capable devices assume critical roles, thereby maintaining both security and operational efficiency in heterogeneous IoMT environments.

In summary, BlockGuard-RD establishes a scalable, secure, and privacy-preserving foundation for next-generation digital healthcare infrastructures. Future work will extend this framework to address scalability in large-scale IoMT deployments and incorporate advanced privacy-preserving techniques for real-world healthcare applications.

CHAPTER 5

CONCLUSION AND PERSPECTIVES

This thesis has explored the convergence of the Internet of Medical Things (IoMT), Federated Learning (FL), and blockchain as enabling technologies for secure, privacy-preserving, and intelligent healthcare infrastructures. Through an extensive analysis of architectural and methodological challenges, ranging from interoperability and scalability to data privacy and energy constraints, it has provided a unified understanding of how distributed intelligence can strengthen IoMT systems.

The **first contribution** of this research was a comprehensive comparative analysis of existing participant selection strategies in Federated Learning. This study established a structured taxonomy that classified selection methods according to their underlying principles, optimization criteria, and privacy implications. The analysis highlighted fundamental trade-offs between accuracy, computational efficiency, and fairness, providing the analytical foundation for the subsequent contributions.

The **second contribution** consisted of the design and implementation of a novel *probabilistic participant selection method* applicable to both centralized and decentralized FL architectures. This method dynamically adjusts the selection probability of each client according to its optimization capacity and privacy level, thereby ensuring a better balance between performance, resource efficiency, and data protection. Experimental validation demonstrated the superiority of the proposed approach over traditional deterministic methods in terms of model accuracy, convergence rate, and fairness.

The **third contribution** introduced the **BlockGuard-RD framework**, a blockchain-enhanced FL architecture integrating the proposed participant selection mechanism within a secure, role-based ecosystem. This framework unifies federated optimization, blockchain consensus, and role determination to enhance transparency, resilience, and robustness against malicious or unreliable participants. Through extensive simulations, BlockGuard-RD was shown to maintain high model performance while providing strong resistance to data poisoning, impersonation, and denial-of-service attacks.

Critical Reflection. While the proposed framework achieved significant progress in security, scalability, and privacy, several practical aspects remain to be addressed. The validation was carried out through simulations; therefore, real-world deployment within

heterogeneous healthcare infrastructures may introduce new challenges such as energy constraints, communication instability, and interoperability with medical standards. Additionally, the probabilistic role assignment model could be extended using reinforcement learning or game-theoretic decision models to improve its adaptability to dynamic environments.

Perspectives. Future research directions include the development of adaptive, AI-driven threat detection modules that leverage federated meta-learning for proactive defense. Extending BlockGuard-RD toward multi-blockchain interoperability could enhance cross-domain collaboration and scalability. Furthermore, experimental deployment in realistic clinical or smart-hospital contexts would provide valuable insight into latency, energy consumption, and user acceptability under real operational conditions.

In conclusion, this thesis delivers a secure, scalable, and intelligent framework for next-generation IoMT ecosystems. By combining Federated Learning, blockchain technology, and adaptive participant management, it contributes a concrete step toward the realization of trustworthy, privacy-aware, and efficient healthcare systems, paving the way for resilient connected medicine.

BIBLIOGRAPHY

[1] Yazdan Ahmad Qadri et al., "The Future of Healthcare Internet of Things: A Survey of Emerging Technologies", in: *IEEE Communications Surveys and Tutorials* 22.*2* (2020), pp. 1121–1167, DOI: 10.1109/COMST.2020.2973314.

[2] Vishnu Suresh, Jino Ramson, and Dr Jegan, "Internet of Medical Things (IoMT) - An Overview", in: *2020 International Conference on Devices, Circuits and Systems (ICDCS)*, Mar. 2020, pp. 101–104, DOI: 10.1109/ICDCS48716.2020.243558.

[3] Fatima Alshehri and Ghulam Muhammad, "A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare", in: *IEEE Access* 9 (2021), pp. 3660–3678, DOI: 10.1109/ACCESS.2020.3047960.

[4] Ahmed E. Khaled, "Internet of Medical Things (IoMT): Overview, Taxonomies, and Classifications", in: *Journal of Computer and Communications* 10.*8* (2022), pp. 64–89.

[5] Qinwang Niu et al., "Toward the Internet of Medical Things: Architecture, Trends and Challenges", in: *Mathematical Biosciences and Engineering* 21.*1* (2024), pp. 650–678, ISSN: 1551-0018, DOI: 10.3934/mbe.2024028, URL: https://www.aimspress.com/article/doi/10.3934/mbe.2024028.

[6] Chenxi Huang et al., "Internet of Medical Things: A Systematic Review", in: *Neurocomputing* 557 (2023), p. 126719, ISSN: 0925-2312, DOI: 10.1016/j.neucom.2023.126719, URL: https://www.sciencedirect.com/science/article/pii/S0925231223008421.

[7] Naeem Askar et al., "Architecture, Protocols, and Applications of the Internet of Medical Things (IoMT)", in: *Journal of Communications* 17.*11* (Oct. 2022), pp. 900–918, DOI: 10.12720/jcm.17.11.900-918.

[8] Venkatesh Upadrista, “Health-IT Reference Architecture – The Internet of Medical Things Architecture for Healthcare Use Cases”, in: *Biomedical Journal of Scientific & Technical Research* 54.*5* (2024), pp. 46334–46342.

[9] M. J. Sudha and S. Viveka, “A Comprehensive Review of Architecture, Classification, Challenges, and Future of the Internet of Medical Things (IoMTs)”, in: *Medical Journal of Babylon* 19.*3* (2022), ISSN: 1812-156X.

