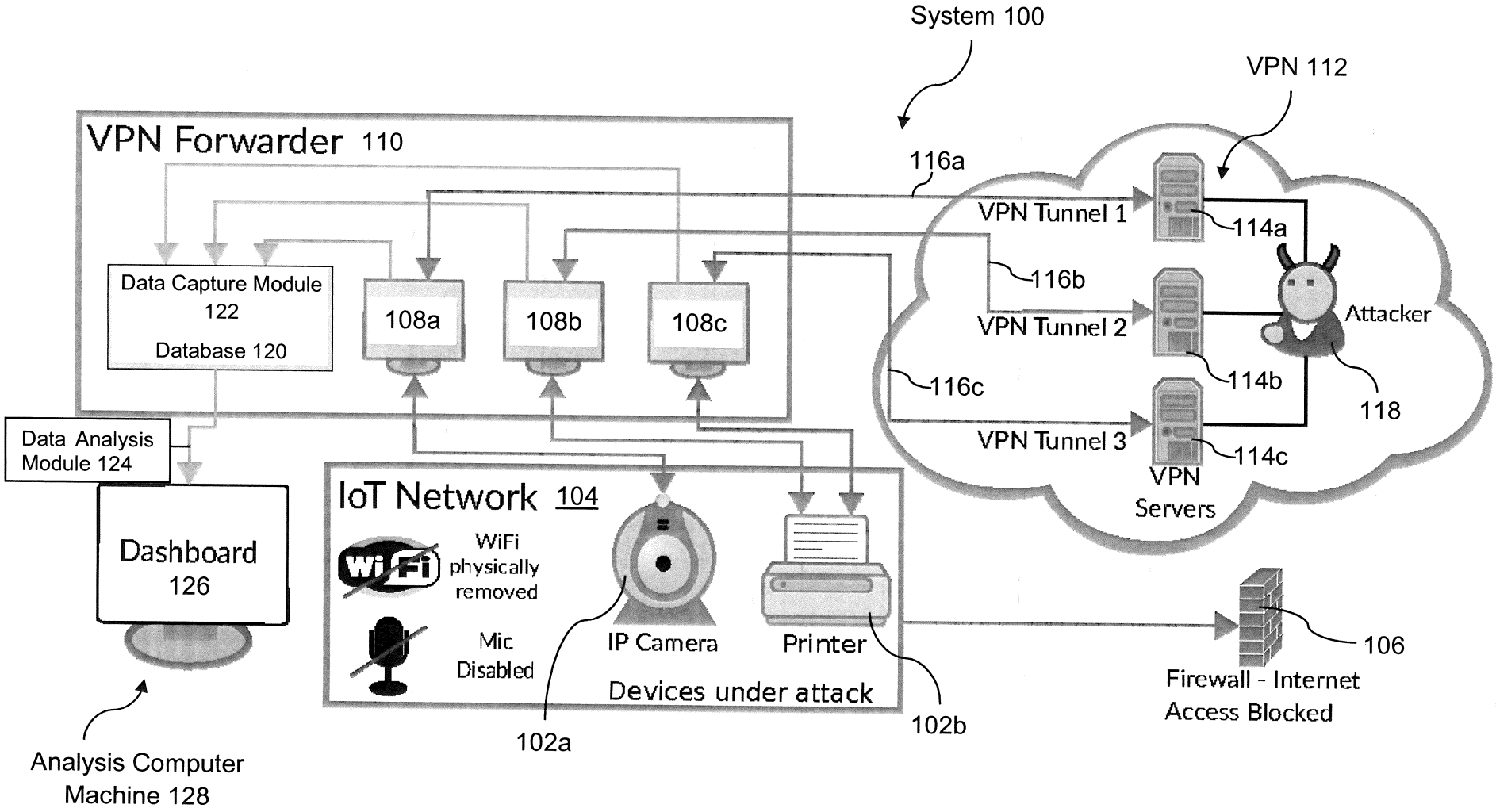

System 100
VPN 112
VPN Forwarder 110
116a
VPN Tunnel 1
114a
116b
VPN Tunnel 2
114b
Attacker
118
116c
VPN Tunnel 3
114c
VPN Servers
Data Capture Module 122
Database 120
108a
108b
108c
Data Analysis Module 124
Dashboard 126
IoT Network 104
WiFi physically removed
Mic Disabled
IP Camera
Printer
Devices under attack
102a
102b
106
Firewall - Internet Access Blocked
Analysis Computer Machine 128

