sensors

MDPI

Review

Federated Learning in Smart City Sensing: Challenges and Opportunities

Ji Chu Jiang [1], Burak Kantarci [1,*], Sema Oktug [2] and Tolga Soyata [3]

[1] School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON K1N 6N5, Canada; jjian057@uottawa.ca
[2] Faculty of Computer and Informatics Engineering, Istanbul Technical University, Maslak, 34469 Istanbul, Turkey; oktug@itu.edu.tr
[3] Whiting School of Engineering, Johns Hopkins University, Baltimore, MD 21218, USA; tolgasoyata@gmail.com
* Correspondence: burak.kantarci@uottawa.ca; Tel.: +1-613-562-5800 (ext. 6955)

Received: 1 September 2020; Accepted: 26 October 2020; Published: 31 October 2020

Abstract: Smart Cities sensing is an emerging paradigm to facilitate the transition into smart city services. The advent of the Internet of Things (IoT) and the widespread use of mobile devices with computing and sensing capabilities has motivated applications that require data acquisition at a societal scale. These valuable data can be leveraged to train advanced Artificial Intelligence (AI) models that serve various smart services that benefit society in all aspects. Despite their effectiveness, legacy data acquisition models backed with centralized Machine Learning models entail security and privacy concerns, and lead to less participation in large-scale sensing and data provision for smart city services. To overcome these challenges, Federated Learning is a novel concept that can serve as a solution to the privacy and security issues encountered within the process of data collection. This survey article presents an overview of smart city sensing and its current challenges followed by the potential of Federated Learning in addressing those challenges. A comprehensive discussion of the state-of-the-art methods for Federated Learning is provided along with an in-depth discussion on the applicability of Federated Learning in smart city sensing; clear insights on open issues, challenges, and opportunities in this field are provided as guidance for the researchers studying this subject matter.

Keywords: federated learning; machine learning; smart cities sensing; internet of things; security; privacy

1. Introduction

The global population is witnessing rapid annual growth, especially within urban city settings [1]. Maintaining efficient management of a wide span of information and resources is becoming increasingly more difficult amid growing population, electronic devices, and data transmission [2]. These challenges associated with the growth of such services has motivated governments to look for efficient ways to manage the operation of a city with respect to resource allocation and triggered initiatives around the world to have a connected city system where each component leverages the use of connected technology; these components include the following: economy and finance, citizens, governance, transportation (i.e., mobility), sustainability (i.e., environment), and smart living [3–6].

The latest advancements in wireless communication technology have propelled the widespread use of smart technologies, cloud computing, and the Internet of Things (IoT) [7]. IoT is the network of devices that enables connectivity between people, things or services [8–11]. Advances in manufacturing, sensor and cloud technologies results in a predicted up to 100 billion (with a minimum

of 50 billion) devices with Internet connectivity by the end of 2020 [12]. The IoT-cloud environment enables data acquisition and transmission from all parts of a city while the data is processed in the cloud at a centralized server. The widespread use of smart technologies within communities and services has created the building blocks of a smart city [13]. Application areas within smart cities span from smart energy grid, smart transportation services, smart water distribution to smart homes [14–18]. A basic smart city ecosystem is displayed in Figure 1. Sensing as a service is also a vital role that contributes to a smart city [1,19,20]. The Sensing as a Service (S^2aaS) concept allows the acquired and aggregated data from embedded/built-in (i.e., non-dedicated) sensors in personal devices available to cloud users. This in turns alleviates companies from the requirement of their own sensing infrastructure. Mobile Crowdsensing is an emerging non-dedicated sensing method within smart cities sensing that uses the falls under the Sensing as a service business model. Where people are recruited into sensing campaigns and are compensated for the data collected by their personal devices [21,22].

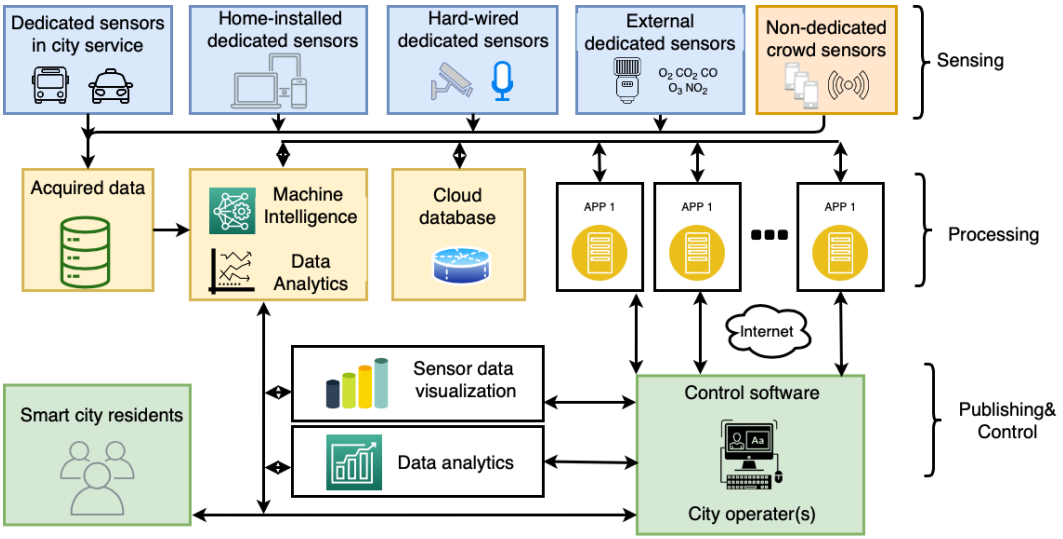

Figure 1. Smart City Sensing Ecosystem [23].

Sensing as a service can address many challenges within smart cities [19]. Sensing allows smart services to self-monitor and react to dynamically changing events. An example of this is transportation, monitoring roads, bridges and providing the collected data to more efficiently direct traffic [24]. The data gathered from sensors enables a more efficient resource distribution in a real-time environment. Sensors are becoming increasingly prevalent and abundant within an urban setting, this is due to the reduced production cost of high-quality sensors and the wide spread embedded nature of sensors within smart devices [25]. Various applications can benefit from S^2aaS and/or Mobile Crowdsensing so to help propel the big data trend in which large amounts of quality data to become available for processing. The data is often processed with machine learning, deep learning and statistical methods to generate a trend or conclusion [26]. For example, the microphones on mobile devices can be used to monitor noise levels in communities. Sensing as a Service and Mobile Crowdsensing is most prevalent in optimizing traffic control in smart cities. Real-time data relating to traffic congestion, road conditions, parking availability and malfunctioning traffic lights are collected and processed [27]. The best routes can be sent to each individual driver to reduce congestion and avoid accidents. Although known obstacles can be shared as they arise, Brisimi et al. [28] proposed a method of detecting street obstacles that uses smartphone sensing information. This scheme can also be applied to crowd control within a city, such as optimizing the exit route for crowds leaving a sports tournament or concert.

Smart city sensing leverage two main types of paradigms with respect to the operational aspects of sensing systems: (1) dedicated and (2) non-dedicated [23]. Dedicated sensing is when a network of sensors is deployed specifically and permanently for a particular sensing application [27].

There is a plethora of sensors that are distributed throughout a city, however, to reduce the load and expand the sensing capabilities, sensing tasks can be subcontracted to non-dedicated sensors. Although non-dedicated sensing is when mobile sensors are recruited to obtain, process and transmit data to a centralized server, these sensors are not specifically created and deployed for a sensing task, therefore they are considered non-dedicated. Sensor-cloud networks are a novel non-dedicated sensing solution for collaborative sensing tasks in smart cities. A sensor-cloud environment enables the connection of physical sensor nodes to a cloud platform where multiple organization and users can use these sensors for their specific applications [29]. These are considered non-dedicated sensors since the end-user dictates the application and uses of these sensors, while the application changes depending on the need. It is a pay-per-use model that alleviates the massive initial investment cost from one organization [30]. An emerging effective non-dedicated paradigm in smart cities sensing is Mobile Crowdsensing, it is cost effect, highly scalable and has vast mobility. Mobile Crowdsensing allows users participate in a sensing event by providing data through their sensor-enabled mobile devices [31]. Modern phones contain a wide array of sensors such as magnetometer, gyroscope, accelerometer, GPS, camera, proximity sensor, microphone, pedometer, ambient light sensor, barometer and thermometer. The operational differences between the sensing paradigms (i.e., dedicated or non-dedicated) are apparent in several aspects, such as security, sensing performance and implementation cost. Dedicated sensing systems often lead to high expenditures for initial deployment and recurring costs for maintenance, whereas when sensors are not dedicated, it becomes possible to eliminate these upfront costs through using the participant's pre-existing devices. The challenges for Mobile Crowdsensing is the process of recruiting users and incentivizing users [32–34]. The availability of users for a sensing event is not guaranteed due to the irrational ad-hoc nature of Mobile Crowdsensing networks. Furthermore, by using user devices for sensing, the users are exposed to potential privacy leaks [35–39].

This survey covers the capabilities and uses of Federated Learning within smart cities sensing applications. This survey gives a review and a qualitative analysis on how the novel Federated Learning solution can be integrated into smart city sensing to solve the challenges that are currently present. There has been surveys that have extensively covered smart cities sensing [40]. Although Federated Learning is an emerging field, there are a few prominent surveys within this field. The study in [41] covered Federated Learning within mobile edge networks.The authors in [42] presented a survey on the threats to Federated Learning, focusing on poisoning attacks and inference attacks. The authors in [43] presented a survey that detailed the current status and challenges of Federated Learning. This survey compliments the aforementioned surveys by introducing the Federated Learning methodology for smart cities sensing. Smart cities sensing is a key collaborative application that can greatly benefit from the Federated Learning methodology.

The rest of the survey is as follows: Section 2 explains the challenges in current smart cities sensing. Section 3 presents current state-of-the-art Federated Learning solutions. Section 4 shows how Federated Learning can be incorporated into smart cities sensing. Section 5 covers the open issues and challenges remaining in smart cities sensing and Federated Learning methodologies. Section 6 concludes the article.

2. Challenges in Smart Cities Sensing

This section covers the major categories that befall smart cities sensing. Habibzadeh et al. [27] classify smart city sensing under dedicated and non-dedicated sensing with the following descriptions for each category: dedicated sensing stands for the traditional way of gathering data where specific sensors are deployed throughout the city to obtain certain sensing data. The range and purpose of these sensors are fixed, therefore optimal planning for node deployment is vital. This limitation also applies to non-dedicated solutions such as sensor-cloud networks. However, within the non-dedicated sensing field, Mobile Crowdsensing that uses sensors present in smart devices to provide sensing services has proven to show comparative advantages with respect to dedicated sensing and sensor networks. Mobile Crowdsensing is becoming more prevalent with its advantages of flexible coverage

areas and low overhead costs. The types of data that can be collected is only limited to the sensors present in the smart devices. The data generated can be used to analyze a wider range applications, especially applications related to human behavior since the source of the data is directly from users. This survey explores opportunities and challenges of integrating federating learning with smart cities sensing. However, most nodes deployed for dedicated sensing are currently not equipped with sufficient processing power to support a Federated Learning scenario. Deployment of nodes dedicated sensing is costly due to the initial investment in sensors, equipping these fixed sensors with processors that are capable of training large machine learning models would incur tremendous overhead costs. With the rise in processing power within smart phones and advent of autonomous vehicles, bridging Federated Learning and non-dedicated sensing is a viable solution.

Mobile Crowdsensing is the most common solution to smart cities non-dedicated sensing. With the growth of mobile Internet technology and applications, mobile smart devices have been widely used and greatly popularized [44]. The advent of wireless communication technology and sensor technology makes the use of mobile sensing devices to build a sensing network in a wider range and more complex environment a reality [45]. Smart mobile devices have improved greatly in many areas, such as computing power, storage capacity, and communication capabilities, they also have integrated rich sensors (such as temperature sensors, gravity sensors, acceleration sensors, and so on) and the ubiquitous sensing network make ordinary users able to participate in sensing activities that helps collect the surrounding environmental conditions provides hardware infrastructure support for ubiquitous depth sensing and computing [46]. However, the allocation of huge sensing tasks and the coordination of large-scale sensing devices are the challenges and barriers to achieving ubiquitous depth sensing, as well as computing [47].

Under these circumstances, the proposal and implementation of the Mobile Crowdsensing, which is a cloud-inspired business model, aims at coupling mobile sensing and crowdsourcing towards bridging the gap between hardware infrastructure and ubiquitous depth sensing and computing to form a brand-new IoT sensing model [48], which is a Mobile Crowdsensing network, by coordinating ordinary users' mobile intelligent devices and mobile sensing devices to perceive their environment and process environmental awareness data through collection, fusion, analysis, mining and other links to restore the user state, situation and environment to collaboratively complete a large sensing task [49]. The mobile network provides a brand-new solution to the complex ubiquitous depth sensing problem [50]. It entails a broad range of scenarios and prospects for applications, and there are new challenges in technology and application research [51].

Mobile Crowdsensing refers to the use of smart mobile devices (e.g., tablets, smart phones, smart wearables, in-vehicle equipment, etc.) that belong to recruited users for a specific sensing campaign and mobile sensing devices as basic sensing units, through mobile Internet or wireless network for conscious or unconscious cooperation to realize the distribution of sensing tasks and the acquisition and processing of the crowd-sensed data to complete complex sensing tasks in real time [52].

Mobile Crowdsensing is usually composed of two parts: the users and the platform [37]. The users are individuals that are recruited for the particular sensing campaign. They use sensors present on smart mobile devices to provide the desired data. The platform is often comprised of a server with data storage centers. The users interact and communicate through the platform according to predefined rules set by the service provider and are compensated based on their contributions [53].

