Chapter 6
Future Research Directions

From Chaps. 2–5, we have shown the existing research status of machine learning driven privacy preservation in IoTs, especially focus on three leading directions using GAN, federated learning, and reinforcement learning. Several advanced technologies and theories are also integrated, for example, differential privacy, game theory, blockchain, etc. Nevertheless, there are still plenty of significant and prospective issues worthy investigating. The popularization of blockchain, digital twin, and artificial intelligence offers a mass of opportunities for researches on machine learning driven privacy preservation in IoTs, but meanwhile they raise new challenges such as unsatisfying data utility and limited communication and computing resources. In addition, there are various other research topics that desiderata consideration in machine learning driven privacy preservation in IoTs. To pave the way for readers and forthcoming researchers, we outline several potentially promising research directions that may be worthy of future efforts.

6.1 Trade-Off Optimization in IoTs

Trade-off between privacy protection and data utility has always been one of the primary targets in privacy preservation field. The reason is as explained above. In privacy preservation domain, data curators will publish sanitized data to all data requestors by conducting irreversible data distortion in most cases. In this case, data utility should be well-considered for the value of the sanitized data.

However, most existing research barely considers limited computing and communication resources, which should be taken into account in IoT scenarios. That makes the trade-off optimization even more complicated. Currently, there are two potential solutions, including both a static model and a dynamic model.

For the static solution, it requires that the designer is experienced in this domain and thereby can identify the issues in each procedure. By deeply understanding such

Y. Qu et al., *Privacy Preservation in IoT: Machine Learning Approaches*,
SpringerBriefs in Computer Science, https://doi.org/10.1007/978-981-19-1797-4_6

a system, an expert may be able to design a novel loss function that can help improve the performance of the machine learning based privacy preservation models and achieve fast convergence under the constrain of limited computing and communication resources. Although the design of a loss function can improve the overall performance, but it is usually case-by-case and can hardly be generalized.

A dynamic solution is usually in a form of a iterated algorithm, for instance, a machine learning algorithm or a game theory based model. The optimization process can be formulated as a Markov Decision Process. To achieve this, all parties' actions, states, and corresponding payoff functions should be modelled. In this case, the payoff function can be modelled as the trade-off between privacy protection, data utility, and resource limitations. The Markov Decision Process can be solved using various ways, such as Q-learning algorithm or state-action-reward-state-action (SARSA) algorithm. However, the adoption of dynamic solutions may bring about extra burden on computing and communication resources. Therefore, the efficiency improvement is also worth further investigating.

6.2 Privacy Preservation in Digital Twined IoTs

Digital twin is a fast emerging technology in recent years. Originated from manufacture industries, digital twin has proved its effectiveness when designing and improving specific physical objects and their interactions. This create opportunities to IoTs as well. In an IoT network, there are various IoT devices such as sensors, cameras, edge devices, vehicles, etc. It is possible to create digital twins for IoT devices in a cloud server to simulate an IoT environment, which has been evidenced in a mass of existing research.

The establishment of digital twined IoT enables the optimization of execution policies of IoT devices, communication efficiency, and a lot more. However, privacy issues emerge since local data of IoT devices should be uploaded to the digital twin. Besides, the digital twins are always located in a server with high computing, communication, and storage devices, such as a cloud server. This poses further challenges to privacy protection due to the existence of multiple attacks like man-in-the-middle attacks.

To preserve the privacy in this case, it is possible to perform federated meta learning. Meta-learning, or learning to learn, is the science of systematically observing how different machine learning approaches perform on a wide range of learning tasks, and then learning from this experience, or meta-data, to learn new tasks much faster than otherwise possible. As is known to all, federated learning is able to achieve privacy-preserving distributed machine learning by exchanging the model parameters or gradients of a commonly-maintained model. By storing local data locally, privacy protection is achieved. However, federated learning meets several bottlenecks, of which a primary challenge is to improve the model performance. Therefore, meta learning can be accommodated in federated learning such that the performance and privacy protection can be balanced. Similar the other IoT scenarios, the adoption of machine learning models result in the consumption of computing and communication resources, which should be considered while establishing such a model.

6.3 Personalized Consensus and Incentive Mechanisms for Blockchain-Enabled Federated Learning in IoTs

6.4 Privacy-Preserving Federated Learning in IoTs

Consensus algorithm for B-FL: The consensus algorithm is the core of any blockchain system, and an ideal consensus algorithm should be computationally efficient and highly secure. PoW and PoS are the two most widely used consensus algorithms but the former is extremely inefficient and costly due to the use of a nonce-finding mechanism, while the later will weaken the decentralization property of blockchain as the miners with a huge number of stakes can dominate the blockchain system. To overcome these drawbacks, we propose to directly use the B-FL mission as a consensus proof, without running a separate consensus proof process nor utilising the miners' stakes as a consensus proof.

