Recommender Systems Using Federated Learning for Privacy Preservation: A Survey

www.surveyx.cn

Abstract

This survey paper explores the intersection of recommender systems and federated learning, focusing on enhancing privacy preservation while maintaining personalized recommendations. Traditional recommender systems, reliant on centralized data aggregation, pose significant privacy risks, especially under regulatory frameworks like GDPR. Federated Learning (FL) emerges as a promising solution, enabling decentralized model training on user devices, thus safeguarding data privacy by transmitting only model updates. Despite its advantages, FL faces challenges such as data heterogeneity, communication overhead, and vulnerabilities to attacks like model poisoning. The survey examines various privacy preservation techniques, including differential privacy, secure multi-party computation, and local differential privacy, highlighting their roles in mitigating privacy risks while ensuring model efficacy. Innovative frameworks such as FedMMF and FedDefender demonstrate significant advancements in privacy-preserving methodologies, enhancing model performance and security. The paper also addresses the challenges of scalability and resource constraints in FL, proposing solutions like adaptive federated dropout and blockchain-based aggregation to optimize efficiency. Future research opportunities include improving client-side defenses, optimizing privacy-utility trade-offs, and exploring novel generative models for better data representation. The survey concludes that federated learning holds transformative potential in privacy-preserving recommender systems, offering a secure, efficient alternative to centralized approaches, and paving the way for future advancements in distributed machine learning.

1 Introduction

1.1 Overview of Recommender Systems

Recommender systems are essential for delivering personalized content or product suggestions, significantly enhancing user experience and engagement across various platforms. By analyzing user preferences and behaviors, these systems effectively manage the vast amount of online information, addressing the issue of information overload through tailored recommendation lists that promote user satisfaction and encourage ongoing interaction [1]. They are widely employed in sectors such as e-commerce for product suggestions, entertainment for content recommendations, and location-based services for identifying points of interest, thereby personalizing content discovery while navigating challenges like data privacy and system scalability [2, 3, 4]. In e-commerce, systems recommend products based on past purchases and browsing history, while streaming services suggest movies or music aligned with individual tastes. Their applications extend to healthcare data analysis and mobile keyboard predictions, with increasing integration into edge devices to enhance privacy.

Conversational recommender systems have emerged as effective solutions for eliciting user preferences, further improving personalization [5]. However, challenges such as statistical heterogeneity and non-IID data distribution continue to impact global model performance tailored for individual

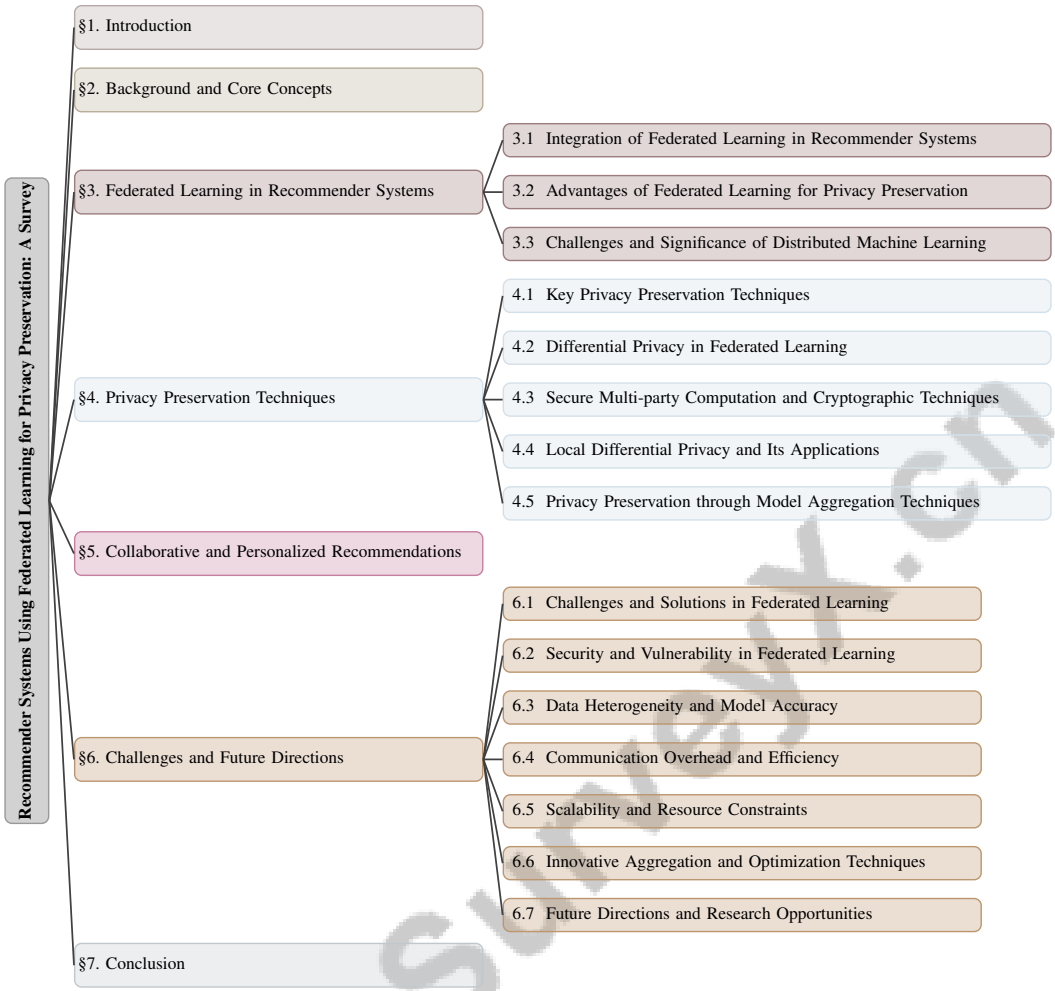


Figure 1: chapter structure

clients [6]. Addressing these challenges is crucial for advancing the effectiveness and privacy of recommender systems.

1.2 Privacy Concerns in Recommender Systems

Traditional recommender systems primarily rely on centralized architectures that aggregate extensive volumes of user data to provide personalized recommendations. This centralization poses significant privacy risks, increasing the potential for unauthorized access and misuse of sensitive user information. The vulnerability to inference attacks is particularly concerning, as adversaries can extract sensitive data even within decentralized federated learning frameworks [7].

The regulatory landscape, exemplified by frameworks like the General Data Protection Regulation (GDPR), highlights the legal and ethical implications of these privacy risks, imposing stringent data handling requirements that complicate centralized system management [8]. In response, federated learning has emerged as a viable alternative, facilitating collaborative model training without exchanging raw user data, thus enhancing privacy preservation [9]. Nonetheless, the transmission of model updates in federated learning can still lead to privacy leakage, as gradients may inadvertently reveal original user ratings [9].

Federated learning systems are also susceptible to model poisoning attacks, where malicious clients send corrupted updates to the central server, jeopardizing the global model's performance and integrity [10]. The challenge of data heterogeneity, stemming from the diverse environments and preferences in clients' datasets, leads to biased local models, complicating the creation of a well-generalized aggregated model.

To address these privacy challenges, innovative techniques such as differential privacy, secure multi-party computation, and local differential privacy are being explored within federated learning systems. These methodologies aim to balance personalization and privacy, ensuring that recommender systems can provide tailored suggestions while safeguarding user confidentiality. Enhancing the robustness and efficiency of privacy-preserving techniques in federated learning requires tackling communication inefficiencies that hinder convergence speed and overall performance. By implementing methods like adaptive mutual knowledge distillation and dynamic gradient compression, as well as exploring communication-reduction techniques such as model compression and partial device participation, communication burdens can be significantly reduced—by up to 94.89

1.3 Introduction to Federated Learning

Federated Learning (FL) represents a pivotal paradigm in machine learning, offering a robust framework for privacy preservation by decentralizing the model training process. Unlike traditional centralized models that require data aggregation on a single server, FL enables training directly on user devices, ensuring that only model updates are communicated to a central server [11]. This approach significantly mitigates privacy risks and reduces data transmission overhead, making it particularly advantageous in sectors with stringent privacy mandates, such as healthcare and finance [8].

In FL, multiple clients collaboratively contribute to a global model without sharing raw data, maintaining user information confidentiality while striving to uphold the quality of recommendations [11]. Each client computes model updates locally, which are aggregated at the central server to refine the global model. This decentralized training mechanism not only addresses privacy concerns prevalent in traditional recommender systems but also enhances data security by keeping sensitive information localized on user devices [8].

Despite its privacy-preserving advantages, FL faces challenges such as membership inference attacks, where adversaries might infer the presence of specific data points within the training set. To counteract such vulnerabilities, FL systems often integrate advanced cryptographic techniques and obfuscation strategies, albeit potentially increasing computational demands or reducing model accuracy [8].

Innovative approaches, such as combining FL with blockchain technology, have been proposed to further enhance privacy and data security. Blockchain provides a secure and immutable ledger for model updates, significantly improving transparency and accountability within federated learning ecosystems. By enabling decentralized data sharing without transferring sensitive information to centralized servers, blockchain fosters a privacy-preserving environment where multiple clients can collaboratively train machine learning models. This architecture mitigates risks associated with data privacy and security, such as cyberattacks and data leakage, while allowing for the integration of techniques like smart contracts and differential privacy, ensuring fairness and integrity across diverse stakeholders in the network [12, 13, 14, 15, 16]. These advancements underscore FL's potential not only to safeguard privacy but also to build trust and foster collaboration in distributed machine learning environments.

1.4 Objectives and Structure of the Survey

This survey explores the intersection of recommender systems and federated learning, focusing on enhancing privacy preservation while maintaining the efficacy of personalized recommendations. A key objective is to elucidate how federated learning can empower users by enabling control over their private data, thereby addressing the challenges of traditional centralized recommender systems [17]. Through an in-depth analysis of existing literature and methodologies, this survey aims to highlight federated learning's potential in overcoming privacy concerns and enhancing user trust.

The survey is structured to comprehensively cover fundamental aspects and advancements in the field. It begins by introducing recommender systems, emphasizing privacy's importance and federated learning's role in safeguarding user data. It provides a thorough exploration of collaborative recommendation and distributed machine learning, including definitions and contextual significance of key terms relevant to federated learning and privacy-preserving techniques in recommendation systems. By examining the interplay between user preferences, data privacy, and the challenges posed by heterogeneous data sources, the survey underscores the importance of these concepts in enhancing recommendation accuracy and user experience in location-based social networks [2, 18, 19, 20].