Figure 1

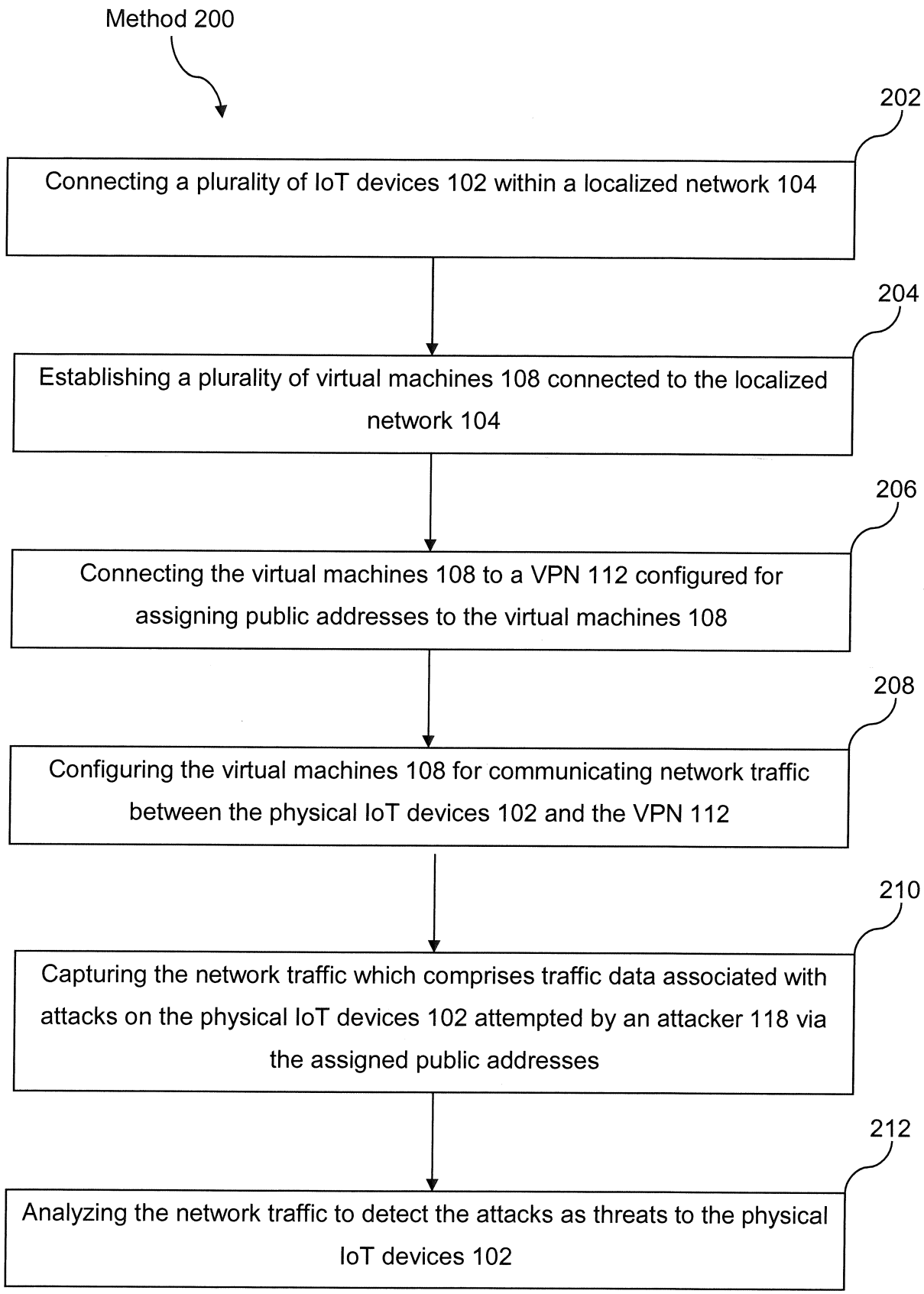

Method 200
202
Connecting a plurality of IoT devices 102 within a localized network 104
204
Establishing a plurality of virtual machines 108 connected to the localized network 104
206
Connecting the virtual machines 108 to a VPN 112 configured for assigning public addresses to the virtual machines 108
208
Configuring the virtual machines 108 for communicating network traffic between the physical IoT devices 102 and the VPN 112
210
Capturing the network traffic which comprises traffic data associated with attacks on the physical IoT devices 102 attempted by an attacker 118 via the assigned public addresses
212
Analyzing the network traffic to detect the attacks as threats to the physical IoT devices 102

