**Toward Detection and Attribution of Cyber-Attacks in IoT-enabled Cyber-physical Systems**

**ABSTRACT:**

Securing Internet of Things (IoT)-enabled cyberphysical systems (CPS) can be challenging, as security solutions developed for general information / operational technology (IT / OT) systems may not be as effective in a CPS setting. Thus, this paper presents a two-level ensemble attack detection and attribution framework designed for CPS, and more specifically in an industrial control system (ICS). At the first level, a decision tree combined with a novel ensemble deep representationlearning model is developed for detecting attacks imbalanced ICS environments. At the second level, an ensemble deep neural network is designed for attack attribution. The proposed model is evaluated using real-world datasets in gas pipeline and water treatment system. Findings demonstrate that the proposed model outperforms other competing approaches with similar computational complexity.

**EXISTING SYSTEM:**

Internet of Things (IoT) devices are increasingly integrated in cyber-physical systems (CPS), including in critical infrastructure sectors such as dams and utility plants. In these settings, IoT devices (also referred to as Industrial IoT or IIoT) are often part of an Industrial Control System (ICS), tasked with the reliable operation of the infrastructure. ICS can be broadly defined to include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and systems that comprise programmable logic controllers (PLC) and Modbus protocols.

**Disadvantage:**

1. Less Security.

2. Less Accuracy.

**PROPOSED SYSTEM:**

the proposed framework. In this framework, the attack detection method detects the attacks by analyzing the ICS input features using the combination of ensembled unsupervised DNNs and a decision tree. If an attack is detected, the sample is passed to several DNNs for detailed analysis. If the attacks were previously unseen/unknown, the unseen attack detection module would detect it and label it as an unseen attack. This will be passed on for detailed security analysis. Otherwise, the attack attribution method detects the attribute of the attack.

**Advantage:**

1. More Security.

2. More Accuracy.

**SYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS:**

# Processor - Pentium –IV

* Speed - 1.1 GHz
* RAM - 256 MB(min)
* Hard Disk - 20 GB
* Key Board - Standard Windows Keyboard
* Mouse - Two or Three Button Mouse
* Monitor - SVGA

**SOFTWARE REQUIREMENTS:**

* Operating System - Windows7/8
* Programming Language - Python