Combating Hard or Soft Disasters with Privacy-Preserving Federated Mobile Buses-and-Drones based Networks

1st Bo Ma
Department of Information
Technology and Software Engineering
Auckland University of Technology
, Auckland, New Zealand
bo.ma@aut.ac.nz

2nd Jinsong Wu
School of Artificial Intelligence,
Guilin University of Electronic Technology, Guilin, China,
Department of Electrical Engineering,
Universidad de Chile, Santiago, Chile
wujs@ieee.org

3nd William Liu
Department of Information,
Technology and Software Engineering
Auckland University of Technology
, Auckland, New Zealand
william.liu@aut.ac.nz

4nd Luca Chiaraviglio
Department of Electronic Engineering,
Technology and Software Engineering
Tor Vergata University of Rome
, Rome,Italy
luca.chiaraviglio@uniroma2.it

5nd Xing Ming
Department of Information,
Technology and Software Engineering
Auckland University of Technology
, Auckland, New Zealand
Xing.Ming@aut.ac.nz

***Abstract*—It is foreseeable the popularity of the mobile edge computing enabled infrastructure for wireless networks in the incoming fifth generation (5G) and future sixth generation (6G) wireless networks. Especially after a 'hard' disaster such as earthquakes or a 'soft' disaster such as COVID-19 pandemic, the existing telecommunication infrastructure, including wired and wireless networks, is often seriously compromised or with infectious disease risks and should-not-close-contact, thus cannot guarantee regular coverage and reliable communications services. These temporarily-missing communications capabilities are crucial to rescuers, health-carers, or affected or infected citizens as the responders need to effectively coordinate and communicate to minimize the loss of lives and property, where the 5G/6G mobile edge network helps. On the other hand, the federated machine learning (FML) methods have been newly developed to address the privacy leakage problems of the traditional machine learning held normally by one centralized organization, associated with the high risks of a single point of hacking. After detailing current state-of-the-art both in privacy-preserving, federated learning, and mobile edge communications networks for 'hard' and 'soft' disasters, we consider the main challenges that need to be faced. We envision a privacy-preserving federated learning enabled buses-and-drones based mobile edge infrastructure (ppFL-AidLife) for disaster or pandemic emergency communications. The ppFL-AidLife system aims at a rapidly deployable resilient network capable of supporting flexible, privacy-preserving and low-latency communications to serve large-scale disaster situations by utilizing the existing public transport networks, associated with drones to maximally extend their radio coverage to those hard-to-reach disasters or should-not-close-contact pandemic zones.**

***Index Terms*—Infectious disease surveillance, Federated Machine Learning, Privacy-Preserving(PP)**

I. Introduction

A study of recent natural disasters [1] has revealed the enormous scale, complexity, and destructive power of such events and the fact that the negative economic impact and costs of human lives are large. Moreover, disasters such as the earthquakes, hurricane, flooding, and fire, for instance, they can cause significant physical damage to the available electronic equipment, which are essential units forming the communications networks thus causing severe disruptions even full loss of emergency communications. On the other hand, the current COVID-19 pandemic raises a new challenge of 'soft' damage [2] because this type of infectious disease causes accessibility risks when closes to contact the person or communities infected, while emergency communications are critical for saving lives for physical- or soft- disaster recovery. Some studies [3], [4] shows that unmanned aerial vehicle (UAV) assisted 5G mobile edge networks are promising to address the above challenges because of its flexibility, scalability, especially low-latency communications and computing between the edge-cloudlets to the end-user devices. The UAVs and mobile terminals are key units to gather timeliness information for planning emergency responses, while privacy control is emerging for information gathering and broadcasting during the disasters [5]. How to control the privacy level is an important issue when gathering information during disasters.

For example, where a rescue UAV is searching any survivor who might have a mobile phone, it is very helpful if that mobile phone is able to automatically distribute detailed information on the location of the terminal and also related personal information such as age, name, phone number, any chronic

