applied sciences

MDPI

Article

A Comprehensive Survey on Privacy-Preserving Techniques in Federated Recommendation Systems

Muhammad Asad *, Saima Shaukat, Ehsan Javanmardi, Jin Nakazato and Manabu Tsukada

Graduate School of Information Science and Technology, Department of Creative Informatics, The University of Tokyo, Tokyo 113-8654, Japan; saima@g.ecc.u-tokyo.ac.jp (S.S.); ejavanmardi@g.ecc.u-tokyo.ac.jp (E.J.); jin-nakazato@g.ecc.u-tokyo.ac.jp (J.N.); mtsukada@g.ecc.u-tokyo.ac.jp (M.T.)

* Correspondence: asad@g.ecc.u-tokyo.ac.jp

Abstract: Big data is a rapidly growing field, and new developments are constantly emerging to address various challenges. One such development is the use of federated learning for recommendation systems (FRSs). An FRS provides a way to protect user privacy by training recommendation models using intermediate parameters instead of real user data. This approach allows for cooperation between data platforms while still complying with privacy regulations. In this paper, we explored the current state of research on FRSs, highlighting existing research issues and possible solutions. Specifically, we looked at how FRSs can be used to protect user privacy while still allowing organizations to benefit from the data they share. Additionally, we examined potential applications of FRSs in the context of big data, exploring how these systems can be used to facilitate secure data sharing and collaboration. Finally, we discuss the challenges associated with developing and deploying FRSs in the real world and how these challenges can be addressed.

Keywords: federated recommendation systems; privacy preserving; big data; data sharing

Citation: Asad, M.; Shaukat, S.; Javanmardi, E.; Nakazato, J.; Tsukada, M. A Comprehensive Survey on Privacy-Preserving Techniques in Federated Recommendation Systems. *Appl. Sci.* **2023**, *13*, 6201. https://doi.org/10.3390/app13106201

Academic Editors: Arcangelo Castiglione, Pan Zhou and Xiaofeng Ding

Received: 30 March 2023
Revised: 29 April 2023
Accepted: 16 May 2023
Published: 18 May 2023

1. Introduction

In recent years, recommendation systems have become a popular tool to address information overload in many real-world fields such as news, E-commerce, and healthcare [1–4]. This requires collecting a large amount of sensitive information about users, such as user attributes, social relations, contextual information, and behaviors [5]. Unfortunately, a central server is needed to store these data, leading to the potential risks of data privacy leakage, such as selling user data to a third party without consent or malicious attackers stealing the data [6]. Additionally, due to privacy concerns and regulatory restrictions, it is difficult to integrate data from other platforms to improve the performance of the recommendation system [7]. For example, the General Data Protection Regulation (GDPR) has set strict rules for collecting user data and sharing data between different platforms, which can lead to an inadequate amount of data for the recommendation system, thus decreasing its performance [8].

To overcome this challenge, Google introduced federated learning, a privacy-preserving distributed learning scheme that allows participants to collaborate to train a machine learning model without exchanging real data [9]. Instead, intermediate parameters such as model parameters and gradients are exchanged between participants. This has opened up a new field of application for recommendation systems known as federated recommendation systems (FRSs), which combine federated learning with recommendation systems for privacy-preserving recommendation systems [10]. In Figure 1, we present the generic training procedure of FRSs.

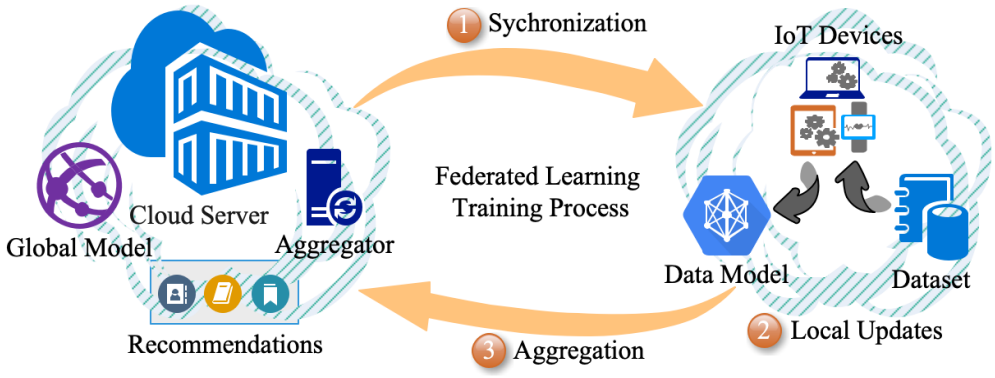

Figure 1. This figure represents the generic training procedure of FRSs, where a set of IoT devices is connected to the cloud server. Firstly, the cloud server synchronizes with the IoT devices and creates personalized recommendations; secondly, those IoT devices train the local learning models individually and then upload those trained learning models to the cloud server. Finally, the cloud server aggregates those local models to generate new recommendations for the next round.

1.1. Privacy Concerns

The FRS is an innovative approach that seeks to provide a privacy-aware paradigm for model training by avoiding direct exposure to real user data [11,12]. However, there are still some core concerns that need to be addressed in order to make this approach fully effective. These concerns include finding the exact privacy-preserving technique that not only provides the trustworthiness of the data, but also achieves higher accuracy. Moreover, the scalability of the approach must be further explored in order to make it applicable to a wide range of use cases:

- **User-side concerns**: the primary privacy concern of a user in an FRS is that personal data are shared across multiple entities [13,14]. These data may include sensitive information such as name, address, age, gender, and financial information. If these data are not properly secured and shared securely, this could lead to a potential violation of an individual's privacy [15]. In addition, the user may be unaware of how his/her data are being used, leading to a potential breach of his/her privacy. On the other hand, an FRS can itself pose privacy risks due to the potential for profiling. This means that the user's data are used to build a profile of his/her interests and activities, which can then be used to create targeted advertisements or other manipulative tactics. This can lead to a potential violation of an individual's right to privacy.
- **Server-side concerns**: An FRS is vulnerable to attacks by malicious actors, who can disrupt the federated system by manipulating user ratings, injecting false information, and taking over the federated system [16,17]. Attackers can also employ various techniques, such as data poisoning, distributed denial-of-service attacks, and brute force attacks, to disrupt the system [18]. Furthermore, attackers may be able to access user data through unencrypted channels or modify the recommendations generated by the system to suit their interests.

1.2. Related Work

Several surveys have focused on FRS, but they cannot provide comprehensive solutions to address the effects of privacy and security issues in big data applications. In [19], the study investigated the characteristics and challenges of federated learning in detail, but did not provide enough detail on FRSs. In [20], the authors gave an accurate definition of federated learning and its different architectures and applications, such as the FRS. In [21], the authors provided a comprehensive categorization of recommendation methods, as well as discussed their respective limitations. In addition, several surveys were conducted that focused on the privacy and security of federated learning. In [22], the study identified and analyzed the potential privacy threats and security vulnerabilities in federated learning.

Similarly, in [23], the authors elaborated on the assumptions, reasons, principles, and differences between the various attacks and defenses in the privacy and robustness fields of federated learning, but none of them particularly focused on FRSs. Despite this, most of these surveys focused on either recommendation systems or federated learning separately, and few surveyed specific problems in FRSs. For example, in [10], the study proposed a classification for FRSs from the perspective of federated learning and investigated the algorithm-level and system-level challenges for FRSs. These surveys may provide insight into the capabilities of FRSs, but they did not offer solutions that can effectively deal with privacy and security within the framework of the system.

1.3. Our Contribution

Compared to the existing surveys, this survey paper provides the impact of FRSs on privacy-preserving techniques in big data. It presents a comprehensive review of the main challenges and existing approaches to enable data sharing while preserving user privacy. Furthermore, it compared various privacy-preserving techniques, including differential privacy, secure multiparty computation, homomorphic encryption, tokenization, anonymization, and pseudonymization. Furthermore, this survey provides an overview of the targeted applications and industry of FRSs. Moreover, a detailed description of the public datasets used in FRSs is provided, highlighting the unique challenges posed by big data sharing. Finally, this survey paper provides real-world challenges for future research directions.

The rest of the paper is organized to provide an in-depth exploration of the field of FRSs. Section 2 provides the necessary overview of the research. Section 3 delves into the details of privacy-preserving techniques used in this area. Section 4 examines the applications and industries that are targeted with FRSs. Section 5 looks at the publicly available datasets for FRSs. Section 6 delves into the future directions and challenges that can be faced in real-world applications. Lastly, Section 7 concludes the survey and provides an overall summary of the research.

2. Overview of the FRS

An FRS is a distributed system for providing a personalized product and content recommendations across multiple platforms [24]. It is designed to leverage the collective intelligence of the network of participants, providing a more comprehensive view of the user's preferences and needs [25]. Below, we precisely explain the main entities in FRSs. Figure 2 presents the architectural overview of the FRS.

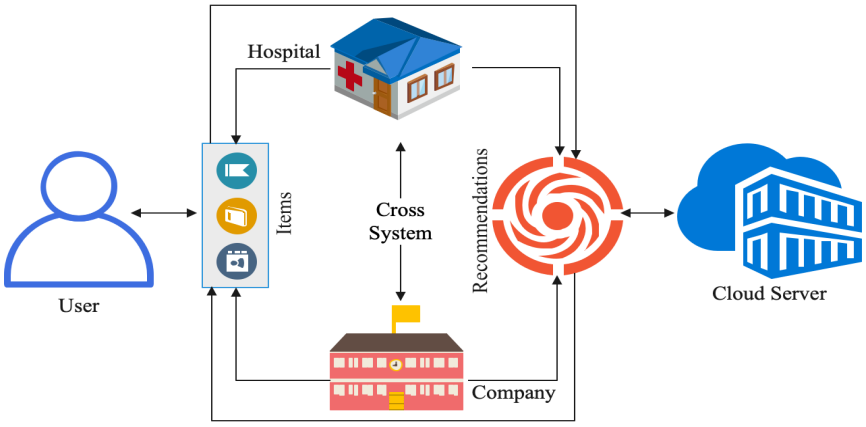

Figure 2. Overview of the FRS entities.

- **User**: The user entity in an FRS is an individual identified by his/her unique ID. The user is the primary person interacting with the system and provides information to generate personalized recommendations [26]. This includes user preferences, interests, purchase history, and other data that can be used to suggest relevant items. The user

entity is also used to store information related to the user's interactions with the system, such as ratings, reviews, feedback, etc. This information can be used to help improve the accuracy of future recommendations.

- **Item**: The item entity in the FRS refers to the items recommended to the users. This could include products, services, books, movies, music, etc. [27]. The items can come from different sources, such as websites, stores, or catalogs. The recommendation system uses the item entity to suggest items to users based on their preferences and interests. The item entity also contains information about the items, such as the price, description, and other relevant details.
- **Cross-system**: The cross-system entity in an FRS is a type of user profile created by combining user data from multiple systems [28]. This allows for more accurate recommendation algorithms to be developed and deployed across multiple systems [29]. For example, if a system collects user data from multiple different websites and platforms, the cross-system entity can be used to create a unified profile of a user across all of these different sources. This unified profile can then be used to generate more accurate recommendations, such as suggesting a product that a user might like based on his/her preferences across all of the different systems.
- **Recommendation**: A recommendation entity in an FRS allows individual users to access personalized recommendations from multiple sources [30,31]. This type of system is useful for organizations that have multiple data sources and need to be able to provide personalized recommendations to individual users based on their historical experience [32]. The recommendation entity acts as a central hub that can aggregate data from multiple sources and provide tailored recommendations to individual users. This helps organizations make decisions more quickly and efficiently, allowing them to increase customer satisfaction and loyalty.
- **Cloud server**: A cloud server is an entity in an FRS that stores user information and makes recommendations for other users [33]. The cloud server is responsible for collecting data from multiple sources, processing them, and making recommendations. It also is a hub for other participating entities, such as individual users, content providers, and recommendation systems. By connecting these entities, the federated server can provide more accurate and personalized recommendations to users [34].

2.1. Architecture of FRS

The architecture of an FRS can be divided into the following four components, as shown in Figure 3:

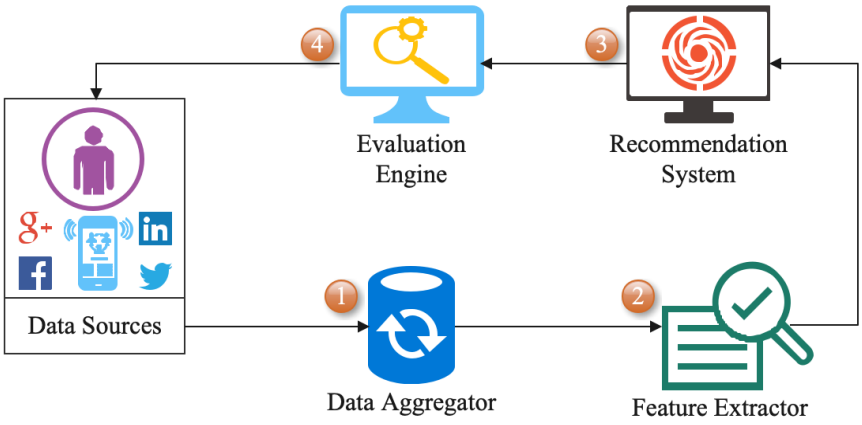

Figure 3. Architecture of the FRS, divided into four components used for user's data sources.

