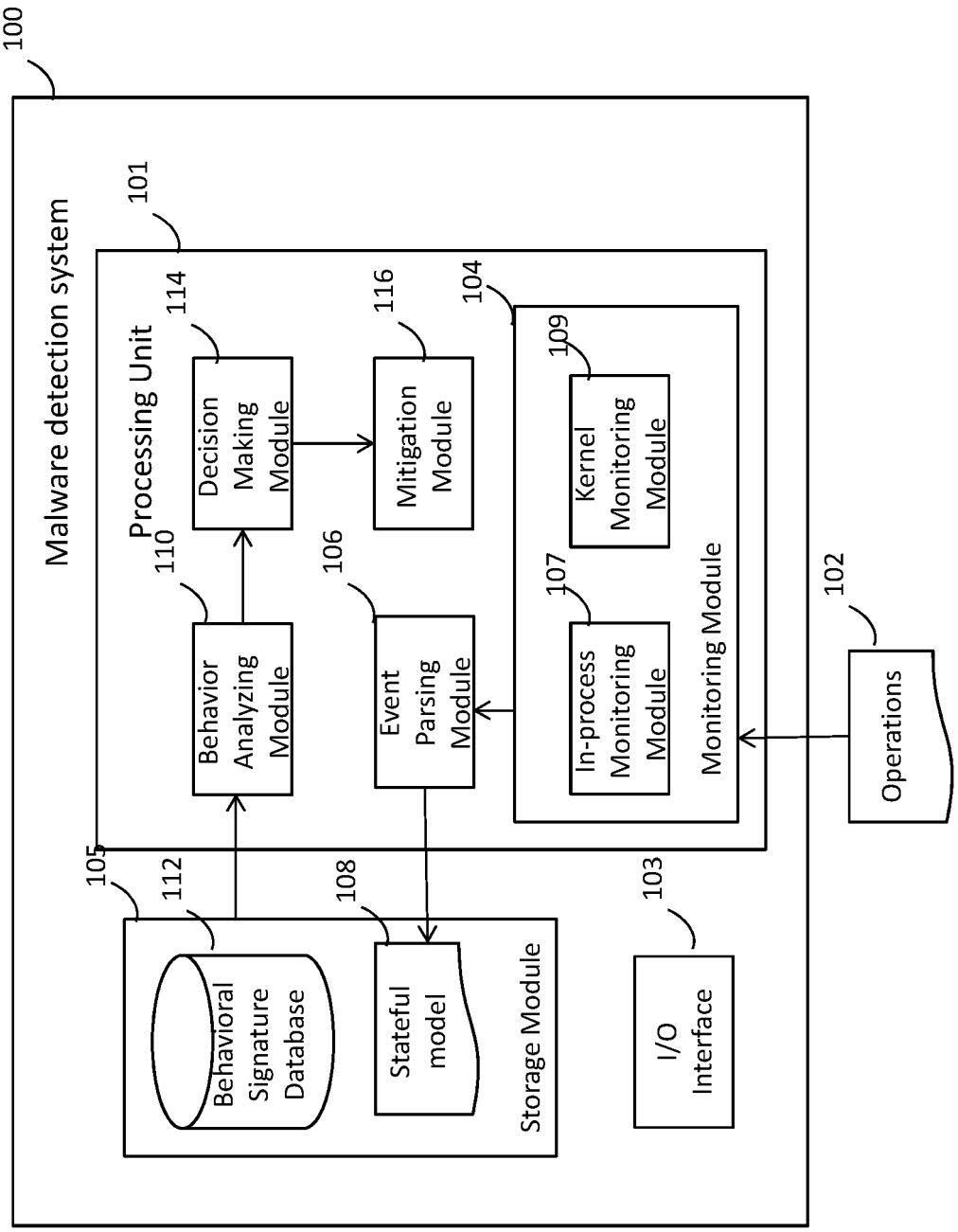
100
Malware detection system
101
Processing Unit
114
Decision Making Module
116
Mitigation Module
104
109
Kernel Monitoring Module
110
Behavior Analyzing Module
106
Event Parsing Module
107
In-process Monitoring Module
Monitoring Module
102
Operations
105
112
Behavioral Signature Database
108
Stateful model
Storage Module
103
I/O Interface

