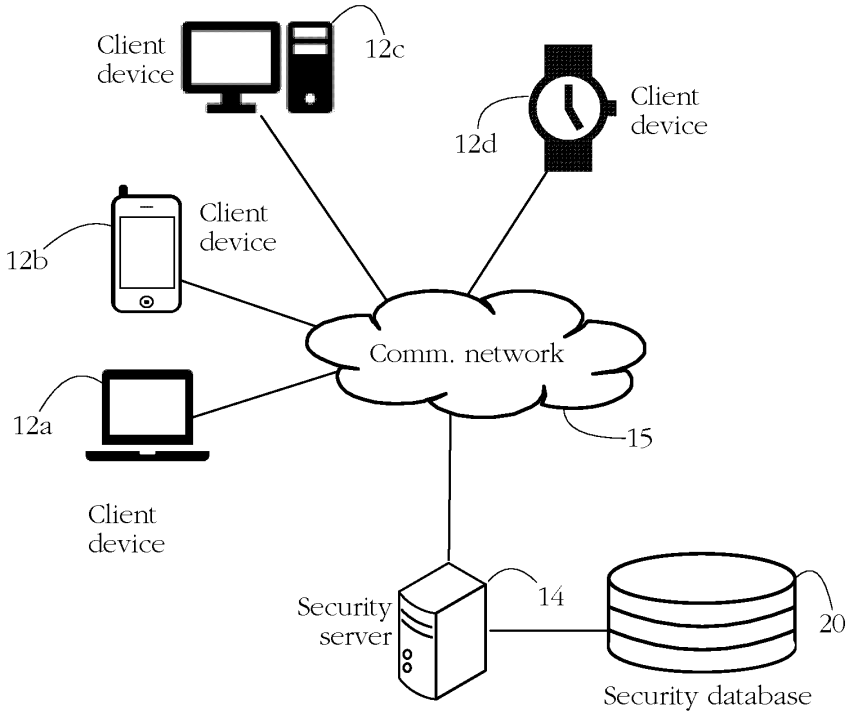
Client device
12c
Client device
12d
Client device
12b
Comm. network
12a
15
Client device
Security server
14
20
Security database

FIG. 1

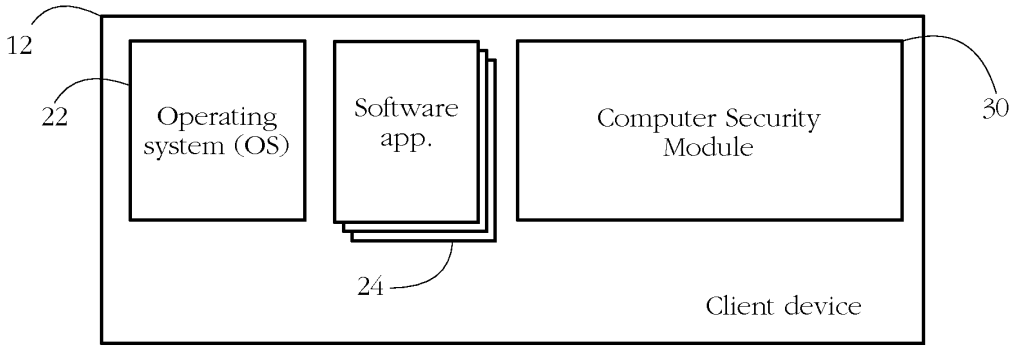
12
22
Operating system (OS)
Software app.
Computer Security Module
30
24
Client device