1. **Data aggregator**: This component is responsible for collecting and processing data from multiple sources (e.g., websites and mobile apps). The data aggregator then stores the data in a unified format, allowing the recommendation system to access the data from all sources in one place [35]. It can be used to create user profiles and

determine user preferences, as well as to enable recommendations to be made across multiple platforms [36].

2. **Feature extractor**: This component is a critical part of the FRS architecture. It is responsible for extracting key features from data sources in order to create a unified representation of the data [37]. This unified representation enables the system to compare data from different sources and make recommendations accurately. Furthermore, it enables the system to generalize the data, reducing the amount of data that need to be processed [38]. The feature extractor component can extract features such as user preferences, user demographics, item attributes, and item ratings.
3. **Recommendation system**: A recommendation system is a key component of an FRS. It generates user recommendations based on the data gathered from the different federated sources [39]. The system uses algorithms to analyze the data and create personalized recommendations for the users. The goal is to provide the most-relevant and accurate recommendations tailored to users' interests and preferences [40]. The recommender system is also responsible for updating the recommendations as new data are added to the federated sources. This helps ensure that the recommendations remain relevant and up-to-date [41].
4. **Evaluation engine**: This component measures the system's performance, such as user engagement, user satisfaction, and other metrics [42]. The evaluation engine collects and analyzes data from different sources and uses machine learning algorithms to identify patterns in the data and evaluate the system's performance. It also provides feedback to the other components in the system, such as the content providers, to enable further optimization [43,44]. The evaluation engine ensures fairness and accuracy in the system.

2.2. Categories of FRS

In this section, we explore the different categories of FRSs and discuss how FRSs can be used to improve the accuracy and efficiency of recommendations. We also present how these categories can pose serious privacy concerns to users' sensitive data. In Figure 4, we present the categories of FRSs. In Table 1, we briefly highlight the pros and cons of each below mentioned FRS technique.

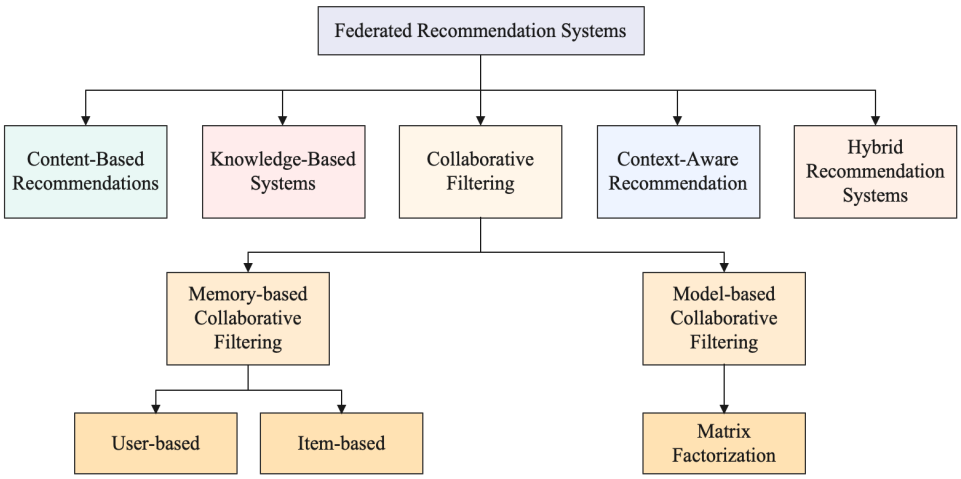

Figure 4. Categories of federated recommendation systems.

- **Content-based filtering**: This type of FRS uses content-based information to provide personalized recommendations to users without needing to collect and store personal user data [45,46]. FRSs work by aggregating data from multiple sources, such as online stores, websites, and other applications, and using algorithms to detect patterns in the data. To this end, content-based filtering uses information about the content of the recommended items, such as genre, author, or keywords, to generate recom-

mendations [47]. Content-based filtering has several advantages over other forms of FRSs. It does not require any user data, so it can protect user privacy by avoiding the need to collect and store any sensitive personal information. Additionally, it is less resource-intensive than other forms of FRSs, since it does not require creating a centralized database to store user data. Moreover, it is easy to implement since it does not require a complex algorithm to generate the recommendations [48]. Content-based filtering is often used in conjunction with other forms of FRSs, such as collaborative filtering, in order to generate more accurate and personalized recommendations [49]. This category is becoming increasingly popular among online retailers and other businesses due to its effectiveness and privacy-preserving benefits. However, content-based filtering requires access to the user's interaction data to make recommendations, which means that the system can access the user's preferences and behavior, which could be sensitive information. Therefore, without proper privacy measures in place, content-based filtering systems can pose a risk to the user's privacy.

- **Knowledge-based systems**: This type of system uses a "knowledge base" to create recommendations based on user preferences and behavior, rather than relying solely on data collected from an individual user [50,51]. This means that the system does not collect any data from the user, instead relying on a pre-existing collection of information. The knowledge base is typically a collection of data about different products, services, or experiences [52]. It contains information about the characteristics of each item, such as its features, price, popularity, and ratings. Using these data, the system can generate recommendations tailored to the user's interests without collecting any personal information from the user. However, knowledge-based systems require access to the user's explicit knowledge about items and preferences to make recommendations. This means that the system has access to the user's sensitive information, which can be a serious concern from the user's perspective [53,54].
- **Collaborative filtering**: This type of FRS prioritizes user privacy while providing effective and accurate recommendations [55]. It uses the user's data to generate personalized recommendations [56,57]. Moreover, the system uses data from similar users to make recommendations to the user. This means that the system can make accurate recommendations by accessing limited users' data or having to share it with other users or systems. The collaborative filtering approach works by first identifying similar users who have the same demographic characteristics, tastes, or preferences [16,58]. Next, the system takes the data from these similar users and uses them to make recommendations to the user. This data might include past purchases, ratings, or reviews. The system then uses these data to develop recommendations for the user [59]. One major privacy issue with collaborative filtering is that it requires access to sensitive user behavior data to make recommendations. These data can include information about the user's past purchases, searches, and interactions with other users. Therefore, without proper privacy measures in place, these data can be vulnerable to unauthorized access, misuse, or disclosure [60].
- **Context-aware recommendation**: This type of FRS uses context-aware techniques to help tailor the recommendations to the users in a way that is more meaningful and tailored to their interests and needs [61,62]. Context-aware recommendation systems are designed to consider the user's current context when making recommendations, such as his/her location, time, and surrounding environment [63,64]. This allows the system to make more accurate and personalized recommendations that better suit the users' needs and preferences [65]. By taking into account the user's current context, the system can provide recommendations that are more accurate and relevant to the user's needs [66,67]. This type of system can help reduce the amount of data that need to be collected and stored by the system, as the data used to generate the recommendations are already present in the user's context [68]. The privacy concern with context-aware recommendations is that they require access to a wide range of user data, including location, device information, and social media activity, to make

personalized recommendations. These data can be sensitive and reveal private information about the user's behavior, interests, and preferences. Therefore, it is important for context-aware recommendation systems to implement robust privacy-preserving techniques to protect user privacy while still providing effective recommendations.

- **Hybrid recommendation systems**: Hybrid recommendation systems are a type of FRS that combine the capabilities of traditional centralized and distributed recommendation systems to provide users with the best of both worlds [3]. Hybrid recommendation systems enable users to make use of personalized recommendations while also protecting their privacy. In a hybrid system, the data are stored in a central repository, and the recommendation algorithm is executed by a federated learning system [69]. The central repository stores all of the user's profile data, and the federated learning system executes the recommendation algorithm without any user data being shared between the two. This allows the system to remain secure and the user data to remain private. Besides, the hybrid system allows different algorithms to be used. For example, collaborative filtering can be used in conjunction with content-based filtering to provide a more accurate recommendation [70]. Furthermore, the system can be adapted to different data sources, such as social media and web analytics. This type of system also has the advantage of scalability. As new users join the system, the recommendation algorithm can be updated without requiring additional user data to be shared [71]. This makes the system more efficient and effective and allows for more users to be accommodated. The primary privacy concern with hybrid recommendation systems is the extensive collection of user data from various sources required to make accurate and diverse recommendations. These data can include sensitive user behavior, profile, and contextual data, which if not properly protected, can lead to unauthorized access and unintended disclosure of personal information. Thus, such systems must prioritize the implementation of robust privacy-preserving techniques, such as data anonymization, homomorphic encryption, and differential privacy, to mitigate the risks of data breaches and ensure that user privacy is not compromised.

Table 1. Comparison of categories of FRSs.

Category	Techniques	Advantages and Disadvantages
Content-Based Filtering	Recommends items similar to those the user has liked before	Effective at recommending niche items; limited to recommending items with similar characteristics; may not work well for users with varying interests
Knowledge-Based Systems	Uses knowledge about user preferences and item attributes to recommend items	Allows for more personalized recommendations; can recommend items outside of the user's usual preferences; requires many data and expert knowledge; may not work well for users with varying interests
Collaborative Filtering	Recommends items based on the preferences of similar users	Can recommend items outside of the user's usual preferences; can work well with large datasets; requires many user data to be effective; can suffer from the "cold start" problem for new users and items
Context-Aware Recommendation	Recommends items based on additional contextual information, such as time of day or location	Can provide more personalized recommendations based on specific situations; requires additional data sources and can be difficult to implement
Hybrid Recommendation Systems	Combines two or more of the above techniques	Can provide more accurate recommendations by leveraging the strengths of multiple techniques; can be complex to implement and requires additional computational resources

3. Privacy Techniques

FRSs pose a unique privacy concern due to their distributed nature. Since the training data are processed and stored across multiple nodes, it is more difficult to ensure data privacy than with a centralized approach. Existing research has shown that the central server can infer sensitive information from the intermediate parameters. For instance, a server can identify items the user has interacted with based on the non-zero gradients sent by the client [72]. Moreover, the server can also infer ratings from the user-uploaded gradients in two consecutive rounds [73]. To address those concerns, privacy-preserving techniques have been developed to protect user data privacy while still allowing FRSs to operate efficiently, as shown in Figure 5. In this section, we present these privacy-preserving techniques of FRSs and compare their advantages and limitations.

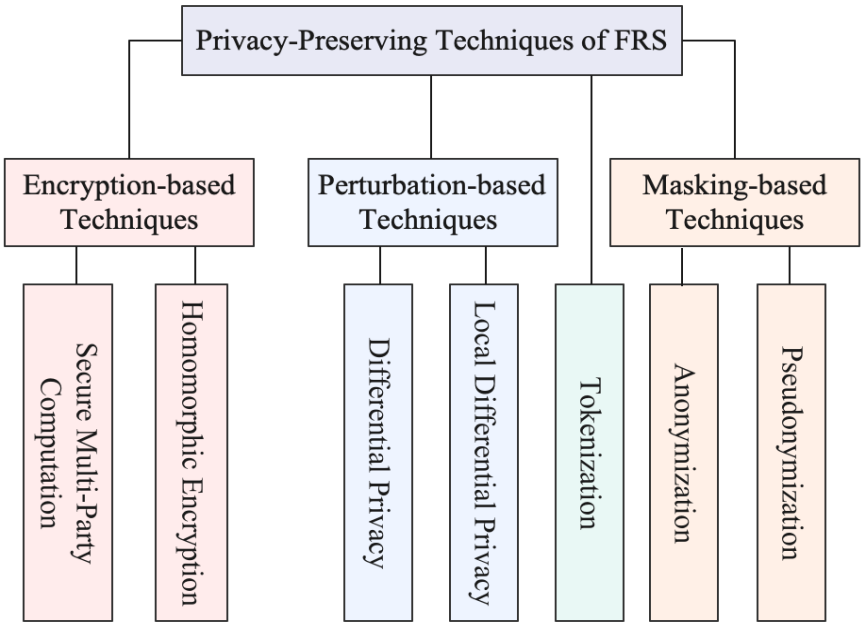

Figure 5. Privacy-preserving techniques used in FRSs.

3.1. Differential Privacy

On the one hand, differential privacy (DP) is a privacy-preserving technique that provides a mathematical guarantee of privacy [74,75]. It works by adding random noise to the data, making it difficult to identify individual data within the dataset [76]. This technique has been used in various contexts, including recommendation systems. For example, in [77], the study used DP to protect the privacy of users in a collaborative filtering-based recommendation system. The authors added Laplace noise to the user ratings to ensure privacy preservation. Similarly, in [78], the study used DP to protect the privacy of user ratings in a matrix factorization approach to recommendations.

On the other hand, local differential privacy (LDP) is a variant of DP that is used for federated learning. Instead of adding noise to the entire dataset, LDP adds noise to each user's data before sending them to the server [79]. This ensures that the server never has access to the raw data, but still can obtain useful information. Several studies have been conducted in this context; for example, in [80], the study used LDP to protect the privacy of users in a matrix-factorization-based recommendation system. Similarly, in [81], the authors improved the matrix factorization using LDP for recommendation systems.

