



(54) **OUTPUT OF BASELINE BEHAVIORS
CORRESPONDING TO FEATURES OF
ANOMALOUS EVENTS**

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

(71) Applicant: **Microsoft Technology Licensing, LLC,**
Redmond, WA (US)

(57) **ABSTRACT**

(72) Inventors: **Idan Yehoshua HEN**, Tel Aviv (IL);
Andrey KARPOVSKY, Kiryat Motzkin (IL)

(73) Assignee: **Microsoft Technology Licensing, LLC,**
Redmond, WA (US)

(21) Appl. No.: **17/578,145**

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

Publication Classification

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

(2006.01)

According to examples, an apparatus may include a processor and a memory on which is stored machine-readable instructions that when executed by the processor, may cause the processor to determine baseline behaviors from collected data. The processor may also detect that an anomalous event has occurred and may determine at least one feature of the anomalous event that caused the event to be determined to be anomalous. The processor may further identify, from the determined baseline behaviors, a set of baseline behaviors corresponding to the determined at least one feature. The processor may still further generate a message to include an indication that the anomalous event has been detected and the identified set of baseline behaviors and may output the generated message.

```
graph TD
    NE[NETWORK ENVIRONMENT 100]
    subgraph APPARATUS 102
        P[PROCESSOR 104]
        M[MEMORY 106]
        subgraph DATA_STORE 108
            BB[BASELINE BEHAVIORS 112]
            SBB[SET OF BASELINE BEHAVIORS 116]
            AE[ANOMALOUS EVENT 114]
            MSG[MESSAGE 118]
        end
        NI[NETWORK INTERFACE 110]
    end
    APPARATUS_102 <--> N((NETWORK 130))
    N <--> NE1[NETWORK ENTITY 140]
    subgraph NE1
        CD[COLLECTED DATA 142]
    end
    N <--> EA[EVENT A 120a]
    N <--> EB[EVENT B 120b]
    N <--> EN[EVENT N 120n]
    subgraph EA
        FEA[FEATURE(S) 122a]
    end
    subgraph EB
        FEB[FEATURE(S) 122b]
    end
    subgraph EN
        FEN[FEATURE(S) 122n]
    end
```