

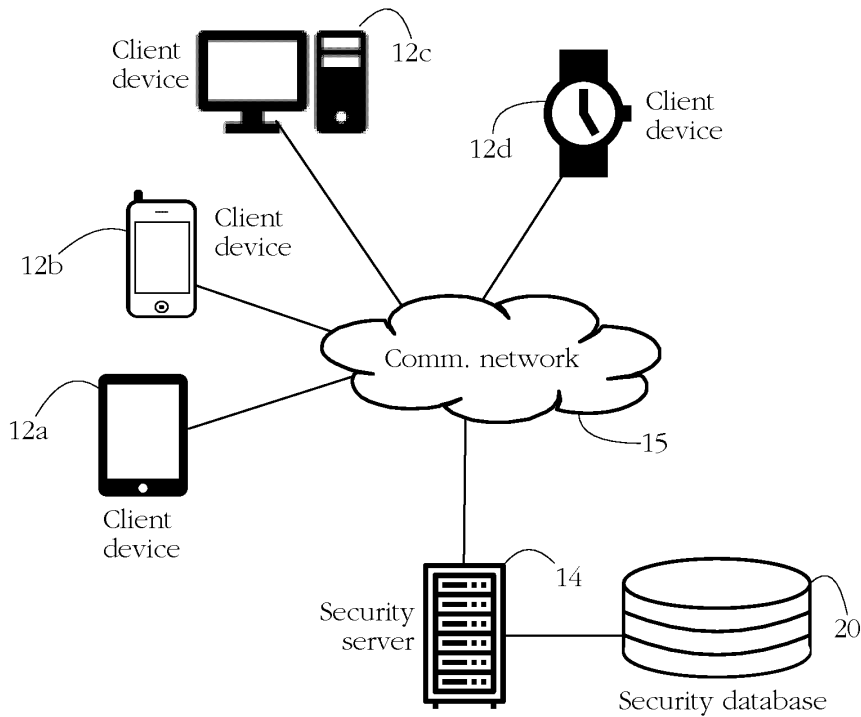


FIG. 1

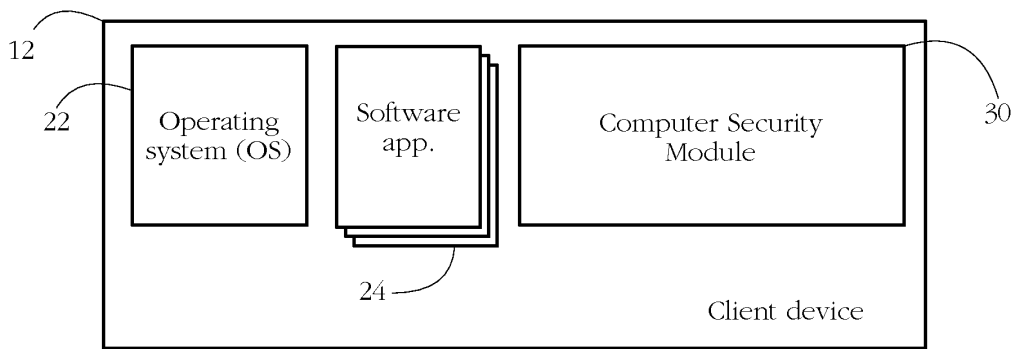


FIG. 2

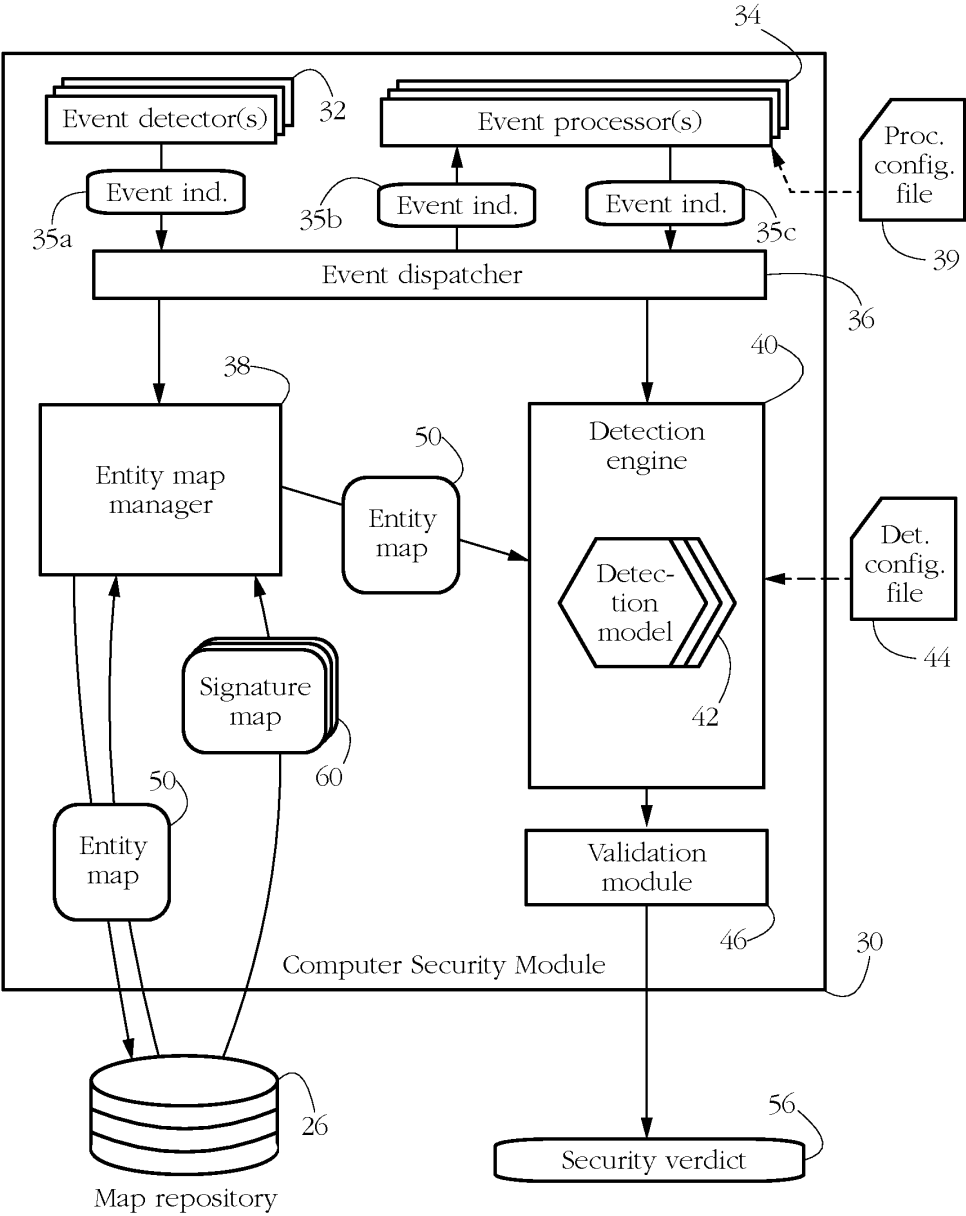


FIG. 3

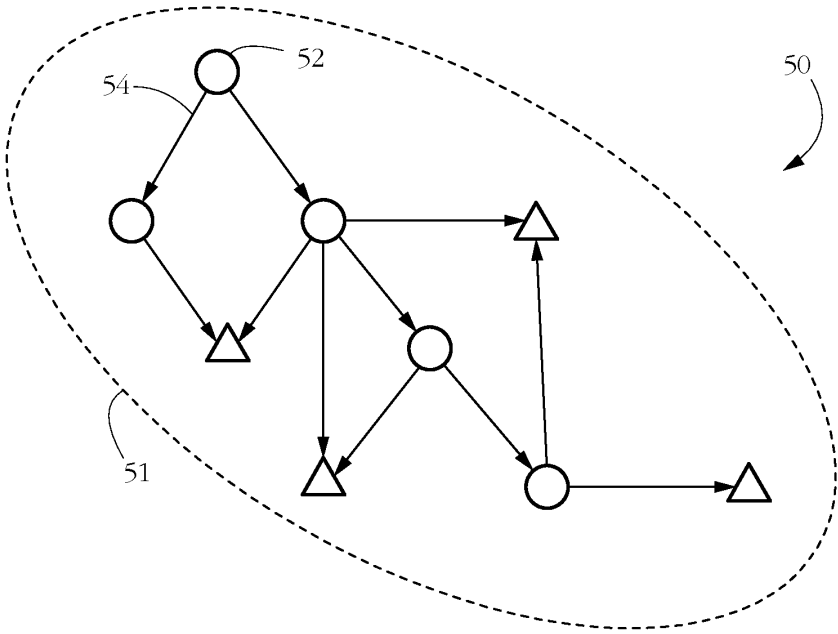


FIG. 4

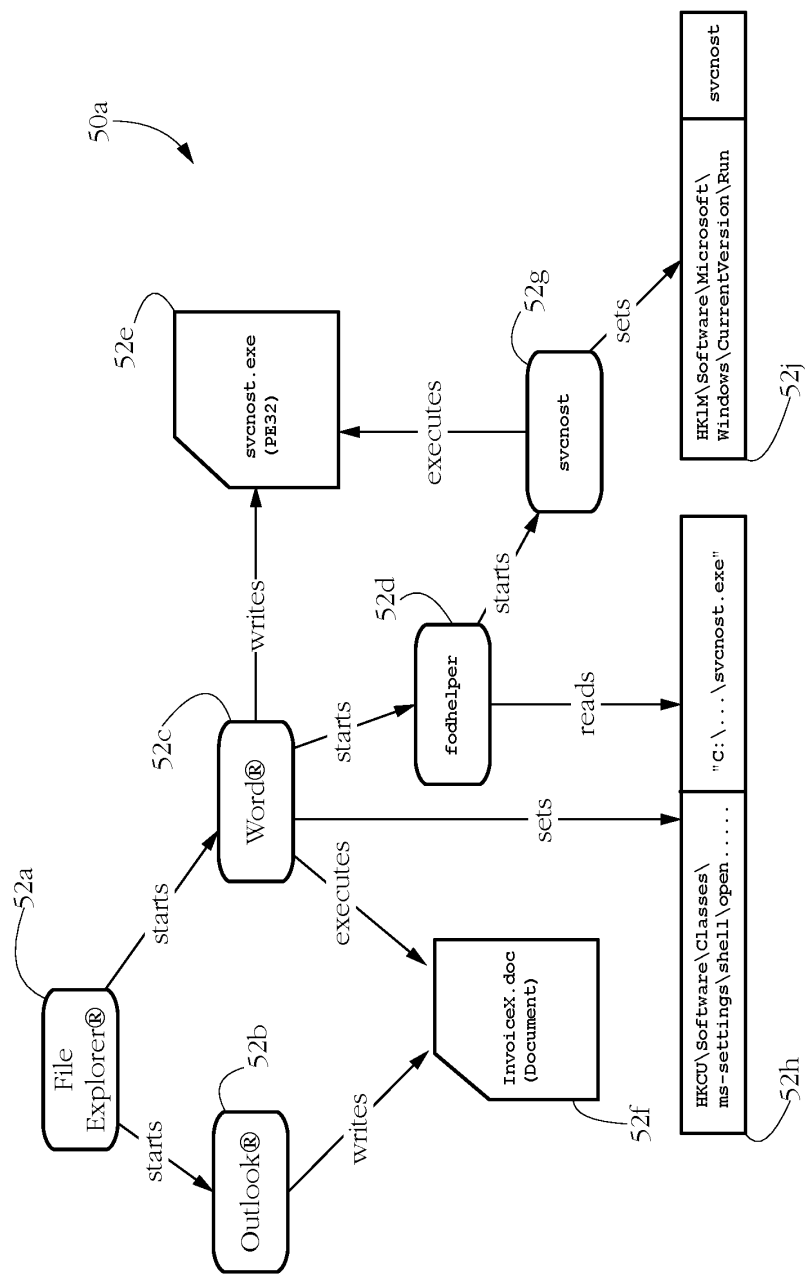


FIG. 5-A

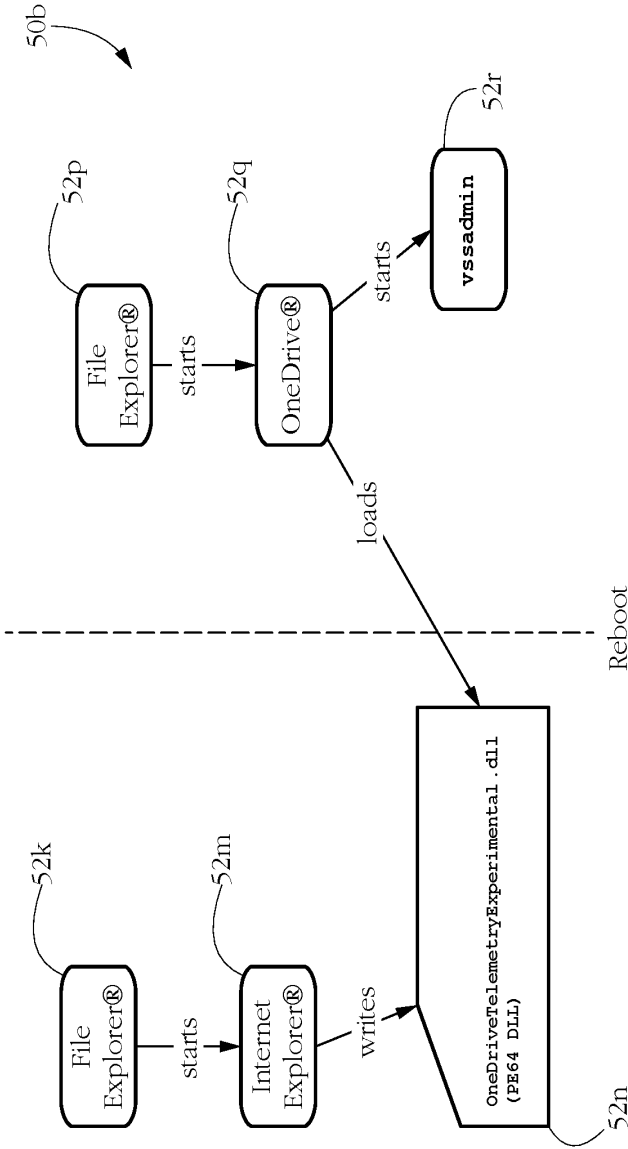


FIG. 5-B

6/16

```
{
  "Entities": [
    "Worker1": {
      "PID" : "17366",
      "ExecutablePath" : "C:\ProgramFiles\...\Office19Outlook.exe",
      "VersionInfo": {
        "CompanyName": "Microsoft Corporation",
        "Build": "16.0.4229.1003",
      }
      "TLaunch" : "01d84ec52d51d0d6",
      "TTermination" : "NaN",
      "Flags" : {
        "ExecutesExternalCode" : "IsNotSet",
        ...
      }
    },
    "Resource1": {
      "Type": "word document",
      "Path" : "C:\Users\RaduP\...\InvoiceX.doc",
      "Flags" : {
        "HasExternalOrigin" : "IsSet",
        "Overwritten" : "IsNotSet",
        ...
      }
    },
    ...
  ],
  "Relations": [
    {
      "From": "Worker1",
      "To": "Resource1",
      "Type": "Drop"
    },
    ...
  ]
}
```

