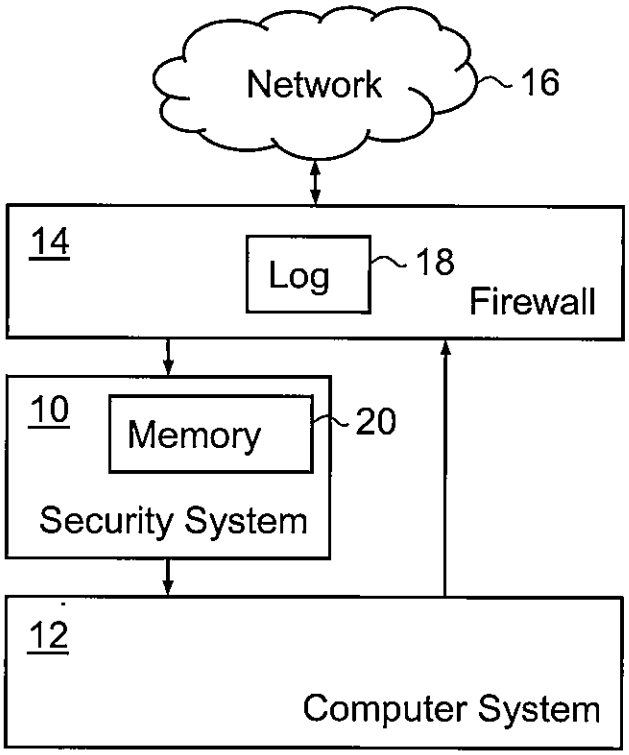
Network
16
14
Log
18
Firewall
10
Memory
20
Security System
12
Computer System

Figure 1

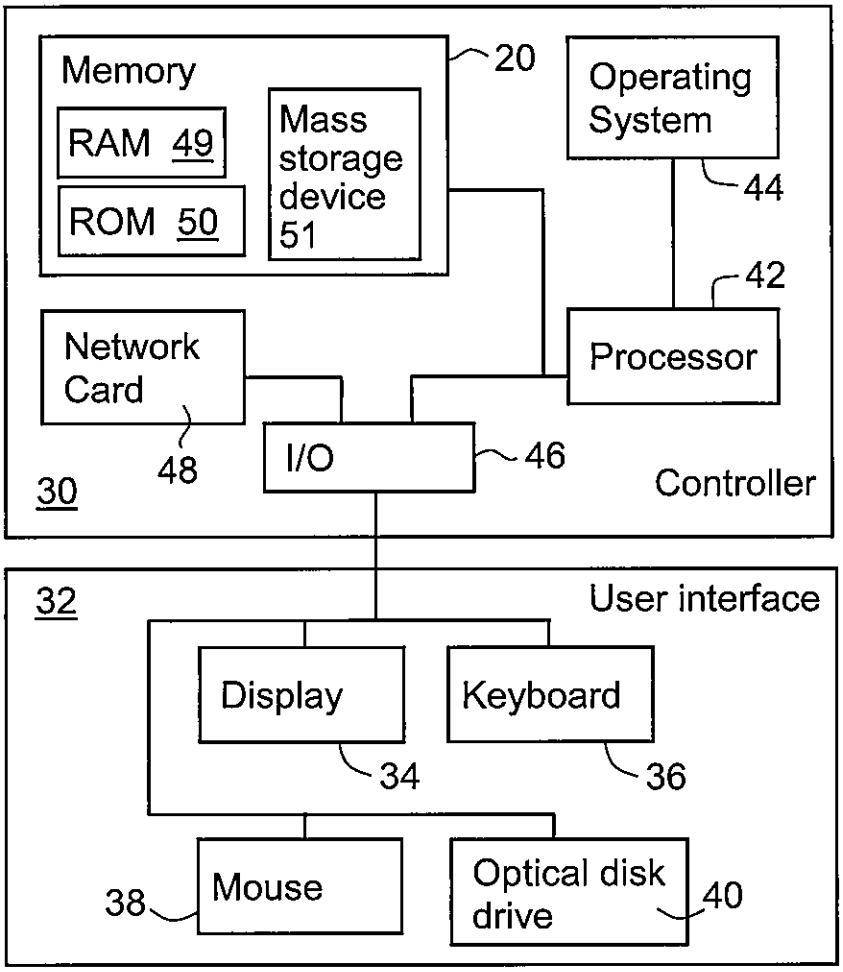
Memory
RAM 49
ROM 50
Mass storage device 51
20
Operating System
44
42
Network Card
48
Processor
I/O
46
30
Controller
32
User interface
Display
Keyboard
34
36
38
Mouse
Optical disk drive
40

