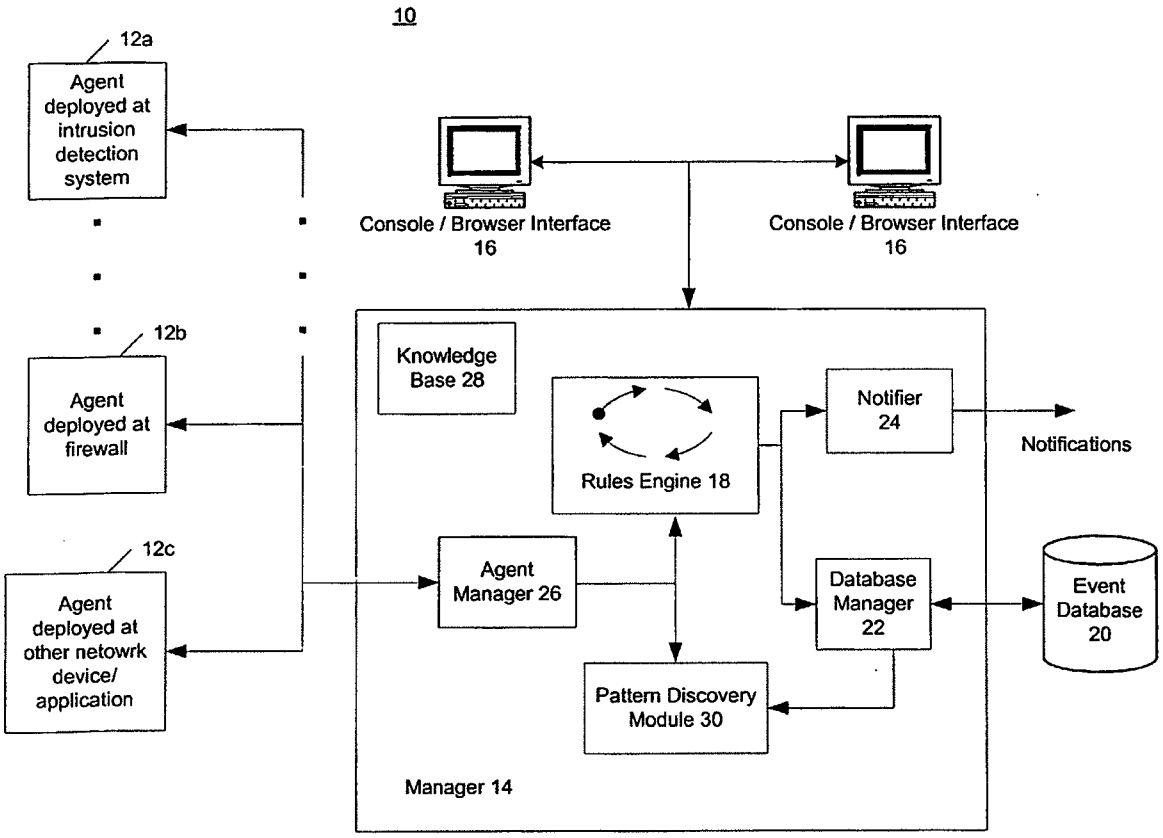

10
12a
Agent deployed at intrusion detection system
12b
Agent deployed at firewall
12c
Agent deployed at other netowrk device/ application
Console / Browser Interface 16
Console / Browser Interface 16
Knowledge Base 28
Rules Engine 18
Notifier 24
Notifications
Agent Manager 26
Database Manager 22
Event Database 20
Pattern Discovery Module 30
Manager 14

