
SWARM LEARNING: A SURVEY OF CONCEPTS, APPLICATIONS, AND TRENDS

A PREPRINT

Elham Shammar

School of Cyber Science and Engineering,
Wuhan University, Wuhan, China
eshammar@whu.edu.cn

Xiaohui Cui

School of Cyber Science and Engineering,
Wuhan University, Wuhan, China
xcui@whu.edu.cn

Mohammed A. A. Al-qaness

College of Physics and Electronic
Information Engineering
Zhejiang Normal University
Jinhua 321004, China
alqaness@zjnu.edu.cn

February 28, 2025

ABSTRACT

Deep learning (DL) models have raised privacy and security concerns due to their reliance on large datasets on central servers. As the number of devices on the Internet of Things (IoT) increases, artificial intelligence (AI) will be crucial for resource management, data processing, and knowledge acquisition. To address those issues, federated learning (FL) has introduced a novel approach to building a versatile, large-scale machine learning (ML) framework that operates in a decentralized and hardware-agnostic manner. However, FL faces network bandwidth limitations and data breaches. To reduce the central dependency in FL and increase scalability, swarm learning (SL) has been proposed in collaboration with Hewlett Packard Enterprise (HPE). SL represents a decentralized ML framework that leverages blockchain technology for secure, scalable, and private data management. A blockchain-based network enables the exchange and aggregation of model parameters among participants, thus mitigating the risk of a single point of failure and eliminating communication bottlenecks. This survey introduces the principles of SL, its architectural design, and its fields of application. In addition, it highlights numerous research avenues that require further exploration by academic and industry communities to unlock the full potential and applications of SL.

Keywords IoT, Blockchain, Swarm Learning; Edge Computing, Security, Decentralized Machine Learning, Federated Learning, Privacy Preservation

1 Introduction

The number of Internet of Things (IoT) devices is expected to grow rapidly over the next five years. In 2019, a third of all IoT devices were used in healthcare, and this is predicted to increase to 40%, representing \$6.2 trillion of the global IoT market by 2025 [1]. By 2030, there will likely be 29 billion IoT devices in different industries, and IoMT devices could potentially save \$300 billion, particularly in chronic disease management and telemedicine [2, 3]. This market is expected to generate \$135 billion in revenue by 2025. In addition, the global healthcare market is projected to reach \$6.2 trillion by 2028 [4], highlighting the need for advances in AI, resource management, data processing, and knowledge extraction, all driven by the rapid growth of 5G and Multi-Access Edge Computing (MEC) [5].

Deep learning (DL) increases the power of IoT by allowing devices to handle large amounts of data, improve decision making through better pattern recognition, and enhance system performance in real-time applications such as smart

cities, healthcare, and self-driving cars. However, these modern DL models raise serious concerns about privacy and security, mainly because they rely on centralized servers to store large datasets [6]. Although cloud-based local learning has certain advantages, there are drawbacks as well, such as increased security threats, traffic, and data redundancy. Data ownership and privacy concerns are another problem with traditional centralized learning approaches [4]. One such solution is federated learning (FL), which allows decentralized cooperation while maintaining data privacy. However, FL has to contend with issues like bandwidth constraints and cyberthreats. Distributed FL (DFL) [7] and swarm learning (SL), a new strategy created in collaboration with Hewlett Packard Enterprise (HPE) [6], are two promising answers to these issues.

DFL and SL both aim to improve privacy and reduce reliance on centralized data storage. DFL allows model training on multiple nodes without needing a central server, making the process more flexible and decentralized [8, 9, 10]. On the other hand, SL takes advantage of blockchain to build a decentralized peer-to-peer network, which improves both security and privacy. By combining blockchain with federated learning, SL removes the central server altogether, allowing training to happen directly at each node, where only the parameter weights are shared. This approach reduces the risks associated with storing data in one central location. Blockchain’s consensus mechanisms ensure the process remains secure, while SL uses smart contracts for more secure, privacy-friendly data sharing. Unlike traditional federated learning, which aggregates local gradients, SL uses a more secure and streamlined process that includes steps such as node registration, authentication, training, gradient sharing, and result aggregation using the Federated Average method [11, 12, 13].

SL’s decentralized approach boosts fault tolerance, scalability, and privacy, making it a great fit for a range of sectors such as healthcare, automotive, finance, smart cities, edge computing, IoT, and the metaverse. In healthcare, SL ensures secure collaborative training while keeping patient data protected [14]. In industries, SL helps make faster and more informed decisions by allowing independent learning agents to work together, which is in good agreement with the goals of Industry 4.0 [15, 16, 17, 18]. In the finance sector, SL plays a key role in detecting fraud while ensuring that customer information remains private [19]. For smart cities, it can improve things like traffic flow and public transport management. Furthermore, SL supports data ownership, helps meet regulatory standards, sparks innovation, and gives businesses a competitive edge by accelerating the speed with which they can bring new products to market [20].

This survey offers a detailed analysis of SL, delving into its architecture, components, and practical applications. It highlights how SL’s integration with blockchain improves both security and scalability, while also examining its adaptability in dynamic real-world settings. Unlike the study by Evangelia et al. [21], which does not provide much insight into practical deployment, this article offers a clearer picture of how scalable SL is and how it performs in real-world applications. Although Tajabadi et al. [22] focus primarily on healthcare uses of SL, this work broadens the discussion by exploring how SL handles non-IID data, enhances security through blockchain and improves node coordination efficiency. In doing so, it fills the gaps left by earlier surveys, offering a more well-rounded view of SL’s potential in decentralized learning systems.

This paper is motivated by the growing need to explore and unlock the full potential of SL as a decentralized, privacy-focused machine learning (ML) framework. We look closer at how SL can be implemented in real-world scenarios, assess its strengths and challenges, and examine how it is being applied across different industries. With data privacy becoming more critical and the growth of IoT devices, this survey aims to provide useful insights for researchers and professionals looking to leverage SL for secure, scalable, and efficient ML solutions in various domains.

1.1 Paper objectives and contribution

The key advantages of SL call for a deeper look at its current research and practical applications, as well as a careful identification of areas that need further development. This survey explores the potential of SL in decentralized learning environments, highlights both technical and operational challenges, and suggests possible directions for future advancements. Specifically, it focuses on how advanced cryptographic methods can enhance security and how SL can be adapted to new technologies such as edge computing and the Internet of Things.

This work consolidates existing knowledge, highlights research gaps, and outlines strategic directions for the broader adoption of SL. As a resource, this survey aims to guide scholars, researchers, and practitioners in expanding SL’s application across various industries, thus maximizing its impact and utility.

In summary, the main contribution of this paper can be presented as follows:

- We present the first survey paper in the field of SL. To the best of our knowledge, this paper is the first review on SL.
- We provide a comprehensive overview of the existing literature on SL and its current applications to give the readers a complete picture of this new and promising research direction.

- We studied and analyzed the current applications of SL. We categorized them into healthcare, transportation, industry, robotic systems, smart homes, financial services, multimedia IoT, fake news detection, and Metaverse.
- We present an in-depth analysis of the current limitations and challenges facing SL. We explore how these issues impact their development and deployment. In addition, we discuss potential future directions to improve SL technologies and applications. We suggest avenues for advancement and areas that are ready for further research to enhance the effectiveness and applicability of SL technologies.

The structure of this paper, illustrated in Fig.1, is as follows: Section 2 introduces SL, covering its fundamental concepts and components. Sections 3 and 4 discuss the applications of SL and the challenges associated with its implementation, respectively. Section 5 outlines potential future research directions for SL. Finally, the paper concludes in Section 6.

2 Research Methodology

The primary motivation for this study is to answer the research questions in Subsection 2.1. We aim to explore the core concepts, architecture, and components of SL, compare it with other decentralized learning approaches, and identify its real-world applications and challenges.

2.1 Research Questions

The following research questions guide the exploration of Swarm Learning (SL), its architecture, applications, and challenges, aiming to deepen the understanding of this emerging decentralized learning approach.

1. How do the key concepts, architecture, and components of SL function together in a distributed learning environment?
2. How does SL compare with FL, distributed FL, decentralized FL, and swarm intelligence regarding performance, privacy, and scalability?
3. What are the specific applications of SL in industries such as healthcare, finance, and IoT, and how do these applications benefit from its use?
4. What are the primary challenges faced during the adoption and implementation of SL in real-world applications, particularly regarding data privacy, communication overhead, and system scalability?

2.2 Papers Selection

We conducted a thorough search in six databases: IEEE, PubMed, Science Direct, Scopus, Springer, and Web of Science. We retrieved 30 papers from IEEE, 12 from PubMed, 129 from Science Direct, 87 from Scopus, 28 from Springer, and 56 from Web of Science. After screening for relevance to SL and excluding articles on swarm intelligence and optimization, we identified 84 papers that met our inclusion criteria.

The number of SL research papers has grown steadily, as shown in Fig. 2. Starting with four papers in 2020, it increased to five in 2021, 14 in 2022, and a substantial increase to 29 in 2023. In 2024, there were 28 publications, reflecting the growing importance of SL. The number for 2025 stands at only four due to the survey being finalized in February 2025, providing a snapshot of SL research up to that time. This upward trend highlights the increasing academic interest in SL, driven by advances in computational power, data availability, the rise of IoT devices, privacy-preserving AI techniques, and the need for decentralized solutions in sectors such as healthcare, autonomous driving, and smart cities.

3 Swarm Learning (SL)

SL, developed in collaboration with HPE [6], is a decentralized machine learning framework that enables the training of the model on the device without the need to transfer raw data. By keeping data localized on the data owner's site, SL substantially reduces data traffic by avoiding the transmission of raw data [23]. Using blockchain technology, SL enhances privacy and security by exchanging only the model parameters and weights, not the actual data itself. This approach utilizes smart contracts to manage the training and updating of decentralized ML models using local user data, separating it from traditional centralized systems or even FL frameworks that rely on a central server to gather model updates [19]. Furthermore, SL incorporates advanced data privacy and security mechanisms, making it an ideal, flexible, and secure solution for content caching in modern network architectures [24].

SL employs a permissioned blockchain network and a decentralized hardware infrastructure to facilitate secure member onboarding, dynamic leader election, and efficient merging of model parameters. The system utilizes standardized AI

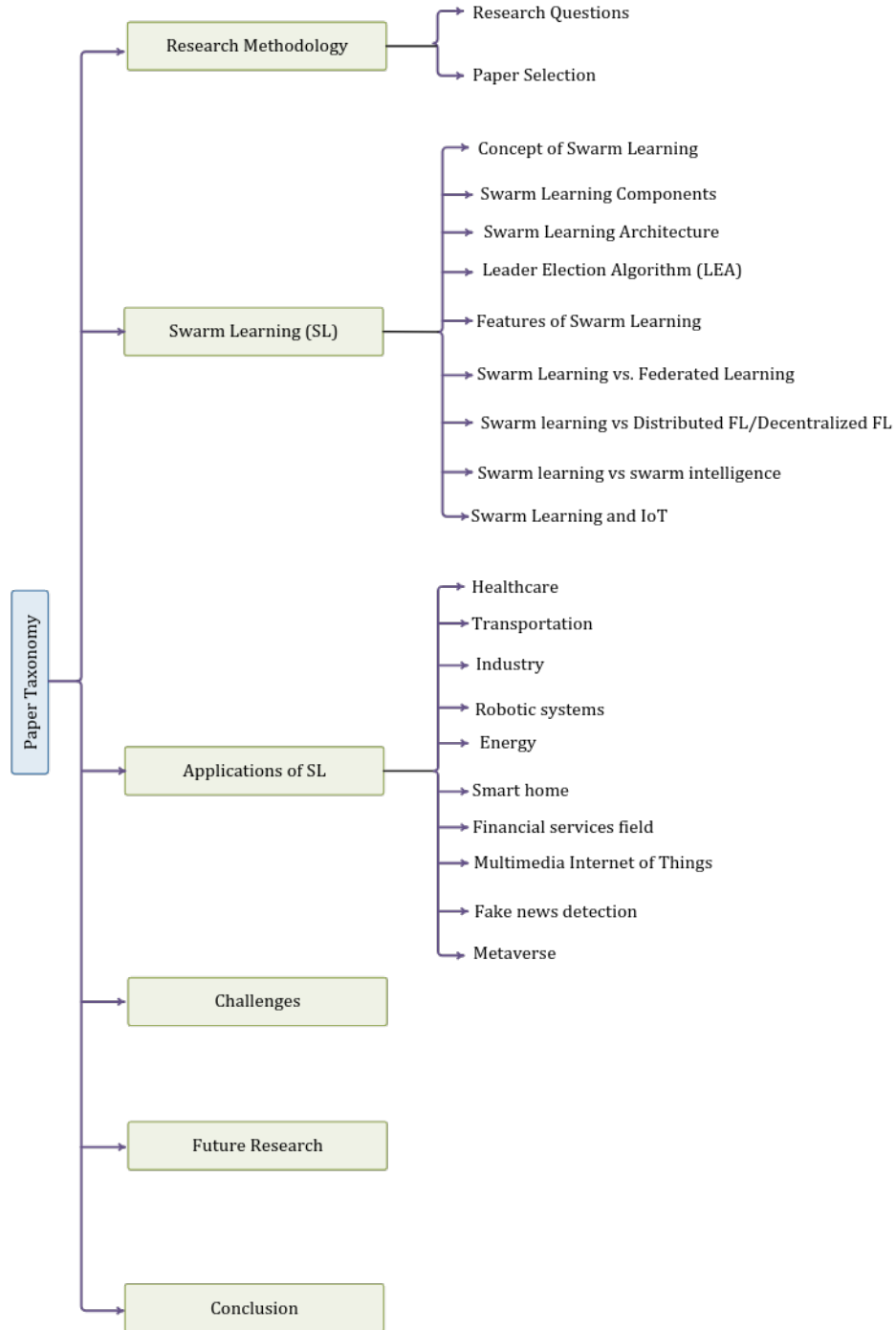


Figure 1: Paper Structure

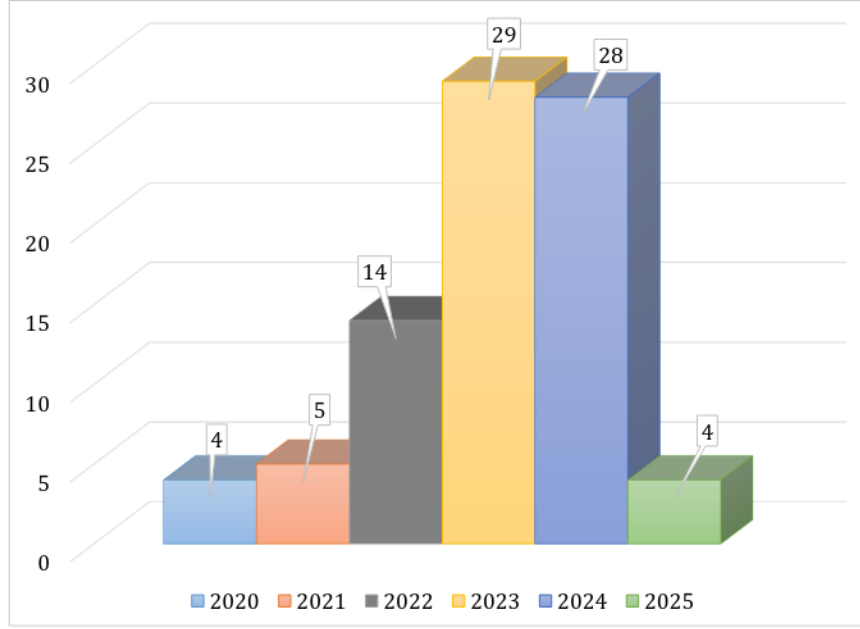


Figure 2: Annual increase in the number of Swarm Learning research papers.

engines within a distributed ML context to ensure secure and reliable operations. An SL library supports an iterative AI learning process that leverages decentralized data, adhering rigorously to the prevailing privacy and security standards [25]. This structured approach secures data and streamlines the computational process between various network nodes.