DOI 10.1109/IRI49571.2020.00013

disease or drug use history for best responses. On the other hand, their privacy should be protected in the usage phase, i.e., the sensitive personal information should be kept secret but UAVs/ responders can still obtain personalized information customized to each person. In addition, due to the constraints of battery and load capacity, the flying UAVs are in the open-air prone to different failures such as accidental attacks by the drone-hunters or being hacked by another spy-drone, or non-accidental failures, and the data privacy [6], especially during the emergency becoming paramount. Privacy-preserving has become more and more sophisticated for machine learning in recent years, as many privacy problems occurred during practical applications such as disasters. In addition, more problems have emerged with the privacy-preserving centralised machine learning methods, which encouraged academia and industry to look at the federated machine learning technology. It sounds a better solution to address the privacy issue, and also aligns with the ICT technological trend of increasingly more distributed system architectures and more powerful cutting-edge devices. In order to protect data privacy, the machine learning framework tends to combine with data transformation to improve the performance of privacy preservation [7]. The term "privacy leakage" is defined as the accidental or unintentional transmission of private or sensitive data to an unauthorized entity/individual. "Privacy leakage incidents" are the cases of media reports containing sensitive information, which are exposed by an (possibly unknown) attacker and subsequently (illegally) acquired by the other attackers [8]. In order to measure the level of privacy leakage, certain methods have been provided by academia and industry, including data leakage prevention [9], information leak detection and prevention (ILDP) [10], content monitoring and filtering (CMF) [11], information protection and control (IPC) [12].

In the above context, several questions arise: What is the current state-of-the-art in the field of 5G UAV-assisted mobile edge, and privacy-preserving FML research? What are the main challenges that need to be faced when integrating these two communications and computing technologies? Is it possible to define a holistic system architecture explicitly designed for -federated mobile-edge infrastructure with a privacy-preservation manner for combating various 'hard' or 'soft' disasters? The goal of this paper is to shed light on these issues and to define future research directions. Specifically, we believe that a privacy-preserving federated mobile edge infrastructure should be built around the following pillars: i) possibility in recruiting public bus as deployable edge nodes associated with UAVs to cover those hard-to-reach or should-not-to-contact zones, ii) exploitation of new privacy-preserving FML methods with efficiencies in term of computing speed, and at scale, iii) leveraging the trade-off between privacy protection and data utility for learning the disaster dynamic and best responses to save lives.

The rest parts of the paper are organized as follows. Section 2 reviews the state-of-the-art. Section 3 reports the main challenges and also details our vision to address these challenges. Finally, Section 4 concludes the work and layouts the potential research directions.

II. State-of-The-Art

A. 5G UAV-assisted Mobile Edge Network for Disaster

Mobile edge computing (MEC) [4] is an emerging paradigm that provides cloud services closer to mobile users via leveraging the available resources in the access networks. MEC significantly reduces the network latency, providing location awareness and mobility support by enabling computation and storage capacity located at the edge network compared to the conventional far-end cloud solutions. In addition, many end-user devices with low processor and storage capacity are able to offload their computation to the MEC in order to prolong their battery life.

The terrestrial base stations (BSs) cannot fully satisfy the agility and resilience requirements of cellular networks under the stress caused by disasters, and a possible solution to this problem, we believe is through unmanned aerial vehicles (UAVs), mounted with BS units. The high-quality communications services are critical to saving human lives and for recovery operations in case of disaster and emergency communications. Although these situations are temporary or unexpected, it is not feasible to invest a huge amount of money on a static base station to provide revenue for such a short time during a rare event. UAVs could be a cost-effective and flexible solution as presented in [20]. The advantage of using UAVs is that they can be deployed rapidly as a complement to the remaining heterogeneous networks and also they constitute an effective approach to provide service to reach those hard-to-reach or should-not-to-contact areas affected by a disaster.

B. Privacy-Preserving Approach

The privacy-preserving data mining methods can be classified into five main classes [13] such as randomisation methods (distributed); the k-anonymity and l-diversity methods (hidden); distributed privacy preservation (distributed); downgrading the effectiveness of data mining results (incomplete), and differential privacy (incomplete). After processing the data by using one of these methods, the sensitive attribute values cannot be easily identified to track their provenance. Also, given the user is uncertain (i.e., previously unknown), the data may contain limited or no information about the original user, which means that the user can hardly be marked.

1) k-anonymity Algorithm(1997): To protect the data privacy, Samaratiy and Sweeney proposed the partial information hiding method named k-anonymity algorithm [14]. This algorithm aims to hide the data tuple in the database in order to protect privacy. When the data is released to somebody, the known data cannot be connected with the specific person unless linking private information altogether, hence, even the most sensitive attributes in the database can be protected via this method.

