US 20230231860A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2023/0231860 A1**

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

(54) **IOT DEVICE IDENTIFICATION BY MACHINE LEARNING WITH TIME SERIES BEHAVIORAL AND STATISTICAL FEATURES**

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

(72) Inventors: **Ke Tian**, San Jose, CA (US); **Yilin Zhao**, San Jose, CA (US); **Xiaoyi Duan**, San Jose, CA (US); **Jun Du**, Cupertino, CA (US)

(21) Appl. No.: **17/578,293**

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

Publication Classification

(51) **Int. Cl.**

H04L 9/40	(2006.01)
G06N 5/02	(2006.01)
G06N 7/00	(2006.01)

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

CPC ***H04L 63/1425*** (2013.01); ***G06N 5/022*** (2013.01); ***G06N 7/005*** (2013.01); ***H04L 63/20*** (2013.01)

(57) **ABSTRACT**

Identifying Internet of Things (IoT) devices with packet flow behavior including by using machine learning models is disclosed. Information associated with a network communication of an IoT device is received. A determination of whether the IoT device has previously been classified is made. In response to determining that the IoT device has not previously been classified, a determination is made that a probability match for the IoT device against a behavior signature exceeds a threshold. The behavior signature includes at least one time series feature for an application used by the IoT device. Based at least in part on the probability match, a classification of the IoT device is provided to a security appliance configured to apply a policy to the IoT device.