Han et al. [26] bridge the gap between SL theory and practice by conducting experiments on three public datasets, demonstrating the suitability of SL in various scenarios, even with unbalanced, polluted, or biased data. However, challenges like backdoor attacks, blockchain integration complexity, and computational overhead persist. Han et al. [27] evaluated SL’s performance in noisy and unbalanced datasets, focusing on scalability and resource utilization. Their work highlights SL’s potential in decentralized environments while addressing real-world issues such as dataset distribution and deployment strategies.

Mantovani et al. [28] introduced a Key Performance Indicator (KPI) to evaluate SL performance in distributed healthcare analysis. Their approach eliminates central server management by distributing model parameters across nodes and addressing privacy concerns. Using data from the Intensive Care Unit (ICU) of the Medical Information Mart for Intensive Care (MIMIC) Electronic Health Records (EHR) database, they demonstrated SL’s potential to improve data privacy and collaboration in decentralized healthcare analysis.

SL addresses several key issues in FL and provides many benefits in security, privacy, and scalability. SL can envision ways to develop more secure, private, and faster distributed ML applications from different domains. To address gradient leakage and data privacy concerns in Federated Learning (FL), Madni et al. [11] developed a decentralized secure framework that combined blockchain with Swarm Learning (SL). SL ensures data privacy and model parameter secrecy, authenticating only trusted nodes and maintaining data integrity through blockchain mechanisms. Research shows that SL outperforms current anomaly detection methods in ML, offering better precision and mitigating gradient leakage, a key limitation in FL.

In two articles [29], [30], Xu et al. tackled data heterogeneity, security, and communication bottlenecks in FL by proposing a robust edge learning framework for IoT devices. They introduced Byzantine-Robust and Communication-Efficient Distributed SL (CB-DSL), the first comprehensive theoretical analysis of FL with Particle Swarm Optimization (PSO). This framework includes a closed-form formula for assessing the convergence rate of CB-DSL, demonstrating its superiority over traditional FL methods like Federated Averaging (FedAvg) and provides a model divergence analysis for improving learning outcomes in non-IID scenarios.

The following subsections discuss the architecture, components, features, and applications of SL, covering the application and hardware layers, the leader election process, and model aggregation techniques. We compare SL with FL and Swarm Intelligence, focusing on data sharing, decentralization, and security. These subsections also explore the role of SL in IoT, improving real-time data processing and security, and conclude with an overview of how SL addresses challenges in distributed learning systems.

3.1 Concept of SL

ML can, in theory, be carried out locally with sufficient data and computing resources (Fig. 3 (A) [14]). However, data and computation exist separately. In cloud computing, data are centrally transported (Fig. 3 (B) [14]), improving the volume of data available for training and improving the outcomes of ML. However, this approach presents challenges such as increased data traffic, duplication, and data privacy concerns. In FL, a central server manages the parameter settings while the data remain at the contributor’s location, with local computing performed at the data storage site (Fig. 3 (C) [14]). SL eliminates the need for a central server, distributing parameters across the swarm network and developing models locally with private data (Fig. 3 (D) [14]).

SL’s decentralized structure accelerates training by enabling local data processing at edge nodes, reducing latency, and leveraging computational power across decentralized nodes. It minimizes communication overhead and uses blockchain for secure model updates, while dynamic leader elections optimize training. SL effectively handles non-IID data, improving model robustness and accuracy, and optimizes resource use between nodes with varying computational capacities [14].

However, integrating ML into SL can complicate training rate assessments. Variations in ML architecture and complexity affect convergence and efficiency, while SL’s decentralized nature and differing computational resources may impact scalability. Blockchain synchronization introduces overhead, and adapting ML methods for SL complicates performance evaluation. Comparative studies with centralized and federated systems are needed to assess SL’s real-world benefits.

3.2 SL Components

As shown in Fig. 4 [31], the SL framework consists of various nodes:

- **Swarm Learning (SL) node:** SL nodes run the core of SL, sharing learnings and incorporating insights.
- **Swarm Network (SN) node:** Using the Ethereum blockchain, the SN nodes communicate with each other to track training progress and save global state information about the model. Additionally, during initialization, every SL node is registered with an SN node, and each SN node manages the training pipeline for its corresponding SL nodes. Note that the model parameters are not recorded by the blockchain; instead, it simply stores metadata such as the model state and the training progress.
- **Swarm Operator (SWOP) nodes:** SWOP nodes manage SL operations, performing tasks such as starting and stopping Swarm runs, building and upgrading ML containers, and sharing models for training.
- **SL Command Interface (SWCI) nodes:** SWCI nodes monitor the framework and can connect to any SN node in a given framework.
- **SL Management User Interface (SLM-UI):** SLM-UI nodes are GUI management tools used to install the framework, deploy Swarm training, monitor progress, and track past runs[31].
- **SPIFFE SPIRE Server node:** SPIFFE SPIRE Server node ensures the SL framework’s security. An SPIRE Agent Workload Attestor plugin is included in each SN or SL node, and it interacts with the SPIRE Server nodes to verify the identities of each node and to obtain and maintain a SPIFFE Verifiable Identity Document (SVID) [26].
- **License Server (LS) node** installs and manages the license to run the SL framework[26].

SL security and digital identity are handled by X.509 certificates, which can be generated by users or standard security software such as SPIRE. SL components communicate using TCP/IP ports, and participating nodes must be able to access each other’s ports[31].

3.3 SL Architecture

SL architecture consists of two primary layers: the application layer, which includes the ML platform, blockchain, and SL Library (SLL), and the infrastructure (hardware) layer, which includes domain-specific data sources and models, such as mission-related or geographic datasets [4].

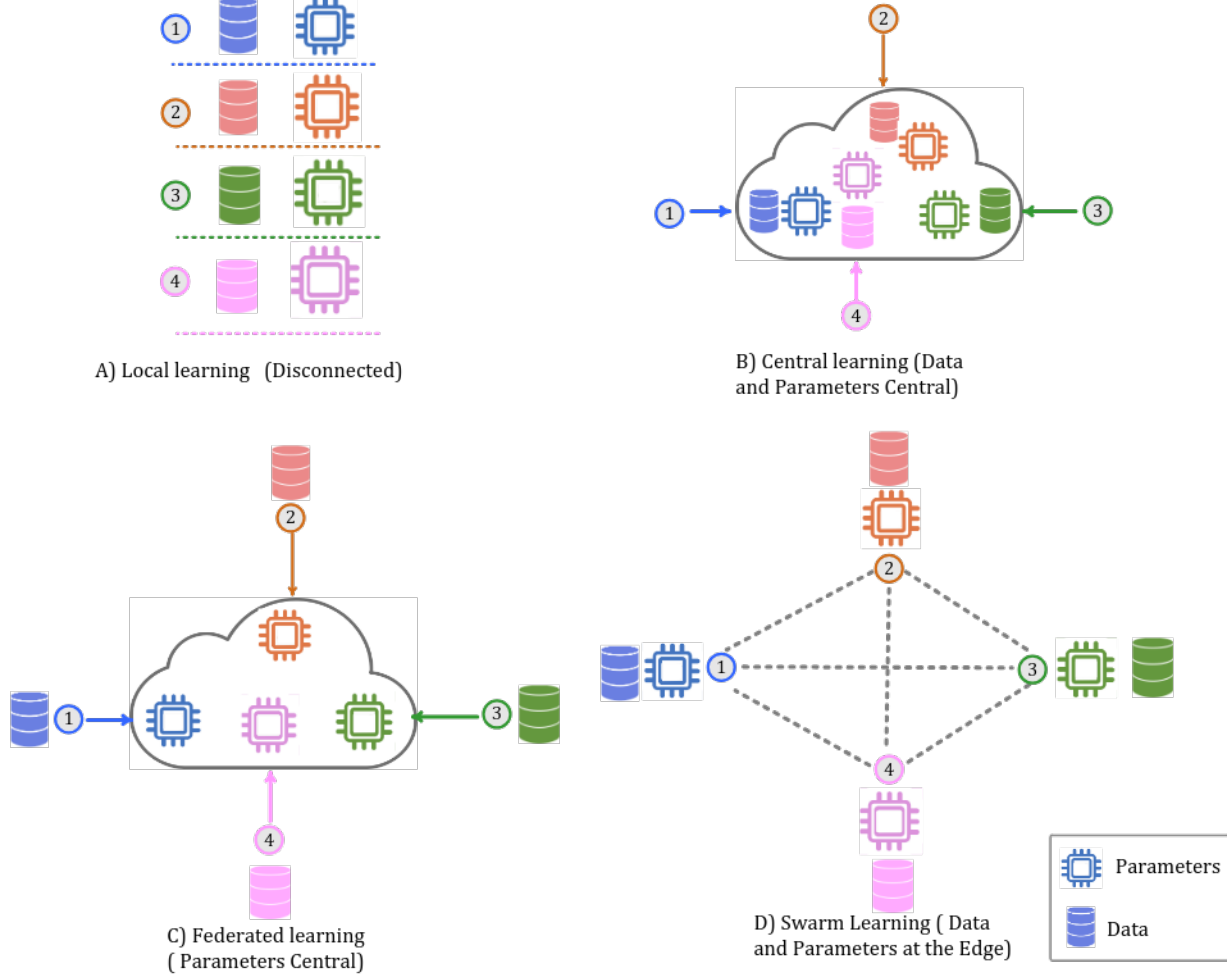


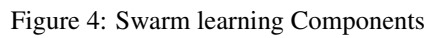
Figure 3: Comparative overview of learning models

The SL system includes two components: Swarm edge nodes and the Swarm blockchain network [23]. Blockchain integration provides several advantages: (1) local data storage, (2) reduced data traffic by avoiding original data exchange, (3) no need for a centralized secure network, (4) enhanced data security against model attacks, and (5) equal rights for all members when merging model parameters [25].

Fig. 5 [6, 14, 32] illustrates the architecture of the SL system. The system consists of multiple Swarm edge nodes (C_i), where each node C_i uses local private data D_i to train its local model L_i . After training, each node shares its model parameters with the network. The nodes are recognized, authorized, and registered with a smart contract in a peer-to-peer blockchain to ensure network security. In each training cycle, selected nodes disclose their model parameters to a Swarm API. A temporary leading node (C) aggregates the parameters into a global model G using a weighted average method [6]. The process ensures a decentralized and secure collaborative learning mechanism, facilitated by blockchain technology [14].

Swarm edge nodes must first register through the blockchain's smart contract to participate in model training. Once registered, each node downloads the initial global model from the blockchain, trains its local model, and uploads the model parameters to the leader node. The smart contract dynamically selects the leader, which aggregates the parameters of the local model and generates an updated global model, which is then redistributed to the nodes for further training [23].

Model sharing in SL is treated as a data transfer process between participating blockchains, which requires secure, consistent, and adaptable methods of interaction. Traditional solutions, such as third-party trust entities or centralized hubs such as Cosmos, are incompatible with the decentralized nature of SL [33].



3.4 Leader Election Algorithm (LEA)

8

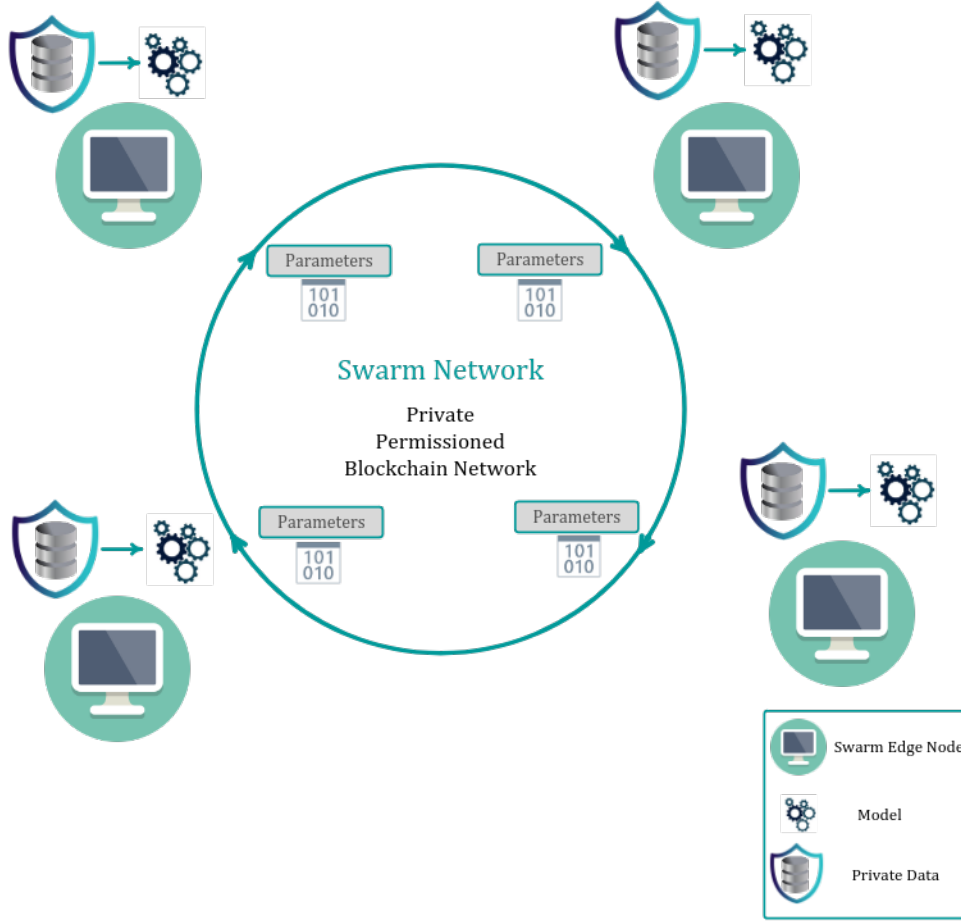


Figure 5: Swarm learning system architecture

decentralized decision-making. However, the unfairness of the leader election mechanism could cause nodes to use excessive amounts of bandwidth, which would result in inefficiencies and possibly bottlenecks. Participants may be unhappy with this discrepancy because they believe it is unfair and because nodes with higher data traffic may be more easily targeted by attackers[26]

The current LEA speculated to be a Proof of Stake (PoS), relies on leadership election on nodes' stakes or account balances. The authors in [26] recommended switching from PoS to a Proof of Work (PoW) model, in which nodes compete to solve cryptographic puzzles and leadership is established by meeting predetermined hash value requirements. By equating the likelihood of becoming a leader based on processing power, this technique seeks to guarantee a more fair distribution of network load among nodes. Future efforts will focus on collaborating with Hewlett Packard Enterprise (HPE) to enhance the fairness and effectiveness of LEA in SL.

3.5 Features of SL

SL encompasses several distinct features that strengthen its application in decentralized settings:

- A. **Privacy Preservation:** SL keeps data at each node, minimizing the risk of privacy breaches and confidentiality.
- B. **Decentralization:** SL reduces the risk of a single point of failure or data monopoly by eliminating the need for central data storage or authority for model aggregation.
- C. **Continuous Learning:** Models are continuously updated with new data available at each node, adapting to new conditions such as emerging diseases.
- D. **Data Diversity and Volume:** SL handles larger and more varied data sets from multiple nodes, improving model robustness and generalization.