FIG. 2

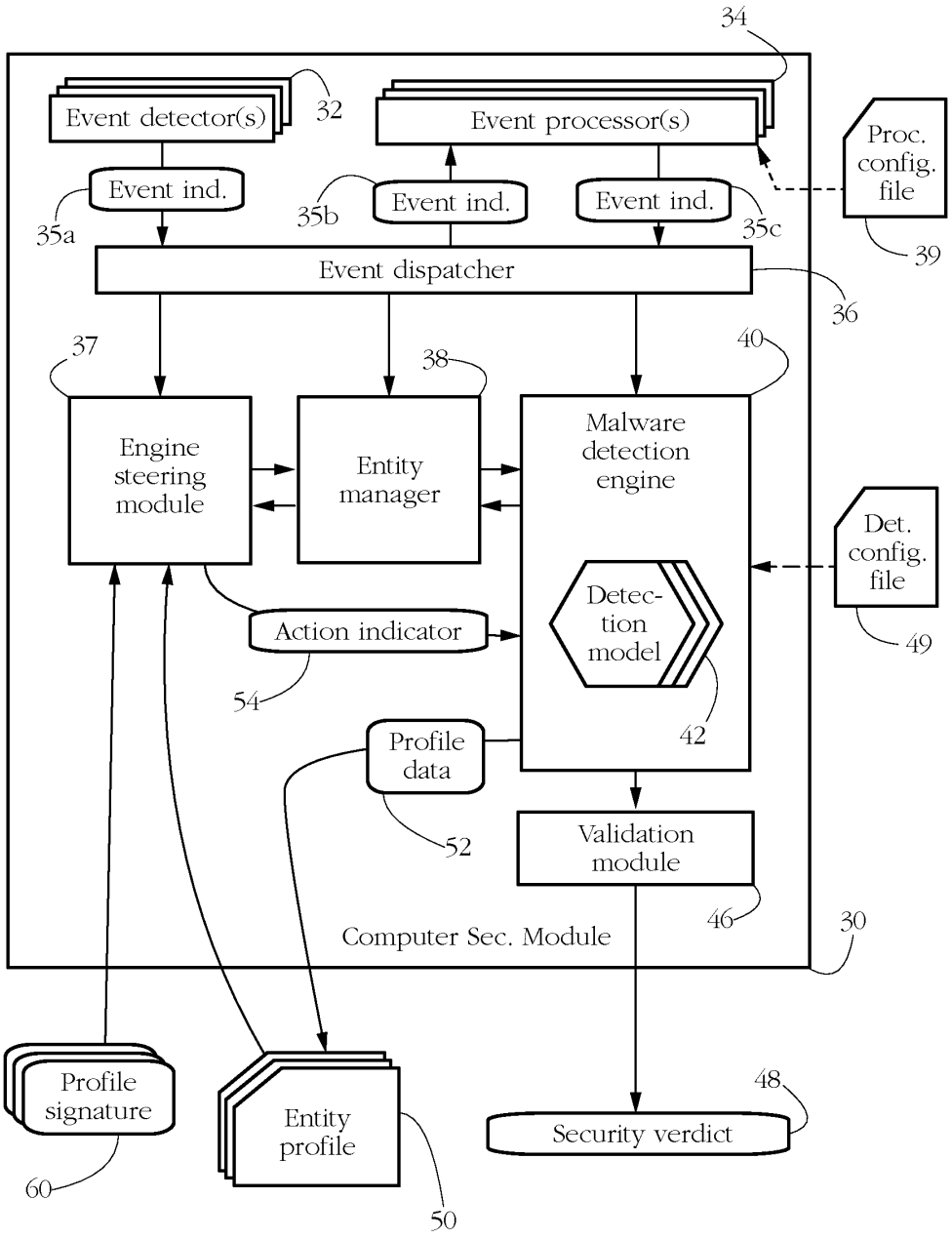
34
Event detector(s)
32
Event processor(s)
Proc. config. file
39
Event ind.
35a
Event ind.
35b
Event ind.
35c
Event dispatcher
36
37
38
40
Engine steering module
Entity manager
Malware detection engine
Det. config. file
49
Detec-tion model
42
Action indicator
54
Profile data
52
Validation module
46
Computer Sec. Module
30
Profile signature
60
Entity profile
50
48
Security verdict