[10] R, Sindhuja, Arvind S., Kapse, and Avinash S., Kapse, “A Survey of Internet of Medical Things (IoMT) Applications, Architectures and Challenges in Smart Healthcare Systems”, in: *ITM Web Conf.* 56 (2023), p. 05013, DOI: 10.1051/itmconf/20235605013, URL: https://doi.org/10.1051/itmconf/20235605013.

[11] Metty Paul et al., “Digitization of healthcare sector: A study on privacy and security concerns”, in: *ICT Express* (Feb. 2023), DOI: 10.1016/j.icte.2023.02.007.

[12] Mert Melih Ozcelik, Ibrahim Kok, and Suat Ozdemir, “A Survey on Internet of Medical Things (IoMT): Enabling Technologies, Security and Explainability Issues, Challenges, and Future Directions”, in: *Expert Systems* 42.*5* (2025), e70010 EXSY-Sep-23-2505.R1, e70010, DOI: https://doi.org/10.1111/exsy.70010, eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/exsy.70010, URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/exsy.70010.

[13] Awais Akram et al., “Secure and Interoperable IoMT-Based Smart Homes”, in: *IEEE Consumer Electronics Magazine* (2025), pp. 1–6, DOI: 10.1109/MCE.2025.3534442.

[14] Sita Rani et al., “Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review”, in: *Knowledge-Based Systems* 274 (2023), p. 110658, ISSN: 0950-7051, DOI: https://doi.org/10.1016/j.knosys.2023.110658, URL: https://www.sciencedirect.com/science/article/pii/S0950705123004082.

[15] Darin Mansor Mathkor et al., "Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends", in: *Journal of Infection and Public Health* 17.*4* (2024), pp. 559–572, ISSN: 1876-0341, DOI: https://doi.org/10.1016/j.jiph.2024.01.013, URL: https://www.sciencedirect.com/science/article/pii/S1876034124000194.

[16] Jing Wang, Mohammad Tabrez Quasim, and Bo Yi, "Privacy-preserving heterogeneous multi-modal sensor data fusion via federated learning for smart healthcare", in: *Information Fusion* 120 (2025), p. 103084, ISSN: 1566-2535, DOI: https://doi.org/10.1016/j.inffus.2025.103084, URL: https://www.sciencedirect.com/science/article/pii/S1566253525001575.

[17] H. Brendan McMahan et al., *Communication-Efficient Learning of Deep Networks from Decentralized Data*, 2023, arXiv: 1602.05629 [cs.LG], URL: https://arxiv.org/abs/1602.05629.

[18] C. Hu, J. Jiang, and Z. Wang, "Decentralized Federated Learning: A Segmented Gossip Approach", in: *arXiv preprint* (2019), arXiv:1909.02207.

[19] K. Chang et al., "Distributed Deep Learning Networks Among Institutions for Medical Imaging", in: *Journal of the American Medical Informatics Association* 25.*8* (2018), pp. 945–954, URL: https://doi.org/10.1093/jamia/ocy017.

[20] Xuhui Chen et al., "When Machine Learning Meets Blockchain: A Decentralized, Privacy-preserving and Secure Design", in: Dec. 2018, pp. 1178–1187, DOI: 10.1109/BigData.2018.8622598.

[21] Fan Lai et al., "Oort: Efficient Federated Learning via Guided Participant Selection", in: *15th USENIX Symposium on Operating Systems Design and Implementation (OSDI 2021)* (2021), DOI: 10.48550/arXiv.2010.06081.

[22] Z. Jiang et al., "Pisces: Efficient Federated Learning via Guided Asynchronous Training", in: *Proceedings of the 13th Symposium on Cloud Computing SoCC '22*, New York, NY, USA: Association for Computing Machinery, 2022, pp. 370–385, URL: https://doi.org/10.1145/3542929.3563463.

[23] X. Yao et al., "Federated Learning with Unbiased Gradient Aggregation and Controllable Meta Updating", in: *arXiv preprint* (2019), arXiv:1910.08234.

[24] T. Li et al., "Federated Optimization in Heterogeneous Networks", in: *arXiv preprint* (2020), arXiv:2003.00295.

[25] J. Wang et al., "Tackling the Objective Inconsistency Problem in Heterogeneous Federated Optimization", in: *arXiv preprint* (2020), arXiv:2002.07659.

[26] K. Shivam et al., "Decentralized Federated Learning Through Proxy Model Sharing", in: *Nature Communications* 14.*1* (2023), URL: https://doi.org/10.1038/s41467-023-38569-4.

[27] X. Li et al., "Heterogeneity-aware Fair Federated Learning", in: *Information Sciences* 619 (2023), pp. 968–986, URL: https://www.sciencedirect.com/science/article/pii/S0020025522013202.

[28] B. R. Chaudhury et al., *Fairness in Federated Learning via Core-Stability*, Unpublished manuscript, 2022.

[29] P. Kairouz et al., "Advances and Open Problems in Federated Learning", in: *Foundations and Trends® in Machine Learning* 14.*1–2* (2021), pp. 1–210.

[30] Wagan SA et al., "Internet of medical things and trending converged technologies: A comprehensive review on real-time applications", in: *Journal of King Saud University- Computer and Information Sciences* 34.*10, Part B* (2022), pp. 9228–9251, URL: https://www.sciencedirect.com/science/article/pii/S1319157822003263.

[31] Alajlan R, Alhumam N, and Frikha M, "Cybersecurity for Blockchain-Based IoT Systems: A Review", in: *Applied Sciences* 13.*13* (2023), URL: https://www.mdpi.com/2076-3417/13/13/7432.

[32] Singh N and Das A, "TFAS: two factor authentication scheme for blockchain enabled IoMT using PUF and fuzzy extractor", in: *The Journal of Supercomputing* (2023), pp. 1–50.