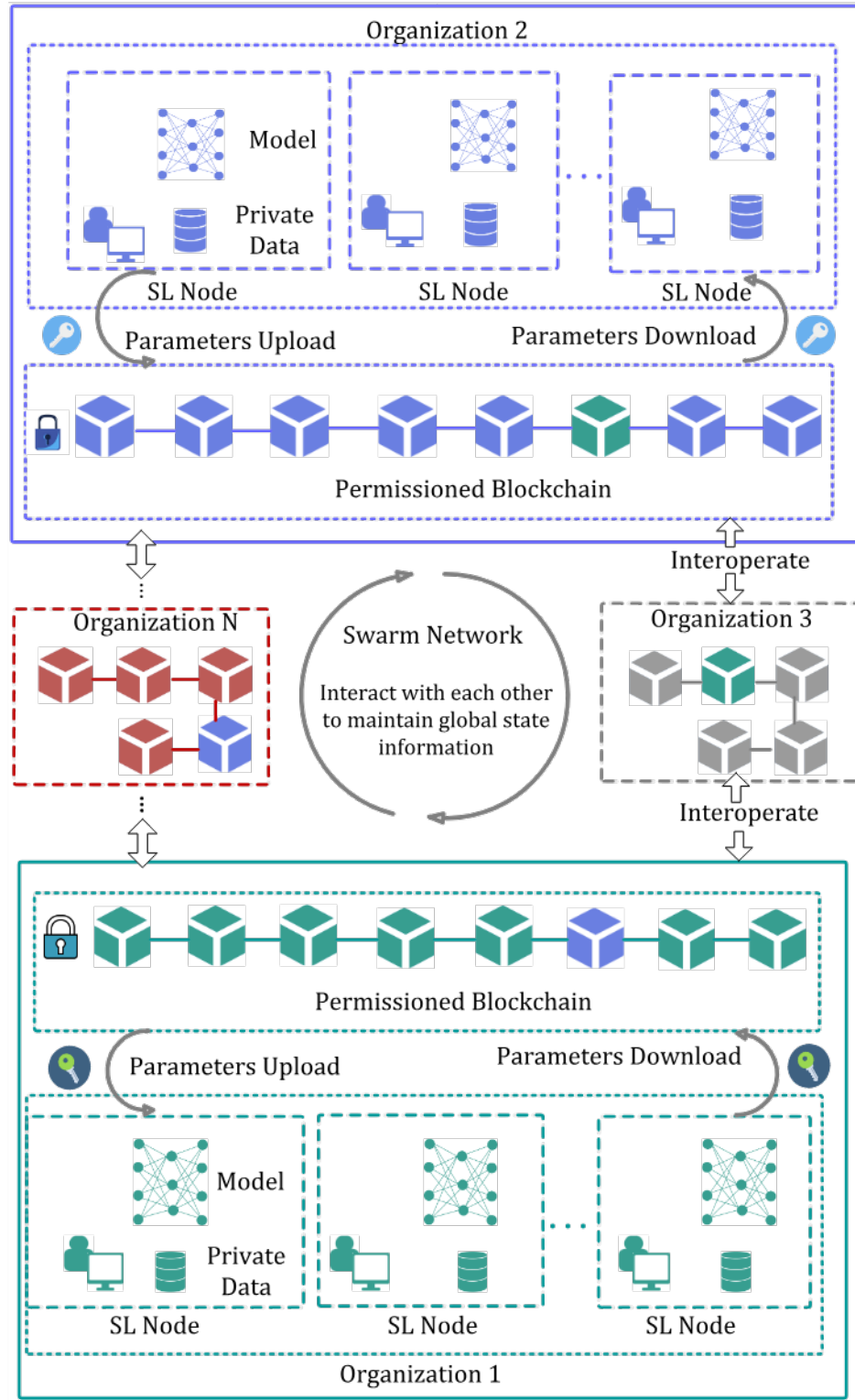


Figure 6: Workflow of SL with multiple permissioned blockchains. The chains of different colors belong to different participating organizations

- E. **Collaborative Learning:** Nodes collaborate to train a shared model, benefiting from shared insights without actual data transfer, which is crucial for maintaining patient confidentiality.

3.6 Swarm Learning vs. Federated Learning

SL and FL are two distributed learning approaches that enable the aggregation of collaborative models between multiple participating nodes [34], [35]. Through a series of training rounds, a global model is generated. Importantly, these techniques ensure that participating nodes do not need to share their proprietary datasets, thus maintaining data privacy. However, there are two fundamental differences between SL and FL [25, 36]:

- **Information Transmission:** In FL, participating nodes exchange local model parameters and global model updates with a central server. In contrast, SL employs a peer-to-peer network, leveraging blockchain technology and edge computing to allow secure and equitable communication between nodes, without the need for a central server [6, 37, 38, 39].
- **Central Server Requirement:** FL relies on a central server to aggregate the model parameters from the participating nodes and generate the global model. In contrast, SL operates without a central server. In SL, each participating node has the opportunity to be selected as a temporary server during each training cycle to compile and aggregate model updates [6]. Using blockchain-based Swarm networks for decentralized and secure parameter exchange, SL eliminates the need for a central server [25].

3.7 SL vs Distributed FL/Decentralized FL

Decentralized FL and SL focus on distributed learning by combining edge computing, blockchain, and peer-to-peer networks. With decentralized FL, the need for a central server is eliminated, enabling direct communication between nodes. Blockchain is used to create a more organized system, with a consensus mechanism that helps to update the global model. SL, which is developed by HPE Enterprise, uses blockchain to ensure data integrity, verify nodes, and maintain traceability, while improving data privacy by keeping data local and using cryptographic methods.

In decentralized FL, nodes work together to train a global model without needing a central coordinator, while SL uses a leader election mechanism to collect updates and update the blockchain. Both approaches decentralize ML and keep data localized, but SL also integrates blockchain for enhanced security and dynamic network management. Both methods are ideal for environments where data integrity and auditability are crucial. Future research could focus on comparing these methods in practice and developing hybrid models that combine the strengths of SL and FL.

Beltrán et al. [8] compared Decentralized Federated Learning (DFL) and Centralized Federated Learning (CFL), highlighting the benefits of DFL, such as improved fault tolerance and scalability. They analyzed DFL applications in healthcare, Industry 4.0, mobile services, and more. Hallaji et al. [40] discussed the security and privacy of DFL, highlighting its robustness and the need for continuous research to mitigate risks. Zhang et al. [7] and Mohammed et al. [41] reviewed the integration of DFL with blockchain, discussing its operational workflow, challenges such as communication overhead and recommending further research.

Islam et al. [42] introduced FLAG (Digital Twin-Based Drone-Assisted Secure Data Aggregation Scheme) for FL in AIoT. FLAG improves AIoT security using drones for data collection and FL training while ensuring privacy through differential privacy. It stores data securely on the blockchain, with a dual validation system to prevent malicious updates. FLAG also uses Digital Twins for efficient training and aggregation, especially in low-connectivity areas. Unlike SL, which uses peer-to-peer collaboration, FLAG enhances security with drone-assisted aggregation and blockchain, ensuring data integrity and privacy with differential privacy and multilayer authentication, making it more suitable for high-threat, low-connectivity environments.

Zhu et al. [43] proposed T-BFL, a framework that enhances FL security and efficiency. It integrates a Decentralized Reputation Management (DRM) system for secure model aggregation and optimized blockchain consensus. T-BFL adjusts the difficulty of consensus in the on-chain phase and the reputation of the node in the off-chain phase, while also presenting a dynamic energy allocation algorithm. Although both SL and T-BFL use blockchain for decentralized learning, T-BFL focuses on optimizing consensus and resource allocation, while SL emphasizes secure data management and aggregation. Yu et al. [44] examined the privacy benefits of decentralized FL compared to centralized FL, particularly in the context of distributed optimization. Their analysis shows that decentralized FL offers better privacy protection, minimizing information leakage through local gradient exchange and aggregation. Unlike SL, which uses decentralized FL but lacks distributed optimization, this approach includes advanced privacy mechanisms such as gradient differences and privacy limits, emphasizing privacy advantages over SL's peer-to-peer collaboration model.

Table 1: Comparison of SL and Distributed FL/Decentralized FL

Feature	SL	DFL
Central Server	No central server; uses blockchain for communication and decision-making between nodes.	No central server; nodes share model updates, typically via a server for coordination.
Use of Blockchain	Yes, blockchain offers data protection, trust in nodes, and model update security.	Blockchain may be used but is not central to DFL; it may help organize model updates and ensure consistency.
Privacy and Security	High privacy as data stays local; uses cryptography for added security.	Privacy may vary based on setup; some DFL approaches could involve centralized components for aggregation, raising privacy concerns.
Data Sharing	Only model updates are shared, keeping data private and reducing leak risks.	Only model updates (gradients) are shared, but depending on the setup, central server involvement might expose data.
Scalability	Highly scalable, works well in large decentralized networks without a central server.	Scalable, but may face issues with bandwidth and coordination in large networks without blockchain.
Leader Election	Uses a leader election process where nodes decide who will manage model updates.	No designated leader; updates happen between nodes, sometimes with a central server's involvement.
Consensus Mechanism	Blockchain ensures consensus, preventing fraud and ensuring alignment across nodes.	Consensus mechanisms may be used but are less critical in DFL; it focuses on aggregating model updates.
Fault Tolerance	Very high; if a node fails, others can continue without disruption.	Moderate fault tolerance; depends on the server's capacity, and failure can disrupt the entire system.
Best For	Ideal for privacy-sensitive industries like healthcare and finance.	Suitable for general use cases in industries with fewer privacy concerns, like mobile networks or manufacturing.
Implementation Complexity	More complex; requires blockchain expertise and setting up a decentralized network.	Easier to implement in environments familiar with federated learning and central aggregation.

Tan et al. [45] proposed FU-ISTANet-L, a federated learning model for efficient CSI feedback in distributed edge networks. It minimizes communication overhead by sharing only model parameters and handling heterogeneity of data. Compared to SL, which focuses on decentralized aggregation, FU-ISTANet-L improves efficiency by reducing communication costs, offering advantages in non-IID data and privacy-sensitive communication. Xiao et al. [46] introduced FeCGAN, a distributed generative adversarial network for data augmentation in vertical federated learning. The model addresses insufficient data overlap between participants using a central generator and distributed discriminators to generate synthetic data while maintaining privacy. Compared to SL, which focuses on decentralized aggregation, FeCGAN emphasizes data augmentation and heterogeneous data processing, making it more suitable for environments where data alignment between participants is limited.

Wei et al. [47] introduced the differential privacy-based DP-ZOCoA algorithm for unbalanced networks that vary in time in FL. This approach integrates differential privacy, ensuring privacy during federated model training without explicit gradients. Unlike SL, which focuses on decentralized aggregation, DP-ZOCoA emphasizes privacy and optimization in unbalanced, dynamic environments, enhancing efficiency and privacy protection. Liang et al. [48] proposed ODACT, a privacy-preserving algorithm for communication-efficient survival analysis in multicenter studies. ODACT minimizes communication rounds while performing distributed survival analysis, ensuring data privacy. Unlike SL, which focuses on decentralized aggregation, ODACT reduces communication overhead by aggregating data locally and sharing minimal updates, making it more suitable for multicenter healthcare applications.

The choice between DFL and SL depends on specific requirements such as security, scalability, flexibility, data privacy, and cost. SL is ideal for highly regulated fields, such as healthcare and finance, where data integrity is critical. DFL offers better scalability and flexibility for resource-constrained environments but may be more complex to implement. SL provides enhanced security and is suitable for applications that require strict data provenance, while DFL offers more flexibility in handling data privacy and scalability challenges. Table 1 compares SL with Distributed FL/Decentralized FL, highlighting their key features, privacy mechanisms, blockchain use, and their distinctive advantages in different applications.

3.8 SL vs swarm intelligence

Swarm intelligence is a branch of artificial intelligence (AI) that uses the principles of basic agent behavior research to provide algorithms for scheduling, routing, and optimization problems. Particle Swarm Optimization (PSO), Bee Colony Optimization (BCO), and Ant Colony Optimization (ACO) are examples of swarm intelligence algorithms. In contrast, SL is a subset of ML that focuses on distributed and dedicated learning without sharing raw data. SL emphasizes decentralized and collaborative ML in a privacy-preserving manner, while swarm intelligence focuses on problem solving and process optimization, drawing natural influences from a variety of systems.

Although SL and Swarm Intelligence have related names and are inspired by natural swarm behaviors, which may be confusing, it is important to compare them because, in computational and system design settings, they serve distinct purposes and operate on different principles within computational and system design contexts. Exploring the intersections and differences between SL and swarm intelligence can lead to the development of hybrid approaches that leverage the strengths of both. By comparing SL and swarm intelligence, researchers can identify new application areas that may benefit from either approach or a combination of both, aiding in educational and research development. Ultimately, comparing SL and swarm intelligence improves the effective deployment of these technologies in various domains.

SL provides an innovative set of effective solutions to the difficulties of conventional optimization algorithms in swarm intelligence. By addressing these issues, SL overcomes the limitations of traditional optimization algorithms in swarm intelligence and also opens new possibilities to solve complex, dynamic, and large-scale optimization problems in a secure, efficient, and privacy-preserving manner.

The Bacterial Foraging Optimization (BFO) algorithm, introduced by Kevin M. Passino in 2002, is a nature-inspired optimization technique based on *E. coli*'s natural foraging behavior. It has been applied in various fields, including engineering, control systems, and optimization problems. However, BFO has limitations depending on the problem's nature and implementation details, and its performance may not be ideal in all cases. Gan and Xiao [49] introduced SL strategies to improve convergence accuracy and prevent premature convergence in BFO. This includes cooperative communication with the best bacteria and competitive learning mechanisms around the world, improving optimal solutions and swarm diversity, and addressing standard BFO deficiencies.

Bolshakov et al. [50] have developed a deep reinforcement learning algorithm called Deep Reinforcement Ant Colony Optimization (DRACO), inspired by traditional ant colony optimization and designed for cooperative homogeneous SL. DRACO aims to shape collective behavior in decentralized systems of independent agents, offering an alternative to centralized learning. The advantages of the algorithm include natural parallelization, solving collective tasks beyond the reach of single agents, increased reliability, faster environmental exploration, and economic and energy efficiency.

3.9 Swarm Learning and IoT

In traditional cloud-based systems, IoT devices typically send data to central servers to be processed. This results in bottlenecks, privacy violations in transit, and delays. With SL, the processing is local on the device or on nearby edge servers, reducing the quantity of sensitive data that must be sent across the network and shortening the response time. By storing data locally and sharing them securely with the help of blockchain technology, SL improves the privacy and security of data. The method helps to ensure compliance with data protection laws like GDPR by retaining sensitive information in the local sphere. SL also allows IoT devices to learn and adapt in real time perpetually, providing instant analysis and updates. Its decentralized nature also makes it very fault-tolerant, making it an ideal application for healthcare monitoring and industrial automation. It also scales well without the need for a central server, making it suitable for large IoT networks. With the utilization of SL, IoT networks are made more efficient, secure, and complying with privacy regulations, making them ideal for processing large amounts of data. The next section shall elaborate further on the use of SL in IoT applications.

This section outlined SL, emphasizing its decentralized structure and blockchain integration, which enhance security, privacy, and scalability. We compared SL with SL and Swarm Intelligence, highlighting its unique advantages such as serverless architecture and secure collaborative learning. Additionally, SL's potential in IoT was explored, focusing on data privacy and processing speed. In general, SL shows promise as an efficient and privacy-preserving ML solution for industries that require high data integrity and regulatory compliance.