2.1. Data Trustworthiness

An efficient Mobile Crowdsensing campaign tightly depends on the truthfulness of the crowd-sensed data. The reliability of gathered data can heavily impact the analysis outcome [54]. This is often done by malicious users or attackers that want to sway the outcome into a scenario that is beneficial to them. This can be done by either submitting false data or by distorting the data during the transmission process. Therefore, ensuring data trustworthiness is a vital step to an efficient and reliable sensing campaign [55]. Cryptographic technologies such as digital signatures, message authentication

codes and biometrics are the main methodologies to authenticate the users [56–58]. However, these methods do not always guarantee that the data provided by the users is authentic. The data division and other processing measures will bring challenges to the authenticity and integrity of the data [59]. In addition, infrastructure can also be deployed in the sensing area as a reference point and eyewitness for sensing data to verify the authenticity of the sensing data submitted by users, but this solution requires additional expensive infrastructure deployment costs [60,61].

2.2. User Incentives

In the Mobile Crowdsensing network, ordinary users are chosen to participate and provide sensing data to complete the social sensing tasks [32,62,63]. However, users participating in sensing needs to pay a certain price (such as consumption of resources, disclosure of privacy, etc.) [34]. Without a certain incentive and compensation mechanism, it is difficult to attract a large participant population to actively participate in large-scale social tasks [33]. Many studies have been proposed based on this incentive mechanism, such as using game theory to explore user habits and preferences, and evaluating and improving the relevance of online search engines [64].

Due to the constraints that limit the participation of users and heterogeneity of the crowdsensing environment affecting the quality of the acquired data, the development of Mobile Crowdsensing has been seriously affected [65]. In response to this problem, the Mobile Crowdsensing incentive mechanism adopts appropriate incentives models to encourage and stimulate participants to participate in sensing tasks [66]. Incentive methods yield different results depending on the participant groups.

The research of the Mobile Crowdsensing incentive mechanism not only needs to adopt appropriate incentive methods, but more importantly, through different incentive methods, solve the core problems faced by both the server platform and the participants in maximizing their respective utility, so as to achieve the role of incentives [67]. The main task of the sensing task server is to incentivize more participants under the condition that the payment cost is minimum, or the payment cost is controllable [68]. Both the participation level of the participants needs to be improved, and the sensing data of the participants must be high quality and reliable [69]. Privacy and resource consumption are two major reasons that prevents a capable user from actively participating in a sensing task [70].

Adopting appropriate incentives can achieve certain incentive effects [71]. However, the study of incentive mechanisms is not only a study of incentives, but more importantly, through the use of reasonable incentives and effective key technologies, both the server platform and the participants maximize the core problems faced by each utility to achieve the role of incentives [72]. These core issues are mainly concerned with: participation level, completion quality, payment control, efficiency and energy consumption, privacy and security, and online real-time processing as reported by Khan et al. [73]. These issues will be elaborated below.

(1) Participation level: The incentive mechanism is used for user recruitment into a sensing campaign. An increased participation rate improves the success rate for the sensing campaign [74]. At the same time, preserving participants will result in long-term collaborations that is beneficial to both parties [35]. The server platform not only expects that participants will join the sensing campaigns, it also expects that any joining participant will remain in the crowdsensing system for an extended length of time to provide long-term data sensing for the sensing task [75]. In addition, the feedback effect of the participation level on the incentive mechanism is also a problem worthy of study [76].

(2) Completion quality: The completion of the sensing task is not only dependent on participation rate, it is also necessary to consider the impact of user location, user behavior, and data quality on the quality of task completion [77]. Mobile Crowdsensing tasks are mostly position-sensitive [78]. The user geo-coordinates will impact the overall quality and value of the sensed data [79]. Participants may intentionally report false data due to their inherent selfishness to affect the perceived data quality [80].

In addition, the sensitivity of the sensing device itself and the limitations of the participants themselves will also affect the task completion quality [81].

(3) Payment control: As a server platform, it is often necessary to pay a certain amount of remuneration to the participants' perceived data. The payment should be proportional to the quality of user-provided data [82]. Users should be compensated based on the utility they bring to the sensing task [83].

(4) Efficiency and energy consumption: Efficiency and energy consumption not only mean that the server needs an efficient algorithm to process the incentive procedure, but also that the participant hopes that the incentive procedure can lower the resource usage on the sensing device end [84]. The resource consumption of the sensing device is an important factor that prevents participants from participating in a sensing campaign [85]. The mechanism needs to minimize the consumption of these resources [86]. Efficient algorithms are an indispensable part of the incentive mechanism to improve efficiency and reduce running time [87].

(5) Privacy and security: This category includes the privacy concerns of users and the security measures to protect the data in motion and at rest in the server [88]. Participants do not want to disclose personal privacy data when uploading data in sensing tasks, especially location-sensitive Mobile Crowdsensing [89]. Participants may be dishonest Therefore, the uploaded false data poses data security problems for the server [90]. In addition, malicious attacks by malicious users or other entities also need to be considered [91].

(6) Online real time: According to the difference in processing times, the incentives can be processed either online or offline [92]. Offline processing refers to that the server platform needs to make decisions about the allocation of submitted sensing tasks depending on the information gathered from the individuals in a participant pool [93]. The dynamic random participation of participants and the requirement for real-time feedback require an online mechanism to motivate participants in real time [94].

2.3. Data Quality Management

The Mobile Crowdsensing network uses the user's existing equipment for sensing, therefore the sensing data is possibly neither accurate nor reliable [95]. Although it has benefits of low cost, large sensing scale and fine granularity, it also brings a huge challenge in terms of data sensing quality management [96]. If these inaccurate and unreliable sensing data are not processed, it would be difficult to directly use those data in sensing applications [97]. Optimal data quality management is needed for a successful group-aware network. In other words, in a sensing network, data acquisition is easier however quality management for the acquired data is difficult [98]. The key lies in solving the problem of inaccuracy and unreliability of the perceived data, i.e., data sensing quality management. In traditional sensor networks, because sensors can be calibrated before deployment or their sensing tolerances are known, their data sensing quality management is easier, and the key lies in data acquisition, such as how sensors reduce sensing energy consumption, and reliably transfer data to the center [99].

The sources of sensing data are usually different users and sensors, which have the characteristics of multiple modalities and strong correlations. It is necessary to intelligently analyze and explore these data information to find valuable information and make full use of its value, realize the qualitative change from data to information and finally to knowledge [100]. In the exploration of the value of data information, designing the storage and processing of big data, data quality management, and multi-modal data exploration and other aspects of technology is an important challenge [101].

2.4. Node Deployment

The complexity and variability of IoT environments present grand challenges for node deployment in the sensing layer. This directly impacts the data collection and analysis process due since the issues will be stemmed from the data source.

Environmental impacts can affect the deterioration of sensor components and thus affect the sensing capabilities of those sensors. Interference might be present in the surrounding areas and cause communication loss. These factors cause unavoidable loss that in turn lead to incomplete data [102].

Another major issue is the coverage area of the deployed nodes. The coverage area is predefined in dedicated sensors; therefore, this metric can be optimized for certain scenarios. It cannot be changed, whereas sensing requirements often change over time. Mobile Crowdsensing sensing nodes are often mobile and can adapt depending on the sensing task. However, the population and device density and participation rate are all factors that can hinder the sensing campaign. Mobile Crowdsensing is completely reliant on the crowd availability. This means that Mobile Crowdsensing sensors performs best in well populated urban metropolitan districts where there is an ample amount of people with smart devices to achieve a wide coverage [103].

2.5. Energy Consumption

Resource consumption is still a major challenge in mobile devices during sensing campaigns. These resources include computing, communication and energy resources [104]. Optimizing resource allocation is a key step to improving efficiency in sensing campaigns [105]. However, dynamically allocating resources with for different devices is a difficult task. Oftentimes multiple categories of sensing data are used for one sensing goal, this adds more layers of complexity in the balance of resource allocation. An example of this is when GPS, Wi-Fi and cellular proximity is used to mine positional data. In this case, GPS data consumes the most energy but provides the highest accuracy, a balance between data quality and energy consumption must be evaluated [106].

In the process of continuous application of sensor networks, it is paramount to overcome problems such as node energy, bandwidth and resource constraints in computing, etc., in order to effectively realize its practicality [107]. With the continuous change of time, the quantity of users and the availability of sensors have changed. It is difficult to carry out modeling and prediction work on energy and bandwidth requirements, and it is difficult to complete the sensing task effectively. When selecting an effective subset of users, you need to think about the choice [108]. In the face of a large user pool with different sensing abilities, a more targeted selection methodology needs to be selected. In the case of resource constraints, rationalize the sensing and communication resources [109].

The availability of sensors and sensing tasks changes overtime, therefore developing a model to accurately predict energy consumption with the wide range of unknown and unpredictable parameters is difficult [110].

In addition, many Mobile Crowdsensing applications need to adopt continuous data collection methods to transmit data to the corresponding data centers. The connection between mobile cellular networks and the Internet performs the sensing data transmission, resulting in increased data traffic [111]. Mobile cellular networks bring great pressure. A more effective data transmission method is strongly desired, for example, according to the short-distance wireless communication method, the use of user contact or hotspot sharing to achieve data transmission [112].

2.6. User Privacy Protection

Preserving the privacy for participating users in Mobile Crowdsensing campaigns is a top priority for the server. First, a user mobile device can contain sensitive personal data. Secondly, personal information can be concluded by analyzing the data provided by the user. For example, by collecting sensory data related to the user location on the device (such as GPS, electronic compass, magnetic field sensor, etc.), the user's precise location information can be obtained [36]. Through continued monitoring, the user's home and work address can be pin pointed and their daily routine can be cataloged [113]. Sensory data can be mined from motion sensors that can be used to deduct the living habits and health information related to a certain user.

Another scenario is when motion sensor data is mined from the user, this information can be used to generate a portfolio of the user's daily routine and health information. With the combination

of environmental sensory data, it would be possible to track and predict the user location at any given time [114]. By collecting the sensory data of the biometric sensor, you can discover the user's various biometric features, such as sound, images, fingerprints, basic physiological characteristics, and other highly sensitive privacy information. In addition, collecting the daily use data of users can also mine the user's usage habits, hobbies and behavior characteristics and other deep-level private information [115]. Mobile Crowdsensing enables the optimization of many control sectors, such as pollution, public transportation, traffic congestion, road conditions, etc. However, if sensory data is leaked during the transmission process, it will threaten the privacy of vast amounts of user [116]. Therefore, having appropriate measures to ensure user privacy is preserved is vital in the success of sensing tasks.

3. Review of Federated Learning Solutions

In 2016, Google first proposed the concept of Federated Learning, it is a methodology that is often leveraged for joint training of data in multiple edge devices (such as mobile phones) for centralized model training, and is used in scenarios such as input method improvement [117]. As a new generation of artificial intelligence technology, Federated Learning is penetrating the key difficulties of commercial AI application bottlenecks by solving problems such as data privacy and lack of data and it is reshaping the financial, medical, and urban security fields [43].

In modern times, most enterprises have difficulties in obtaining large quantities of quality data for AI model training. At the same time, the regulatory environment is also gradually strengthening data protection, and relevant policies are being introduced continuously [118]. The data owned by commercial companies often have huge potential value. Often these institutions will not provide their own data to other companies, resulting in data often appearing in the form of islands. Mobile phones and wearable devices are very common data generation devices in modern times [119], which generate huge amounts of data in various forms every day. Considering the requirements of computing power, data transmission, and personal privacy, system deployments are increasingly inclined to store data locally, and model calculations are performed by edge devices [120]. The goal is to design a machine learning framework that meets data privacy, security and regulatory requirements so that artificial intelligence systems can leverage the use of their data more efficiently and accurately [121].

Federated Learning is essentially a distributed machine learning technology or machine learning framework. The formal definition of Federated Learning can be defined as: Joint training of machine learning models with distributed devices and local data under federation. Federated Learning requires learning a global statistical model from the massive information stored in millions of remote devices [117]. Federated Learning methodologies enables machine learning models to be trained effectively while ensuring legal compliance by preserving data privacy of the participants. Federated Learning defines a machine learning framework under a virtual model, which is designed to solve the problem of different data owners collaborating without exchanging data [122]. The virtual model is the best model for all parties to aggregate data together, and their respective regions serve local targets according to the model. Federated Learning requires that the modeling result should be infinitely close to the traditional model, i.e., the data of multiple data owners are gathered in one place for modeling results [123]. Under the federated mechanism, each participant has the same identity and status and can establish a shared data strategy. Since the data does not transfer, it does not reveal user privacy or affect data specifications [124].

There are three major components of federated learning: data sources, Federated Learning systems, and users. The relationship between the three is shown in the Figure 2. Under the Federated Learning system, each data source performs data preprocessing, then jointly establishes and learns the model, and feeds back the output results to the client. The central server first saves the initial data and distributes it to the participating users [125]. Then the participants uses their own collected local data to train a local model. The parameters of the local model are then transmitted to the central server, while the participating user's local data remain on their devices [41]. The central server then aggregates

the parameters of the uploaded local models to build a global model. The updated global model would then be distributed back to the local users for additional training with local data. This procedure can be re-run until a desired outcome is seen, often when the global model shows a clear convergence. Each user is treated equally without bias in this process [126].

Federated Learning effectively solves the problem of common use of data by two or more data-using entities (clients) without contributing data, and solves the problem of data islands. In addition, under the premise that the data characteristics of each client are aligned, the global model of Federated Learning can obtain the same modeling effect as the centralized storage of data [127].