Figure 1

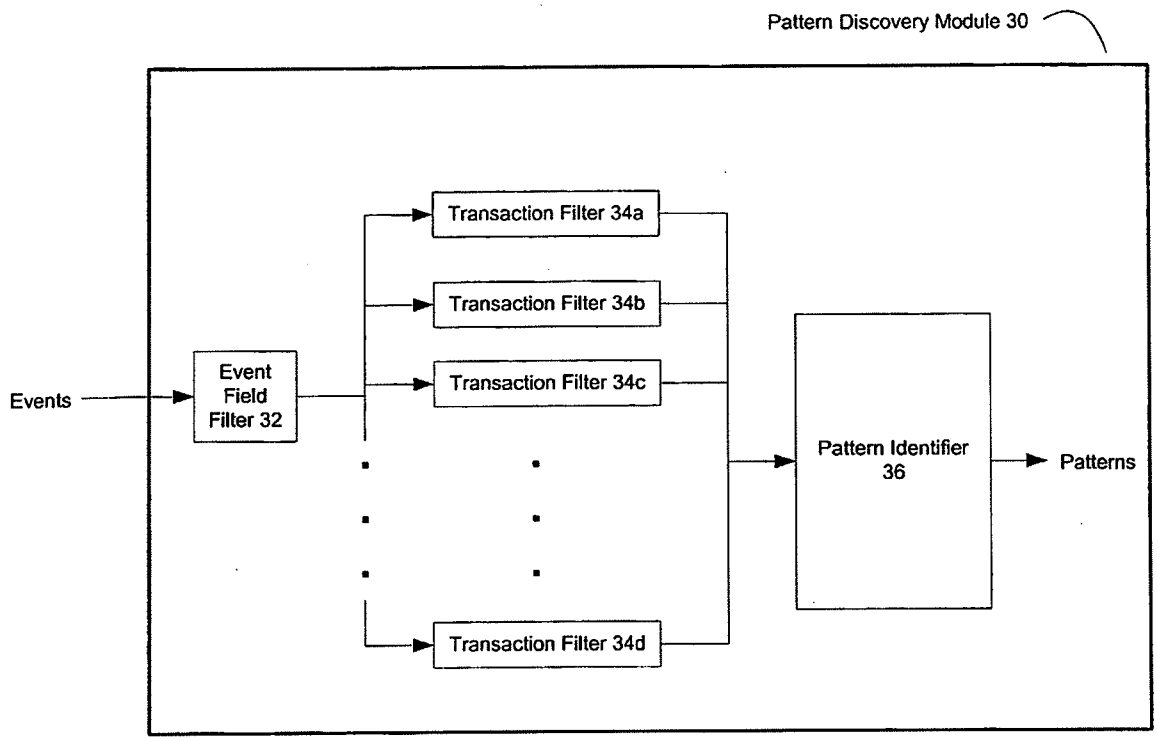

Pattern Discovery Module 30
Events
Event Field Filter 32
Transaction Filter 34a
Transaction Filter 34b
Transaction Filter 34c
Transaction Filter 34d
Pattern Identifier 36
Patterns

Figure 2

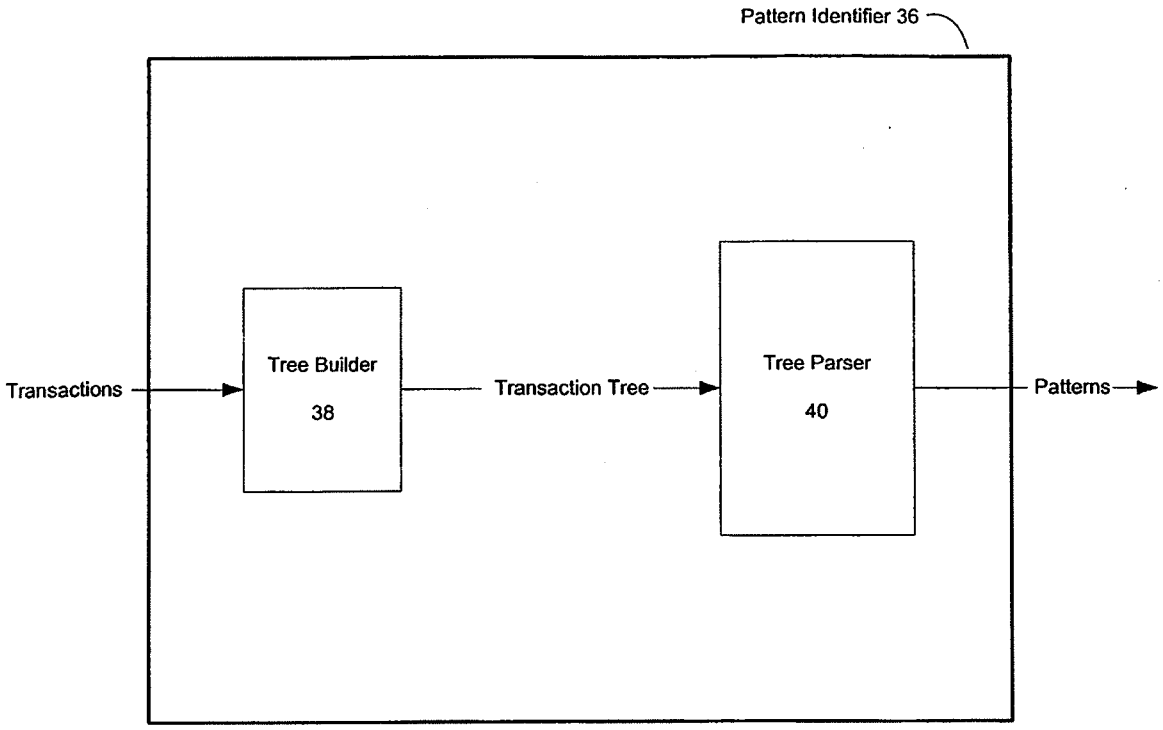

Pattern Identifier 36
Transactions
Tree Builder
38
Transaction Tree
Tree Parser
40
Patterns