4 Applications of SL

SL is used in many fields, such as healthcare, autonomous vehicle systems, environmental monitoring, and robotics, as shown in Fig.7, to improve diagnostic precision, traffic flow, and safety. SL enables data aggregation without

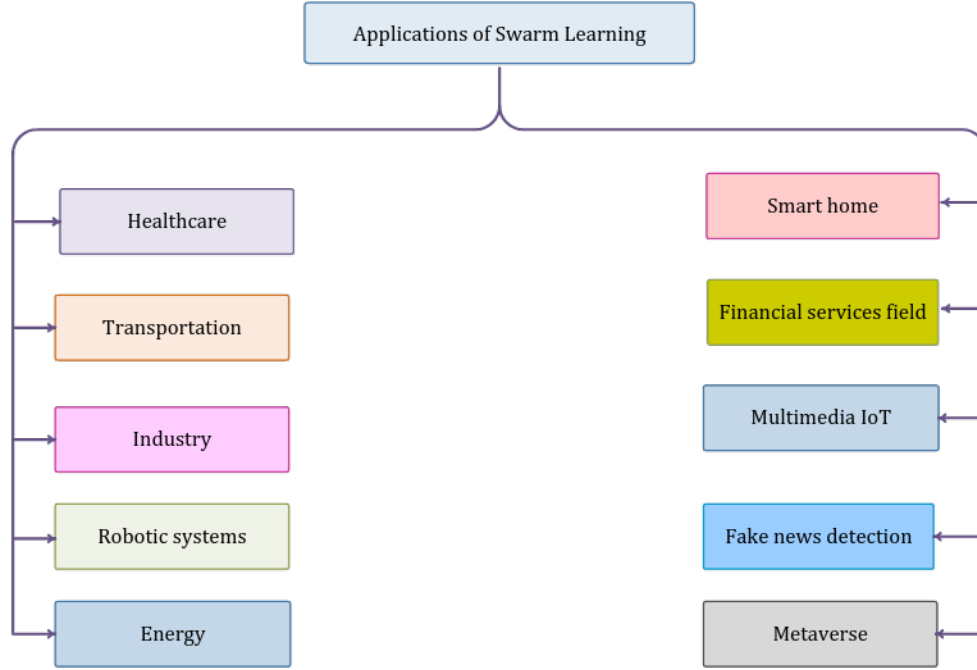


Figure 7: Swarm learning applications

compromising privacy, allows communication and learning from experiences, and encourages cooperative robots for complex tasks. Its potential to revolutionize distributed systems and information processing is significant. The following subsections discuss the applications of SL in the reviewed papers.

4.1 Healthcare

Modern hospitals generate vast amounts of sensitive patient data, which are restricted by legal and privacy concerns, hindering AI model effectiveness due to small datasets. Distributed DL helps reduce communication and computing costs, but still faces privacy challenges [23], [51]. SL allows for local ML model training across health nodes, such as hospitals, ensuring data privacy by exchanging and aggregating model parameters without central data collection. The integration of blockchain in SL guarantees data security and confidentiality [51].

As shown in Fig.8[52], the SLN plays a central role by using its unique digital identifier to train local models with private data and contribute to a collective global model. The SNN, pivotal for consensus within the blockchain, manages communication between the SLN and PBN, overseeing the training process, and maintaining the model's status. Lastly, the permissioned blockchain network underpins the model-sharing aspect of SL, safeguarding the security and confidentiality of the process, and facilitating effective collaboration between SLNs.

SL has demonstrated better performance in healthcare applications, such as COVID-19 profiles and chest X-ray images, allowing ongoing learning and enhancement across many data sources while closely respecting privacy laws such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). It offers opportunities for the development of cooperative research and diagnostics across hospitals and research institutions networks and is flexible enough to fit a variety of medical data environments. For example, German university hospitals are using SL to evaluate COVID-19 patient data and create AI-based algorithms for the detection of novel biomarkers. SL will become a crucial tool for collaborative healthcare research and precision treatment [23, 51, 53].

For example, when hospitals use SL to manage COVID-19 data, they first gather encrypted and anonymized patient data, including symptoms and treatments. Every hospital sets up a separate SL node for safe local data processing. By eliminating raw data exchange, these nodes preserve data privacy by locally training models and sharing just the model parameters over a blockchain. These parameters are then combined by a blockchain consensus method to update and synchronize the global model across all nodes. Real-time deployment of this continually improving model enables more effective diagnosis and treatment plans. SL improves predictive models by integrating diverse datasets from multiple nodes, improving accuracy and treatment efficacy. It prioritizes privacy and security by keeping

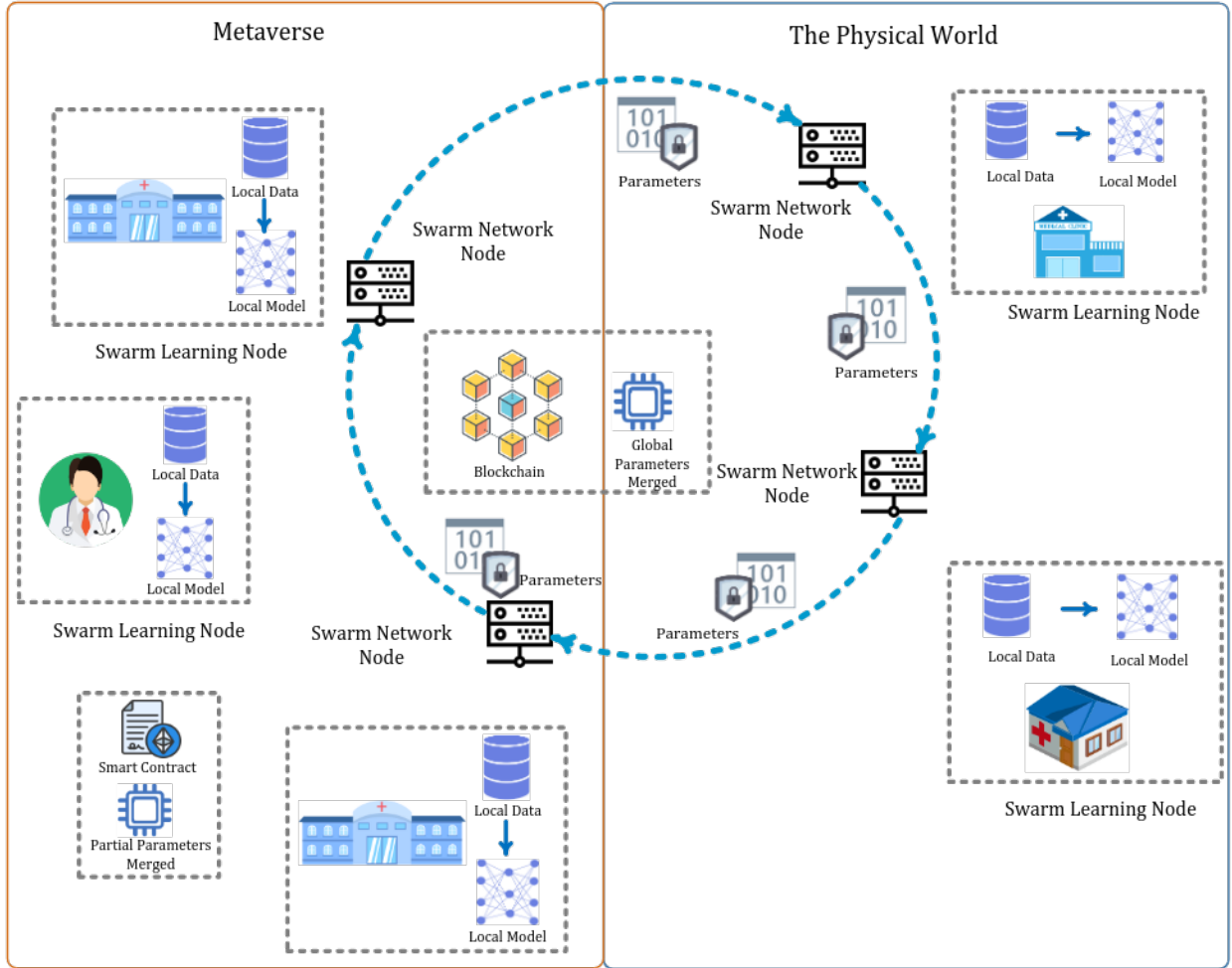


Figure 8: The framework of metaverse swarm learning, which enables cross-domain cooperation between metaverse and the physical world via blockchain

sensitive patient data on-premises, reducing reliance on central repositories. SL also increases efficiency in hospitals by implementing personalized treatment plans. It is highly scalable, allowing easy integration of new nodes without significant infrastructure changes [14].

Warnat-Herresthal et al. [14] showcased the effectiveness of Swarm Learning (SL) in training AI models on large histopathology datasets, including over 5,000 patients. They developed disease classifiers for COVID-19, tuberculosis, leukemia, and lung pathologies, demonstrating the potential of SL to enhance medical imaging analysis without need for centralized data collection. Fan et al. [25] explored the fairness issues in SL, specifically within healthcare applications such as the classification of skin lesions. Their work demonstrated that SL outperformed centralized models without amplifying biases, though it also highlighted the complexities of implementing SL. Wang et al. [54] introduced SL-GAN, a framework that addresses non-IID data in decentralized ML, advancing the field by enhancing the quality of synthetic data through differential privacy techniques.

Aggarwal et al. [55] proposed DeMed, a decentralized privacy preservation system for medical image processing, combining blockchain and self-supervised learning to securely aggregate data, thus addressing challenges in decentralized systems. Chen et al. [23] and Li et al. [56] integrated homomorphic encryption with SL, ensuring secure model updates while preserving privacy. Their work introduced novel encryption methods to handle offline participants and mitigate model poisoning risks. Gao et al. [57] presented a methodology to mitigate the forgetting of global knowledge during local training, improving medical image segmentation with multicenter data. They introduced techniques such as Label Skew-Aware Loss (LaSA) and Feature Skew-Aware Regularization (FeSA) to address label and feature skew.

Yuan et al. [58] utilized Swarm Reinforcement Learning (SRL) and blockchain in MEC networks to optimize disease diagnosis, improve task offloading, and partitioning efficiency. Saldanha et al. [37] applied SL to the identification of gastric cancer biomarkers, suggesting that further research with more biomarkers and larger cohorts would strengthen their findings. Pan et al. [59] proposed an SL-driven system for drug development, improving bioavailability without compromising safety. Saldanha et al. [38] also used SL to train models on large histopathological datasets to predict markers of colorectal cancer. Zhang et al. [52] introduced a framework for sharing secure AI models in metaverse healthcare, addressing security, fairness, and data quality. Mohammed et al. [60] developed a decentralized disease diagnosis system using SL for nail images, achieving performance comparable to centralized models.

Shashank et al. [61] demonstrated the potential of SL as a privacy-preserving approach to analyze breast cancer data from various datasets, improving clinical research while maintaining data privacy. Purkayastha et al. [62] integrated user feedback into AI model training using SL and a few-shot learning, improving the collaboration between radiographers and AI through continuous training. Shriyan et al. [63] employed SL for cataract detection, proposing scalable, privacy-preserving healthcare solutions. He et al. [64] introduced DP-SL-GAN to tackle non-IID data in decentralized ML by generating synthetic data while maintaining privacy, achieving improved model performance. Finally, Saldanha et al. [65] combined weakly supervised learning with SL for breast cancer detection, showcasing enhanced collaboration between institutions and reducing the need for extensive annotations.

These articles highlight the versatility and transformative potential of SL in diverse healthcare applications, addressing privacy, scalability, and computational challenges, while paving the way for more efficient and secure decentralized machine learning systems. Table 2 summarizes the main contributions of these articles.

4.2 Transportation

Advancements in communication and computing technologies have greatly improved the Internet of Vehicles (IoV), which plays a key role in improving traffic management, emergency response, and efficiency in Intelligent Transportation Systems (ITS). FL and Federated Deep Learning (FDL) have been introduced to address privacy concerns in IoV applications [66], [67]. However, while SL offers significant advantages, its application in collaborative Vehicle Trajectory Prediction (VTP) presents challenges, including high communication overhead due to global network communication and increased blockchain costs as the network scales, reducing its effectiveness for large-scale deployments [66].

Lin et al. [68] proposed a cooperative framework for Vehicle Users (VUs) in the IoV, enabling model training without a central coordinator. Their approach considers VU mobility and incorporates an incentive system based on iterative auctions to encourage participation. The optimization model aims to balance social welfare and market equilibrium, offering a scalable solution for decentralized IoV learning environments. Fan et al. [69] introduced CB-DSL, a robust SL framework designed to address data heterogeneity, communication constraints, and security challenges in edge IoT networks. This innovative approach combines biological intelligence with AI to enhance model performance for traffic management, demonstrated through SUMO simulations and real-world healthcare data. CB-DSL improves forecast accuracy and optimizes real-time traffic signal control.

To overcome the limitations of FDL in IoV environments, Wang et al. [67] developed IoV-SFDL, a framework that integrates SL with FDL. The framework addresses communication overhead, vehicle movement, and erratic network conditions by leveraging credibility-based weight adjustment to accelerate model convergence, making it more effective for IoV applications. Hou et al. [66] introduced Hierarchical SL (HierSL), an edge-assisted framework for Vehicle Trajectory Prediction (VTP) in IoV systems. HierSL optimizes collaborative learning by reducing the reliance on global communication and blockchain, offering significant performance improvements over traditional SL and centralized learning, as demonstrated through tests on the NGSIM US-101 dataset.