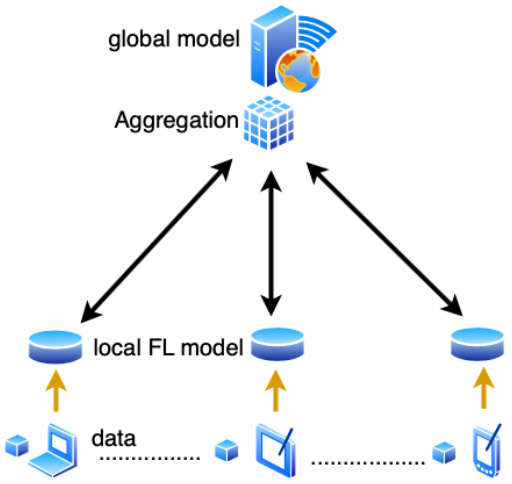

Figure 2. Basic Federated Learning Architecture: Users use local data to train local models, the local models are used to update the global model in the base station. The aggregated global model is passed to the local models for further training. These steps are repeated until the global model converges.

Federated Learning differs from the traditional distributed machine learning due to the participating devices and dataset properties. In traditional distributed machine learning, the edge nodes are all of equal processing power and the data split is equally divided and often found in Independent and Identically distributed (IID) format whereas in Federated Learning, data is often found in non-IID format, where the data varies in quality, diversity and quantity This is due to the heterogeneous nature of participating hardware devices and variability of using user local data for training [128].

According to the distribution of data sources of the participating parties, Federated Learning can often be split into three types, they are specifically horizontal, vertical and transfer Federated Learning.

Horizontal Federated Learning: When the user characteristics of the two data sets overlap more and the user overlaps less, the dataset is divided horizontally along the user dimension the part of the data that contains the same user characteristics but not the same users is taken out [129].

- Step 1: Each participant downloads the latest model from server A;
- Step 2: Each participant trains the model using local data, uploads the encrypted gradient to server A, and server A aggregates the gradient update model parameters of each user;
- Step 3: Server A returns the updated model to each participant;
- Step 4: Each participant updates their own model.

In traditional machine learning, the data and training are all done in a centralized location and the data is often obtained from data centers. Horizontal Federated Learning can be related to distributed machine learning. Where the difference is that the data used is local device data instead of a distributed partition of data owned by the server. Each machine in Federated Learning obtains the initial global model from the server, training is then done on each device's local data (followed by the model parameters of the local model) is shared with the server to perform any required updates in the global

model. The server aggregates the local model parameters sent by each machine to obtain the global model, the updated global model is then sent back to the participating users and these steps are re-run until a global model convergence is present [130].

In this process, each machine has the same and complete model, and the machines do not communicate and do not depend on each other. During the prediction, each machine can also independently predict. This process can be viewed as a sample-based distributed model training [131]. Google initially adopted the horizontal federated method to solve the issue of locally updating models by end users.

The joint multi-party training methodology in horizontal Federated Learning stems from distributed machine learning. Distributed machine learning represents a distributed split of training data, devices and completion of training [132]. The parameter server is adopted from distributed machine learning, it accelerates the training process by storing data on working nodes while allocating computing resources through the centralized scheduling node [133]. Although the working node becomes the participating users, they have ownership over local data and is independent to the server. Compared to the parameter server where the central node has the highest authority, in Federated Learning the working nodes has the freedom to participate, this adds layers of complexity when it comes to scheduling an optimal learning environment [134]. Horizontal Federated Learning is the strongest candidate for wide adoption in smart cities crowdsensing due to the nature of selective user selection for specific sensing data in Mobile Crowdsensing. Oftentimes, the data would share the same user space and differentiate in feature space. Take smart healthcare as an example: in order to share the same user space, the server would recruit users with the same health illnesses; however, the collected local data would have different features [131].

Vertical Federated Learning: this is often used when there is an increased user space overlap in datasets and a decreased feature space overlap. The data is then divided in the vertical direction. Vertical Federated Learning allows the aggregation of these split features without interfering with the user privacy requirements [21]. At present, machine learning models are all built under the framework of a vertical Federated Learning system [135]. Examples include but are not limited to logistic regression and decision tree models that are built under the vertical Federated Learning framework. There are two learning steps, which are shown in the Figure 3.

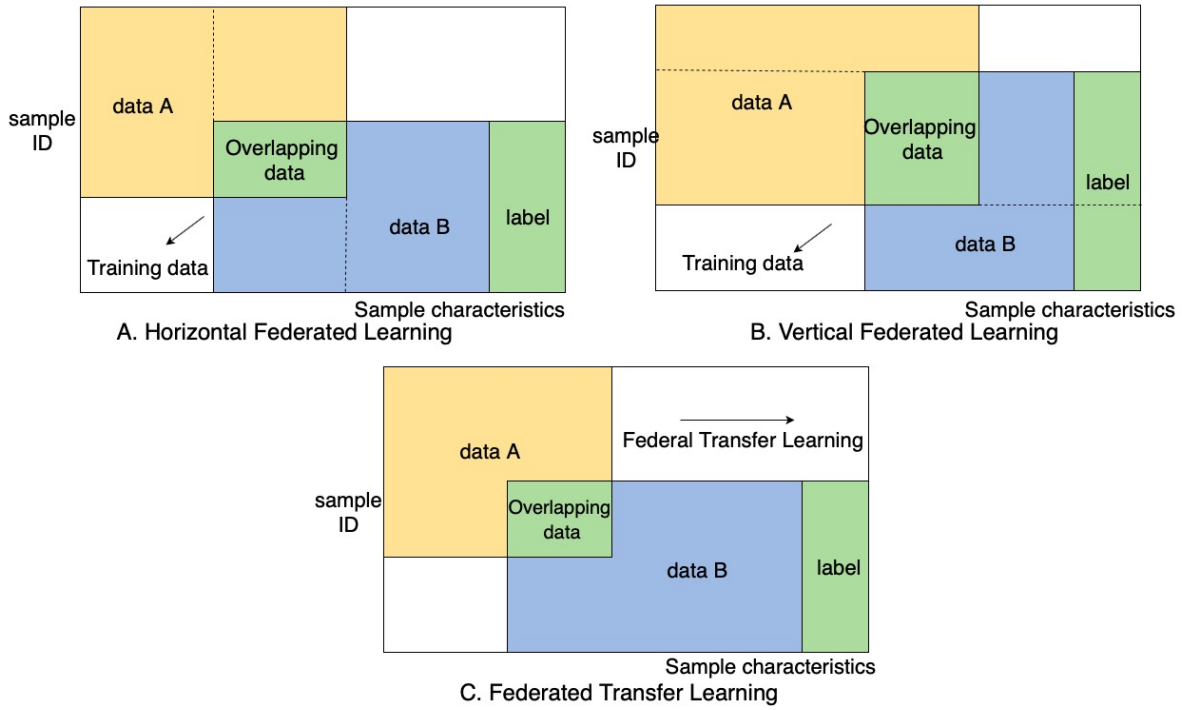

Figure 3. Horizontal, Vertical and Transfer Federated Learning.

Initially, the encrypted samples are aligned at the system level. This is to ensure that user privacy is not leaked within the enterprise sensing level. The samples are then used for training an encrypted model. The collaborator C sends the public key to A and B to encrypt the data to be transmitted; while A and B train their respective models with their local data, an intermediate step of exchanging gradients and losses occurs between A and B; the gradients are then calculated again after the exchange as well as having an additional mask added, both gradients are then sent to C. C then proceeds to decrypt the received gradients and returns it back to A and B. This is followed by the removal of the mask and updating of the model by A and B [117].

During this process, the participants do not communicate with each other therefore they are unaware of the data features of other participants. After the model is trained, only the portion of the model supported by their own model parameters are returned to them. Since each participant can only obtain the model parameters related to himself, both parties need to cooperate in the prediction. The result of the joint modeling is that both parties obtain data protection and jointly improve the model effect without the loss of model [136].

Vertical Federated Learning can be benefited by the industry or governments more than the masses. A major application for vertical federated learning would be in smart retail or smart finance sector. This is because the data collected from these sectors is often used to profile consumers. For example, the bank may have information relating to consumer spending habits, but a retailer may have information on consumer personal preferences in terms item selection. The bank and retailer cover a large user space that intersect, each providing different features [117].

Federated transfer learning is often used for transfer learning models with deep convolutions neural networks. Using pre-trained models on generalized datasets as a basis and training the scarce amount of data to orient the base model for a specific application. The core of transfer learning is to find the similarity between the source domain and the target domain [137]. The goal of transfer learning is to build effective application-specific models for cases with data is scarce. This is accomplished through leveraging models that are already fully trained and effective for a source domain that is related to the target domain. Then using the available data, to orient the model for use in the target domain. Applications of federated transfer learning would be teaching autonomous vehicles to recognize new signs and road conditions through deep neural networks. Figure 3 shows a representation of horizontal, vertical and federated transfer learning.

A standardized Federated Learning protocol was introduced by Bonawitz et al. [138] to promote the scalability of Federated Learning algorithms. This protocol is repeated during each round of training and consists of 3 steps each time.

- Selection: At the beginning of each training round, a predefined subset of participating users is selected. This selection method can be adjusted or calibrated based on the server requirements or with a custom selection methodology.
- Configuration: The server uses the selected aggregation method and sends the training parameters and model configuration to the selected participants. The participants can proceed to model training.
- Reporting: The participants have trained their models and update the server with their parameters and the server aggregates the updates.

Nishio et al. [139] proposed FedCS, a Federated Learning protocol to improve client selection under heterogeneous device scenarios. The steps of FedCS consists of initialization, resource request, client selection, global model distribution, scheduled update and upload of local model parameters, local model aggregation steps followed by iteration of steps from resource request to local model aggregation. The FedCS protocol enables accelerated federated training process by allowing the server to receive more updates and aggregate more models within the same time frame due to selecting clients based on their resource constraints.

FedGRU was proposed in [140] or small-scale Federated Learning applications, specifically in joint traffic control where private information is often not shared between organizations. The initial global model is pre-trained using public datasets that applies to the selected application domain. The global model is distributed to each participant and trained with local data, and each participant uploads their trained model parameters through encrypted parameters. Finally, the cloud then aggregates all participant models for a new global model followed by distributing it back to each participant.

3.1. Aggregation Methods

The Federated Average (FedAvg) [141] algorithm (illustrated in Figure 4) is an effective yet simple algorithm that is most commonly used for federated aggregation. The FedAvg aggregation consists of equal distribution of model parameters for every local model.

For FedAvg, the gradients of all participants S_t is initialized to w_o. Each round each, local model is trained on its local data and updates the model, given by $w^t \leftarrow w^t - \eta \bigtriangledown \ell(w; b)$ The gradients of the local models are given by w_t. The gradients are aggregated by the server each round, the updates can be categorized as $w_{t+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^k$ The parameters are averaged between all uploaded models.

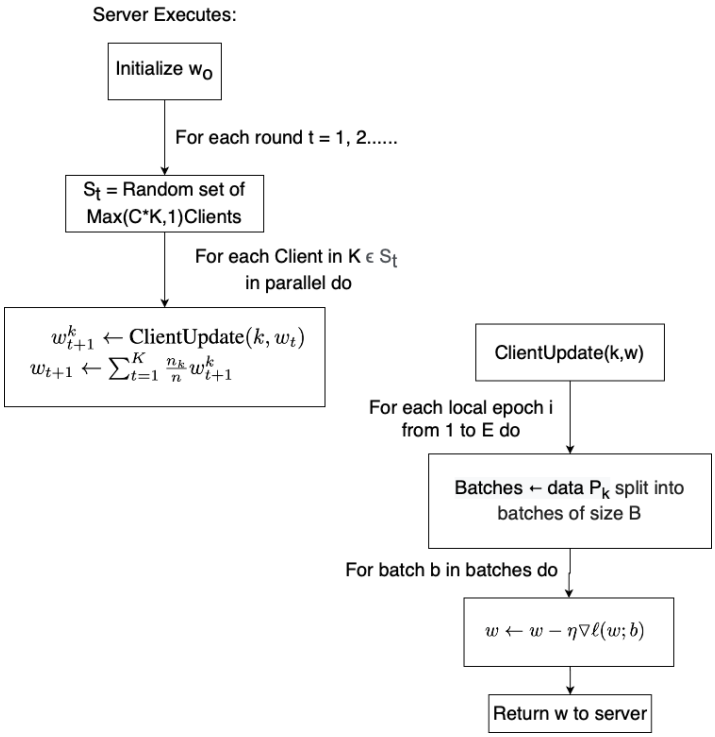

Figure 4. FedAvg algorithm proposed by McMahan et al. [142] that is widely used as a standard algorithm.

The study in [143] propose FedProx to improve upon FedAvg. FedProx tackles the problem of heterogeneity within the Federated Learning environment. This includes the hardware and software variability in participating mobile devices and the statistical heterogeneity by the non-identically distributed data across devices. This is done by introducing a tunable proximal parameter to ensure a better convergence. It addresses statistical heterogeneity by restricting the impact of each local update to the initial global model and addresses system heterogeneity by safely incorporating various degrees of local work.

The study in [144] propose Loss-based Adaptive Boosting (LoAdaBoost) FedAvg to further improve upon FedAvg. This is done so by comparing the loss of the local model in the current epoch to the median loss of the previous epoch. The local model is retrained if it is higher than the previous

median loss. A faster convergence is observed with this method, and thus the communication costs can be reduced.

3.2. Reputation Models to Ensure Data Trustworthiness

Reputation models have been proposed by [145,146] to ensure reliability and trustworthiness of mobile devices.