56a

56b

50c

FIG. 6

7/16

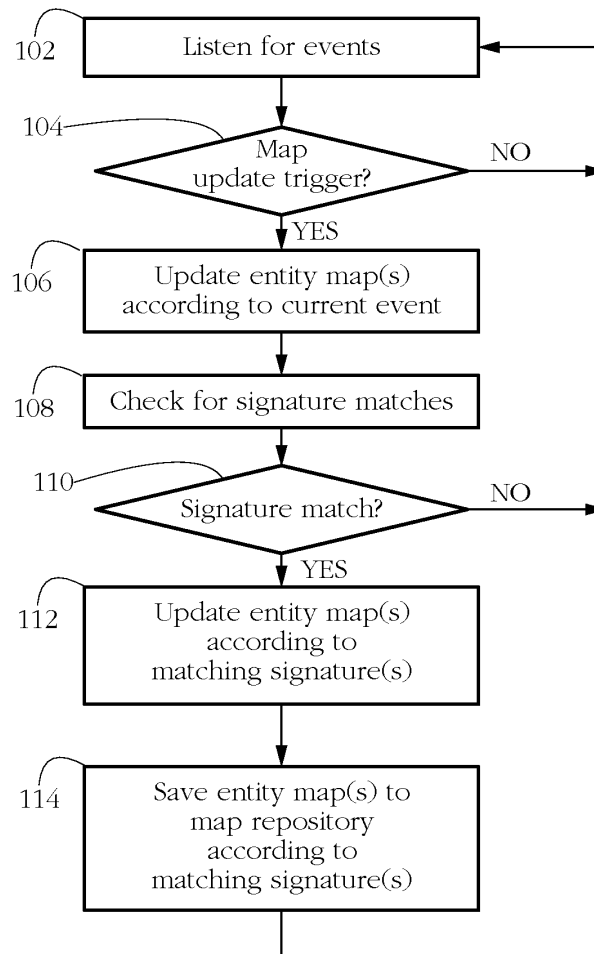


FIG. 7

8/16

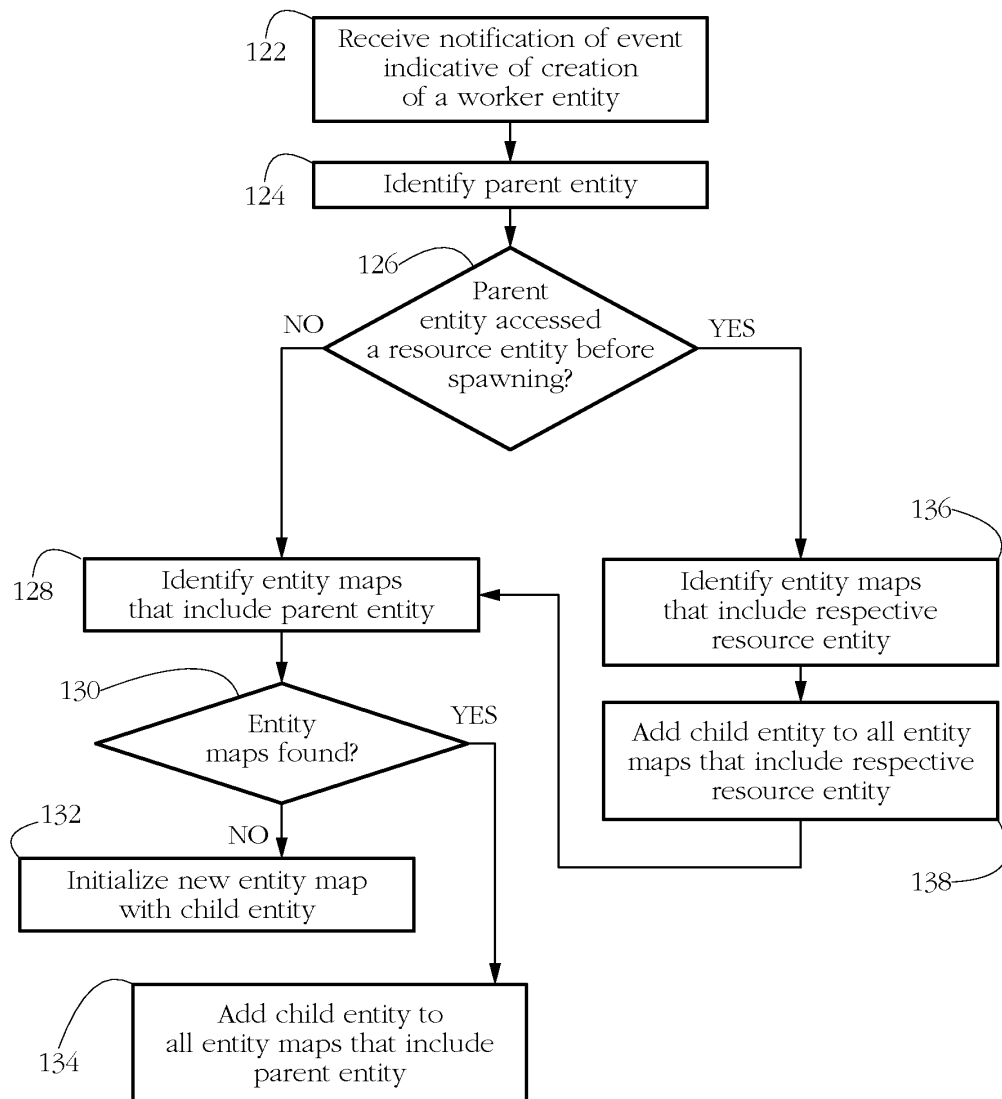


