Federated Learning-based Personalized Recommendation Systems: An Overview on Security and Privacy Challenges

Danish Javeed, Muhammad Shahid Saeed, Prabhat Kumar, Alireza Jolfaei, Shareeful Islam and A. K. M. Najmul Islam

***Abstract*—The recent advancement in next-generation Consumer Electronics (CE) has created the problems of information overload and information loss. The significance of Personalized Recommendation Systems (PRS) to efficiently and effectively extract useful user information is seen as an ideal solution to provide users with personalized content and services and therefore is used in different application domains including healthcare, e-commerce, social media, etc. Security and privacy are the two major challenges of the existing PRS for next-gen CE data. Federated learning (FL) has the potential to elevate the aforementioned challenges by sharing local recommender parameters while keeping all the training data on the device and therefore is seen as a promising technique to enhance security and privacy in PRS for the next-gen CE data. In this survey, we have first discussed the enhancement of the existing CE technologies, a holistic review of security and privacy challenges in current PRS, and the advantage of FL-based PRS for next-gen CE. Finally, we list a few open issues and challenges that can guide researchers and practitioners to further drive research in this promising area.**

***Index Terms*—Consumer Electronics, Federated Learning, Privacy, Personalized Recommendation Systems, Security**

I. Introduction

THE recent advancement in Artificial Intelligence (AI) Virtual Reality (VR)/Augmented Reality (AR), and Internet of Things (IoT) has significantly revolutionized the Consumer Electronics (CE) market. According to the "Statista Research Department", the global revenue of CE market will show an increase of US$ 125.5 billion between 2023 and 2028 [1]. These facts show the tremendous and steep growth of the CE devices and as a result, a "data lake" is expected to be formed. The majority of CE is connected to the Internet to offer consumers countless services [2]. However, the amount of information on the Internet has significantly outpaced the need of consumer requirements and, thus poses an information overload problem that prevents timely access to online resources of interest [3]. This has led to a greater-than-ever growth in demand for recommender systems. Recommender systems are information filtering systems that address the issue of information overload by selecting key information fragments from enormous amounts of dynamically generated data in accordance with user choices, interests, or observed behavior towards the item [4]. Furthermore, there is a lot of research being done on Personalized Recommendation Systems (PRS), which leverage personalization in the domain of product recommendations [5]. On another hand, most PRS uses centralized servers to store and process consumer data. Specifically, the cloud servers are equipped with powerful computing resources and therefore are used to understand, visualize and extract pertinent information. However, sending the consumer confidential data to cloud servers brings some inherent challenges related to security and privacy, where the attacker or malicious cloud can hack or steal PRS data, and it can result in data leaks and identity theft [6], [7]. The data might also be sold to third-party companies that want to utilize it for product recommendation, which is another potential privacy problem.

Federated Learning (FL) is one of the emerging technologies that enable the execution of machine learning models in a distributed manner. In FL-based PRS, CE devices are not needed to exchange their own data; instead, they train on-device using model parameters that are given by a coordinating server [8]. The model is specifically trained locally by all participating users, and updated model parameters are communicated with the cloud server to conduct aggregation and to create a new set of parameters to be utilized in the following iteration [9]. Until a specific degree of accuracy is reached, this procedure is repeated continuously over a number of iterations. Even though the FL-based PRS solves the security and privacy issues of consumers but still it has some other challenges related to computation and communication cost, explainability in FL-based PRS, and working of FL-based PRS in 5G and beyond networks.

A. Our Contribution

The main contributions of this survey paper are as follows: First, we discussed the relationship between consumer electronics with personalized recommendation systems (PRS) and how federated learning can enhance the security and privacy challenges in PRS for the next-gen CE data. Second, we have discussed the state-of-the-art techniques used to enhance data

Danish Javeed is with the Software College, Northeastern University, Shenyang 110169, China. (Email: 2027016@stu.neu.edu.cn)

Muhammad Shahid Saeed is with Dalian University of Technology, Dalian, China. (Email: shahidsaeedrana@gmail.com)

Prabhat Kumar and A. K. M. Najmul Islam are with the Department of Software Engineering, LUT School of Engineering Science, LUT University, 53850 Lappeenranta, Finland (Email: prabhat.kumar@lut.fi, najmul.islam@lut.fi).

Alireza Jolfaei is with the College of Science and Engineering, Flinders University, Adelaide, Australia. (Email: alireza.jolfaei@flinders.edu.au)

Shareeful Islam is with the School of Computing and Information Science, Anglia Ruskin University, UK. Email: shareeful.islam@aru.ac.uk

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2023.3318754

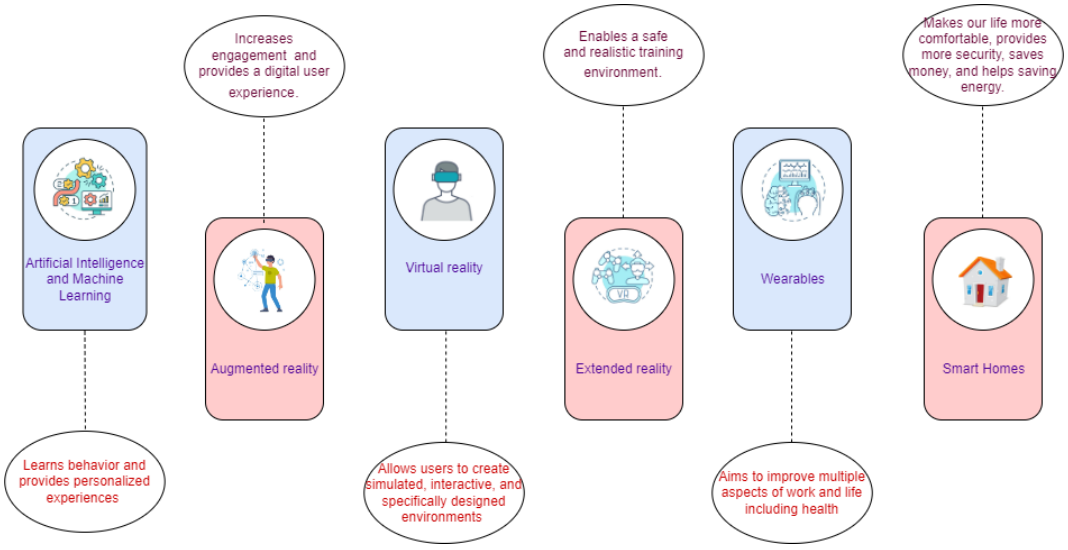

Fig. 1: Advancements in the Next-gen Consumer Electronics.

privacy and security and low-latency network communication. The rest of the article is organized as follows: In Section II, we gave an overview of next-gen CE, PRS, and FL. In Section III, we discussed the shortcoming of PRS and how FL-based PRS can enhance security and privacy. In Section IV, we discussed the challenges in implementing FL-based PRS for next-gen CE and finally, we conclude the paper in Section V.