The benefits of using DP and LDP in FRS include the ability to protect user privacy while still allowing the server to obtain useful information from the data [82–84]. Moreover, it ensures that the raw data are never exposed to the server, which is important for protecting user privacy. The limitations of using DP and LDP in FRSs include the fact that the noise added to the data can lead to inaccurate results, as well as increased computation time due

to the need to add the noise [85]. Besides, it is difficult to determine the optimal noise level for a given dataset, which can lead to inaccurate results. Therefore, it is essential to design a system that can effectively trade off between recommendation accuracy and privacy.

3.2. Secure Multi-Party Computation

Secure multi-party computation (SMPC) is a cryptographic technique that allows two or more parties to securely compute a function over their private data without any of the parties being able to access the data of the other parties [86,87]. In other words, SMPC ensures that the private data of each party remain secure while still allowing the parties to obtain the result of the computation over all the data without ever having to share the data themselves.

SMPC has been used in FRSs to protect user data and enable collaborative recommendations across multiple parties. For example, in [88], the study used SMPC to create a privacy-preserving collaborative filtering system that allows multiple parties to generate personalized recommendations without sharing the user data. Similarly, in [89], the study used SMPC in blockchain for privacy preservation.

The benefits of using SMPC in FRSs include the ability to protect user data privacy, the ability to generate personalized recommendations from multiple parties collaboratively, and the ability to create a decentralized recommendation system [90,91]. However, the use of SMPC also has some limitations, such as the high computational cost associated with secure computation, as well as the complexity of designing and implementing secure multi-party protocols.

3.3. Homomorphic Encryption

Homomorphic encryption is a type of encryption that allows computations to be performed on encrypted data without having to decrypt it [92]. In an FRS, homomorphic encryption allows for data to be encrypted and shared between multiple parties while allowing for the computation of recommendations based on the encrypted data [93]. There are two main types of homomorphic encryption used in FRSs: fully homomorphic encryption (FHE) and partially homomorphic encryption (PHE). FHE allows for the computation of arbitrary functions on encrypted data, while PHE allows only specific computations, such as addition or multiplication [94].

Several studies have used homomorphic encryption in recommendation systems with promising results. For example, a recent study [95] developed a privacy-preserving system for matrix factorization using FHE. Another study [96] proposed a privacy-preserving user-based recommendation system using homomorphic encryption. The main benefit of homomorphic encryption in FRSs is that it provides a high level of privacy and security for users, as their data are encrypted and remain confidential [97,98]. However, the main limitation of homomorphic encryption is that it is computationally expensive, which can reduce the system's overall performance.

3.4. Tokenization

Tokenization in FRSs helps to break down the data into smaller components (tokens) to make them easier to analyze and process. This includes breaking down the text into words, sentences, and phrases and breaking down numerical data into numbers and other values [99]. Tokenization also helps to ensure privacy and data security by preventing the leakage of sensitive user data, such as personal information and preferences [100,101]. Several studies have used tokenization in FRSs. For example, in [102], the authors used tokenization to improve the performance of an FRS. They used a tokenization method based on the federated learning framework, which allowed the recommendation model to learn from distributed data sources without compromising user privacy. In [103], the authors used tokenization to improve the accuracy of an FRS by splitting the data into smaller parts.

The benefits of using tokenization in FRSs include improved accuracy, privacy, and scalability. In particular, tokenization allows the system to process data more quickly and accurately while ensuring user privacy [104,105]. In addition, it allows the system to scale

to larger datasets without compromising performance. On the other hand, the limitations of using tokenization in FRSs include the complexity of the tokenization process and the potential for data loss [106]. Tokenization can be computationally intensive and time-consuming, and it can lead to data loss if the tokens are not generated correctly. Besides, some tokens may be more difficult to process than others, leading to potential accuracy issues.

3.5. Anonymization

Anonymization is a privacy-preserving technique in an FRS that is used to protect users' data privacy by concealing their identities [107,108]. The main idea of this technique is to mask users' identity information, such as user ID, username, and other user-related information, while still maintaining their data utility. This technique can protect users' identity information in the FRS while allowing the system to generate useful and accurate recommendations.

There have been several studies that have utilized the anonymization technique in FRS, showing the effectiveness of the technique [109–111]. Anonymization is easy to implement, as it only requires masking the user's identity information. The limitations of using anonymization in FRSs include the potential for data leakage, as well as the risk of data distortion due to the masking of user identity information [112].

3.6. Pseudonymization

Pseudonymization is a privacy-preserving technique used in FRSs to protect the privacy of users by replacing their identifiable attributes with a pseudonym [113,114]. It is a method of masking the true identity of a user while allowing his/her to be identified by his/her pseudonym. Pseudonymization can protect a user's sensitive attributes, such as age, gender, and location, as well as his/her explicit and implicit preferences. Several studies have been conducted on this matter [115–117].

The benefits of using the pseudonymization technique in FRSs include improved privacy for users, as their data are not stored, and only their pseudonym is used to identify them [118]. Furthermore, pseudonymization also allows for better scalability of an FRS as the amount of data stored is reduced and the data can be divided into smaller chunks [119]. However, there are also some limitations to using pseudonymization in FRSs. One of the main drawbacks is that it can be difficult to accurately link a user's pseudonym with his/her true identity and preferences. Furthermore, pseudonymized data can also be vulnerable to dictionary attacks and re-identification attacks.

3.7. Comparison

The aforementioned privacy mechanisms have been widely utilized in FRSs to offer stronger privacy protection. Table 2 details the comparison between these mechanisms. Similarly, Table 3 overviews privacy-preserving techniques, including their descriptions, domains, platforms, and environments. Firstly, the main objects of protection vary between the mechanisms. The tokenization mechanism secures user interaction behaviors, while the remaining mechanisms protect user ratings. Moreover, homomorphic encryption can also integrate data from other participants in a secure manner. Secondly, homomorphic encryption and secure multi-party computation are both encryption-based mechanisms, which protect privacy while maintaining accuracy, but the high computational cost of homomorphic encryption restricts its application in large-scale industrial settings. Secret multi-party computation reduces the computation cost, but increases the communication costs. On the other hand, differential privacy and local differential mechanisms protect privacy by adding random noise, which has low computational costs and does not add any communication costs. Nonetheless, adding random noise will unavoidably influence model performance to a certain degree.

Table 2. Comparison between several privacy-preserving techniques.

Reference	Privacy Type	Privacy Target	Privacy	C/C Costs
[34,120–123]	Differential Privacy	Ratings	High	Low
[25,86–88,111,124]	SMPC	Ratings	Low	High
[31,35,73,125–127]	Homomorphic Encryption	High-Order Graphs Social Features Ratings	Moderate	High
[103,128–130]	Tokenization	Prediction	Low	Low
[24,131]	Anonymization	User's data	High	High
[72,132–135]	Pseudonymization	User's data	Moderate	Low

In column "Privacy", we compare privacy with respect to accuracy. **High** means a good tradeoff between privacy and accuracy. **Moderate** means high privacy, but lower accuracy. **Low** means poor privacy and poor accuracy. **C/C** stands for communication/computation costs.

Table 3. Privacy-preserving techniques in various domains, platforms, and environments.

Privacy-Preserving Technique	Description	Domain	Platform	Environment
Differential Privacy	A technique that adds noise to the data to protect individual privacy while still allowing for useful analysis	Healthcare, social science, finance	Google, Apple, Microsoft	Cloud computing, big data
Secure Multi-Party Computation	A technique that allows multiple parties to jointly compute a function without revealing their inputs to each other	Banking, insurance, healthcare	Intel SGX, IBM Homomorphic Encryption Toolkit	Cloud computing, IoT
Homomorphic Encryption	A technique that allows computations to be performed on encrypted data without decrypting them	Healthcare, finance, government	Microsoft SEAL, IBM Homomorphic Encryption Toolkit	Cloud Computing, IoT
Tokenization	A technique that replaces sensitive data with non-sensitive data, while preserving their meaning	Payment processing, E-commerce	Stripe, Braintree	Cloud computing, web
Anonymization	A technique that removes personally identifiable information from data	Social media, market research	Facebook, Twitter, Google	Web, mobile
Pseudonymization	A technique that replaces personally identifiable information with a pseudonym	Healthcare, research	AWS, Azure	Cloud computing, big data

4. Applications and Target Industry

The FRS is a powerful tool that can be utilized in various applications and target industries. It enables secure and privacy-preserving data sharing for big data and provides real-time recommendations across multiple sources [136]. However, sharing data means that users must reveal their private information, such as name and address, which can easily be taken advantage of by third-party companies [137,138]. In particular, this private

information can be used in the retail industry to provide personalized product recommendations to customers, in the healthcare industry to identify potential treatments for patients [139], in the finance industry to suggest financial products to customers [140], and in content recommendation for E-commerce websites and for recommending movies and shows on streaming services [141]. In Figure 6, we present the potential applications and target industries of FRSs and outline their details in the following subsections. In Table 4, we present potential real-time applications and targeted industries of FRSs.

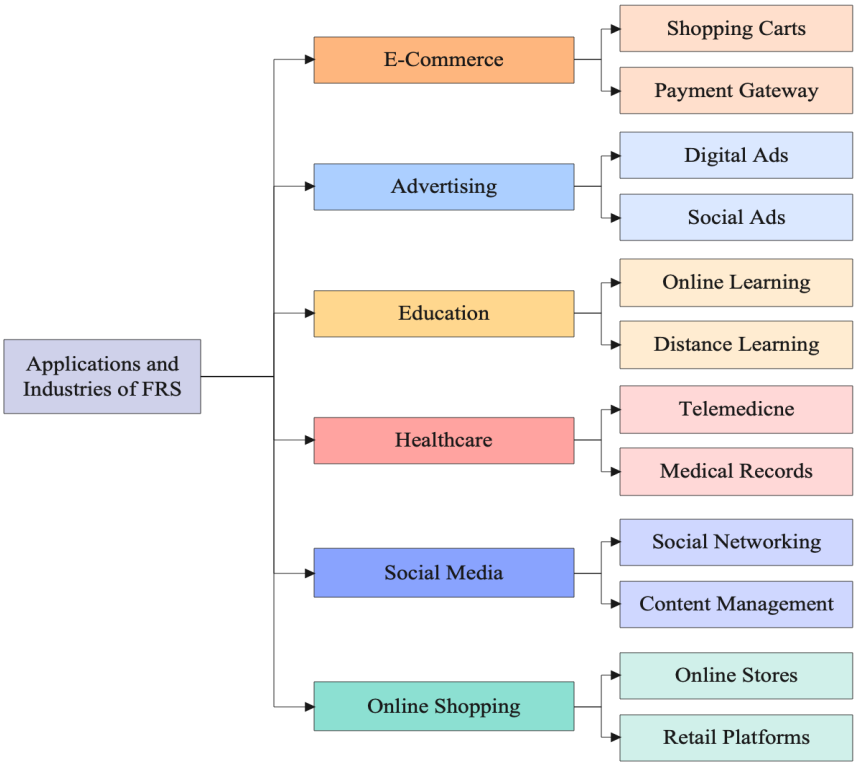

Figure 6. Applications and target industries of FRSs.

Table 4. Real-time applications and targeted industries of FRSs.

Application	Online Shopping	Social Media	Healthcare	Education	Advertising
Personalized Recommendations	✓	✓	✓	✓	✓
Cross-Platform Recommendations	✓	✓	✓	✓	✓
Improved User Engagement	✓	✓		✓	✓
Targeted Marketing	✓	✓			✓
Better Patient Outcomes			✓		
Efficient Learning				✓	

4.1. Online Shopping

Currently, online shopping services are becoming increasingly popular and are involved in various aspects of our lives [14]. A large amount of private information of users is collected and stored centrally by online shopping service providers, which poses a serious risk of privacy leakage [142–144]. User data may be sold to third parties by service providers or stolen by external hackers. FRSs can help users enjoy personalized recommendation services while maintaining personal privacy, make the service providers more trusted by users, and ensure the recommendation service complies with the regulations [145]. For example, an FRS can be designed to implement various popular recommendation

algorithms to support many online shopping services and deploy them on a real-world content recommendation application.

4.2. Social Media

Social media in FRSs allows users to interact with each other and share content, such as comments, photos, videos, and links [135,146]. This is a platform that allows users to create networks, post content, and engage with one another in various ways. Social media can include sites such as Facebook, Twitter, LinkedIn, Instagram, Pinterest, and YouTube [147]. Studies have found that recommender systems can help to increase the accuracy and relevancy of recommendations by leveraging the vast amount of user data from social media platforms [148–152]. Therefore, using an FRS can enable the personalization of recommendations by leveraging user preferences and interests from social media profiles and can eliminate bias by incorporating the collective wisdom of users from different social media platforms. FRSs can benefit social media in a number of ways, i.e., they can provide more accurate and relevant recommendations, which can increase user engagement and satisfaction. They can also help reduce bias and personalize recommendations, which can improve the user experience [153]. Moreover, they can provide better insights into user preferences and interests, which can be used to inform marketing campaigns and product development.