FIG. 3

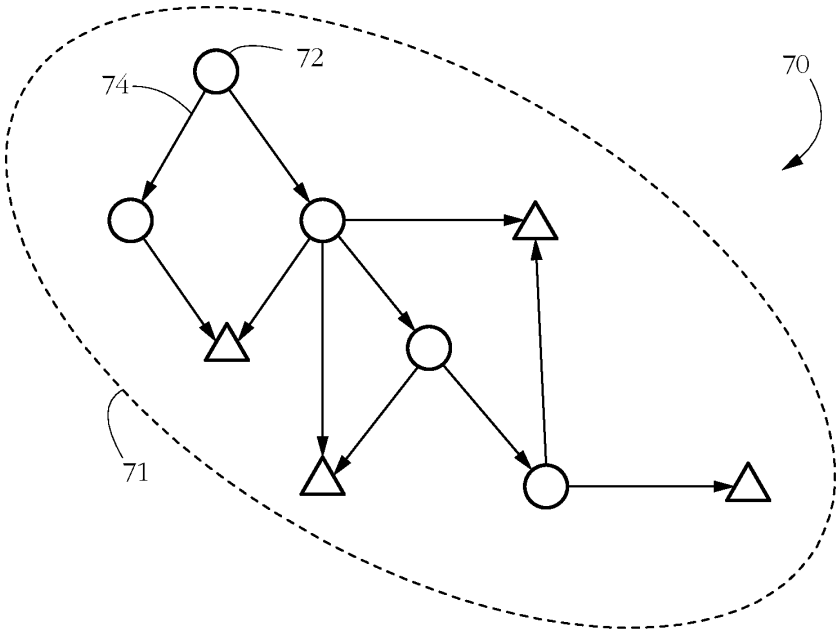


FIG. 4

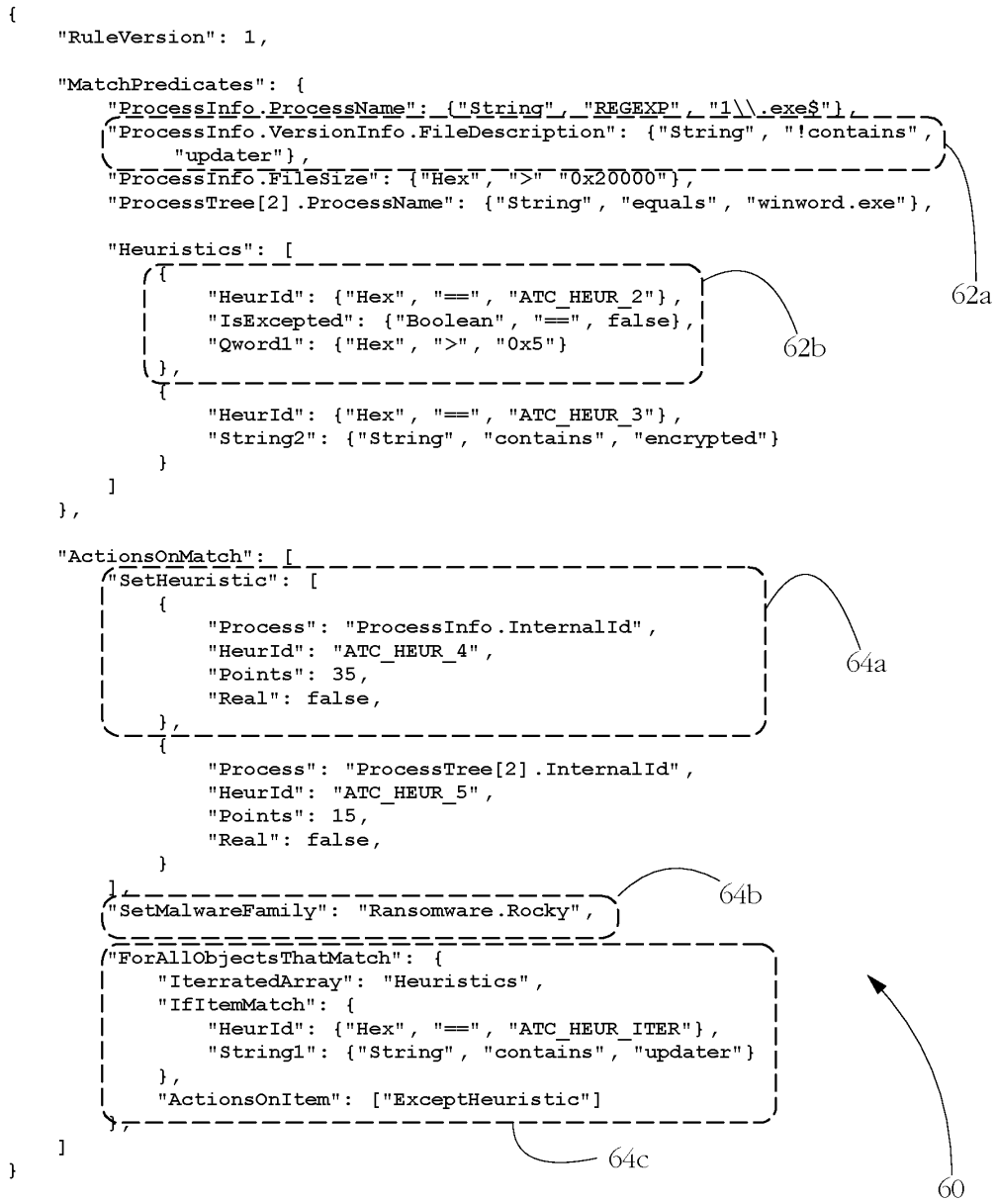
{
"RuleVersion": 1,
"MatchPredicates": {
"ProcessInfo.ProcessName": {"String", "REGEXP", "1\\.exe$"},
"ProcessInfo.VersionInfo.FileDescription": {"String", "!contains", "updater"},
"ProcessInfo.FileSize": {"Hex", ">" "0x20000"},
"ProcessTree[2].ProcessName": {"String", "equals", "winword.exe"},
"Heuristics": [
{
"HeurId": {"Hex", "==", "ATC_HEUR_2"},
"IsExcepted": {"Boolean", "==", false},
"Qword1": {"Hex", ">", "0x5"}
},
{
"HeurId": {"Hex", "==", "ATC_HEUR_3"},
"String2": {"String", "contains", "encrypted"}
}
]
},
"ActionsOnMatch": [
"SetHeuristic": [
{
"Process": "ProcessInfo.InternalId",
"HeurId": "ATC_HEUR_4",
"Points": 35,
"Real": false,
},
{
"Process": "ProcessTree[2].InternalId",
"HeurId": "ATC_HEUR_5",
"Points": 15,
"Real": false,
}
],
"SetMalwareFamily": "Ransomware.Rocky",
"ForAllObjectsThatMatch": {
"IterratedArray": "Heuristics",
"IfItemMatch": {
"HeurId": {"Hex", "==", "ATC_HEUR_ITER"},
"String1": {"String", "contains", "updater"}
},
"ActionsOnItem": ["ExceptHeuristic"]
},
]
}
62a
62b
64a
64b
64c
60