Fig. 1

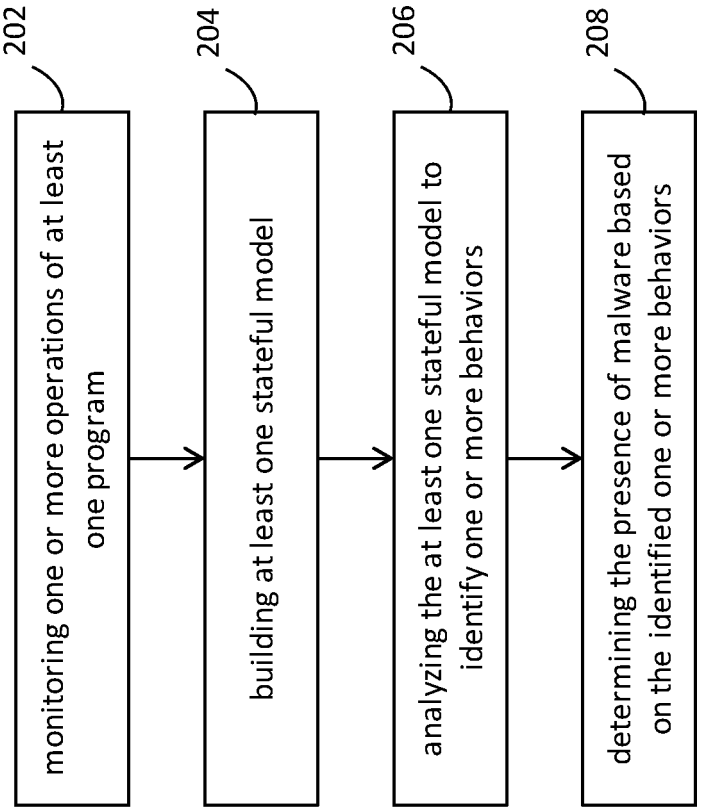
202
monitoring one or more operations of at least one program
204
building at least one stateful model
206
analyzing the at least one stateful model to identify one or more behaviors
208
determining the presence of malware based on the identified one or more behaviors

Fig. 2

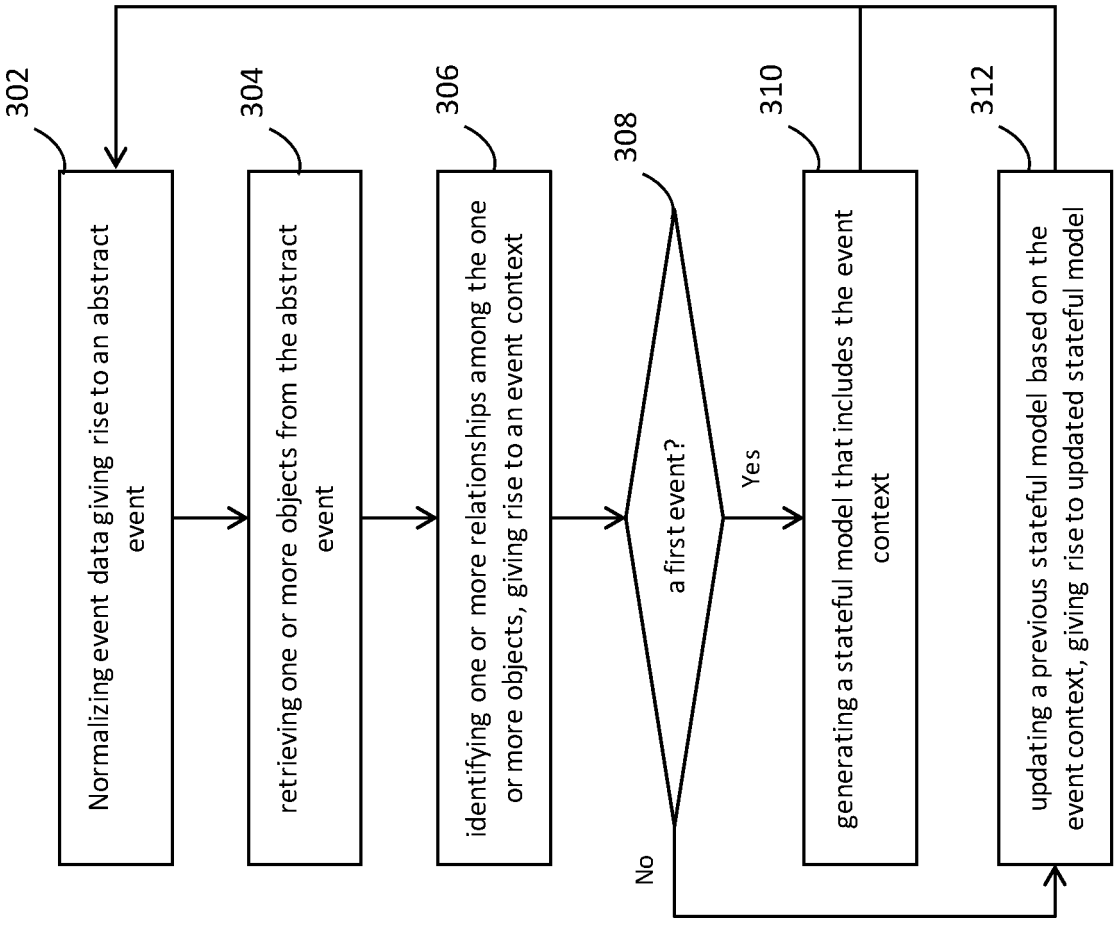
302
Normalizing event data giving rise to an abstract event
304
retrieving one or more objects from the abstract event
306
identifying one or more relationships among the one or more objects, giving rise to an event context
308
a first event?
Yes
No
310
generating a stateful model that includes the event context
312
updating a previous stateful model based on the event context, giving rise to updated stateful model