Subsequent sections focus on integrating federated learning in recommender systems, discussing its advantages and the challenges it addresses. The survey also examines various privacy preservation techniques, including differential privacy and secure multi-party computation, and their application in federated learning environments. Furthermore, the role of collaborative and personalized recommendations is analyzed, highlighting how these systems leverage local data for tailored suggestions while maintaining privacy.

Finally, the survey addresses challenges and future directions in federated learning for recommender systems, proposing potential solutions and identifying research opportunities. The concluding section summarizes key findings, reiterating the significance of federated learning in enhancing privacy preservation in recommender systems and underscoring the potential for future advancements in this field.The following sections are organized as shown in Figure 1.

2 Background and Core Concepts

2.1 Definitions of Recommender Systems and Privacy Concerns

Recommender systems are advanced computational tools designed to enhance user satisfaction by providing personalized suggestions based on user interactions and preferences across platforms like e-commerce, streaming services, and social media [21]. These systems leverage user data to predict preferences and offer tailored recommendations, but their centralized architecture raises significant privacy concerns due to the aggregation of extensive user data, which increases risks of unauthorized access and data breaches [22].

Federated learning addresses these privacy challenges by enabling decentralized model training without sharing raw data, thus enhancing privacy [23, 7]. However, federated learning systems are not immune to privacy risks; model updates can inadvertently expose sensitive information, and privacy inference attacks may exploit local user data preferences, leading to privacy violations in sensitive applications [9].

The non-IID nature of data across clients in federated learning complicates privacy preservation, often resulting in a trade-off between model accuracy and privacy. Existing methods struggle to balance these aspects, with some sacrificing accuracy or incurring additional computational and communication costs [8]. Innovative approaches, such as the FedGC framework, enhance model performance while preserving privacy by allowing clients to generate diverse data using a publicly available generative model [24]. Advanced privacy-preserving techniques, such as Differential Privacy, are crucial to maintaining user data confidentiality while ensuring effective recommendations in federated learning environments [25].

As federated learning in recommender systems evolves, addressing privacy concerns is vital for protecting user data and ensuring the integrity of personalized recommendations. Developing robust privacy-preserving techniques that incentivize client participation and enhance the overall effectiveness of federated recommender systems remains a pivotal area of research [26].

2.2 Federated Learning: A Paradigm for Privacy Preservation

Federated Learning (FL) is a transformative approach in distributed machine learning, offering a robust framework for privacy preservation through decentralized training and data locality on user devices [27]. Unlike traditional centralized models that aggregate sensitive data on a central server, FL transmits only model updates, significantly reducing privacy risks associated with data breaches [11]. This framework complies with regulatory standards like the General Data Protection Regulation (GDPR), ensuring adherence to stringent data protection mandates.

FL's core strength lies in its use of cryptographic techniques and privacy-preserving algorithms, such as secure multi-party computation and differential privacy, to protect user data during training and aggregation. Despite its potential to enhance privacy through decentralized training on edge devices, FL faces challenges that undermine its effectiveness, including vulnerabilities related to model parameter sharing, which can expose sensitive user data, and the communication overhead associated with existing FL approaches. Studies show that attackers may exploit model gradients to reconstruct private information, raising security concerns [28, 29, 30].

Techniques such as knowledge distillation, exemplified by FedKD, address these issues by facilitating efficient communication between clients through updates from a smaller mentee model while leveraging larger mentor models for improved learning. FL's adaptability to environments with unbalanced and non-IID data underscores its significance as a privacy-preserving approach in distributed systems [11]. The integration of advanced privacy-preserving techniques and innovative frameworks positions FL as a critical paradigm for achieving privacy in distributed systems. While challenges such as utility loss and efficiency reduction persist, ongoing research continues to refine FL methodologies to balance the dual imperatives of data privacy and model efficacy.

3 Federated Learning in Recommender Systems

The convergence of federated learning (FL) and recommender systems is increasingly significant due to its potential to address privacy issues while delivering personalized user experiences. This section delves into the methodologies and frameworks that support FL integration in recommender systems, highlighting their impact on user privacy and system efficiency. Figure 2 illustrates the hierarchical structure of federated learning in recommender systems, emphasizing the integration techniques, as well as the privacy and efficiency advantages. Additionally, it outlines the challenges and significance of distributed machine learning within this context, providing a visual representation that complements the discussion of these critical components.

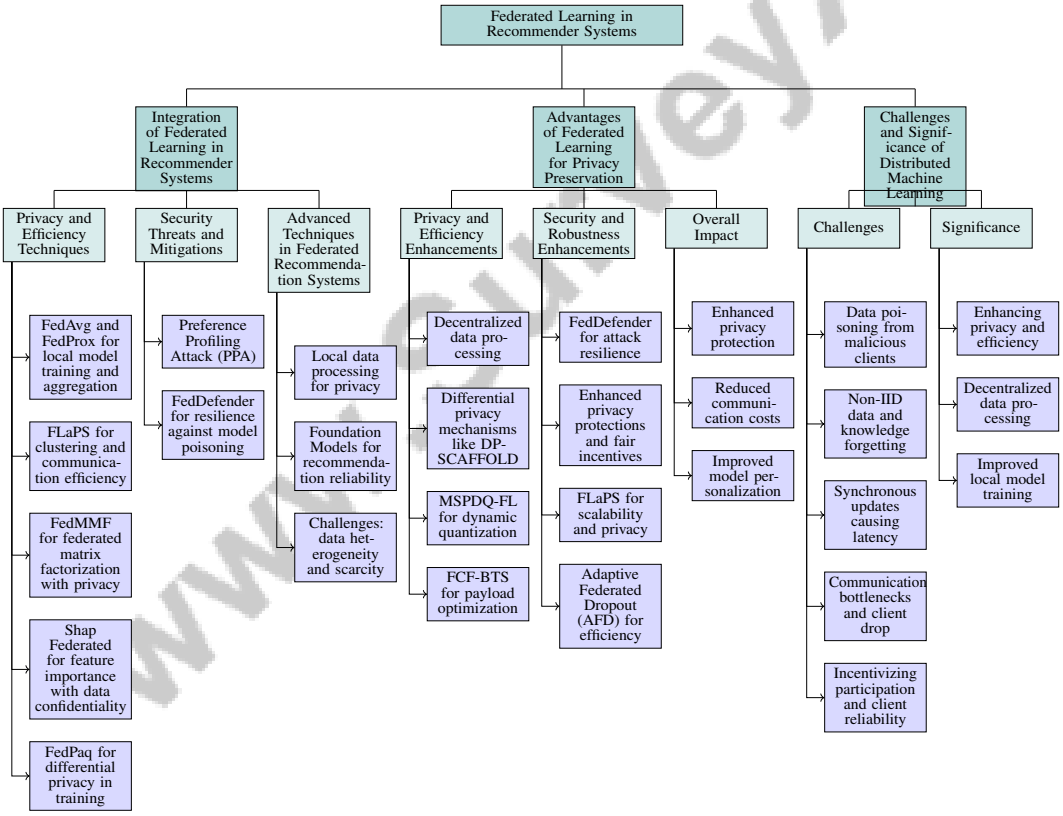


Figure 2: This figure illustrates the hierarchical structure of federated learning in recommender systems, highlighting the integration techniques, privacy and efficiency advantages, and the challenges and significance of distributed machine learning within this context.

3.1 Integration of Federated Learning in Recommender Systems

Federated learning enhances privacy in recommender systems by enabling decentralized model training, where data remains on local devices, transmitting only model updates to a central server, thus mitigating risks associated with centralized data aggregation [31, 11]. Techniques like FedAvg and

FedProx exemplify this approach, facilitating local model training and aggregation while safeguarding sensitive data.

Advanced methodologies further bolster privacy and efficiency in federated recommender systems. The Federated Learning and Privately Scaling (FLaPS) method uses clustering to enhance privacy and communication efficiency [32]. The FedMMF framework applies personalized masks from local data for federated matrix factorization, utilizing masked ratings to preserve user privacy [9]. To counter privacy inference challenges, the Shap Federated method employs Shapley values for feature importance insights while maintaining data confidentiality [8]. The FedPaq algorithm improves convergence rates through differential privacy, ensuring data protection during training [33].

Despite these advancements, federated learning encounters security threats like the Preference Profiling Attack (PPA), exploiting gradient sensitivity to infer user preferences, posing privacy risks [7]. Robust frameworks such as FedDefender enhance resilience against model poisoning attacks through attack-tolerant meta updates and global knowledge distillation [10].

As illustrated in Figure 3, Federated Recommendation Systems (FRS) utilize advanced techniques to improve user privacy by processing data locally on client devices, addressing challenges like data heterogeneity and scarcity. This figure highlights key aspects such as privacy enhancement, advanced methodologies, and security threats, categorizing the main approaches and challenges faced in implementing federated learning to improve privacy and efficiency while addressing potential security risks. This approach not only preserves sensitive information but also leverages state-of-the-art models, such as Foundation Models, to enhance recommendation reliability and efficiency, marking it as a promising area for future research in personalized content delivery [22, 4, 17, 34]. By leveraging local data processing and advanced privacy-preserving methodologies, federated learning has the potential to transform privacy-preserving recommender systems.

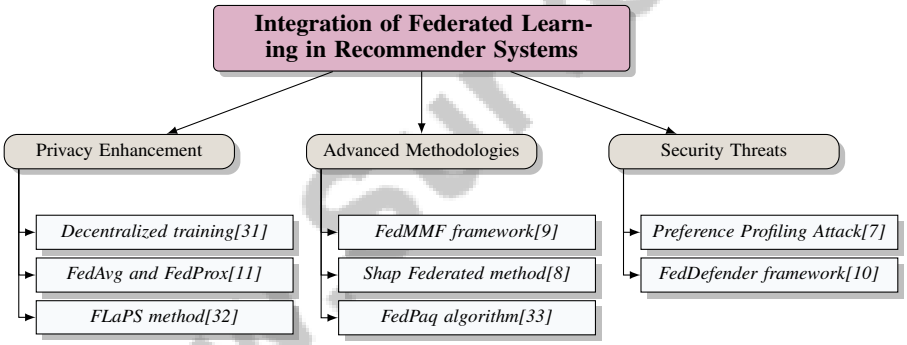


Figure 3: This figure illustrates the integration of federated learning in recommender systems, highlighting key aspects such as privacy enhancement, advanced methodologies, and security threats. It categorizes the main approaches and challenges faced in implementing federated learning to improve privacy and efficiency while addressing potential security risks.