FIG. 5

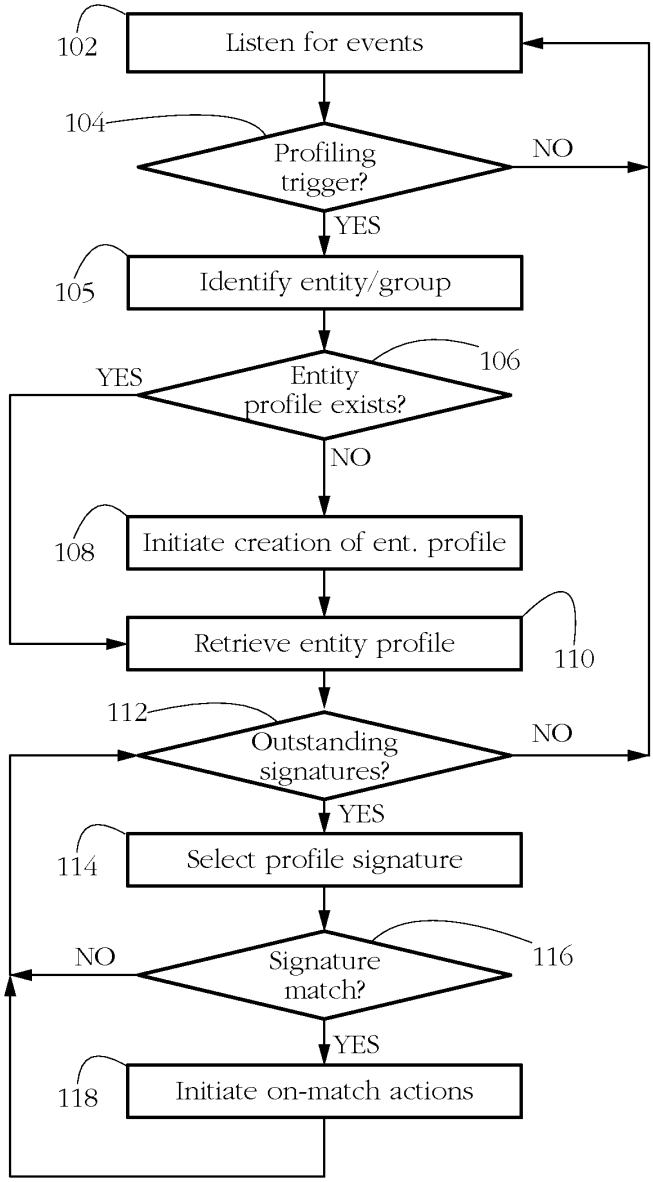
102
Listen for events
104
Profiling trigger?
NO
YES
105
Identify entity/group
106
Entity profile exists?
YES
NO
108
Initiate creation of ent. profile
Retrieve entity profile
110
112
Outstanding signatures?
NO
YES
114
Select profile signature
Signature match?
116
NO
YES
118
Initiate on-match actions

