Strong aspects:

Authors first identify three challenges in large-scale PPTD over data streams, among which efficiency decrease caused by growing size of participating workers is the focus of this paper.

To improve efficiency against growing number of workers, authors states that dividing workers into multiple communities is an efficient, however, insecure way. To tackle the efficiency and privacy conflicts, authors propose an improved data aggregation scheme based on double masking technique with the help of fog nodes, called SecAgg. It requires each fog node to perform an extra "Re-masking" round. On the one hand, this scheme can support any grouping strategy and groups of arbitrary sizes so that each worker is supposed to maintain a connection with only his neighbors which can greatly reduce the computational overheads caused by generating masks and secret sharing and communication overheads caused by distributing the shares. On the other hand, the improved data aggregation scheme achieves the same privacy level as original double masking technique. Based on the SecAgg, authors construct the FPTD from the improved data aggregation scheme which gains good efficiency improvement. Finally, authors design and execute detailed experiments to prove the efficiency improvement. The logic and structure of the paper is clear and easy to understand. Experiments and analysis are clear and convincing.

Weak aspects:

First, the proposed data aggregation scheme adds an extra round called "Re-masking", which may potentially cause longer waiting time for each worker and thus, bigger probability of dropouts. Second, the FPTD constructed from the improved data aggregation scheme ensures the privacy of weights of each worker by letting each worker hold his own weights. Though authors assume workers to be honest to avoid the problem, there may exist workers who tend to modify their weights to obtain more incentives. Such existence of malicious workers raises trust concerns. Moreover, the security analysis is rough and informal. The security analysis consists mainly of statements instead of formal proof. In addition, correction of spelling and grammar mistakes is needed. Finally, the paper contains some misuse of symbols.

Recommended changes:

Correction of spelling and grammar mistakes is needed. In section II, more related works should be included. In section III.A, authors should give detailed rules of the symbols.