3.2 Advantages of Federated Learning for Privacy Preservation

Federated learning offers a revolutionary approach to privacy preservation in recommender systems by decentralizing data processing, ensuring sensitive information remains on user devices. This framework significantly reduces risks associated with centralized data storage, enabling collaborative AI model development without compromising user privacy [21]. Local data processing enhances privacy, reduces latency, and facilitates efficient model updates without transferring raw data.

Integrating differential privacy mechanisms within FL frameworks, such as DP-SCAFFOLD, ensures individual data confidentiality while maintaining model accuracy [35]. This balance between accuracy, privacy guarantees, and low device overhead makes FL a robust choice for privacy-sensitive applications. Group-level knowledge sharing in federated learning significantly enhances performance compared to traditional methods, improving both privacy and efficiency [24].

FL improves model performance and communication efficiency. The MSPDQ-FL framework achieves enhanced privacy preservation without sacrificing accuracy, reducing communication costs through

dynamic quantization [36]. Similarly, the FCF-BTS method achieves a 90% reduction in model payload with minimal impact on recommendation performance [37].

Security and robustness are further enhanced by frameworks like FedDefender, which reduce computational overhead and improve resilience against various attacks [10]. Rückel et al.'s approach introduces enhanced privacy protections, verifiable model updates, and fair incentive mechanisms for client participation, strengthening privacy-preserving capabilities of FL systems [12].

Innovative methodologies like FLaPS offer significant advantages in scalability and privacy protection, allowing faster training and reduced communication costs compared to traditional federated learning [32]. The Adaptive Federated Dropout (AFD) method optimizes communication and computational efficiency by enabling clients to dynamically select and train on sub-models based on a score map of the model's activations [27].

The advantages of federated learning in privacy preservation are multifaceted, encompassing enhanced privacy protection, reduced communication costs, and improved model personalization. By leveraging these benefits, federated learning has the potential to revolutionize privacy-preserving recommender systems, ensuring robust feature importance results for host features while maintaining the privacy of guest features [8].

3.3 Challenges and Significance of Distributed Machine Learning

Distributed machine learning within the federated learning framework presents a complex landscape of challenges and opportunities. A primary challenge is the risk of data poisoning from malicious clients, which can severely compromise model integrity through corrupted updates [38]. This issue is compounded by difficulties in ensuring convergence under privacy protection measures and the complexities introduced by scaling up the system, which can lead to inefficiencies and increased vulnerability.

Data heterogeneity across clients complicates federated learning, as non-IID data distributions can significantly degrade the global model's performance [39]. This heterogeneity can lead to knowledge forgetting in the global model, causing instability and inconsistency in its performance. Additionally, synchronous updates in the cloud exacerbate latency issues due to varying computational capabilities of edge devices, impacting overall system efficiency [1].

Communication bottlenecks represent another significant challenge, particularly in environments with numerous clients and limited network bandwidth, increasing stragglers and client drop probabilities, thereby degrading user experience [27]. The trade-off between reducing communication overhead through techniques like model compression and maintaining low training variance is further complicated by data heterogeneity among devices [33].

Incentivizing participation and ensuring client reliability are critical issues, as a lack of incentives can deter participation, and random client selection may inadvertently include malfunctioning or malicious participants [16]. The absence of reliable metrics to evaluate client trustworthiness exacerbates this problem, potentially allowing unreliable or malicious participants into the training process [40].

Despite these challenges, the significance of distributed machine learning in federated learning lies in its potential to enhance privacy and efficiency through decentralized data processing. Innovative approaches that enable clients with scarce labeled data to access knowledge from those with more comprehensive datasets can facilitate improved local model training [41]. Addressing the challenges of security, communication, and data heterogeneity is crucial to realizing the full potential of distributed machine learning and ensuring the robustness and reliability of federated learning systems.

4 Privacy Preservation Techniques

The increasing emphasis on privacy in machine learning necessitates effective strategies to protect user data while supporting collaborative model training. Table 5 offers a comprehensive comparison of key privacy preservation methods utilized in federated learning, elucidating their respective strategies and efficiencies in enhancing data security and user privacy. Additionally, Table 1 presents a detailed summary of privacy preservation methods in federated learning, showcasing the diverse strategies employed to enhance data security and user privacy across different frameworks and applications.

Category	Feature	Method
Key Privacy Preservation Techniques	Data Noise Addition Security Enhancement User-Specific Protections	ULMIA[42], PDC-FRS[43] AFD[27] FedMMF[9]
Differential Privacy in Federated Learning	Privacy Enhancement	FLaPS[32], FL[11]
Secure Multi-party Computation and Cryptographic Techniques	Privacy and Security Measures	AIMPA[44], DPSMPC-FL[45], SeSoRec[46], FLUD[47]
Local Differential Privacy and Its Applications	Privacy Enhancement Quantization Techniques	PPSGD[48], LDP-Fed[49], LDP-Fed[50] MSPDQ-FL[36]
Privacy Preservation through Model Aggregation Techniques	Advanced Aggregation Strategies Gradient and Payload Optimization Hierarchical and Efficient Frameworks	pFedES[51], rCL4FedRec[52] FCF[34], FCF-BTS[37] pFedNet[53], HAF-Edge[54]

Table 1: This table provides a comprehensive overview of various privacy preservation techniques employed in federated learning. It categorizes these methods into key areas such as privacy preservation techniques, differential privacy, secure multi-party computation, local differential privacy, and model aggregation techniques. The table also lists specific features and methods associated with each category, highlighting the diverse approaches to maintaining data confidentiality and security in collaborative machine learning environments.

This section delves into key privacy preservation techniques in federated learning, highlighting their significance in maintaining user trust and enhancing model performance.

4.1 Key Privacy Preservation Techniques

Method Name	Privacy Techniques	Data Confidentiality	Model Aggregation
MSPDQ-FL[36]	Local Differential Privacy	Privacy Enhancement Techniques	Model Splitting
FedMMF[9]	Cryptographic Techniques	Privacy Leakage	Secure Aggregation Protocol
AFD[27]	-	-	Server Aggregates Updates
PDC-FRS[43]	Differential Privacy	Local Differential Privacy	Parameter Aggregation Methods
ULMIA[42]	Popularity Randomization	Membership Inference Attacks	Secure Multi-party Computation

Table 2: This table presents a comparative analysis of various privacy-preserving methods employed in federated learning frameworks. It highlights the specific privacy techniques, data confidentiality measures, and model aggregation strategies utilized by each method, providing insights into their effectiveness in enhancing privacy and maintaining data security.

In federated learning, ensuring privacy is crucial for user trust and model effectiveness. Differential privacy (DP) is a fundamental approach, introducing random noise to data or model updates to protect individual data points from inference attacks [55]. Advanced frameworks like MSPDQ-FL enhance privacy and communication efficiency through model splitting and adaptive quantization, effectively managing privacy-utility trade-offs [36].

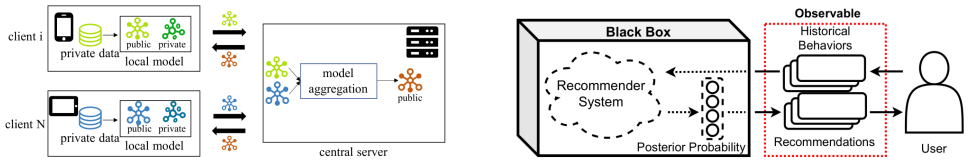
Cryptographic methods, especially secure multi-party computation (SMPC), are vital for collaborative model training without compromising data confidentiality. The FedMMF framework exemplifies this by using locally generated personalized masks to safeguard private data while maintaining model effectiveness [9]. Such integration of cryptographic techniques within federated learning strengthens privacy.

Blockchain technology decentralizes data storage, reducing leakage risks and incentivizing device participation in federated learning [25]. Techniques like LightFR generate binary codes for users and items, ensuring confidentiality while enabling accurate recommendations.

Anomaly detection enhances privacy and security by identifying malicious updates, improving model convergence. Combining this with decentralized reputation management via consortium blockchain creates a robust framework for reliable federated learning [27].

The integration of differential privacy, SMPC, blockchain, and anomaly detection effectively addresses data confidentiality challenges in federated learning, leveraging decentralized client devices for local processing of sensitive information. The ongoing evolution of these privacy-preserving techniques is crucial for robust privacy protection in federated learning systems [45, 56]. Table 2 provides a comprehensive overview of key privacy preservation techniques in federated learning, detailing the methods and their respective approaches to safeguarding data privacy and secure model aggregation.

As illustrated in Figure 4, key methodologies for safeguarding privacy in machine learning and user interaction systems are highlighted. "Client-Side Model Aggregation for Privacy-Preserving Machine



(a) Client-Side Model Aggregation for Privacy-Preserving Machine Learning[43]

(b) Recommender System and User Interaction[42]

Figure 4: Examples of Key Privacy Preservation Techniques

Learning" ensures privacy by allowing only public model aggregation while "Recommender System and User Interaction" relies on inferred probabilities from historical behaviors, treating the system as a black box. These examples illustrate the balance of data utility with stringent privacy requirements [43, 42].

4.2 Differential Privacy in Federated Learning

Differential privacy (DP) is pivotal in federated learning (FL), providing strong privacy guarantees while enabling collaborative model training across decentralized datasets. It ensures that the inclusion or exclusion of a single data point minimally impacts model output, safeguarding individual privacy [11]. Integrating DP into federated learning frameworks is crucial for balancing privacy, communication efficiency, and training variance [33].

A notable advancement is the use of DP in federated generative adversarial networks (GANs), which enhances privacy and robustness across diverse applications [57]. This integration allows for the generation of synthetic data that retains the statistical properties of the original dataset without compromising individual data points.