The study in [145,147] uses blockchain and multi-weight subjective logic to formulate reputation scores; the reputation is calculated based on previous interactions and opinions of other task publishers. This reputation is then stored within an open-access consortium blockchain. A reputation threshold is set during the user selection, therefore lower reputation users will not be selected. After a model is trained, the performance of the local device is evaluated, using the Reject on Negative Impact (RONI) [148] method for Independent and Identically Distribute (IID) data. As well as using the FoolsGold [149] scheme for non-IID data. RONI detects poisoning attacks by comparing the performance of the local update to a preset update threshold. If the model does not improve over the preset threshold then it will be rejected for global model aggregation. The FoolsGold scheme looks at the gradient diversity of the local updates, if a user repeatedly uploads similar gradients every iteration then it deemed unreliable.

The study in [146] formulates the reputation score of a user by comparing the testing accuracy in three distinct ways. The test accuracy of the local model is compared to the average test accuracy of that epoch, the previous global model test accuracy and the temporary global model test accuracy. A temporary global model is aggregated each epoch to evaluate the capabilities of the combined training of the current epoch, the previous global model is used as a comparison to see how much the local models have improved upon the last epoch. The average test accuracy is used to measure how well the local model is performing compared to its peers. A reputation threshold is set for selecting suitable users to participate in the Federated Learning training. If a user falls below the threshold a set amount of times they will be eliminated from the Federated Learning event.

3.3. Privacy Preservation

Privacy Preservation is a key issue in Mobile Crowdsensing, the Federated Learning methodology helps prevent raw data from being sent to the centralized server; however, there are other privacy concerns within the Federated Learning framework and improvements that can be built and incorporated to the Federated framework [150].

Federated Learning methods can leverage Differential Privacy to further prevent information leakage. Oftentimes differential privacy schemes face a challenge to address a trade-off between two objectives: convergence rate and privacy. With this in mind, the authors in [41] propose noising before model aggregation Federated Learning (NbAFL) which satisfies differential privacy by varying protection levels with variances of artificial noise. This method shows that with as the protection level increases the convergence performance decreases, and where an increasing number of clients can improve convergence rate when given a constant protection level.

Liu et al. [150] focused on the improve privacy preservation when sharing model updates without increasing communication cost. They achieved this by proposing sketching algorithms to obfuscate the original data by using independent hash functions. The identities of the user can be concealed during each round of updates due to each user having their own hash indices and seeds.

Hao et al. [151] propose a Privacy Enhanced Federated Learning (PEFL) scheme that uses differential privacy by adding noise according to Gaussian distribution to local models. The perturbed gradients vector of the users is then encrypted into the Brakerski Gentry Vaikuntanathan (BGV) encrypted internal ciphertext. It is then integrated into an augmented learning with error (A-LWE) external ciphertext for secure aggregation. The internal ciphertexts are first all aggregated, then the server decrypts the external ciphertexts. The internal ciphertexts are summed, the aggregated value is easily decrypted by the server while withholding the privacy of the user.

3.4. BlockChain

Blockchain is often used to preserve privacy in distributed computing environments. Blockchain has been widely used in Federated Learning schemes.

Awan et al. [152] aim for user privacy preservation, and to do so they propose a method that uses the immutability and decentralized trust properties of blockchain for a secure aggregation process. Their model relies on homomorphic encryption the combined with re-encryption, blockchain and verification. The server generates a pair of private and public task keys while the aggregator generates a pair of private and public batch keys, the public keys are distributed to participating users. The aggregator fuses the updates received from the users, and the aggregated updates are re-encrypted, in which the server would only be able to get the aggregated results. Blockchain also enables easy tracking of client contributions, the contribution can be evaluated by evaluating the global model before and after aggregation.

Lu et al. [153] propose Blockchain, differential privacy with Federated Learning to solve the issue of data islands for industrial IoT applications. For differential privacy, they added noise at the initial stage onto the original data. This may affect the accuracy of the trained models compared to adding noise to the gradients.

Lyu et al. [154] consider fairness in their blockchain-enabled Federated Learning scheme. A local credibility mechanism is used to promote evaluation between users to ensure fairness. Another mechanism to guarantee fairness is that the global server distributes different versions of the global model to the participants based on their contributions. For privacy preservation the authors propose a layered encryption scheme. Blockchain 2.0 is used to store the credibility values of the users, these values are relative to each user's contributions.

Zhao et al. [155] incorporates blockchain-based Inter-Planetary File System (IPFS) with differential privacy to improve privacy of Federated Learning. Noise is added to the extracted features to ensure differential privacy. Local model updates are sent to the IPFS. IPFS is a file system that allows edge devices to communicate with the same file. Instead of storing actual files on the IPFS, hashes of data location on the blockchain is stored. The immutable nature of blockchains allow for transparency in terms of tracking the model updates from malicious users.

An overview of Research covered within this section can be seen in Table 1.

Table 1. Overview of Federated Learning Research covered with key ideas, methodologies, open issues and opportunities for future research.

Area	Ref.	Motivation and Key Idea	Proposed Approach	Open Issues and Further Opportunities
Protocol	[138]	Scalable production system for Federated Learning	Standard protocol as a basis for Federated Learning	Need for optimization for application-specific scenarios
	[139]	Promote client selection under heterogeneous resource scenarios	FedCS protocol to select users based on their resource availability	Relies on the truthfulness of user resource availability submissions.
	[140]	Federated Learning for traffic prediction models	Suitable protocol for small-scale Federated Learning enabled traffic control	Extension to larger scale of recruited clients.
Aggregation	[141]	A standard aggregation method	FedAvg algorithm to aggregate the average model parameters of updates	An alternative to equally weighing all local model updates during aggregation.
	[143]	Optimize Federated Learning in heterogeneous networks	Proximal parameter to limit the impact of variable updates allowing partial work to be done	Solutions for the cases where not all updates are of positive contribution
	[144]	Optimize Federated Learning through data distribution	Loss-based Adaptive Boosting to compare local model losses prior to aggregation	Extensions to consider heterogeneous contribution scenarios during aggregation
Reputation Models	[145]	Incentive to promote reliable Federated Learning	Multi-weight subjective logic to formulate reputation scores	Advanced reputation scores to directly reflect performance of users
	[146]	Enhanced client selection to improve model performance	Local model performance metrics to formulate reputation scores	Minimum computational overhead for assessment of reputation scores for every user
	[147]	Reputation-awareness	Interaction records to generate reputation opinions	Reputation scores to reflect performance of users directly

Table 1. *Cont.*

Area	Ref.	Motivation and Key Idea	Proposed Approach	Open Issues and Further Opportunities
Differential Privacy	[150]	Enhanced privacy preservation through sketching	Obfuscation of the original data to achieve differential privacy	Performance versus privacy gain
	[41]	Differential privacy in Federated Learning	Noise before model aggregation	Considering varied size and distribution of user data
	[151]	Enhanced privacy and efficiency of Federated Learning in industrial AI applications	Add noise according to Gaussian distribution to local models	Extensive analyses on high-dimensional data
BlockChain	[152]	Accountable Federated Learning	Combine aggregator and blockchain to preserve privacy of users	Fairness assurance in participant rewarding
	[153]	Enhanced privacy for Federated Learning	Noise at the initial stage onto the original data, and use BlockChain to facilitate the Federated Learning process	Tackle potential performance issues due to noising too early
	[154]	Improved fairness and privacy in Federated Learning	Scale rewards with respect to participant contribution	Extension to non-IID scenarios
	[155]	Privacy Preserving Federated Learning for industrial IoT applications	Use blockchain with Inter-Planetary File System (IPFS) and noise to local model features	Extension to non-IID data or heterogeneous device scenarios

4. Opportunities for Federated Learning in Smart Cities Sensing

Federated Learning can benefit smart cities sensing in multiple aspects [32]. This is most evident when incorporating Federated Learning methodologies for Mobile Crowdsensing tasks, by bridging the gap between data sensing machine learning model training while preserving user privacy. It is possible to use Federated Learning with dedicated smart city sensors; however, oftentimes they do not have the processing power to compute advanced deep learning and machine learning models. The overhead cost of redeploying existing dedicated sensors and manufacturing cost of producing dedicated sensors with higher processing capabilities would be expensive and inefficient. However, in Mobile Crowdsensing the use of personal smart devices that have enough processing capabilities are a prime candidate to integrate with Federated Learning. Along with the growth in smart technologies, more advanced Federated Learning models can be used. This section will go in detail in terms of how Federated Learning can address certain challenges within Mobile Crowdsensing, this includes data privacy, communication costs and training efficiency.

The benefit of the Federated Learning can be seen in two major aspects. First, Federated Learning helps preserve the security of the user by never uploading the raw collected data. Secondly, it is possible to assess the quality of the user's collected data by testing the local models prior to aggregation.

4.1. User Incentives

The additional layers of privacy preservation that is present in Federated Learning schemes will better facilitate user participation.

By having a direct way to measure each individual user's utility and contribution to the federated sensing campaign, better compensation can be made to the participating users. This will deter users that do not have the capability to provide quality local data.

In Federated Learning, only the trained model parameters need to be uploaded to a server, this represents less bandwidth usage for the user compared to traditional Mobile Crowdsensing. This helps relieve users of high bandwidth costs, which in return incentivizes their participation.

The server in Federated Learning gains a quantifiable revenue from the local data and training progress that the recruited users contribute. Rewarding the participants with viable payout for their contributions is the basis of incentive mechanisms in Federated Learning schemes. The user incentive scheme leverages game theory [117] and contract theory [145]. Games such as the coalition game and labor union game can be used where marginal contribution of the participants are used to gauge pay-offs. Rewards such as reputation, lotteries and auctions can be used as incentive mechanisms. The study in [156] proposes a pay-off sharing incentive scheme that focuses on fairness between participants. Their achieved fairness by modeling the contribution, regret distribution and expectation

fairness criteria. Their goal is to concurrently maximize the total utility of the platform by ensuring maximum fairness among participant contributions. The study in [145] proposes a method that uses the junctions of contract theory with reputation scores where higher reputation users would be motivated to users with high-quality data to participate. The authors in [157] propose an incentive method that scores models based on their performance results.

Federated Learning incentive models inherit the advantages of Mobile Crowdsensing incentive methods through the capability of more accurately gauging the utility of a participant. This is due to evaluation methods that can directly measure the performance of their contributed model, evaluating a machine learning model is easier and more concrete than evaluating the contribution of raw sensing data [158].

Federated Learning also allows a user to obtain more payout through the same collected sensing data. Thus, since there will be more computational overhead, a higher payout should be given. Therefore, at the cost of more inconvenience, the users would be able to yield a higher payout by providing the same amount of data. This combined with the security benefits that Federated Learning presents would help incentivize users to participate in Federated Learning-based sensing applications [156].

4.2. Data Quality

Mobile Crowdsensing allows users to participate in a sensing event for a particular goal. However, oftentimes, a challenge is to determine the quality of data that each user provides [95]. Integration of Federated Learning-based approaches enables comparison of the loss value or test accuracy of the trained local model to check the viability of the provided user data. The Federated Learning methodology will be able to provide a direct analysis of each user's data quality. The organizers of the sensing campaign can a predetermined desired output as the model test set and at each epoch the local model performance is tested to see if an improvement is present. If an improvement is seen then the local model is accepted for global aggregation.

This in turn reduces the risk of compensating users that intentionally provide poor data or has device-side issues. This method also directly addresses the device heterogeneity problem within Mobile Crowdsensing, where data is gathered from a multitude of different sensors and devices.

4.3. Data Privacy Protection

The ever-increasing stringent Data privacy laws are a key challenge in Mobile Crowdsensing, it is preventing the user recruitment and inhibiting the collection of certain types of sensed data. By never uploading the raw collected data of the users and only uploading the trained local model parameters, the user data is protected can be further protected.

Federated Learning methodologies can incorporate Blockchain and differential privacy to better improve the user privacy [155]. By incorporating noise, the output of the local models will not change the model inherently but will improve the privacy guarantee. The Global model convergence is reduced as privacy is increased with differential privacy. Blockchain is a popular privacy preserving methodology for training neural network models in a distributed environment.

4.4. Server Side Overhead

In traditional Mobile Crowdsensing schemes the server must overlook the transmission of data, storage of data and data preprocessing. Mobile Crowdsensing that is used for model training would also need to train the model in a centralized location. These processes incur large overhead costs and maintenance, reducing those requirements would lower the threshold for smart city sensing campaigns.

Mobile Crowdsensing incurs large communication costs with the transfer of raw data into the server. This places a burden on the server itself to process this data and takes a large amount of bandwidth from the users as well. The user resources in terms of bandwidth can be reduced whereas the trade-off is the energy consumption of the devices are increased. In a Federated Learning scheme,

the parameter set of the model is transferred to the server as opposed to uploading a bulk of raw data. Lin et al. [159] propose Deep Gradient Compression and it yielded a communication bandwidth reduction in the order of two magnitudes for complex models.

Training complex models is time consuming and requires vast amount of computing power, by leveraging a decentralized approach it will accelerate the training process while providing a more generalized and rich data pool.

4.5. Federated Learning Applications

A few examples of Federated Learning applications that contributes to smart city sensing are covered in this section.

4.5.1. Federated Visual Security Sensing

Smart security is an emerging field that is part of the smart cities phenomenon. Traditionally, security relies on the combination cameras, monitoring rooms and personnel to manually detect possible threats. Definitions of abnormalities depend on predefined set of rules. This type of threat detection is labor-intensive and inefficient. Although large amount of data is collected through access cards, cameras, sensors, etc., they are often not used together. The value of the individual data islands is not fully used [160]. Therefore, smart security solutions are highly desired [161].

AI-based model can be used for early warning, real-time high-precision location determination, movement recognition and analysis behavior, to predict travel trajectory and user abnormal behavior, thereby improving community safety and community management efficiency [162]. Federated Learning can be established to train multi-community data for security models while preserving the privacy between communities [163].