Fig. 3

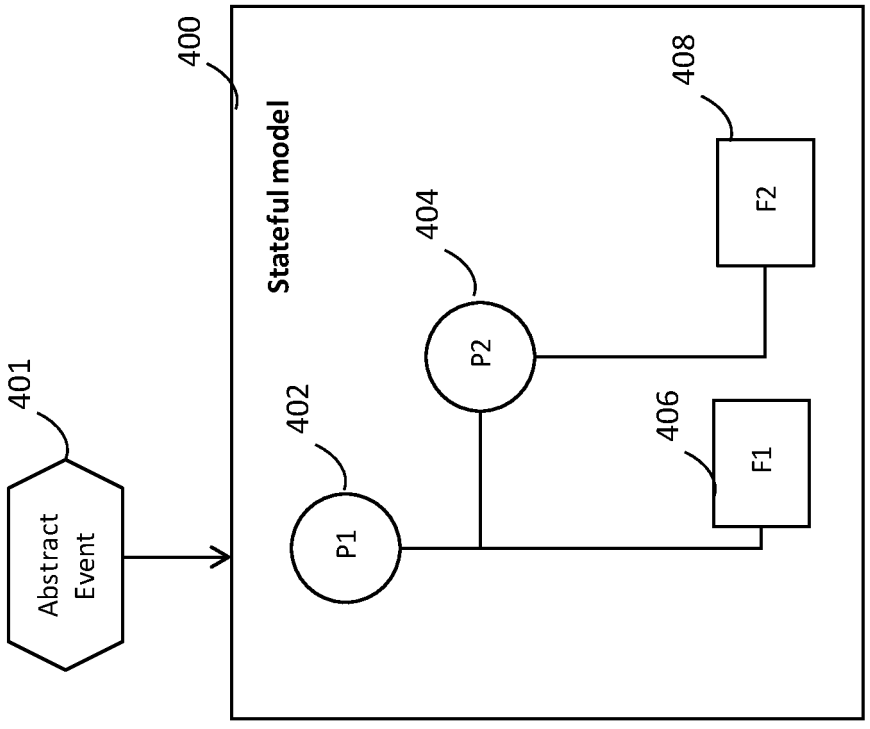
401
Abstract Event
400
Stateful model
402
P1
404
P2
406
F1
408
F2

