An interaction index based Deep Learning framework for predictive and preventive measures for IoTs

This era has vision an explosive growth of devices, a digital world where people, objects and machines are interacting with one another, controlled by internet. This rendezvous of physical and virtual world, termed as Internet of things, has led to efficiency improvements, economic growth and less human exertions. IoT devices increased by 31 % every year to 8.4 billion by year 2017 and there should be around 30 billion devices used by the current year 2020 with global market value of $7.1 trillion. Despite of their wide deployment, Due to the complexity of design and implementation in both hardware and software, as well as the lack of security functions and abilities, IoT devices are becoming an attractive target for cyber criminals who take advantage of weak authentication, outdated firmwares, and malwares to compromise IoT devices.

We proposed an interaction index framework based on deep learning for predictive analysis. Our framework will help the data scientists to analyze data. This framework will be based on machine learning techniques and libraries to analyze data on multiple techniques with less technical skills. When the data is processed by framework, the application will display an eye-friendly interface in which data scientists can instinctively see the patterns and trends of the data to take notes for any predictions and prior to any disaster, the respective preventive measures can be taken.

**Problem Statement**

“The case where an application lies about its intention for requesting a permission or intentionally violates the user's expectation of an applications behavior is not so well researched.” [ref: Jemal, Identifying cyber threats to mobile-IoT applications in edge computing paradigm]

* **Research Proposal**
  + Our research is to find a predictive malware detection technique based upon an interaction index between permissions used and invasions found

**Applications / Motivation**

* First Application
  + Research Area: Intrusion Detection
  + Applications: Smart City / Smart Home
  + Example: Someone tries to enter home / a gated community / a city when it wasn’t allowed to enter
* Second Example
  + Research Area: Malware Detection
  + Applications: Mobile Sensors IoT
  + Details: The malware has become an increasing problem for Mobile-Internet of Things applications in edge computing platform. Variants of malware can be identified once their general characteristics are known and overtly malicious behavior can be identified.
  + Example:

**Related Work**

* First Related Work
  + Author: Jemal
  + Title: Identifying cyber threats to mobile-IoT applications in edge computing paradigm
  + Details:

We particularly focus on a greater set of permissions which may be leveraged for other purposes, for example by using sensors to record user credentials or monitoring a user's movements. This research will attempt to identify such scenarios by employing behavioral analysis to determine when and how permissions are used.

They also perform static and dynamic analysis to predict the behavior of application logic yet to execute.

They have described various techniques of intrusion detection such as signature based, anomaly based, behavior based etc. Methods for implementing these techniques include neural networks, data mining etc

* Second Related Work
  + Author: Somya
  + Title: Methods and Techniques of Intrusion Detection: A Review