Based on machine learning, smart security can perform post event analysis and self-learning, constantly accumulating experience, and continuously improve pre-warning capabilities. Federated Learning offers a machine learning training scheme that allows the use of the large amounts of collected data in daily applications [163].

4.5.2. Federated Autonomous Vehicles

Navigating the dynamically changing, complex and diverse roads is a difficult task for autonomous vehicles [164]. Accidents are highly probable due to the sudden events caused by pedestrians or other vehicles. Industries require large number of drivers for long distance delivery services as a part of the supply chain every year [165]. Autonomous vehicles will improve efficiency by enabling continuous operation without the need for human intervention.

The development of Internet of Vehicles (IoV) and Road Networking technologies will propel autonomous vehicles to become a technological direction with extremely high social value and economic value [166]. Horizontal Federated Learning can be introduced to contribute to more robust machine learning models by fusing sensor information such as cameras, ultrasonic sensors, millimeter wave radar, LiDAR of different vehicles [167]. Vehicular sensing networks are an integral role in smart cities as they provide a vast amount of sensory information and can directly impact smart traffic control [168].

Autonomous vehicles should interact with the IoV, vehicle-road collaboration, and even the entire transportation system to create a better driving environment [169]. Interactive learning should take place between the vehicle and the system environment so that it can assist with other city sensing applications, such as city traffic lights, cameras and road side units through vertical Federated Learning to better integrate information from different sources under privacy protection.

Communication between vehicles is vitally important. Samarakoon et al. [170] propose a Federated Learning-based approach to achieve ultra-reliable low latency communications in vehicles. Lyapunov optimization is used to calculate the joint power and resource allocations to enable low latency communication for vehicular users.

Sensing, decision-making and control are the three core modules of autonomous vehicles. Among them, the sensing of sensor information input such as LiDAR, camera (monocular, binocular, surround-view camera) provides input for the planning stage [171]. At the same time, because the vehicle will generate massive sensory data during the driving process, the original data may involve privacy issues, Federated Learning can be leveraged for real-time adjustments to the AI-based models for dynamic adaptability without compromising the privacy of the data owner.

4.5.3. Federated Aided Diagnosis

Artificial intelligence applications in clinical research are enabled by the digital transformation of medical treatment and clinical information [172]. Medical information is intertwined tightly with patient privacy, and protecting this highly sensitive information is the joint responsibility of all parties including hospitals, artificial intelligence companies and relevant regulatory agencies.

Smart healthcare that leverages Federated Learning can equalize the performance discrepancies between hospitals and provide high-quality test results. By assisting doctors in diagnosis, the burden on the medical system can be reduced [173]. Through standardized data, a horizontal Federated Learning model can be used to ensure that patient data is only kept in the hospital of origin [117]. The Federated Learning model allows for continuous improvements as more medical data is added.

The study in [174] used electronic health records to train an AI model for predicting cardiac events. Smart healthcare based on Federated Learning will empower clinical diagnosis and other subdivisions on the basis of protecting patient privacy, and will promote high-quality medical resources at extremely low cost [175].

5. Open Issues, Related Challenges and Opportunities

Figure 5 illustrates our proposed taxonomy of Federated Learning. The major steps in a Federated Learning scheme is user recruitment, local training and uploading of model parameters, aggregation of local models and the privacy preservation mechanics that is used throughout to ensure that the privacy of data is preserved. The blocks highlight in red are the fields that still need further investigation. Coverage area is very crucial in sensing tasks although currently researchers have not focused on the challenges with regards to sensing coverage in Federated Learning schemes. Aggregation methods that can further optimize federated learning performance is still an area that still requires further research, currently most Federated Learning schemes use the FedAvg algorithm for model aggregation; however, application-specific aggregation methodologies can be developed. The energy consumption and heterogenous nature of participating device computational power and their effects on Federated Learning schemes is also an area that offers opportunities for future research.

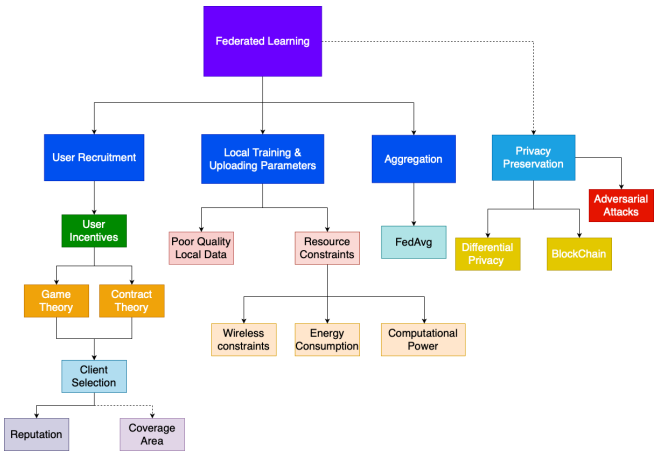

Figure 5. Proposed Taxonomy for Federated Learning.

This section covers the challenges and open issues regarding incorporating Federated Learning into smart city sensing.

5.1. Energy Consumption

In Mobile Crowdsensing, energy consumption is a major issue, and it is a metric that is used for calculating the user compensation. By using Federated Learning, the utility of the user can be better gauged; however, Federated Learning consumes much more of the users battery. Depending on the model that is being trained and the amount of local data battery drain can be significant enough to deter users from participating. A proper method to optimize battery usage during Federated Learning is desired, as well as a compensation scheme that is scalable depending on the Federated Learning sensing campaign.

Previous studies have tackled communication challenges regarding Federated Learning [176,177]. However, they often do not take into account the energy consumption of the participating users. Within a fixed training time, unavailability due to outage decreases as energy consumption decreases. Similarly, in the case of a fixed energy consumption guideline, the amount of communication rounds is proportional to outage probability. Therefore, the problem can be oriented by given an energy consumption threshold, optimize the learning performance, or vice versa [178]. The study in [176] optimized energy consumption based on the communication time given to each user as well as the selection of computation parameters. This methodology assumes a strongly convex loss function is present, which is not always the case. The study in [179] optimizes energy consumption as a whole through an adaptive method that gives more bandwidth to users with less computation power and gives priority to participants with strong computation power.

There are many incentive methodologies that have been developed for Mobile Crowdsensing that considers energy consumption. We envision the adaptation of Mobile Crowdsensing incentive methodologies to include the increased energy consumption to appropriately compensate and incentivize participants.

5.2. Adversarial Attacks

Federated Learning methodology is susceptible to adversarial attacks, defense mechanisms for a more secure process is still required.

The study in [180] showed how Generative Adversarial networks (GANs) with a multitask discriminator can extract user specific data quietly on the server side. However, the study in [181] showed that adversarial participants can launch white-box membership inference attacks to trace training data records.

Poisoning attacks and inference attacks are most prevalent [42]. Poisoning attacks may target data or local model updates to prevent model training or to initiate a bias towards certain favored features that are beneficial to the adversary. Inference attacks target the privacy of the participants. The exchange of gradients for local updates often can cause privacy leakage [182]. The attacked can conduct property inference by observing the difference between local model updates of a specific user to gain information about that user.

Attacks can be carried out insiders such as server or users as well as outside adversaries. Insider attacks are more impactful than outsider attacks, they are often categorized into a single attack [183,184], byzantine attacks [185] and sybil attacks [149,184].

Participant-level DP can help protect users; however, the exchange in convergence rate and accuracy may not be an attractive solution [142]. Participant-level DP is often used for large participants pools such as thousands of users. Further work is needed to verify the ability of participant-level DP to protect smaller participant pools as well as ensuring that the model converges properly on smaller participant pools [42].

5.3. Data Distribution

The data distribution within Federated Learning environment is often categorized into two categories, IID and non-IID data. Non-IID data can be caused by the unbalanced quantity, features and labels.

Non-IID data is much more prevalent situation in a real-world scenario. Zhao et al. [186] showed that non-IID scenarios can lead to significant degradation in the performance of Federated Learning models, which is caused by the weight divergence due to distribution of devices, classes and population. They also suggested a global shared dataset partition to help improve training with non-IID data. They showed that by sharing 5% of data a 30% increase in accuracy can be observed. However, this increases communication costs with models and assumes that such dataset partition is always accessible. This method also increases the susceptibility to data poisoning and adversarial attacks.

Koppararpu et al. [187] propose FedFMC which is a based on a lifelong learning technique [118] for training non-IID data. FedFMC dynamically forks a single global model into different groups depending on its performance on each device dataset. Devices will be grouped to achieve different global models specific to their dataset. This allows the grouped devices to focus on different aspects of the model depending on their dataset properties. At the end, all the forked models are merged. However, this method makes the model more susceptible to an adversarial attack by grouping devices with similar qualities.

6. Summary and Conclusions

Federated Learning has appeared as a distributed machine learning concept that uses local data of distributed devices to collaborate with the objective of contributing to the training a global model. It has shown promising performance in preserving the privacy of the participants by training local models and uploading the model parameters to the server instead of uploading the raw data. Privacy preservation is an ongoing challenge in smart cities sensing due to the increasing privacy regulation. A subset of the data gathering from smart cities sensing is often used for training purposes in machine learning models. With these in mind, leveraging Federated Learning for smart cities sensing is envisioned. The participants will be able to provide their data with additional layers of privacy preservation. The quality of data acquired from the participants can be directly gauged by measuring the performance improvements gained due to the contributions of their local data. Communication cost can be reduced with the transmission of model parameters instead of raw data. Moreover, it is possible to empower additional privacy preserving methodologies in Federated Learning-assisted smart cities sensing such as various applications of differential privacy as well as blockchain.

Smart city sensing is an integral part to the smart city ecosystem. This review article has initially presented an overview of smart city sensing and its applications. This has been followed by a discussion on the challenges of smart city sensing in both dedicated and non-dedicated scenarios. These include major areas such as data trustworthiness, user incentives, data quality management, node deployment energy consumption and user privacy protection. By presenting Federated Learning as a promising methodology for preserving privacy within smart cities sensing, state-of-the-art Federated Learning solutions have been presented in Section 3. To present the founding blocks, vertical, horizontal and federated transfer learning as well as other improvements over standard Federated Learning have also been introduced. More specifically in the areas of model aggregation methods, reputation-aware models and privacy preservation methods and Blockchain integration have been reviewed. Lastly, the applications and areas where Federated Learning can help benefit and tackle challenges within smart city sensing have been shown.

Federated Learning is still in its infancy; hence, there are still various challenges faced in adversarial settings. Further research into defense mechanisms is necessary to ensure security of Federated Learning-assisted smart cities sensing. The nature of a Federated Learning environment presents the issue of the statistical heterogeneity of the distributed data, as well as the hardware heterogeneity of participating devices. Although these issues are mitigated through various proposed

methods, they have not been eliminated completely. Last but not least, thorough analysis on node deployment and coverage area for federated smart sensing is an issue that needs to be resolved before Federated Learning can be widely adopted for smart cities sensing.

Author Contributions: J.C.J. worked on studying and drafting the state of the art and survey of the Federated Learning approaches in Smart Cities. Technical verification has been done by B.K., S.O. and T.S. All authors wrote the paper collaboratively. J.C.J. created the illustrative images. All authors have read and agreed to the published version of the manuscript.

Funding: This material is based upon works supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) under Grant RGPIN/2017-04032.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hancke, G.P.; Hancke, G.P., Jr. The role of advanced sensing in smart cities. *Sensors* **2013**, *13*, 393–425. [CrossRef]
2. Okai, E.; Feng, X.; Sant, P. Smart Cities Survey. In Proceedings of the 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, UK, 28–30 June 2018; pp. 1726–1730.
3. Giffinger, R.; Haindlmaier, G.; Kramar, H. The role of rankings in growing city competition. *Urban Res. Pract.* **2010**, *3*, 299–312. [CrossRef]
4. Bibri, S.E.; Krogstie, J. On the social shaping dimensions of smart sustainable cities: A study in science, technology, and society. *Sustain. Cities Soc.* **2017**, *29*, 219–246. [CrossRef]
5. Yigitcanlar, T.; Kamruzzaman, M.; Foth, M.; Sabatini-Marques, J.; da Costa, E.; Ioppolo, G. Can cities become smart without being sustainable? A systematic review of the literature. *Sustain. Cities Soc.* **2019**, *45*, 348–365. [CrossRef]
6. Silva, B.N.; Khan, M.; Han, K. Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustain. Cities Soc.* **2018**, *38*, 697–713. [CrossRef]
7. Zhao, K.; Ge, L. A survey on the internet of things security. In Proceedings of the 2013 9th International Conference on Computational Intelligence and Security, Leshan, China, 14–15 December 2013; pp. 663–667.
8. Vermesan, O.; Friess, P.; Guillemin, P.; Gusmeroli, S.; Sundmaeker, H.; Bassi, A.; Jubert, I.S.; Mazura, M.; Harrison, M.; Eisenhauer, M.; et al. Internet of things strategic research roadmap. *Internet Things Glob. Technol. Soc. Trends* **2011**, *1*, 9–52.
9. Ngu, A.H.; Gutierrez, M.; Metsis, V.; Nepal, S.; Sheng, Q.Z. IoT middleware: A survey on issues and enabling technologies. *IEEE Internet Things J.* **2016**, *4*, 1–20. [CrossRef]
10. Ray, P.P. A survey of IoT cloud platforms. *Future Comput. Inform. J.* **2016**, *1*, 35–46. [CrossRef]
11. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.; Du, X.; Ali, I.; Guizani, M. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Commun. Surv. Tutor.* **2020**, 22, 1646–1685. [CrossRef]
12. Sundmaeker, H.; Guillemin, P.; Friess, P.; Woelfflé, S. Vision and challenges for realising the Internet of Things. *Clust. Eur. Res. Proj. Internet Things Eur. Commision* **2010**, *3*, 34–36.
13. Caragliu, A.; Del Bo, C.; Nijkamp, P. Smart cities in Europe. *J. Urban Technol.* **2011**, *18*, 65–82. [CrossRef]
14. Pouryazdan, M.; Kantarci, B.; Soyata, T.; Song, H. Anchor-Assisted and Vote-Based Trustworthiness Assurance in Smart City Crowdsensing. *IEEE Access* **2016**, *4*, 529–541. [CrossRef]
15. Habibzadeh, H.; Soyata, T.; Kantarci, B.; Boukerche, A.; Kaptan, C. Sensing, communication and security planes: A new challenge for a smart city system design. *Comput. Netw.* **2018**, *144*, 163–200. [CrossRef]
16. Habibzadeh, H.; Nussbaum, B.H.; Anjomshoa, F.; Kantarci, B.; Soyata, T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustain. Cities Soc.* **2019**, *50*, 101660. [CrossRef]
17. Habibzadeh, H.; Dinesh, K.; Shishvan, O.R.; Boggio-Dandry, A.; Sharma, G.; Soyata, T. A Survey of Healthcare Internet of Things (HIoT): A Clinical Perspective. *IEEE Internet Things J.* **2019**, *7*, 53–71. [CrossRef]
18. Habibzadeh, H.; Kaptan, C.; Soyata, T.; Kantarci, B.; Boukerche, A. Smart City System Design: A Comprehensive Study of the Application and Data Planes. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–38. [CrossRef]

19. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Sensing as a service model for smart cities supported by internet of things. *Trans. Emerg. Telecommun. Technol.* **2014**, *25*, 81–93. [CrossRef]
20. Sheng, X.; Tang, J.; Xiao, X.; Xue, G. Sensing as a service: Challenges, solutions and future directions. *IEEE Sens. J.* **2013**, *13*, 3733–3741. [CrossRef]
21. Liu, Y.; Kang, Y.; Zhang, X.; Li, L.; Cheng, Y.; Chen, T.; Hong, M.; Yang, Q. A communication efficient vertical federated learning framework. *arXiv* **2019**, arXiv:1912.11187.
22. Capponi, A.; Fiandrino, C.; Kantarci, B.; Foschini, L.; Kliazovich, D.; Bouvry, P. A survey on mobile crowdsensing systems: Challenges, solutions, and opportunities. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2419–2465. [CrossRef]
23. Habibzadeh, H.; Boggio-Dandry, A.; Qin, Z.; Soyata, T.; Kantarci, B.; Mouftah, H.T. Soft sensing in smart cities: Handling 3Vs using recommender systems, machine intelligence, and data analytics. *IEEE Commun. Mag.* **2018**, *56*, 78–86. [CrossRef]
24. Zaslavsky, A.; Perera, C.; Georgakopoulos, D. Sensing as a service and big data. *arXiv* **2013**, arXiv:1301.0159.
25. Lau, B.P.L.; angijerathne, N.; Ng, B.K.K.; Yuen, C. Sensor fusion for public space utilization monitoring in a smart city. *IEEE Internet Things J.* **2017**, *5*, 473–481. [CrossRef]
26. Mohammadi, M.; Al-Fuqaha, A. Enabling cognitive smart cities using big data and machine learning: Approaches and challenges. *IEEE Commun. Mag.* **2018**, *56*, 94–101. [CrossRef]
27. Habibzadeh, H.; Qin, Z.; Soyata, T.; Kantarci, B. Large-scale distributed dedicated-and non-dedicated smart city sensing systems. *IEEE Sens. J.* **2017**, *17*, 7649–7658. [CrossRef]
28. Brisimi, T.S.; Cassandras, C.G.; Osgood, C.; Paschalidis, I.C.; Zhang, Y. Sensing and classifying roadway obstacles in smart cities: The street bump system. *IEEE Access* **2016**, *4*, 1301–1312. [CrossRef]
29. Dash, S.K.; Mohapatra, S.; Pattnaik, P.K. A survey on applications of wireless sensor network using cloud computing. *Int. J. Comput. Sci. Emerg. Technol.* **2010**, *1*, 50–55.
30. Misra, S.; Chatterjee, S.; Obaidat, M.S. On theoretical modeling of sensor cloud: A paradigm shift from wireless sensor network. *IEEE Syst. J.* **2014**, *11*, 1084–1093. [CrossRef]
31. Shu, L.; Chen, Y.; Huo, Z.; Bergmann, N.; Wang, L. When mobile crowd sensing meets traditional industry. *IEEE Access* **2017**, *5*, 15300–15307. [CrossRef]
32. Zhang, X.; Yang, Z.; Sun, W.; Liu, Y.; Tang, S.; Xing, K.; Mao, X. Incentives for mobile crowd sensing: A survey. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 54–67. [CrossRef]
33. Jin, H.; Su, L.; Chen, D.; Nahrstedt, K.; Xu, J. Quality of information aware incentive mechanisms for mobile crowd sensing systems. In Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Hangzhou, China, 22–25 June 2015; pp. 167–176.
34. Jaimes, L.G.; Vergara-Laurens, I.J.; Raij, A. A survey of incentive techniques for mobile crowd sensing. *IEEE Internet Things J.* **2015**, *2*, 370–380. [CrossRef]
35. Lin, J.; Yang, D.; Li, M.; Xu, J.; Xue, G. Frameworks for privacy-preserving mobile crowdsensing incentive mechanisms. *IEEE Trans. Mob. Comput.* **2017**, *17*, 1851–1864. [CrossRef]
36. Wu, D.; Si, S.; Wu, S.; Wang, R. Dynamic trust relationships aware data privacy protection in mobile crowd-sensing. *IEEE Internet Things J.* **2017**, *5*, 2958–2970. [CrossRef]
37. Jin, H.; Su, L.; Xiao, H.; Nahrstedt, K. Inception: Incentivizing privacy-preserving data aggregation for mobile crowd sensing systems. In Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Paderborn, Germany, 5–8 July 2016; pp. 341–350.
38. Ni, J.; Zhang, K.; Xia, Q.; Lin, X.; Shen, X.S. Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing. *IEEE Trans. Mob. Comput.* **2019**, *19*, 1317–1331. [CrossRef]
39. Zhou, J.; Cao, Z.; Dong, X.; Vasilakos, A.V. Security and privacy for cloud-based IoT: Challenges. *IEEE Commun. Mag.* **2017**, *55*, 26–33. [CrossRef]
40. Du, R.; Santi, P.; Xiao, M.; Vasilakos, A.V.; Fischione, C. The Sensable City: A Survey on the Deployment and Management for Smart City Monitoring. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1533–1560. [CrossRef]
41. Wei, K.; Li, J.; Ding, M.; Ma, C.; Yang, H.H.; Farokhi, F.; Jin, S.; Quek, T.Q.; Poor, H.V. Federated learning with differential privacy: Algorithms and performance analysis. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3454–3469. [CrossRef]
42. Lyu, L.; Yu, H.; Yang, Q. Threats to Federated Learning: A Survey. *arXiv* **2020**, arXiv:2003.02133.
43. 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]

44. Guo, B.; Wang, Z.; Yu, Z.; Wang, Y.; Yen, N.Y.; Huang, R.; Zhou, X. Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm. *ACM Comput. Surv. (CSUR)* **2015**, *48*, 7. [CrossRef]
45. Ganti, R.K.; Ye, F.; Lei, H. Mobile crowdsensing: Current state and future challenges. *IEEE Commun. Mag.* **2011**, *49*, 32–39. [CrossRef]
46. Ma, H.; Zhao, D.; Yuan, P. Opportunities in mobile crowd sensing. *IEEE Commun. Mag.* **2014**, *52*, 29–35. [CrossRef]
47. Wang, L.; Zhang, D.; Wang, Y.; Chen, C.; Han, X.; M'hamed, A. Sparse mobile crowdsensing: Challenges and opportunities. *IEEE Commun. Mag.* **2016**, *54*, 161–167. [CrossRef]
48. Zhou, Z.; Liao, H.; Gu, B.; Huq, K.M.S.; Mumtaz, S.; Rodriguez, J. Robust mobile crowd sensing: When deep learning meets edge computing. *IEEE Netw.* **2018**, *32*, 54–60. [CrossRef]
49. Sherchan, W.; Jayaraman, P.P.; Krishnaswamy, S.; Zaslavsky, A.; Loke, S.; Sinha, A. Using on-the-move mining for mobile crowdsensing. In Proceedings of the 2012 IEEE 13th International Conference on Mobile Data Management, Bengaluru, India, 23–26 July 2012; pp. 115–124.
50. Liu, Y.; Guo, B.; Wang, Y.; Wu, W.; Yu, Z.; Zhang, D. TaskMe: Multi-task allocation in mobile crowd sensing. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Heidelberg, Germany, 12–16 September 2016; pp. 403–414.
51. Xiao, Y.; Simoens, P.; Pillai, P.; Ha, K.; Satyanarayanan, M. Lowering the barriers to large-scale mobile crowdsensing. In Proceedings of the 14th Workshop on Mobile Computing Systems and Applications, Jekyll Island, GA, USA, 26–27 February 2013; p. 9.
52. Wan, J.; Liu, J.; Shao, Z.; Vasilakos, A.V.; Imran, M.; Zhou, K. Mobile crowd sensing for traffic prediction in internet of vehicles. *Sensors* **2016**, *16*, 88. [CrossRef]
53. Hu, X.; Li, X.; Ngai, E.C.H.; Leung, V.C.; Kruchten, P. Multidimensional context-aware social network architecture for mobile crowdsensing. *IEEE Commun. Mag.* **2014**, *52*, 78–87. [CrossRef]
54. Marjanović, M.; Antonić, A.; Žarko, I.P. Edge computing architecture for mobile crowdsensing. *IEEE Access* **2018**, *6*, 10662–10674. [CrossRef]
55. He, D.; Chan, S.; Guizani, M. User privacy and data trustworthiness in mobile crowd sensing. *IEEE Wirel. Commun.* **2015**, *22*, 28–34. [CrossRef]
56. White, D.E.; Oelke, N.D.; Friesen, S. Management of a large qualitative data set: Establishing trustworthiness of the data. *Int. J. Qual. Methods* **2012**, *11*, 244–258. [CrossRef]
57. Pouryazdan, M.; Kantarci, B. The smart citizen factor in trustworthy smart city crowdsensing. *IT Prof.* **2016**, *18*, 26–33. [CrossRef]
58. Pouryazdan, M.; Kantarci, B.; Soyata, T.; Foschini, L.; Song, H. Quantifying User Reputation Scores, Data Trustworthiness, and User Incentives in Mobile Crowd-Sensing. *IEEE Access* **2017**, *5*, 1382–1397. [CrossRef]
59. Bertino, E. Data trustworthiness—Approaches and research challenges. In *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*; Springer: Wroclaw, Poland, 2014; pp. 17–25.
60. Suhail, S.; Hong, C.S.; Lodhi, M.A.; Zafar, F.; Khan, A.; Bashir, F. Data trustworthiness in iot. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–15 January 2018; pp. 414–419.
61. Bertino, E.; Dai, C.; Kantarcioglu, M. The challenge of assuring data trustworthiness. In Proceedings of the International Conference on Database Systems for Advanced Applications, Brisbane, Australia, 21–23 April 2009; pp. 22–33.
62. Ogie, R.I.; Forehead, H.; Clarke, R.J.; Perez, P. Participation Patterns and Reliability of Human Sensing in Crowd-Sourced Disaster Management. *Inf. Syst. Front.* **2017**, *20*, 713–728. [CrossRef]
63. Dasari, V.S.; Kantarci, B.; Simsek, M. Trustworthiness and Comfort-Aware Participant Recruitment for Mobile Crowd-Sensing in Smart Environments. In Proceedings of the 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 29 June–3 July 2019; pp. 1–6.
64. Luo, T.; Kanhere, S.S.; Huang, J.; Das, S.K.; Wu, F. Sustainable Incentives for Mobile Crowdsensing: Auctions, Lotteries, and Trust and Reputation Systems. *IEEE Commun. Mag.* **2017**, *55*, 68–74. [CrossRef]
65. Wen, Y.; Shi, J.; Zhang, Q.; Tian, X.; Huang, Z.; Yu, H.; Cheng, Y.; Shen, X. Quality-driven auction-based incentive mechanism for mobile crowd sensing. *IEEE Trans. Veh. Technol.* **2014**, *64*, 4203–4214. [CrossRef]
66. Yang, G.; He, S.; Shi, Z.; Chen, J. Promoting cooperation by the social incentive mechanism in mobile crowdsensing. *IEEE Commun. Mag.* **2017**, *55*, 86–92. [CrossRef]

