US 20240214412A1

(19) United States

(12) Patent Application Publication

MO et al.

(10) Pub. No.: US 2024/0214412 A1

(43) Pub. Date: Jun. 27, 2024

(54) **HIERARCHICAL NOVELTY DETECTION USING INTENDED STATES FOR NETWORK SECURITY**

(71) Applicant: **VMware LLC**, Palo Alto, CA (US)

(72) Inventors: **Zhen MO**, Sunnyvale, CA (US); **Vijay GANTI**, Fremont, CA (US); **Debessay Fesehaye KASSA**, Mountain View, CA (US); **Barak RAZ**, San Francisco, CA (US); **Honglei LI**, Mountain View, CA (US)

(21) Appl. No.: **18/342,101**

(22) Filed: **Jun. 27, 2023**

Related U.S. Application Data

(63) Continuation of application No. 16/900,240, filed on Jun. 12, 2020, now Pat. No. 11,729,207.

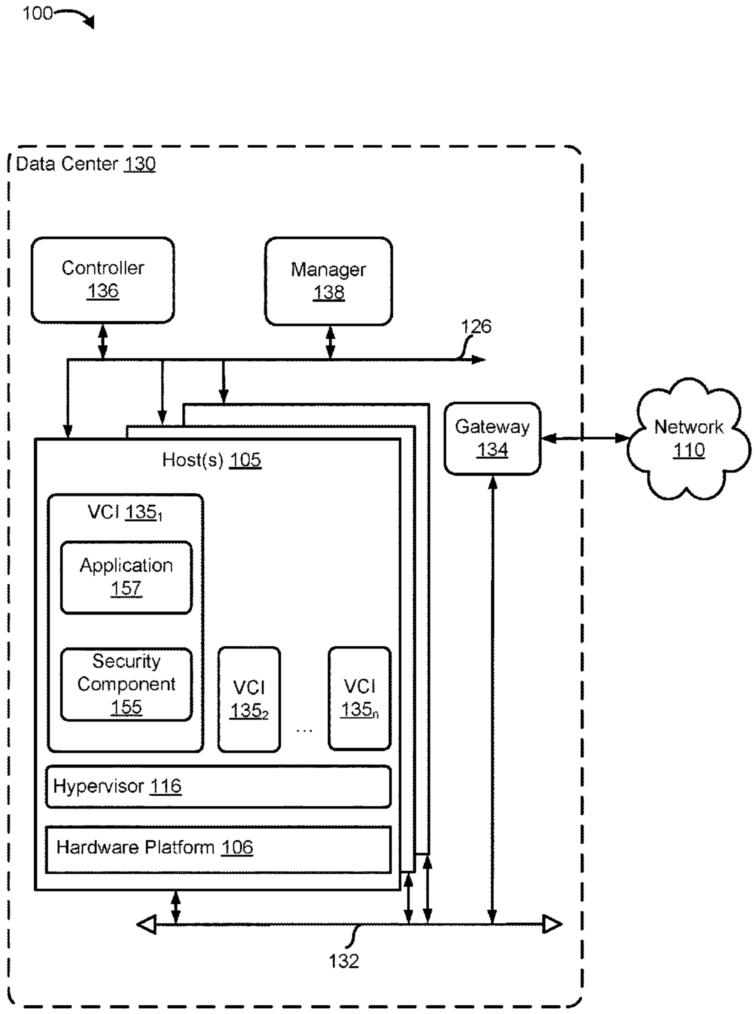
Publication Classification

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

(52) **U.S. Cl.**
CPC *H04L 63/1441* (2013.01); *H04L 63/0236* (2013.01); *H04L 63/1416* (2013.01); *H04L 63/1425* (2013.01); *H04L 63/20* (2013.01)

(57) **ABSTRACT**

The disclosure provides an approach for detecting and preventing attacks in a network. Embodiments include determining a plurality of network behaviors of a process by monitoring the process. Embodiments include generating a plurality of intended states for the process based on subsets of the plurality of network behaviors. Embodiments include determining a plurality of intended state clusters by applying a clustering technique to the plurality of intended states. Embodiments include determining a state of the process. Embodiments include identifying a given cluster of the plurality of intended state clusters that corresponds to the state of the process. Embodiments include selecting a novelty detection technique based on a size of the given cluster. Embodiments include using the novelty detection technique to determine, based on the given cluster and the state of the process, whether to generate a security alert for the process.


100
Data Center 130
Controller 136
Manager 138
126
Gateway 134
Network 110
Host(s) 105
VCI 135_1
Application 157
Security Component 155
VCI 135_2
...
VCI 135_n
Hypervisor 116
Hardware Platform 106
132