Figure 3

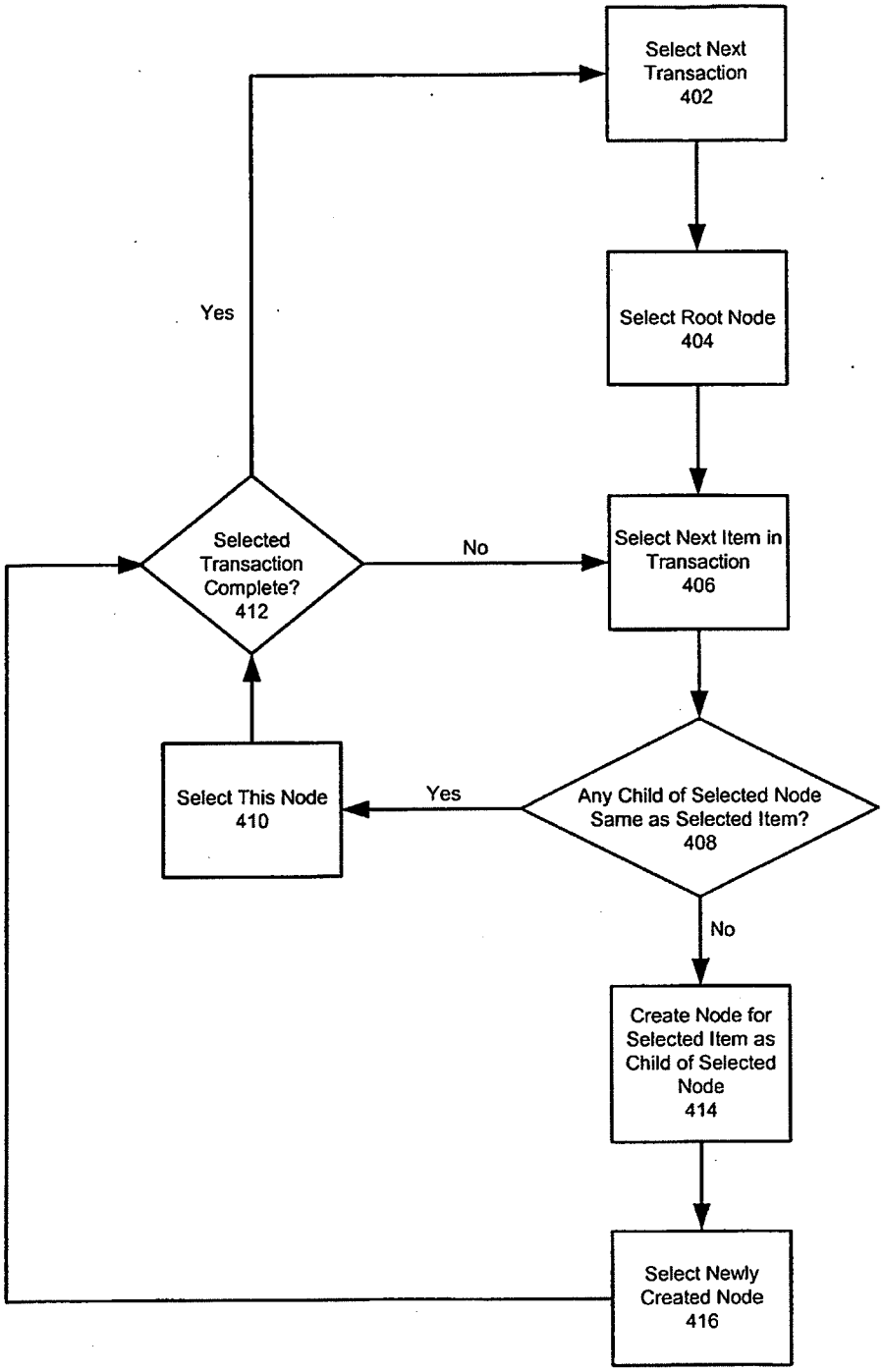

Select Next Transaction 402
Select Root Node 404
Select Next Item in Transaction 406
Any Child of Selected Node Same as Selected Item? 408
Yes
No
Create Node for Selected Item as Child of Selected Node 414
Select Newly Created Node 416
Selected Transaction Complete? 412
No
Yes
Select This Node 410
Yes

Figure 4