4.3. Healthcare

The healthcare industry is one of the most-heavily regulated industries in the world, and using FRSs to share data can help reduce the burden of compliance [154,155]. In particular, FRSs can allow various healthcare providers share patient data, medical records, and other relevant information while maintaining the privacy of individual data. Researchers have studied the potential of FRSs for healthcare data sharing [156,157]. The consensus is that FRSs can provide a secure, efficient, and cost-effective way to share sensitive patient data between organizations. Studies have also shown that FRSs can reduce the cost of healthcare data storage, improve the quality of care, and reduce the burden of compliance with data privacy regulations [158,159]. FRSs can benefit healthcare in a number of ways. For one, they can allow for more secure and efficient data sharing between healthcare providers. By using FRSs, organizations can share data without sacrificing the privacy of individual data [160]. Moreover, FRSs can reduce the cost of healthcare data storage and improve the quality of care by allowing a more comprehensive view of each patient [161]. Finally, FRSs can reduce the burden of compliance with data privacy regulations, as data can be stored in a secure and encrypted manner [162].

4.4. Education

Education can be defined as the process of preparing individuals for life, work, and citizenship through the acquisition of knowledge, skills, values, beliefs, and habits. In an FRS, education uses computers and other electronic technologies to facilitate those acquisitions [163,164]. In particular, FRSs allow for a more personalized and tailored educational experience, allowing students to progress at their own pace and according to their interests [165]. There has been increasing research into using recommendations in the education industry [166]. Several studies have focused on the use of a recommendation system to provide personalized and tailored educational experiences through the use of computer-based learning [167–169]. Such research has highlighted the potential of recommendations to increase student engagement, improve student performance, and reduce the need for teachers to provide instruction. To this end, FRSs can provide personalized and tailored educational experiences to students of all ages and backgrounds. By leveraging the power of computers and other electronic technologies, FRSs can provide students with personalized feedback and guidance tailored to their learning needs.

4.5. Advertising

Advertising in an FRS identifies and targets potential customers by delivering customized messages and offers. This is usually accomplished through personalization and contextualization, leveraging user data and preferences, geography, and other demographic characteristics [170–172]. In FRSs, the main goal of advertising is to increase the visibility of products and services and to increase the likelihood of conversion [173]. Recent research has highlighted the potential of FRSs to facilitate better advertisement targeting. In [174], it was found that a recommendation system using a machine learning approach can improve the accuracy of ads by up to 20%. This improvement was attributed to the ability of recommendations to model user preferences and characteristics more accurately, allowing for better targeting of ads. Moreover, FRSs can help reduce the cost associated with advertising campaigns, as well as the amount of effort needed to build and maintain the campaigns. On the other hand, privacy preservation is an essential component of any recommendation system. This is due to the fact that recommendation relies on the collection and analysis of user data [175]. Without proper privacy measures, user data can be easily exposed to malicious actors, leading to privacy violations and potential data misuse [176]. Therefore, FRSs must employ privacy measures such as data anonymization, data encryption, and access control in order to ensure the privacy of users.

4.6. E-Commerce

E-commerce is the buying and selling products and services over the Internet [125]. It enables customers to access a wide range of products, services, and information from businesses worldwide. The increase in E-commerce activity has led to an increased usage of recommendation systems [177,178]. To this end, FRSs can allow different data sources to collaborate in order to provide personalized recommendations to customers. A literature review on the application of FRSs in E-commerce revealed the various advantages [179–181]. First, FRSs can help reduce the cost of data access and storage. By sharing data across different sources, FRSs can provide a more efficient and cost-effective way of accessing and storing data. Furthermore, FRSs can improve the accuracy of recommendations by providing more relevant and personalized recommendations [182]. This can increase customers' satisfaction and loyalty by providing customers with better recommendations that are tailored to their individual needs.

5. Publicly Available Datasets

This section provides a list of publicly available datasets for FRSs. These datasets cover a wide range of topics, including movie ratings, TV show ratings, music tastes, consumer preferences, and more. Each dataset has been carefully curated to contain relevant information for developing FRSs. Those datasets are available for free download and can be used to train and test the performance of FRSs. In Table 5, we show the list of those datasets and discuss the details in the following subsections.

Table 5. Publicly available datasets that can be used for the development of FRSs.

Name	Category	Variables	Data Type	License	Format
Amazon [183]	Reviews	Users, Reviews	Text, Numeric	Open-Source	CSV
MovieLens [184]	Movies	Ratings, Genres	Numeric	Open-Source	CSV
Yelp [185]	Reviews	Users, Reviews	Text, Numeric	Open-Source	JSON
Film Trust [186]	Movies	Ratings, Genres	Numeric	Open-Source	CSV
Goodreads [187]	Books	Reviews, Ratings	Text, Numeric	Open-Source	XML
Netflix [188]	Movies	Ratings, Genres	Numeric	Open-Source	JSON
LastFM [189]	Music	Listeners, Genres	Numeric	Open-Source	CSV
Douban [190]	Movies/Books	Reviews, Ratings	Text, Numeric	Open-Source	XML
BookCrossing [191]	Books	Reviews, Ratings	Text, Numeric	Open-Source	XML

5.1. Amazon Reviews Dataset

The Amazon Reviews dataset is a set of data collected from customers who have purchased products from the Amazon platform. These data can be used to create an FRS that can accurately predict what products a user might be interested in based on his/her past purchase and browsing behaviors. The Amazon Reviews dataset provides the necessary data needed to create a robust FRS that can recommend relevant products to users.

5.2. MovieLens Dataset

The MovieLens dataset is a popular dataset used for collaborative filtering. The dataset comprises ratings from over 20 million users for more than 10,000 movies. It contains ratings from 0.5 to 5, with 0.5 being the lowest and 5 being the highest. In terms of FRSs, the MovieLens dataset is used to provide users with personalized movie recommendations based on the ratings of other users. It does this by considering the similarity between users and the ratings they have given to the movies. For example, if User A and User B both rated a particular movie highly, then it is likely that the system would recommend that movie to both users. This is performed by calculating the similarity between users and their ratings and then identifying movies that are popular among users with similar tastes.

5.3. Yelp Dataset

The Yelp dataset is a publicly available dataset that contains reviews, ratings, and other metadata related to businesses and services. It is a popular data source for recommendation systems, both in the context of federated learning and non-federated learning. In an FRS, the Yelp dataset can be used to build personalized user recommendations. Specifically, the dataset can be used to build a collaborative filtering model that considers user preferences and item ratings. The collaborative filtering model can then create personalized user recommendations based on his/her preferences and other related factors.

5.4. Film Trust Dataset

The Film Trust dataset is a collection of data about user ratings and preferences for movies. It was developed as part of the Netflix Prize competition and can be used to build an FRS. The dataset contains movie ratings from over 500,000 users. Each user rated at least 20 movies, and the ratings range from 1 to 5 stars. The dataset also includes user movie preferences and demographic information. The demographic information includes gender, age, zip code, and occupation. In the case of FRSs, the system allows users to share their ratings and preferences, and the system can then use these data to make recommendations. For example, if a user shares his/her ratings and preferences with his/her peers, the system can recommend other movies that the user may be interested in.

5.5. Goodreads Dataset

The Goodreads dataset is a dataset of book ratings and reviews from the popular book recommendation website, Goodreads. The dataset contains over 6 million user-generated ratings of and reviews on books, authors, and other related items, as well as over 1 million user-generated book reviews. This dataset can be useful for FRSs because it allows for the creation of personalized recommendations that are tailored to the interests of each user. The dataset also includes information about the books, authors, and reviews so that the FRS can provide personalized recommendations based on the user's interests.

5.6. Netflix Dataset

The Netflix dataset is a collection of user ratings of movies in the Netflix library. It can be used for creating an FRS, which allows users to make recommendations to one another without revealing their individual preferences. The dataset comprises over 20 million ratings from over 480,000 users for over 17,000 movies. The data are provided in a matrix containing users, movies, and their ratings. This allows for creating a collaborative filtering system, where users can make recommendations to one another based on the ratings

they have given to movies. Moreover, this dataset provides additional information, such as release year, genre, and user age, which can be used to build a more personalized recommendation system.

5.7. LastFM Dataset

The LastFM Dataset is a collection of user-generated music-listening data from the Last.fm online music service. The dataset is well suited for FRSs, as it contains large amounts of user-specific music-listening data from various users. These data can create personalized recommendations for users, as they are more likely to be interested in music similar to what they have already listened to. The dataset includes user IDs, the artist name, the release name, the song title, the album name, the number of plays, and the timestamp when the song was played. These data can be used to create more detailed recommendations for each user. By analyzing the number of plays and the timestamp of each song, the system can identify which songs are most-popular among users and make recommendations accordingly.

5.8. Douban Dataset

The Douban dataset is a large collection of user-generated content from the popular Chinese social networking site Douban. It is a useful resource for FRSs, providing a rich data source for understanding user preferences and behaviors. The dataset contains user ratings, reviews, and tags for movies, books, and music. It also contains user profiles, including age, gender, location, and occupation. All this information can be used to build a robust FRS.

5.9. BookCrossing Dataset

The BookCrossing dataset is a collection of user ratings and book ratings from a website called BookCrossing. It is composed of three tables: BX-Books, BX-Users, and BX-Book-Ratings. The BX-Books table contains the ISBN, title, author, and publisher information for the books that have been rated by the users. The BX-Users table contains the users' information, including their age, location, and book ratings. The BX-Book-Ratings table contains the ratings that the users have given to each book. The BookCrossing dataset is a great resource for training an FRS, as the system can use the ratings from multiple users to create a personalized recommendation for each user.

6. Future Directions and Real-World Challenges

In this section, we discuss the need for further research and development in order to optimize the effectiveness of FRS. We first show the existing limitations, issues, and challenges in Table 6. Then, we look at the potential challenges that need to be overcome for FRS to be implemented successfully. In Figure 7, we show the overview of future directions while we discuss the details of them in the following subsections.

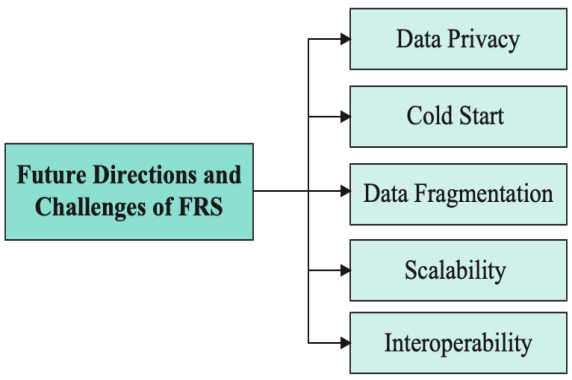

Figure 7. Directions that should be followed in FRSs for future developments.

Table 6. Current security protocols, limitations, issues, and challenges in FRSs.

System	Security Protocols	Limitations	Issues and Challenges
Content-Based Filtering	Secure aggregation	Data privacy and security concerns	Develop more scalable and efficient secure aggregation methods, improve data sharing protocols
Knowledge-Based Systems	Access control and authorization	Limited scalability, reduced accuracy	Lack of data for knowledge-based models
Collaborative Filtering	Access control, authentication	Data privacy and security concerns	The reliability of data between different parties
Context-Aware Recommendation	Secure aggregation, authentication, and authorization	High computational overhead	Lack of data for context-aware models
Hybrid Recommendation Systems	Access control, authentication, authorization	High computational overhead, reduced accuracy	Improve scalability, develop secure aggregation methods, explore privacy-preserving MPC techniques

6.1. Data Privacy

- **Future directions**: Data privacy is an increasingly important issue in FRSs. In order to ensure that all users' data are secure, FRSs must have security protocols in place for exchanging data between different organizations. These protocols should be designed to protect user privacy by preventing unauthorized access to user data and by allowing users to control with whom their data are shared. In addition, the FRS must take steps to ensure that user data are not misused or abused. This could include implementing policies and procedures for data security and monitoring, as well as developing technologies to detect any unauthorized access or misuse of user data.
- **Real-world challenges**: A major challenge for FRSs is ensuring that user data are secure, both in terms of the data exchanged between different organizations and the data stored on each organization's servers. To address this challenge, FRSs must ensure that all data exchanged between different organizations are encrypted, secure, and adequately protected. Besides, the system must ensure that each organization's servers are secure and that all user data are stored in a secure manner that prevents unauthorized access or misuse.

6.2. Cold Start Problem

The cold start problem is a challenge faced by FRSs when providing accurate and personalized recommendations. This problem arises when there are no existing data available to predict user preferences accurately. Without these data, the system cannot make accurate recommendations and may default to providing generic suggestions. As a result, users may be less likely to engage with the system, leading to a decrease in customer satisfaction:

- **Future directions**: These may include collecting more user data, such as preferences, likes, and dislikes, and implementing techniques such as collaborative filtering that allow the system to draw connections between similar users and their preferences. Moreover, techniques such as deep learning may be used to understand user behavior better. The FRS may also benefit from integrating external data sources, such as social media, from personalizing the user experience further.
- **Real-world challenges**: These include protecting user privacy, balancing accuracy and complexity, and ensuring scalability. To ensure user privacy, FRSs must be designed with privacy-preserving techniques in mind. The complexity of the model must be balanced with its accuracy, as complex models may be difficult to interpret and may not be able to predict user preferences accurately. Finally, the system must be able

to handle large amounts of data when scaling, as more data will allow for more accurate predictions.

