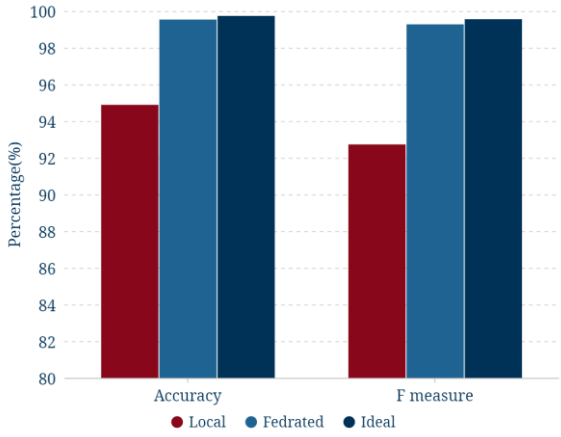
Blockchain based Federated Learning for Intrusion Detection for Internet of Things

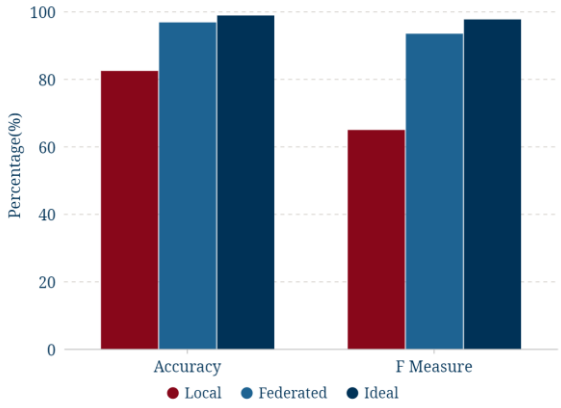
Nan SUN , Wei WANG, Yongxin TONG, Kexin LIU

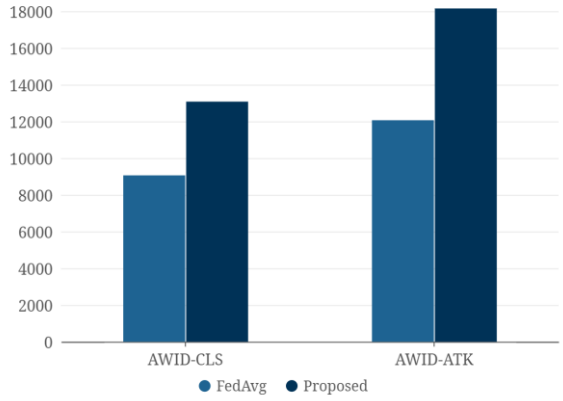
Frontiers of Computer Science, DOI: 10.1007/s11704-023-3026-8

Problems & Ideas

- Problems of conventional intrusion detection approaches:
  - Data privacy and security need to be protected during the training process.
  - Existing algorithms inadequately address the fine-grained classification of unknown attack types.
- Ideas: A blockchain based federated intrusion detection architecture utilizing the information contained in the labeled data as the prior knowledge to discover new attack types



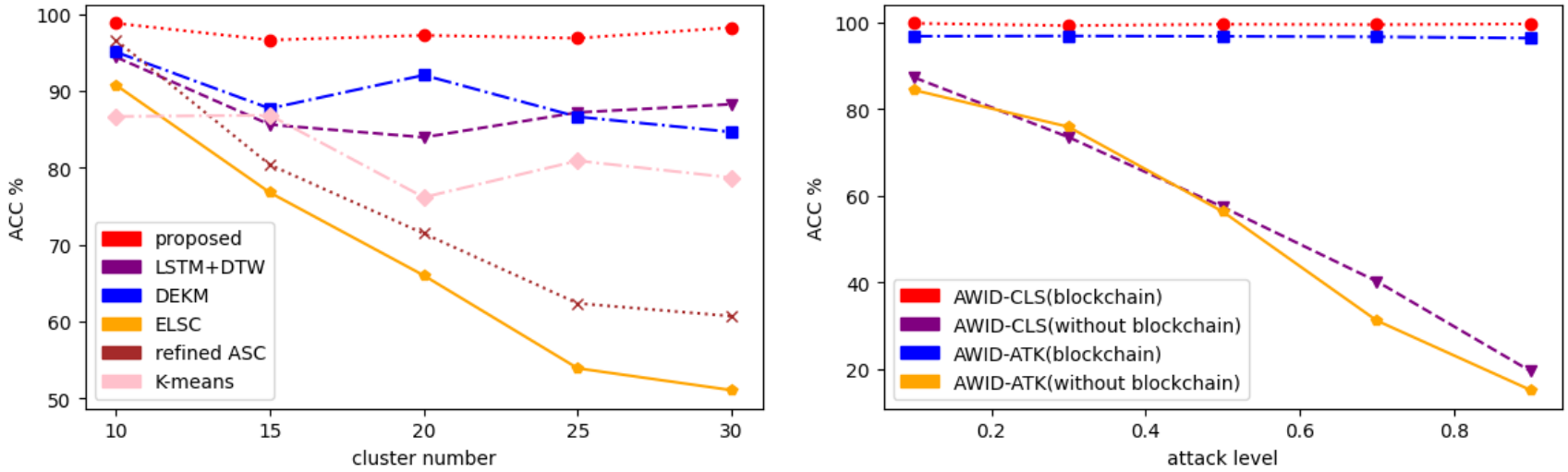




Comparison results using different training manners. Left: Accuracy and F measure of AWID-CLS dataset; Middle: Accuracy and F measure of AWID-ATK dataset; Right: Running time of different datasets under the proposed and FedAvg algorithms.

Main Contributions

- Contributions:
  - The blockchain technique is introduced in the training architecture to ensure secure and distributed coordination of federated training;
  - A collaborative model parameters verification mechanism and proof-of-stake consensus mechanism are adopted in the training process, excluding malicious entities from the training process;
  - An end-to-end clustering algorithm is employed in each entity to distinguish different attack types, by adopting the spatial-temporal features dissimilarity of data set.



Comparison results of AWID dataset. Left: ACC of different algorithms for AWID-ATK dataset under different cluster number; Right: ACC for dataset with and without blockchain under different attack level.