Chapter 9

Related Work

Privacy-preserving machine learning is not a novel concept. A number of proposals exist that combine decision tree based classification of private data in a multi-party setting (e.g. [23, 47, 24]). One possible approach is to leverage homomorphic encryption schemes [4, 69]. Another approach is the use of Differential Privacy (DP), as introduced by Dwork et al. [29]. It can be argued, that this is the only mathematically rigorous definition of privacy in the context of machine learning and big data analysis. Through extensive research and growing industry acceptance, DP has become the standard of privacy over the past decade [6]. Multiple DP-GBDT solutions [45, 1, 48, 68] have been proposed since then. The combination of DP-GBDT with SGX enclaves has not been as thoroughly researched however. To our knowledge, there are two works that take a relatively similar approach to this thesis:

Allen et al. (2019) "*An Algorithmic Framework For Differentially Private Data Analysis on Trusted Processors*" [6]. Their high-level goal and architecture are the same as ours: Run DP algorithms inside SGX enclaves and eliminate leakage. Specifically, this work proposes a mathematical model for designing DP algorithms in TEE-based setting. They assume that the leakage only consists of (i) the output model and (ii) memory access trace. In this setting they ensure that DP guarantees hold for three selected algorithms. Decision trees are not among them. Further their focus lies more on the algorithmic side, which means they don't consider an entire system with data provisioning from users, disk as persistent storage, and so on.

Law et al. (2020) "*Secure collaborative training and inference for XGBoost*" [44]. The authors present a privacy-preserving system for multiparty training and inference of XGBoost [18] (efficient, open-source GBDT library) models. Their goal is to protect the privacy of each party's data as well as the integrity of the computation with SGX enclaves. However, they only consider side-channel leakage through memory access patterns. For this purpose, multiple data-oblivious building blocks for GBDT are created. Another difference to our approach is that no DP mechanisms are used. In other words, they aim for complete obliviousness of the entire algorithm, while we only selectively harden certain areas to achieve DP.