World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:16, No:11, 2022

ANOVA-Based Feature Selection and Machine Learning System for IoT Anomaly Detection

Authors : Muhammad Ali

Abstract : Cyber-attacks and anomaly detection on the Internet of Things (IoT) infrastructure is emerging concern in the domain of data-driven intrusion. Rapidly increasing IoT risk is now making headlines around the world. denial of service, malicious control, data type probing, malicious operation, DDos, scan, spying, and wrong setup are attacks and anomalies that can affect an IoT system failure. Everyone talks about cyber security, connectivity, smart devices, and real-time data extraction. IoT devices expose a wide variety of new cyber security attack vectors in network traffic. For further than IoT development, and mainly for smart and IoT applications, there is a necessity for intelligent processing and analysis of data. So, our approach is too secure. We train several machine learning models that have been compared to accurately predicting attacks and anomalies on IoT systems, considering IoT applications, with ANOVA-based feature selection with fewer prediction models to evaluate network traffic to help prevent IoT devices. The machine learning (ML) algorithms that have been used here are KNN, SVM, NB, D.T., and R.F., with the most satisfactory test accuracy with fast detection. The evaluation of ML metrics includes precision, recall, F1 score, FPR, NPV, G.M., MCC, and AUC & ROC. The Random Forest algorithm achieved the best results with less prediction time, with an accuracy of 99.98%.

Keywords : machine learning, analysis of variance, Internet of Thing, network security, intrusion detection
Conference Title : ICMIML 2022 : International Conference on Machine Intelligence and Machine Learning
Conference Location : Amsterdam, Netherlands
Conference Dates : November 03-04, 2022