US 20240214396A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2024/0214396 A1**

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

(54) **CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM**

(71) Applicant: **SANDS LAB INC.**, Seoul (KR)

(72) Inventors: **Ki Hong KIM**, Seoul (KR); **Sung Eun PARK**, Seongnam-si (KR); **Min Jun CHOI**, Seoul (KR); **Hyun Jong LEE**, Seoul (KR)

(73) Assignee: **SANDS LAB INC.**, Seoul (KR)

(21) Appl. No.: **18/132,951**

(22) Filed: **Apr. 10, 2023**

(30) **Foreign Application Priority Data**

Dec. 27, 2022 (KR) 10-2022-0185519

Publication Classification

(51) **Int. Cl.**
H04L 9/40 (2006.01)
H04L 41/16 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1416*** (2013.01); ***H04L 41/16*** (2013.01); ***H04L 63/1433*** (2013.01)

(57) **ABSTRACT**

Provided is a cyber threat information processing method including collecting a webpage and classifying data included in the webpage or data linked according to link depth, detecting whether the data included in the webpage or the linked data is malicious on a plurality of layers, the plurality of layers including at least two of antivirus-based malicious pattern detection, signature malicious pattern detection according to a certain rule, or malignancy detection according to an artificial intelligence (AI) algorithm for the data, and providing or storing record data of the webpage when the data is detected to be malicious as a result of the detection.