[33] Yaacoub JPA et al., "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations", in: *Internet of Things and Cyber-Physical Systems* 3 (2023), pp. 280–308, URL: https://www.sciencedirect.com/science/article/pii/S2667345223000238.

[34] Fernández-Alemán JL et al., "Security and privacy in electronic health records: A systematic literature review", in: *Journal of Biomedical Informatics* 46.*3* (2013), pp. 541–562, URL: https://www.sciencedirect.com/science/article/pii/S1532046412001864.

[35] Hatzivasilis G et al., "Review of security and privacy for the Internet of Medical Things (IoMT)", in: (2019), pp. 457–464.

[36] Wang Z, "Blind batch encryption-based protocol for secure and privacy-preserving medical services in smart connected health", in: *IEEE Internet of Things Journal* 6.*6* (2019), pp. 9555–9562.

[37] Gull S, Parah SA, and Muhammad K, "Reversible data hiding exploiting Huffman encoding with dual images for IoMT based healthcare", in: *Computer Communications* 163 (2020), pp. 134–149.

[38] Salim MM et al., "Homomorphic Encryption Based Privacy-Preservation for IoMT", in: *Applied Sciences* 11.*18* (2021), URL: https://www.mdpi.com/2076-3417/11/18/8757.

[39] Bonawitz K et al., "Practical secure aggregation for privacy-preserving machine learning", in: (2017), pp. 1175–1191.

[40] Wei K et al., "Federated Learning With Differential Privacy: Algorithms and Performance Analysis", in: *IEEE Transactions on Information Forensics and Security* 15 (2020), pp. 3454–3469.

[41] Dwork C, Roth A, et al., "The algorithmic foundations of differential privacy", in: *Foundations and Trends® in Theoretical Computer Science* 9.*3–4* (2014), pp. 211–407.

[42] Triastcyn A and Faltings B, "Federated learning with bayesian differential privacy", in: (2019), pp. 2587–2596.

[43] Karale S and Ranaware V, "Applications of blockchain technology in smart city development: A research", in: *International Journal of Innovative Technology and Exploring Engineering* 8.*11* (2019), pp. 556–559.

[44] Dai HN, Imran M, and Haider N, "Blockchain-enabled internet of medical things to combat COVID-19", in: *IEEE Internet of Things Magazine* 3.*3* (2020), pp. 52–57.

[45] Jin H et al., "Cross-cluster federated learning and blockchain for internet of medical things", in: *IEEE Internet of Things Journal* 8.*21* (2021), pp. 15776–15784.

[46] Chen Z et al., "Zero Knowledge Clustering Based Adversarial Mitigation in Heterogeneous Federated Learning", in: *IEEE Transactions on Network Science and Engineering* 8.*2* (2021), pp. 1070–1083.

[47] Lycklama H et al., "RoFL: Robustness of Secure Federated Learning", in: (2023).

[48] Asad M, Moustafa A, and Aslam M, "CEEP-FL: A comprehensive approach for communication efficiency and enhanced privacy in federated learning", in: *Applied Soft Computing* 104 (2021), p. 107235, URL: https://www.sciencedirect.com/science/article/pii/S1568494621001587.

[49] Elayan H, Aloqaily M, and Guizani M, "Digital twin for intelligent context-aware IoT healthcare systems", in: *IEEE Internet of Things Journal* 8.*23* (2021), pp. 16749–16757.

[50] S. Latif et al., "How 5G (and concomitant technologies) will revolutionize healthcare", in: *arXiv preprint* (2017), arXiv:1708.08746.

[51] M. S. Al-Rakhami et al., "FallDeF5: A Fall Detection Framework Using 5G-based Deep Gated Recurrent Unit Networks", in: (2021).

[52] H. N. Qureshi et al., "Communication Requirements in 5G-Enabled Healthcare Applications: Review and Considerations", in: *Healthcare MDPI* (2022), p. 293.

[53] J. Konečný et al., "Federated Learning: Strategies for Improving Communication Efficiency", in: (2017).

[54] B. Bhattacharya, "5G and IoMT: Moving Towards Modernization of Healthcare", in: *International Journal of Engineering Research Technology (IJERT)* 11 (2022), pp. 968–986, URL: https://www.ijert.org/5g-and-iomt-moving-towards-modernization-of-healthcare.

[55] S. Razdan and S. Sharma, "Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies", in: *IETE Technical Review* 39.*4* (2022), pp. 775–788, URL: https://doi.org/10.1080/02564602.2021.1927863.

[56] M. Liyanage et al., "5G Privacy: Scenarios and Solutions", in: *2018 IEEE 5G World Forum (5GWF)*, 2018, pp. 197–203.

[57] YC Yang et al., "Influential usage of big data and artificial intelligence in healthcare", in: *Computational and Mathematical Methods in Medicine* 2021 (2021), p. 2021.

[58] J Wu et al., "Topology-aware Federated Learning in Edge Computing: A Comprehensive Survey", in: (2023).

[59] Ç Dilibal, "Development of edge-IoMT computing architecture for smart healthcare monitoring platform", in: *2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, IEEE, 2020, pp. 1–4.

[60] SU Khan, AY Zomaya, and A Abbas, *Handbook of large-scale distributed computing in smart healthcare*, Springer, 2017.

[61] Gausiya Yasmeen, Nashra Javed, and Tasneem Ahmed, "Interoperability: A challenge for iomt", in: *ECS Transactions* 107.*1* (2022), p. 4459.

[62] Muhammad Shafiq et al., "Advances in IoMT for Healthcare Systems", in: *Sensors* 24.*1* (2024), ISSN: 1424-8220, URL: https://www.mdpi.com/1424-8220/24/1/10.