Yin et al. [20] proposed a Multi-Region Asynchronous SL (MASL) framework that combines blockchain, edge computing, and FL to address the challenges of non-IID data and secure data sharing in large-scale IoV networks. MASL improves anomaly detection and improves data privacy by coordinating intra-regional and cross-regional sharing, making it a valuable solution for IoV systems. To mitigate urban traffic congestion, Liu et al. [70] presented DDaaS, a 6G-enabled solution. The system employs SL for parameter training, congestion prediction, and signal light management, demonstrated through SUMO simulations. DDaaS successfully reduces traffic congestion and improves prediction accuracy, offering a scalable approach to smart city traffic management. Mishra et al. [71] proposed a privacy-preserving SL approach for autonomous driving, addressing concerns related to the use of sensors and cameras. The framework allows secure model training and sharing across nodes, ensuring privacy while maintaining performance, and offering a more effective solution compared to traditional methods and other distributed machine learning approaches. Huang et al. [72] created a Directed Acyclic Graph (DAG)-based SL framework for IoV that integrates blockchain and edge computing to ensure secure and asynchronous model training. Their approach addresses

Table 2: Swarm Learning in Healthcare

Ref	Application	Contributions	Methodology	Datasets	Key Findings	Future Work
[14]	Medical imaging	Demonstrated SL potential for medical imaging analysis.	SL for pathology image analysis	Tuberculosis, leukemia, COVID-19, lung pathologies	Enhanced analysis through multicentric collaboration, maintaining data privacy.	Expand to other medical fields for broader global collaboration.
[25]	Skin disease	Investigated fairness in SL.	SL in skin lesion classification	Skin lesions	Maintained fairness with heterogeneous data without performance loss.	Improve model fairness and address bias.
[54]	Clinical settings	Addressed non-IID data challenges in ML.	SL-GAN for non-IID data	Tuberculosis, leukemia, COVID-19	Overcame challenges in decentralized ML for clinical use.	Further optimize decentralized ML and explore new algorithms.
[55]	Medical image analysis	Developed a privacy-preserving decentralized framework.	Blockchain-based SL	Chest X-rays	Used blockchain for privacy-preserving model training.	Expand to more complex tasks, increasing disease variety.
[23]	Privacy-preserving techniques	Applied homomorphic encryption in SL.	Paillier encryption with FedAvg aggregation	MNIST dataset	Advanced secure model updates while preserving data privacy.	Improve defense against model poisoning and handle offline participants.
[57]	Medical imaging	Solved global knowledge forgetting in local training.	Local knowledge assembly, LaSA loss	FeTS, M&Ms, MSProsMRI	Addressed Non-IID data issues, enhancing segmentation accuracy.	Apply to systems with unidirectional input constraints.
[58]	Disease diagnosis	Cooperative DNN partitioning for disease diagnosis.	Swarm Reinforcement Learning in MEC networks	VGG16, ResNet18	Accelerated disease diagnosis with minimal latency.	Validate in real clinical settings.
[37]	Molecular biomarkers	Predict biomarkers in gastric cancer.	SL-trained MSI and EBV models	Bern, Leeds, TUM Cohort, TCGA	Improved biomarker prediction with multicentric data.	Expand to more biomarkers and datasets.
[59]	Drug development	SL-based drug prediction system.	AI-driven discovery	DPN, DDN, DTN	Enhanced therapeutic effects of nitrate.	Clinical trials and pharmacokinetic studies.
[38]	Medical imaging	Predict molecular alterations in colorectal cancer.	Retrospective image analysis using SL	Northern Ireland, UK, TCGA	Demonstrated SL feasibility in predicting molecular features.	Expand to other oncology areas and improve scalability.
[52]	Metaverse healthcare	Secure AI model sharing in the metaverse.	Parameter merging for SL nodes	COVID-19, PAMAP datasets	Enhanced healthcare model reliability with SL.	Improve security and fairness in model-sharing.
[60]	Disease diagnosis	Diagnose from nail images using SL.	Transfer learning with SL nodes	Nail disease datasets	High diagnostic accuracy while maintaining privacy.	Expand to other medical data types and refine model training.
[61]	Cancer research	Utilized large medical data for cancer research.	SL for decentralized cancer diagnosis	WDBC, WPBC, BreakHis	Achieved decentralized learning with privacy adherence.	Expand decentralized training to improve oncology outcomes.
[62]	Radiology	Enhanced Human-AI partnerships.	SL with user feedback	WDBC, WPBC, BreakHis	Improved personalized radiological assessments.	Optimize Human-AI interaction.
[63]	Eye disease detection	Novel cataract detection method using SL.	VGG-19 architecture and SL integration	ODIR dataset	Highlighted SL's advantage over traditional methods.	Expand to detect more diseases.
[64]	Clinical ML	DP-SL-GAN for non-IID data handling with data augmentation and differential privacy.	SL, differential privacy, teacher-student sharing.	Clinical datasets	Improves performance and privacy over existing methods.	Explore scalability and expand to other domains.
[65]	Medical imaging	Combines weak supervision with SL for breast cancer detection in MRI.	SL for decentralized training	US, Switzerland, UK, Germany, Greece datasets	3D-ResNet-101 outperforms other models, SL enables multi-center collaboration with data privacy.	Expand SL to other medical fields and improve model robustness.

Table 3: Swarm Learning in Transportation

Ref	Application	Contributions	Methodology	Datasets	Key Findings	Future Work
[68]	IoV	Framework for cooperative model training without central coordinator	Cooperative SL with incentive mechanism	-	Communication-efficient; enhances social welfare	Improve incentive mechanisms for fair participation
[69]	Edge IoT	Byzantine-robust Distributed SL for traffic management	Evaluates model performance under i.i.d. and non-i.i.d. conditions	CIFAR-10, MNIST	Improves accuracy, addresses local optima	Validate in real-world settings and tackle more challenges
[67]	IoV	IoV-SFDL: Overcomes communication overhead and privacy issues in IoV	Integrates SL into Federated DL framework	NGSIM	Enhances model convergence speed	Expand to more dynamic IoV scenarios
[66]	VTP in IoV	Edge-assisted VTP framework	Hierarchical SL with two-layer learning	NGSIM US-101	Reduces global communication reliance, improves security	Optimize system topology for better efficiency
[20]	IoV	Secure framework for large-scale data sharing in IoVs	MASL with hierarchical blockchain	GTSRB	Improves scalability and security, preserves privacy	Improve training methods, expand blockchain integration
[70]	ITS	DDaaS for traffic congestion reduction	SL-based traffic simulation	-	Improves traffic management, reduces congestion	Enhance traffic control algorithms
[71]	Autonomous Driving	SL-based training method for autonomous driving systems	SL for privacy and performance	Kitti 3d	Superior privacy and potential performance gains	Compare with other distributed techniques
[72]	IoV	Improves data sharing and model training in IoV	Directed Acyclic Graph-based SL with edge computing	GTSRB	Enhances training and attack detection	Develop more robust attack detection mechanisms

challenges such as unreliable communications and malicious attacks by using a dynamic vehicle association algorithm to enhance model training efficiency while ensuring data privacy and security.

Table 3 shows the main contributions of these articles.

4.3 Industry

The Industrial Internet of Things (IIoT), driven by IoT, big data, and digital twin (DT) technologies, improves productivity and interoperability in advanced manufacturing. However, DT faces challenges in adapting to dynamic industrial environments and security concerns [73]. SL is transforming manufacturing by enabling intelligent real-time agents for resource allocation, production line optimization, and problem resolution without centralized control. This approach supports Industry 4.0 and smart manufacturing, creating resilient and intelligent factories for the future [74], [18]. However, there is limited research on the integration of SL with IIoT, particularly with regard to reliability in complex industrial environments with high temperatures and noise[73].

Pongfai et al. [15] introduced the Dragonfly SL process (D-SLP) algorithm, a novel approach designed for non-linear feedback control systems, which significantly enhances robustness, performance, and stability. Through comprehensive simulations, the algorithm demonstrated superior control capabilities for permanent magnet synchronous motors, although challenges related to unidirectional input constraints and dead zones persist. In a subsequent paper [16], the authors leveraged a deterministic Q-SLP algorithm to optimize the parameters of the PID controller, resulting in improved system performance, stability, and convergence time. The approach was validated against conventional methods such as IPSO and WOA, showing superior convergence and performance in the simulations. In their third contribution [75], an adaptive SLP method was proposed for multiple-input / multiple-output (MIMO) systems, allowing dynamic adjustment of PID controller parameters to enhance stability and resilience. This method was successfully validated using a two-wheel inverted pendulum system.

Sun et al. [17] propose a diagnostic system for the diagnosis of rotating machinery bearing faults, addressing major concerns of data privacy and scarce labeled data. Their new approach leverages convolutional neural networks (CNNs) and adversarial domain networks to facilitate local training without data sharing. Based on this study [18], they introduced an improved approach to the diagnosis of machine component faults with greater diagnosis accuracy and efficiency through the integration of local models such as AlexNet and Chebyshev filters.

Xiang et al. [73] introduced a paradigm-changing architecture for IIoT systems, with DT technology and credibility-weighted SL being applied to alleviate privacy threats and communication costs. They utilized a DRL approach to optimize system reliability and energy consumption, and an optimization problem was formulated to optimize operational efficiency and sustainability in the IIoT setting. Wang et al. [74] proposed an innovative solution to optimize robot assembly cells through cooperative multi-agent SL with DT technology. This model considers each component as an autonomous agent that dynamically responds to issues resulting from mechanical structure, networked software, and hardware integration. The approach supports dynamic reconfiguration, which allows manufacturing systems to respond effectively to dynamic production demands and cycles.

Table 4: Swarm Learning in Industry

Ref	Application	Contributions	Methodology	Datasets	Key Findings	Future Work
[15]	Nonlinear control systems	D-SLP algorithm for tuning control parameters with secure data sharing	Dragonfly algorithm with SL protocols	-	Superior control performance	Explore specific system constraints.
[16]	PID controller optimization	Optimized PID autotuning with deterministic Q-SLP algorithm	Swarm and learning for PID parameter refinement	CPC system	Improved convergence and performance	Not specified
[17]	Diagnostic frameworks	Framework for bearing fault diagnosis in rotating machinery	Adversarial domain networks with CNNs	CRWU, HITsz, XJTU-SY, SCU	Improved fault diagnosis efficiency	Not specified
[73]	IIoT	IIoT architecture enhanced by credibility-weighted SL	Digital Twin and credibility-weighted SL	MNIST dataset	Increased system reliability	Address practical concerns for operational efficiency
[74]	Robotic assembly cells	Optimized layout for reconfigurable robotic assembly	Multi-agent SL with digital twin	-	Improved layout optimization	Adapt to rapid manufacturing changes
[76]	Engine lifecycle data management	Blockchain-based method for data integrity	Blockchain with trusted application for validation	NASA open dataset	Enhanced data integrity	Optimize collaborative learning and data usage
[77]	Industrial analytics	Proposes IFBDAchain for secure federated learning with blockchain.	SL with Hyperledger fabric.	Fault classification, KPI prediction	Outperforms local learning in accuracy with non-i.i.d. data.	Improve scalability, real-time applications, and security.
[78]	Industrial robotics	CNN-integrated SL for privacy-preserving fault diagnosis.	CNNs with SL for decentralized training	Harmonic reducer dataset	Improved accuracy and efficiency without a central server.	Expand to other systems and optimize integration.

Luo and Zhang [76] suggested a blockchain-based approach to manage engine data integrity with a focus on preventing tampering and data deletion. Using SL, the solution ensures the privacy of the model parameter while enabling collaborative learning, thus making the best use of the data and improving the credibility of the system. Jiang et al. [77] presented a hybrid model driven by SL and blockchain techniques to attain collaborative and secure industrial big data analytics. IFBDAchain framework supports privacy protection and data integrity between various factories based on Hyperledger fabric. It improves fault classification and KPI prediction performance even in non-IID and imbalanced data settings and strengthens collaboration with robust privacy mechanisms and verification methods. Haodong et al. [78] proposed a data privacy-preserving diagnostic algorithm for industrial robot harmonic reducers, in which CNNs are integrated with SL. This architecture shares model parameters rather than raw data, improving computational efficiency and fault diagnosis accuracy in industrial environments without a central server, demonstrating its huge potential for practical use.

These SL-based architectures bring considerable improvements to industrial systems, improving efficiency, security, and scalability, and solving issues like data privacy, communication overhead, and reliability, thus making more robust and intelligent operations possible.

4.4 Robotic systems

Collaborative learning among multiple robots can significantly accelerate learning processes by forming a swarm, allowing them to share knowledge centrally or decentrally. In the context of SL, the nodes within the network exchange locally learned models without relying on a central authority. For networked robotic applications, a group of interconnected robots can either collaborate or work independently to complete tasks. Rangu and Nair [79] proposed a method that uses mobile agents to execute SL on a group of robots, where each agent learns a task. The approach employs a distributed learning model, with the mobile agent compiling and disseminating the learned models locally as it moves through a network of both simulated and real robots. Their experiment demonstrated the effectiveness of SL by using a mixed group of robots, recognizing the prohibitive cost of deploying a swarm of only real robots. By applying reinforcement learning at the local level, SL was proven to be efficient and practical in networks comprising both simulated and real robots.

4.5 Energy

The energy sector is adopting ML for forecasting, but privacy and scalability issues hinder centralized approaches. SL, a decentralized blockchain method, enables privacy-preserving collaboration between organizations, improving the

accuracy of forecasts without sharing raw data. This section explores the benefits of SL in improving model performance and ensuring data privacy[80]. Lei et al. [80] proposed a distributed SL strategy for energy sector problems, assuming cooperative, trustworthy parties with high data privacy. The approach addresses photovoltaic power generation and geophysical well-log prediction, analyzing data volume impact, local epoch variation, and security concerns. The results show that SL enables high-performance, secure collaborative learning without a central server, although limitations are discussed.

4.6 Smart home

Edge Intelligence (EI) integrates edge computing and AI in smart homes, real-time video analysis, and precision agriculture. However, centralized ML models have limitations such as data privacy breaches and communication overhead[81]

SL is transforming smart home ecosystems by enabling decentralized decision-making processes. This allows smart devices to communicate and learn from each other's experiences, optimizing energy consumption, security, and automation. Smart thermostats, lighting, and appliances can adjust settings based on occupants' habits, ensuring comfort and energy efficiency. SL also allows security networks to analyze data and adapt without human intervention.

Xu et al. [81] introduced a new cooperative SL framework to overcome central ML issues by leveraging decentralized SL to predict thermal comfort. This approach reduces communication overhead and improves model performance by leveraging real data from all nodes within the edge computing network. The framework's effectiveness was demonstrated through an extensive empirical investigation using a Non-IID thermal comfort dataset.

Liu et al.[82] developed ADONIS, a framework to detect abnormal behavior in IoT devices. It uses SL, knowledge distillation, and human-computer interaction (HCI) to improve security and operational efficiency. The decentralized approach reduces the risk of central node failure and reduces latency and energy consumption. ADONIS can be applied to smart cities and IoVs, and its adaptability makes it suitable for various applications. Future research includes further enhancements and refinement of parameter aggregation methods.

4.7 Financial services field

By using decentralized networks for data analysis, decision making, and risk management, SL is completely changing the financial services industry. The decentralized nature of SL transforms data-driven decisions in the complex financial landscape. Enhance investment recommendations and fraud detection rates while protecting against single-point failure. Using SL, financial organizations can modify their strategy in response to current market conditions and consumer trends. John et al.[19] used SL for credit scoring in Peer-to-Peer lending on a blockchain platform in the financial services industry, ensuring user data privacy and secure transactions. The decentralized model training and credit scoring process eliminate centralized data storage risks. Future work includes testing with real-time datasets and improving user experience.

4.8 Multimedia Internet of Things

By enabling the processing and dissemination of decentralized content in real-time in environments containing IoT devices, SL is transforming the Multimedia IoT ecosystem. This method guarantees that the content is personalized for each user, minimizes latency, and maximizes the utilization of network capacity. Furthermore, processing data locally on devices improves security and privacy by reducing the possibility that private information will be hacked.

Zhang et al.[83] have improved the privacy and security of multimedia IoT devices using Radio Frequency Fingerprinting (RFF) for identity authentication. They integrated differential privacy, specifically the Gaussian mechanism, into SL to protect RFF data. They also proposed a novel node evaluation mechanism to prevent malicious nodes from affecting the accuracy and integrity of the model. By guaranteeing the security of the underlying IoT devices through enhanced privacy protection in SL, the research paves the way for safe multimedia services.