FIG. 6

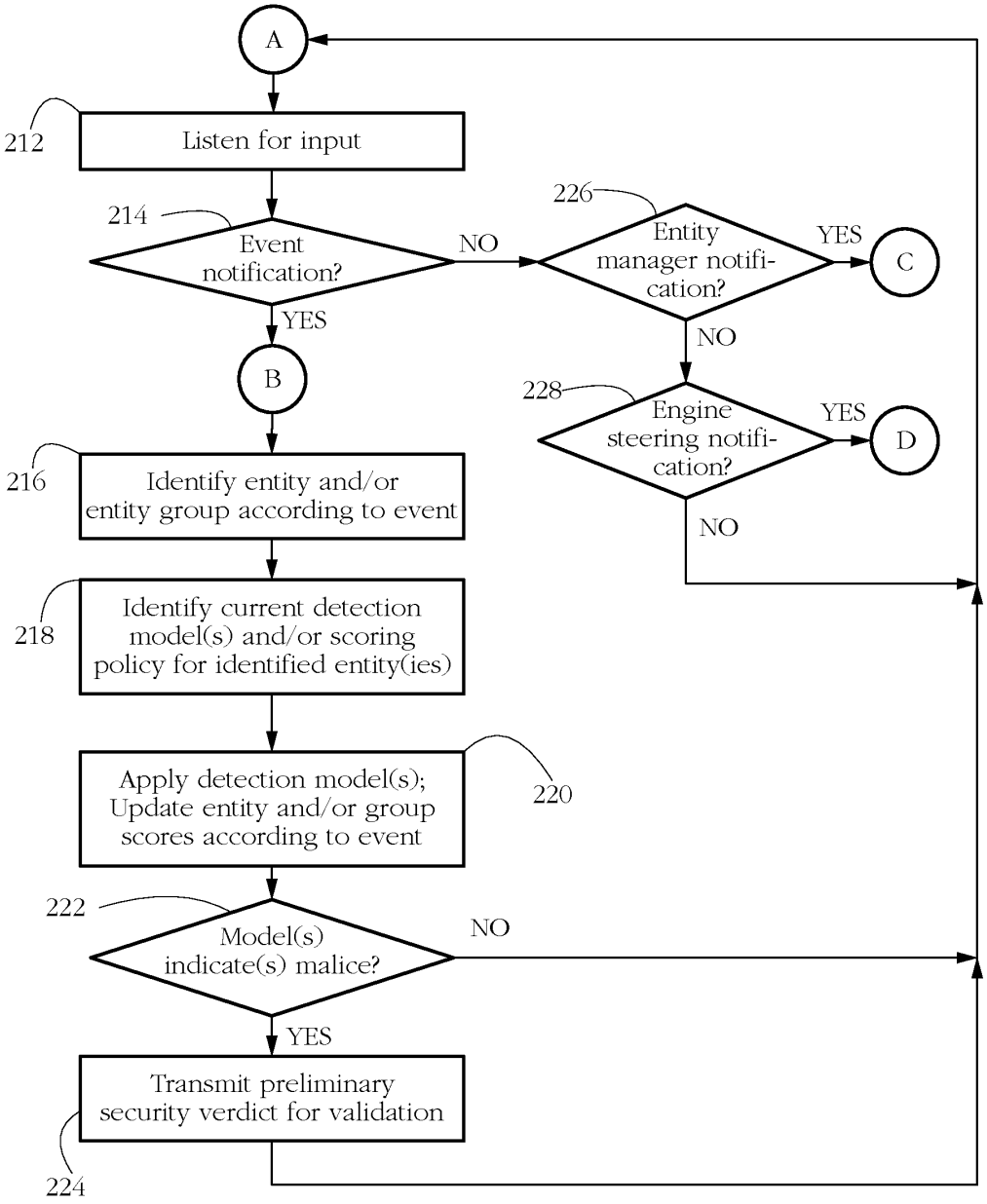
A
212
Listen for input
214
Event notification?
NO
226
Entity manager notifi-cation?
YES
C
YES
B
NO
228
Engine steering notifi-cation?
YES
D
NO
216
Identify entity and/or entity group according to event
218
Identify current detection model(s) and/or scoring policy for identified entity(ies)
Apply detection model(s); Update entity and/or group scores according to event
220
222
Model(s) indicate(s) malice?
NO
YES
Transmit preliminary security verdict for validation
224