II. Preliminaries

A. Overview of Next-gen Consumer Electronics

Consumer electronics (CE) have always been a driving force in technology innovation. From the invention of the television to the first mobile phone, these devices have changed how we communicate, entertain ourselves, and our daily lives [10], [11]. Today, we are on the edge of the next generation of consumer electronics (Next-gen CE), and the possibilities are endless. Next-gen CE is the latest and upcoming electronic device designed to enhance user experience and offer advanced features, capabilities, and performance. These devices are built using cutting-edge technologies characterized by their ability to connect seamlessly with other devices, services, and platforms. Fig. 1 shows the recent advancement in the next-gen CE. Some of the key trends and advancements in the next-gen CE include [2]:

1) Artificial Intelligence (AI) and Machine Learning (ML): One of the most significant technological advancements over the past decade has been the rise of AI and ML. These technologies have been integrated into various industries, including smart agriculture [12], healthcare [13], finance [14], smart industries [15], and transportation [16]. AI and ML can potentially revolutionize how we interact with our devices in CE. For instance, smart homes and virtual assistants have made significant progress in recent years, allowing us to control our home devices with our voices. The Next-gen CE will have more sophisticated AI and ML algorithms, enabling them to learn from our behavior and provide personalized experiences [3]. Moreover, AI and ML can enhance the cameras and sensors on our devices. They can automatically adjust the lighting, contrast, and focus based on the user's environment, ensuring the best possible photo or video. Furthermore, AI can be used to power facial recognition technology, allowing our devices to unlock or authenticate purchases with a single glance [17].

2) Augmented reality: Augmented reality (AR) is another technology molding the Next-gen CE. AR can lay over digital content in the real world, resulting in a flawless blend of the physical and virtual worlds. [18]. It is already being used in mobile apps, such as Pokemon Go and Snapchat, but it is expected to be used in a wider range of CE devices in the future. AR could be used in smart glasses, for example, to provide users with a heads-up display of information or to overlay digital content onto real-world objects.

3) Virtual reality: Virtual reality (VR) is another technology that is shifting the Next-gen CE. VR can generate immersive digital atmospheres in which users can interrelate and explore. VR is already used in entertainment and gaming [19], but it is likely to be used in a wider range of CE devices in the upcoming years. It could be used in education to create mesmerizing learning experiences, or in healthcare to imitate medical procedures.

4) Extended Reality (XR): Extended Reality (XR) is a term that defines the spectrum of technologies encompassing VR, AR, and mixed reality (MR). XR is capable of changing the way we experience education, medical treatment, entertainment, and education [20]. The advancement in standalone VR and AR headsets is one of the most substantial progresses in XR. Such devices provide users with complete mobility by not needing a smartphone or a PC to function. Further, they are also affordable in price, making them more reachable to the average consumer. XR can also be used to improve educational experiences by letting students discover historical sites, witness scientific phenomena, and even conduct experiments in a simulated environment [21].

5) Wearables: Wearable Technology (WT) has been around for a while, with devices like smartwatches and fitness track-

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2023.3318754

ers, becoming progressively popular in recent years. The next generation of WT promises to be even more influential, with devices that can measure the activity of a human brain, monitor health metrics, and even analyze sweat to analyze hydration levels [22]. WT will also become more integrated into our daily lives. For example, smart clothing, which is capable of monitoring vital signs and adjusting its temperature based on the environment of the user. Wearables will also grow more sophisticated, with gadgets that look like jewellery.[23].

6) Smart homes: The rise of smart homes will also change the Next-gen CE. It uses internet-connected devices to automate and regulate several household tasks, such as light systems, security, and heating [24]. Smart home devices are already popular, with products like Amazon Echo and Nest Thermostat [25]. Nevertheless, the next generation of smart home devices is expected to be even more advanced. For example, smart home devices could be furnished with AI abilities to learn from the behavior of the user and make decisions about controlling numerous household functions [26].

B. Personalized Recommendation System

Recommendation technology (RT) is a key component of IoT services since it may be in assistance of consumers in getting information and better service anytime, anyplace [27]. A personalized recommendation system (PRS) is a type of information filtering system that anticipates a user's interests or preferences and recommends content that is likely to be of interest to them. These technologies are often employed to deliver a more personalized experience for users in e-commerce, social networking, and entertainment platforms. [4]. Some key concepts in PRS are Content-Based Filtering (CBF), Collaborative Filtering (CF), Hybrid Filtering (HF), User Profile (UP), and Item Profile (IP). The CF is considered the most well-known and adopted recommendation technique [28], [29]. It predicts a user's preferences based on the preferences of other users who exhibit similar behavior or have comparable interests. It can be based on user-based or item-based similarity [30], [31]. The CF has no specific criteria, such as metadata or description for the recommended goods. It is capable of dealing with a wide range of things, including books and music [32]. As a result, it has been widely used in commercial applications [33].

On the other hand, CPF predicts a user's preferences based on the characteristics of the items that the user has interacted with or shown interest in. It can be based on item features or item descriptions [5]. Moreover, the HF combines CF and CBF to provide personalized recommendations. It can overcome the limitations of each technique and provide more accurate and diverse recommendations [34]. According to a recent analysis by the authors of [35], Amazon's recommendation algorithm accounted for more than 30% of the total sales volume. Moreover, RS is a vital component of cloud computing [6], [7]. While the CF systems have seen significant success, several disadvantages still remain, i.e., scalability cold-start, etc. The researchers have proposed various techniques to solve such issues. For example, the authors of [36]and [37] proposed hybrid recommendation models to eliminate the cold-start. Moreover, in [38], the authors claim that Singular Value Decomposition and Matrix Factorization models can efficiently eliminate sparsity issues.

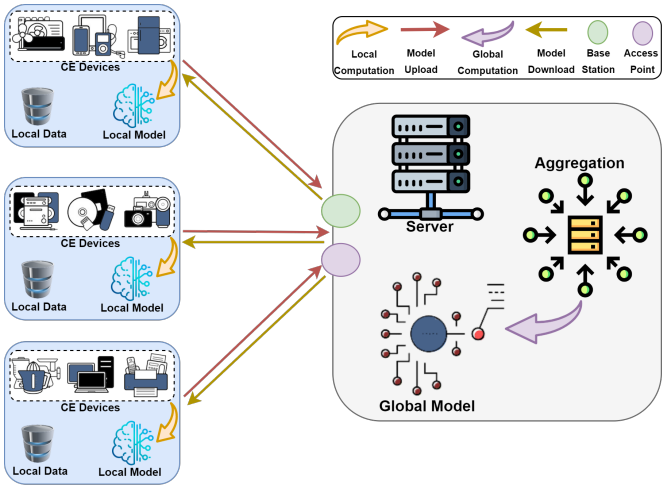

Fig. 2: Architecture of FL for CE.

C. Federated Learning Concept

The demand for a significant amount of data for ML/DL model training in CE has prompted a slew of projects aiming at pooling data from disparate sources. The CE data, on the other hand, may have substantial commercial value, making it less to freely share with cloud providers.