67. Jin, H.; Su, L.; Ding, B.; Nahrstedt, K.; Borisov, N. Enabling privacy-preserving incentives for mobile crowd sensing systems. In Proceedings of the 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), Nara, Japan, 27–30 June 2016; pp. 344–353.
68. Jin, H.; Su, L.; Xiao, H.; Nahrstedt, K. Incentive mechanism for privacy-aware data aggregation in mobile crowd sensing systems. *IEEE/ACM Trans. Netw.* **2018**, *26*, 2019–2032. [CrossRef]
69. Wang, J.; Tang, J.; Yang, D.; Wang, E.; Xue, G. Quality-aware and fine-grained incentive mechanisms for mobile crowdsensing. In Proceedings of the 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), Nara, Japan, 27–30 June 2016; pp. 354–363.
70. Gisdakis, S.; Giannetsos, T.; Papadimitratos, P. Security, privacy, and incentive provision for mobile crowd sensing systems. *IEEE Internet Things J.* **2016**, *3*, 839–853. [CrossRef]
71. Han, G.; Liu, L.; Chan, S.; Yu, R.; Yang, Y. HySense: A hybrid mobile crowdsensing framework for sensing opportunities compensation under dynamic coverage constraint. *IEEE Commun. Mag.* **2017**, *55*, 93–99. [CrossRef]
72. Ogie, R.I. Adopting incentive mechanisms for large-scale participation in mobile crowdsensing: From literature review to a conceptual framework. *Hum. Centric Comput. Inf. Sci.* **2016**, *6*, 24. [CrossRef]
73. Khan, F.; Rehman, A.U.; Zheng, J.; Jan, M.A.; Alam, M. Mobile crowdsensing: A survey on privacy-preservation, task management, assignment models, and incentives mechanisms. *Future Gener. Comput. Syst.* **2019**, *100*, 456–472. [CrossRef]
74. Zheng, Z.; Wu, F.; Gao, X.; Zhu, H.; Tang, S.; Chen, G. A budget feasible incentive mechanism for weighted coverage maximization in mobile crowdsensing. *IEEE Trans. Mob. Comput.* **2016**, *16*, 2392–2407. [CrossRef]
75. Gao, H.; Liu, C.H.; Tang, J.; Yang, D.; Hui, P.; Wang, W. Online quality-aware incentive mechanism for mobile crowd sensing with extra bonus. *IEEE Trans. Mob. Comput.* **2018**, *18*, 2589–2603. [CrossRef]
76. Jin, H.; Su, L.; Nahrstedt, K. CENTURION: Incentivizing multi-requester mobile crowd sensing. In Proceedings of the IEEE Conference on Computer Communications (IEEE INFOCOM 2017), Atlanta, GA, USA, 1–4 May 2017; pp. 1–9.
77. Xiong, J.; Chen, X.; Yang, Q.; Chen, L.; Yao, Z. A task-oriented user selection incentive mechanism in edge-aided mobile crowdsensing. *IEEE Trans. Netw. Sci. Eng.* **2019**. [CrossRef]
78. Zhao, D.; Ma, H.; Liu, L. Frugal online incentive mechanisms for mobile crowd sensing. *IEEE Trans. Veh. Technol.* **2016**, *66*, 3319–3330. [CrossRef]
79. Li, H.; Ota, K.; Dong, M.; Guo, M. Mobile crowdsensing in software defined opportunistic networks. *IEEE Commun. Mag.* **2017**, *55*, 140–145. [CrossRef]
80. Xu, J.; Rao, Z.; Xu, L.; Yang, D.; Li, T. Incentive mechanism for multiple cooperative tasks with compatible users in mobile crowd sensing via online communities. *IEEE Trans. Mob. Comput.* **2019**, *19*, 1618–1633. [CrossRef]
81. Zhang, X.; Jiang, L.; Wang, X. Incentive mechanisms for mobile crowdsensing with heterogeneous sensing costs. *IEEE Trans. Veh. Technol.* **2019**, *68*, 3992–4002. [CrossRef]
82. Wu, Y.; Li, F.; Ma, L.; Xie, Y.; Li, T.; Wang, Y. A context-aware multiarmed bandit incentive mechanism for mobile crowd sensing systems. *IEEE Internet Things J.* **2019**, *6*, 7648–7658. [CrossRef]
83. Nan, W.; Guo, B.; Huangfu, S.; Yu, Z.; Chen, H.; Zhou, X. A cross-space, multi-interaction-based dynamic incentive mechanism for mobile crowd sensing. In Proceedings of the 2014 IEEE 11th International Conference on Ubiquitous Intelligence and Computing and 2014 IEEE 11th International Conference on Autonomic and Trusted Computing and 2014 IEEE 14th International Conference on Scalable Computing and Communications and Its Associated Workshops, Bali, Indonesia, 9–12 December 2014; pp. 79–186.
84. Suliman, A.; Otrok, H.; Mizouni, R.; Singh, S.; Ouali, A. A greedy-proof incentive-compatible mechanism for group recruitment in mobile crowd sensing. *Future Gener. Comput. Syst.* **2019**, *101*, 1158–1167. [CrossRef]
85. Duan, Z.; Tian, L.; Yan, M.; Cai, Z.; Han, Q.; Yin, G. Practical incentive mechanisms for IoT-based mobile crowdsensing systems. *IEEE Access* **2017**, *5*, 20383–20392. [CrossRef]
86. Nie, J.; Xiong, Z.; Niyato, D.; Wang, P.; Luo, J. A socially-aware incentive mechanism for mobile crowdsensing service market. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, UAE, 9–13 December 2018; pp. 1–7.
87. Wang, Z.; Li, J.; Hu, J.; Ren, J.; Li, Z.; Li, Y. Towards privacy-preserving incentive for mobile crowdsensing under an untrusted platform. In Proceedings of the IEEE Conference on Computer Communications (IEEE INFOCOM 2019), Paris, France, 29 April–2 May 2019; pp. 2053–2061.

88. Zhang, X.; Xue, G.; Yu, R.; Yang, D.; Tang, J. Robust incentive tree design for mobile crowdsensing. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; pp. 458–468.
89. Zhang, X.; Liang, L.; Luo, C.; Cheng, L. Privacy-preserving incentive mechanisms for mobile crowdsensing. *IEEE Pervasive Comput.* **2018**, *17*, 47–57. [CrossRef]
90. Zhao, B.; Tang, S.; Liu, X.; Zhang, X. PACE: Privacy-preserving and quality-aware incentive mechanism for mobile crowdsensing. *IEEE Trans. Mob. Comput.* **2020**. [CrossRef]
91. Chen, X.; Liu, M.; Zhou, Y.; Li, Z.; Chen, S.; He, X. A truthful incentive mechanism for online recruitment in mobile crowd sensing system. *Sensors* **2017**, *17*, 79. [CrossRef]
92. Angelopoulos, C.M.; Nikoletseas, S.; Raptis, T.P.; Rolim, J.D. Characteristic utilities, join policies and efficient incentives in mobile crowdsensing systems. In Proceedings of the 2014 IFIP Wireless Days (WD), Rio de Janeiro, Brazil, 12–14 November 2014; pp. 1–6.
93. Dimitriou, T.; Krontiris, I. Privacy-respecting auctions as incentive mechanisms in mobile crowd sensing. In Proceedings of the IFIP International Conference on Information Security Theory and Practice, Heraklion, Crete, Greece, 24–25 August 2015; pp. 20–35.
94. Tao, D.; Zhong, S.; Luo, H. Staged incentive and punishment mechanism for mobile crowd sensing. *Sensors* **2018**, *18*, 2391. [CrossRef] [PubMed]
95. Yang, S.; Wu, F.; Tang, S.; Gao, X.; Yang, B.; Chen, G. On designing data quality-aware truth estimation and surplus sharing method for mobile crowdsensing. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 832–847. [CrossRef]
96. Liu, S.; Zheng, Z.; Wu, F.; Tang, S.; Chen, G. Context-aware data quality estimation in mobile crowdsensing. In Proceedings of the IEEE Conference on Computer Communications (IEEE INFOCOM 2017), Atlanta, GA, USA, 1–4 May 2017; pp. 1–9.
97. Luo, T.; Huang, J.; Kanhere, S.S.; Zhang, J.; Das, S.K. Improving IoT data quality in mobile crowd sensing: A cross validation approach. *IEEE Internet Things J.* **2019**, *6*, 5651–5664. [CrossRef]
98. Zhao, C.; Yang, S.; Yan, P.; Yang, Q.; Yang, X.; McCann, J. Data quality guarantee for credible caching device selection in mobile crowdsensing systems. *IEEE Wirel. Commun.* **2018**, *25*, 58–64. [CrossRef]
99. Wei, X.; Wang, Y.; Tan, J.; Gao, S. Data quality aware task allocation with budget constraint in mobile crowdsensing. *IEEE Access* **2018**, *6*, 48010–48020. [CrossRef]
100. Li, W.; Li, F.; Sharif, K.; Wang, Y. When user interest meets data quality: A novel user filter scheme for mobile crowd sensing. In Proceedings of the 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), Shenzhen, China, 15–17 December 2017; pp. 97–104.
101. Xia, X.; Zhou, Y.; Li, J.; Yu, R. Quality-aware sparse data collection in MEC-enhanced mobile crowdsensing systems. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1051–1062. [CrossRef]
102. Poe, W.Y.; Schmitt, J.B. Node deployment in large wireless sensor networks: Coverage, energy consumption, and worst-case delay. In Proceedings of the Asian Internet Engineering Conference, Bangkok, Thailand, 18–20 November 2009; pp. 77–84.
103. Younis, O.; Krunz, M.; Ramasubramanian, S. Node clustering in wireless sensor networks: Recent developments and deployment challenges. *IEEE Netw.* **2006**, *20*, 20–25. [CrossRef]
104. Wang, L.; Zhang, D.; Yan, Z.; Xiong, H.; Xie, B. effSense: A novel mobile crowd-sensing framework for energy-efficient and cost-effective data uploading. *IEEE Trans. Syst. Man Cybern. Syst.* **2015**, *45*, 1549–1563. [CrossRef]
105. Liu, C.H.; Zhang, B.; Su, X.; Ma, J.; Wang, W.; Leung, K.K. Energy-aware participant selection for smartphone-enabled mobile crowd sensing. *IEEE Syst. J.* **2015**, *11*, 1435–1446. [CrossRef]
106. Wang, J.; Wang, Y.; Zhang, D.; Helal, S. Energy saving techniques in mobile crowd sensing: Current state and future opportunities. *IEEE Commun. Mag.* **2018**, *56*, 164–169. [CrossRef]
107. Wang, L.; Zhang, D.; Xiong, H. effSense: Energy-efficient and cost-effective data uploading in mobile crowdsensing. In Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication, Zurich, Switzerland, 8–12 September 2013; pp. 1075–1086.
108. Wang, J.; Tang, J.; Xue, G.; Yang, D. Towards energy-efficient task scheduling on smartphones in mobile crowd sensing systems. *Comput. Netw.* **2017**, *115*, 100–109. [CrossRef]
109. Zhou, Z.; Feng, J.; Gu, B.; Ai, B.; Mumtaz, S.; Rodriguez, J.; Guizani, M. When mobile crowd sensing meets UAV: Energy-efficient task assignment and route planning. *IEEE Trans. Commun.* **2018**, *66*, 5526–5538. [CrossRef]

110. Xiong, H.; Zhang, D.; Wang, L.; Chaouchi, H. EMC 3: Energy-efficient data transfer in mobile crowdsensing under full coverage constraint. *IEEE Trans. Mob. Comput.* **2014**, *14*, 1355–1368. [CrossRef]
111. Marjanović, M.; Skorin-Kapov, L.; Pripužić, K.; Antonić, A.; Žarko, I.P. Energy-aware and quality-driven sensor management for green mobile crowd sensing. *J. Netw. Comput. Appl.* **2016**, *59*, 95–108. [CrossRef]
112. Tomasoni, M.; Capponi, A.; Fiandrino, C.; Kliazovich, D.; Granelli, F.; Bouvry, P. Why energy matters? Profiling energy consumption of mobile crowdsensing data collection frameworks. *Pervasive Mob. Comput.* **2018**, *51*, 193–208. [CrossRef]
113. Xiong, J.; Ma, R.; Chen, L.; Tian, Y.; Li, Q.; Liu, X.; Yao, Z. A personalized privacy protection framework for mobile crowdsensing in IIoT. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4231–4241. [CrossRef]
114. Alsheikh, M.A.; Jiao, Y.; Niyato, D.; Wang, P.; Leong, D.; Han, Z. The Accuracy-Privacy Tradeoff of Mobile Crowdsensing. *arXiv* **2017**, arXiv:1702.04565.
115. Ma, R.; Xiong, J.; Lin, M.; Yao, Z.; Lin, H.; Ye, A. Privacy protection-oriented mobile crowdsensing analysis based on game theory. In Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, Australia, 1–4 August 2017; pp. 990–995.
116. Wang, Z.; Hu, J.; Lv, R.; Wei, J.; Wang, Q.; Yang, D.; Qi, H. Personalized privacy-preserving task allocation for mobile crowdsensing. *IEEE Trans. Mob. Comput.* **2018**, *18*, 1330–1341. [CrossRef]
117. Yang, Q.; Liu, Y.; Cheng, Y.; Kang, Y.; Chen, T.; Yu, H. Federated learning. *Synth. Lect. Artif. Intell. Mach. Learn.* **2019**, *13*, 1–207. [CrossRef]
118. Kairouz, P.; McMahan, H.B.; Avent, B.; Bellet, A.; Bennis, M.; Bhagoji, A.N.; Bonawitz, K.; Charles, Z.; Cormode, G.; Cummings, R.; et al. Advances and Open Problems in Federated Learning. *arXiv* **2019**, arXiv:1912.04977.
119. Xu, G.; Li, H.; Liu, S.; Yang, K.; Lin, X. Verifynet: Secure and verifiable federated learning. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 911–926. [CrossRef]
120. Lim, W.Y.B.; Luong, N.C.; Hoang, D.T.; Jiao, Y.; Liang, Y.C.; Yang, Q.; Niyato, D.; Miao, C. Federated learning in mobile edge networks: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2031–2063. [CrossRef]
121. Wang, X.; Han, Y.; Wang, C.; Zhao, Q.; Chen, X.; Chen, M. In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning. *IEEE Netw.* **2019**, *33*, 156–165. [CrossRef]
122. Niknam, S.; Dhillon, H.S.; Reed, J.H. Federated Learning for Wireless Communications: Motivation, Opportunities, and Challenges. *IEEE Commun. Mag.* **2020**, *58*, 46–51. [CrossRef]
123. Bonawitz, K.; Ivanov, V.; Kreuter, B.; Marcedone, A.; McMahan, H.B.; Patel, S.; Ramage, D.; Segal, A.; Seth, K. Practical secure aggregation for federated learning on user-held data. *arXiv* **2016**, arXiv:1611.04482.
124. Abad, M.S.H.; Ozfatura, E.; Gunduz, D.; Ercetin, O. Hierarchical federated learning across heterogeneous cellular networks. In Proceedings of the ICASSP 2020–2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 4–8 May 2020; pp. 8866–8870.
125. Zhao, Y.; Zhao, J.; Jiang, L.; Tan, R.; Niyato, D. Mobile edge computing, blockchain and reputation-based crowdsourcing iot federated learning: A secure, decentralized and privacy-preserving system. *arXiv* **2019**, arXiv:1906.10893.
126. Zhao, Z.; Feng, C.; Yang, H.H.; Luo, X. Federated-Learning-Enabled Intelligent Fog Radio Access Networks: Fundamental Theory, Key Techniques, and Future Trends. *IEEE Wirel. Commun.* **2020**, *27*, 22–28. [CrossRef]
127. Chai, Z.; Fayyaz, H.; Fayyaz, Z.; Anwar, A.; Zhou, Y.; Baracaldo, N.; Ludwig, H.; Cheng, Y. Towards taming the resource and data heterogeneity in federated learning. In Proceedings of the 2019 {USENIX} Conference on Operational Machine Learning (OpML 19), Santa Clara, CA, USA, 20 May 2019; pp. 19–21.
128. Wang, S.; Tuor, T.; Salonidis, T.; Leung, K.K.; Makaya, C.; He, T.; Chan, K. Adaptive federated learning in resource constrained edge computing systems. *IEEE J. Sel. Areas Commun.* **2019**, *37*, 1205–1221. [CrossRef]
129. Gao, D.; Ju, C.; Wei, X.; Liu, Y.; Chen, T.; Yang, Q. HHHFL: Hierarchical Heterogeneous Horizontal Federated Learning for Electroencephalography. *arXiv* **2019**, arXiv:1909.05784.
130. Wang, G.; Dang, C.X.; Zhou, Z. Measure contribution of participants in federated learning. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; pp. 2597–2604.
131. Li, S.; Cheng, Y.; Liu, Y.; Wang, W.; Chen, T. Abnormal client behavior detection in federated learning. *arXiv* **2019**, arXiv:1910.09933.
132. Wang, G. Interpret federated learning with shapley values. *arXiv* **2019**, arXiv:1905.04519.