FIG. 8

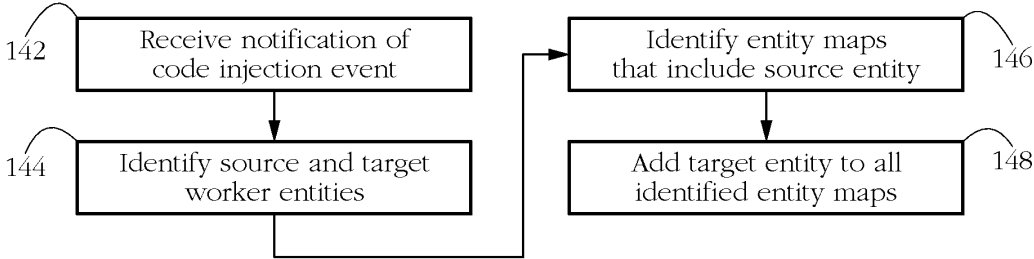


FIG. 9

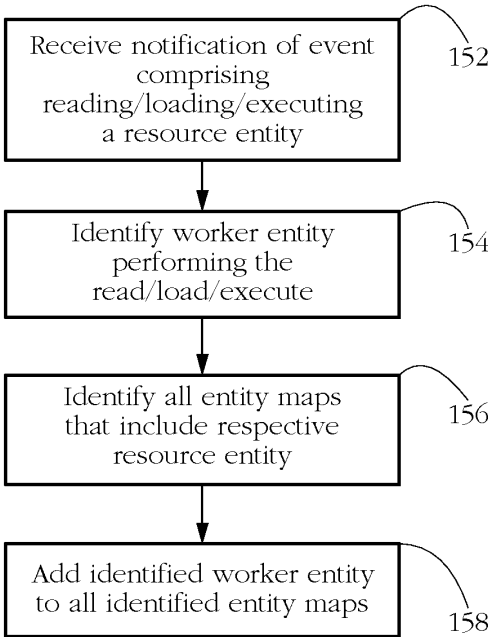


FIG. 10

