US 20230231857A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2023/0231857 A1**

Neupane et al. (43) **Pub. Date: Jul. 20, 2023**

(54) **DEEP LEARNING PIPELINE TO DETECT MALICIOUS COMMAND AND CONTROL TRAFFIC**

(71) Applicant: **Palo Alto Networks, Inc.**, Santa Clara, CA (US)

(72) Inventors: **Ajaya Neupane**, San Jose, CA (US); **Yuwen Dai**, Santa Clara, CA (US); **Stefan Achleitner**, Arlington, VA (US); **Yu Fu**, Campbell, CA (US); **Shengming Xu**, San Jose, CA (US)

(21) Appl. No.: **17/577,925**

(22) Filed: **Jan. 18, 2022**

Publication Classification

(51) **Int. Cl.**
H04L 9/40 (2006.01)
G06N 3/04 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1416*** (2013.01); ***H04L 63/1425*** (2013.01); ***H04L 63/145*** (2013.01); ***G06N 3/04*** (2013.01)

(57) **ABSTRACT**

Detection of command and control malware is disclosed. A network traffic session is monitored. Automatic feature identification for real-time malicious command and control traffic detection based on a request header of the monitored network traffic session using a deep learning model is performed.