The FLaPS architecture demonstrates effective use of differential privacy, achieving efficient model training while maintaining stringent privacy standards through device clustering and differentially private communication [32]. Despite challenges like potential decreases in model accuracy due to noise addition, empirical studies suggest that differential privacy can enhance privacy without significantly compromising model accuracy, preserving the efficacy of federated learning systems [11].

Differential privacy remains a cornerstone of privacy-preserving federated learning, offering robust protection for individual data points while enabling effective model training. Continuous research and refinement of DP techniques are essential for balancing privacy and utility in distributed learning environments, addressing adversarial threats that may exploit vulnerabilities in machine learning systems [55, 29, 56, 58].

4.3 Secure Multi-party Computation and Cryptographic Techniques

Method Name	Privacy Preservation	Scalability and Efficiency	Collaborative Computation
SeSoRec[46]	Secret Sharing Protocol	Linear Complexity Method	Secure Matrix Multiplication
FLUD[47]	Privacy-preserving Voting	Optimized Smpc Protocols	Secure Multi-Party Computation
AIMPA[44]	Community-driven Privacy	-	Collaborative Strategies
DPSMPC-FL[45]	Differential Privacy	Local Model Training	Secure Multi-party Computation

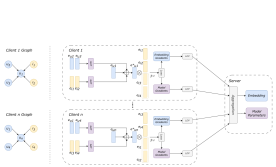
Table 3: Comparison of privacy-preserving methods in federated learning frameworks, focusing on the aspects of privacy preservation, scalability and efficiency, and collaborative computation. The table highlights different approaches, including secret sharing, differentially private computation, and community-driven privacy, illustrating their roles in enhancing secure multi-party computation.

Secure multi-party computation (SMPC) and cryptographic techniques are critical for data privacy in federated learning frameworks. These methods enable collaborative computations over inputs while ensuring no party learns beyond the output. SMPC facilitates privacy-preserving model training by allowing clients to compute joint functions without revealing individual data [46].

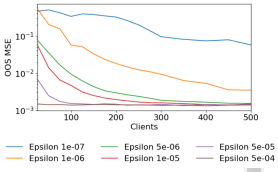
Integrating SMPC with social recommendation models illustrates enhanced recommendation performance while maintaining data confidentiality. Secure computation protocols protect sensitive information, enabling accurate and private recommendations [46]. A comprehensive survey highlights the effectiveness of SMPC alongside other techniques such as perturbation and aggregation, collectively fortifying federated systems' privacy architecture [38].

Applying SMPC protocols within frameworks like FLUD optimizes efficiency and scalability, essential for privacy preservation in large-scale deployments [47]. By minimizing computational overhead and enhancing scalability, these protocols facilitate seamless integration of privacy-preserving mechanisms in federated learning environments.

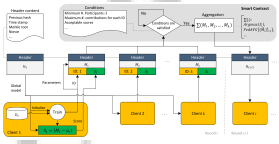
SMPC and cryptographic techniques are integral to safeguarding data privacy in federated learning, facilitating secure computations and improving scalability. Advanced methodologies enable personalized recommendations while protecting user privacy. Techniques like personalized masks from local data safeguard sensitive information without compromising accuracy. Collaborative model training allows organizations to utilize large datasets for personal information extraction without sharing raw data, enhancing privacy and efficiency [9, 29]. Continuous refinement of SMPC and cryptographic approaches is essential for maintaining the integrity and confidentiality of decentralized learning processes.



(a) Graph-based Federated Learning with Graph Attention Networks (GATs)[44]



(b) The image shows the convergence of the OOS MSE (Out-of-Sample MSE) for different values of epsilon () across different numbers of clients (n).[45]



(c) A diagram illustrating a distributed training process for a machine learning model[59]

Figure 5: Examples of Secure Multi-party Computation and Cryptographic Techniques

As demonstrated in Figure 5, secure multi-party computation and cryptographic methods are pivotal in ensuring data confidentiality and integrity during collaborative computations. The first example showcases a federated learning framework utilizing Graph Attention Networks (GATs), where clients with their own graph data collaborate with a server to aggregate model parameters and embedding gradients. This exemplifies how secure multi-party computation enables decentralized learning without compromising individual client data. The second example highlights the convergence of Out-of-Sample Mean Squared Error (OOS MSE) across varying client numbers and privacy parameters (epsilon), demonstrating the integration of differential privacy into secure computations to balance privacy and model performance. Lastly, the distributed training process diagram underscores the collaborative learning paradigm, where multiple clients contribute to training a global model, emphasizing the role of cryptographic techniques in ensuring data security throughout the training process. These examples collectively underscore the importance of advanced privacy preservation techniques in modern data-driven applications [44, 45, 59]. Additionally, Table 3 provides a comparative analysis of various methods employed in federated learning frameworks to ensure privacy preservation, scalability, and collaborative computation.

4.4 Local Differential Privacy and Its Applications

Local Differential Privacy (LDP) enhances user privacy by obfuscating individual data points before they leave the user's device, providing strong privacy guarantees even against potentially untrusted servers [55]. In federated learning environments, LDP allows data to remain on local devices while contributing to global model training by adding noise to the data or its gradients before transmission, ensuring sensitive information is not exposed during aggregation [36].

LDP is particularly relevant in scenarios involving highly sensitive user data, such as healthcare and financial services. By employing LDP, federated learning systems can maintain high privacy levels

while leveraging valuable insights from distributed data sources [33]. This approach fosters user trust and encourages broader participation in federated learning networks.

A key challenge in implementing LDP is balancing privacy and model accuracy. The introduction of noise can degrade model quality, necessitating sophisticated algorithms to optimize this balance. Techniques such as adaptive noise addition and privacy budget allocation have been proposed to address these issues, ensuring robust performance while adhering to stringent privacy standards [55].

Additionally, LDP is instrumental in enabling privacy-preserving federated learning in edge computing environments, where computational resources are limited, and data privacy is paramount. By decentralizing data processing and employing local perturbation techniques, federated learning systems can efficiently utilize edge devices without compromising user privacy [36]. This capability is essential for scaling federated learning applications across diverse and resource-constrained environments.

(a) Privacy Noise and Excess Risk in Stochastic Gradient Descent[48]

Privacy-Preserving Federated Learning Method	Efficient	Locally Defined Privacy Guarantee	Protection from Inference Attacks	Handles Complex Models
SMC [6]	✗	✗	–	✓
ϵ-DP Parameter Sharing [19]	✓	✓	–	✓
Local Optimizer [2]	–	✓	✓	✗
Hybrid-One [23]	✗	✗	✓	–
Continuous ϵ-LDP [26]	✓	✓	✓	✗
LDP-Fed	✓	✓	✓	✓

(b) Comparison of Privacy-Preserving Federated Learning Methods[50]

Privacy-Preserving Federated Learning Method	Efficient	Locally Defined Privacy Guarantee	Protection from Inference Attacks	Handles Complex Models
SMC [6]	✗	✗	–	✓
ϵ-DP Parameter Sharing [19]	✓	✓	–	✓
Local Optimizer [2]	–	✓	✓	✗
Hybrid-One [23]	✗	✗	✓	–
Continuous ϵ-LDP [26]	✓	✓	✓	✗
LDP-Fed	✓	✓	✓	✓

(c) Comparison of Privacy-Preserving Federated Learning Methods[49]

Figure 6: Examples of Local Differential Privacy and Its Applications

As illustrated in Figure 6, Local Differential Privacy (LDP) has emerged as a crucial technique for safeguarding individual data while enabling meaningful analysis. The first subfigure examines the impact of privacy noise on excess risk during stochastic gradient descent (SGD), a key optimization technique in machine learning. By varying privacy noise levels, the study explores how these adjustments affect performance and risk, providing insights into the trade-offs between privacy and accuracy. The subsequent subfigures present comparative analyses of various privacy-preserving federated learning methods, critical for decentralized data processing without compromising individual privacy. These comparisons encompass diverse criteria, such as efficiency, locally defined privacy guarantees, protection from inference attacks, and the ability to handle complex models. Collectively, these examples highlight LDP's versatility and applicability in enhancing privacy across different machine learning frameworks [48, 50, 49].

4.5 Privacy Preservation through Model Aggregation Techniques

Benchmark	Size	Domain	Task Format	Metric
FL-Bench[60]	60,000	Computer Vision	Image Classification	Accuracy, Time-to-Accuracy
CFL-Bench[61]	60,000	Image Classification	Classification	ARI, AMI
WikiPII[29]	77,703	Personal Information Extraction	Named Entity Recognition	F1-score
FL-Benchmark[62]	1,000,000	Image Classification	Backdoor Attack	Accuracy, F1-score
FL-GAN[63]	15,000	Finance	Classification	JSD, WD
PrivacyFL[64]	70,000	Computer Vision	Classification	Accuracy, Latency
FL-Edge[26]	60,000	Image Classification	Image Classification	Test Accuracy, Training Time
P2P-FL-DP[25]	70,000	Image Classification	Classification	Accuracy, Loss

Table 4: Summary of benchmarks used in evaluating federated learning model aggregation techniques, detailing their size, domain, task format, and performance metrics. The table provides a comprehensive overview of various datasets utilized in assessing the effectiveness of privacy-preserving strategies in federated learning frameworks.

Model aggregation techniques are vital in enhancing privacy preservation within federated learning frameworks by ensuring that only model updates, rather than raw data, are transmitted between clients and the central server. This approach significantly reduces the risk of data breaches and unauthorized access to sensitive information [34]. In federated collaborative filtering (FCF), for instance, clients send only gradients to the server, maintaining user privacy while facilitating collaborative model training [34].

Advanced aggregation methods, such as those implemented in pFedES, achieve significant improvements in test accuracy and efficiency by reducing communication and computational costs,

enhancing the scalability and practicality of federated learning systems [51]. The pFedES framework, for example, achieves a 1.61% higher test accuracy compared to the best baseline while reducing communication costs by 99.6% and computational costs by 82.9% [51].

Hierarchical aggregation frameworks, like HAF-Edge, utilize distance-based weighting to assign greater importance to models trained on more balanced data distributions, improving overall model performance while preserving privacy [54]. This method enhances aggregation efficiency and addresses challenges posed by data heterogeneity across clients [54].