Federated Learning (FL) addresses data governance challenges and privacy concerns by empowering shared learning without data centralization. For example, FL resolves the issue of insufficient data by providing data privacy, trust factor between heterogeneous domains, and delocalization [39]. It is an ML-based method that allows multiple devices or systems to collaboratively train a model without sharing their raw data with a Central Server (CS). Instead, the training takes place locally on each device or system, and only the updates to the model parameters are communicated to a CS, where they are aggregated to form an improved model. At the same time, having a model trained on larger landscape data is another advantage of this federated environment. With its advanced architectures, It has transformed many AI-based applications by providing novel privacy-enhancing and distributed AI solutions [40]. FL is especially appealing for constructing dispersed CE systems because it pushes AI tasks, such as data training, to the network edge at CE devices where the data resides. Consequently, the data of the user is never exchanged openly with a third party, consenting to cooperative training of a shared Global Model (GM) that benefits the CE users and network operators with regard to privacy improvement and network resource savings.

The FL concept in CE networks comprises CE devices and an Aggregation Server (AS). The AS is located at the Access point (AP) or Base station (BS), as shown in Fig 2. In the Next-gen CE network, the FL plays a vital role in achieving complete intelligence in CE system at the network edge since

TABLE I: Analysis of existing challenges for PRS in next-gen CE

Ref	Mentioned challenges	Security	Privacy	Confidentiality	Integrity	Authenticity	Consequences
[41]	Unauthorized access	✓	×	✓	✓	✓	Malicious control over the system
[42]	Data breaches	×	✓	✓	✓	×	Leakage of sensitive data
[43]	Fraudulent activities	✓	×	×	×	✓	Lack of trust in PRS
[44]	Inference attack	×	✓	✓	×	✓	Attackers may obtain private information.
[45]	The durability of the algorithm	✓	×	×	✓	×	Operational malfunctions in PRS
[46]	Instant Response	✓	×	×	✓	×	Decrease in PRS usage
[47]	Lack of transparency	×	✓	✓	×	×	Offers a smooth road to revealing privacy.

the BS is not capable of gathering the data from the scattered CE devices for training. In the FL process, each CE user trains a shared model where each device or system has its own dataset, and they are not all combined into a central dataset. After this, a Local Model (LM) trains the ML model on a device or system using the local data. The LM is updated with each training iteration and is used to compute the updates that are sent to the CS. It is responsible for coordinating the training process across the devices and systems. Hereinafter, the CS receives updates from LMs and aggregates them to form an improved GM without considerably compromising the privacy of the user data. The model aggregation can be performed using various techniques, including federated averaging and FL with differential privacy [48].

III. Overview of FL-based PRS for Next-gen Consumer Electronics

A. Security and Privacy Challenges in PRS for Next-gen Consumer Electronics

Personalized Recommendation Systems (PRS) have surprisingly revolutionized the way users interact with next-gen CE by acting as an advisory bridge between CE and end-consumers. However, some potential security and privacy challenges are associated with it that possess notorious impacts [49]. PRS majorly relies on collecting tons of consumers' data, including their interaction patterns, browsing history, cookies, frequently called queries, etc. [50]. The data may also contain personally Identifiable Information (PII), such as an identity number, credit card details, and banking credentials. The data stored in PRS is then analyzed to predict the behavior of consumers towards a specific entity [31]. The entire process of collecting, storing, and analyzing consumers' data increases the probability of malicious activities and makes PRS a favorite target for attackers. Unauthorized access to the system's resources is one of the most common adversarial practices performed by the bad elements. Despite such unauthorized access, the extensive operational process of PRS may have consequences that may disclose the confidentiality, authenticity, and even integrity of consumers' data in some scenarios [41]. Data breaching is another possible malicious approach that may be performed by attackers to obtain valuable information from consumers. Such a hazardous situation leads to a variety of serious risks, including identity theft, misuse of data, and reputational damage [42]. Access to online banking data opens the door to a variety of finance-related fraudulent activities as well, which is another serious challenge currently surrounding PRS [43].

Inference attack is another major challenge in PRS that may have critical outcomes. This attack is knowingly performed with the bad intention of exploiting deterministic information about the targeted audience. The inference attack adopts a superficially precarious approach that is technically complex in nature. The adversarial elements send a series of specially constructed queries to the recommendation system and then analyze the system's responses against identical queries to draw an answering pattern. After examining a handful of streams of queries along with recommendations, the attacker may retrieve sensitive information about the consumers that was not intended to be disclosed. In the absence of an adequate security matrix, PRS may be a desired target for such crucial attacks that flash an alarming situation to exploit the privacy and confidentiality of consumers [44]. Various research studies objectify the algorithm of PRS in terms of its limited immunity against mega-security threats. The algorithm is highly susceptible to systematic alterations, leading to unfair analysis of data and biased recommendations. The weakness of the algorithm makes the overall durability of PRS a question mark [45]. In the case of next-gen CE, higher accuracy in recommendations is a vital objective to be achieved. Additionally, the recommendation system should be capable enough to provide consumers with diversified recommendations for preferable decision-making. The adaptability of new preferences from the consumer side is another common phenomenon that modern recommendation systems are suffering from. An effective PRS should be responsive enough to adopt new preferences and return up-to-date recommendations. The weak algorithm may not only lack the ability to provide accurate and diversified recommendations but may also lack the ability to maintain updated recommendations [46].

The next major challenge is operational transparency to avoid any misconceptions regarding the large amounts of consumer data taken by PRS. While considering the confidentiality and privacy norms of consumers' data, the information collected from individuals must be treated in an ethical way by ensuring transparency in its usage [47]. Transparency should also be provided in practical aspects by educating the end consumers about the way recommendations are generated. Some recommendation systems obtain consumer data irrespective of future use, including location and their interaction patterns with other devices. Consumers must be aware of the futuristic scope of this data and its possible relevance to getting more personalized recommendations. The negligence may encourage the unwanted sharing of this data with third-party organizations for various other purposes. Hence, there

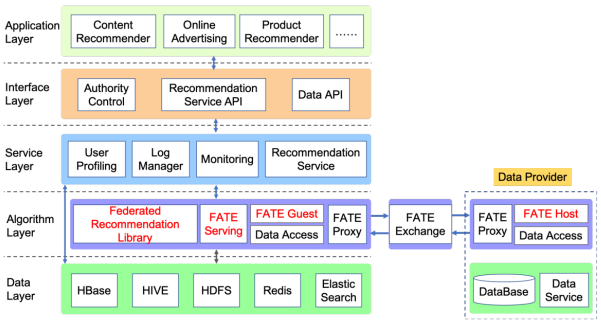

Fig. 3: Architecture of the Federated Recommender System [51].

must be an appropriate framework to provide consumers with useful insight into their data and its processing operations to get recommendations about next-gen CE. Table I provides a comprehensive insight into the existing challenges for PRS in next-gen CE.

1) Secure Data Sharing Issues: While employing a PRS for specific recommendations in next-gen CE, secure data sharing between authorized entities should be the prominent objective. To meet such desired secure communication challenges, PRS must be competent enough to mitigate the possibilities of any unwanted data security threat in the future. PRS collects a diversified variety of consumer data to ensure its smooth operations and to provide optimized recommendations. Generally, the more detailed information about the consumers is, the more accurate will be the generated recommendation [52]. Accordingly, the risks of significant data security threats increase, urging the need for a secure data exchange framework between end-consumers and PRS. When the extracted data consists of critical information of consumers, e.g. PII, financial details, and medical data, the need for secure data sharing increases exponentially [53], there are several possible ways for data leakage in PRS designed for next-gen CE.