Figure 2

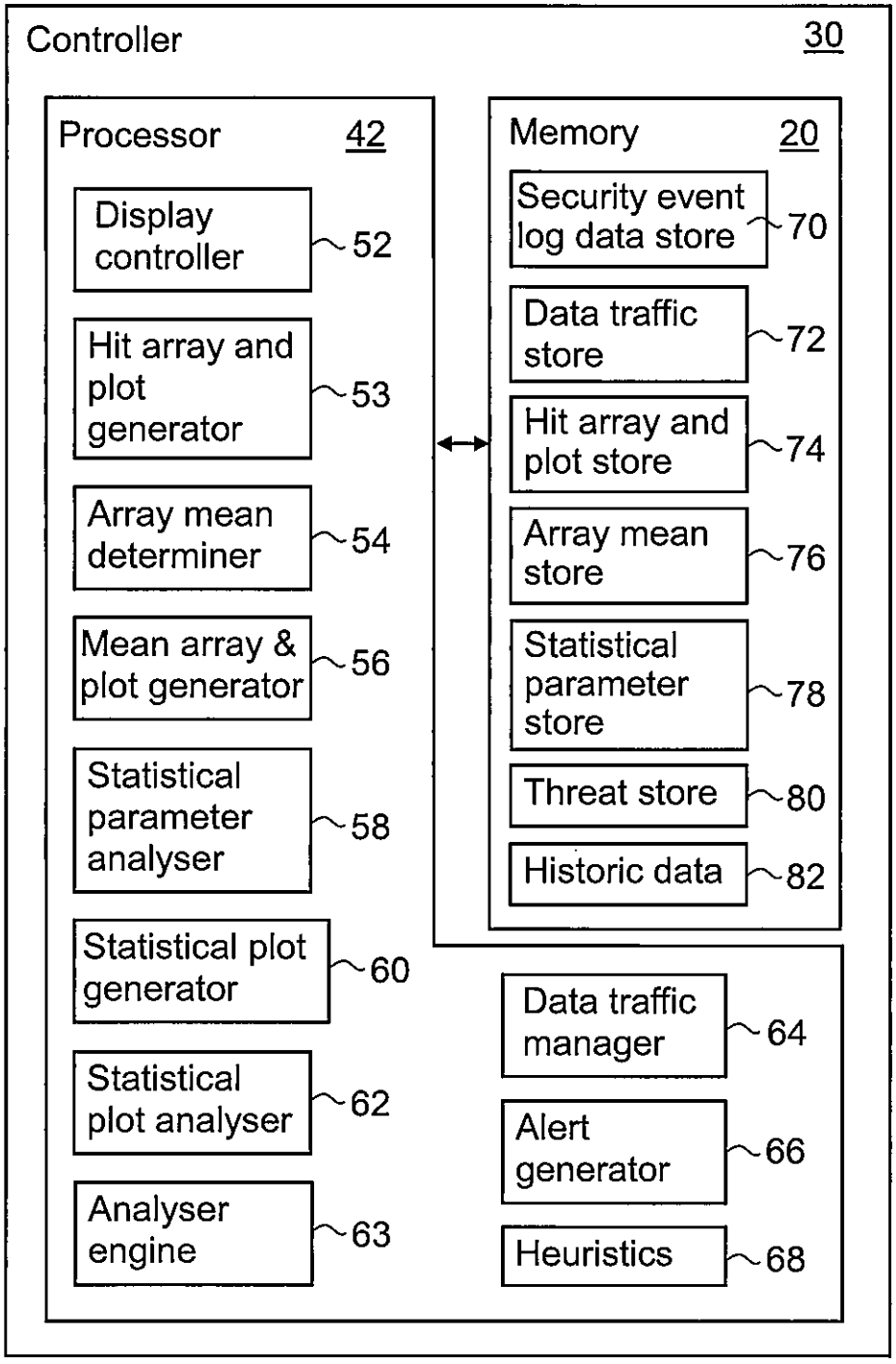
Controller
30
Processor
42
Display controller
52
Hit array and plot generator
53
Array mean determiner
54
Mean array & plot generator
56
Statistical parameter analyser
58
Statistical plot generator
60
Statistical plot analyser
62
Analyser engine
63
Memory
20
Security event log data store
70
Data traffic store
72
Hit array and plot store
74
Array mean store
76
Statistical parameter store
78
Threat store
80
Historic data
82
Data traffic manager
64
Alert generator
66
Heuristics
68

