(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 963 489 B8**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Bibliography INID code(s) 73

(48) Corrigendum issued on:
06.11.2024 Bulletin 2024/45

(45) Date of publication and mention of the grant of the patent:
02.10.2024 Bulletin 2024/40

(21) Application number: **20727021.6**

(22) Date of filing: **28.04.2020**

(51) International Patent Classification (IPC):
G06F 21/56 *(2013.01)* ***H04L 9/40*** *(2022.01)*
G06N 3/044 *(2023.01)* ***G06N 3/045*** *(2023.01)*
G06N 3/049 *(2023.01)* ***G06N 3/088*** *(2023.01)*
G06N 5/01 *(2023.01)* ***G06N 20/10*** *(2019.01)*
G06N 7/01 *(2023.01)* ***G06N 20/20*** *(2019.01)*

(52) Cooperative Patent Classification (CPC):
G06F 21/562; G06N 3/044; G06N 3/045; G06N 3/049; G06N 3/088; G06N 5/01; G06N 7/01; G06N 20/10; G06N 20/20; H04L 63/1441;
G06F 21/563; H04L 63/145

(86) International application number:
PCT/US2020/030247

(87) International publication number:
WO 2020/223222 (05.11.2020 Gazette 2020/45)

(54) **MACHINE LEARNING MODEL SCORE OBFUSCATION USING STEP-FUNCTION, POSITION-DEPENDENT NOISE**

MASCHINENLERNMODELLWERTVERSCHLEIERUNG UNTER VERWENDUNG VON SCHRITTFUNKTIONALEM POSITIONSABHÄNGIGEM RAUSCHEN

OBSCURCISSEMENT DE SCORE DE MODÈLE D'APPRENTISSAGE AUTOMATIQUE UTILISANT DU BRUIT À FONCTION EN ESCALIER DÉPENDANT DE LA POSITION

(84) Designated Contracting States:
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

(30) Priority: **30.04.2019 US 201916399665**
30.04.2019 US 201916399718
30.04.2019 US 201916399701
30.04.2019 US 201916399735
30.04.2019 US 201916399677

(43) Date of publication of application:
09.03.2022 Bulletin 2022/10

(73) Proprietor: **Cylance Inc.**
Irving, TX 75039 (US)

(72) Inventors:
- **BUCKINGHAM, Hailey**
Waterloo, ON N2K 0A7 (CA)
- **BEVERIDGE, David, N.**
Waterloo, ON N2K 0A7 (CA)

(74) Representative: **Murgitroyd & Company**
165-169 Scotland Street
Glasgow G5 8PL (GB)

(56) References cited:
US-A1- 2017 220 929 **US-A1- 2018 013 772**
US-A1- 2018 330 379

- **FAKHR MOHAMED WALEED: "A multi-key compressed sensing and machine learning privacy preserving computing scheme", 2017 5TH INTERNATIONAL SYMPOSIUM ON COMPUTATIONAL AND BUSINESS INTELLIGENCE (ISCBI), IEEE, 11 August 2017 (2017-08-11), pages 75 - 80, XP033159090, ISBN: 978-1-5386-1771-7, [retrieved on 20170928], DOI: 10.1109/ISCBI.2017.8053548**

Processed by Luminess, 75001 PARIS (FR)

(Cont. next page)

- **MKHAIL KAZDAGLI ET AL: "Exploiting Latent Attack Semantics for Intelligent Malware Detection", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 6 August 2017 (2017-08-06), XP080951659**
- **TIANWEI ZHANG ET AL: "Privacy-preserving Machine Learning through Data Obfuscation", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 5 July 2018 (2018-07-05), XP081244226**