Title (en)

SYSTEMS AND METHODS FOR PROVIDING A SYSTEMIC ERROR IN ARTIFICIAL INTELLIGENCE ALGORITHMS

Title (de)

SYSTEME UND VERFAHREN ZUR BEREITSTELLUNG EINES SYSTEMISCHEN FEHLERS IN ALGORITHMEN MIT KÜNSTLICHER INTELLIGENZ

Title (fr)

SYSTÈMES ET PROCÉDÉS DE FOURNITURE D'ERREUR SYSTÉMIQUE DANS DES ALGORITHMES D'INTELLIGENCE ARTIFICIELLE

Publication

**EP 4229554 A1 20230823 (EN)**

Application

**EP 21880894 A 20211012**

Priority

- US 202063090933 P 20201013
- US 2021054542 W 20211012

Abstract (en)

[origin: WO2022081553A1] Disclosed is a process for testing a suspect model to determine whether it was derived from a source model. An example method includes receiving, from a model owner node, a source model and a fingerprint associated with the source model, receiving a suspect model at a service node, based on a request to test the suspect model, applying the fingerprint to the suspect model to generate an output and, when the output has an accuracy that is equal to or greater than a threshold, determining that the suspect model is derived from the source model. Imperceptible noise can be used to generate the fingerprint which can cause predictable outputs from the source model and a potential derivative thereof.

IPC 8 full level

**G06N 3/02** (2006.01)

CPC (source: EP)

**G06N 3/045** (2023.01); **G06N 3/08** (2013.01); **G06N 3/096** (2023.01); G06F 21/64 (2013.01)

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

Designated validation state (EPC)

KH MA MD TN

DOCDB simple family (publication)

**WO 2022081553 A1 20220421**; **WO 2022081553 A4 20220616**; CA 3195434 A1 20220421; EP 4229554 A1 20230823; EP 4229554 A4 20240403

DOCDB simple family (application)

**US 2021054542 W 20211012**; CA 3195434 A 20211012; EP 21880894 A 20211012