Figure 3

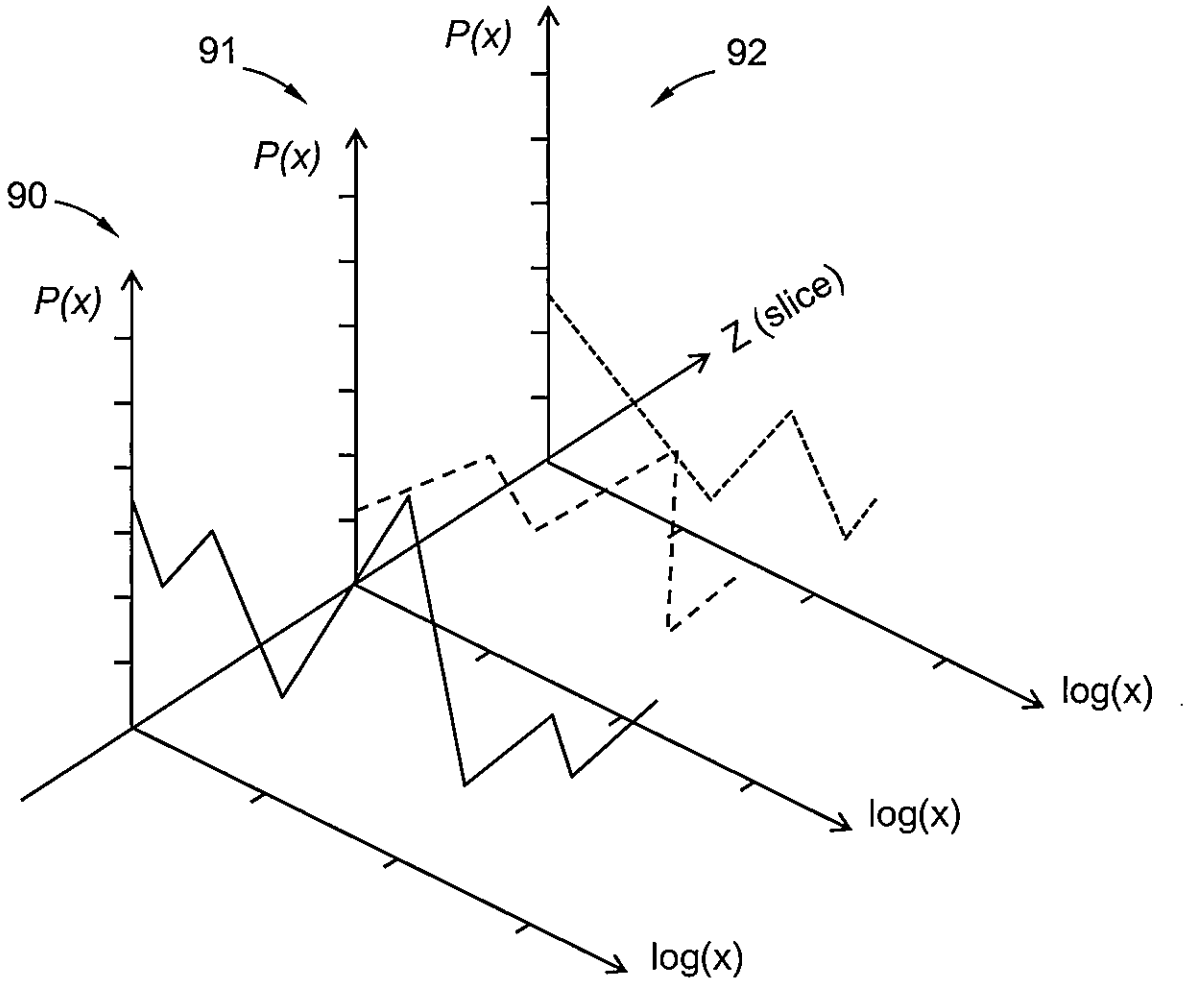


Figure 4

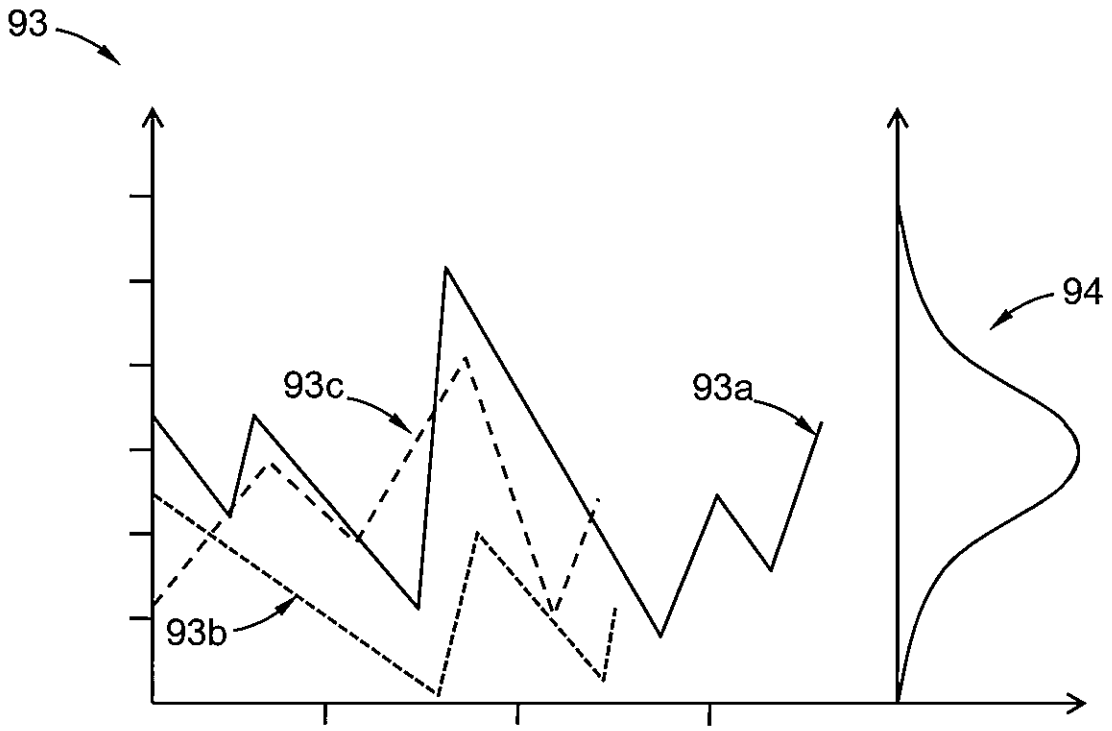


Figure 5

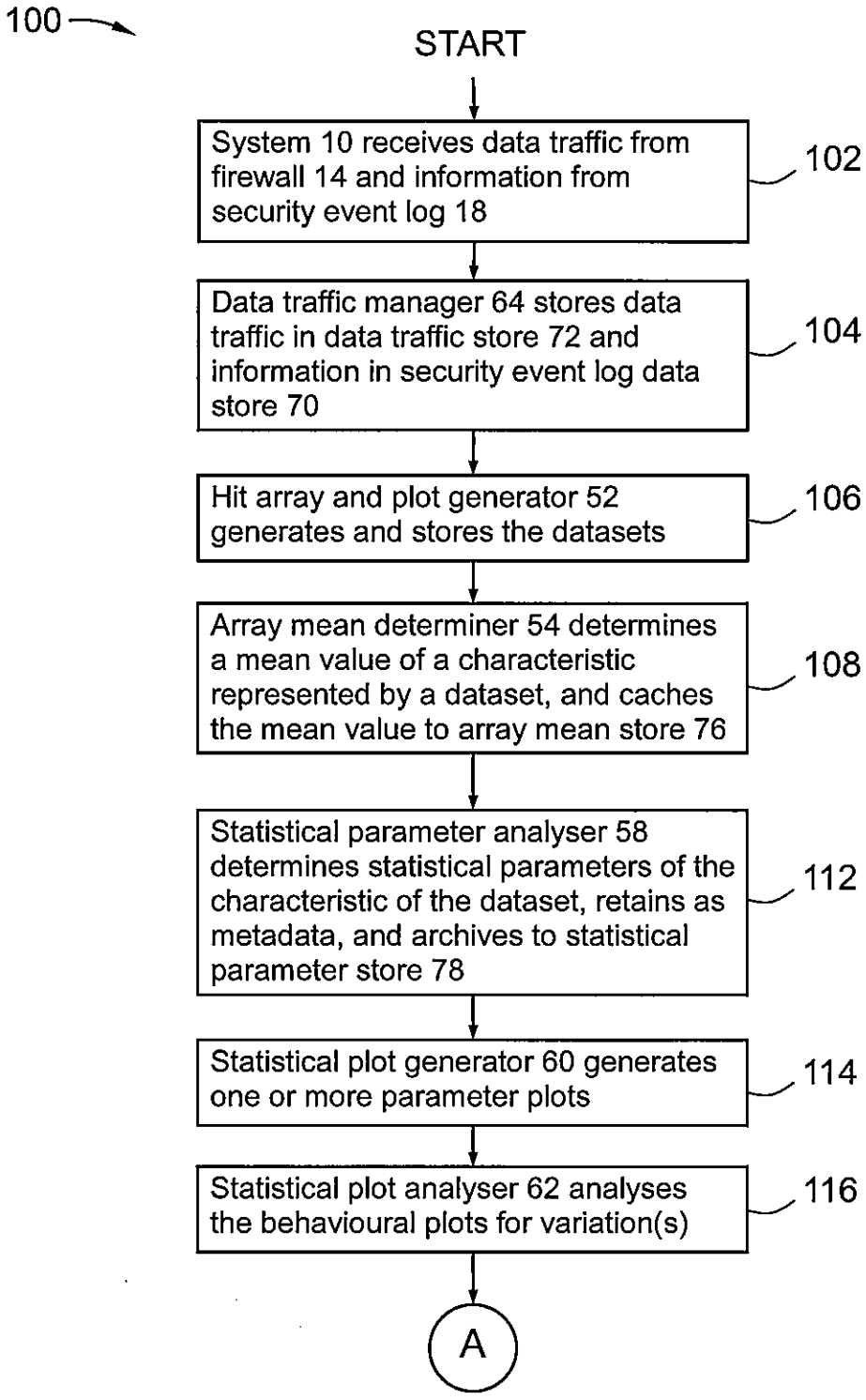
100
START
System 10 receives data traffic from firewall 14 and information from security event log 18
102
Data traffic manager 64 stores data traffic in data traffic store 72 and information in security event log data store 70
104
Hit array and plot generator 52 generates and stores the datasets
106
Array mean determiner 54 determines a mean value of a characteristic represented by a dataset, and caches the mean value to array mean store 76
108
Statistical parameter analyser 58 determines statistical parameters of the characteristic of the dataset, retains as metadata, and archives to statistical parameter store 78
112
Statistical plot generator 60 generates one or more parameter plots
114
Statistical plot analyser 62 analyses the behavioural plots for variation(s)
116
A

