**CONCLUSION**

This paper proposed a novel two-stage ensemble deep learning-based attack detection and attack attribution frame-work for imbalanced ICS data. The attack detection stage uses deep representation learning to map the samples to the new higher dimensional space and applies a DT to detect the attack samples. This stage is robust to imbalanced datasets and capable of detecting previously unseen attacks. The attack attribution stage is an ensemble of several one-vs-all classifiers, each trained on a specific attack attribute. The entire model forms a complex DNN with a partially connected and fully connected component that can accurately attribute cyber-attacks, as demonstrated. Which are similar to those of other DNN-based techniques in the literature. Moreover, the proposed framework can detect and attribute the samples timely with a better recall and f-measure than previous works.