COMP3217 COURSEWORK 2

MUHAMAD ABEED SAHARUDIN (STUDENT ID: 33371806)

March 27, 2024

1 Problem Statement

The problem given is to detect physical cyber-attacks on a power system framework configuration using machine learning (ML). The training data given to train the ML algorithm are 2 `.csv` files, each containing 6,000 system traces, with each of those containing 128 features. From the first training file, the last column is a marker that serves as a label indicating whether an event to the power system is a normal event (labelled as 0) or a data injection attack (labelled as 1). The second file represents the same thing, with the addition of the third event, a command injection attack (labelled as 2).

2 Pipeline Design

3 Training Evaluation

4 Conclusion