Figure 6A

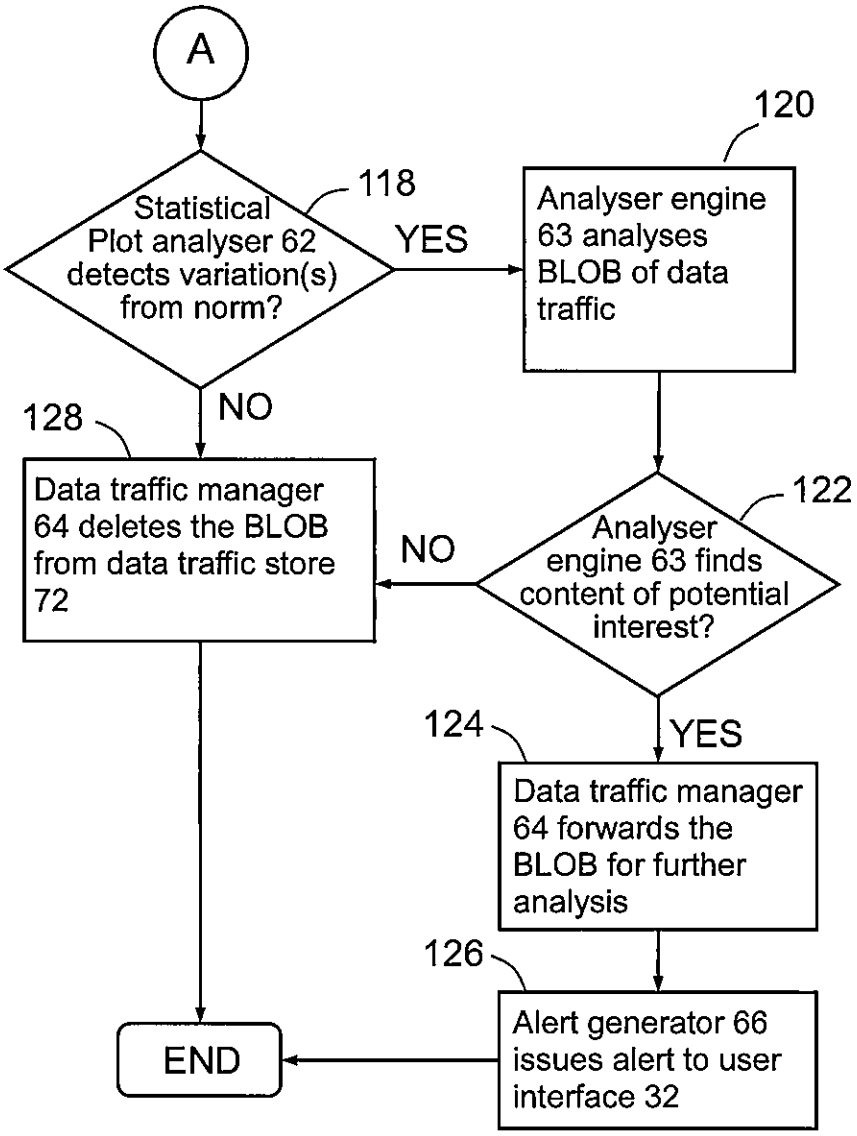
A
118
Statistical Plot analyser 62 detects variation(s) from norm?
YES
120
Analyser engine 63 analyses BLOB of data traffic
NO
128
Data traffic manager 64 deletes the BLOB from data traffic store 72
NO
122
Analyser engine 63 finds content of potential interest?
YES
124
Data traffic manager 64 forwards the BLOB for further analysis
126
Alert generator 66 issues alert to user interface 32
END

Figure 6B