Communication-efficient regularizers, such as those employed in medical federated model mixtures, further contribute to privacy preservation by minimizing data transmission overhead during model training [53]. This is complemented by payload optimization techniques like FCF-BTS, enabling efficient data handling without compromising user privacy or requiring additional computational resources on user devices [37].

Robust federated learning frameworks also incorporate mechanisms to counteract potential threats such as model poisoning attacks. The rCL4FedRec framework introduces a popularity-based regularizer to enhance the resilience of federated recommender systems, maintaining model integrity and privacy in the face of adversarial attacks [52].

Model aggregation techniques are integral to the privacy-preserving architecture of federated learning. By enhancing communication efficiency and employing advanced aggregation methods, federated learning techniques provide accurate recommendations while effectively safeguarding user privacy. These approaches address critical challenges such as data heterogeneity and security threats, ensuring that sensitive user information remains protected while enabling effective model training on decentralized data sources. Strategies like secure weighted aggregation and noise-robust training methods optimize model performance amidst varying data quality and reliability [11, 65, 66, 29].

As depicted in Figure 7, which illustrates the key aspects of privacy preservation in federated learning, model aggregation techniques are crucial for ensuring data privacy while maintaining robust model performance. The figure highlights various techniques such as FCF gradients, pFedES accuracy, and HAF-Edge weighting for model aggregation; medical regularizers and FCF-BTS payload for communication efficiency; and rCL4FedRec attacks, secure aggregation, and AnoFel anonymity for robustness and security. The first example, "TinyImageNet: Scalability and Performance of a Distributed Aggregator for Image Classification," presents a graph comparing runtime across models like TinyImageNet, CIFAR10, and MNIST as client numbers increase, highlighting the scalability and efficiency of distributed aggregators. The second example, "Cloud Provider Platform with Training Enclave and Param Server Enclave," illustrates a cloud-based system where training and parameter server enclaves are secured using trusted hardware (SGX), ensuring protection for both the service provider's code and the ML model. Lastly, the "Deep Federated Learning with Double-Perturbation" example depicts a federated learning framework where multiple clients collaboratively train a global model, preserving privacy through global and local model perturbations, allowing for secure aggregation while introducing controlled noise to protect sensitive data. Together, these examples underscore the diverse approaches and innovations in privacy preservation through model aggregation techniques [67, 58, 68]. Additionally, Table 4 presents a detailed comparison of benchmarks that are instrumental in evaluating the efficiency and privacy-preserving capabilities of model aggregation techniques in federated learning.

Feature	Differential Privacy in Federated Learning	Secure Multi-party Computation and Cryptographic Techniques	Local Differential Privacy and Its Applications
Privacy Technique	Random Noise	Secure Computation	Local Obfuscation
Data Handling	Data Remains Local	Joint Computation	Noise Addition
Efficiency	Communication Efficiency	Scalability	Edge Computing

Table 5: This table provides a comparative analysis of three prominent privacy preservation techniques in federated learning: Differential Privacy, Secure Multi-party Computation, and Local Differential Privacy. It highlights the core privacy techniques, data handling methods, and efficiency metrics associated with each approach, offering insights into their distinct mechanisms for safeguarding data privacy while maintaining model performance.

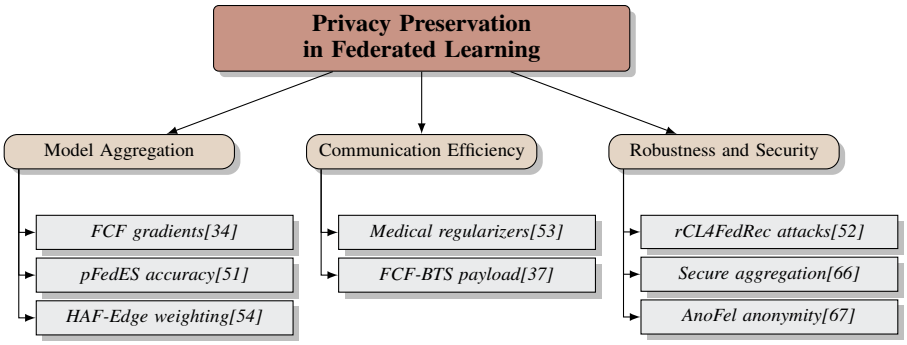


Figure 7: This figure illustrates the key aspects of privacy preservation in federated learning, focusing on model aggregation, communication efficiency, and robustness and security. It highlights various techniques such as FCF gradients, pFedES accuracy, and HAF-Edge weighting for model aggregation; medical regularizers and FCF-BTS payload for communication efficiency; and rCL4FedRec attacks, secure aggregation, and AnoFel anonymity for robustness and security.

5 Collaborative and Personalized Recommendations

5.1 Leveraging Local Data for Personalized Recommendations

Federated learning-based recommender systems enhance user experience by utilizing local data to create personalized models without centralizing sensitive information. This approach ensures confidentiality by processing data locally on user devices, mitigating risks of data breaches [69]. By leveraging user-specific interaction patterns, federated learning generates highly personalized recommendations, particularly beneficial for sensitive populations [69]. Maintaining data locality not only enhances privacy but also reduces transmission overhead, resulting in more efficient and scalable systems.

Local data utilization fosters adaptive models that respond to shifts in user preferences, crucial for delivering timely recommendations. This adaptability improves user satisfaction and engagement, highlighting federated learning's potential in privacy-preserving recommender systems. By enabling model training without raw data transmission, federated learning aligns with data privacy regulations like GDPR and mitigates data leakage risks, including attribute inference attacks. Innovations such as privacy-preserving aggregation and personalized masking further enhance recommendation effectiveness, allowing users to maintain data control while receiving high-quality, personalized suggestions [22, 9, 70, 34].

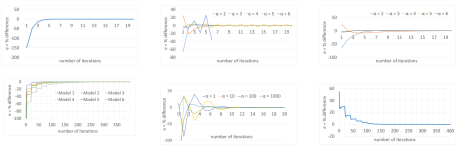
5.2 Techniques for Privacy Preservation in Personalized Recommendations

Advanced techniques ensure privacy preservation in personalized recommendation systems, protecting user data while delivering tailored content. Differential privacy introduces noise to data or model updates to prevent individual user identification, effective in federated learning environments where only perturbed model updates are shared [55, 36]. Secure multi-party computation (SMPC) enables secure computations over inputs while keeping data private, ensuring sensitive information remains undisclosed during collaborative training [46].

Local differential privacy (LDP) obfuscates data before leaving the user's device, valuable in sensitive scenarios like healthcare or finance, allowing for recommendations without exposing raw data [33]. Model aggregation techniques transmit only model updates, reducing data breach risks and maintaining user privacy [34]. Combining these methodologies provides a comprehensive framework for maintaining privacy in personalized recommendations, enhancing federated learning systems' accuracy and reliability while managing data heterogeneity and mitigating security threats [22, 4, 17].

As illustrated in Figure 8, maintaining user privacy in personalized recommendations involves overcoming complex challenges. The first image presents a mathematical equation emphasizing differential privacy's complexities in online collaborative filtering, balancing personalization with privacy. The second image compares models in an optimization process, showcasing privacy-

$$\frac{\phi(x_k) + \phi(x_\ell)}{\phi(x'_k) + \phi(x'_\ell)} = \frac{\phi(x'_k + \theta_k) + \phi(x_\ell)}{\phi(x'_k) + \phi(x'_\ell)} \leq \frac{\phi(x'_k) + \phi(x_\ell + \theta_k)}{\phi(x'_k) + \phi(x'_\ell)}.$$



(a) The image shows a mathematical equation involving the function $(\mathrm{x}_k) and (x_l), along with the variables x'_k, x'_l, and x_k + x_l$.[71]

(b) Comparison of Different Models in Optimization Process[34]

Figure 8: Examples of Techniques for Privacy Preservation in Personalized Recommendations

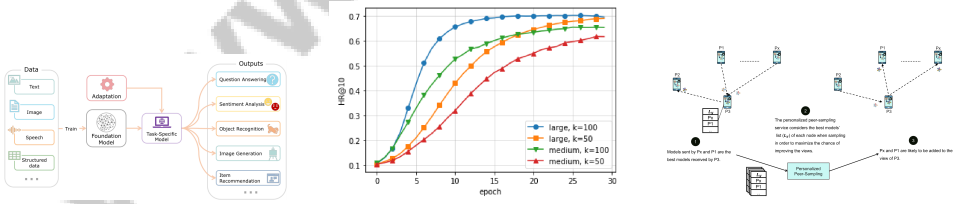
preserving techniques' efficacy in achieving optimal recommendations without compromising user data [71, 34].

5.3 Frameworks and Models Enhancing Collaborative Recommendations

Frameworks and models that enhance collaborative recommendations in privacy-preserving environments are crucial for maintaining user privacy while delivering accurate content. Federated learning integration into collaborative systems decentralizes data processing, enabling secure model training across distributed datasets and keeping sensitive user data on local devices [69].

The Federated Collaborative Filtering (FCF) model exemplifies this integration by performing collaborative filtering without centralizing user data, transmitting only model updates to preserve privacy while generating personalized recommendations [34]. The pFedES framework introduces personalized federated learning, employing model heterogeneity to tailor recommendations, improving test accuracy and efficiency [51]. Hierarchical aggregation frameworks like HAF-Edge enhance recommendations by prioritizing models trained on balanced data distributions, addressing data heterogeneity challenges [54].

Integrating advanced privacy-preserving techniques, including differential privacy and SMPC, ensures sensitive information protection during training and aggregation, safeguarding user privacy while maintaining recommendation efficacy [46]. These models present a secure and efficient alternative to traditional systems, reducing privacy risks and adhering to legal regulations while enabling collaborative systems to leverage user feedback for high performance and accuracy [29, 21, 34].



(a) Adaptive Foundation Model for Multitask Learning[4]

(b) The image shows the performance of different models on a dataset over time.[72]

(c) Personalized Peer-Sampling Service for Mobile Devices[3]

Figure 9: Examples of Frameworks and Models Enhancing Collaborative Recommendations

As depicted in Figure 9, collaborative and personalized recommendations have advanced through innovative frameworks and models. The "Adaptive Foundation Model for Multitask Learning" demonstrates a foundational model tailored for specific tasks, enhancing collaborative recommendations through multitask learning capabilities. A line graph highlights model performance over time, emphasizing continuous evaluation and optimization. The "Personalized Peer-Sampling Service for Mobile Devices" exemplifies a targeted recommendation system, personalizing sampling by considering the best models for each node, enhancing recommendation efficiency and user experience. These examples illustrate the dynamic nature of collaborative systems driven by adaptive models and personalized services [4, 72, 3].

