**Detection of Cyber Attacks Using Artificial Intelligence**

**OJECTIVE:**

The primary goal of this project is to determine the cyber-attack whether there will be attack or not and to know this we have used the Support Vector , Decision Tree, Random forest, Extra Tree Classifier and ad boost and neural network classifier classification techniques.

**ABSTRACT:**

Cyber-physical systems(cps) have made significant progress in many dynamic applications due to the integration between physical processes, computational resources, and communication capabilities. However, cyber-attacks are a major threat to these systems. Unlike faults that occurs by accidents cyber-physical systems, cyber-attacks occur intelligently and stealthy. Some of these attacks which are called deception attacks, inject false data from sensors or controllers, and also by compromising with some cyber components, corrupt data, or enter misinformation into the system. If the system is unaware of the existence of these attacks, it won’t be able to detect them, and performance may be disrupted or disabled altogether. Therefore, it is necessary to adapt algorithms to identify these types of attacks in these systems. It should be noted that the data generated in these systems is produced in very large number, with so much variety, and high speed, so it is important to use machine learning algorithms to facilitate the analysis and evaluation of data and to identify hidden patterns. In this research, the CPS is modeled as a network of agents that move in union with each other, and one agent is considered as a leader, and the other agents are commanded by the leader. The proposed method in this study is to use the structure of deep neural networks for the detection phase, which should inform the system of the existence of the attack in the initial moments of the attack. The use of resilient control algorithms in the network to isolate the misbehave agent in the leader-follower mechanism has been investigated. In the presented control method, after the attack detection phase with the use of a deep neural network, the control system uses the reputation algorithm to isolate the misbehave agent. Experimental analysis shows us that deep learning algorithms can detect attacks with higher performance that usual methods and can make cyber security simpler, more proactive, less expensive and far more effective.

**Existing Method:**

In the existing system, implementation of machine learning algorithms is bit complex to build due to the lack of information about the data visualization. Mathematical calculations are used in existing system for model building this may takes the lot of time and complexity. To overcome all this, we use machine learning packages available in the scikit-learn library.

**Disadvantages:**

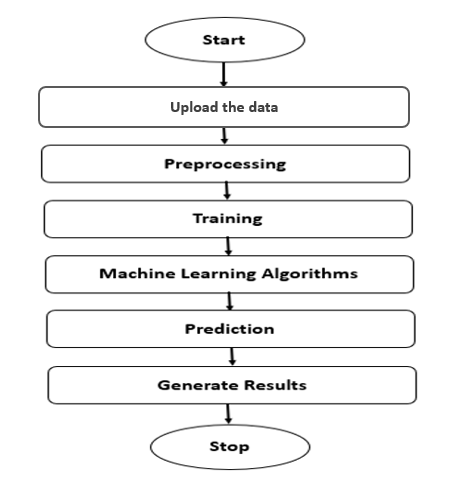
* High complexity.
* Time consuming.

**Proposed System:**

Proposed several machine learning models to classify whether there will be a cyber attack or not, but none have adequately addressed this misdiagnosis problem. Also, similar studies that have proposed models for evaluation of such performance classification mostly do not consider the heterogeneity and the size of the data Therefore, we propose a Support Vector , Decision Tree, Random forest, Extra Tree Classifier and ad boost and neural network classifier classification techniques.

**Advantages**:

* Highest accuracy
* Reduces time complexity.

**Block Diagram:**

**SOFTWARE AND HARDWARE REQUIREMENTS:**

**Hardware:**

Operating system : Windows 7 or 7+

RAM : 8 GB

Hard disc or SSD : More than 500 GB

Processor : Intel 3rd generation or high or Ryzen with 8 GB Ram

**Software:**

Software’s : Python 3.6 or high version

IDE : PyCharm.

Framework : Flask

**LEARNING OUTCOMES:**

* About Classification in machine learning.
* About pre-processing techniques.
* About ensemble algorithm.
* About flask framework.
* Knowledge on PyCharm Editor.