[63] Niyaz Ahmad Wani et al., "Explainable AI-driven IoMT fusion: Unravelling techniques, opportunities, and challenges with Explainable AI in healthcare", in: *Information Fusion* 110 (2024), p. 102472, ISSN: 1566-2535, DOI: https://doi.org/10.1016/j.inffus.2024.102472, URL: https://www.sciencedirect.com/science/article/pii/S1566253524002501.

[64] Ahmed Bouriche and Sihem Bouriche, “A systematic review on security vulnerabilities to preveny types of attacks in iomt”, in: *International Journal of Computations, Information and Manufacturing (IJCIM)* 2.*2* (2022).

[65] Michael Lee and Alice Kim, “Threats and Countermeasures in Federated Learning and Blockchain-based IoMT”, in: *IEEE Transactions on Information Forensics and Security* 19 (2024), pp. 120–135.

[66] Raj Patel and Neha Gupta, “Scalability Challenges in Large-Scale IoMT Deployments”, in: *IEEE Internet of Things Journal* 10.*5* (2023), pp. 200–215.

[67] Li Wang and Ankit Singh, “Efficient Resource Management for Distributed Learning in IoMT”, in: *ACM Transactions on Sensor Networks* 15.*2* (2024), pp. 75–90.

[68] Carlos Fernandez and Maria Rossi, “Power Consumption in IoMT Devices: Challenges and Solutions”, in: *Elsevier Future Generation Computer Systems* 128 (2023), pp. 340–355.

[69] Wei Zhao and Emily Brown, “Energy-Efficient Algorithms for Secure and Private Learning in IoMT”, in: *IEEE Transactions on Green Communications and Networking* 8.*1* (2024), pp. 110–125, URL: ADD_URL_HERE.

[70] Yusuf Ahmed and Xia Chen, “Green IoT Approaches for Sustainable IoMT Systems”, in: *Springer Sustainable Computing: Informatics and Systems* 36 (2023), pp. 280–295.

[71] Takayuki Nishio and Ryo Yonetani, “Client Selection for Federated Learning with Heterogeneous Resources in Mobile Edge”, in: *CoRR* abs/1804.08333 (2018), arXiv: 1804.08333, URL: http://arxiv.org/abs/1804.08333.

[72] Sicong Zhou et al., “PIRATE: A Blockchain Based Secure Framework of Distributed Machine Learning in 5G Networks”, in: *IEEE Network* 34.*6* (2020), DOI: 10.1109/MNET.001.1900658.

[73] Zhifeng Jiang et al., “Pisces: Efficient Federated Learning via Guided Asynchronous Training”, in: *Proceedings of the 13th Symposium on Cloud Computing*, SoCC22, San Francisco, California: Association for Computing Machinery, 2022, ISBN:

9781450394147, DOI: 10.1145/3542929.3563463, URL: https://doi.org/10.1145/3542929.3563463.

[74] Jack Goetz et al., *Active Federated Learning*, 2019, arXiv: 1909.12641 [cs.LG].

[75] Ang Li et al., "Hermes: an efficient federated learning framework for heterogeneous mobile clients", in: *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, MobiCom '21, New Orleans, Louisiana: Association for Computing Machinery, 2021, pp. 420–437, ISBN: 9781450383424, DOI: 10.1145/3447993.3483278, URL: https://doi.org/10.1145/3447993.3483278.

[76] Jianxin Zhao et al., "Participant Selection for Federated Learning With Heterogeneous Data in Intelligent Transport System", in: *IEEE Transactions on Intelligent Transportation Systems* 24.*1* (2023), DOI: 10.1109/TITS.2022.3149753.

[77] Yuwei Wang and Burak Kantarci, "A Novel Reputation aware Client Selection Scheme for Federated Learning within Mobile Environments", in: *2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (2020), DOI: 10.1109/CAMAD50429.2020.9209263.

[78] Attia Qammar et al., "Blockchain Based Optimized Edge Node Selection and Privacy Preserved Framework for Federated Learning", in: *Cluster Computing* (2023), DOI: 10.1007/s10586-023-04145-0.

[79] Zhifeng Jiang et al., *Lotto: Secure Participant Selection against Adversarial Servers in Federated Learning*, To appear, 2024, DOI: 10.48550/arXiv.2401.02880, arXiv: 2401.02880 [cs.CR], URL: https://arxiv.org/abs/2401.02880.

[80] Laraib Javed et al., "ShareChain: Blockchain enabled Model for Sharing Patient Data Using Federated Learning and Differential Privacy", in: *Expert Systems* 40.*5* (2023), e13131, DOI: 10.1111/exsy.13131.

[81] Huang Zeng et al., "A Federated Learning Framework with Blockchain Based Auditable Participant Selection", in: *Computers, Materials & Continua* 79.*3* (2024),

DOI: 10.32604/cmc.2024.052846, URL: https://www.techscience.com/cmc/v79n3/55240.

[82] Y. Li et al., "REWAFL: Residual Energy and Wireless Aware Participant Selection for Efficient Federated Learning over Mobile Devices", in: (2023), DOI: 10.48550/arXiv.2309.13643, arXiv: 2309.13643 [cs.LG], URL: https://arxiv.org/abs/2309.13643.

[83] Guowen Xu et al., "VerifyNet: Secure and Verifiable Federated Learning", in: *IEEE Transactions on Information Forensics and Security* 15 (2020), DOI: 10.1109/TIFS.2019.2929409.

[84] Chunlin Tian et al., *Ranking based Client Selection with Imitation Learning for Efficient Federated Learning*, Accepted for publication, 2024, DOI: 10.48550/arXiv.2405.04122, arXiv: 2405.04122 [cs.LG], URL: https://arxiv.org/abs/2405.04122.

[85] Yuchen Shi et al., "SAM: An Efficient Approach With Selective Aggregation of Models in Federated Learning", in: *IEEE Internet of Things Journal* 11.*11* (2024), DOI: 10.1109/JIOT.2024.3373822.