However, many weaknesses and limitations of this algorithm have been found by previous researchers. The most noticeable problem with the algorithm is also its strength – the Domain Generalisation Hierarchy (DGH) functions [15]. DGH

functions are created by implementing customised hierarchies depending on the data. For example, the hierarchies have been created to generalise users' information address in the database, when a user wants to remove some specific residential information from the database, he/she needs to remove the city information, then province, and so on.

2) L-diversity Algorithm (2006): L-diversity is an extension of the k-anonymity algorithm. The improvement has been made is to calculate a utility matrix, which shows how much data can be protected. For example, when the user's data shows some date at 18:00:53 on February 3rd, 1993, the utility matrix will protect this data as XXX, 3rd, 19xx, xx:00:53, whose the utility rate is very high in the matrix. Whilst, the date protection under the k-anonymity algorithm would be just as Feb,3rd,xx93,18:00:xx with a very low utility rate, even equal to zero. Therefore, the utility matrix is adopted to cluster private and sensitive data. Then, the algorithm can classify and merge the above data in different categories by using a similar greedy algorithm with data loss punishment [16].

3) The (a,d)diversity Algorithm (2007): In Wang's paper [17], it madks s_j as the user's records defining as s has sensitive attributes, the quantity of s is j, and bk is the background knowledge. In addition, $RiskRanking(s_i) \in bk$ is risk coefficient according to the Bayes formula. It has:

$$RiskRanking(s_i|bk) = \frac{Risk(s_j)P(bk|s_i)}{\Sigma_(j=1)^f Risk(s_j)P(bk|s_i)} \quad (1)$$

$P(bk|s)$ is the sum of the probable background risk and $bk|s$ is existing as the sensitive attribute values at the same time.

If a certain sensitive attribute value is much higher than others in some conditions, the attacker will easily obtain this sensitive attribute value via bk unit with the already-known conditions. If the higher sensitive attribute values are more than one, the probability of leaking sensitive attribute value would be reduced, thus an algorithm called (a,d)diversity can be applied [17]. Before introducing, the preparatory definitions of this algorithm are required.

Definition 1 ((a,d)diversity)**.** *If a sensitive feature contains at least one alien value and their quantity is d, each value contains at least one similar value and their quantity is s. It has called the equivalence group according to the (a,d) diversity property. If each equivalence in the data source T is matching the property of (a,d) diversity, it has called T to input the table and this form is (a,d) diversity.*

4) The t-closeness Algorithm (2007): Li [18] tried to offset the defect of l-diversity in his research. He assumed that observer A has some individuals' sensitive attribute A_0. Then, in a hypothetical step, observer A gave a completely generalised data table where all attributes are in a quasi-identifier. The observer A acquired information Q, and the sensitive attribute value in the whole data set was defined as A_1. The observer, according to the quasi-identifier values, was able to find the individual's record in an equivalence class and calculate the distribution P of sensitive attribute values. The observers can deduce A_2 from previously acquired data.

Definition 2 (t-closeness)**.** *An equivalence class has t-closeness if the distance between the distribution of a sensitive attribute in this class and the distribution in the whole table is no more than a threshold t. A table is able to have t-closeness if all equivalence classes have t-closeness.*

5) The ε-Differential Algorithm (2006): The k-anonymity and l-diversity algorithms are based on the assumption that none of the sensitive information attributes has been leaked to an attacker. While the ε-differential assumes the worst situation that the attacker has access to all of the sensitive attribute values except one record. When the data resources D_1 and D_2 exist, only one record in these two data resources is different [19]. Whatever the attacker searches, the result would be "same" due to the same index, so the attacker cannot deduce any sensitive attribute value from the probability of sensitive attributes belonging to the data resource.

Definition 3 (ε-differential privacy)**.** *The function θ provide privacy for ε-differential if for all data sets $[x_1], [x_2]$, the users' single data will be modified and filled out of range as $L \subset Range(\theta)$ [20],*

$$\mathbb{P}R(\theta(x_1) \in L) \leq e^{\theta} \times \mathbb{P}R(\theta(x_2) \in L) \quad (2)$$

After this process, the data set will go through a sanitiation approach [21] , also called a noise addition: Let $f(X)$ be as user's response for a data search process, $Y(X)$ as a noise addition process, and $\theta(X) = f(X) + Y(X)$, $\theta(X)$ as the result. In this process, some noises will be added to data with Laplace distribution, the zero mean will generate Y(X), and the scale of the parameter would be distributed in $[0, \frac{\Delta(f)}{\theta}]$. Here θ represents the parameter of differential privacy, and $\Delta(f)$ means the f corresponding to the L-diversity.