Figure 2

Table 300

IoT Device Class	Brand	Model	Vulnerabilities	Password Difficulty Level
IP Camera	D-Link	DCS-942L	CVE-2017-7852	Default
IP Camera	D-Link	DCS-942L	CVE-2017-7852	Default
IP Camera	Vstarcam	C7837	CVE-2017-5674	Default
IP Camera	Aztech	WIPC409HD	CVE-2017-9765	Default
IP Camera	Trendnet	TV-IP762IC	-	Easy
IP Camera	Trendnet	TV-IP410	Yes	Difficult
IP Camera	Sineoji	PT528V	CVE-2017-9765	Difficult
Printer	HP	6830	-	Default
Router	D-Link	DIR-615	CVE-2017-7404	Easy
SmartThings Hub	Samsung	STH-ETH-200	Yes	Default
Smart Plug	Belkin	-	Yes	Default
Motion Sensor	Belkin	-	Yes	Default

Figure 3

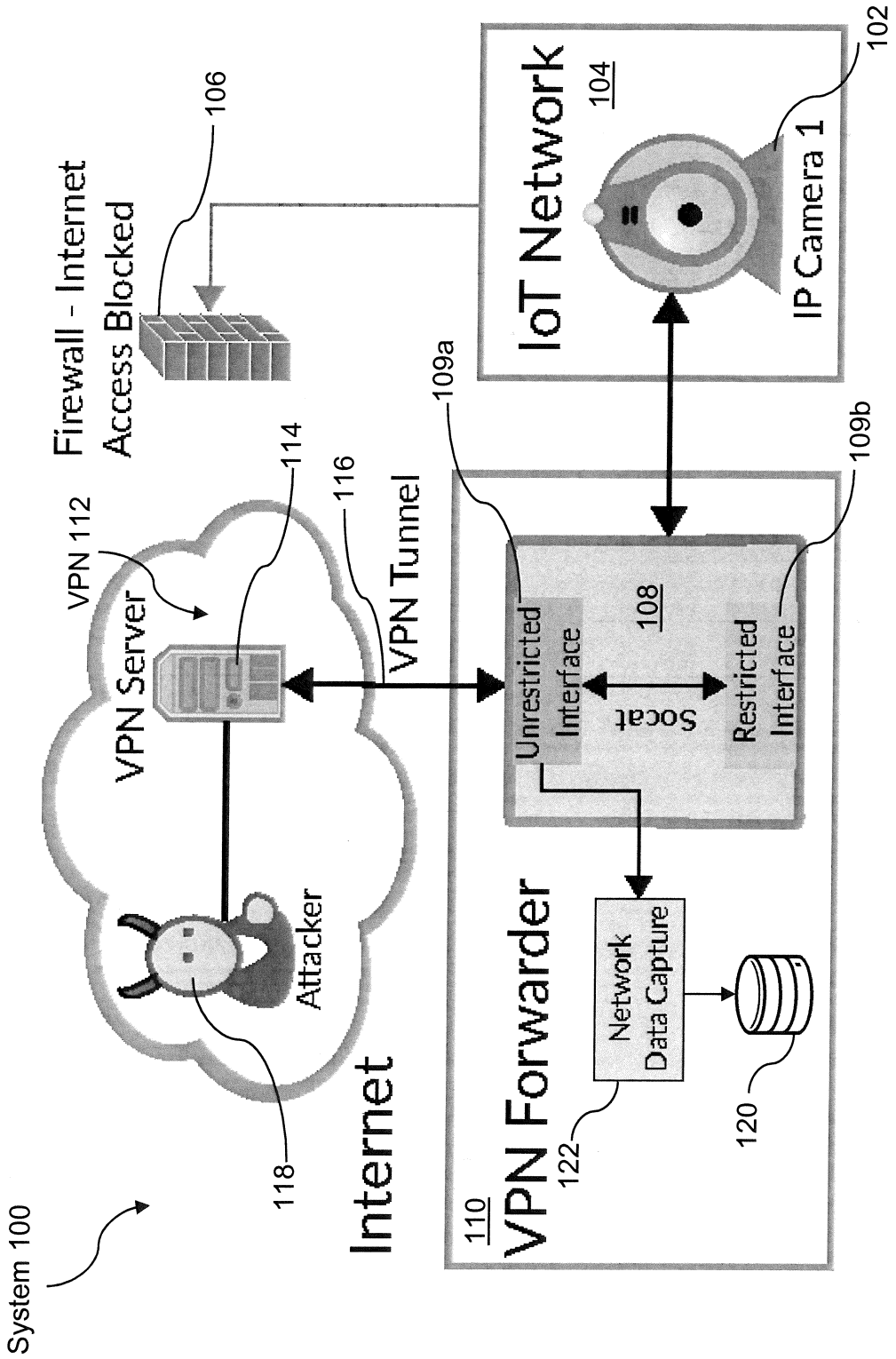

System 100
Internet
VPN Server
VPN 112
Attacker
118
114
116
VPN Tunnel
Firewall - Internet
Access Blocked
106
IoT Network
104
IP Camera 1
102
109a
109b
VPN Forwarder
110
Unrestricted
Interface
108
Socat
Restricted
Interface
Network
Data Capture
122
120

Figure 4

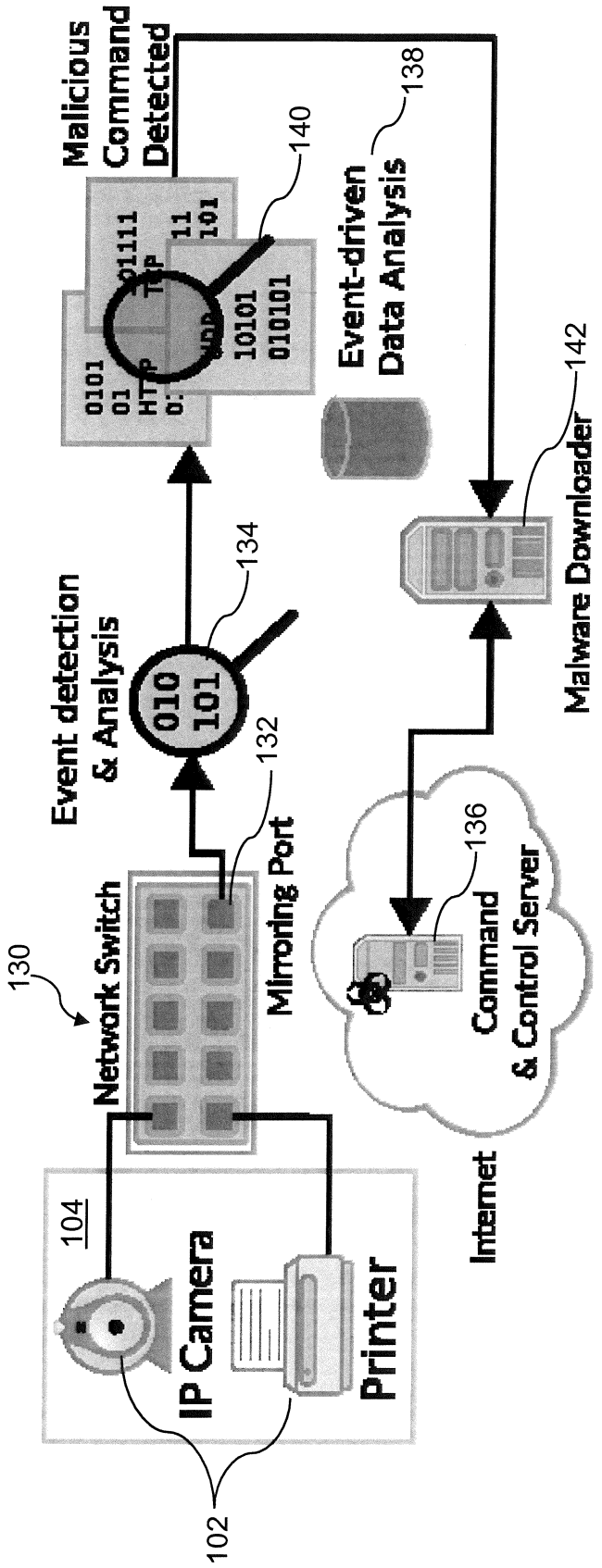

Malicious Command Detected
Event-driven Data Analysis
138
140
142
Malware Downloader
Event detection & Analysis
134
010 101
132
Mirroring Port
130
Network Switch
Internet
136
Command & Control Server
104
IP Camera
Printer
102