The data obtained from consumers is stored in PRS data repositories, and insufficient access control over such data databases offers a smooth ground for malicious attempts on consumers' data. The successful attempts result in data leakage, data tempering, or even the elimination of important information [54]. Hence, it becomes a vital challenge to protect these databases from attackers by designing comprehensive access controls. PRS formulates a generic systematic architecture in which the data communication from consumers to PRS repositories is regulated through a central server [55]. This plane transmission channel is easier to take over than a secure communication line containing end-to-end encrypted data [56]. In the case of next-gen CE, most consumers' devices are integrated with third-party mobile applications that take unauthorized control of that particular device. Hence, the data transmitted from or to such devices is observed by some third-party element triggering the chances of data breaches [57]. Most of the back-end algorithms of PRS are empowered by cloud services to instantly adopt new consumer preferences and ensure instant recommendations in return. If a secure communication protocol does not leverage the data transmission, the swear data exposure may occur to sabotage the confidentiality and privacy of consumers' data [58]. The possible data communication challenges for PRS in next-gen CE are enlisted in Table II.

2) Resource-Constrained Consumer Devices: The term" Resource-Constrained" describes the availability of limited resources. From a CE perspective, the resource-constrained nature of devices indicates small devices with less computation power, storage, and processing units. The integration of PRS with next-gen resource-constrained CE is encircled by an extensive range of challenges that must be addressed appropriately. Most next-gen CE, such as wearables, smartwatches, and small gaming units, come with limited computational resources. That fact hinders their way of reflecting effective collaboration with PRS [59]. The availability of limited computational capacity is not an ideal situation for running complex and optimized PRS algorithms. These circumstances introduce the concept of lightweight algorithms. However, various studies have proven the compromised nature of lightweight algorithms. Hence, there is a trade-off between the security and convenient execution of PRS algorithms on next-gen CE. Resource-constrained CE may also negatively impact the trustworthiness of PRS by blocking their way of implementing complex security measures. The high-efficiency privacy and data security protocols have convoluted processing that expects an adequate implementation ecosystem. Resource-constrained CE needs to welcome such complex computational alliances resulting in unsatisfactory security practices [60].

The next dominant challenge is finite memory units in CE that are good enough for their own. However, it requires large memory units to be compatible enough with PRS as broad memory bases invite extended data arrays that act as a supplement for more accurate recommendations by PRS [61]. Communication limitations are another notable challenge for PRS to be operational for next-gen CE. Most of the PRS are empowered by various cloud services to respond to CE with personalized recommendations instantly. However, the resource-constrained CE may suffer from poor connectivity issues because of limited communication resources. This may impact the overall quality of the communication stream by causing latency, unwanted noise, and even communication breakage in the worst cases. As a result of this resource-constrained nature of CE, it becomes a hectic task to interact and be synchronized with the cloud service configured between PRS and next-gen CE [62]. The instant response from CE is also a significant challenge for PRS. As the resource-constrained CE are equipped with limited resources, it becomes difficult for such devices to exhibit synchronized progress with the cloud server connecting PRS with CE. This scenario results in the slow performance of PRS and unnecessary communication delays [63]. Power consumption is another crucial factor in resource-constrained CE. These devices are powered by small-scale batteries that do not offer enough support to cater to intensive recommendation algorithms [64].

Moving forward, scalability is another serious challenge PRS must face while entertaining next-gen CE. It is observed that each CE device has its predefined working attributes and

TABLE II: Secure data communication challenges in PRS

Ref	Challenges	Consequences	Possible Combats
[54]	Security of PRS data repositories	Data breaches may occur	Implementing access controls
[55]	Protecting central data governance server	Disclosing confidentiality and privacy of consumers	Ensuring a reliable authentication mechanism
[56]	Ensuring end-to-end encrypted data stream	Sniffing or observing sensitive data	Imposing a complex encryption protocol
[57]	Data safety against third-party applications	Data leaks, unauthorized access to information	Making some data-sharing policies
[58]	Implementing a secure data communication channel	Information disclosure to attackers	Establishing a secure communication protocol

processing patterns. To obtain more accurate recommendations, it is advised to broaden the databases containing data from various identical units by creating a cluster of relevant CE devices. This practice helps to collect vast amounts of data and, after necessary processing, yields comprehensive recommendations to all participant CE devices. Due to the predefined interaction pattern, and lack of quick alterations, CE devices lack to shake hands with other identical CE devices. While expanding the application brackets of PRS over multiple CE devices becomes an unsettled task to configure multiple CE over PRS [65]. A broader overview of challenges for PRS in resource-constrained next-gen CE is given in Table III.

B. FL-based PRS for Next-gen Consumer Electronics: Characteristics and Impact

The next-generation consumer electronics environs smart devices purely designed at the consumer grade such as wearable, body implants, virtual reality gadgets, personal entertainment units, etc. Their intelligent nature makes them entirely different from traditional electronic devices. The warm adaptability of such next-generation consumer electronics devices demands these devices to be more functional and efficient. Therefore, PRS are integrated to make the user experience better. A PRS effectively analyzes scalable data and provides optimal suggestions recommended by the recommendation engines. PRS must need to be capable to accommodate the expectations of clients. However, we have seen that the learning process of PRS raises serious security and privacy challenges due to the fact that the CE data is often stored and analyzed on centralized cloud storage. FL has the ability to overcome this challenge by training the model on the devices. FL-based PRS are well-trained, which made them an excellent choice for next-generation consumer electronics.

1) Data Privacy and Security Enhancement: FL enables participant devices to jointly learn a shared prediction model. This method keeps the training data on the device, rather than uploading and storing the data on a central server. FL also employs secure aggregation to maintain the confidentiality of client updates. As a result, the server is unable to determine the value or source of the users' model updates. This diminishes the probability of inference and data attribution attacks. Typically sensitive scenarios that intend to stringent privacy regulations, gain security advantages by the local storage of personal information. It alleviates the burden of aggregating data on a central and external server, thereby making the data less vulnerable to breaches. The central server is the core coordinator, and it manages clients, centralizes their local models, and keeps the global model up-to-date. FL optimization is an iterative process that improves the global ML model with each iteration. FL is generally based on predefined parameters in an initial training phase. The model parameters are then disseminated to the participating clients and will be revised based on client feedback in subsequent steps. In the local model training, a list of participants is established where each client receives the global model and fine-tuning parameters, which are based on their local data for a given number of training epochs. The updated model weights are then transmitted to the central server to update the global model. The central server accumulates the updated models of all participating clients. Then by combining their parameters, it produces an updated general model.

