Patent Search

Invention Title	ARTIFICIAL INTELLIGENCE PROTECTION MEASURES AGAINST ARTIFICIAL INTELLIGENCE ATTACKS
Publication Number	26/2023
Publication Date	30/06/2023
Publication Type	INA
Application Number	202341038228
Application Filing Date	03/06/2023
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMPUTER SCIENCE
Classification (IPC)	G06N 030200, G06N 030800, G06N 050400, G06N 200000, G16H 502000

Inventor

Name	Address	Country	Nat
Dr. Shaik Jakeer Hussain	Associate Professor, INSTITUTE OF AERONAUTICAL ENGINEERING Hyderabad.	India	Ind
Dr. Thumu Srinivas Reddy	Associate Professor, Malla Reddy Engineering College (A), Hyderabad.	India	Ind
Dr. P.Saritha	Associate Professor, Malla Reddy Engineering College (A), Hyderaabad.	India	Ind
Dr. Chaganti B N Lakshmi	Professor, TKR College of Engineering and Technology, Hyderabad..	India	Ind

Applicant

Name	Address	Country	Nat
Dr. Shaik Jakeer Hussain	Associate Professor, INSTITUTE OF AERONAUTICAL ENGINEERING Hyderabad.	India	Ind
Dr. Thumu Srinivas Reddy	Associate Professor, Malla Reddy Engineering College (A), Hyderabad.	India	Ind
Dr. P.Saritha	Associate Professor, Malla Reddy Engineering College (A), Hyderaabad.	India	Ind
Dr. Chaganti B N Lakshmi	Professor, TKR College of Engineering and Technology, Hyderabad..	India	Ind

Abstract:

7. ABSTRACT A method and system of protecting an artificial intelligence (AI) application comprises parameters of the AI application and are identified. An assessmen vulnerability of the AI application is performed. A combination of protection measures comprising two or more protection measures against at least two different att least one dataset, and determining whether the combination of protection measures is successful in defending the AI application. A target configuration of an AI moc the AI application is determined based on the assessed vulnerability of the AI application. An AI enhanced algorithm is determined to adjust the AI model to include a combination of most computationally efficient defenses based on the target configuration. The adjusted AI model is used to protect the AI application. The figure ass the abstract is Fig. 1.

Complete Specification

Description:4. DESCRIPTION

Technical Field of the invention

The present invention generally relates to computer systems and its applications and more particularly, relates to identify protection measures for Artificial Intellige systems.
Background of the invention

Machine learning (ML) is a subfield of computer science that evolved from the study of pattern recognition and computational learning theory in artificial intelligenc Today, ML is increasingly used to construct algorithms that can learn from and make predictions based on reference data.

The ML algorithms are used in an ever-increasing number of applications, including facial recognition, medical diagnoses, autonomous vehicles, access control, etc. studies have shown that machine learning classifiers can be deceived to provide incorrect predictions. As the number of systems that use such AI increase and are security sensitive areas, the safety of such AI systems is of growing concern. Indeed, by at least one calculation more than 300 research papers have been devoted t different concerns regarding approaches to AI system protection

View Application Status