[86] Ahmad Faraz Khan et al., "FLOAT: Federated Learning Optimizations with Automated Tuning", in: EuroSys 24 (2024), DOI: 10.1145/3627703.3650081, URL: https://doi.org/10.1145/3627703.3650081.

[87] Sachin D N et al., "FedCure: A Heterogeneity Aware Personalized Federated Learning Framework for Intelligent Healthcare Applications in IoMT Environments", in: *IEEE Access* PP (Jan. 2024), DOI: 10.1109/ACCESS.2024.3357514.

[88] Linlin You et al., "SLMFed: A Stage Based and Layer Wise Mechanism for Incremental Federated Learning to Assist Dynamic and Ubiquitous IoT", in: *IEEE Internet of Things Journal* PP (Jan. 2024), DOI: 10.1109/JIOT.2024.3353793.

[89] Rahul Atul Bhope et al., "FLIPS: Federated Learning using Intelligent Participant Selection", in: *Proceedings of the 24th International Middleware Conference*, New York, NY, USA: Association for Computing Machinery, 2023, ISBN:

9798400701771, DOI: 10.1145/3590140.3629123, URL: https://doi.org/10.1145/3590140.3629123.

[90] Bin Jia et al., "Blockchain Enabled Federated Learning Data Protection Aggregation Scheme With Differential Privacy and Homomorphic Encryption in IIoT", in: *IEEE Transactions on Industrial Informatics* 18.*6* (2022), DOI: 10.1109/TII.2021.3085960.

[91] Pedro Miguel Sánchez Sánchez et al., "FederatedTrust: A solution for trustworthy federated learning", in: *Future Generation Computer Systems* 152 (2024), DOI: 10.1016/j.future.2023.10.013, URL: https://www.sciencedirect.com/science/article/pii/S0167739X23003886.

[92] Li Zhang et al., "Homomorphic Encryption Based Privacy Preserving Federated Learning in IoT Enabled Healthcare System", in: *IEEE Transactions on Network Science and Engineering* 10.*5* (2023), DOI: 10.1109/TNSE.2022.3185327.

[93] Muneeb Ul Hassan, Mubashir Husain Rehmani, and Jinjun Chen, "Differential Privacy in Blockchain Technology: A Futuristic Approach", in: *CoRR* abs/1910.04316 (2019), DOI: 10.48550/arXiv.1910.04316, arXiv: 1910.04316, URL: http://arxiv.org/abs/1910.04316.

[94] Mikail Mohammed Salim et al., "Homomorphic Encryption Based Privacy-Preservation for IoMT", in: *Applied Sciences* 11.*18* (2021), ISSN: 2076-3417, DOI: 10.3390/app11188757, URL: https://www.mdpi.com/2076-3417/11/18/8757.

[95] Peyman Vafadoost Sabzevar et al., "Anomaly Detection in IoMT Environment Based on Machine Learning: An Overview", in: *Computer and Knowledge Engineering* 7.*2* (2024), pp. 65–74.

[96] Moustafa Mamdouh et al., "Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions", in: *Computers and Security* 111 (2021), p. 102491, ISSN: 0167-4048, DOI: https://doi.org/10.1016/j.cose.2021.102491, URL: https://www.sciencedirect.com/science/article/pii/S0167404821003151.

[97] Archana Rani et al., "A smart agent-based approach for privacy preservation and threat mitigation to enhance security in the Internet of Medical Things", in: *Journal of Autonomous Intelligence* 7.*5* (2024), p. 1629, ISSN: 2630-5046, DOI: 10.32629/jai.v7i5.1629, URL: https://jai.front-sci.com/index.php/jai/article/view/1629.

[98] Mireya Lucia Hernandez-Jaimes et al., "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures", in: *Internet of Things* 23 (2023), p. 100887, ISSN: 2542-6605, DOI: https://doi.org/10.1016/j.iot.2023.100887, URL: https://www.sciencedirect.com/science/article/pii/S254266052300210X.

[99] Leyou Zhang et al., "Blockchain-Aided Anonymous Traceable and Revocable Access Control Scheme With Dynamic Policy Updating for the Cloud IoT", in: *IEEE Internet of Things Journal* 11.*1* (2024), pp. 526–542, DOI: 10.1109/JIOT.2023.3287190.

[100] Haibin Zhang et al., "Blockchain-Based Trust Management for Internet of Vehicles", in: *IEEE Transactions on Emerging Topics in Computing* 9.*3* (2021), pp. 1397–1409, DOI: 10.1109/TETC.2020.3033532.

[101] Wenjia Li and Houbing Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks", in: *IEEE Transactions on Intelligent Transportation Systems* 17.*4* (2016), pp. 960–969, DOI: 10.1109/TITS.2015.2494017.

[102] Chenyue Zhang et al., "AIT: An AI-Enabled Trust Management System for Vehicular Networks Using Blockchain Technology", in: *IEEE Internet of Things Journal* 8.*5* (2021), pp. 3157–3169, DOI: 10.1109/JIOT.2020.3044296.

[103] Abdullah Lakhan et al., "Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare", in: *IEEE Journal of Biomedical and Health Informatics* 27.*2* (2023), pp. 664–672, DOI: 10.1109/JBHI.2022.3165945.

[104] Masoumeh Jafari and Fazlollah Adibnia, "Securing IoMT healthcare systems with federated learning and BigchainDB", in: *Future Generation Computer Systems* 165 (2025), p. 107609, ISSN: 0167-739X, DOI: https://doi.org/10.1016/j.future.2024.107609, URL: https://www.sciencedirect.com/science/article/pii/S0167739X24005739.