To reduce biases, this step must incorporate multiple factors, including client confidence and participation frequency. In a decentralized system, there is no longer a central server that acts as an initiator, coordinator, or model aggregator. Researchers have designed an anomaly detection framework to investigate the presence of unwanted entities in IoT-enabled smart environments. The proposed scheme classifies possible attacks by consuming minimal computational resources. The FL-based operational segment is devoted to ensuring on-device training of local data models, and the Gated Recurrent Unit (GRU) offers extra layers of security to ensure the privacy of clients. The model proves a protected shield against common adversaries e.g. man-in-the-middle attacks, Denial of Service (DoS) attacks, and Modbus query flood attacks [66]. Another effort towards privacy preservation is made in [67], which mainly focuses to prohibit the retrieval of irrelevant information. The model filters the spam images in the raw data, and after that, these responsible clients are flagged to take part in the training phase. The system is employed with Convolutional Neural Network (CNN) and is trained on a customized dataset. In [68], the Authors addressed the integration of blockchain technologies with the FL to enhance the security and privacy metrics. A smart contract-based secure algorithm is proposed that directly measures the accuracy of the updated global model. Thus, it is unnecessary to assume that participants in the FL training process are trustworthy. Initial findings indicate that the algorithm offers a high degree of protection against model poisoning attacks. They anticipate that the obtained results can be used as a baseline for implementing the algorithm on various blockchain technologies.

Blockchain driven another security approach is described [69], where authors Develop a blockchain-enabled decentralized and asynchronous FL-based IoT anomaly detection scheme. The proposed method has the potential to boost efficiency while remaining robust and privacy-preservative. Researchers have designed a novel privacy-preserving tree-boosting algorithm named Secure Boost [70]. The core ob-

TABLE III: Analysis of existing challenges for PRS in next-gen CE

Ref	Category	Consequences	Trade-off
[59]	Computation	Limitations in computing complex recommendation algorithms	Reliable data exchange
[60]	Processing	Poor performance in running secure communication protocols	Data security and privacy
[61]	Memory	Unable to store vast data attributes for comprehensive recommendations	Accurate recommendations
[62]	Network connectivity	Incapable of maintaining synchronous connectivity with cloud services	Stable communication
[63]	Responsiveness	No instant response to cloud services of PRS	Instant response
[64]	Power	Not enough power to execute time-intensive computations	Long-run processing
[65]	Scalability	Configuration issues with other identical CE devices	Multi-facet recommendations

jective is to train a high-quality model with private data separated over multiple clients. Secure Boost aligns entities under a privacy-preserving protocol and then builds boosting trees across multiple parties using a carefully designed encryption strategy. This FL system lets multiple parties with common user samples but different feature sets jointly learn from a vertically partitioned dataset. The Secure Boost model embraces identical accuracy with non-federated gradient tree-boosting algorithms.

2) Low-latency Network Communication: Latency is an imperative component to evaluate the performance of a communication system. It states the duration taken by a data packet to travel from the sender to the receiver end. In traditional ML approaches, the clients send raw data to the server end, unnecessarily occupying the bandwidth for a sustainable period [71]. However, FL has outpaced this concept by introducing a new pattern of communication. It enables the clients to transmit only the updated model parameters rather than sending whole chunks of raw data. In this way, the network resources are efficiently managed, and considerably low latency occurs in the communication channel [72]. The latency in FL systems is remarkably lower than the centralized systems. Such performance makes FL an ideal choice for sensitive networks where minor communication delays may result in severe reactions. Health monitoring systems, sensitive manufacturing units, and smart grids are some valuable examples of aforementioned sensitive networks [73].

The second major FL component is latency-based scheduling or preferred scheduling. In normal ML approaches, the clients are imposed to send a whole stream containing the raw data, and this data is revised in each iteration [74]. That mechanism overburdened the system resources, especially the network bandwidth remain occupied. However, FL permits preferred scheduling in which the parameters are preferably defined. The clients are supposed to follow these parameters, and they do not even need to propagate an entire stream of data. Rather, they transmit only the updated models. In this way, FL calculates the time consumption of each iteration, which makes the communication process more robust, and responsive [75].

IV. Challenges and Future Research Directions

In this section, we have discussed the challenges of implementing FL for PRS. The main challenges are listed below:

A. Computation and Communication Cost

Computing and communication play a critical role to achieve PRS optimized performance. User devices need to communicate and update various intermediate parameter values with the server to generate recommendation results in their local system. This can pose a huge communication overhead which directly impacts the model performance. Additionally, users of consumer electronics devices and infrastructure may have varying capabilities relating to storage, speed, and computational power that certainly impact the overall training efficiency, delaying the whole process and reducing the efficiency of the global recommendation model [76]. However, communication cost incurs much great overhead cost than computation in case numerous users' devices are sending their model parameters to the central server [77]. There is a pressing need to reduce the computation and communication cost within Next-gen CE for an efficient recommendation model for individual users' needs.

Several methods are proposed which aim to improve the model efficiency and reduce the computation and communication overhead notably important-based model updating, client selection, model compression, asynchronous communication, etc. Important-based model update strategy considers an important part of the global model to reduce the communicate parameterized size instead of choosing all parameters. A multi-arm bandit method (FCF-BTS) is proposed which aims to select a specific part of the global model for a smaller payload to the client [78]. However, this approach also reduces the overall model accuracy. The client selection approach selects clients based on resource constraints such as limited computation resources or poor wireless channel conditions instead of random client selection to enhance the efficiency and performance of the global model. Fedcs protocol is considered where the server sends a resource request to each client to check the downloading, updating, and uploading time of local models so that the server can update the clients during the restricted time by following the greedy approach [79]. The shortest upload time is considered to select the client followed by a scheduling mechanism based on the maximum remaining bandwidth for enhancing the uploading efficiency[8]. Model compression is another widely used method that compresses the communication parameters for each communication which reduces the scale of parameter transmission. A novel coreset-based FL framework is considered that investigates the data redundancy in the dataset that trains corsets instead of training the whole dataset using the regular network model and similar

accuracy is achieved [9]. Structured and sketched updates are considered to decrease the uplink communication costs by updating from a pre-specified structure parameterized using fewer variables or compressing the full local update before communicating to the server.

Despite all these methods, there are still challenges to tackle the computation and communication cost issues. In particular, important-based model updating reduces the recommendation performance as well as raises privacy concerns. Due to the diversity of the users' devices and the inherent complexity of the users' network environment client selection problem requires an optimized selection approach. Model compression significantly reduces the communication cost but at the same time increases the overall computational overhead. To this end, future research directions need to investigate trade-off issues between computation and communication cost based on the users' consumer devices capacity and infrastructure as well as develop methods to achieve optimal compression of network model parameters taken into account the trade-off parameters. Additionally, the design of efficient and trustworthy FL for PRS is also required to improve overall efficiency and reduce communications costs. Generally, user consumer electronic devices are intelligent and numerous devices are connected to the dynamic and complex infrastructure, therefore client selection model should also need to follow the dynamic schedule strategy to ensure robust performance from the users' devices.

B. Explainability in FL-based PRS

As stated previously, FL empowers data sharing while preserving privacy within a decentralized context. PRS heavily relies on the data for developing informed recommendation models. Federated Recommended Systems (FedRS) is now widely considered to improve recommendation performance with the ability to collaborate the data from different systems. However, despite these significant benefits, FEdRS exhibits many challenges some of which are discussed notably relating to the computation and communication costs and privacy. Additionally, stakeholders within the PRS ecosystem including users and service providers also demand a transparent, fair, and understandable PRS model which should be accurate and meaningful to them [80]. Explainability (XAI) is the core for the development of trustworthy FedRS models, which ensure a certain level of explainability (i.e., details and reasons a model gives to make its functioning clear or easy to understand) and transparency (i.e., characteristics of a model to be inherently understandable for a human) of the generated models [81], [82]. European Commission's Ethic Guidelines for Trustworthy AI mentioned that "AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned" [83]. The XAI in FL should ensure an adequate degree of explainability of the FL-based PRS to develop FedRS. To this end, XAI in FL aims to contribute trustworthy PRS that ensures a transparent, fair, and understandable recommended system to all user levels.