We assume that noise $[lap(b) = e]^{-\frac{\omega}{b}}$ follows a symmetrical exponential distribution and the standard deviation is $\sqrt{2}b$, where $b = \frac{\Delta f}{\theta}$, then the probability density function is:

$$p(x) = \frac{\theta}{2\Delta(f)} e^{-\frac{\omega\theta}{\Delta(f)})} \quad (3)$$

In probability density function, $\Delta(f)$ is varied. If θ is small, in order to balance differential private data, more Laplace noises need to be added. While if $\Delta(f)$ is small, the algorithm performs better because of less added noise. When θ decreases, $lap(\frac{\Delta(f)}{\theta})$ curve flattens, meanwhile the expected noise magnitude turns larger. When θ is fixed, the high-sensitivity function f tends to be a more flatter curve, and the magnitude of noise will also be changed considerably.

Compared with previous ones, this method is more effective in protecting privacy with the existence of distributed machine learning or deep learning system, because ε-differential privacy(DP) method neither breaks data itself nor changes the structure of a data set. The only thing that needs to do is measuring the Laplace noise with the same or similar probability distribution of an input data set.

C. Federated Deep Learning

Federated deep learning [22] is one of the machine learning methods, which trains the algorithms without converting multiple decentralised torrent tools or local data models to the data models on the centralised server. This approach is a complement to traditional centralised machine learning practices where all data samples are uploaded to a server. The work [23] has shown that federated deep learning models or federated learning (FL) models have great potentials in learning effective representations and demonstrating cutting-edge performance in computer vision and natural language processing applications. In deep learning models, the symptoms are being learned in a way that is neither supervised nor proven. Although deep learning models are more attractive than the shallow models which cannot automatically learn features (e.g., the effective feature representations are being learned from textual content), this work has been constrained by the size of collaborative learning and the similarity model which inherit the feature from original data. So deep learning methods can be integrated with collaborative learning.

Some researchers had applied differential privacy (DP) to evaluate mechanisms for transporting, indexing, and searching for data. In recent days, more work has been done aiming to link differential privacy to statistical objectives [24]. Some researchers have developed algorithms for private robust estimators, point and histogram estimation, and principal components analysis, etc. [25]. Moreover, FL methods have been illustrated by previous researchers to use differential privacy to connect with machine learning, as the connection between statistical privacy and data statistical features has been applied in recent works, and the statistics serve the basis of machine learning.

D. Privacy-Preserving Federated Deep Learning

1) Distributed Selective Stochastic Gradient Descent: Stochastic gradient descent (SGD) is a way to simplify the objective function with the correct elements of understanding (e.g., division) [26]. This is considered to be a measure of using gradient descent optimisation because it replaces the true gradient (calculated from all the data sets) in its estimation (calculated from the optional data set). While the basic concept of archaeology can be traced back to the Robbins-Monroe algorithm in the 1950s, strong nationalist culture has become an important mechanism for machine learning [27].

Recent works demonstrated that the Distribution Selected SGD is vulnerable to the inference attack [28], e.g., reconstruction attack and membership attack by malicious servers/clients, because the shared model is updated according to those private data, and the attacks‘ patterns are encoded into the model parameters. Therefore, if a corresponding decoder could be constructed, the private data or statistics would be recovered inversely.

2) Privacy-Preserving Federated Deep Learning: Federated machine learning algorithms have exciting features and wide-range potentials. However, as the data frequently contains sensitive personal or organisational information, there are real privacy concerns associated with the development of this technology. Motivated by this observation, Konečný and McMahan initiated the differentially private federated deep learning [29], which aims to construct learning algorithms that provide strong privacy protections for the training data.

In order to improve privacy-preserving in federated machine learning frame, Reza and Vitaly [30] improved current SGD methods, named as Distributed Selective Stochastic Gradient Descent (DSSGD). It has proposed that the collaborative learning DSSGD, where the data providers, i.e., clients, train locally on a shared model, then the server is to collect those local models/updates to estimate/update a global model instead of directly assessing the private data from the clients. Further, the global model is sent back to clients, iterating the local training process. In the same token, FL proposed a variant of decentralised learning with higher efficiency. The key improvement lies in the way of updating the global model, specifically, DSSGD performs the aggregated update while the federated learning conducts the averaged update. Hence, DSSGD is more suitable for the commonly non-IID and unbalanced data distribution among clients in the real world.