Figure 5A

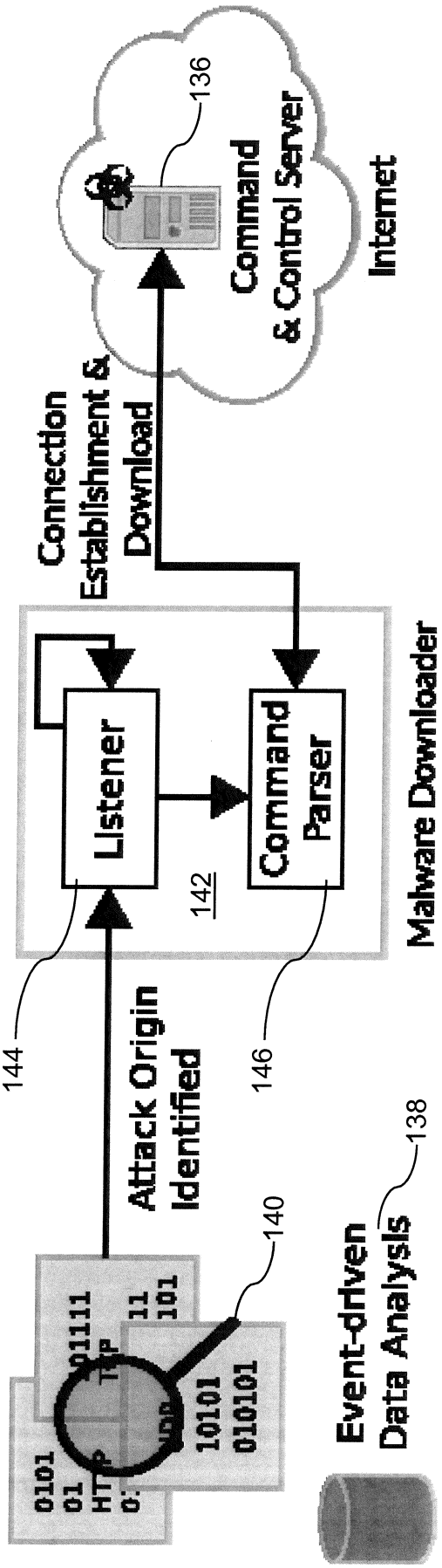

Internet
Command & Control Server
136
Connection Establishment & Download
Malware Downloader
Listener
Command Parser
142
144
146
Attack Origin Identified
140
Event-driven Data Analysis
138