Based on the proposed B-FL process above, we will develop the new consensus algorithm in the following way. In Phase 1, each participating miner uses their local data to train a local model. Once completing the local model training, they will broadcast the local model parameters to other participating miners. When a predefined percentage of miners have completed their local model training or a predefined time length is reached, Phase 1 ends. All the miners who have successfully completed their work are eligible for participating in Phase 2 and those miners who did not complete Phase 1 will be excluded from being involved in the next phase. In Phase 2, each miner eligible for this phase will execute a smart contract containing a model verification algorithm and a model selection algorithm to verify the authenticity of all local models and select those authentic local models suitable for aggregation. Phase 2 will finish once a predefined percentage of miners have completed their work or a predefined time length is reached. The miners whose local models have been selected for aggregation will proceed to Phase 3 and those whose local models are classified as falsified or unsuitable for aggregation will be excluded from participating in the next phase. In Phase 3, each miner eligible for this phase will execute a smart contract containing a model aggregation algorithm to aggregate the selected local models to generate their global model. Then the miner will store the generated global model parameters into a candidate block and broadcast it to the blockchain system. When a predefined percentage of miners have completed their work or a predefined time length is reached, each miner eligible for this phase will vote for a (different) global model whose model parameters are the closest to their own. If two or more models have the same closeness to their own, the one that was generated the earliest will be chosen. After a predefined time period, the global model receiving the highest number of votes is elected as the final global model in that B-FL round. The associated miner is recognised as the winning miner of that B-FL round and the associated candidate block is formally appended on the blockchain system, which ends the consensus process. As an inherent part of the consensus algorithm development, we will analyse the robustness of the proposed consensus algorithm against attacks and study how the algorithmic parameters, such as those predefined percentages of miners and predefined time lengths, will affect its performance. Based on the findings, we will refine the proposed consensus algorithm accordingly.

Incentive algorithm for B-FL: The ultimate objective of B-FL is to motivate miners to actively participate in the B-FL process to collectively produce high-quality models within the shortest possible timeframe. The incentive mechanisms used in traditional blockchain systems are not suitable for B-FL as they only award the winning miner. Intuitively, it is better to devise a personalized incentive algorithm to award all the miners who have made valuable contributions to B-FL. The proposed awarding principles are as follows. Firstly, in each B-FL round, every miner whose local model was selected for aggregation will be awarded and the award amount depends on the quality of the model (the higher quality the better) and the time spending on training the model (the shorter time the better). This awarding principle is reasonable as producing a high-quality local model in a short timeframe requires the miner to use more high-quality data and computing power to train their local model in Phase 1 and use more computing power to perform local model verification and selection in Phase 2. Secondly, the miners who participated in the whole Phase 3 to determine the final global model and the winning miner will receive an additional award. Thirdly, the winning miner will receive a further top-up award. In addition to these awarding principles, certain constraints should be imposed to avoid the over-fitting issue when determining the award amount since over-fitting will weaken the extensiveness to diverse data from different miners. Based on the proposed awarding principles and constraints, an award mapping algorithm will be proposed to map the miners' contributions to the actual rewards to be allocated. We will also investigate how to optimize the award mapping algorithm by considering its impact on model accuracy, model training convergence speed, miner participation rate, etc.

6.5 Federated Generative Adversarial Network in IoTs

In this section, we discuss our plan on federated generative adversarial network for IoT applications in practice.

The basic idea is that a central server, usually a cloud server or a edge server, servers as the Discriminator. At the same time, each IoT end device works as a Generator and generates synthetic data using its local data. The synthetic data is then uploaded to the central server for discrimination. As the central server has a full vision of all generated synthetic data, it can perform discrimination in a powerful way. Then all the local Generators game with a central Discriminator iteratively until convergence.

The difficult part of this model includes the high communication overhead since the synthetic data should be uploaded to the central server. Besides, the synthetic data may leak privacy information during transmission.

Therefore, another potential solutions is that each IoT device trains a GAN model locally and send the GAN model parameters to a central server for aggregation. This can significantly reduce the communication overhead but requires certain degree of computation resources of IoT devices.

Therefore, there should be a trade-off between these two methods. That is also part of our research plan in the future.