Geyer and Klein [31] introduced a new idea to generate noise and added it into DSSGD. They require the users to terminate contributing data set during training and analyse the distributed model. In addition, they proposed an algorithm for differential privacy-preserving federated optimisation at the user terminal. Their method improved the privacy level via changing the original master generation into decentralised noise generation. However, their research ignores the convergence performance of SGD, which is, when they update the noise sample, the change could impact on all terminals. In detail, if the data size is very small on a certain platform, the convergence performance should be very slow, which makes that the output data can hardly be used.

In March of 2020, Huang and Su [32] have found a solution that if pruning a given layer of the neural network is equivalent to adding a certain amount of deferentially private noise to its hidden-layer activation. The hidden layer can be added in Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), which theoretically can draw a connection between neural network pruning and differential privacy. In their work [32], the noise has been analysed via the concentration results among the central tools such as the Chernoff bound and Hoeffding's inequality. In addition, following from classical random Gaussian, they connected ‘1-sensitivity with neural network layers noise in folded Gaussian zone. At last, they measured and tested the privacy leakage under attack, and obtained an acceptable result. Despite no obvious problem from their work, they can further improve attack and defense work with more Generative adversarial network tests to refine the result.

III. Our Vision on ppFL-AidLife System

According to the above technological advancements and the challenges identified for disaster communications, our vision is to develop a buses-and-drones based mobile edge infrastructure that is movable to effectively and efficiently

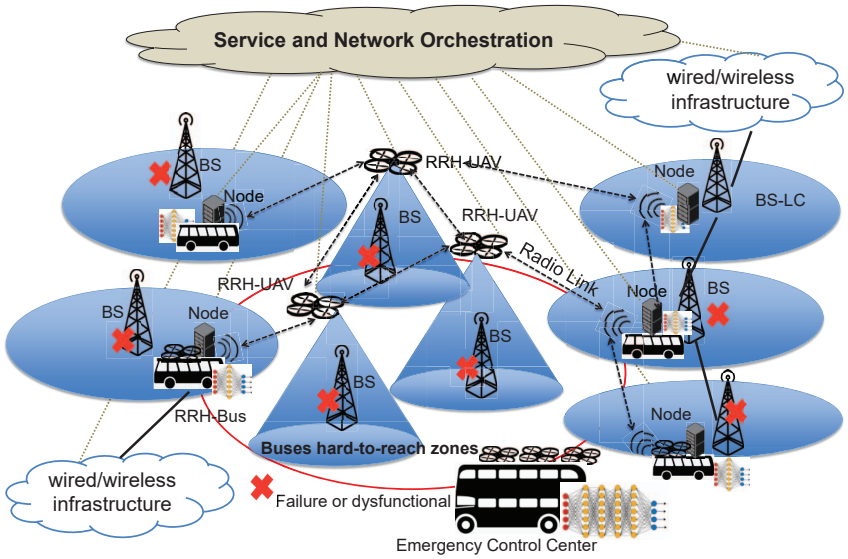

Fig. 1: Vision of the privacy-preserving federated learning embedded buses-and-drones mobile edge infrastructure (ppFL-AidLife) for disaster and emergency communications. (BS= Base Station LC = Large Cell, RRH = Remote Radio Head, UAV = Unmanned Aerial Vehicle, NODE = Reconfigurable network element that can be functioned as micro edge/cloud data-center, Baseband Unit (BBU), SDN switch)

support a wide range of communications and computations e.g., ML/FML services, also with a privacy-preservation manner. Fig. 1 shows the proposed ppFL-AidLife architecture for a large- scale 'hard' disaster or 'soft' pandemic scenario. Specifically, for the disaster/infected region, the coverage and connectivity could be provided by using remote radio head (RRH) mounted on top of the UAVs and buses i.e., RRH-UAV and RRH-Bus according to the various coverage scales and reliable communications requirements. Each RRH-UAV establishes connections with the other RRH-UAVs flying in the same zone. Moreover, the RRH-UAV could establish a radio connection with the baseband unit (BBU) mounted in nodes hosted by the buses for edge computing, storage, and data processing. The challenge here is to develop efficient solutions to reduce the amount of information exchanged between the RRH-UAV and the buses-Node, and also the data privacy-preservation. Notice that the UAV can be recharged by the power resources e.g., petrol-fed power generator or batteries located in the buses (which have sufficient physical space and can also carry heavy loads). If needed, the UAVs can continuously fly in the atmosphere in order to provide basic coverage, contact, and emergency services including information gathering and broadcasting, otherwise, they can fly back to the buses for recharging and/or waiting for next missions.