Explainability for PRS ensures that the models should be easily understandable and provide straightforward reasoning for the recommendation results. However, this task is quite challenging specifically the development of a trustworthy, unbiased, and understandable PRS model requires multiple stages including data presentation, recommendation, and evaluation in a complex and dynamic environment. To this end, future work needs to focus on developing methods and models within multiple aspects including novel data processing techniques, FL-based explainable learning models, and advanced representation learning techniques that aim to remove the bias and retain the genuine data while preserving the privacy of the extracted data [84] [76]. Additionally, the PRS model needs to consider beyond accuracy oriented approach for an effective trustworthy model evaluation. In this context, future direction needs to consider the development of novel trustworthiness evaluation schemes and metrics from both technical and ethical dimensions taking into account the accuracy, transparency, explainability, and privacy of the model as well as the model's impact on the potential user groups. The aforementioned future directions advocate to consider human-centric approaches for achieving Explainability in FL-based PRS.

C. Integration of 5G and Beyond Networks

The emergence of 5G technology significantly increases the wider adoption of PRS due to the high data transmission rate and low energy consumption across the networks within diverse platforms. This technology facilities faster high-volume data transmission and supports the development of real-time PRS by reducing the time interval between the user's behavior and the system's feedback and updating the recommendation model accordingly. Therefore 5G accelerates the development of the PRS based on the evolving needs of the relevant stakeholder. Data for the PRS can be collected from various sources including cloud infrastructure which certainly increase the transmission latency and volume and the processing model of 5G can determine based on the data and latency. The application of 5G technology in the PRS will improve efficiency and enhance the user experience with the recommended system. Despite the benefits, 5G can also pose challenges specifically relating to potential cyber-attacks and data leakage due to the transmission of huge data volume [85] [86]. Therefore, there is a need to develop methods and techniques to enhance the capability of real-time PRS with the integration of 5G technology.

The future research direction of PRS needs to develop robust algorithms for the real-time PRS model driven by 5G and other technologies including AI and IoT. PRS needs to provide a good user interface so that the user can easily understand and operate with the personalized recommendation model and value the identified products. 5G can process large volumes of data which can provide better-customized recommendations, but this can pose data leakage and loss [87]. It is necessary to develop new models and techniques to reduce the transmission delay and filter unnecessary information for a more secure and reliable recommendation system.

V. Conclusion

In this review paper, we discussed the next-generation consumer electronics and how personalized recommendation

systems can accurately model user preferences from their historical interactions. Then, we discussed the security and privacy challenges of personalized recommendation systems and the importance of federated learning to enhance data privacy and security with low-latency network communication. Finally, we outlined a few challenges that need to be addressed while implementing federated learning-based personalized recommendation systems for next-gen consumer electronics.

REFERENCES

[1] S. C. M. Insights, "Revenue of the consumer electronics market worldwide from 2018 to 2028," 2023, online; accessed 10-April-2023. [Online]. Available: https://www.statista.com/forecasts/1286653/worldwide-consumer-electronics-market-revenue

[2] M. A. Kesselman and W. Esquivel, "Technology on the move, consumer electronics show 2022: the evolving metaverse and much more," *Library Hi Tech News*, no. ahead-of-print, 2022.

[3] M. G. Kibria, K. Nguyen, G. P. Villardi, O. Zhao, K. Ishizu, and F. Kojima, "Big data analytics, machine learning, and artificial intelligence in next-generation wireless networks," *IEEE access*, vol. 6, pp. 32 328–32 338, 2018.

[4] Y. Tian, B. Zheng, Y. Wang, Y. Zhang, and Q. Wu, "College library personalized recommendation system based on hybrid recommendation algorithm," *Procedia CIRP*, vol. 83, pp. 490–494, 2019.

[5] U. Javed, K. Shaukat, I. A. Hameed, F. Iqbal, T. M. Alam, and S. Luo, "A review of content-based and context-based recommendation systems," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 16, no. 3, pp. 274–306, 2021.

[6] M. Rahhali, L. Oughdir, Y. Jedidi, Y. Lahmadi, and M. Z. El Khattabi, "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, 2022, pp. 89–99.

[7] A. Khoshkbarforoushha, A. Khosravian, and R. Ranjan, "Elasticity management of streaming data analytics flows on clouds," *Journal of Computer and System Sciences*, vol. 89, pp. 24–40, 2017.

[8] C. Du, "Bandwidth constrained client selection and scheduling for federated learning over sd-wan," *IET Communications*, vol. 16, pp. 187–194(7), January 2022. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/cmu2.12333

[9] K. Li and C. Xiao, "Cbfl: A communication-efficient federated learning framework from data redundancy perspective," *IEEE Systems Journal*, vol. 16, no. 4, pp. 5572–5583, 2022.

[10] B. Burke, "Gartner top strategic technology trends for 2022," 2020.

[11] D. Javeed, M. S. Saeed, I. Ahmad, P. Kumar, A. Jolfaei, and M. Tahir, "An intelligent intrusion detection system for smart consumer electronics network," *IEEE Transactions on Consumer Electronics*, 2023.

[12] D. Javeed, T. Gao, M. S. Saeed, and P. Kumar, "An intrusion detection system for edge-envisioned smart agriculture in extreme environment," *IEEE Internet of Things Journal*, 2023.

[13] T. Panch, H. Mattie, and L. A. Celi, "The "inconvenient truth" about ai in healthcare," *NPJ digital medicine*, vol. 2, no. 1, p. 77, 2019.

[14] L. Cao, "Ai in finance: challenges, techniques, and opportunities," *ACM Computing Surveys (CSUR)*, vol. 55, no. 3, pp. 1–38, 2022.

[15] D. Javeed, T. Gao, M. S. Saeed, and M. T. Khan, "Fog-empowered augmented intelligence-based proactive defensive mechanism for iot-enabled smart industries," *IEEE Internet of Things Journal*, 2023.

[16] E. K. Nti, S. J. Cobbina, E. E. Attafuah, E. Opoku, and M. A. Gyan, "Environmental sustainability technologies in biodiversity, energy, transportation and water management using artificial intelligence: A systematic review," *Sustainable Futures*, p. 100068, 2022.

[17] J. Singh, Y. Goel, S. Jain, and S. Yadav, "Virtual mouse and assistant: A technological revolution of artificial intelligence," *arXiv preprint arXiv:2303.06309*, 2023.

[18] Y. Yin, P. Zheng, C. Li, and L. Wang, "A state-of-the-art survey on augmented reality-assisted digital twin for futuristic human-centric industry transformation," *Robotics and Computer-Integrated Manufacturing*, vol. 81, p. 102515, 2023.

