US 20240214413A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2024/0214413 A1**

Parga Jimenez et al. (43) **Pub. Date: Jun. 27, 2024**

(54) **CYBER-HARDENING USING ADVERSARIAL SIMULATED ATTACKING AND DEFENDER SYSTEMS AND MACHINE LEARNING**

(71) Applicant: **International Business Machines Corporation**, Armonk, NY (US)

(72) Inventors: **Juan Pablo Parga Jimenez**, Guadalajara (MX); **Humberto Orozco Cervantes**, Tonalá (MX); **Jose Ramon Navarro Marquez**, Zapopan (MX)

(21) Appl. No.: **18/086,439**

(22) Filed: **Dec. 21, 2022**

Publication Classification

(51) **Int. Cl.**

H04L 9/40	(2006.01)
G06N 7/08	(2006.01)
H04L 41/16	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/145*** (2013.01); ***G06N 7/08*** (2013.01); ***H04L 41/16*** (2013.01)

(57) **ABSTRACT**

In one general embodiment, a computer-implemented method includes applying a plurality of known cyber-attack techniques and variations thereof against a simulated defender system using a simulated attacking system. Known cyber-attack defense techniques are applied to the defender system. Instances of the defender system are logged in association with various combinations of respective cyber-attack techniques, various cyber-attack defense techniques, simulated system configurations, and simulated system outcomes as training instances. A machine learning model is trained using the logged training instances. A production product configuration is input to the trained machine learning model. Information related to cyber-hardening of the production product is output from the trained machine learning model.