6.3. Data Fragmentation

The use of FRSs is becoming increasingly popular due to the fact that they enable organizations to manage and store data in a distributed manner without compromising privacy. However, when data are stored in a distributed manner, there is a risk of data fragmentation. Data fragmentation occurs when the data are split into pieces and stored in different locations. This can cause problems with accessing and utilizing the data, as well as with data consistency:

- **Future directions**: To address the issue of data fragmentation, research should focus on approaches to facilitate seamless data transfer between different locations and to ensure that the data are consistent and up-to-date. This could include the development of distributed databases, distributed query processing, and distributed data analytics. Moreover, research should focus on developing methods for federated learning with fragmented data. These methods should aim to reduce the computational cost of training models and improve the accuracy of the models.
- **Real-world challenges**: Data fragmentation can be a significant challenge in FRSs, as it can lead to inconsistent data and can make it difficult to access and utilize the data. In addition, privacy concerns may prevent the data from being shared across different locations, further exacerbating the problem of data fragmentation. As such, organizations will need to develop policies and technologies to facilitate data transfer and to ensure that the data are consistent and up-to-date. Moreover, organizations will need to ensure the security of the data and protect the privacy of users.

6.4. Scalability Issues

FRSs hold great promise for improving the quality and accuracy of personalized recommendations, but they can also be difficult to scale. As the number of sources and users grows, the complexity of managing data across multiple sources and ensuring the accuracy of recommendations can become increasingly difficult:

- **Future directions**: In order to address the scalability issues associated with FRSs, researchers are developing improved methods for managing and processing data across multiple sources. This includes optimizing algorithms to reduce the number of data transfers, as well as utilizing distributed computing architectures and artificial intelligence to manage data better. In addition, researchers must continue to explore methods of improving the accuracy of federated recommendations, such as using transfer learning, ensemble learning, and other latest machine learning techniques.
- **Real-world challenges**: There are scalability concerns about data privacy and security, as well as the need for robust methods for managing user profiles and managing conflicts between multiple sources. Moreover, as federated systems become more complex and involve more stakeholders, it will be important to develop governance models and mechanisms for cooperation among the different parties involved.

6.5. Lack of Interoperability

Interoperability is the ability of different systems to work together and exchange information. Without interoperability, FRSs would be unable to share information, limiting their effectiveness. This could lead to a lack of the personalization and accuracy of recommendations. Moreover, this would create a barrier between users and their data, making it difficult for them to find the most-relevant content.

- **Future directions**: These may include developing standards and protocols for data exchange between systems, as well as utilizing open-source solutions that allow different systems to communicate with each other. In addition, developing technologies

such as blockchain could provide solutions to ensure data privacy and security while allowing interoperability.

- **Real-world challenges**: The main challenge in achieving interoperability in FRSs is the need for systems to be able to share data without compromising privacy or security. Moreover, different systems may have different data formats, making it difficult for them to communicate with each other. Developing standards and protocols for data exchange could help address this challenge, as could the development of open-source solutions. In addition, ensuring data privacy and security in federated systems could be a difficult task, as data may need to be shared between different systems. Utilizing blockchain technology could help address this challenge, allowing for secure data sharing while ensuring privacy.

7. Conclusions

This paper discussed the potential of federated recommendation systems for protecting user privacy while allowing organizations to benefit from the data they share. We explored how federated recommendation systems allow for secure data sharing and collaboration in the context of big data. In addition, we identified the challenges associated with developing and deploying these systems in the real world. With the increasing demand for privacy, federated recommendation systems provide a powerful tool for protecting user data while allowing organizations to benefit from the data they share. With the right tools and practices in place, federated recommendation systems can help organizations navigate the complex landscape of data privacy.

Author Contributions: Methodology, M.A.; Validation, S.S.; Writing—original draft, M.A.; Writing—review & editing, M.A., S.S., and J.N.; Visualization, E.J.; Supervision, M.T.; Project administration, E.J., and J.N.; Funding acquisition, M.T. All authors have read and agreed to the published version of the manuscript.

Funding: These research results were obtained from the commissioned research by the National Institute of Information and Communications Technology (NICT), Japan.

Conflicts of Interest: The authors declare no conflict of interest regarding the publication of this research article.

References

1. Fayyaz, Z.; Ebrahimian, M.; Nawara, D.; Ibrahim, A.; Kashef, R. Recommendation systems: Algorithms, challenges, metrics, and business opportunities. *Appl. Sci.* **2020**, *10*, 7748. [CrossRef]
2. Naumov, M.; Mudigere, D.; Shi, H.J.M.; Huang, J.; Sundaraman, N.; Park, J.; Wang, X.; Gupta, U.; Wu, C.J.; Azzolini, A.G.; et al. Deep learning recommendation model for personalization and recommendation systems. *arXiv* **2019**, arXiv:1906.00091.
3. Ko, H.; Lee, S.; Park, Y.; Choi, A. A survey of recommendation systems: Recommendation models, techniques, and application fields. *Electronics* **2022**, *11*, 141. [CrossRef]
4. Himeur, Y.; Sayed, A.; Alsalemi, A.; Bensaali, F.; Amira, A.; Varlamis, I.; Eirinaki, M.; Sardianos, C.; Dimitrakopoulos, G. Blockchain-based recommender systems: Applications, challenges and future opportunities. *Comput. Sci. Rev.* **2022**, *43*, 100439. [CrossRef]
5. Deldjoo, Y.; Jannach, D.; Bellogin, A.; Difonzo, A.; Zanzonelli, D. A survey of research on fair recommender systems. *arXiv* **2022**, arXiv:2205.11127.
6. Huang, J.; Tong, Z.; Feng, Z. Geographical POI recommendation for Internet of Things: A federated learning approach using matrix factorization. *Int. J. Commun. Syst.* **2022**, e5161. [CrossRef]
7. Jeong, W.h.; Kim, S.j.; Park, D.s.; Kwak, J. Performance improvement of a movie recommendation system based on personal propensity and secure collaborative filtering. *J. Inf. Process. Syst.* **2013**, *9*, 157–172. [CrossRef]
8. Di Noia, T.; Tintarev, N.; Fatourou, P.; Schedl, M. Recommender systems under European AI regulations. *Commun. ACM* **2022**, *65*, 69–73. [CrossRef]
9. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; y Arcas, B.A. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the Artificial Intelligence and Statistics, Lauderdale, FL, USA, 20–22 April 2017; pp. 1273–1282.
10. Yang, L.; Tan, B.; Zheng, V.W.; Chen, K.; Yang, Q. Federated recommendation systems. In *Federated Learning: Privacy and Incentive*; Springer: Cham, Switzerland, 2020; pp. 225–239.
11. Chen, Z.; Sun, F.; Tang, Y.; Chen, H.; Gao, J.; Ding, B. Studying the impact of data disclosure mechanism in recommender systems via simulation. *ACM Trans. Inf. Syst.* **2023**, *41*, 1–26. [CrossRef]

12. Anelli, V.W.; Di Noia, T.; Di Sciascio, E.; Ferrara, A.; Mancino, A.C.M. Addressing Privacy in Recommender Systems with Federated Learning. In Proceedings of the IIR2022: 12th Italian Information Retrieval Workshop, Milan, Italy, 29–30 June 2022.
13. Zhang, B.; Wang, N.; Jin, H. Privacy concerns in online recommender systems: Influences of control and user data input. In Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS 2014), Menlo Park, CA, USA, 9–11 July 2014; pp. 159–173.
14. Pu, P.; Chen, L.; Hu, R. Evaluating recommender systems from the user's perspective: Survey of the state of the art. *User Model. User-Adapt. Interact.* **2012**, *22*, 317–355. [CrossRef]
15. Knijnenburg, B.P.; Willemsen, M.C.; Gantner, Z.; Soncu, H.; Newell, C. Explaining the user experience of recommender systems. *User Model. User-Adapt. Interact.* **2012**, *22*, 441–504. [CrossRef]
16. Lin, W.; Leng, H.; Dou, R.; Qi, L.; Pan, Z.; Rahman, M.A. A federated collaborative recommendation model for privacy-preserving distributed recommender applications based on microservice framework. *J. Parallel Distrib. Comput.* **2023**, *174*, 70–80. [CrossRef]
17. Yuan, W.; Yang, C.; Nguyen, Q.V.H.; Cui, L.; He, T.; Yin, H. Interaction-level Membership Inference Attack Against Federated Recommender Systems. *arXiv* **2023**, arXiv:2301.10964.
18. Zhang, S.; Yin, H. Comprehensive Privacy Analysis on Federated Recommender System against Attribute Inference Attacks. *arXiv* **2022**, arXiv:2205.11857.
19. Li, T.; Sahu, A.K.; Talwalkar, A.; Smith, V. Federated learning: Challenges, methods, and future directions. *IEEE Signal Process. Mag.* **2020**, *37*, 50–60. [CrossRef]
20. Yang, Q.; Liu, Y.; Chen, T.; Tong, Y. Federated machine learning: Concept and applications. *ACM Trans. Intell. Syst. Technol. (TIST)* **2019**, *10*, 1–19. [CrossRef]
21. Adomavicius, G.; Tuzhilin, A. Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. *IEEE Trans. Knowl. Data Eng.* **2005**, *17*, 734–749. [CrossRef]
22. Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Huang, Y.; Dehghantanha, A.; Srivastava, G. A survey on security and privacy of federated learning. *Future Gener. Comput. Syst.* **2021**, *115*, 619–640. [CrossRef]
23. Lyu, L.; Yu, H.; Ma, X.; Chen, C.; Sun, L.; Zhao, J.; Yang, Q.; Philip, S.Y. Privacy and robustness in federated learning: Attacks and defenses. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**. [CrossRef]
24. Ali, W.; Kumar, R.; Deng, Z.; Wang, Y.; Shao, J. A federated learning approach for privacy protection in context-aware recommender systems. *Comput. J.* **2021**, *64*, 1016–1027. [CrossRef]
25. Tan, B.; Liu, B.; Zheng, V.; Yang, Q. A federated recommender system for online services. In Proceedings of the 14th ACM Conference on Recommender Systems, Virtual Event, 22–26 September 2020; pp. 579–581.
26. Zhang, C.; Xie, Y.; Bai, H.; Yu, B.; Li, W.; Gao, Y. A survey on federated learning. *Knowl.-Based Syst.* **2021**, *216*, 106775. [CrossRef]
27. Teimoori, Z.; Yassine, A.; Hossain, M.S. A secure cloudlet-based charging station recommendation for electric vehicles empowered by federated learning. *IEEE Trans. Ind. Inform.* **2022**, *18*, 6464–6473. [CrossRef]
28. Kalloori, S.; Klingler, S. Horizontal cross-silo federated recommender systems. In Proceedings of the 15th ACM Conference on Recommender Systems, Amsterdam, The Netherlands, 27 September–1st October 2021; pp. 680–684.
29. Liu, S. Multi-Dimensional Federated Learning in Recommender Systems. Ph.D. Thesis, Rutgers University-School of Graduate Studies, New Brunswick, NJ, USA, 2022.
30. Neumann, D.; Lutz, A.; Müller, K.; Samek, W. A Privacy Preserving System for Movie Recommendations using Federated Learning. *arXiv* **2023**, arXiv:2303.04689.
31. Du, Y.; Zhou, D.; Xie, Y.; Shi, J.; Gong, M. Federated matrix factorization for privacy-preserving recommender systems. *Appl. Soft Comput.* **2021**, *111*, 107700. [CrossRef]
32. Martins, G.B.; Papa, J.P.; Adeli, H. Deep learning techniques for recommender systems based on collaborative filtering. *Expert Syst.* **2020**, *37*, e12647. [CrossRef]
33. Banabilah, S.; Aloqaily, M.; Alsayed, E.; Malik, N.; Jararweh, Y. Federated learning review: Fundamentals, enabling technologies, and future applications. *Inf. Process. Manag.* **2022**, *59*, 103061. [CrossRef]
34. Wang, Y.; Tian, Y.; Yin, X.; Hei, X. A trusted recommendation scheme for privacy protection based on federated learning. *CCF Trans. Netw.* **2020**, *3*, 218–228. [CrossRef]
35. Imran, M.; Yin, H.; Chen, T.; Nguyen, Q.V.H.; Zhou, A.; Zheng, K. ReFRS: Resource-efficient federated recommender system for dynamic and diversified user preferences. *ACM Trans. Inf. Syst.* **2023**, *41*, 1–30. [CrossRef]
36. Zenebe, A.; Norcio, A.F. Representation, similarity measures and aggregation methods using fuzzy sets for content-based recommender systems. *Fuzzy Sets Syst.* **2009**, *160*, 76–94. [CrossRef]
37. Bhatti, U.A.; Huang, M.; Wu, D.; Zhang, Y.; Mehmood, A.; Han, H. Recommendation system using feature extraction and pattern recognition in clinical care systems. *Enterp. Inf. Syst.* **2019**, *13*, 329–351. [CrossRef]
38. Kurt, Z.; Özkan, K. An image-based recommender system based on feature extraction techniques. In Proceedings of the 2017 International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 5–8 October 2017; pp. 769–774.
39. Lü, L.; Medo, M.; Yeung, C.H.; Zhang, Y.C.; Zhang, Z.K.; Zhou, T. Recommender systems. *Phys. Rep.* **2012**, *519*, 1–49. [CrossRef]
40. Jalalirad, A.; Scavuzzo, M.; Capota, C.; Sprague, M. A simple and efficient federated recommender system. In Proceedings of the 6th IEEE/ACM International Conference on Big Data Computing, Applications and Technologies, Auckland, New Zealand, 2–5 December 2019; pp. 53–58.