[19] R. Llamas, "Worldwide augmented and virtual reality hardware forecast, 2018–2022. january 2018."

[20] M. DARWISH, S. KAMEL, and A. ASSEM, "Extended reality for enhancing spatial ability in architecture design education," *Ain Shams Engineering Journal*, p. 102104, 2023.

[21] L. Gong, Å. Fast-Berglund, and B. Johansson, "A framework for extended reality system development in manufacturing," *IEEE Access*, vol. 9, pp. 24 796–24 813, 2021.

[22] S. M. Iqbal, I. Mahgoub, E. Du, M. A. Leavitt, and W. Asghar, "Advances in healthcare wearable devices," *NPJ Flexible Electronics*, vol. 5, no. 1, p. 9, 2021.

[23] J. J. Ferreira, C. I. Fernandes, H. G. Rammal, and P. M. Veiga, "Wearable technology and consumer interaction: A systematic review and research agenda," *Computers in Human Behavior*, vol. 118, p. 106710, 2021.

[24] X. M. Alimdjanovna *et al.*, "Climate control and light control in a smart home," *European Journal of Interdisciplinary Research and Development*, vol. 8, pp. 149–155, 2022.

[25] L. Reid and G. Sisel, "Digital care at home: Exploring the role of smart consumer devices," *Health & Place*, vol. 80, p. 102961, 2023.

[26] S. S. Gill, M. Xu, C. Ottaviani, P. Patros, R. Bahsoon, A. Shaghaghi, M. Golec, V. Stankovski, H. Wu, A. Abraham *et al.*, "Ai for next generation computing: Emerging trends and future directions," *Internet of Things*, vol. 19, p. 100514, 2022.

[27] R. Ranjan, O. Rana, S. Nepal, M. Yousif, P. James, Z. Wen, S. Barr, P. Watson, P. P. Jayaraman, D. Georgakopoulos *et al.*, "The next grand challenges: Integrating the internet of things and data science," *IEEE Cloud Computing*, vol. 5, no. 3, pp. 12–26, 2018.

[28] Y. Koren, S. Rendle, and R. Bell, "Advances in collaborative filtering," *Recommender systems handbook*, pp. 91–142, 2021.

[29] N. Nassar, A. Jafar, and Y. Rahhal, "A novel deep multi-criteria collaborative filtering model for recommendation system," *Knowledge-Based Systems*, vol. 187, p. 104811, 2020.

[30] J. Bu, X. Shen, B. Xu, C. Chen, X. He, and D. Cai, "Improving collaborative recommendation via user-item subgroups," *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 9, pp. 2363–2375, 2016.

[31] F. Wang, H. Zhu, G. Srivastava, S. Li, M. R. Khosravi, and L. Qi, "Robust collaborative filtering recommendation with user-item-trust records," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 4, pp. 986–996, 2021.

[32] X. Wu, B. Cheng, and J. Chen, "Collaborative filtering service recommendation based on a novel similarity computation method," *IEEE Transactions on Services Computing*, vol. 10, no. 3, pp. 352–365, 2015.

[33] F. Xue, X. He, X. Wang, J. Xu, K. Liu, and R. Hong, "Deep item-based collaborative filtering for top-n recommendation," *ACM Transactions on Information Systems (TOIS)*, vol. 37, no. 3, pp. 1–25, 2019.

[34] H. Ning, S. Dhelim, and N. Aung, "Personet: Friend recommendation system based on big-five personality traits and hybrid filtering," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 3, pp. 394–402, 2019.

[35] B. Smith and G. Linden, "Two decades of recommender systems at amazon. com," *Ieee internet computing*, vol. 21, no. 3, pp. 12–18, 2017.

[36] Z. Zhou, Z. Cheng, L.-J. Zhang, W. Gaaloul, and K. Ning, "Scientific workflow clustering and recommendation leveraging layer hierarchical analysis," *IEEE Transactions on Services Computing*, vol. 11, no. 1, pp. 169–183, 2016.

[37] W. Zhang and J. Wang, "A collective bayesian poisson factorization model for cold-start local event recommendation," in *Proceedings of the 21th ACM SIGKDD international conference on knowledge discovery and data mining*, 2015, pp. 1455–1464.

[38] A. Paterek, "Improving regularized singular value decomposition for collaborative filtering," in *Proceedings of KDD cup and workshop*, vol. 2007, 2007, pp. 5–8.

[39] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Transactions on Communications*, vol. 68, no. 8, pp. 4734–4746, 2020.

[40] B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things," *IEEE Internet of Things Journal*, 2022.

[41] A. A. Khaliq, A. Anjum, A. B. Ajmal, J. L. Webber, A. Mehbodniya, and S. Khan, "A secure and privacy preserved parking recommender system using elliptic curve cryptography and local differential privacy," *IEEE Access*, vol. 10, pp. 56 410–56 426, 2022.

[42] Y. Himeur, A. Sayed, A. Alsalemi, F. Bensaali, A. Amira, I. Varlamis, M. Eirinaki, C. Sardianos, and G. Dimitrakopoulos, "Blockchain-based recommender systems: Applications, challenges and future opportunities," *Computer Science Review*, vol. 43, p. 100439, 2022.

[43] K. Sruthi and S. Prabhu, "Influence of consumer decisions by recommendar system in fashion e-commerce website," in *2022 International Conference on Decision Aid Sciences and Applications (DASA)*. IEEE, 2022, pp. 421–424.

[44] S. Zhang, W. Yuan, and H. Yin, "Comprehensive privacy analysis on federated recommender system against attribute inference attacks," *IEEE Transactions on Knowledge and Data Engineering*, 2023.

[45] M. Dong, F. Yuan, L. Yao, X. Wang, X. Xu, and L. Zhu, "A survey for trust-aware recommender systems: A deep learning perspective," *Knowledge-Based Systems*, vol. 249, p. 108954, 2022.

[46] D. Nawara and R. Kashef, "Context-aware recommendation systems in the iot environment (iot-cars)–a comprehensive overview," *IEEE Access*, vol. 9, pp. 144 270–144 284, 2021.

[47] A. Vultureanu-Albişi and C. Bădică, "Recommender systems: An explainable ai perspective," in *2021 International Conference on INnovations in Intelligent SysTems and Applications (INISTA)*. IEEE, 2021, pp. 1–6.

[48] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*. PMLR, 2017, pp. 1273–1282.

[49] G. Wei, Q. Wu, and M. Zhou, "A hybrid probabilistic multiobjective evolutionary algorithm for commercial recommendation systems," *IEEE Transactions on Computational Social Systems*, vol. 8, no. 3, pp. 589–598, 2021.

[50] B. Cao, Y. Zhang, J. Zhao, X. Liu, Ł. Skonieczny, and Z. Lv, "Recommendation based on large-scale many-objective optimization for the intelligent internet of things system," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 15 030–15 038, 2021.

[51] B. Tan, B. Liu, V. Zheng, and Q. Yang, "A federated recommender system for online services," in *Proceedings of the 14th ACM Conference on Recommender Systems*, 2020, pp. 579–581.