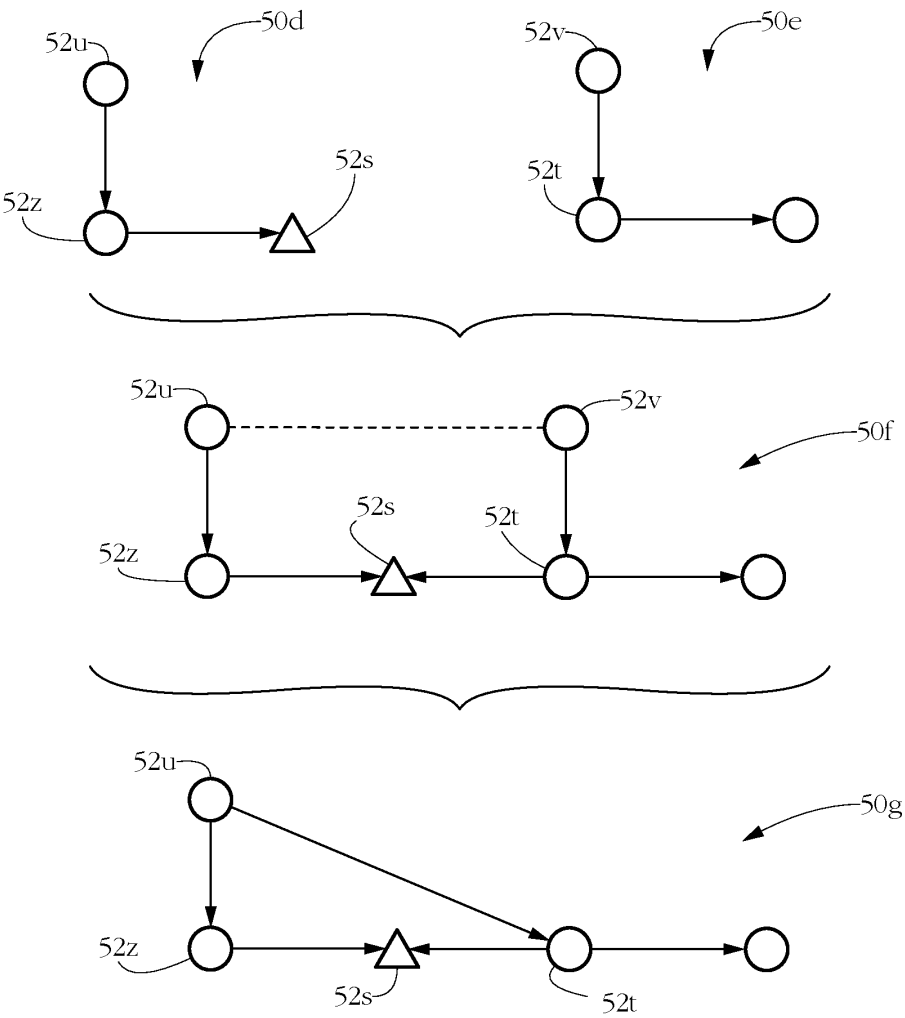


FIG. 11

11/16

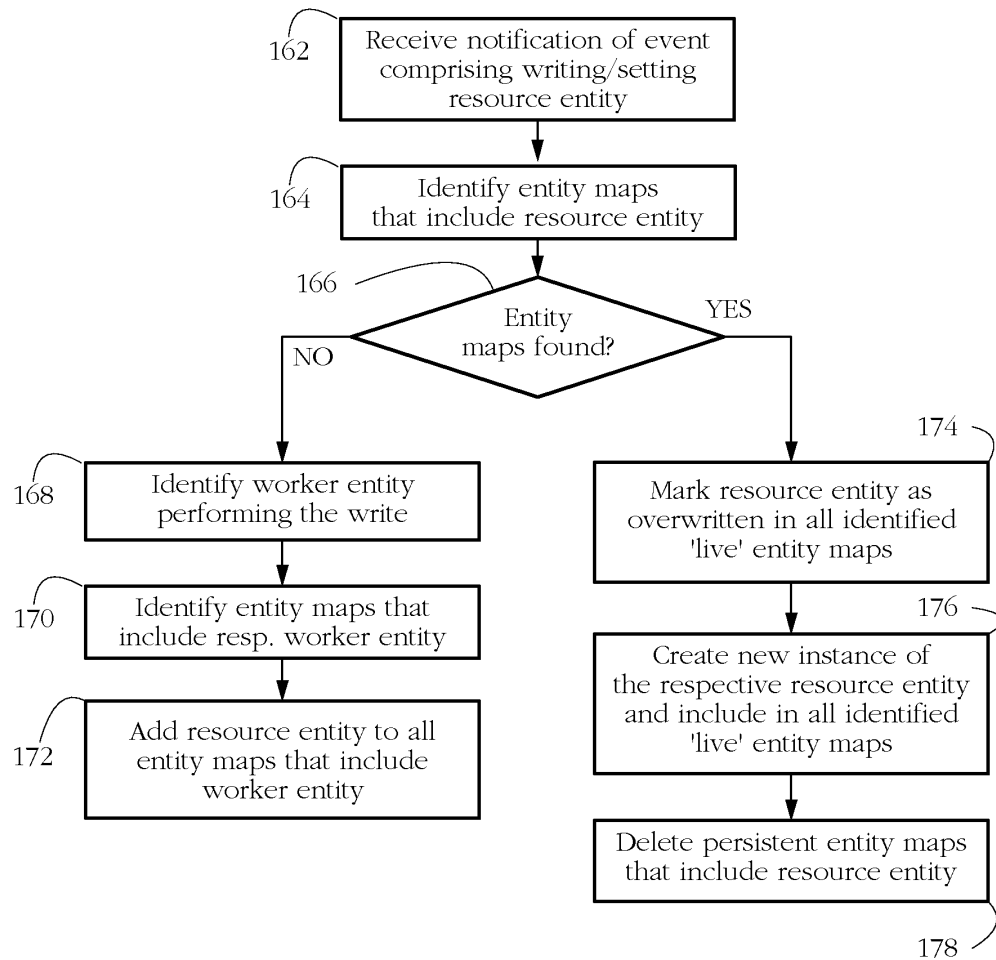


FIG. 12

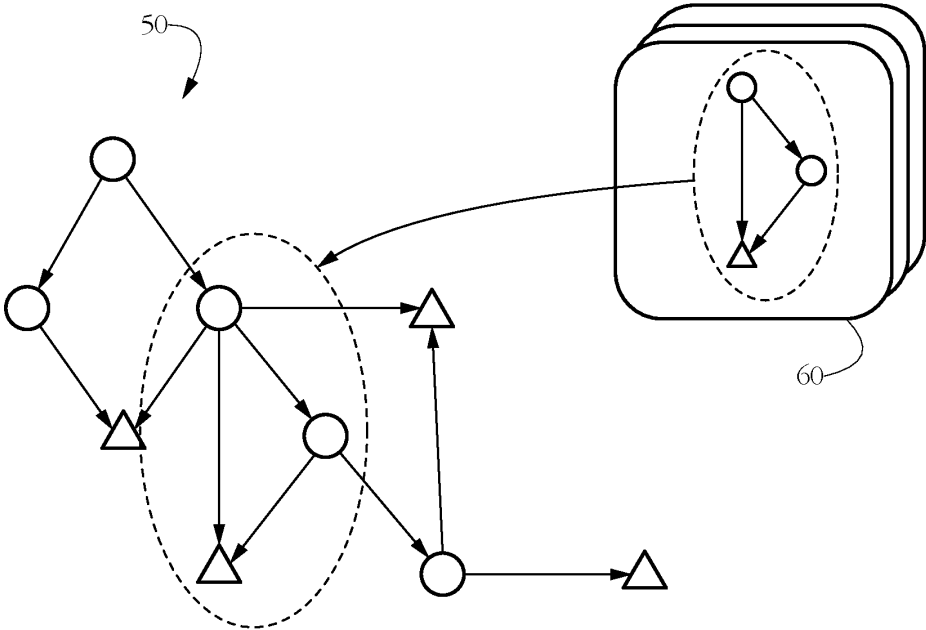