FIG. 7-A

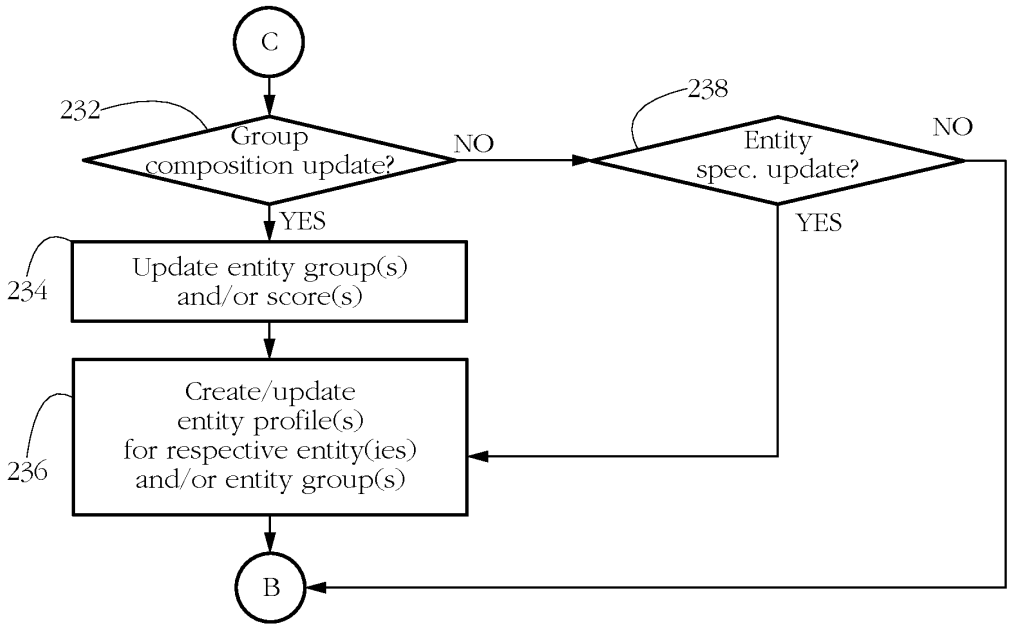
C
232
Group composition update?
NO
238
Entity spec. update?
NO
YES
YES
234
Update entity group(s) and/or score(s)
236
Create/update entity profile(s) for respective entity(ies) and/or entity group(s)
B

FIG. 7-B

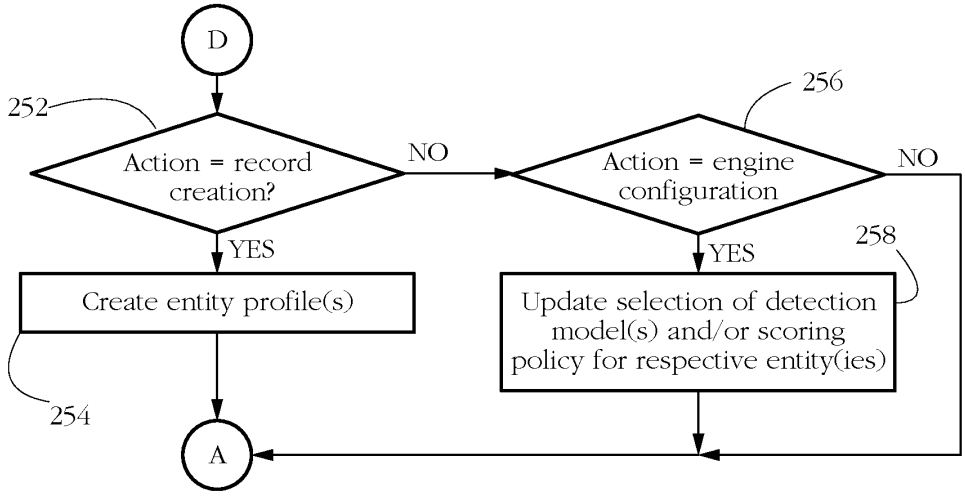
D
252
Action = record creation?
NO
256
Action = engine configuration
NO
YES
YES
258
Create entity profile(s)
Update selection of detection model(s) and/or scoring policy for respective entity(ies)
254
A

