Paper No: SC-19 **Smart Computing**

Detection of IoT Malware Based on Forensic Analysis of Network Traffic Features

Nisais Nimalasingam*
Department of Industrial Management
University of Kelaniya, Sri Lanka
nisaisn_im16051@stu.kln.ac.lk

Janaka Senanayake
Department of Industrial Management
University of Kelaniya, Sri Lanka
janakas@kln.ac.lk

Chathura Rajapakse
Department of Industrial Management
University of Kelaniya, Sri Lanka
chathura@kln.ac.lk

***Abstract* - The usage of Internet of Things (IoT) devices is getting unavoidable lately, from handheld devices to factory automated machines and even IoT embedded automotive vehicles. On average, 100+ devices are connected to the IoT world per second, and the volume of data generated by these devices and added to the space is just too enormous. The value of the data costs more, and sometimes it is invaluable, and it maypull over the cybercriminals and eventually increases the number of cybercrimes. Therefore, the need to identify malwarein IoT is a timely requirement. This research work applies Machine Learning (ML) models and yields an efficient lead to identifying the IoT malware using forensic analysis of their network traffic features by selecting the foremost unique features and combining them with the binary features of the malware families. An outsized dataset with many network traffic collections used various network traffic features. Thus, the proposed model's detection accuracy of almost 100% was achieved from the model during the experimental phase of the study, which was a result of the feature extraction process for each malware type. This model can be further improved by considering the fog level implementation of the IoT layer, wherethe learning will help identify a malicious packet transfer to thenetwork at level zero.**

Keywords - feature selection, forensic analysis, IoT Malware,IoT network traffic, Machine Learning