6 Challenges and Future Directions

6.1 Challenges and Solutions in Federated Learning

Federated Learning (FL) offers a promising framework for privacy-preserving machine learning but faces significant challenges that affect its optimization. A key issue is the vulnerability of server-side defenses to sophisticated attacks, particularly in non-IID scenarios where benign and malicious updates appear indistinguishable, threatening the integrity of the global model [10]. Robust aggregation techniques are essential to withstand adversarial attacks while preserving model accuracy.

Traditional privacy-preserving methods, such as differential privacy, often degrade model performance due to the substantial noise introduced to protect gradients, creating a trade-off between privacy and utility [73]. This challenge is compounded by non-IID data complexities and federated systems' scalability, which can lead to performance degradation in practical applications [57].

Data heterogeneity is another obstacle, leading to overfitting and noisy gradients that impact learning effectiveness [31]. Device drops and insufficient privacy mechanisms further limit scalability [32]. Additionally, the computational burden on user devices, especially in resource-constrained environments, restricts the effectiveness of privacy-preserving frameworks [9].

Innovative solutions have emerged to mitigate these challenges. The Aero framework combines strong privacy guarantees with low device overhead, advancing federated learning systems [11]. Adaptive federated dropout (AFD) reduces communication costs and enhances model generalization by selectively training sub-models tailored to client-specific data distributions [27].

Future research should focus on optimizing the proximal term in FedProx and exploring alternative privacy-preserving techniques to accommodate varying device capabilities [11]. Extending personalized masks to other federated learning tasks and integrating them with differential privacy could enhance privacy guarantees while maintaining model utility [9]. Addressing these challenges with innovative solutions will optimize federated learning systems for privacy-preserving machine learning applications.

6.2 Security and Vulnerability in Federated Learning

Federated Learning (FL) introduces unique security challenges due to its decentralized nature, exposing the system to various vulnerabilities and potential attacks. A taxonomy categorizes these threats by nature and target, with insider threats posing significant risks to the learning process's integrity and confidentiality [74]. Malicious participants within the FL network can manipulate model updates or infer sensitive information from shared gradients.

Despite FL's theoretical robustness against privacy breaches, many privacy attack methods lack robust experimental evidence in realistic FL scenarios [30]. This gap highlights the need for comprehensive evaluations of privacy attack strategies under real-world conditions.

To address these security challenges, strategies include implementing a verify-before-aggregate (VBA) procedure to filter out malicious training results, developing fragmented federated learning (FFL) protocols to enhance privacy while maintaining model accuracy, and exploring collaborative training techniques that leverage noisy annotated datasets to improve robustness against attacks [28, 38, 75, 29, 76]. Robust aggregation techniques ensure adversarial updates do not compromise the global model's integrity, while differential privacy mechanisms obfuscate individual data contributions, reducing information leakage risk.

Secure multi-party computation and cryptographic techniques can safeguard data during training, enabling secure computations without revealing individual data points. Anomaly detection techniques are crucial for enhancing FL's security and efficiency by identifying and mitigating malicious activities from participating clients. These techniques address issues such as client drift and erroneous or malicious training data submission, improving model convergence rates and reducing communication overhead [28, 77, 76].

6.3 Data Heterogeneity and Model Accuracy

Data heterogeneity poses a significant challenge in federated learning, affecting global models' accuracy and reliability. The core issue arises from the statistical heterogeneity of client data,

preventing a single global model from effectively serving all clients [78]. This heterogeneity is pronounced among different industrial participants, each with varying data distributions and quality, complicating consistent model performance [79].

Benchmark studies underscore the necessity of understanding these data distributions to optimize federated learning, especially under diverse heterogeneity scenarios [61]. Existing optimization-based methods often struggle with this fundamental issue, limiting their effectiveness in enhancing federated learning performance [24]. Furthermore, data heterogeneity can lead to forgetting knowledge from previous training rounds, complicating the learning process and degrading model accuracy [39].

Innovative solutions such as FedDiff leverage diffusion models to generate high-quality synthetic data that captures client data distributions' diversity, enhancing model performance by providing a more representative training set [80]. However, these methods may still face challenges in highly heterogeneous settings, where significant differences in data distributions can affect pseudo labels' reliability and, consequently, the model's performance [41].

Moreover, the computational overhead associated with certain federated learning processes, such as voting and staking, can adversely affect system performance in high-scale applications, posing additional challenges in managing data heterogeneity [81]. Addressing these challenges requires a concerted effort to develop sophisticated algorithms and techniques that effectively manage the diverse data landscapes inherent in federated learning environments.

6.4 Communication Overhead and Efficiency

Communication overhead is a critical concern in federated learning systems, significantly impacting the learning process's efficiency and scalability. The decentralized nature of federated learning necessitates frequent communication between clients and the central server for model updates. This communication can become a bottleneck, particularly in environments with limited network bandwidth or many participating clients [33]. The challenge is further exacerbated by increased training variance when applying differential privacy measures, which may hinder convergence speed and necessitate more communication rounds to achieve satisfactory model performance [33].

To enhance communication efficiency in federated learning, several strategies have been proposed. Model compression techniques, including quantization and sparsification, significantly decrease the size of model updates exchanged between clients and the server. This reduction alleviates communication overhead while enhancing privacy by minimizing data transmission, as demonstrated by the compressed Loopless Gradient Descent (L2GD) algorithm that integrates a bidirectional compression mechanism. Dynamic quantization methods further refine this process by adjusting the quantization interval to reduce errors, improving both communication efficiency and model accuracy in heterogeneous environments [36, 82, 83].

Adaptive communication protocols also play a vital role in optimizing communication efficiency in decentralized systems. These protocols dynamically modify the frequency and size of model updates based on real-time assessments of network conditions and individual user requirements, reducing overhead while maintaining model accuracy [3, 84]. This adaptability ensures optimal use of communication resources, minimizing unnecessary data transfer and latency.

Federated learning frameworks benefit from advanced aggregation methods that prioritize updates from clients with more informative data or higher computational capabilities. By selectively aggregating model updates, these methods enhance communication efficiency, ensuring that only the most informative updates crucial for improving the global model's performance are utilized [2, 82, 57, 19].

A comprehensive strategy to mitigate communication overhead should incorporate advanced techniques such as efficient data compression methods, adaptive communication protocols, and strategic aggregation techniques that enhance model performance while addressing data heterogeneity and privacy concerns. Recent advancements, including personalized federated learning algorithms and novel approaches like Adaptive Federated Dropout, illustrate the importance of tailoring communication strategies to reduce convergence time and improve model generalization across diverse, resource-constrained edge devices [33, 83, 85, 27]. By optimizing these aspects, federated learning systems can achieve greater scalability and efficiency, enabling them to handle larger datasets and more participants while maintaining robust privacy guarantees.

6.5 Scalability and Resource Constraints

Scalability and resource constraints are pivotal challenges in implementing federated learning systems, directly impacting their feasibility and efficiency across diverse environments. The inherent decentralization of federated learning requires coordinating numerous client devices, each with varying computational capabilities and network conditions, leading to significant scalability issues [11]. The variability in device resources complicates the maintenance of consistent performance and reliability in FL applications [27].

A primary concern is the computational burden on client devices, particularly those with limited processing power or energy resources, which restricts their ability to participate effectively in federated learning tasks [9]. This constraint necessitates developing lightweight algorithms and optimization techniques that minimize computational demands while preserving model accuracy and privacy [11].

Moreover, the scalability of federated learning systems is often hindered by communication overhead, as the need for frequent model updates between clients and the central server can lead to network congestion and increased latency [33]. Strategies such as model compression, adaptive communication protocols, and efficient aggregation methods are essential to alleviate these bottlenecks and enhance the scalability of federated learning frameworks [33].

Innovative approaches like the adaptive federated dropout (AFD) method address these challenges by allowing clients to dynamically select and train sub-models based on their resource availability, optimizing computational efficiency and reducing communication costs [27]. Additionally, integrating decentralized aggregation techniques, such as those enabled by blockchain technology, can further enhance scalability by distributing the aggregation process across multiple nodes, reducing reliance on a central server [25].

Effectively tackling scalability and resource constraints in federated learning necessitates a multifaceted strategy that integrates innovative algorithms, optimizes communication protocols, and leverages decentralized processing techniques. This approach addresses the inherent statistical and system heterogeneity of data across distributed networks while mitigating communication bottlenecks and enhancing data privacy, ultimately facilitating robust machine learning model development from decentralized edge devices while preserving user confidentiality [86, 85]. By overcoming these challenges, federated learning systems can achieve greater scalability and adaptability, enabling deployment across a wide range of applications and environments.

6.6 Innovative Aggregation and Optimization Techniques

Innovative aggregation and optimization techniques are essential for enhancing federated learning systems' performance and efficiency. These techniques address critical challenges, including communication overhead, data heterogeneity, and model convergence, vital for improving these systems' scalability and robustness. They tackle issues from varying client capabilities and data distributions, ensuring efficient resource utilization and enabling training models catering to diverse hardware constraints and data characteristics. By facilitating improved collaboration among decentralized clients while preserving data privacy, these techniques lead to more effective and reliable federated learning applications [19, 82, 85, 86].

One promising approach involves hierarchical aggregation methods, enhancing model performance by structuring the aggregation process across multiple layers or levels. This method allows for more efficient handling of diverse data distributions and reduces the communication burden by aggregating updates at intermediate levels before transmitting them to the central server [54]. Leveraging hierarchical structures enables federated learning systems to achieve better scalability and adaptability to varying network conditions and client capabilities.

Incorporating adaptive optimization algorithms that dynamically adjust learning rates and update frequencies based on client-specific data characteristics and resource availability is another innovative technique. These algorithms enhance model convergence by tailoring the optimization process to each client's unique conditions, improving federated learning's overall efficiency and effectiveness [27].