As the second alternative to provide wireless access connectivity in disasters or pandemics, the exploitation of BS Large Cells (LCs) is needed which can enable coverage radius in the order of 50 km. Such cells can be spread in those areas where the users' requirements are low in terms of bandwidth and delay. LCs could be powered by Solar Panels (SPs) and/or petrol-fed power generators carried by buses since the power grid is assumed to be not present or to be unreliable or non-accessible in the case of a large- scale disaster or pandemic. In an optimistic case, there might be still some terrestrial BSs working or accessible, then the buses-and-drones federated edge infrastructure can be further connected to the global infrastructure through these still-working and accessible BSs. Otherwise, it can at least provide regional communications and computation services just for local activities. Furthermore, we foresee the technical exploration of low-cost, low-power, and portable network components (i.e., the reconfigurable nodes introduced in Fig. 1, which are shown in Fig. 1 as the Nodes). Such portable devices can virtualize the different functionalities, which include the radio, computation, data mining, and machine learning, communications and caching, etc. Each functionality can be enabled or disabled according to where the node is located in infrastructure. Finally, the ppFL-AidLife infrastructure needs to be controlled by a centralized orchestrator i.e., the head of the federated edge system, which can holistically manage and optimize the networking, computing, data mining, and machine learning, communications and caching resources. For example, when high data rate video streaming and processing are needed in the rescue scene, the computing and caching resources could be allocated into the Nodes close to the users. At the same time, the coordination of UAVs, Buses, and BS LCs, as well as the coordination to decrease/increase their coverage could be done according to the users' density and the way their needs change over time learned and predicted through historical data. Additionally, the orchestrator needs to optimize the resource allocations by also considering the variation of power available from the UAVs, Nodes, and Buses.

IV. Conclusion and Future Works

We have focused on discussions in providing privacy-preserving emergence communications and computing (e.g., ML) services during the 'hard' (such as earthquakes) disasters and 'soft' (such as COVID-19) pandemics. After a deep dive into a current state-of-the-art, we have considered the main challenges that need to be faced for full exploitation of 5G UAVs-assisted mobile edge communications, networking, and privacy-preserving FML areas. In order to achieve this goal, we have discussed a number of architectural features, including the adoption of a buses-and-drones flexible infrastructure forming solution through the instant reusability of public bus systems. Moreover, more efficient privacy protection FL with a trade-off between privacy protection level and data utility for learning, thus a reference ppFL-AidLife architecture. For future, we may have a number of research activities, especially plan to validate and numerically analyse the proposed architecture in terms of its performance on privacy protection, learning accuracy, communications and computing latency and its scalability to accommodate massive users and/or more complex multimedia data demands, at scale.

References

[1] E. Yulianto, P. Utari, and I. A. Satyawan, "Communication technology support in disaster-prone areas: Case study of earthquake, tsunami and liquefaction in palu, indonesia," *International Journal of Disaster Risk Reduction*, p. 101457, 2020.

[2] D. S. W. Ting, L. Carin, V. Dzau, and T. Y. Wong, "Digital technology and covid-19," *Nature Medicine*, vol. 26, no. 4, pp. 459–461, 2020.

[3] M. Narang, W. Liu, J. Gutierrez, and L. Chiaraviglio, "A cyber physical buses-and-drones mobile edge infrastructure for large scale disaster emergency communications," in *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*. IEEE, 2017, pp. 53–60.

[4] M. Narang, S. Xiang, W. Liu, J. Gutierrez, L. Chiaraviglio, A. Sathiaseelan, and A. Merwaday, "Uav-assisted edge infrastructure for challenged networks," in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2017, pp. 60–65.

[5] S. Kiyomoto, K. Fukushima, and Y. Miyake, "Security issues on it systems during disasters: a survey," *Journal of Ambient Intelligence and Humanized Computing*, vol. 5, no. 2, pp. 173–185, 2014.

[6] E. Vattapparamban, İ. Güvenç, A. İ. Yurekli, K. Akkaya, and S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2016, pp. 216–221.