Fig. 4a

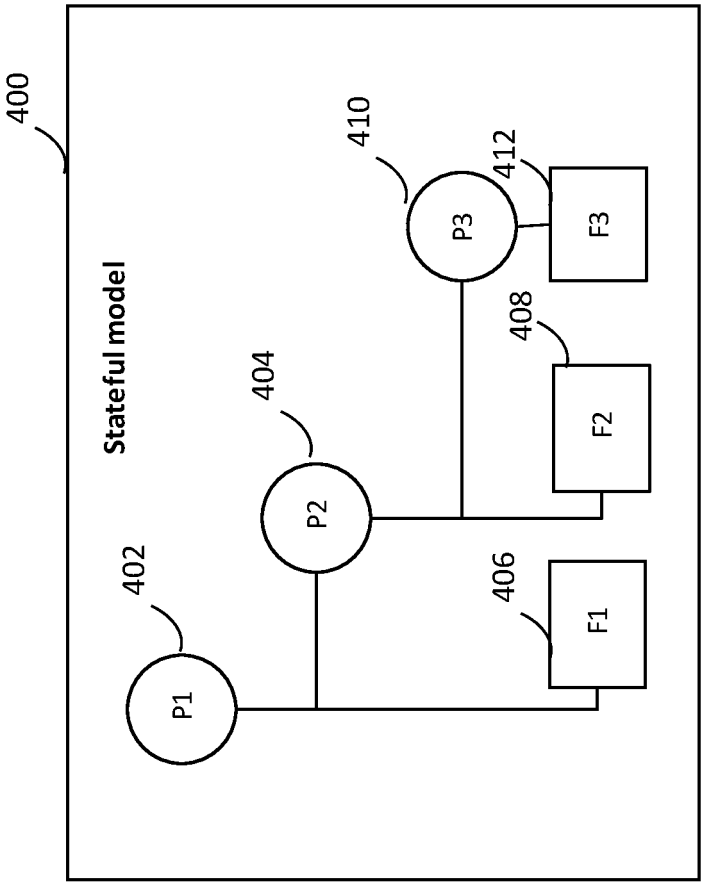
400
Stateful model
402
P1
404
P2
406
F1
408
F2
410
P3
412
F3

Fig. 4b

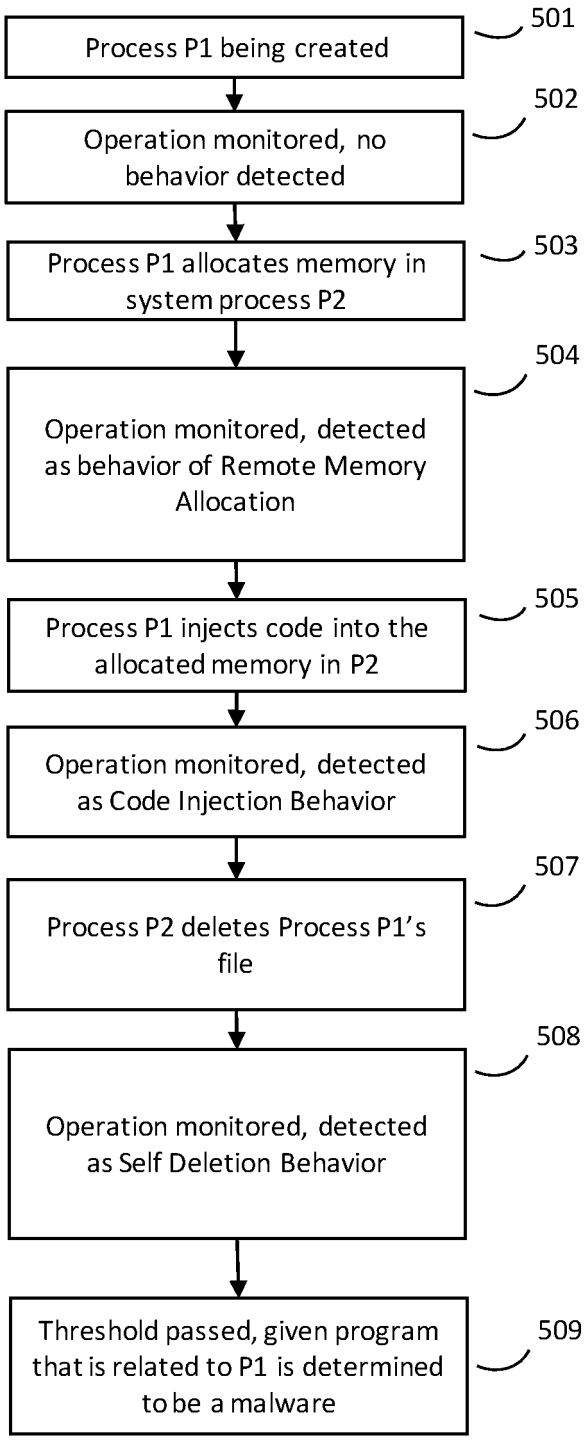
Process P1 being created
501
Operation monitored, no behavior detected
502
Process P1 allocates memory in system process P2
503
Operation monitored, detected as behavior of Remote Memory Allocation
504
Process P1 injects code into the allocated memory in P2
505
Operation monitored, detected as Code Injection Behavior
506
Process P2 deletes Process P1's file
507
Operation monitored, detected as Self Deletion Behavior
508
Threshold passed, given program that is related to P1 is determined to be a malware
509

Fig. 5