4.9 Fake news detection

Social media has significantly impacted the distribution of information, but the lack of systematic management has led to the spread of fake news. ML techniques like CNN and recurrent neural networks (RNN) can detect fake news, but centralized detection can violate user privacy. Decentralized methods such as SL offer privacy-preserving learning on local data, reducing hacking risks, and allowing users to maintain confidentiality without sharing data [84]. Dong et al.[84] developed Human-in-the-loop Based SL (HBSL), a decentralized method to detect fake news. HBSL uses SL and human-in-the-loop (HITL) techniques to detect fake news between nodes, ensuring user privacy. It incorporates

Table 5: Swarm Learning Applications

Field	Ref	Application	Contributions	Methodology	Datasets	Key Findings	Future Work
Robotic systems	[79]	Networked robotic applications	SL with mobile agents for collaborative model training	Robots learn locally, mobile agent aggregates models	-	Efficient SL in robot swarm	Not specified
Energy systems	[80]	Decentralized collaborative learning for energy forecasting	SL with blockchain for secure, privacy-preserving model training	Energy forecasting, geophysical well logs	-	Outperforms centralized and federated learning with better privacy	Explore scalability and integration with more diverse energy datasets
Smart home	[81]	Edge intelligent computing networks	Cooperative SL for thermal comfort prediction	Stochastic gradient descent in a cyclic network	Non-IID thermal comfort dataset	Reduced communication, enhanced privacy	Optimize model performance for real-world data
	[82]	IoT abnormal behavior detection	ADONIS framework for IoT anomaly detection	SL with knowledge distillation	Traffic dataset	Enhanced IoT security and efficiency	Refine parameter aggregation and communication
Financial services	[19]	Credit scoring in P2P lending	Blockchain-based SL for credit scoring	Web 3.0 lending platform for secure transactions	Universal Bank dataset	Ensures privacy and secure transactions	Test dynamic datasets and explore other platforms
Multimedia IoT	[83]	IoT device security using RFF	SL with differential privacy for identity authentication	RFF dataset	-	Enhanced privacy and security in IoT	Extend methodologies to broader IoT applications
Fake news detection	[84]	Decentralized fake news detection	HBSL with user feedback for improved detection	Local learning and collaborative updates	LIAR dataset	Improved fake news detection accuracy	Design models tailored to specific nodes
Metaverse	[85]	6G-Metaverse XR communication	SL for secure resource trading in 6G-Metaverse	SL and blockchain for decentralized resource management	Custom dataset	Effective in XR communication and resource trading	Investigate SL customization for hardware resource management

user feedback, allowing models to be continuously updated. The method was validated using a benchmark dataset (LIAR), which shows its superiority over existing methods.

4.10 Metaverse

The Metaverse faces challenges in reliable extended reality (XR) data transmission due to a lack of incentives and untrust among users. To address these issues, a configurable SL-based safe resource trading mechanism is proposed in [85]. This framework includes subchains for decentralized intelligent reflective surfaces (IRS) resource management and intelligent allocation, a smart contract-enabled scheme, and a decentralized federated learning-driven IRS allocation scheme. Experimental results demonstrate the effectiveness of this configurable SL-based resource trading for reliable XR communication.

Table 5 shows the main contributions of those articles.

5 Challenges

SL enables decentralized collaboration, improving efficiency and privacy in applications such as IoT and healthcare. However, it faces challenges such as security risks, non-IID data, and fairness issues, which limit its wider adoption. The following subsections explore these challenges.

5.1 Attacks on SL

SL has the potential to handle distributed large-scale data better than FL, but it also faces significant security issues that require more scrutiny. In the stages of SL, as shown in Fig.9 [6], different attacks can occur: unreliable parties may compromise data during local training and before the locally trained metadata are secured on the blockchain, it might be vulnerable to various network attacks like Eclipse and DDoS. Furthermore, malicious participants could introduce harmful parameters during the merging process, potentially introducing backdoors into the global model. 1) Data poisoning might occur in the local training phase; 2) eclipse attacks could occur in the blockchain P2P network in the metadata upload phase; and 3) the global model could be hacked by poisoned parameters in the parameter aggregation phase [6].

5.1.1 Backdoor attacks against distributed SL

Despite its advantages in privacy and decentralized training, SL faces significant security challenges, notably backdoor attacks that compromise the integrity and reliability of the system. These attacks manipulate data and training processes,

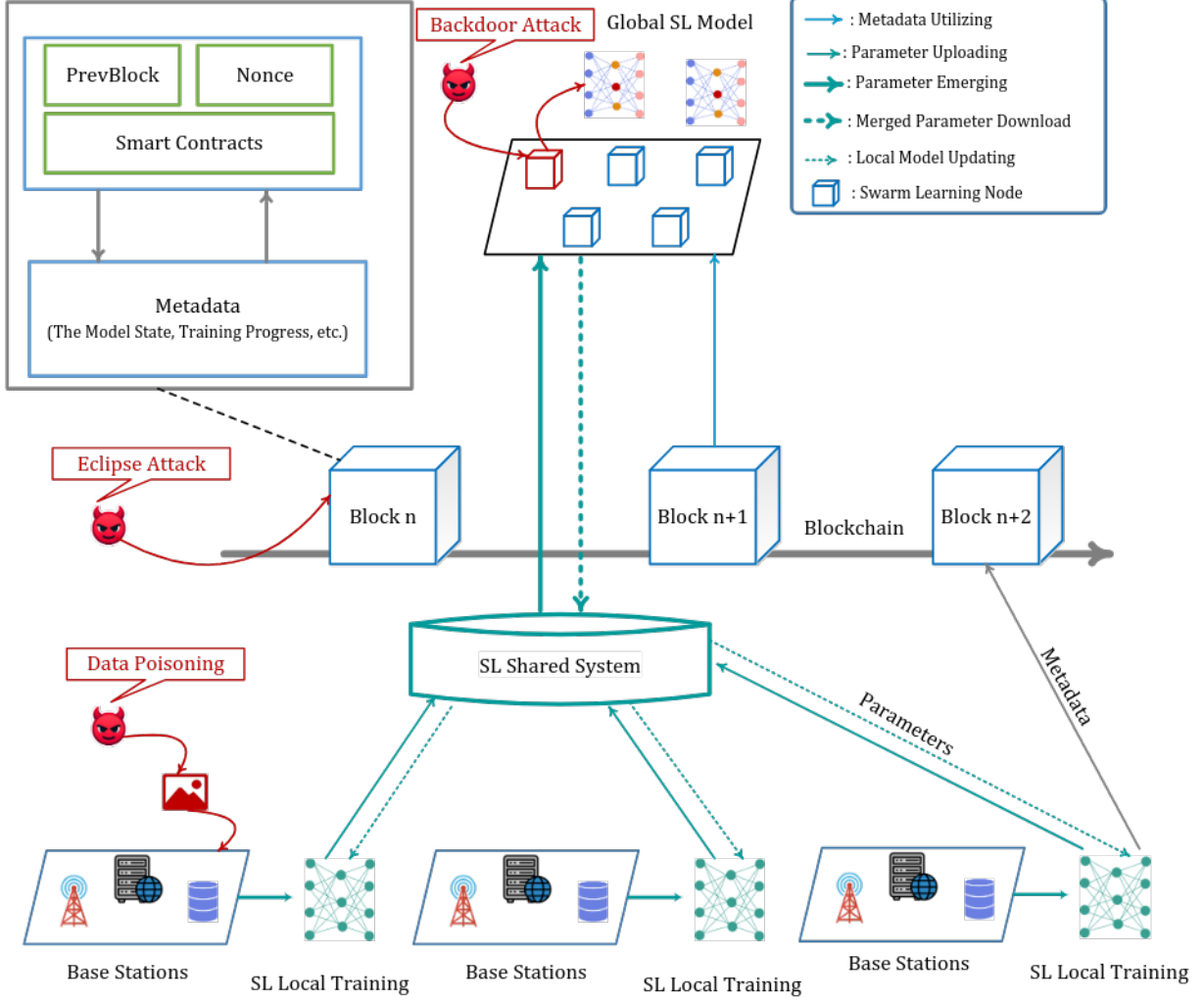


Figure 9: Attack on swarm learning

producing incorrect output. The decentralized nature of SL, coupled with non-IID data, complicates the detection of such attacks. Mitigating backdoor attacks requires advanced security measures, robust practices, and innovative collaborative learning techniques to maintain the integrity and trustworthiness of decentralized machine learning environments [6, 39].

Chen et al. [6] examined backdoor threats in SL using a pixel pattern backdoor attack method in different datasets (MNIST, CIFAR-10, SVHN). Their study explored various scenarios, including other network sizes, data distributions (IID vs. non-IID), attack targets (single vs. multi-target), and attack types (single-shot vs. multiple-shot). They proposed security strategies such as L2 regularization and noise injection, which were experimentally validated to mitigate the impacts of backdoor attacks.

Yang et al. [39] identified a hybrid vulnerability in SL, where backdoor and eclipse attacks spread backdoors covertly. They introduced the sample-specific eclipse (SSE) strategy, targeting high-contribution nodes to reduce attack costs and accelerate backdoor spread. This study is the first to combine distributed backdoor poisoning with eclipse attacks, revealing how they can work together to stealthily spread backdoors in the SL network. Their proposed strategy focuses on nodes with significant data contributions, enabling faster and more resource-efficient backdoor propagation.

5.1.2 Poisoning attack

SL faces unique challenges from poisoning attacks. Poisoning can compromise the collective learning process, affecting model parameters and performance. The decentralized nature of SL complicates detection, as there is no central authority to monitor data quality or model updates. Therefore, robust decentralized consensus mechanisms are needed to detect and mitigate poisoned inputs [39, 83, 33]. Qi Y. et al.[33] developed strategies to prevent poisoning attacks and ensure the integrity and security of the SL process.

Rongxuan et al.[86] suggested a Zero Trust Architecture (ZTA)-based defense mechanism for SL to resist poisoning attacks in decentralized learning environments. It identifies a certain flaw in which an attacker 'header' node may poison the model. The defense mechanism is centered around continuous risk calculation and anomaly detection, facilitating dynamic reactions towards threats. The scheme also uses the Manhattan distance and accuracy difference for the detection and avoidance of both header node and edge node threats. The efficiency of the proposed defense method is demonstrated through extensive experiments, demonstrating its implementability in real-world scenarios.

5.1.3 Eclipse attack

An Eclipse attack in SL involves an attacker controlling the network communication between nodes. This fits perfectly in peer-to-peer systems where nodes share information and model updates without any central authority [39]. An attacker can isolate a victim node or a group of nodes by controlling their network link, even supplying them with incorrect information or model updates [87]. This would impact the integrity of the model and its performance. In order to protect against Eclipse attacks, robust peer discovery and management measures need to be utilized, such as heterogeneous peer connections, peer identity verification, and identifying network patterns that could signify control over communication channels[39].

5.1.4 Denial of service attacks (DoDs) attack

DoS attacks compromise decentralized decision making by poisoning adversarial updates or corrupting the aggregation of model parameters, which can bias decisions in critical applications such as healthcare and autonomous driving. To protect against these attacks, there should be effective consensus mechanisms and anomaly detection techniques to ensure that only reliable updates are incorporated into model aggregation [6, 86].

5.1.5 Sponge attack

. Sponge attack is a DoS attack that takes place in decentralized systems where they are flooded with spurious data, straining system resources and causing significant slowdowns. This interference prevents the ML processes from converging appropriately. Due to the fact that decentralized systems have no centralized point of control, detection and counteractions are difficult, particularly when weaker nodes are attacked. [6, 86].

5.1.6 Inference attacks

Inference attacks aim to deduce sensitive information about the training data used by a model, such as recovering private or sensitive attributes. They can be used to determine if a specific data record was part of the training set, infer specific attributes or features of data instances, or attempt to reconstruct a model's parameters. Inference attacks focus on extracting information about the training data or model behavior, such as determining if specific data were used in training or guessing private attributes based on model outputs. Decentralized ML methods allow multiple nodes to collaboratively learn a shared model without exchanging local data, typically using blockchain technology [88]. Inference attacks exploit shared model updates or the final model to infer properties of the training data or identify unique characteristics of individual participants' datasets. Advanced cryptographic and privacy-preserving techniques such as homomorphic encryption, secure multi-party computation, and differential privacy are employed to protect against inference attacks. However, the balance between privacy protection and model performance is a critical challenge in SL[83].

5.1.7 Model inversion attacks

Model inversion attacks aim directly at reconstructing the inputs used to train the model, effectively reversing the model's computations to approximate or reveal the actual data. They often target models that provide detailed or confident predictions, which can inadvertently reveal information about the training data [89]. While inference attacks often derive indirect information about the data or its attributes, model inversion attacks engage in a more direct and complex effort to recreate the original training inputs themselves. In SL, where nodes collaborate to train a model without sharing their local datasets. The decentralized nature of SL allows each node to contribute to the model's

learning by updating it based on local data. However, shared model updates or predictions can leak information, potentially inferring specific characteristics or reconstructing aspects of the original training data. To defend against model inversion attacks, strategies such as output perturbation, differential privacy mechanisms, access controls, and strict query limits can be implemented[83].

5.2 Non-IID Problem in SL

SL enables participants to register, train models, and exchange parameters through edge nodes, ensuring data sovereignty and confidentiality. However, SL performance is significantly affected by non-independent and identically distributed (Non-IID) data[54], which can lead to inconsistent model updates and degraded aggregate performance. When data is dispersed unevenly among various network nodes or participants, it is called the non-IID problem in SL. This implies that distinct statistical characteristics, such as mean, variance, and data distribution patterns, may exist in the dataset at each node. Several factors, including variations in patient demographics, the type of medical equipment used, or even the particular focus or specialization of the medical institutes providing the data, could contribute to this heterogeneity in the data. Non-IID data problems include quantity, label, and feature skews. Feature skew and label skew are caused by differences in imaging protocols or demographics, leading to inconsistencies in annotations and Non-IID label distributions. Various strategies, including elastic weight consolidation and batch normalization, have been proposed to address the skews of the features, labels, and quantities in classification tasks. However, these methods do not fully consider label skew, which could cause suboptimal performance[57], [90].

Two types of strategy are now being used to tackle the non-IID challenge: algorithm-based and data-based approaches. Algorithm-based methods align local models with global models, while data-based methods balance distribution but require a trusted central coordinator. Furthermore, with non-IID data, convergence problems may arise when utilizing Generative Adversarial Networks (GAN) for data augmentation[54].

To address the non-IID problem in SL, methods must be created that can either reduce the impact of data heterogeneity or take advantage of it to increase the global model's resilience and generalizability. Strategies such as advanced aggregation techniques, personalized models, and data augmentation can improve the robustness and generalizability of the global model[57]. Currently, effective solutions to address the problem of non-IID in SL have not yet been established[54].

5.3 Fairness and bias in SL

Fairness and bias in ML models indicate how they could perform or reflect dominant groupings in the data in an unbalanced way. The impact of SL on model bias and fairness has not yet been fully assessed, even though fairness issues have been considered in the context of FL. In[25], the authors suggested comparing SL with centralized learning and subgroup-specific model training to investigate the fairness of SL in medical imaging tasks without the need for additional bias mitigation techniques. To provide insight into how SL might balance performance and fairness in healthcare applications, their study seeks to determine if SL's fairness features are more in line with centralized learning or subgroup-specific training.

Future research should focus on developing algorithms that ensure fairness in SL by providing personalized models based on node contributions. This approach needs to balance performance and fairness, encouraging greater participation from nodes with higher contributions. Empirical studies and comparisons with traditional models are necessary to evaluate the effectiveness and scalability of this approach in real world scenarios [91].

6 Future Research

SL addresses privacy and data integration issues, but research gaps exist, indicating potential areas for further exploration.

- **Security and Trust:** While SL leverages blockchain for security and trust, further research is needed to address potential vulnerabilities, such as advanced cyber threats and insider attacks. Strong trust mechanisms and tailored security measures are crucial for SL networks. Swarm-FHE [92] enhances SL security by integrating fully homomorphic encryption with blockchain, enabling secure collaborative model training even with compromised participants. Additionally, Li et al. [50] combine blockchain and lightweight homomorphic encryption to ensure model security, data privacy, and computational efficiency, offering a competitive alternative to Federated Learning in remote ML applications [93].
- **Dynamic Node Management:** Enhancing the robustness and dependability of SL systems may involve investigating dynamic techniques for node participation and incentive mechanisms to guarantee nodes' continued and productive engagement in the swarm network.

