**SYSTEM ANALYSIS**

**Existing System**

Popular attack detection and attribution approaches include those based on signatures and anomalies. To mitigate the known limitations in both signature-based and anomaly-based detection and attribution approaches. There has been renewed interest in utilizing attack detection and attribution solutions based on Machine Learning (ML) or Deep Neural Networks (DNN) in recent times. Attack detection approaches can be categorized into network-based or host-based approaches. Supervised clustering, single-class or multi-class Support Vector Machine (SVM), fuzzy logic, Artificial Neural Network (ANN), and DNN are commonly used techniques for attack detection in network traffic.

**ADVANTAGES:**

1. These techniques analyze real-time traffic data to detect malicious attacks in a timely manner.

2. Hybrid based approaches are effective at detecting unusual activates, they are not reliable due to frequent network upgrades, resulting in different Intrusion Detection System (IDS).

**DISADVANTAGES**:

1. Attack detection that considers only network and host data may fail to detect sophisticated attacks or insider attacks.

2. The approach fails to detect unseen attacks and suffers from a high false positive rate.

**Proposed system:**

In this we present our proposed novel two-stage ensemble deep learning-based attack detection and attack attribution framework for imbalanced ICS datasets.

* In the first stage, an ensemble representation learning model combined with a Decision Tree (DT) is designed to detect attacks in an imbalanced environment.
* Once the attack is detected, several one-vs-all classifiers will ensemble together to form a larger DNN to classify the attack attributes with a confidence interval during the second stage.

**ADVANTAGES:**

1. We develop a novel two-phase ensemble ICS attack detection method capable of detecting both previously seen and unseen attacks. The proposed deep representation learning results in this method being robust to imbalanced data.

2. The proposed method can accurately attribute attacks with high similarity. This is the first ML-based attack attribution method in ICS/IIoT at the time of this research.

3. We analyze the computational complexity of the proposed attack detection and attack attribution framework, demonstrating that despite its superior performance, its computational complexity is similar to that of other DNN.