Figure 5B

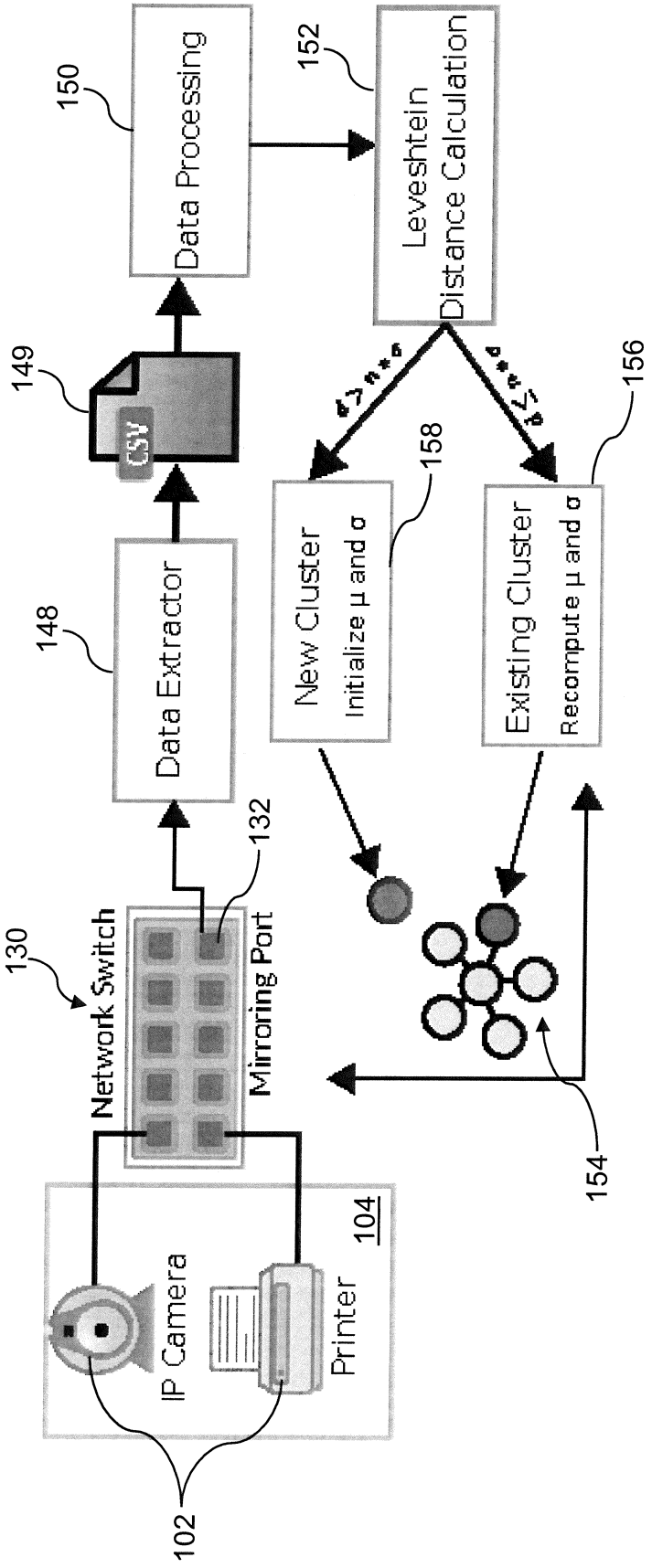

Data Processing
150
Leveshtein
Distance Calculation
152
CSV
149
Data Extractor
148
New Cluster
Initialize μ and σ
158
Existing Cluster
Recompute μ and σ
156
Network Switch
130
Mirroring Port
132
IP Camera
Printer
104
102
154