- **Optimizing Leader Election:** The leader election process in SL can lead to disproportionate bandwidth consumption, inefficiencies, and potential bottlenecks, causing dissatisfaction among participants and potentially compromising network security. To address these challenges, [26] suggested refining the leader election mechanism for more equitable network load distribution.
- **Scalability and Efficiency:** The ability of SL to expand across a growing number of nodes and a variety of data formats while maintaining efficiency and model performance should be investigated. Enhancing model aggregation techniques and communication protocols could be the main areas of research to facilitate widespread implementations of SL.
- **Interoperability and Standards:** For SL to succeed, standards compliance and interoperability amongst various systems are essential. To solve issues with data format, protocols, and compliance, research could examine methods for SL to seamlessly integrate into existing IT systems. Qi et al.[33] developed a blockchain twin mechanism to improve the interoperability and efficiency of SL on different blockchains, introducing an incentive mechanism for active participation, thus improving the overall performance and security of the SL process.
- **Energy Efficiency:** Considering the possible magnitude of SL deployments, especially in the context of IoT, the development of power-saving learning algorithms is of the utmost importance. The emphasis of such research would be on minimizing the energy usage of devices involved in the SL process, a factor that is particularly critical for devices running on batteries or sensors located remotely.
- **Cross-domain Applications:** Investigating the potential use of SL in diverse sectors like healthcare, autonomous vehicles, smart cities, and manufacturing can be extremely advantageous. Each of these areas poses distinct challenges and demands, and customized SL approaches could result in significant advancements in how these sectors employ decentralized learning.
- **Data Heterogeneity and Non-IID Data:** To efficiently tackle the non-IID issue in SL, forthcoming studies might concentrate on the creation of a hybrid model adaptation method that merges both algorithmic innovations and robust data management strategies. The goal of this method should be to reduce the effects of data heterogeneity and boost the performance and unification of the global model in a distributed environment.
- **Advanced-Data Augmentation Techniques:** Investigate the application of advanced generative models, like variational autoencoders (VAEs) or enhanced GANs, to produce synthetic data samples. These samples can efficiently supplement sparse or imbalanced datasets across different nodes, thereby addressing the non-IID problem.
- **Ethical AI and Fairness:** As SL models become more widespread, it is crucial to ensure that these models do not perpetuate or exacerbate biases. Research could focus on developing fairness-sensitive algorithms that promote ethical AI practices within SL frameworks.
- **Resource Management:** As mentioned in[26], adding more Swarm coordinator nodes on resource overhead is negligible. However, the resource overhead increases linearly with the number of Swarm edge nodes added, indicating that scaling these nodes should be done carefully. This observation provides valuable guidance and actionable recommendations for developers and researchers applying SL effectively in real-world scenarios. Optimizing the use of computational resources across distributed networks is crucial, especially for resource-constrained environments like IoT devices. More work is needed to reduce communication overhead and improve computational efficiency [27].
- **Deployment Optimization:** Further investigation is needed on how to optimize SL for real-world deployment, particularly concerning the scalability of SL in diverse environments with different network conditions and data distributions [27].
- **Integrating ML into SL:** Integrating ML methods into the SL framework can introduce challenges in analyzing the specific contributions of SL to training rate improvements. SL uses blockchain technology to synchronize model updates amongst nodes. Although confidentiality and integrity are guaranteed, the overhead resulting from blockchain operations (such as consensus processes and transaction validations) may outweigh the anticipated gains in training speed from concurrent decentralized training. Therefore, integrating ML methods into SL may complicate the assessment of training rate improvements. Empirical studies and benchmarking against traditional systems are needed to assess its benefits in real-world scenarios.
- **Communication overhead:** The Swarm Mutual Learning (SML) framework introduces the Adaptive Mutual Distillation Algorithm and Global Parameter Aggregation Algorithm, which help reduce communication overhead and improve model accuracy [94]. However, optimizing these algorithms for larger datasets and more complex applications remains challenging. Further research is needed to refine the distillation techniques for better knowledge transfer efficiency and explore alternative encryption methods to enhance security while minimizing communication costs.

7 Conclusion

SL is a cutting-edge and promising decentralized ML innovation that accommodates secure, efficient, and privacy-preserving collaborative learning independent of data centralization. The review provides invaluable information on the benefits of SL and demonstrates how SL accommodates secure, confidential, and efficient collaborative ML for distributed networks. The main advantages of SL include improved data privacy, reduced chances of centralized data breaches, and the ability to learn from disparate data sources without data transfer, thus avoiding privacy risks. SL can be applied across a wide range of domains, from healthcare to IoV and industrial settings where data confidentiality and learning from distributed and sensitive data are of concern. However, SL must overcome a couple of challenges to reach its full potential.

However, SL must address several challenges to fully realize its potential. Issues such as non-IID data, fairness, bias, and vulnerability to attacks must be carefully considered. To overcome these hurdles, robust decentralized consensus mechanisms and advanced cryptographic techniques are essential to maintain the integrity and privacy of the system. These challenges present significant opportunities for further research and development, offering a broad scope for scholars and practitioners interested in advancing the field of decentralized ML.

References

- [1] Faisal Alsubaei, Abdullah Abuhussein, Vivek Shandilya, and Sajjan Shiva. Iomt-saf: Internet of medical things security assessment framework. *Internet of Things*, 8:100123, 2019.
- [2] Samira A Baho and Jemal Abawajy. Analysis of consumer iot device vulnerability quantification frameworks. *Electronics*, 12(5):1176, 2023.
- [3] Ali Ghubaish, Tara Salman, Maede Zolanvari, Devrim Unal, Abdulla Al-Ali, and Raj Jain. Recent advances in the internet-of-medical-things (iomt) systems security. *IEEE Internet of Things Journal*, 8(11):8707–8718, 2020.
- [4] Vitaly A Dovgal. Swarm learning based on the artificially intelligent edge. In *CEUR Workshop Proceedings*, volume 3057, pages 260–265, 2021.
- [5] Yuwei Sun, Hideya Ochiai, and Hiroshi Esaki. Decentralized deep learning for multi-access edge computing: A survey on communication efficiency and trustworthiness. *IEEE Transactions on Artificial Intelligence*, 3(6):963–972, 2021.
- [6] Kongyang Chen, Huaiyuan Zhang, Xiangyu Feng, Xiaoting Zhang, Bing Mi, and Zhiping Jin. Backdoor attacks against distributed swarm learning. *ISA transactions*, 2023.
- [7] Haoran Zhang, Shan Jiang, and Shichang Xuan. Decentralized federated learning based on blockchain: concepts, framework, and challenges. *Computer Communications*, 216:140–150, 2024.
- [8] Enrique Tomás Martínez Beltrán, Mario Quiles Pérez, Pedro Miguel Sánchez Sánchez, Sergio López Bernal, Jérôme Bovet, Manuel Gil Pérez, Gregorio Martínez Pérez, and Alberto Huertas Celdrán. Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges. *IEEE Communications Surveys & Tutorials*, 2023.
- [9] Banhirup Sengupta, Souvik Sengupta, Susham Nandi, and Anthony Simonet-Boulogne. Blockchain and federated-learning empowered secure and trustworthy vehicular traffic. In *2022 IEEE/ACM 15th International Conference on Utility and Cloud Computing (UCC)*, pages 346–351. IEEE, 2022.
- [10] Mohamed Ghanem, Fadi Dawoud, Habiba Gamal, Eslam Soliman, Tamer El-Batt, and Hossam Sharara. Flobc: A decentralized blockchain-based federated learning framework. In *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*, pages 85–92. IEEE, 2022.
- [11] Hussain Ahmad Madni, Rao Muhammad Umer, and Gian Luca Foresti. Blockchain-based swarm learning for the mitigation of gradient leakage in federated learning. *IEEE Access*, 11:16549–16556, 2023.
- [12] Dincy R. Arikkat, Mert Cihangiroglu, Mauro Conti, Rafidha Rehiman K.A., Serena Nicolazzo, Antonino Nocera, and Vinod P. Sectis: A framework to secure cti sharing. *Future Generation Computer Systems*, 164:107562, 2025.
- [13] Ran Wang, Cheng Xu, Shuhao Zhang, Fangwen Ye, Yusen Tang, Sisui Tang, Hangning Zhang, Wendi Du, and Xiaotong Zhang. Matswarm: trusted swarm transfer learning driven materials computation for secure big data sharing. *Nature Communications*, 15(1):9290, 2024.
- [14] Stefanie Warnat-Herresthal, Hartmut Schultze, Krishnaprasad Lingadahalli Shastry, Sathyanarayanan Manamohan, Saikat Mukherjee, Vishesh Garg, Ravi Sarveswara, Kristian Händler, Peter Pickkers, N Ahmad Aziz, et al. Swarm learning for decentralized and confidential clinical machine learning. *Nature*, 594(7862):265–270, 2021.

- [15] Jirapun Pongfai, Wudhichai Assawinchaichote, Peng Shi, and Xiaojie Su. Novel d-slp controller design for nonlinear feedback control. *IEEE Access*, 8:128796–128808, 2020.
- [16] Jirapun Pongfai, Xiaojie Su, Huiyan Zhang, and Wudhichai Assawinchaichote. Pid controller autotuning design by a deterministic q-slp algorithm. *IEEE Access*, 8:50010–50021, 2020.
- [17] Shilong Sun, Haodong Huang, Tengyi Peng, Changqing Shen, and Dong Wang. A data privacy protection diagnosis framework for multiple machines vibration signals based on a swarm learning algorithm. *IEEE Transactions on Instrumentation and Measurement*, 72:1–9, 2023.
- [18] Shilong Sun, Haodong Huang, Tengyi Peng, and Dong Wang. An improved data privacy diagnostic framework for multiple machinery components data based on swarm learning algorithm. *IEEE Transactions on Instrumentation and Measurement*, 2023.
- [19] Antony Prince John, Jagadhiswaran Devaraj, Lathaselvi Gandhimaruthian, and Javid Ali Liakath. Swarm learning based credit scoring for p2p lending in block chain. *Peer-to-Peer Networking and Applications*, 16(5):2113–2130, 2023.
- [20] Hongbo Yin, Xiaoge Huang, Yuhang Wu, Chengchao Liang, and Qianbin Chen. Multi-region asynchronous swarm learning for data sharing in large-scale internet of vehicles. *IEEE Communications Letters*, 2023.
- [21] Evangelia Fragkou and Dimitrios Katsaros. A joint survey in decentralized federated learning and tinyml: A brief introduction to swarm learning. *Future Internet*, 16(4):413, 2024.
- [22] Mohammad Tajabadi, Roman Martin, and Dominik Heider. Privacy-preserving decentralized learning methods for biomedical applications. *Computational and Structural Biotechnology Journal*, 23:3281–3287, 2024.
- [23] Lijie Chen, Shaojing Fu, Liu Lin, Yuchuan Luo, and Wentao Zhao. Privacy-preserving swarm learning based on homomorphic encryption. In *International Conference on Algorithms and Architectures for Parallel Processing*, pages 509–523. Springer, 2021.
- [24] Jiajin Yang, Lixing Chen, Junhua Tang, Jianhua Li, and Wu Yang. Swarm reinforcement learning for collaborative content caching in information centric networks. In *ICC 2023-IEEE International Conference on Communications*, pages 384–390. IEEE, 2023.
- [25] Di Fan, Yifan Wu, and Xiaoxiao Li. On the fairness of swarm learning in skin lesion classification. In *Clinical Image-Based Procedures, Distributed and Collaborative Learning, Artificial Intelligence for Combating COVID-19 and Secure and Privacy-Preserving Machine Learning: 10th Workshop, CLIP 2021, Second Workshop, DCL 2021, First Workshop, LL-COVID19 2021, and First Workshop and Tutorial, PPML 2021, Held in Conjunction with MICCAI 2021, Strasbourg, France, September 27 and October 1, 2021, Proceedings 2*, pages 120–129. Springer, 2021.
- [26] Jialiang Han, Yun Ma, and Yudong Han. Demystifying swarm learning: A new paradigm of blockchain-based decentralized federated learning. *arXiv preprint arXiv:2201.05286*, 2022.
- [27] Jialiang Han, Yudong Han, Ying Zhang, Xiang Jing, and Yun Ma. Demystifying swarm learning: An emerging decentralized federated learning system. In *2024 IEEE 24th International Symposium on Cluster, Cloud and Internet Computing (CCGrid)*, pages 367–373, 2024.
- [28] Matteo Mantovani, Riccardo Scheda, Carlo Combi, and Stefano Diciotti. A Key Performance Indicator to Analyze Swarm Learning Performances with EHR . In *2024 IEEE 12th International Conference on Healthcare Informatics (ICHI)*, pages 620–625, Los Alamitos, CA, USA, June 2024. IEEE Computer Society.
- [29] Xin Fan, Yue Wang, Yan Huo, and Zhi Tian. Efficient distributed swarm learning for edge computing. In *ICC 2023-IEEE International Conference on Communications*, pages 3627–3632. IEEE, 2023.
- [30] Xin Fan, Yue Wang, Yan Huo, and Zhi Tian. Robust distributed swarm learning for intelligent iot. In *ICC 2023-IEEE International Conference on Communications*, pages 973–978. IEEE, 2023.
- [31] Hewlett Packard. Swarm learning. <https://github.com/HewlettPackard/swarm-learning>, 2023. Accessed: March 2023.
- [32] Joachim L Schultze, Maren Büttner, and Matthias Becker. Swarm immunology: harnessing blockchain technology and artificial intelligence in human immunology. *Nature Reviews Immunology*, 22(7):401–403, 2022.
- [33] Yuxin Qi, Xi Lin, Jun Wu, and Yunyun Han. Game-aided blockchain twin for incentive and relay-free model sharing in heterogeneous chain-driven swarm learning. *IEEE Systems Journal*, 2023.
- [34] Caner Korkmaz, Halil Eralp Kocas, Ahmet Uysal, Ahmed Masry, Oznur Ozkasap, and Baris Akgun. Chain fl: Decentralized federated machine learning via blockchain. In *2020 Second international conference on blockchain computing and applications (BCCA)*, pages 140–146. IEEE, 2020.

