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

**Nomica Choudhry**

nomica@yahoo.com

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abilities, IoT devices are becoming an attractive target for cyber criminals who take advantage of weak authentication, outdated firmware, and malwares to compromise IoT devices.

1. INTRODUCTION
   1. Background
      1. Activation Protocol

Activation functions are important for a Artificial Neural Network to learn and understand the complex patterns. The main function of it is to introduce non-linear properties into the network. What it does is, it calculates the ‘weighted sum’ and adds direction and decides whether to ‘fire’ a particular neuron or not. There are several kinds of non-linear activation functions, like Sigmoid, Tanh, ReLU and leaky ReLU.

The sigmoid function is an activation function where it scales the values between 0 and 1 by applying a threshold. [ref: <https://analyticsindiamag.com/most-common-activation-functions-in-neural-networks-and-rationale-behind-it/>]

* + 1. General Protocols to for predictive analysis and preemptive analysis
    2. Research Specific Protocols using NN for predictive analysis and preemptive analysis
  1. Research Issues
     1. Issue 1
     2. Issue 2
  2. Research Problem, Motivation and Objective
     1. 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]

* + 1. Motivation
       1. Why are we researching a security protocol?
       2. Why are we researching an AI based security protocol?
       3. Why are we researching a regression protocol?
    2. Research Objective

The purpose of this research is to find a predictive malware detection technique based upon an interaction index between permissions used and invasions found.

* + 1. Research Application
* 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 Application
  + 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:
  1. The Contributions

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.

* 1. Thesis Organization

1. SURVEY
   1. Overview of the Research in the field and Taxonomy
   2. Surveyed Research 1

Author: Jemal

Title: Identifying cyber threats to mobile-IoT applications in edge computing paradigm

* + 1. Brief Overview

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.

* + 1. Pros
    2. Cons
    3. Comparative Analysis with our work
  1. Surveyed Research 2

Author: Somya

Title: Methods and Techniques of Intrusion Detection: A Review

* + 1. Brief Overview
    2. Pros
    3. Cons
    4. Comparative Analysis with our work
  1. Surveyed Research 3
     1. Brief Overview
     2. Pros
     3. Cons
     4. Comparative Analysis with our work
  2. Summary of the Surveyed Research Work

1. SYSTEM MODEL & EVALUATION METRICS
   1. The scope of the Research

In this section, we describe the scope and limitations of the research.

* 1. Frequently Used Terms
  2. System Model
  3. Evaluation Metrics

Define terms like accuracy, error, convergence, correctness, etc.

* 1. Simulation Model
     1. Simulator Design Architecture
     2. System Parameters
     3. Simulation Settings and Desired Output

1. PROPOSED PROTOCOL
   1. Describe the Protocol
   2. Present the Pseudo Code of the Protocol
   3. Describe the State Diagram of the Protocol
   4. Describe the Activity Diagram of the Protocol
   5. Critically analyze the Protocol
      1. Pros
      2. Cons
      3. Future Work
2. SIMULATIONS & RESULTS
3. REFERENCES