[105] Jawad Rahman et al., "BlockFL: A Blockchain-enabled Federated Learning System for Securing IoVs", in: *2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall)*, 2024, pp. 1–6, DOI: 10.1109/VTC2024-Fall63153.2024.10757945.

[106] Guanjin Qu et al., "ChainFL: A Simulation Platform for Joint Federated Learning and Blockchain in Edge/Cloud Computing Environments", in: *IEEE Transactions on Industrial Informatics* 18.*5* (2022), pp. 3572–3581, DOI: 10.1109/TII.2021.3117481.

[107] Cong T. Nguyen et al., "FedChain: Secure Proof-of-Stake-Based Framework for Federated-Blockchain Systems", in: *IEEE Transactions on Services Computing* 16.*4* (2023), pp. 2642–2656, DOI: 10.1109/TSC.2023.3240235.

[108] Shekha Chenthara et al., "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology", in: *PLOS ONE* 15.*12* (Dec. 2020), pp. 1–35, DOI: 10.1371/journal.pone.0243043, URL: https://doi.org/10.1371/journal.pone.0243043.

[109] Wafa Bouras et al., "Analysis Study of Participant Selection Methods in Federated Learning", in: *2024 2nd International Conference on Electrical Engineering and Automatic Control (ICEEAC)*, 2024, pp. 1–6, DOI: 10.1109/ICEEAC61226.2024.10576424.

[110] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", in: *Satoshi Nakamoto* (2008).

[111] J. Almalki et al., "Enabling blockchain with IoMT devices for healthcare", in: *Information* 13.*10* (2022), p. 448.

[112] D. Randall, P. Goel, R. Abujamra, et al., "Blockchain applications and use cases in health information technology", in: *Journal of Health & Medical Informatics* 8.*3* (2017), pp. 8–11.

[113] S. Jabbar et al., "Blockchain-enabled supply chain: Analysis, challenges, and future directions", in: *Multimedia Systems* 27 (2021), pp. 787–806.

[114] J. Ktari et al., "IoMT-based platform for e-health monitoring based on the blockchain", in: *Electronics* 11.*15* (2022), p. 2314.

[115] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—Review and open research challenges", in: *Sensors* 21.*17* (2021), p. 5874.

[116] S. J. Ralston, "Postdigital prospects for blockchain-disrupted higher education: Beyond the theater, memes and marketing hype", in: *Postdigital Science and Education* 2.*2* (2020), pp. 280–288.

[117] R. Dautov, S. Distefano, and R. Buyya, "Hierarchical data fusion for smart healthcare", in: *Journal of Big Data* 6.*1* (2019), pp. 1–23.

[118] G. J. Joyia et al., "Internet of Medical Things (IoMT): Applications, benefits and future challenges in healthcare domain", in: *Journal of Communications* 12.*4* (2017), pp. 240–247.

[119] L. Zhou et al., "Beekeeper: A blockchain-based IoT system with secure storage and homomorphic computation", in: *IEEE Access* 6 (2018), pp. 43472–43488.

[120] M. A. Jan et al., "Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions", in: *Journal of Network and Computer Applications* 175 (2021), p. 102918.

[121] M. Niranjanamurthy, B. Nithya, and S. Jagannatha, "Analysis of blockchain technology: Pros, cons and SWOT", in: *Cluster Computing* 22 (2019), pp. 14743–14757.

[122] M. N. M. Bhutta et al., "A survey on blockchain technology: Evolution, architecture and security", in: *IEEE Access* 9 (2021), pp. 61048–61073.

[123] H. Guo and X. Yu, "A survey on blockchain technology and its security", in: *Blockchain: Research and Applications* 3.*2* (2022), p. 100067.

[124] Z. Zheng et al., "An overview of blockchain technology: Architecture, consensus, and future trends", in: *2017 IEEE International Congress on Big Data (BigData Congress)*, IEEE, 2017, pp. 557–564.

[125] X. Xu et al., "A taxonomy of blockchain-based systems for architecture design", in: *2017 IEEE International Conference on Software Architecture (ICSA)*, IEEE, 2017, pp. 243–252.

[126] R. Arul et al., "Multi-modal secure healthcare data dissemination framework using blockchain in IoMT", in: *Personal and Ubiquitous Computing* (2021), pp. 1–13.

[127] S. R. Mallick and S. Sharma, "EMRI: A scalable and secure blockchain-based IoMT framework for healthcare data transaction", in: *2021 19th OITS International Conference on Information Technology (OCIT)*, IEEE, 2021, pp. 261–266.

[128] A. Cretarola, G. Figà-Talamanca, and C. Grunspan, "Blockchain and cryptocurrencies: Economic and financial research", in: (2021), pp. 1–7.

[129] *Anaconda Distribution*, `https://www.anaconda.com`, 2024.

[130] Python Software Foundation, *Python Programming Language*, `https://www.python.org`, 2024.

[131] PyTorch Team, *PyTorch: An Open Source Machine Learning Framework*, `https://pytorch.org`, 2024.

[132] Hao Miao, Han Yu Li, and Felix X. Yu, *Plato: A Federated Learning Research Framework*, `https://github.com/TL-System/Plato`, 2023.

[133] Philip Schmidt et al., "Introducing WESAD, a Multimodal Dataset for Wearable Stress and Affect Detection", in: *Proceedings of the 20th ACM International Conference on Multimodal Interaction*, ICMI '18, Boulder, CO, USA: Association for Computing Machinery, 2018, pp. 400–408, ISBN: 9781450356923, DOI: 10.1145/3242969.3242985, URL: https://doi.org/10.1145/3242969.3242985.

[134] Qingming Li et al., "Emulating Full Client Participation: A Long Term Client Selection Strategy for Federated Learning", in: *arXiv preprint arXiv:2405.13584* (2024), DOI: 10.48550/arXiv.2405.13584, arXiv: 2405.13584 [cs.LG], URL: https://arxiv.org/abs/2405.13584.

