# CONCLUSION

The ability to protect SCADA-based IIOT networks against cyber attacks increases their trustworthiness. The existing security methods along with machine learning algorithms were inefficient and inaccurate for protecting IIOT networks. In this article, we proposed a cyber attacks detection mechanism using enhanced deep and ensemble learning in a SCADA-based IIOT network. The proposed mechanism is reliable and accurate because an ensemble detection model was built using a combination of the PRU and the DT. The proposed method was evaluated across 15 datasets generated from a SCADA-based network, and a considerable increase in terms of classification accuracy was obtained. Compared to state-of-the-art techniques, the obtained outcomes of our method exhibited a good balance between reliability, trustworthiness, classification accuracy, and model complexity, resulting in improved performance.

In the future, we will employ more powerful deep learning models to further improve trustworthiness by detecting cyber attacks accurately. In addition, we will try to formulate and assess its performance in real-world scenarios. Also, we will work on the selection of optimal features in scenarios when the features are not sufficient.