The integration of advanced model compression techniques, such as quantization and sparsification, further optimizes communication efficiency by reducing the size of model updates transmitted between

clients and the server. These techniques minimize data transfer without significantly compromising model accuracy, addressing one of the primary bottlenecks in federated learning [33].

Additionally, decentralized aggregation frameworks enabled by blockchain technology offer a novel approach to enhancing the security and transparency of the aggregation process. Distributing the aggregation task across multiple nodes reduces reliance on a central server and improves the resilience of federated learning systems against potential attacks [25].

The advancement of federated learning systems significantly relies on developing and implementing innovative aggregation and optimization techniques, as these methods address key challenges such as data privacy, communication bottlenecks, and the statistical heterogeneity of decentralized data sources. Ultimately, they enhance the performance, stability, and scalability of machine learning models trained on local data from multiple edge devices [86, 60, 85]. By addressing these challenges and enhancing the efficiency of the learning process, these techniques pave the way for more robust and scalable federated learning applications across various domains.

6.7 Future Directions and Research Opportunities

Future research in federated learning (FL) and privacy preservation is poised to tackle critical challenges and explore innovative pathways to enhance these technologies' robustness, efficiency, and applicability across various domains. A significant focus area is developing comprehensive frameworks to manage the multifaceted nature of heterogeneity in FL, including emerging trends in transfer learning and model personalization [19]. This involves optimizing the balance between privacy and accuracy, particularly in complex federated learning scenarios, by refining noise levels, aggregation strategies, and testing frameworks like MSPDQ-FL in diverse practical applications [36].

Moreover, enhancing the usability of federated learning with differential privacy is essential, necessitating the exploration of new optimization techniques and addressing the practical challenges of implementing these systems in real-world scenarios [55]. Future research should also prioritize developing sophisticated privacy budget allocation schemes and personalized federated learning frameworks that consider social interests, further optimizing privacy-preserving mechanisms [73].

Scalability remains a critical research direction, emphasizing novel generative models and the challenges posed by non-IID data distributions [57]. Personalized data generation strategies, integration of different generative models, and development of filtering techniques for low-quality generated data are promising areas for future exploration [24]. Additionally, addressing non-IID data challenges and enhancing personalization through integrating large pre-trained models in federated settings are vital avenues for future inquiry [31].

Improving client-side defense mechanisms and investigating their applicability to other attack types in federated learning is crucial for enhancing security [10]. Future work should also focus on developing lightweight encryption methods, enhancing the efficiency of federated NAS frameworks, and addressing adversarial threats to improve the robustness of federated learning systems [6].

Exploring variations in clustering, data aggregation methods, and testing frameworks on real-world mobile devices will advance the practical application of federated learning [32]. Additionally, refining methods to improve the granularity of feature importance for guest data will enhance interpretability and transparency in federated learning systems [8].

By addressing these future research directions and opportunities, the reliability, scalability, and security of federated learning technologies can be significantly enhanced, paving the way for more robust, efficient, and secure distributed learning systems. Future work will also explore the impact of dynamically selected sub-models on model fairness and investigate potential personalization of clients' sub-models [27].

7 Conclusion

Federated learning (FL) represents a pivotal shift in enhancing privacy within recommender systems by decentralizing data processing and enabling local model training. This approach significantly reduces the privacy risks linked to centralized data aggregation, providing robust privacy assurances while maintaining high-quality recommendations. The integration of differential privacy with FL

further strengthens these capabilities, although balancing privacy and practical implementation remains a challenge.

Frameworks like FedMMF illustrate the potential of safeguarding data privacy without compromising on training efficiency or model performance, showcasing FL's capacity to match the recommendation quality of traditional centralized systems. These advancements highlight FL's role in enhancing user privacy, reducing communication overhead, and enabling real-time analytics.

Despite these strides, practical implementation challenges persist, warranting further research to address these issues. Future developments are expected to optimize FL's integration with other privacy-enhancing technologies, improve scalability, and refine algorithms to better handle data heterogeneity and resource limitations.

References

[1] Ruiyuan Wu, Anna Scaglione, Hoi-To Wai, Nurullah Karakoc, Kari Hreinsson, and Wing-Kin Ma. Federated block coordinate descent scheme for learning global and personalized models, 2021.

[2] Yeting Guo, Fang Liu, Zhiping Cai, Hui Zeng, Li Chen, Tongqing Zhou, and Nong Xiao. Prefer: Point-of-interest recommendation with efficiency and privacy-preservation via federated edge learning. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 5(1):1–25, 2021.

[3] Yacine Belal, Aurélien Bellet, Sonia Ben Mokhtar, and Vlad Nitu. Pepper: Empowering user-centric recommender systems over gossip learning, 2022.

[4] Zhiwei Li, Guodong Long, Chunxu Zhang, Honglei Zhang, Jing Jiang, and Chengqi Zhang. Navigating the future of federated recommendation systems with foundation models. *arXiv preprint arXiv:2406.00004*, 2024.

[5] Zhuohua Li, Maoli Liu, and John C. S. Lui. Fedconpe: Efficient federated conversational bandits with heterogeneous clients, 2024.

[6] Hangyu Zhu, Haoyu Zhang, and Yaochu Jin. From federated learning to federated neural architecture search: A survey, 2020.

[7] Chunyi Zhou, Yansong Gao, Anmin Fu, Kai Chen, Zhiyang Dai, Zhi Zhang, Minhui Xue, and Yuqing Zhang. Ppa: Preference profiling attack against federated learning, 2022.

[8] Guan Wang. Interpret federated learning with shapley values, 2019.

[9] Liu Yang, Junxue Zhang, Di Chai, Leye Wang, Kun Guo, Kai Chen, and Qiang Yang. Practical and secure federated recommendation with personalized masks, 2022.

[10] Sungwon Park, Sungwon Han, Fangzhao Wu, Sundong Kim, Bin Zhu, Xing Xie, and Meeyoung Cha. Feddefender: Client-side attack-tolerant federated learning, 2023.

[11] Sofia Zahri, Hajar Bennouri, and Ahmed M. Abdelmoniem. An empirical study of efficiency and privacy of federated learning algorithms, 2023.

[12] Timon Rückel, Johannes Sedlmeir, and Peter Hofmann. Fairness, integrity, and privacy in a scalable blockchain-based federated learning system, 2021.

[13] Sin Kit Lo, Yue Liu, Qinghua Lu, Chen Wang, Xiwei Xu, Hye-Young Paik, and Liming Zhu. Blockchain-based trustworthy federated learning architecture, 2021.

[14] Amir Afaq, Zeeshan Ahmed, Noman Haider, and Muhammad Imran. Blockchain-based collaborated federated learning for improved security, privacy and reliability, 2022.

[15] Anudit Nagar. Privacy-preserving blockchain based federated learning with differential data sharing, 2019.

[16] Zhilin Wang, Qin Hu, Minghui Xu, Yan Zhuang, Yawei Wang, and Xiuzhen Cheng. A systematic survey of blockchained federated learning, 2024.

[17] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, Antonio Ferrara, and Fedelucio Narducci. Federank: User controlled feedback with federated recommender systems. In *Advances in Information Retrieval: 43rd European Conference on IR Research, ECIR 2021, Virtual Event, March 28–April 1, 2021, Proceedings, Part I 43*, pages 32–47. Springer, 2021.

[18] Viraj Kulkarni, Milind Kulkarni, and Aniruddha Pant. Survey of personalization techniques for federated learning, 2020.

[19] Dashan Gao, Xin Yao, and Qiang Yang. A survey on heterogeneous federated learning. *arXiv preprint arXiv:2210.04505*, 2022.

[20] Tomoya Yanagi, Shunnosuke Ikeda, Noriyoshi Sukegawa, and Yuichi Takano. Privacy-preserving recommender system using the data collaboration analysis for distributed datasets, 2024.

[21] Jiangcheng Qin and Baisong Liu. A novel privacy-preserved recommender system framework based on federated learning, 2020.

[22] Vasileios Perifanis and Pavlos S Efraimidis. Federated neural collaborative filtering. *Knowledge-Based Systems*, 242:108441, 2022.

[23] M. A. P. Chamikara, P. Bertok, I. Khalil, D. Liu, and S. Camtepe. Privacy preserving distributed machine learning with federated learning, 2021.

[24] Rui Ye, Xinyu Zhu, Jingyi Chai, Siheng Chen, and Yanfeng Wang. Federated learning empowered by generative content, 2023.

[25] Hadeel Abd El-Kareem, Abd El-Moaty Saleh, Ana Fernández-Vilas, Manuel Fernández-Veiga, and asser El-Sonbaty. Using decentralized aggregation for federated learning with differential privacy, 2023.

[26] Anirban Das and Thomas Brunschwiler. Privacy is what we care about: Experimental investigation of federated learning on edge devices, 2019.

[27] Nader Bouacida, Jiahui Hou, Hui Zang, and Xin Liu. Adaptive federated dropout: Improving communication efficiency and generalization for federated learning, 2020.

[28] Ghazaleh Shirvani, Saeid Ghasemshirazi, and Behzad Beigzadeh. Federated learning: Attacks, defenses, opportunities, and challenges, 2024.

[29] Rajitha Hathurusinghe, Isar Nejadgholi, and Miodrag Bolic. A privacy-preserving approach to extraction of personal information through automatic annotation and federated learning, 2021.

[30] Hangyu Zhu, Liyuan Huang, and Zhenping Xie. Privacy attack in federated learning is not easy: An experimental study, 2024.

[31] Ibrahim Abdul Majeed, Sagar Kaushik, Aniruddha Bardhan, Venkata Siva Kumar Tadi, Hwang-Ki Min, Karthikeyan Kumaraguru, and Rajasekhara Duvvuru Muni. Comparative assessment of federated and centralized machine learning, 2022.

[32] Sudipta Paul, Poushali Sengupta, and Subhankar Mishra. Flaps: Federated learning and privately scaling, 2020.

[33] Nima Mohammadi, Jianan Bai, Qiang Fan, Yifei Song, Yang Yi, and Lingjia Liu. Differential privacy meets federated learning under communication constraints, 2021.

[34] Muhammad Ammad ud din, Elena Ivannikova, Suleiman A. Khan, Were Oyomno, Qiang Fu, Kuan Eeik Tan, and Adrian Flanagan. Federated collaborative filtering for privacy-preserving personalized recommendation system, 2019.