41. Anelli, V.W.; Deldjoo, Y.; Di Noia, T.; Ferrara, A.; Narducci, F. Federank: User controlled feedback with federated recommender systems. In Proceedings of the Advances in Information Retrieval: 43rd European Conference on IR Research, ECIR 2021, Virtual Event, March 28–April 1, 2021; Proceedings, Part I 43; Springer: Berlin/Heidelberg, Germany, 2021; pp. 32–47.
42. Khan, F.K.; Flanagan, A.; Tan, K.E.; Alamgir, Z.; Ammad-Ud-Din, M. A payload optimization method for federated recommender systems. In Proceedings of the 15th ACM Conference on Recommender Systems, Amsterdam, The Netherlands, 27 September–1st October 2021; pp. 432–442.
43. Jie, Z.; Chen, S.; Lai, J.; Arif, M.; He, Z. Personalized federated recommendation system with historical parameter clustering. *J. Ambient. Intell. Humaniz. Comput.* **2022**, 1–11. [CrossRef]
44. Chen, H.; Fu, C.; Hu, C. An efficient and secure recommendation system based on federated matrix factorization in digital economy. *Pers. Ubiquitous Comput.* **2022**, 1–12. [CrossRef]
45. Huang, M.; Li, H.; Bai, B.; Wang, C.; Bai, K.; Wang, F. A federated multi-view deep learning framework for privacy-preserving recommendations. *arXiv* **2020**, arXiv:2008.10808.
46. Alamgir, Z.; Khan, F.K.; Karim, S. Federated recommenders: Methods, challenges and future. *Clust. Comput.* **2022**, *25*, 4075–4096. [CrossRef]
47. Wang, D.; Liang, Y.; Xu, D.; Feng, X.; Guan, R. A content-based recommender system for computer science publications. *Knowl.-Based Syst.* **2018**, *157*, 1–9. [CrossRef]
48. Qin, Y.; Li, M.; Zhu, J. Privacy-preserving federated learning framework in multimedia courses recommendation. *Wirel. Netw.* **2023**, *29*, 1535–1544. [CrossRef]
49. Albayati, A.N.K.; Ortakci, Ö.Ü.Y. Recommendation Systems on Twitter Data for Marketing Purposes using Content-Based Filtering. In Proceedings of the 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 9–11 June 2022; pp. 1–5.
50. Huang, W.; Liu, J.; Li, T.; Ji, S.; Wang, D.; Huang, T. FedCKE: Cross-Domain Knowledge Graph Embedding in Federated Learning. *IEEE Trans. Big Data* **2022**, *9*, 792–804. [CrossRef]
51. Eren, M.E.; Richards, L.E.; Bhattarai, M.; Yus, R.; Nicholas, C.; Alexandrov, B.S. FedSPLIT: One-Shot Federated Recommendation System Based on Non-negative Joint Matrix Factorization and Knowledge Distillation. *arXiv* **2022**, arXiv:2205.02359.
52. Hejazinia, M.; Huba, D.; Leontiadis, I.; Maeng, K.; Malek, M.; Melis, L.; Mironov, I.; Nasr, M.; Wang, K.; Wu, C.J. Fel: High capacity learning for recommendation and ranking via federated ensemble learning. *arXiv* **2022**, arXiv:2206.03852.
53. Wazzeh, M.; Ould-Slimane, H.; Talhi, C.; Mourad, A.; Guizani, M. Warmup and Transfer Knowledge-Based Federated Learning Approach for IoT Continuous Authentication. *arXiv* **2022**, arXiv:2211.05662.
54. Chen, P.; Du, X.; Lu, Z.; Wu, J.; Hung, P.C. Evfl: An explainable vertical federated learning for data-oriented artificial intelligence systems. *J. Syst. Archit.* **2022**, *126*, 102474. [CrossRef]
55. Perifanis, V.; Efraimidis, P.S. Federated neural collaborative filtering. *Knowl.-Based Syst.* **2022**, *242*, 108441. [CrossRef]
56. Hu, P.; Yang, E.; Pan, W.; Peng, X.; Ming, Z. Federated one-class collaborative filtering via privacy-aware non-sampling matrix factorization. *Knowl.-Based Syst.* **2022**, *253*, 109441. [CrossRef]
57. Eren, M.E.; Bhattarai, M.; Solovyev, N.; Richards, L.E.; Yus, R.; Nicholas, C.; Alexandrov, B.S. One-Shot Federated Group Collaborative Filtering. In Proceedings of the 2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA), Nassau, Bahamas, 12–14 December 2022.
58. Anelli, V.W.; Deldjoo, Y.; Di Noia, T.; Ferrara, A.; Narducci, F. User-controlled federated matrix factorization for recommender systems. *J. Intell. Inf. Syst.* **2022**, *58*, 287–309. [CrossRef]
59. Zhou, Y.; Liu, J.; Wang, J.H.; Wang, J.; Liu, G.; Wu, D.; Li, C.; Yu, S. Usst: A two-phase privacy-preserving framework for personalized recommendation with semi-distributed training. *Inf. Sci.* **2022**, *606*, 688–701. [CrossRef]
60. Luo, J.; Yi, X.; Han, F.; Yang, X. An efficient privacy-preserving recommender system in wireless networks. *Wirel. Netw.* **2022**, 1–12. [CrossRef]
61. Huang, H.; Li, R.; Liu, J.; Zhou, S.; Lin, K.; Zheng, Z. Contextfl: Context-aware federated learning by estimating the training and reporting phases of mobile clients. In Proceedings of the 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS), Bologna, Italy, 10–13 July 2022; pp. 570–580.
62. Latif, S.; Nayyer, M.Z.; Raza, I.; Hussain, S.A.; Jamal, M.H.; Hur, S.; Ashraf, I. Cloudlet Federation Based Context-Aware Federated Learning Approach. *IEEE Access* **2022**, *10*, 109153–109166. [CrossRef]
63. Chagas, A.B. A Recommender System to Support the Development of Context-Aware Intelligent Transportation Systems. 2022. Available online: https://repositorio.ufpe.br/handle/123456789/46362 (accessed on 29 March 2023).
64. Ali, W.; Kumar, J.; Mawuli, C.B.; She, L.; Shao, J. Dynamic context management in context-aware recommender systems. *Comput. Electr. Eng.* **2023**, *107*, 108622. [CrossRef]
65. Qu, Z.; Duan, R.; Chen, L.; Xu, J.; Lu, Z.; Liu, Y. Context-aware online client selection for hierarchical federated learning. *IEEE Trans. Parallel Distrib. Syst.* **2022**, *33*, 4353–4367. [CrossRef]
66. Garcıa-Alonso, J.; Murillo, J.M.; Berrocal, J. Towards Proactive Context-Aware IoT Environments by Means of Federated Learning. In Proceedings of the ICWE 2021 Workshops: ICWE 2021 International Workshops, BECS and Invited Papers, Biarritz, France, 18–21 May 2021; Revised Selected Papers; Springer Nature: Cham, Switzlerland, 2022; p. 27.
67. Rentero-Trejo, R.; Flores-Martín, D.; Galán-Jiménez, J.; García-Alonso, J.; Murillo, J.M.; Berrocal, J. Using Federated Learning to Achieve Proactive Context-Aware IoT Environments. *J. Web Eng.* **2022**, *21*, 53–74. [CrossRef]

68. Raza, S.; Ding, C. Progress in context-aware recommender systems—An overview. *Comput. Sci. Rev.* **2019**, *31*, 84–97. [CrossRef]
69. Sharma, S.; Rana, V.; Malhotra, M. Automatic recommendation system based on hybrid filtering algorithm. *Educ. Inf. Technol.* **2022**, *27*, 1523–1538. [CrossRef]
70. Walek, B.; Fajmon, P. A hybrid recommender system for an online store using a fuzzy expert system. *Expert Syst. Appl.* **2023**, *212*, 118565. [CrossRef]
71. Seth, R.; Sharaff, A. A Comparative Overview of Hybrid Recommender Systems: Review, Challenges, and Prospects. *Data Min. Mach. Learn. Appl.* **2022**, *3*, 57–98.
72. Wu, C.; Wu, F.; Cao, Y.; Huang, Y.; Xie, X. Fedgnn: Federated graph neural network for privacy-preserving recommendation. *arXiv* **2021**, arXiv:2102.04925.
73. Chai, D.; Wang, L.; Chen, K.; Yang, Q. Secure federated matrix factorization. *IEEE Intell. Syst.* **2020**, *36*, 11–20. [CrossRef]
74. Shen, S.; Zhu, T.; Wu, D.; Wang, W.; Zhou, W. From distributed machine learning to federated learning: In the view of data privacy and security. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e6002. [CrossRef]
75. Asad, M.; Moustafa, A.; Yu, C. A critical evaluation of privacy and security threats in federated learning. *Sensors* **2020**, *20*, 7182. [CrossRef]
76. Dash, B.; Sharma, P.; Ali, A. Federated Learning for Privacy-Preserving: A Review of PII Data Analysis in Fintech. *Int. J. Softw. Eng. Appl. IJSEA* **2022**, *13*. [CrossRef]
77. Yang, E.; Huang, Y.; Liang, F.; Pan, W.; Ming, Z. FCMF: Federated collective matrix factorization for heterogeneous collaborative filtering. *Knowl.-Based Syst.* **2021**, *220*, 106946. [CrossRef]
78. Li, Z.; Ding, B.; Zhang, C.; Li, N.; Zhou, J. Federated matrix factorization with privacy guarantee. *Proc. VLDB Endow.* **2021**, *15*, 900–913. [CrossRef]
79. Truex, S.; Liu, L.; Chow, K.H.; Gursoy, M.E.; Wei, W. LDP-Fed: Federated learning with local differential privacy. In Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking, Heraklion, Greece, 27 April 2020; pp. 61–66.
80. Zheng, X.; Guan, M.; Jia, X.; Guo, L.; Luo, Y. A Matrix Factorization Recommendation System-Based Local Differential Privacy for Protecting Users' Sensitive Data. *IEEE Trans. Comput. Soc. Syst.* **2022**. [CrossRef]
81. Wang, Y.; Gao, M.; Ran, X.; Ma, J.; Zhang, L.Y. An improved matrix factorization with local differential privacy based on piecewise mechanism for recommendation systems. *Expert Syst. Appl.* **2023**, *216*, 119457. [CrossRef]
82. Zheng, H.; Hu, H.; Han, Z. Preserving user privacy for machine learning: Local differential privacy or federated machine learning? *IEEE Intell. Syst.* **2020**, *35*, 5–14. [CrossRef]
83. Rodríguez-Barroso, N.; Stipcich, G.; Jiménez-López, D.; Ruiz-Millán, J.A.; Martínez-Cámara, E.; González-Seco, G.; Luzón, M.V.; Veganzones, M.A.; Herrera, F. Federated Learning and Differential Privacy: Software tools analysis, the Sherpa. ai FL framework and methodological guidelines for preserving data privacy. *Inf. Fusion* **2020**, *64*, 270–292. [CrossRef]
84. Hu, H.; Dobbie, G.; Salcic, Z.; Liu, M.; Zhang, J.; Lyu, L.; Zhang, X. Differentially private locality sensitive hashing based federated recommender system. *Concurr. Comput. Pract. Exp.* **2021**, e6233. [CrossRef]
85. Hou, D.; Zhang, J.; Ma, J.; Zhu, X.; Man, K.L. Application of Differential Privacy for Collaborative Filtering Based Recommendation System: A Survey. In Proceedings of the 2021 12th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Xi'an, China, 10–12 December 2021; pp. 97–101.
86. Kanagavelu, R.; Wei, Q.; Li, Z.; Zhang, H.; Samsudin, J.; Yang, Y.; Goh, R.S.M.; Wang, S. CE-Fed: Communication efficient multi-party computation enabled federated learning. *Array* **2022**, *15*, 100207. [CrossRef]
87. Byrd, D.; Polychroniadou, A. Differentially private secure multi-party computation for federated learning in financial applications. In Proceedings of the First ACM International Conference on AI in Finance, New York, NY, USA, 15–16 October 2020; pp. 1–9.
88. Wang, Y.; Tong, Y.; Shi, D. Federated latent dirichlet allocation: A local differential privacy based framework. In Proceedings of the AAAI Conference on Artificial Intelligence, New York, NY, USA, 7–12 February 2020; Volume 34, pp. 6283–6290.
89. Zhou, J.; Feng, Y.; Wang, Z.; Guo, D. Using secure multi-party computation to protect privacy on a permissioned blockchain. *Sensors* **2021**, *21*, 1540. [CrossRef]
90. Tran, A.T.; Luong, T.D.; Karnjana, J.; Huynh, V.N. An efficient approach for privacy preserving decentralized deep learning models based on secure multi-party computation. *Neurocomputing* **2021**, *422*, 245–262. [CrossRef]
91. Bonawitz, K.; Ivanov, V.; Kreuter, B.; Marcedone, A.; McMahan, H.B.; Patel, S.; Ramage, D.; Segal, A.; Seth, K. Practical secure aggregation for privacy-preserving machine learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 1175–1191.
92. Soni, K.; Panchal, G. Data security in recommendation system using homomorphic encryption. In *Proceedings of the Information and Communication Technology for Intelligent Systems (ICTIS 2017)*; Springer: Cham, Switzerland, 2018; Volume 1, pp. 308–313.
93. Ou, W.; Zeng, J.; Guo, Z.; Yan, W.; Liu, D.; Fuentes, S. A homomorphic-encryption-based vertical federated learning scheme for rick management. *Comput. Sci. Inf. Syst.* **2020**, *17*, 819–834. [CrossRef]
94. Mahmood, Z.H.; Ibrahem, M.K. New fully homomorphic encryption scheme based on multistage partial homomorphic encryption applied in cloud computing. In Proceedings of the 2018 1st Annual International Conference on Information and Sciences (AiCIS), Fallujah, Iraq, 20–21 November 2018; pp. 182–186.
95. Kim, S.; Kim, J.; Koo, D.; Kim, Y.; Yoon, H.; Shin, J. Efficient privacy-preserving matrix factorization via fully homomorphic encryption. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, Xi'an, China, 30 May–June 3 2016; pp. 617–628.