- [35] Tian Wang, Yan Liu, Xi Zheng, Hong-Ning Dai, Weijia Jia, and Mande Xie. Edge-based communication optimization for distributed federated learning. *IEEE Transactions on Network Science and Engineering*, 9(4):2015–2024, 2021.
- [36] Xiaokang Zhou, Wang Huang, Wei Liang, Zheng Yan, Jianhua Ma, Yi Pan, I Kevin, and Kai Wang. Federated distillation and blockchain empowered secure knowledge sharing for internet of medical things. *Information Sciences*, 662:120217, 2024.
- [37] Oliver Lester Saldanha, Hannah Sophie Muti, Heike I Grabsch, Rupert Langer, Bastian Dislich, Meike Kohlruss, Gisela Keller, Marko van Treeck, Katherine Jane Hewitt, Fiona R Kolbinger, et al. Direct prediction of genetic aberrations from pathology images in gastric cancer with swarm learning. *Gastric cancer*, 26(2):264–274, 2023.
- [38] Oliver Lester Saldanha, Philip Quirke, Nicholas P West, Jacqueline A James, Maurice B Loughrey, Heike I Grabsch, Manuel Salto-Tellez, Elizabeth Alwers, Didem Cifci, Narmin Ghaffari Laleh, et al. Swarm learning for decentralized artificial intelligence in cancer histopathology. *Nature Medicine*, 28(6):1232–1239, 2022.
- [39] Zheng Yang, Gaolei Li, Jun Wu, and Wu Yang. Propagable backdoors over blockchain-based federated learning via sample-specific eclipse. In *GLOBECOM 2022-2022 IEEE Global Communications Conference*, pages 2579–2584. IEEE, 2022.
- [40] Ehsan Hallaji, Roozbeh Razavi-Far, Mehrdad Saif, Boyu Wang, and Qiang Yang. Decentralized federated learning: A survey on security and privacy. *IEEE Transactions on Big Data*, 2024.
- [41] Mazin Abed Mohammed, Abdullah Lakhan, Karrar Hameed Abdulkareem, Dilovan Asaad Zebari, Jan Nedoma, Radek Martinek, Seifedine Kadry, and Begonya Garcia-Zapirain. Energy-efficient distributed federated learning offloading and scheduling healthcare system in blockchain based networks. *Internet of Things*, 22:100815, 2023.
- [42] Anik Islam and Soo Young Shin. A digital twin-based drone-assisted secure data aggregation scheme with federated learning in artificial intelligence of things. *IEEE Network*, 37(2):278–285, 2023.
- [43] Weihao Zhu, Long Shi, Jun Li, Bin Cao, Kang Wei, Zhe Wang, and Tao Huang. Trustworthy blockchain-assisted federated learning: Decentralized reputation management and performance optimization. *IEEE Internet of Things Journal*, 12(3):2890–2905, 2025.
- [44] Wenrui Yu, Qiongxiu Li, Milan Lopuhaä-Zwakenberg, Mads Græsbøll Christensen, and Richard Heusdens. Provable privacy advantages of decentralized federated learning via distributed optimization. *IEEE Transactions on Information Forensics and Security*, 20:822–838, 2025.
- [45] Chongyang Tan, Donghong Cai, Fang Fang, Zhiguo Ding, and Pingzhi Fan. Federated unfolding learning for csi feedback in distributed edge networks. *IEEE Transactions on Communications*, 73(1):410–424, 2025.
- [46] Yunpeng Xiao, Xufeng Li, Tun Li, Rong Wang, Yucai Pang, and Guoyin Wang. A distributed generative adversarial network for data augmentation under vertical federated learning. *IEEE Transactions on Big Data*, 11(1):74–85, 2025.
- [47] M. Wei, W. Yu, D. Chen, M. Kang, and G. Cheng. Privacy distributed constrained optimization over time-varying unbalanced networks and its application in federated learning. *IEEE/CAA J. Autom. Sinica*, 12(2):335–346, Feb. 2025.
- [48] C Jason Liang, Chongliang Luo, Henry R Kranzler, Jiang Bian, and Yong Chen. Communication-efficient federated learning of temporal effects on opioid use disorder with data from distributed research networks. *Journal of the American Medical Informatics Association*, page ocae313, 01 2025.
- [49] Xiaobing Gan and Baoyu Xiao. Improved bacterial foraging optimization algorithm with comprehensive swarm learning strategies. In *Advances in Swarm Intelligence: 11th International Conference, ICSI 2020, Belgrade, Serbia, July 14–20, 2020, Proceedings 11*, pages 325–334. Springer, 2020.
- [50] Vladislav Bolshakov, Alexander Alfmimtsev, Sergey Sakulin, and Nikita Bykov. Deep reinforcement ant colony optimization for swarm learning. In *Advances in Neural Computation, Machine Learning, and Cognitive Research V: Selected Papers from the XXIII International Conference on Neuroinformatics, October 18–22, 2021, Moscow, Russia*, pages 9–15. Springer, 2022.
- [51] Matthias Becker. Swarm learning for decentralized healthcare. *Der Hautarzt*, 73(4):323–325, 2022.
- [52] Guoqiang Zhang, Yueyue Dai, Jian Wu, Xiaojie Zhu, and Yunlong Lu. Swarm learning-based secure and fair model sharing for metaverse healthcare. *Mobile Networks and Applications*, pages 1–12, 2023.
- [53] Joachim L Schultze. Building trust in medical use of artificial intelligence-the swarm learning principle. *Journal of CME*, 12(1):2162202, 2023.

- [54] Zirui Wang, Shaoming Duan, Chengyue Wu, Wenhao Lin, Xinyu Zha, Peiyi Han, and Chuanyi Liu. Generative data augmentation for non-iid problem in decentralized clinical machine learning. In *2022 4th International Conference on Data Intelligence and Security (ICDIS)*, pages 336–343. IEEE, 2022.
- [55] Garima Aggarwal, Chun-Yin Huang, Di Fan, Xiaoxiao Li, and Zehua Wang. Demed: A novel and efficient decentralized learning framework for medical images classification on blockchain. In *International Workshop on Distributed, Collaborative, and Federated Learning*, pages 100–109. Springer, 2022.
- [56] Yong Li, Haichao Ling, Xianglin Ren, Chun Yu, and Tongtong Liu. Privacy-preserving swarm learning based on lightweight homomorphic encryption and blockchain technology. In *2023 IEEE 5th Eurasia Conference on IOT, Communication and Engineering (ECICE)*, pages 692–697. IEEE, 2023.
- [57] Zheyao Gao, Fuping Wu, Weiguo Gao, and Xiahai Zhuang. A new framework of swarm learning consolidating knowledge from multi-center non-iid data for medical image segmentation. *IEEE Transactions on Medical Imaging*, 2022.
- [58] Xiaohan Yuan, Chuan Sun, and Shuyu Chen. Cooperative dnn partitioning for accelerating dnn-empowered disease diagnosis via swarm reinforcement learning. *Applied Soft Computing*, 148:110844, 2023.
- [59] Wen Pan, Geng Hu, Shaorong Li, Guoqing Li, Xiaoyu Feng, Zhifang Wu, Dong Zhang, Lizheng Qin, Xue Wang, Liang Hu, et al. Nanonitrator: novel enhancer of inorganic nitrate’s protective effects, predicated on swarm learning approach. *Science Bulletin*, 68(8):838–850, 2023.
- [60] Aasim Mohammed, PS Shrikanth Karthik, Razik Fatin Shariff, Tankala Sunaina, Arti Arya, and Pooja Agarwal. Privacy preserving early disease diagnosis in human nails using swarm learning. In *International Conference on Information and Communication Technology for Intelligent Systems*, pages 117–130. Springer, 2023.
- [61] HS Shashank, Anirudh B Sathyanarayana, Aniruddh Acharya, MR Akhil, and Sujatha R Upadhyaya. Swarm learning for oncology research. In *International Conference on Multi-disciplinary Trends in Artificial Intelligence*, pages 159–168. Springer, 2023.
- [62] Saptarshi Purkayastha, Rohan Isaac, Sharon Anthony, Shikhar Shukla, Elizabeth A Krupinski, Joshua A Danish, and Judy Wawira Gichoya. A general-purpose ai assistant embedded in an open-source radiology information system. In *International Conference on Artificial Intelligence in Medicine*, pages 373–377. Springer, 2023.
- [63] Thilak Shekhar Shriyan, Samyak Maurya, Janavi Srinivasan, Vaibhav Guruprasad Achar, Pooja Agarwal, and Arti Arya. An empirical study on privacy-preserving swarm learning for cataract detection. In *International Conference on Computational & Experimental Engineering and Sciences*, pages 1–13. Springer, 2023.
- [64] Tianyu He, Peiyi Han, Shaoming Duan, Zirui Wang, Wentai Wu, Chuanyi Liu, and Jianrun Han. Generative data augmentation with differential privacy for non-iid problem in decentralized clinical machine learning. *Future Generation Computer Systems*, 160:171–184, 2024.
- [65] O.L. Saldanha, J. Zhu, G. Müller-Franzes, and et al. Swarm learning with weak supervision enables automatic breast cancer detection in magnetic resonance imaging. *Commun Med*, 5, 2025.
- [66] Xuwei Hou, Lixing Chen, Junhua Tang, Jianhua Li, and Wu Yang. Hierarchical swarm learning for edge-assisted collaborative vehicle trajectory prediction. In *ICC 2023-IEEE International Conference on Communications*, pages 4144–4149. IEEE, 2023.
- [67] Zhe Wang, Xinhang Li, Tianhao Wu, Chen Xu, and Lin Zhang. A credibility-aware swarm-federated deep learning framework in internet of vehicles. *Digital Communications and Networks*, 2023.
- [68] Shangjing Lin, Yueying Li, Bei Zhuang, Tao Ning, Ziyi Li, Chunhong Zhang, and Zheng Hu. Double auction mechanism for cooperative swarm learning in internet of vehicles. In *2022 IEEE Globecom Workshops (GC Wkshps)*, pages 1102–1108. IEEE, 2022.
- [69] Xin Fan, Yue Wang, Yan Huo, and Zhi Tian. Cb-dsl: Communication-efficient and byzantine-robust distributed swarm learning on non-iid data. *IEEE Transactions on Cognitive Communications and Networking*, 2023.
- [70] Yibing Liu, Lijun Huo, Jun Wu, and Ali Kashif Bashir. Swarm learning-based dynamic optimal management for traffic congestion in 6g-driven intelligent transportation system. *IEEE Transactions on Intelligent Transportation Systems*, 2023.
- [71] Abhishek Mishra, OP Joy Jefferson, Pradish Kapur, Kiran Kannur, Pooja Agarwal, and Arti Arya. Swarm learning in autonomous driving: A privacy preserving approach. In *Proceedings of the 2023 15th International Conference on Computer Modeling and Simulation*, pages 271–277, 2023.
- [72] Xiaoge Huang, Hongbo Yin, Qianbin Chen, Yu Zeng, and Jianfeng Yao. Dag-based swarm learning: a secure asynchronous learning framework for internet of vehicles. *Digital Communications and Networks*, 2023.

- [73] Wei Xiang, Jie Li, Yuan Zhou, Peng Cheng, Jiong Jin, and Kan Yu. Digital twin empowered industrial iot based on credibility-weighted swarm learning. *IEEE Transactions on Industrial Informatics*, 2023.
- [74] Likun Wang, Zi Wang, Kevin Gumma, Alison Turner, and Svetan Ratchev. Multi-agent cooperative swarm learning for dynamic layout optimisation of reconfigurable robotic assembly cells based on digital twin. *Journal of Intelligent Manufacturing*, pages 1–24, 2024.
- [75] Jirapun Pongfai, Chrissanthi Angeli, Peng Shi, Xiaojie Su, and Wudhichai Assawinchaichote. Optimal pid controller autotuning design for mimo nonlinear systems based on the adaptive slp algorithm. *International Journal of Control, Automation and Systems*, 19:392–403, 2021.
- [76] Zhenjie Luo and Hui Zhang. Blockchain-based engine data trustworthy swarm learning management method. *Blockchain: Research and Applications*, page 100185, 2024.
- [77] Xiaoyu Jiang, Yubin Cheng, Zhihuan Song, Xiaoguang Ma, Lingjian Ye, and Zhiqiang Ge. Swarm learning for secure and effective industrial federated big data analytics. *IEEE Transactions on Reliability*, pages 1–11, 2024.
- [78] Haodong Huang, Shilong Sun, Dong Wang, and Wenfu Xu. Data privacy protection diagnostic algorithm for industrial robot joint harmonic reducers based on swarm learning. *IEEE/ASME Transactions on Mechatronics*, pages 1–10, 2025.
- [79] Gayathri Rangu and Shivashankar B Nair. On mobile-agent-based swarm reinforcement learning in a heterogeneous robotic network. In *Proceedings of the 2023 6th International Conference on Advances in Robotics*, pages 1–6, 2023.
- [80] Lei Xu, Yulong Chen, Yuntian Chen, Longfeng Nie, Xuetao Wei, Liang Xue, and Dongxiao Zhang. Swarm learning for temporal and spatial series data in energy systems: A decentralized collaborative learning design based on blockchain. *Applied Energy*, 381:125053, 2025.
- [81] Rongxu Xu, Wenquan Jin, Anam Nawaz Khan, Sunhwan Lim, and Do-Hyeun Kim. Cooperative swarm learning for distributed cyclic edge intelligent computing. *Internet of Things*, 22:100783, 2023.
- [82] Yibing Liu, Xiongtao Zhang, Lijun Huo, Jun Wu, and Mohsen Guizani. Swarm learning and knowledge distillation empowered self-driving detection against threat behavior for intelligent iot. *IEEE Transactions on Mobile Computing*, 2023.
- [83] Lei Zhang, Lei Feng, Yue Liu, Fanqin Zhou, Boyu Liu, Zheng Jia, Yanru Wang, Hui Liu, and Wenjie Ma. Improved swarm learning with differential privacy for radio frequency fingerprinting. In *2023 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, pages 1–5. IEEE, 2023.
- [84] Xishuang Dong, Shouvon Sarker, and Lijun Qian. Integrating human-in-the-loop into swarm learning for decentralized fake news detection. In *2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA)*, pages 46–53. IEEE, 2022.
- [85] Qianqian Pan, Jun Wu, Xinping Guan, and M Jamal Deen. Swarm learning irs in 6g-metaverse: Secure configurable resources trading for reliable xr communications. In *GLOBECOM 2023-2023 IEEE Global Communications Conference*, pages 74–79. IEEE, 2023.
- [86] Rongxuan Song, Jun Wu, Qianqian Pan, Muhammad Imran, Niddal Naser, Rebet Jones, and Christos Verikoukis. Zero-trust empowered decentralized security defense against poisoning attacks in sl-iot: Joint distance-accuracy detection approach. In *GLOBECOM 2023-2023 IEEE Global Communications Conference*, pages 2766–2771. IEEE, 2023.
- [87] Anurag Gupta and Brian Sadler. Eclipse attack detection on a blockchain network as a non-parametric change detection problem. *arXiv preprint arXiv:2404.00538*, 2024.
- [88] Bosen Rao, Jiale Zhang, Di Wu, Chengcheng Zhu, Xiaobing Sun, and Bing Chen. Privacy inference attack and defense in centralized and federated learning: A comprehensive survey. *IEEE Transactions on Artificial Intelligence*, 2024.
- [89] Hao Fang, Yixiang Qiu, Hongyao Yu, Wenbo Yu, Jiawei Kong, Baoli Chong, Bin Chen, Xuan Wang, and Shu-Tao Xia. Privacy leakage on dnns: A survey of model inversion attacks and defenses. *arXiv preprint arXiv:2402.04013*, 2024.
- [90] Siyuan Liu, Zhiqiang Liu, Zhiwei Xu, Wenjing Liu, and Jie Tian. Hierarchical decentralized federated learning framework with adaptive clustering: Bloom-filter-based companions choice for learning non-iid data in iov. *Electronics*, 12(18):3811, 2023.
- [91] Mohammad Tajabadi and Dominik Heider. Fair swarm learning: Improving incentives for collaboration by a fair reward mechanism. *Knowledge-Based Systems*, 304:112451, 2024.

-
- [92] Hussain Ahmad Madni, Rao Muhammad Umer, and Gian Luca Foresti. Swarm-fhe: Fully homomorphic encryption-based swarm learning for malicious clients. *International journal of neural systems*, page 2350033, 2023.
 - [93] Mengxue Shang, Dandan Zhang, and Fengyin Li. Decentralized distributed federated learning based on multi-key homomorphic encryption. In *2023 International Conference on Data Security and Privacy Protection (DSPP)*, pages 260–265. IEEE, 2023.
 - [94] Kang Haiyan and Wang Jiakang. Swarm mutual learning. *Complex & Intelligent Systems*, 10(6):8063–8077, 2024.