**ABSTRACT**

We like to have simple and automated solutions, but these simple and automated solutions in technology could also contains risks if not deal properly. Due to no international standard of compatibility for IoT, security and privacy concerns are there which needs to be focus. There can be multiple types of attack on IoT networks which can damage the device or steal the sensitive information. Therefore, artificial intelligence (AI) techniques has an ability to detect and classify an unknown network behaviour by learning the network attacks patterns based on large volumes of historical data. We considered Aposemat IoT-23 which is a labelled dataset and created in the Avast laboratory. Basically, the goal of this large dataset is to provide labelled and real IoT attacks. In this paper, we used this dataset, considered the relevant workings, investigate the background and implement the machine learning algorithms such as Decision Tree, Random Forest and Naive Bayes. We also compared the accuracy among these machine learning algorithms on the IoT-23 dataset and showed the most efficient machine learning algorithm is Random Forest as per results by using Aposemat IoT-23 dataset, as well as showed feature engineering techniques to preprocess the mentioned dataset for detection and classification of IoT network attacks.