96. Badsha, S.; Yi, X.; Khalil, I.; Bertino, E. Privacy preserving user-based recommender system. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; pp. 1074–1083.
97. Wang, L.; Wang, Y.; Bai, Y.; Liu, P.; Li, X. POI recommendation with federated learning and privacy preserving in cross domain recommendation. In Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Virtual, 9–12 May 2021; pp. 1–6.
98. Zhang, S.; Li, Z.; Chen, Q.; Zheng, W.; Leng, J.; Guo, M. Dubhe: Towards data unbiasedness with homomorphic encryption in federated learning client selection. In Proceedings of the 50th International Conference on Parallel Processing, Lemont, IL, USA, 9–12 August 2021; pp. 1–10.
99. Han, J.; Khan, A.F.; Zawad, S.; Anwar, A.; Angel, N.B.; Zhou, Y.; Yan, F.; Butt, A.R. Tokenized incentive for federated learning. In Proceedings of the Federated Learning Workshop at the Association for the Advancement of Artificial Intelligence (AAAI) Conference, Qinghai, China, 15–20 July 2022.
100. Bagdasaryan, E.; Song, C.; van Dalen, R.; Seigel, M.; Cahill, Á. Training a Tokenizer for Free with Private Federated Learning. *arXiv* **2022**, arXiv:2203.09943.
101. Hathurusinghe, R.; Nejadgholi, I.; Bolic, M. A privacy-preserving approach to extraction of personal information through automatic annotation and federated learning. *arXiv* **2021**, arXiv:2105.09198.
102. Pandey, S.R.; Nguyen, L.D.; Popovski, P. FedToken: Tokenized Incentives for Data Contribution in Federated Learning. *arXiv* **2022**, arXiv:2209.09775.
103. Bandara, E.; Liang, X.; Shetty, S.; Mukkamala, R.; Rahman, A.; Keong, N.W. Indy528—Federated Learning Model Tokenization with Non-Fungible Tokens (NFT) and Model Cards. In Proceedings of the 2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS), Denver, CO, USA, 19–23 October; pp. 195–201.
104. Nguyen, J.; Wang, J.; Malik, K.; Sanjabi, M.; Rabbat, M. Where to Begin? On the Impact of Pre-Training and Initialization in Federated Learning. *arXiv* **2022**, arXiv:2210.08090.
105. Tian, Y.; Wan, Y.; Lyu, L.; Yao, D.; Jin, H.; Sun, L. FedBERT: When federated learning meets pre-training. *ACM Trans. Intell. Syst. Technol. TIST* **2022**, *13*, 1–26. [CrossRef]
106. Lin, B.Y.; He, C.; Zeng, Z.; Wang, H.; Huang, Y.; Soltanolkotabi, M.; Ren, X.; Avestimehr, S. Fednlp: A research platform for federated learning in natural language processing. *arXiv* **2021**, arXiv:2104.08815.
107. Choudhury, O.; Gkoulalas-Divanis, A.; Salonidis, T.; Sylla, I.; Park, Y.; Hsu, G.; Das, A. Anonymizing data for privacy-preserving federated learning. *arXiv* **2020**, arXiv:2002.09096.
108. Hao, W.; Mehta, N.; Liang, K.J.; Cheng, P.; El-Khamy, M.; Carin, L. Waffle: Weight anonymized factorization for federated learning. *IEEE Access* **2022**, *10*, 49207–49218. [CrossRef]
109. Langelaar, J.; Strömme Mattsson, A. Federated Neural Collaborative Filtering for Privacy-Preserving Recommender Systems. 2021. Available online: https://www.diva-portal.org/smash/get/diva2:1571409/FULLTEXT01.pdf (accessed on 29 March 2023).
110. Van Rooij, S.B.; Bouma, H.; van Mil, J.; ten Hove, J.M. Federated tool for anonymization and annotation in image data. In Proceedings of the Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies VI, Berlin, Germany, 5–8 September 2022; SPIE: Bellingham, WA, USA, 2022; Volume 12275, pp. 90–99.
111. Hu, H.; Dobbie, G.; Salcic, Z.; Liu, M.; Zhang, J.; Zhang, X. A locality sensitive hashing based approach for federated recommender system. In Proceedings of the 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID), Melbourne, Australia, 11–14 May 2020; pp. 836–842.
112. Enthoven, D.; Al-Ars, Z. An overview of federated deep learning privacy attacks and defensive strategies. In *Federated Learning Systems: Towards Next-Generation AI*; Springer: Cham, Switzerland, 2021; pp. 173–196.
113. Peyvandi, A.; Majidi, B.; Peyvandi, S.; Patra, J.C. Privacy-preserving federated learning for scalable and high data quality computational-intelligence-as-a-service in Society 5.0. *Multimed. Tools Appl.* **2022**, *81*, 25029–25050. [CrossRef]
114. Ribeiro, S.L.; Nakamura, E.T. Privacy protection with pseudonymization and anonymization in a health IoT system: Results from ocariot. In Proceedings of the 2019 IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE), Athens, Greece, 28–30 October 2019; pp. 904–908.
115. Khalfoun, B.; Ben Mokhtar, S.; Bouchenak, S.; Nitu, V. EDEN: Enforcing location privacy through re-identification risk assessment: A federated learning approach. *Proc. Acm Interact. Mob. Wearable Ubiquitous Technol.* **2021**, *5*, 1–25. [CrossRef]
116. Saha, S.; Ahmad, T. Federated transfer learning: Concept and applications. *Intell. Artif.* **2021**, *15*, 35–44. [CrossRef]
117. Choudhury, A.; Sun, C.; Dekker, A.; Dumontier, M.; van Soest, J. Privacy-Preserving Federated Data Analysis: Data Sharing, Protection, and Bioethics in Healthcare. In *Machine and Deep Learning in Oncology, Medical Physics and Radiology*; Springer: Cham, Switzerland, 2022; pp. 135–172.
118. Röhrig, R. A Federated Record Linkage Algorithm for Secure Medical Data Sharing. In Proceedings of the German Medical Data Sciences: Bringing Data to Life: Proceedings of the Joint Annual Meeting of the German Association of Medical Informatics, Biometry and Epidemiology (gmds EV) and the Central European Network-International Biometric Society (CEN-IBS), Berlin, Germany, 6–11 September 2020; IOS Press: Amsterdam, The Netherlands, 2021; Volume 278, p. 142.
119. Pramod, D. Privacy-preserving techniques in recommender systems: State-of-the-art review and future research agenda. *Data Technol. Appl.* **2023**, *57*, 32–55 [CrossRef]
120. Li, T.; Song, L.; Fragouli, C. Federated recommendation system via differential privacy. In Proceedings of the 2020 IEEE International Symposium on Information Theory (ISIT), Los Angeles, CA, USA, 21–26 June 2020; pp. 2592–2597.

121. Li, W.; Chen, H.; Zhao, R.; Hu, C. A Federated Recommendation System Based on Local Differential Privacy Clustering. In Proceedings of the 2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI), Atlanta, GA, USA, 18–21 October 2021; pp. 364–369.
122. Minto, L.; Haller, M.; Livshits, B.; Haddadi, H. Stronger privacy for federated collaborative filtering with implicit feedback. In Proceedings of the 15th ACM Conference on Recommender Systems, Amsterdam, The Netherlands, 27 September–1st October 2021; pp. 342–350.
123. Wu, X.; Zhang, Y.; Shi, M.; Li, P.; Li, R.; Xiong, N.N. An adaptive federated learning scheme with differential privacy preserving. *Future Gener. Comput. Syst.* **2022**, *127*, 362–372. [CrossRef]
124. Liu, Z.; Wang, L.; Chen, K. Secure efficient federated knn for recommendation systems. In *Advances in Natural Computation, Fuzzy Systems and Knowledge Discovery*; Springer: Cham, Switzerland, 2021; pp. 1808–1819.
125. Qin, J.; Liu, B.; Qian, J. A novel privacy-preserved recommender system framework based on federated learning. In Proceedings of the 2021 The 4th International Conference on Software Engineering and Information Management, Yokohama, Japan, 16–18 January 2021; pp. 82–88.
126. Wang, Q.; Yin, H.; Chen, T.; Yu, J.; Zhou, A.; Zhang, X. Fast-adapting and privacy-preserving federated recommender system. *VLDB J.* **2022**, *31*, 877–896. [CrossRef]
127. Ying, S. Shared MF: A privacy-preserving recommendation system. *arXiv* **2020**, arXiv:2008.07759.
128. Yang, L.; Zhang, J.; Chai, D.; Wang, L.; Guo, K.; Chen, K.; Yang, Q. Practical and secure federated recommendation with personalized masks. *arXiv* **2021**, arXiv:2109.02464.
129. Wang, W.; Huang, H.; Yin, Z.; Gadekallu, T.R.; Alazab, M.; Su, C. Smart contract token-based privacy-preserving access control system for industrial Internet of Things. *Digit. Commun. Netw.* **2022**, *9*, 337–346. [CrossRef]
130. Dudekula, K.V.; Syed, H.; Basha, M.I.M.; Swamykan, S.I.; Kasaraneni, P.P.; Kumar, Y.V.P.; Flah, A.; Azar, A.T. Convolutional Neural Network-Based Personalized Program Recommendation System for Smart Television Users. *Sustainability* **2023**, *15*, 2206. [CrossRef]
131. Majeed, A.; Lee, S. Attribute susceptibility and entropy based data anonymization to improve users community privacy and utility in publishing data. *Appl. Intell.* **2020**, *50*, 2555–2574. [CrossRef]
132. Lin, G.; Liang, F.; Pan, W.; Ming, Z. Fedrec: Federated recommendation with explicit feedback. *IEEE Intell. Syst.* **2020**, *36*, 21–30. [CrossRef]
133. Liang, F.; Pan, W.; Ming, Z. Fedrec++: Lossless federated recommendation with explicit feedback. In Proceedings of the AAAI Conference on Artificial Intelligence, Online, 2–9 February 2021; Volume 35, pp. 4224–4231.
134. Lin, Z.; Pan, W.; Ming, Z. FR-FMSS: Federated recommendation via fake marks and secret sharing. In Proceedings of the 15th ACM Conference on Recommender Systems, Amsterdam, The Netherlands, 27 September–1 October 2021; pp. 668–673.
135. Liu, Z.; Yang, L.; Fan, Z.; Peng, H.; Yu, P.S. Federated social recommendation with graph neural network. *ACM Trans. Intell. Syst. Technol. (TIST)* **2022**, *13*, 1–24. [CrossRef]
136. Raghuwanshi, S.K.; Pateriya, R.K. Recommendation systems: Techniques, challenges, application, and evaluation. In *Proceedings of the Soft Computing for Problem Solving: SocProS 2017*; Springer: Singapore, 2019; Volume 2, pp. 151–164.
137. Jiang, J.Y.; Li, C.T.; Lin, S.D. Towards a more reliable privacy-preserving recommender system. *Inf. Sci.* **2019**, *482*, 248–265. [CrossRef]
138. Ammad-Ud-Din, M.; Ivannikova, E.; Khan, S.A.; Oyomno, W.; Fu, Q.; Tan, K.E.; Flanagan, A. Federated collaborative filtering for privacy-preserving personalized recommendation system. *arXiv* **2019**, arXiv:1901.09888.
139. Kaur, H.; Kumar, N.; Batra, S. An efficient multi-party scheme for privacy preserving collaborative filtering for healthcare recommender system. *Future Gener. Comput. Syst.* **2018**, *86*, 297–307. [CrossRef]
140. Zheng, S.; Luo, J.; Dong, E.; Chen, C.; Liu, X. SPENDER: A Platform for Secure and Privacy-Preserving Decentralized P2P E-Commerce. *arXiv* **2022**, arXiv:2206.07215.
141. Li, D.; Chen, C.; Lv, Q.; Shang, L.; Zhao, Y.; Lu, T.; Gu, N. An algorithm for efficient privacy-preserving item-based collaborative filtering. *Future Gener. Comput. Syst.* **2016**, *55*, 311–320. [CrossRef]
142. Tareq, S.U.; Noor, M.H.; Bepery, C. Framework of dynamic recommendation system for e-shopping. *Int. J. Inf. Technol.* **2020**, *12*, 135–140. [CrossRef]
143. Venkatesh, V.; Hoehle, H.; Aloysius, J.A.; Nikkhah, H.R. Being at the cutting edge of online shopping: Role of recommendations and discounts on privacy perceptions. *Comput. Hum. Behav.* **2021**, *121*, 106785. [CrossRef]
144. Mazeh, I.; Shmueli, E. A personal data store approach for recommender systems: Enhancing privacy without sacrificing accuracy. *Expert Syst. Appl.* **2020**, *139*, 112858. [CrossRef]
145. Khan, A.R.; Zoha, A.; Mohjazi, L.; Sajid, H.; Abbasi, Q.; Imran, M.A. When federated learning meets vision: An outlook on opportunities and challenges. In Proceedings of the Body Area Networks. Smart IoT and Big Data for Intelligent Health Management: 16th EAI International Conference, BODYNETS 2021, Virtual Event, 25–26 October 2021; Springer: Cham, Switzerland, 2022; pp. 308–319.
146. Saura, J.R.; Ribeiro-Soriano, D.; Palacios-Marqués, D. Evaluating security and privacy issues of social networks based information systems in Industry 4.0. *Enterp. Inf. Syst.* **2022**, *16*, 1694–1710. [CrossRef]