FIG. 7-C

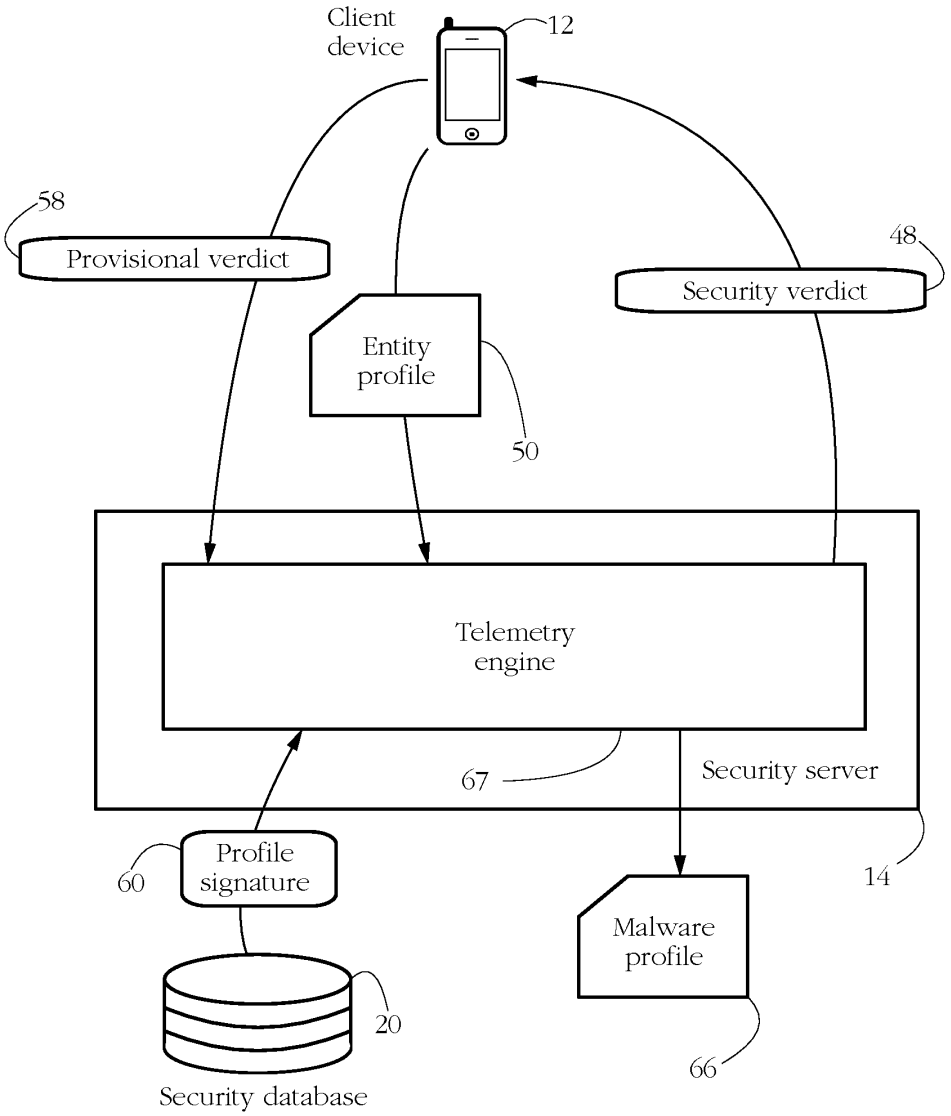
Client device
12
58
Provisional verdict
48
Security verdict
Entity profile
50
Telemetry engine
67
Security server
14
60
Profile signature
Malware profile
20
66
Security database

