ANNAMACHARYA INSTITUTE OF TECHNOLOGY & SCIENCES

(AUTONOMOUS)

Venktapuram (V) Karakambadi Raod, Tirupati-517520,A.P.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING - INTERNET OF THINGS AND CYBER SECURITY INCLUDING BLOCKCHAIN TECHNOLOGY

2021-2025

Predictive Insider Threats And Data Breaches Using Machine Learning

By

21AK1A3635	G.Thanuj sai
21AK1A3605	C.Charan sai
21AK1A3641	K.Yamini
21AK1A3610	P.Indra Kiran Achutha

Under the Guidance of

Mrs. B.JAYA VIJAYA, M.Tech

Assistant professor

Signature of **Project Guide**	**Signature of the** **Project Coordinator**	**Signature of the** **HOD**

Predictive Insider Threats And Data Breaches Using Machine Learning

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.