[52] S. Kanwal, S. Nawaz, M. K. Malik, and Z. Nawaz, "A review of text-based recommendation systems," *IEEE Access*, vol. 9, pp. 31 638–31 661, 2021.

[53] P. M. Alamdari, N. J. Navimipour, M. Hosseinzadeh, A. A. Safaei, and A. Darwesh, "A systematic study on the recommender systems in the e-commerce," *Ieee Access*, vol. 8, pp. 115 694–115 716, 2020.

[54] K. Yu, Z. Guo, Y. Shen, W. Wang, J. C.-W. Lin, and T. Sato, "Secure artificial intelligence of things for implicit group recommendations," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2698–2707, 2021.

[55] Y. Himeur, S. S. Sohail, F. Bensaali, A. Amira, and M. Alazab, "Latest trends of security and privacy in recommender systems: a comprehensive review and future perspectives," *Computers & Security*, p. 102746, 2022.

[56] A. B. Suhaim and J. Berri, "Context-aware recommender systems for social networks: review, challenges and opportunities," *IEEE Access*, vol. 9, pp. 57 440–57 463, 2021.

[57] T. B. Ogunseyi, T. Bo, and C. Yang, "A privacy-preserving framework for cross-domain recommender systems," *Computers & Electrical Engineering*, vol. 93, p. 107213, 2021.

[58] M. del Carmen Rodríguez-Hernández and S. Ilarri, "Ai-based mobile context-aware recommender systems from an information management perspective: Progress and directions," *Knowledge-Based Systems*, vol. 215, p. 106740, 2021.

[59] C. Li, J. Zhang, X. Yang, and L. Youlong, "Lightweight blockchain consensus mechanism and storage optimization for resource-constrained iot devices," *Information Processing & Management*, vol. 58, no. 4, p. 102602, 2021.

[60] Z. Xue, P. Zhou, Z. Xu, X. Wang, Y. Xie, X. Ding, and S. Wen, "A resource-constrained and privacy-preserving edge-computing-enabled clinical decision system: A federated reinforcement learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 9122–9138, 2021.

[61] J. H. Khor, M. Sidorov, and P. Y. Woon, "Public blockchains for resource-constrained iot devices—a state-of-the-art survey," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 11 960–11 982, 2021.

[62] V. A. Thakor, M. A. Razzaque, and M. R. Khandaker, "Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28 177–28 193, 2021.

[63] S. J. Nawaz, S. K. Sharma, M. N. Patwary, and M. Asaduzzaman, "Next-generation consumer electronics for 6g wireless era," *IEEE Access*, vol. 9, pp. 143 198–143 211, 2021.

[64] M. Savi and F. Olivadese, "Short-term energy consumption forecasting at the edge: A federated learning approach," *IEEE Access*, vol. 9, pp. 95 949–95 969, 2021.

[65] C. K. Wu, C.-T. Cheng, Y. Uwate, G. Chen, S. Mumtaz, and K. F. Tsang, "State-of-the-art and research opportunities for next-generation consumer electronics," *IEEE Transactions on Consumer Electronics*, 2022.

[66] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for iot security attacks," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2545–2554, 2021.

[67] A. Makkar, U. Ghosh, D. B. Rawat, and J. H. Abawajy, "Fedlearnsp: Preserving privacy and security using federated learning and edge computing," *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 21–27, 2021.

[68] A. R. Short, H. C. Leligou, M. Papoutsidakis, and E. Theocharis, "Using blockchain technologies to improve security in federated learning systems," in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2020, pp. 1183–1188.

[69] L. Cui, Y. Qu, G. Xie, D. Zeng, R. Li, S. Shen, and S. Yu, "Security and privacy-enhanced federated learning for anomaly detection in iot infrastructures," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3492–3500, 2021.

[70] K. Cheng, T. Fan, Y. Jin, Y. Liu, T. Chen, D. Papadopoulos, and Q. Yang, "Secureboost: A lossless federated learning framework," *IEEE Intelligent Systems*, vol. 36, no. 6, pp. 87–98, 2021.

[71] E. Samikwa, A. Di Maio, and T. Braun, "Adaptive early exit of computation for energy-efficient and low-latency machine learning over iot networks," in *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2022, pp. 200–206.

[72] M. Asad, A. Moustafa, T. Ito, and M. Aslam, "Evaluating the communication efficiency in federated learning algorithms," in *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. IEEE, 2021, pp. 552–557.

[73] W. Qi and H. Su, "A cybertwin based multimodal network for ecg patterns monitoring using deep learning," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 6663–6670, 2022.

[74] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020.

[75] W. Xia, W. Wen, K.-K. Wong, T. Q. Quek, J. Zhang, and H. Zhu, "Federated-learning-based client scheduling for low-latency wireless communications," *IEEE Wireless Communications*, vol. 28, no. 2, pp. 32–38, 2021.

[76] Z. Sun, Y. Xu, Y. Liu, W. He, L. Kong, F. Wu, Y. Jiang, and L. Cui, "A survey on federated recommendation systems," 2023.

[77] Z. Z. L. Y. Wen, J., "A survey on federated learning: challenges and applications," *Int. J. Mach. Learn. Cyber.*, vol. 14, no. 4, p. 513–535, 2023.

[78] F. K. Khan, A. Flanagan, K. E. Tan, Z. Alamgir, and M. A. ud din, "A payload optimization method for federated recommender systems," in *Fifteenth ACM Conference on Recommender Systems*. ACM, sep 2021. [Online]. Available: https://doi.org/10.1145%2F3460231.3474257

[79] T. Nishio and R. Yonetani, "Client selection for federated learning with heterogeneous resources in mobile edge," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. IEEE, may 2019. [Online]. Available: https://doi.org/10.1109%2Ficc.2019.8761315

[80] S. Wang, X. Zhang, Y. Wang, H. Liu, and F. Ricci, "Trustworthy recommender systems," 2022.

[81] A. B. Arrieta, N. Díaz-Rodríguez, J. D. Ser, A. Bennetot, S. Tabik, A. Barbado, S. García, S. Gil-López, D. Molina, R. Benjamins, R. Chatila, and F. Herrera, "Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible ai," 2019.

[82] D. Javeed, T. Gao, P. Kumar, and A. Jolfaei, "An explainable and resilient intrusion detection system for industry 5.0," *IEEE Transactions on Consumer Electronics*, 2023.

[83] "High-level expert group on ai, report, european commission," 2019. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[84] R. U. Yuwen Xiong, Mengye Ren, "Loco: local contrastive representation learning," *NIPS'20: Proceedings of the 34th International Conference on Neural Information Processing Systems*.

[85] Z. Cai and Z. He, "Trading private range counting over big iot data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 2019, pp. 144–153.

[86] W. Huang, B. Liu, and H. Tang, "Privacy protection for recommendation system: A survey," *Journal of Physics: Conference Series*, vol. 1325, no. 1, p. 012087, oct 2019. [Online]. Available: https://dx.doi.org/10.1088/1742-6596/1325/1/012087

[87] G. Li, G. Yin, J. Yang, F. Chen, and J. Wang, "Sdrm-ldp: A recommendation model based on local differential privacy," vol. 2021, 2021. [Online]. Available: https://doi.org/10.1155/2021/6640667