147. Elahi, M.; Jannach, D.; Skjærven, L.; Knudsen, E.; Sjøvaag, H.; Tolonen, K.; Holmstad, Ø.; Pipkin, I.; Throndsen, E.; Stenbom, A.; et al. Towards responsible media recommendation. *AI Ethics* **2022**, *2*, 103–114. [CrossRef]
148. Valkenburg, P.M. Social media use and well-being: What we know and what we need to know. *Curr. Opin. Psychol.* **2022**, *45*, 101294. [CrossRef] [PubMed]
149. Kurdi, B.; Alshurideh, M.; Akour, I.; Tariq, E.; AlHamad, A.; Alzoubi, H. The effect of social media influencers' characteristics on consumer intention and attitude toward Keto products purchase intention. *Int. J. Data Netw. Sci.* **2022**, *6*, 1135–1146. [CrossRef]
150. Kapoor, P.S.; Balaji, M.; Jiang, Y.; Jebarajakirthy, C. Effectiveness of travel social media influencers: A case of eco-friendly hotels. *J. Travel Res.* **2022**, *61*, 1138–1155. [CrossRef]
151. Ibrahim, B.; Aljarah, A. The era of Instagram expansion: Matching social media marketing activities and brand loyalty through customer relationship quality. *J. Mark. Commun.* **2023**, *29*, 1–25. [CrossRef]
152. Kruijt, J.; Meppelink, C.S.; Vandeberg, L. Stop and think! Exploring the role of news truth discernment, information literacy, and impulsivity in the effect of critical thinking recommendations on trust in fake COVID-19 news. *Eur. J. Health Commun.* **2022**, *3*, 40–63. [CrossRef]
153. Singh, D.K.S.; Nithya, N.; Rahunathan, L.; Sanghavi, P.; Vaghela, R.S.; Manoharan, P.; Hamdi, M.; Tunze, G.B. Social network analysis for precise friend suggestion for twitter by associating multiple networks using ml. *Int. J. Inf. Technol. Web Eng. IJITWE* **2022**, *17*, 1–11. [CrossRef]
154. Nguyen, D.C.; Pham, Q.V.; Pathirana, P.N.; Ding, M.; Seneviratne, A.; Lin, Z.; Dobre, O.; Hwang, W.J. Federated learning for smart healthcare: A survey. *ACM Comput. Surv. CSUR* **2022**, *55*, 1–37. [CrossRef]
155. Arikumar, K.; Prathiba, S.B.; Alazab, M.; Gadekallu, T.R.; Pandya, S.; Khan, J.M.; Moorthy, R.S. FL-PMI: Federated learning-based person movement identification through wearable devices in smart healthcare systems. *Sensors* **2022**, *22*, 1377. [CrossRef]
156. Dhiman, G.; Juneja, S.; Mohafez, H.; El-Bayoumy, I.; Sharma, L.K.; Hadizadeh, M.; Islam, M.A.; Viriyasitavat, W.; Khandaker, M.U. Federated learning approach to protect healthcare data over big data scenario. *Sustainability* **2022**, *14*, 2500. [CrossRef]
157. Rahman, A.; Hossain, M.S.; Muhammad, G.; Kundu, D.; Debnath, T.; Rahman, M.; Khan, M.S.I.; Tiwari, P.; Band, S.S. Federated learning-based AI approaches in smart healthcare: Concepts, taxonomies, challenges and open issues. *Clust. Comput.* **2022**, 1–41. [CrossRef] [PubMed]
158. Pouriyeh, S.; Shahid, O.; Parizi, R.M.; Sheng, Q.Z.; Srivastava, G.; Zhao, L.; Nasajpour, M. Secure Smart Communication Efficiency in Federated Learning: Achievements and Challenges. *Appl. Sci.* **2022**, *12*, 8980. [CrossRef]
159. Ahmed, J.; Nguyen, T.N.; Ali, B.; Javed, A.; Mirza, J. On the physical layer security of federated learning based IoMT networks. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 691–697. [CrossRef] [PubMed]
160. Ali, M.; Naeem, F.; Tariq, M.; Kaddoum, G. Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 778–789. [CrossRef]
161. Liu, Z.; Chen, Y.; Zhao, Y.; Yu, H.; Liu, Y.; Bao, R.; Jiang, J.; Nie, Z.; Xu, Q.; Yang, Q. Contribution-aware federated learning for smart healthcare. In Proceedings of the AAAI Conference on Artificial Intelligence, Online, 22 February–1 March 2022; Volume 36, pp. 12396–12404.
162. Wibawa, F.; Catak, F.O.; Kuzlu, M.; Sarp, S.; Cali, U. Homomorphic encryption and federated learning based privacy-preserving cnn training: COVID-19 detection use-case. In Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference, Barcelona, Spain, 15–16 June 2022; pp. 85–90.
163. Ahmad, S.F.; Alam, M.M.; Rahmat, M.K.; Mubarik, M.S.; Hyder, S.I. Academic and administrative role of artificial intelligence in education. *Sustainability* **2022**, *14*, 1101. [CrossRef]
164. Kalugin, V.; Lutsenko, A.; Romanova, I.; Ye, D. Development of teaching programs of artificial intelligence methods in aerospace education. In *Proceedings of the SHS Web of Conferences*; EDP Sciences: Les Ulis, France, 2022; Volume 137, p. 01006.
165. Liu, T.; Wu, Q.; Chang, L.; Gu, T. A review of deep learning-based recommender system in e-learning environments. *Artif. Intell. Rev.* **2022**, *55*, 5953–5980. [CrossRef]
166. Jena, K.K.; Bhoi, S.K.; Malik, T.K.; Sahoo, K.S.; Jhanjhi, N.; Bhatia, S.; Amsaad, F. E-Learning Course Recommender System Using Collaborative Filtering Models. *Electronics* **2022**, *12*, 157. [CrossRef]
167. Rahhali, M.; Oughdir, L.; Jedidi, Y.; Lahmadi, Y.; El Khattabi, M.Z. E-learning recommendation system based on cloud computing. In *WITS 2020: Proceedings of the 6th International Conference on Wireless Technologies, Embedded, and Intelligent Systems*; Springer: Singapore, 2022; pp. 89–99.
168. Sabeima, M.; Lamolle, M.; Nanne, M.F. Towards Personalized Adaptive Learning in e-Learning Recommender Systems. *Int. J. Adv. Comput. Sci. Appl.* **2022**, *13*. [CrossRef]
169. Bourkoukou, O.; El Bachari, E. A Big-Data Oriented Recommendation Method in E-Learning Environment. *Int. J. Emerg. Technol. Learn.* **2022**, *17*, 74–84. [CrossRef]
170. Rodgers, W.; Nguyen, T. Advertising benefits from ethical artificial intelligence algorithmic purchase decision pathways. *J. Bus. Ethics* **2022**, *178*, 1043–1061. [CrossRef]
171. Sethi, V.; Gujral, R.K. Survey of Different Recommendation Systems to Improve the Marketing Strategies on E-commerce. In Proceedings of the 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), Faridabad, India, 26–27 May 2022; Volume 1, pp. 119–125.
172. Hui, B.; Zhang, L.; Zhou, X.; Wen, X.; Nian, Y. Personalized recommendation system based on knowledge embedding and historical behavior. *Appl. Intell.* **2022**, *52*, 954–966. [CrossRef]

173. Ge, Y.; Liu, S.; Fu, Z.; Tan, J.; Li, Z.; Xu, S.; Li, Y.; Xian, Y.; Zhang, Y. A survey on trustworthy recommender systems. *arXiv* **2022**, arXiv:2207.12515.
174. Sima, C.; Fu, Y.; Sit, M.K.; Guo, L.; Gong, X.; Lin, F.; Wu, J.; Li, Y.; Rong, H.; Aublin, P.L.; et al. Ekko: A Large-Scale Deep Learning Recommender System with Low-Latency Model Update. In Proceedings of the 16th USENIX Symposium on Operating Systems Design and Implementation (OSDI 22), Carlsbad, CA, USA, 11–13 July 2022; pp. 821–839.
175. Tian, Y.; Song, B.; Huh, E.N. A novel Threat Evaluation method for privacy-aware system in RFID. *Int. J. Ad Hoc Ubiquitous Comput.* **2011**, *8*, 230–240. [CrossRef]
176. Song, Y.; Lian, R.; Chen, Y.; Jiang, D.; Zhao, X.; Tan, C.; Xu, Q.; Wong, R.C.W. A Platform for Deploying the TFE Ecosystem of Automatic Speech Recognition. In Proceedings of the 30th ACM International Conference on Multimedia, Lisboa, Portugal, 10 October 2022; pp. 6952–6954.
177. He, G. Enterprise E-commerce marketing system based on big data methods of maintaining social relations in the process of E-commerce environmental commodity. *J. Organ. End User Comput. JOEUC* **2021**, *33*, 1–16. [CrossRef]
178. Chen, H. Personalized recommendation system of E-commerce based on big data analysis. *J. Interdiscip. Math.* **2018**, *21*, 1243–1247. [CrossRef]
179. Niu, C.; Wu, F.; Tang, S.; Hua, L.; Jia, R.; Lv, C.; Wu, Z.; Chen, G. Billion-scale federated learning on mobile clients: A submodel design with tunable privacy. In Proceedings of the 26th Annual International Conference on Mobile Computing and Networking, London, UK, 21–25 September 2020; pp. 1–14.
180. Zhang, X.; Guo, C. Research on Open Innovation Intelligent Decision-Making of Cross-Border E-Commerce Based on Federated Learning. *Math. Probl. Eng.* **2022**, *2022*, 9253634. [CrossRef]
181. Wang, H.; Xie, F.; Duan, Q.; Li, J. Federated Learning for Supply Chain Demand Forecasting. *Math. Probl. Eng.* **2022**, *2022*, 4109070. [CrossRef]
182. Mathews, S.M.; Assefa, S.A. Federated Learning: Balancing the Thin Line Between Data Intelligence and Privacy. *arXiv* **2022**, arXiv:2204.13697.
183. Ni, J.; Li, J.; McAuley, J. Justifying recommendations using distantly-labeled reviews and fine-grained aspects. In Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), Hong Kong, China, 3–7 November 2019; pp. 188–197.
184. Harper, F.M.; Konstan, J.A. The movielens datasets: History and context. *Acm Trans. Interact. Intell. Syst. Tiis* **2015**, *5*, 1–19. [CrossRef]
185. Asghar, N. Yelp dataset challenge: Review rating prediction. *arXiv* **2016**, arXiv:1605.05362.
186. Guo, G.; Zhang, J.; Yorke-Smith, N. A novel evidence-based Bayesian similarity measure for recommender systems. *ACM Trans. Web (TWEB)* **2016**, *10*, 1–30. [CrossRef]
187. Wang, J.; Caverlee, J. Recurrent recommendation with local coherence. In Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining, Melbourne, VIC, Australia, 11–15 February 2019; pp. 564–572.
188. Bennett, J.; Lanning, S. The netflix prize. In Proceedings of the KDD Cup and Workshop, San Jose, CA, USA, 12 August 2007; Volume 2007, p. 35.
189. Çano, E.; Morisio, M. Music mood dataset creation based on last. fm tags. In Proceedings of the 2017 International Conference on Artificial Intelligence and Applications, Vienna, Austria, 24–28 April 2017; pp. 15–26.
190. Yang, J.; Yecies, B. Mining Chinese social media UGC: A big-data framework for analyzing Douban movie reviews. *J. Big Data* **2016**, *3*, 1–23. [CrossRef]
191. Ziegler, C.N.; McNee, S.M.; Konstan, J.A.; Lausen, G. Improving recommendation lists through topic diversification. In Proceedings of the 14th International Conference on World Wide Web, Chiba, Japan, 10–14 May 2005; pp. 22–32.