Secure IIoT-enabled industry 4.0

ABSTRACT

The Industrial Internet of things (IIoT) is the main driving force behind smart manufacturing, industrial automation, and industry 4.0. Conversely, industrial IoT as the evolving technological paradigm is also becoming a compelling target for cyber adversaries. Particularly, advanced persistent threats (APT) and especially botnets are the foremost promising and potential attacks that may throw the complete industrial IoT network into chaos. IIoT-enabled botnets are highly scalable, technologically diverse, and highly resilient to classical and conventional detection mechanisms. Subsequently, we propose a deep learning (DL)-enabled novel hybrid architecture that can efficiently and timely tackle distributed, multivariant, lethal botnet attacks in industrial IoT. The proposed approach is thoroughly evaluated on a current state-of-the-art, publicly available dataset using standard performance evaluation metrics. Moreover, our proposed technique has been precisely verified with our constructed hybrid DL-enabled architectures and current benchmark DL algorithms. Our devised mechanism shows promising results in terms of high detection accuracy with a trivial trade-off in speed efficiency, assuring the proposed scheme as an optimal and legitimate cyber defense in prevalent IIoTs. Besides, we have cross-validated our results to show utterly unbiased performance