[135] Yuwei Wang and Burak Kantarci, "A Novel Reputation-aware Client Selection Scheme for Federated Learning within Mobile Environments", in: (2020), pp. 1–6, DOI: 10.1109/CAMAD50429.2020.9209263.

[136] Ferrag MA et al., "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes", in: *Journal of Network and Computer Applications* 101 (2018), pp. 55–82.

[137] Alsubaei F et al., "IoMT-SAF: Internet of medical things security assessment framework", in: *Internet of Things* 8 (2019), p. 100123.

[138] Deebak BD and Al-Turjman F, "Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems Using Internet of Medical Things", in: *IEEE Journal on Selected Areas in Communications* 39.*2* (2021), pp. 346–360.

[139] Almaiah MA et al., "A Novel Hybrid Trustworthy Decentralized Authentication and Data Preservation Model for Digital Healthcare IoT Based CPS", in: *Sensors* 22.*4* (2022), URL: https://www.mdpi.com/1424-8220/22/4/1448.

[140] Tso R et al., "Privacy-preserving data communication through secure multi-party computation in healthcare sensor cloud", in: *Journal of Signal Processing Systems* 89.*1* (2017), pp. 51–59.

[141] Alexan W et al., "IoMT security: Sha3-512, aes-256, rsa and lsb steganography", in: (2021), pp. 177–181.

[142] Alassaf N, Alkazemi B, and Gutub A, "Applicable light-weight cryptography to secure medical data in IoT systems", in: *Arabia* (2003).

[143] Li Z et al., "Rate splitting for multi-antenna downlink: Precoder design and practical implementation", in: *IEEE Journal on Selected Areas in Communications* 38.*8* (2020), pp. 1910–1924.

[144] Manal R, Fatima R, and Tomader M, "Authentication for e-health applications in IoT enabled 5G and proposed solution", in: (2019), pp. 1–6.

[145] Hu R et al., "Personalized Federated Learning With Differential Privacy", in: *IEEE Internet of Things Journal* 7.*10* (2020), pp. 9530–9539.

[146] Kim H et al., "Blockchained on-device federated learning", in: *IEEE Communications Letters* 24.*6* (2019), pp. 1279–1283.

[147] M Khelili et al., "IoMT-fog-cloud based architecture for Covid-19 detection", in: *Biomedical Signal Processing and Control* 76 (2022), p. 103715.

[148] S Bharati et al., "Applications and challenges of cloud integrated IoMT", in: *Cognitive internet of medical things for smart healthcare*, 2021, pp. 67–85.

[149] V Balasubramanian and A Jolfaei, "A scalable framework for healthcare monitoring application using the Internet of Medical Things", in: *Software: Practice and Experience* 51.*12* (2021), pp. 2457–2468.

[150] G Rajesh et al., "Achieving longevity in wireless body area network by efficient transmission power control for iomt applications", in: vol. 14, 3, 2022, pp. 80–89.

[151] Peng He et al., "A survey of internet of medical things: technology, application and future directions", in: *Digital Communications and Networks* (2024), ISSN: 2352-8648, DOI: https://doi.org/10.1016/j.dcan.2024.11.013, URL: https://www.sciencedirect.com/science/article/pii/S2352864824001597.

[152] Radwa Ahmed Osman, "Internet of Medical Things (IoMT) optimization for healthcare: A deep learning-based interference avoidance model", in: *Computer Networks* 248 (2024), p. 110491, ISSN: 1389-1286, DOI: https://doi.org/10.1016/j.comnet.2024.110491, URL: https://www.sciencedirect.com/science/article/pii/S1389128624003232.

[153] Lei Fu et al., "Client selection in federated learning: Principles, challenges, and opportunities", in: *IEEE Internet of Things Journal* (2023).

[154] Ala Gouissem, Zina Chkirbene, and Ridha Hamila, *A Comprehensive Survey On Client Selections in Federated Learning*, 2023, arXiv: 2311.06801 [cs.LG], URL: https://arxiv.org/abs/2311.06801.

[155] Vivian Ihekoronye, Jae Min Lee, and Dong-Seong Kim, "Impact of Adaptive Client Selection on Federated Learning for IoMT Ecosystem", in: Oct. 2024, DOI: 10.1109/ICTC62082.2024.10827188.

[156] Jinyao Yang, Yao Shi, Han Zhang, et al., "MedMNIST v2: A large-scale lightweight benchmark for 2D and 3D biomedical image classification", in: *Scientific Data* 8.*1* (2021), pp. 1–12.

[157] Petar et al., "Exploring the Potential of Bluetooth Low Energy for Wireless Sensing and On-Board Computation in Remote Health Monitoring", in: *2023 8th International Conference on Smart and Sustainable Technologies (SpliTech)* (2023), pp. 1–3, URL: https://api.semanticscholar.org/CorpusID:260387743.

[158] Hongwei Wang, Dai Feng, and Yingyi Liu, "Personalized Medicine with Advanced Analytics", in: *Real-World Evidence in Medical Product Development*, ed. by Weili He, Yixin Fang, and Hongwei Wang, Cham: Springer International Publishing, 2023, pp. 289–320, ISBN: 978-3-031-26328-6, DOI: 10.1007/978-3-031-26328-6_16, URL: https://doi.org/10.1007/978-3-031-26328-6_16.

[159] M. Wazid and P. Gope, "BACKM-EHA: A novel blockchain-enabled security solution for IoMT-based E-healthcare applications", in: *ACM Transactions on Internet Technology* 23.*3* (2023), pp. 1–28.