[7] J. Sakuma and S. Kobayashi, "Large-scale k-means clustering with user-centric privacy-preservation," *Knowledge and Information Systems*, vol. 25, no. 2, pp. 253–279, 2010.

[8] A. Shabtai, Y. Elovici, and L. Rokach, *A survey of data leakage detection and prevention solutions*. Springer Science & Business Media, 2012.

[9] S. Alneyadi, E. Sithirasenan, and V. Muthukkumarasamy, "A survey on data leakage prevention systems," *Journal of Network and Computer Applications*, vol. 62, pp. 137–152, 2016.

[10] M. Sokolova, K. El Emam, S. Rose, S. Chowdhury, E. Neri, E. Jonker, and L. Peyton, "Personal health information leak prevention in heterogeneous texts," in *Proceedings of the Workshop on Adaptation of Language Resources and Technology to New Domains*, 2009, pp. 58–69.

[11] A. Wahlen, L. Nahum, D. Gabriel, and A. Schnider, "Fake or fantasy: rapid dissociation between strategic content monitoring and reality filtering in human memory," *Cerebral Cortex*, vol. 21, no. 11, pp. 2589–2598, 2011.

[12] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. M. Begovic, and A. Phadke, "Wide-area monitoring, protection, and control of future electric power networks," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 80–93, 2010.

[13] C. C. Aggarwal and S. Y. Philip, "A general survey of privacy-preserving data mining models and algorithms," in *Privacy-preserving data mining*. Springer, 2008, pp. 11–52.

[14] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," 1998.

[15] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, "Incognito: Efficient full-domain k-anonymity," in *Proceedings of the 2005 ACM SIGMOD international conference on Management of data*, 2005, pp. 49–60.

[16] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 1, no. 1, pp. 3–es, 2007.

[17] Q. Wang and X. Shi, "(a, d)-diversity: Privacy protection based on l-diversity," in *2009 WRI World Congress on Software Engineering*, vol. 3. IEEE, 2009, pp. 367–372.

[18] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *2007 IEEE 23rd International Conference on Data Engineering*. IEEE, 2007, pp. 106–115.

[19] C. Dwork, "Differential privacy: A survey of results," in *International conference on theory and applications of models of computation*. Springer, 2008, pp. 1–19.

[20] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*. IEEE, 2007, pp. 94–103.

[21] R. Rajalaxmi and A. Natarajan, "A novel sanitization approach for privacy preserving utility itemset mining." *Computer and Information Science*, vol. 1, no. 3, pp. 77–82, 2008.

[22] J. Konečnỳ, B. McMahan, and D. Ramage, "Federated optimization: Distributed optimization beyond the datacenter," *arXiv preprint arXiv:1511.03575*, 2015.

[23] Y. Hu, D. Niu, J. Yang, and S. Zhou, "Fdml: A collaborative machine learning framework for distributed features," in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2019, pp. 2232–2240.

[24] M. Hardt and G. N. Rothblum, "A multiplicative weights mechanism for privacy-preserving data analysis," in *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*. IEEE, 2010, pp. 61–70.

[25] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*. IEEE, 2013, pp. 429–438.

[26] L. Bottou, "Large-scale machine learning with stochastic gradient descent," in *Proceedings of COMPSTAT'2010*. Springer, 2010, pp. 177–186.

[27] L. Bottou and O. Bousquet, "The tradeoffs of large scale learning," in *Advances in neural information processing systems*, 2008, pp. 161–168.

[28] M. A. Rahman, T. Rahman, R. Laganière, N. Mohammed, and Y. Wang, "Membership inference attack against differentially private deep learning model." *Transactions on Data Privacy*, vol. 11, no. 1, pp. 61–79, 2018.

[29] J. Konečnỳ, B. McMahan, and D. Ramage, "Federated optimization: Distributed optimization beyond the datacenter," *arXiv preprint arXiv:1511.03575*, 2015.

[30] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, 2015, pp. 1310–1321.

[31] R. C. Geyer, T. Klein, and M. Nabi, "Differentially private federated learning: A client level perspective," *arXiv preprint arXiv:1712.07557*, 2017.

[32] Y. Huang, Y. Su, S. Ravi, Z. Song, S. Arora, and K. Li, "Privacy-preserving learning via deep net pruning," *arXiv preprint arXiv:2003.01876*, 2020.