133. Song, T.; Tong, Y.; Wei, S. Profit Allocation for Federated Learning. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; pp. 2577–2586.
134. Li, Q.; Wen, Z.; He, B. Federated learning systems: Vision, hype and reality for data privacy and protection. *arXiv* **2019**, arXiv:1907.09693.
135. Yang, K.; Fan, T.; Chen, T.; Shi, Y.; Yang, Q. A quasi-newton method based vertical federated learning framework for logistic regression. *arXiv* **2019**, arXiv:1912.00513.
136. Feng, S.; Yu, H. Multi-Participant Multi-Class Vertical Federated Learning. *arXiv* **2020**, arXiv:2001.11154.
137. Gao, D.; Liu, Y.; Huang, A.; Ju, C.; Yu, H.; Yang, Q. Privacy-preserving heterogeneous federated transfer learning. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; pp. 2552–2559.
138. Bonawitz, K.; Eichner, H.; Grieskamp, W.; Huba, D.; Ingerman, A.; Ivanov, V.; Kiddon, C.; Konečnỳ, J.; Mazzocchi, S.; McMahan, H.B.; et al. Towards federated learning at scale: System design. *arXiv* **2019**, arXiv:1902.01046.
139. Nishio, T.; Yonetani, R. Client Selection for Federated Learning with Heterogeneous Resources in Mobile Edge. In Proceedings of the 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019. [CrossRef]
140. Liu, Y.; Yu, J.J.Q.; Kang, J.; Niyato, D.; Zhang, S. Privacy-Preserving Traffic Flow Prediction: A Federated Learning Approach. *IEEE Internet Things J.* **2020**, *7/8*, 7751–7763.
141. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A.Y. Communication-Efficient Learning of Deep Networks from Decentralized Data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, Fort Lauderdale, FL, USA, 20–22 April 2017; Singh, A., Zhu, J., Eds.; Volume 54, pp. 1273–1282.
142. McMahan, H.B.; Ramage, D.; Talwar, K.; Zhang, L. Learning Differentially Private Recurrent Language Models. *arXiv* **2017**, arXiv:1710.06963.
143. Li, T.; Sahu, A.K.; Zaheer, M.; Sanjabi, M.; Talwalkar, A.; Smith, V. Federated Optimization in Heterogeneous Networks. *arXiv* **2018**, arXiv:1812.06127.
144. Huang, L.; Yin, Y.; Fu, Z.; Zhang, S.; Deng, H.; Liu, D. Loadaboost: Loss-based adaboost federated machine learning on medical data. *arXiv* **2018**, arXiv:1811.12629.
145. Kang, J.; Xiong, Z.; Niyato, D.; Xie, S.; Zhang, J. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. *IEEE Internet Things J.* **2019**, *6*, 10700–10714. [CrossRef]
146. Wang, Y.; Kantarci, B. A Novel Reputation-Aware Client Selection Scheme for Federated Learning within Mobile Environments. In Proceedings of the IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Pisa, Italy, 14–16 September 2020.
147. Kang, J.; Xiong, Z.; Niyato, D.; Zou, Y.; Zhang, Y.; Guizani, M. Reliable Federated Learning for Mobile Networks. *IEEE Wirel. Commun.* **2020**, *27*, 72–80. [CrossRef]
148. Shayan, M.; Fung, C.; Yoon, C.J.; Beschastnikh, I. Biscotti: A ledger for private and secure peer-to-peer machine learning. *arXiv* **2018**, arXiv:1811.09904.
149. Fung, C.; Yoon, C.J.M.; Beschastnikh, I. Mitigating Sybils in Federated Learning Poisoning. *arXiv* **2018**, arXiv:1808.04866.
150. Liu, Z.; Li, T.; Smith, V.; Sekar, V. Enhancing the Privacy of Federated Learning with Sketching. *arXiv* **2019**, arXiv:1911.01812.
151. Hao, M.; Li, H.; Luo, X.; Xu, G.; Yang, H.; Liu, S. Efficient and privacy-enhanced federated learning for industrial artificial intelligence. *IEEE Trans. Ind. Inform.* **2019**, *16*, 6532–6542. [CrossRef]
152. Awan, S.; Li, F.; Luo, B.; Liu, M. Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 2561–2563.
153. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4177–4186. [CrossRef]
154. Lyu, L.; Yu, J.; Nandakumar, K.; Li, Y.; Ma, X.; Jin, J.; Yu, H.; Ng, K.S. Towards Fair and Privacy-Preserving Federated Deep Models. *arXiv* **2019**, arXiv:1906.01167.
155. Zhao, Y.; Zhao, J.; Jiang, L.; Tan, R.; Niyato, D.; Li, Z.; Lyu, L.; Liu, Y. Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices. *IEEE Internet Things J.* **2020**. [CrossRef]

156. Yu, H.; Liu, Z.; Liu, Y.; Chen, T.; Cong, M.; Weng, X.; Niyato, D.; Yang, Q. A fairness-aware incentive scheme for federated learning. In Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, New York, NY, USA, 7–8 February 2020; pp. 393–399.
157. Liu, Y.; Wei, J. Incentives for Federated Learning: A Hypothesis Elicitation Approach. *arXiv* **2020**, arXiv:2007.10596.
158. Zhan, Y.; Li, P.; Qu, Z.; Zeng, D.; Guo, S. A learning-based incentive mechanism for federated learning. *IEEE Internet Things J.* **2020**, *7*, 6360–6368. [CrossRef]
159. Lin, Y.; Han, S.; Mao, H.; Wang, Y.; Dally, W.J. Deep Gradient Compression: Reducing the Communication Bandwidth for Distributed Training. *arXiv* **2017**, arXiv:1712.01887.
160. Braun, T.; Fung, B.C.; Iqbal, F.; Shah, B. Security and privacy challenges in smart cities. *Sustain. Cities Soc.* **2018**, *39*, 499–507. [CrossRef]
161. Zhang, K.; Ni, J.; Yang, K.; Liang, X.; Ren, J.; Shen, X.S. Security and privacy in smart city applications: Challenges and solutions. *IEEE Commun. Mag.* **2017**, *55*, 122–129. [CrossRef]
162. Baig, Z.A.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K.; et al. Future challenges for smart cities: Cyber-security and digital forensics. *Digit. Investig.* **2017**, *22*, 3–13. [CrossRef]
163. Preuveneers, D.; Rimmer, V.; Tsingenopoulos, I.; Spooren, J.; Joosen, W.; Ilie-Zudor, E. Chained anomaly detection models for federated learning: An intrusion detection case study. *Appl. Sci.* **2018**, *8*, 2663. [CrossRef]
164. Schwarting, W.; Alonso-Mora, J.; Rus, D. Planning and decision-making for autonomous vehicles. *Annu. Rev. Control Robot. Auton. Syst.* **2018**, *1*, 187–210 [CrossRef]
165. Talebpour, A.; Mahmassani, H.S. Influence of connected and autonomous vehicles on traffic flow stability and throughput. *Transp. Res. Part C Emerg. Technol.* **2016**, *71*, 143–163. [CrossRef]
166. Gerla, M.; Lee, E.K.; Pau, G.; Lee, U. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In Proceedings of the 2014 IEEE world Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 241–246.
167. Imteaj, A.; Amini, M.H. Distributed sensing using smart end-user devices: Pathway to federated learning for autonomous IoT. In Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 5–7 December 2019; pp. 1156–1161.
168. Wang, J.; Jiang, C.; Zhang, K.; Quek, T.Q.; Ren, Y.; Hanzo, L. Vehicular sensing networks in a smart city: Principles, technologies and applications. *IEEE Wirel. Commun.* **2017**, *25*, 122–132. [CrossRef]
169. Alam, K.M.; Saini, M.; El Saddik, A. Toward social internet of vehicles: Concept, architecture, and applications. *IEEE Access* **2015**, *3*, 343–357. [CrossRef]
170. Samarakoon, S.; Bennis, M.; Saad, W.; Debbah, M. Distributed Federated Learning for Ultra-Reliable Low-Latency Vehicular Communications. *IEEE Trans. Commun.* **2020**, *68*, 1146–1159. [CrossRef]
171. Mahadevan, K.; Somanath, S.; Sharlin, E. Communicating awareness and intent in autonomous vehicle-pedestrian interaction. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 21–26 April 2018; pp. 1–12.
172. Haleem, A.; Javaid, M.; Khan, I.H. Current status and applications of artificial intelligence (AI) in medical field: An overview. *Curr. Med. Res. Pract.* **2019**, *9*, 231–237. [CrossRef]
173. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [CrossRef]
174. Brisimi, T.S.; Chen, R.; Mela, T.; Olshevsky, A.; Paschalidis, I.C.; Shi, W. Federated learning of predictive models from federated electronic health records. *Int. J. Med. Inform.* **2018**, *112*, 59–67. [CrossRef] [PubMed]
175. Catarinucci, L.; De Donno, D.; Mainetti, L.; Palano, L.; Patrono, L.; Stefanizzi, M.L.; Tarricone, L. An IoT-aware architecture for smart healthcare systems. *IEEE Internet Things J.* **2015**, *2*, 515–526. [CrossRef]
176. Tran, N.H.; Bao, W.; Zomaya, A.; NH, N.M.; Hong, C.S. Federated learning over wireless networks: Optimization model design and analysis. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; pp. 1387–1395.
177. Amiri, M.M.; Gündüz, D. Federated learning over wireless fading channels. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 3546–3557. [CrossRef]
178. Jin, R.; He, X.; Dai, H. On the Design of Communication Efficient Federated Learning over Wireless Networks. *arXiv* **2020**, arXiv:2004.07351.

179. Zeng, Q.; Du, Y.; Huang, K.; Leung, K.K. Energy-efficient radio resource allocation for federated edge learning. In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
180. Wang, Z.; Song, M.; Zhang, Z.; Song, Y.; Wang, Q.; Qi, H. Beyond inferring class representatives: User-level privacy leakage from federated learning. In Proceedings of the IEEE Conference on Computer Communications (IEEE INFOCOM 2019), Paris, France, 29 April–2 May 2019; pp. 2512–2520.
181. Nasr, M.; Shokri, R.; Houmansadr, A. Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 739–753.
182. Melis, L.; Song, C.; Cristofaro, E.D.; Shmatikov, V. Exploiting Unintended Feature Leakage in Collaborative Learning. *arXiv* **2018**, arXiv:1805.04049.
183. Bhagoji, A.N.; Chakraborty, S.; Mittal, P.; Calo, S. Analyzing federated learning through an adversarial lens. In Proceedings of the International Conference on Machine Learning, Long Beach, CA, USA, 10–15 June 2019; pp. 634–643.
184. Bagdasaryan, E.; Veit, A.; Hua, Y.; Estrin, D.; Shmatikov, V. How To Backdoor Federated Learning. *arXiv* **2018**, arXiv:1807.00459.
185. Fang, M.; Cao, X.; Jia, J.; Gong, N.Z. Local Model Poisoning Attacks to Byzantine-Robust Federated Learning. *arXiv* **2019**, arXiv:1911.11815
186. Zhao, Y.; Li, M.; Lai, L.; Suda, N.; Civin, D.; Chandra, V. Federated Learning with Non-IID Data. *arXiv* **2018**, arXiv:1806.00582.
187. Kopparapu, K.; Lin, E. FedFMC: Sequential Efficient Federated Learning on Non-iid Data. *arXiv* **2020**, arXiv:2006.10937.