FIG. 13

13/16

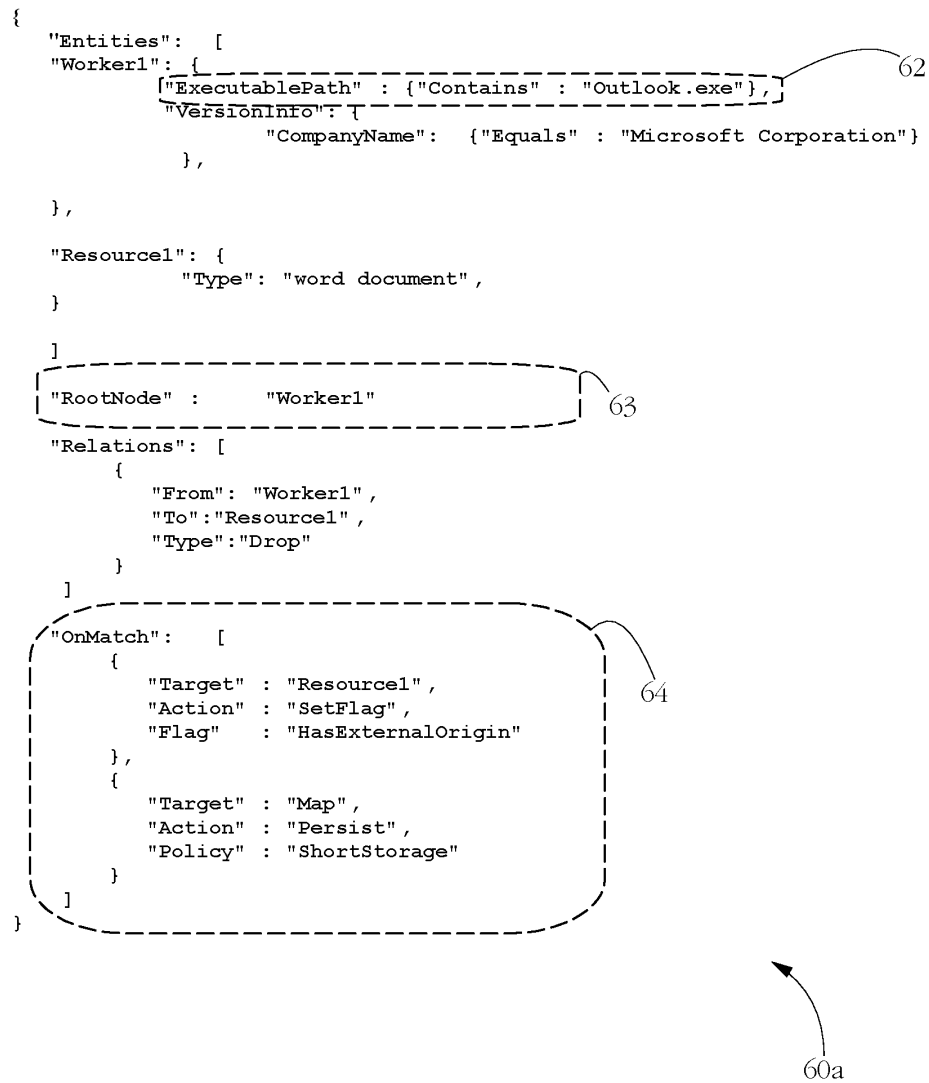


FIG. 14

14/16

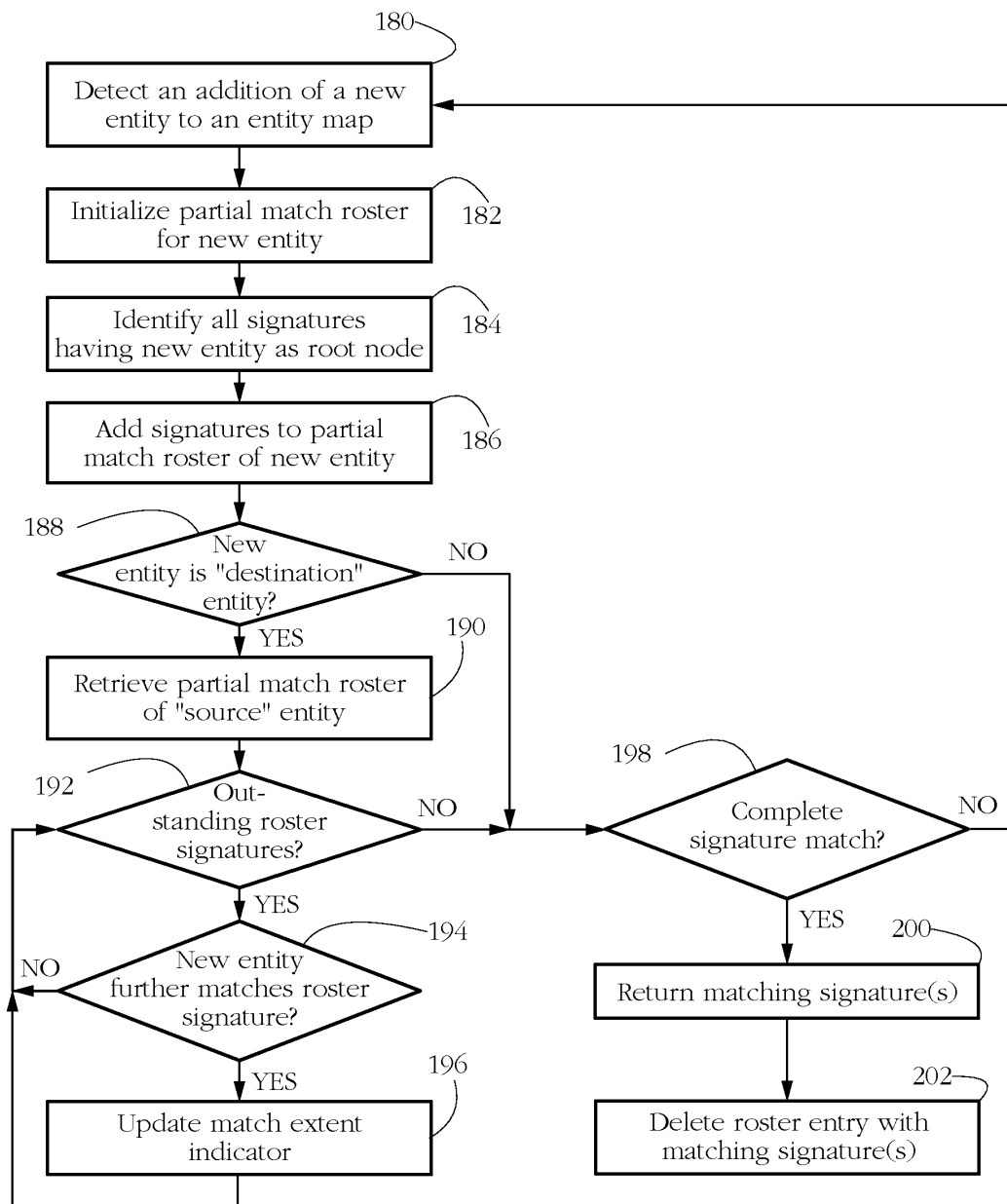