FIG. 8

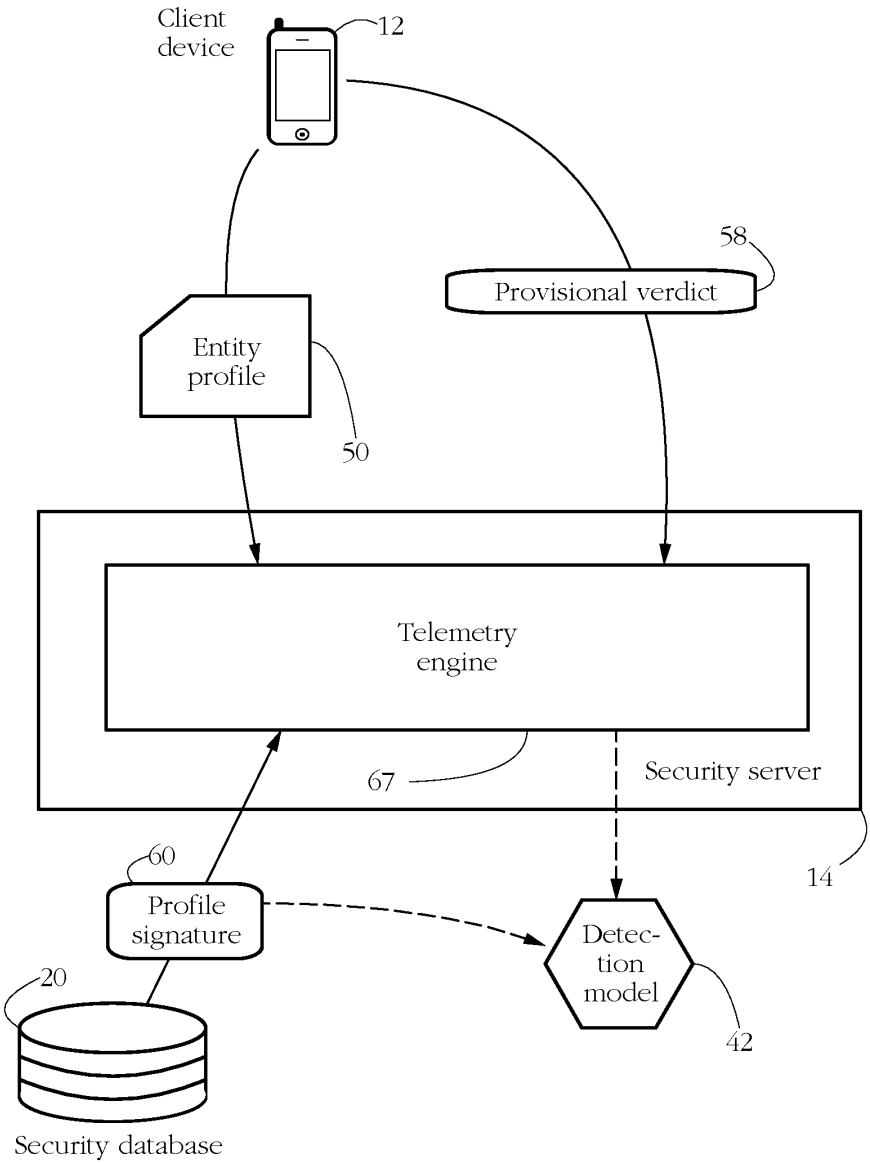
Client device
12
58
Provisional verdict
Entity profile
50
Telemetry engine
67
Security server
14
60
Profile signature
Detec-tion model
20
42
Security database

FIG. 9

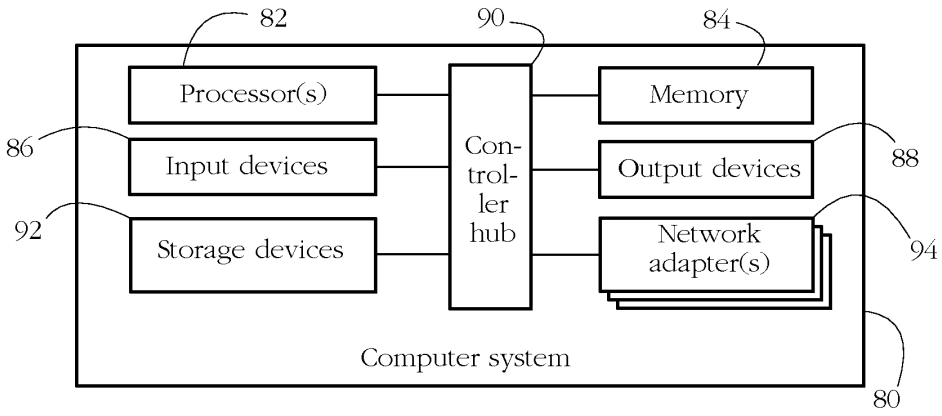
82
90
84
Processor(s)
Memory
86
Input devices
Con-
trol-
ler
hub
Output devices
88
92
Storage devices
Network
adapter(s)
94
Computer system
80

FIG. 10