[35] Maxence Noble, Aurélien Bellet, and Aymeric Dieuleveut. Differentially private federated learning on heterogeneous data, 2023.

[36] Yifan Wang, Xianghui Cao, Shi Jin, and Mo-Yuen Chow. A novel privacy enhancement scheme with dynamic quantization for federated learning, 2024.

[37] Farwa K. Khan, Adrian Flanagan, Kuan E. Tan, Zareen Alamgir, and Muhammad Ammad-Ud-Din. A payload optimization method for federated recommender systems, 2021.

[38] Chuan Ma, Jun Li, Ming Ding, Howard Hao Yang, Feng Shu, Tony Q. S. Quek, and H. Vincent Poor. On safeguarding privacy and security in the framework of federated learning, 2020.

[39] Gihun Lee, Minchan Jeong, Yongjin Shin, Sangmin Bae, and Se-Young Yun. Preservation of the global knowledge by not-true distillation in federated learning, 2022.

[40] Jiawen Kang, Zehui Xiong, Dusit Niyato, Yuze Zou, Yang Zhang, and Mohsen Guizani. Reliable federated learning for mobile networks, 2019.

[41] Uncertainty minimization for personalized federated semi-supervised learning.

[42] Minxing Zhang, Zhaochun Ren, Zihan Wang, Pengjie Ren, Zhumin Chen, Pengfei Hu, and Yang Zhang. Membership inference attacks against recommender systems, 2021.

[43] Chaoqun Yang, Wei Yuan, Liang Qu, and Thanh Tam Nguyen. Pdc-frs: Privacy-preserving data contribution for federated recommender system, 2024.

[44] Marco Arazzi, Mauro Conti, Antonino Nocera, and Stjepan Picek. Turning privacy-preserving mechanisms against federated learning, 2023.

[45] David Byrd and Antigoni Polychroniadou. Differentially private secure multi-party computation for federated learning in financial applications, 2020.

[46] Chaochao Chen, Liang Li, Bingzhe Wu, Cheng Hong, Li Wang, and Jun Zhou. Secure social recommendation based on secret sharing, 2020.

[47] Wenjie Li, Kai Fan, Jingyuan Zhang, Hui Li, Wei Yang Bryan Lim, and Qiang Yang. Enhancing security and privacy in federated learning using low-dimensional update representation and proximity-based defense, 2025.

[48] Alberto Bietti, Chen-Yu Wei, Miroslav Dudík, John Langford, and Zhiwei Steven Wu. Personalization improves privacy-accuracy tradeoffs in federated learning, 2022.

[49] Stacey Truex, Ling Liu, Ka-Ho Chow, Mehmet Emre Gursoy, and Wenqi Wei. Ldp-fed: Federated learning with local differential privacy. In *Proceedings of the third ACM international workshop on edge systems, analytics and networking*, pages 61–66, 2020.

[50] Stacey Truex, Ling Liu, Ka-Ho Chow, Mehmet Emre Gursoy, and Wenqi Wei. Ldp-fed: Federated learning with local differential privacy, 2020.

[51] Liping Yi, Han Yu, Gang Wang, and Xiaoguang Liu. pfedes: Model heterogeneous personalized federated learning with feature extractor sharing, 2023.

[52] Wei Yuan, Chaoqun Yang, Liang Qu, Guanhua Ye, Quoc Viet Hung Nguyen, and Hongzhi Yin. Robust federated contrastive recommender system against model poisoning attack, 2024.

[53] Yawei Zhao, Qinghe Liu, Xinwang Liu, and Kunlun He. Medical federated model with mixture of personalized and sharing components, 2023.

[54] Wentao Gao, Omid Tavallaie, Shuaijun Chen, and Albert Zomaya. Federated learning as a service for hierarchical edge networks with heterogeneous models, 2024.

[55] Xuebin Ren, Shusen Yang, Cong Zhao, Julie McCann, and Zongben Xu. Belt and braces: When federated learning meets differential privacy, 2024.

[56] Sheng Shen, Tianqing Zhu, Di Wu, Wei Wang, and Wanlei Zhou. From distributed machine learning to federated learning: In the view of data privacy and security. *Concurrency and Computation: Practice and Experience*, 34(16):e6002, 2022.

[57] Ashkan Vedadi Gargary and Emiliano De Cristofaro. A systematic review of federated generative models, 2024.

[58] Chaoyu Zhang and Shaoyu Li. State-of-the-art approaches to enhancing privacy preservation of machine learning datasets: A survey, 2025.

[59] Ehsan Hallaji, Roozbeh Razavi-Far, Mehrdad Saif, Boyu Wang, and Qiang Yang. Decentralized federated learning: A survey on security and privacy, 2024.

[60] Gustav A. Baumgart, Jaemin Shin, Ali Payani, Myungjin Lee, and Ramana Rao Kompella. Not all federated learning algorithms are created equal: A performance evaluation study, 2024.

[61] Michael Ben Ali, Omar El-Rifai, Imen Megdiche, André Peninou, and Olivier Teste. Comparative evaluation of clustered federated learning methods, 2024.

[62] Mohammad Naseri, Jamie Hayes, and Emiliano De Cristofaro. Local and central differential privacy for robustness and privacy in federated learning, 2022.

[63] Han Wu, Zilong Zhao, Lydia Y. Chen, and Aad van Moorsel. Federated learning for tabular data: Exploring potential risk to privacy, 2022.

[64] Vaikkunth Mugunthan, Anton Peraire-Bueno, and Lalana Kagal. Privacyfl: A simulator for privacy-preserving and secure federated learning, 2020.

[65] Rahul Sharma, Anil Ramakrishna, Ansel MacLaughlin, Anna Rumshisky, Jimit Majmudar, Clement Chung, Salman Avestimehr, and Rahul Gupta. Federated learning with noisy user feedback, 2022.

[66] Jiale Guo, Ziyao Liu, Kwok-Yan Lam, Jun Zhao, Yiqiang Chen, and Chaoping Xing. Secure weighted aggregation for federated learning, 2021.

[67] Ghada Almashaqbeh and Zahra Ghodsi. Anofel: Supporting anonymity for privacy-preserving federated learning, 2023.

[68] Xue Yang, Depan Peng, Yan Feng, Xiaohu Tang, Weijun Fang, and Jun Shao. Efficiently achieving secure model training and secure aggregation to ensure bidirectional privacy-preservation in federated learning, 2024.

[69] Sharare Zehtabian, Siavash Khodadadeh, Ladislau Bölöni, and Damla Turgut. Privacy-preserving learning of human activity predictors in smart environments, 2021.

[70] Qi Hu and Yangqiu Song. User consented federated recommender system against personalized attribute inference attack, 2023.

[71] Seth Gilbert, Xiao Liu, and Haifeng Yu. On differentially private online collaborative recommendation systems, 2015.

[72] Lorenzo Minto, Moritz Haller, Benjamin Livshits, and Hamed Haddadi. Stronger privacy for federated collaborative filtering with implicit feedback. In *Proceedings of the 15th ACM conference on recommender systems*, pages 342–350, 2021.

[73] Yuntao Wang, Zhou Su, Yanghe Pan, Tom H Luan, Ruidong Li, and Shui Yu. Social-aware clustered federated learning with customized privacy preservation, 2024.

[74] Lingjuan Lyu, Han Yu, and Qiang Yang. Threats to federated learning: A survey, 2020.

[75] Najeeb Moharram Jebreel, Josep Domingo-Ferrer, Alberto Blanco-Justicia, and David Sanchez. Enhanced security and privacy via fragmented federated learning, 2022.

[76] Junjie Tan, Ying-Chang Liang, Nguyen Cong Luong, and Dusit Niyato. Toward smart security enhancement of federated learning networks, 2020.

[77] Dipanwita Thakur, Antonella Guzzo, and Giancarlo Fortino. Anomalous client detection in federated learning, 2024.

[78] Siddharth Divi, Habiba Farrukh, and Berkay Celik. Unifying distillation with personalization in federated learning, 2021.

[79] Jiehan Zhou, Shouhua Zhang, Qinghua Lu, Wenbin Dai, Min Chen, Xin Liu, Susanna Pirttikangas, Yang Shi, Weishan Zhang, and Enrique Herrera-Viedma. A survey on federated learning and its applications for accelerating industrial internet of things. *arXiv preprint arXiv:2104.10501*, 2021.

[80] Matias Mendieta, Guangyu Sun, and Chen Chen. Navigating heterogeneity and privacy in one-shot federated learning with diffusion models, 2024.

[81] Nanqing Dong, Zhipeng Wang, Jiahao Sun, Michael Kampffmeyer, William Knottenbelt, and Eric Xing. Defending against poisoning attacks in federated learning with blockchain, 2024.

[82] Boyu Fan, Siyang Jiang, Xiang Su, Sasu Tarkoma, and Pan Hui. A survey on model-heterogeneous federated learning: Problems, methods, and prospects, 2024.

[83] El Houcine Bergou, Konstantin Burlachenko, Aritra Dutta, and Peter Richtárik. Personalized federated learning with communication compression, 2022.

[84] Jiahao Liu, Jiang Wu, Jinyu Chen, Miao Hu, Yipeng Zhou, and Di Wu. Feddwa: Personalized federated learning with dynamic weight adjustment, 2023.

[85] Taki Hasan Rafi, Faiza Anan Noor, Tahmid Hussain, Dong-Kyu Chae, and Zhaohui Yang. A generalized look at federated learning: Survey and perspectives, 2023.

[86] Ming Liu, Stella Ho, Mengqi Wang, Longxiang Gao, Yuan Jin, and He Zhang. Federated learning meets natural language processing: A survey. *arXiv preprint arXiv:2107.12603*, 2021.

Disclaimer:

SurveyX is an AI-powered system designed to automate the generation of surveys. While it aims to produce high-quality, coherent, and comprehensive surveys with accurate citations, the final output is derived from the AI's synthesis of pre-processed materials, which may contain limitations or inaccuracies. As such, the generated content should not be used for academic publication or formal submissions and must be independently reviewed and verified. The developers of SurveyX do not assume responsibility for any errors or consequences arising from the use of the generated surveys.