FIG. 15

15/16

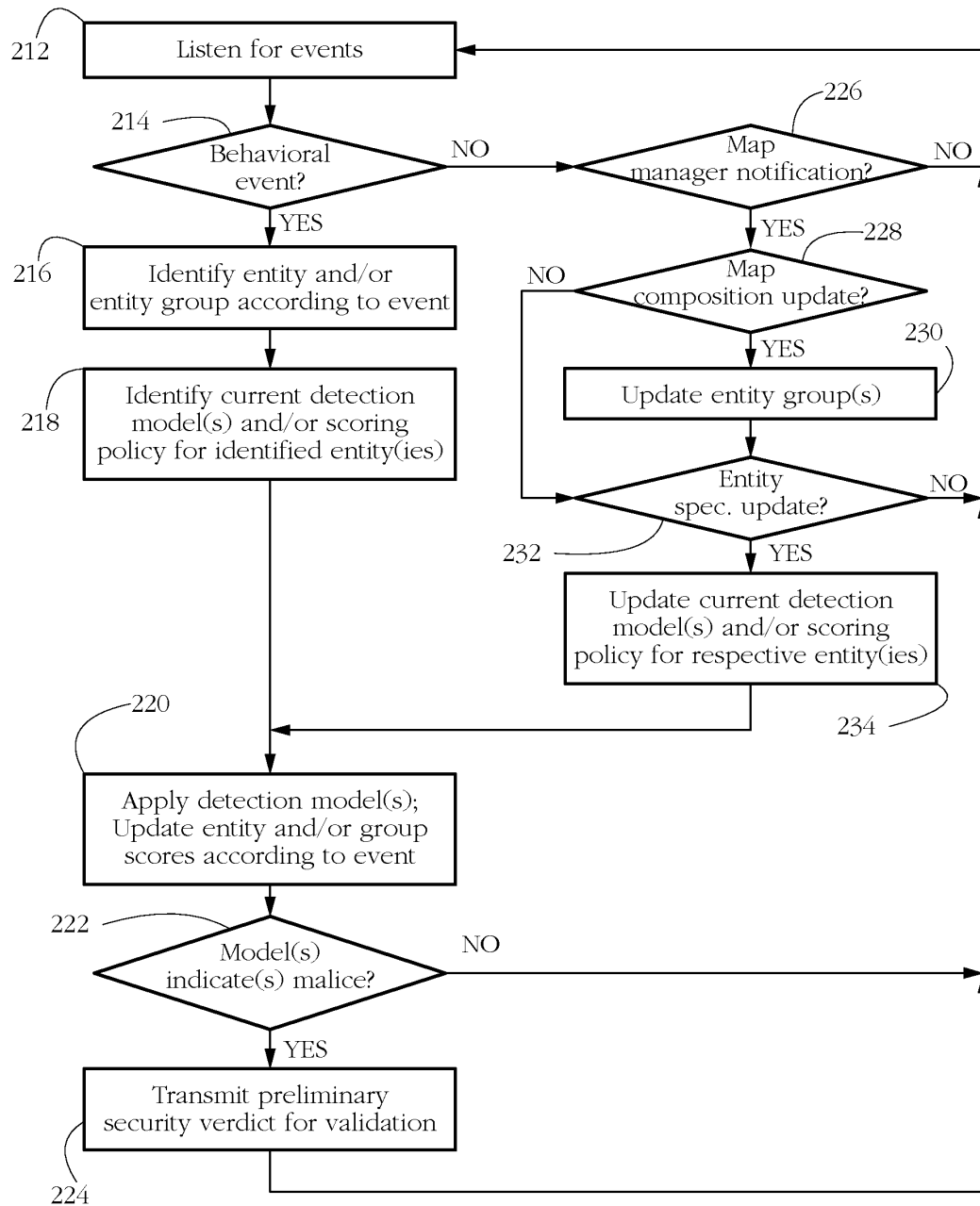


FIG. 16

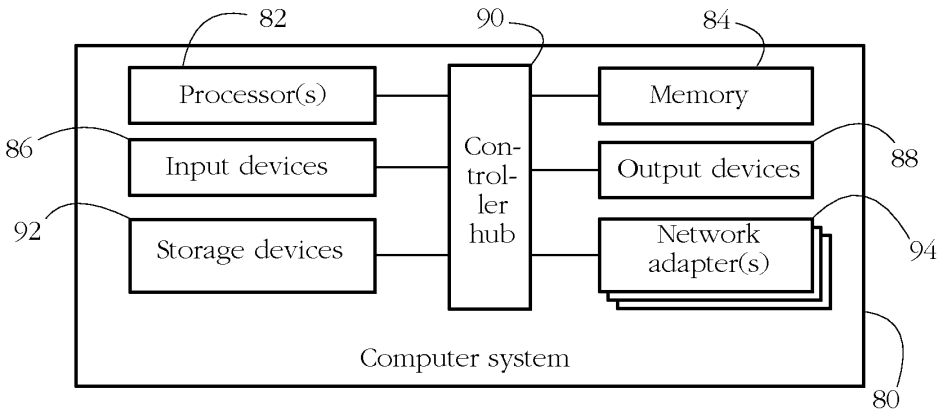


FIG. 17