Title (en)

A METHOD TO PREVENT CAPTURING OF MODELS IN AN ARTIFICIAL INTELLIGENCE BASED SYSTEM

Title (de)

VERFAHREN ZUR VERHINDERUNG DER ERFASSUNG VON MODELLEN IN EINEM AUF KÜNSTLICHER INTELLIGENZ BASIERENDEN SYSTEM

Title (fr)

PROCÉDÉ POUR EMPÊCHER LA CAPTURE DE MODÈLES DANS UN SYSTÈME BASÉE SUR L'INTELLIGENCE ARTIFICIELLE

Publication

EP 4007979 A1 20220608 (EN)

Application

EP 20729697 A 20200528

Priority

- IN 201941025751 A 20190628
- EP 2020064838 W 20200528

Abstract (en)

[origin: WO2020259946A1] The invention discloses a system and a method to prevent unauthorized capturing of models in an Artificial Intelligence based system (AI system) (100). The method comprises the steps: receiving an input (103) from a user; checking whether the input (103) is right input or wrong input; computing information gain extracted by said user when the input (103) is wrong input; locking out said system (100) when said information gain exceeds a pre-defined threshold.

IPC 8 full level

G06N 3/04 (2006.01); **G06N 3/08** (2006.01); **G06N 5/00** (2006.01); **G06N 7/00** (2006.01); **G06N 20/00** (2019.01)

CPC (source: EP)

G06N 3/088 (2013.01); **G06N 5/01** (2023.01); **G06N 7/01** (2023.01); **G06N 20/00** (2018.12); G06N 3/045 (2023.01)

Citation (search report)

See references of WO 2020259946A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

WO 2020259946 A1 20201230; EP 4007979 A1 20220608

DOCDB simple family (application)

EP 2020064838 W 20200528; EP 20729697 A 20200528