

**CHENNAI – PONDICHERRY**

**Evaluating Insider Threat DetectionWorkflow Using Supervised and Unsupervised Learning**

**Abstract**

Insider threat is a prominent cyber-security danger faced by organizations and companies. In this research, we study and evaluate an insider threat detection workflow using supervised and unsupervised learning algorithms. To this end, we study data exploration and analysis, anomaly detection and malicious behaviour classification on a publicly available data set. We evaluate several supervised and unsupervised learning algorithms - HMM, SOM, and DT - using this workflow.