

(19) **United States**

(12) **Patent Application Publication**
Jiao

(10) **Pub. No.: US 2023/0231871 A1**

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

(54) **TRAINING METHOD FOR DETECTION
MODEL, SYSTEM, DEVICE, AND STORAGE
MEDIUM**

Publication Classification

(51) **Int. Cl.**
H04L 9/40 (2006.01)
G06N 20/00 (2006.01)
(52) **U.S. Cl.**
CPC *H04L 63/1441* (2013.01); *G06N 20/00*
(2019.01); *H04L 63/1416* (2013.01)

(71) Applicant: **Huawei Technologies Co., Ltd.**,
Shenzhen (CN)

(72) Inventor: **Lijuan Jiao**, Beijing (CN)

(21) Appl. No.: **18/180,960**

(22) Filed: **Mar. 9, 2023**

Related U.S. Application Data

(63) Continuation of application No. PCT/CN2021/
089390, filed on Apr. 23, 2021.

Foreign Application Priority Data

Sep. 10, 2020 (CN) 202010948783.1

(57) **ABSTRACT**

This application provides a training method for a detection model, a system, a device, and a storage medium, belongs to the field of network security technologies, and further relates to application of an AI technology in the field of network security technologies. Some embodiments of this application provide a method for training a detection model by using federated learning. In the method, a gateway device serves as a participant of federated learning, and a server aggregates model parameters and delivers shared malicious samples for the gateway device. When the gateway device performs model training, the gateway device exchanges information such as the model parameters and the shared samples with the server, to obtain a detection model through training.

