US 20240214404A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2024/0214404 A1

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

(54) SYSTEM AND METHOD FOR DETECTING AND PREVENTING MODEL INVERSION ATTACKS

(71) Applicant: **Nuance Communications, Inc.**, Burlington, MA (US)

(72) Inventors: **Dushyant SHARMA**, Mountain House, CA (US); **Patrick Aubrey NAYLOR**, Reading (GB); **William Francis GANONG, III**, Brookline, MA (US); **Uwe Helmut JOST**, Groton, MA (US); **Ljubomir MILANOVIC**, Vienna (AT)

(21) Appl. No.: **18/146,620**

(22) Filed: **Dec. 27, 2022**

Publication Classification

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

(52) **U.S. Cl.**
CPC ***H04L 63/1425*** (2013.01); ***H04L 63/1491*** (2013.01)

(57) **ABSTRACT**

A method, computer program product, and computing system for executing a plurality of requests to process data using a trained machine learning model. An anomalous pattern of requests including at least a threshold amount of out-of-domain data is identified from the plurality of requests. A potential model inversion attack is detected based upon, at least in part, identifying the anomalous pattern of requests.