[160] Yogesh K. Dwivedi et al., "Resistance to innovation: A dynamic capability model based enquiry into retailers' resistance to blockchain adaptation", in: *Journal of Business Research* 157 (2023), p. 113632, ISSN: 0148-2963, DOI: https://doi.org/10.1016/j.jbusres.2022.113632, URL: https://www.sciencedirect.com/science/article/pii/S0148296322010979.

[161] Seonghyeon Gong and Changhoon Lee, "BLOCIS: Blockchain-Based Cyber Threat Intelligence Sharing Framework for Sybil-Resistance", in: *Electronics* 9.*3* (2020), ISSN: 2079-9292, DOI: 10.3390/electronics9030521, URL: https://www.mdpi.com/2079-9292/9/3/521.

[162] Dimitrios Chatziamanetoglou and Konstantinos Rantos, "Cyber Threat Intelligence on Blockchain: A Systematic Literature Review", in: *Computers* 13.*3* (2024), ISSN: 2073-431X, DOI: 10.3390/computers13030060, URL: https://www.mdpi.com/2073-431X/13/3/60.

[163] Ivan Homoliak et al., "The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses", in: *IEEE Communications Surveys and Tutorials* 23.*1* (2021), pp. 341–390, DOI: 10.1109/COMST.2020.3033665.

[164] Benedikt Putz and Günther Pernul, "Detecting Blockchain Security Threats", in: *2020 IEEE International Conference on Blockchain (Blockchain)*, 2020, pp. 313–320, DOI: 10.1109/Blockchain50366.2020.00046.

[165] Marcos Allende et al., "Quantum-resistance in blockchain networks", in: *Scientific Reports* 13.*1* (2023), p. 5664, ISSN: 2045-2322, DOI: 10.1038/s41598-023-32701-6, URL: https://doi.org/10.1038/s41598-023-32701-6.

[166] Wenjuan Li et al., "Toward a blockchain-based framework for challenge-based collaborative intrusion detection", in: *International Journal of Information Security* 20.*2* (2021), pp. 127–139, ISSN: 1615-5270, DOI: 10.1007/s10207-020-00488-6, URL: https://doi.org/10.1007/s10207-020-00488-6.

[167] Daeheon Choi et al., "Factors Affecting Organizations' Resistance to the Adoption of Blockchain Technology in Supply Networks", in: *Sustainability* 12.*21* (2020), ISSN: 2071-1050, DOI: 10.3390/su12218882, URL: https://www.mdpi.com/2071-1050/12/21/8882.

[168] Neha Garg et al., "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment", in: *IEEE Access* 8 (2020), pp. 95956–95977, DOI: 10.1109/ACCESS.2020.2995917.

[169] Maroua Akkal et al., "An Intrusion Detection System For Detecting DDoS Attacks In Blockchain-Enabled IoMT Networks", in: *2024 7th International Conference on Signal Processing and Information Security (ICSPIS)*, 2024, pp. 1–6, DOI: 10.1109/ICSPIS63676.2024.10812635.

[170] Zounkaraneni Ngoupayou Limbepe, Keke Gai, and Jing Yu, "Blockchain-Based Privacy-Enhancing Federated Learning in Smart Healthcare: A Survey", in: *Blockchains* 3.*1* (2025), ISSN: 2813-5288, DOI: 10.3390/blockchains3010001, URL: https://www.mdpi.com/2813-5288/3/1/1.

[171] Inas Al Khatib, Abdulrahim Shamayleh, and Malick Ndiaye, "Healthcare and the Internet of Medical Things: Applications, Trends, Key Challenges, and Proposed Resolutions", in: *Informatics* 11.*3* (2024), ISSN: 2227-9709, DOI: 10.3390/informatics11030047, URL: https://www.mdpi.com/2227-9709/11/3/47.

[172] Oluwaseun Priscilla Olawale and Sahar Ebadinezhad, "Cybersecurity Anomaly Detection: AI and Ethereum Blockchain for a Secure and Tamperproof IoHT Data Management", in: *IEEE Access* 12 (2024), pp. 131605–131620, DOI: 10.1109/ACCESS.2024.3460428.

[173] Mohammad Kamrul Hasan et al., "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things", in: *IET communications* 16.*5* (2022), pp. 421–432.

[174] Mohammad Faisal Khan and Mohammad Abaoud, "Blockchain-Integrated Security for Real-Time Patient Monitoring in the Internet of Medical Things Using Federated Learning", in: *IEEE Access* 11 (2023), pp. 117826–117850, DOI: 10.1109/ACCESS.2023.3326155.

[175] Ali Ghubaish et al., "Recent advances in the internet-of-medical-things (IoMT) systems security", in: *IEEE Internet of Things Journal* 8.*11* (2020), pp. 8707–8718.

[176] Leilei Du et al., *Dynamic Private Task Assignment under Differential Privacy*, 2023, DOI: 10.48550/arXiv.2302.09511, arXiv: 2302.09511 [cs.CR], URL: https://arxiv.org/abs/2302.09511.

[177] Lin Wang et al., "Delta: Diverse Client Sampling for Fast Federated Learning", in: *Advances in Neural Information Processing Systems (NeurIPS) 36*, 2023, DOI: 10.48550/arXiv.2205.13925, URL: https://arxiv.org/abs/2205.13925.

[178] Zichang Liu et al., "One Pass Distribution Sketch for Measuring Data Heterogeneity in Federated Learning", in: *Advances in Neural Information Processing Systems (NeurIPS) 36*, 2023, DOI: 10.5555/3666122.3666811, URL: https://dl.acm.org/doi/10.5555/3666122.3666811.

[179] Kulaea Taueveeve Pauu et al., “Differential Privacy and Blockchain Empowered Decentralized Graph Federated Learning Enabled UAVs for Disaster Response”, in: *IEEE Internet of Things Journal* (2023), DOI: 10.1109/JIOT.2023.3332216.