Figure 5C

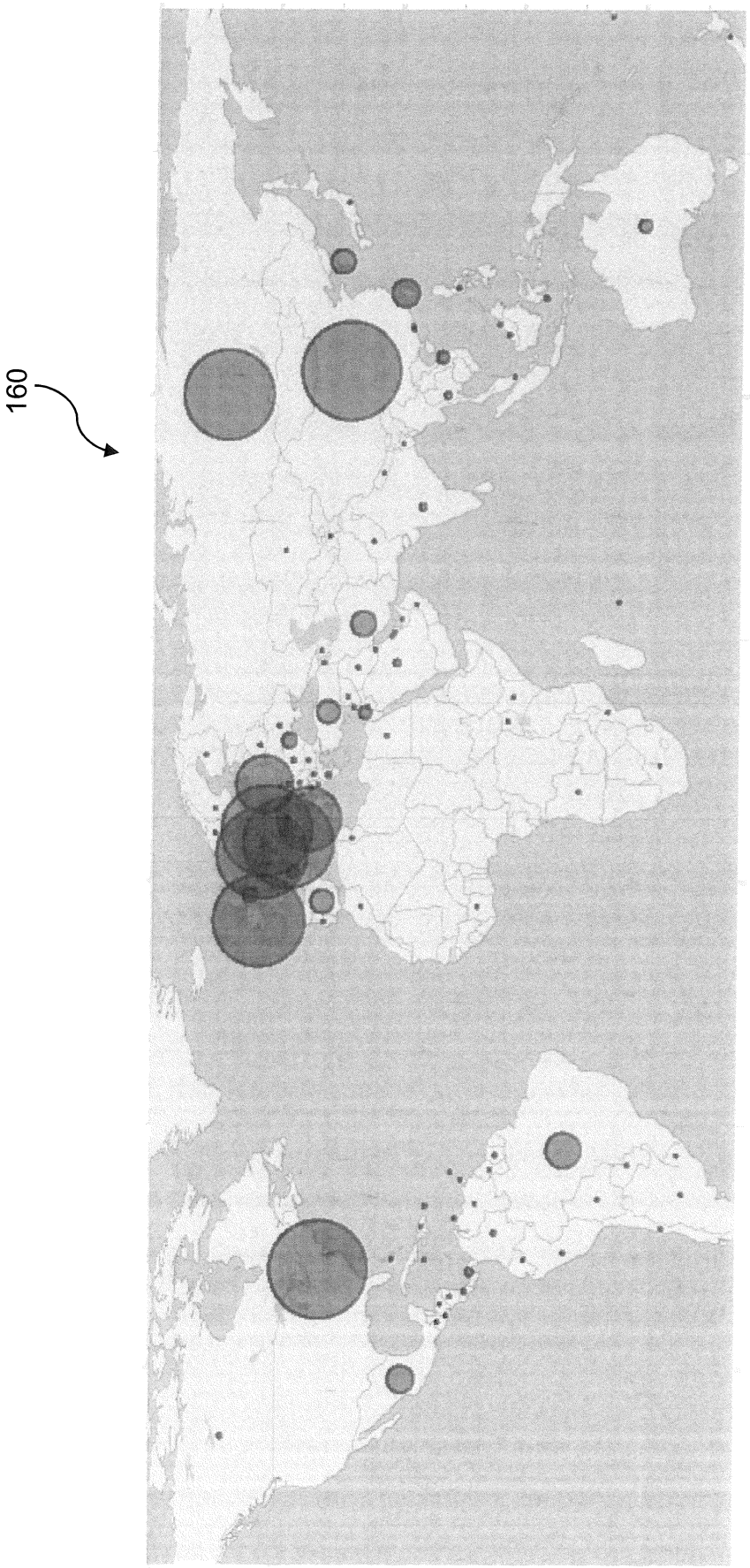


Figure 6

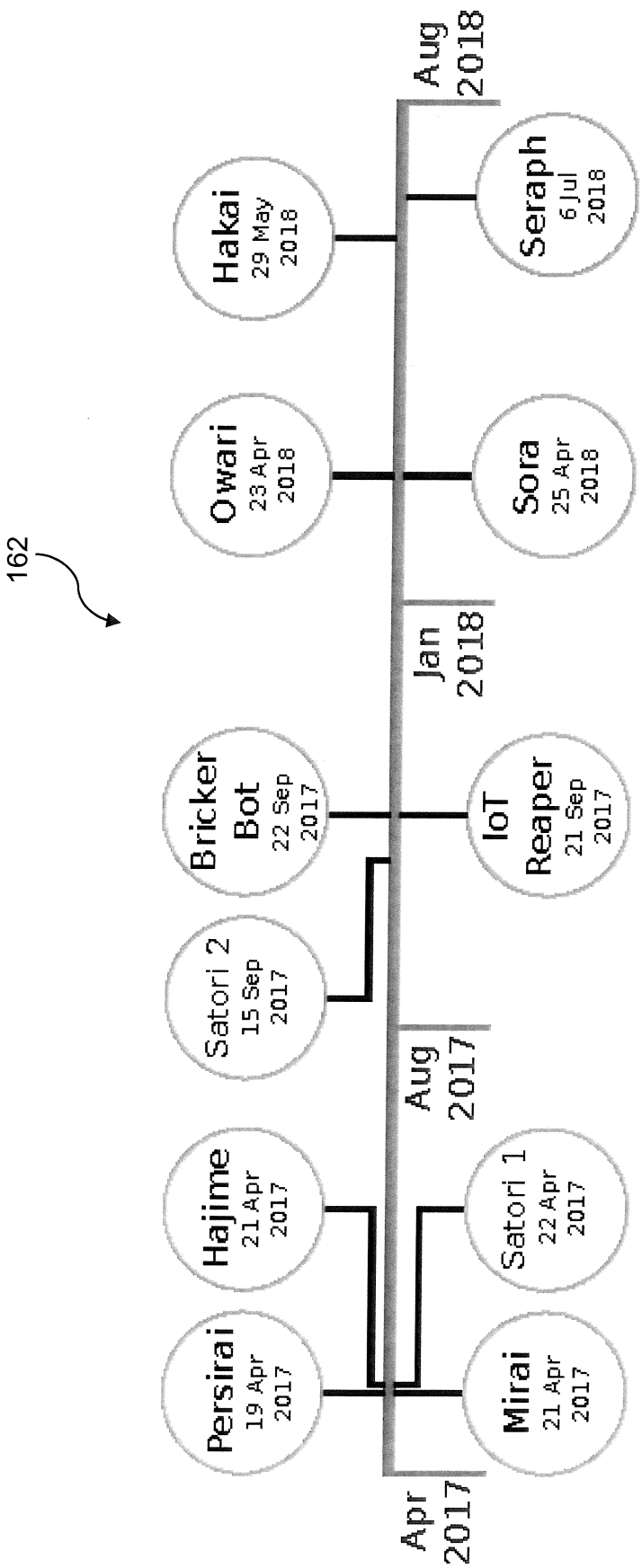
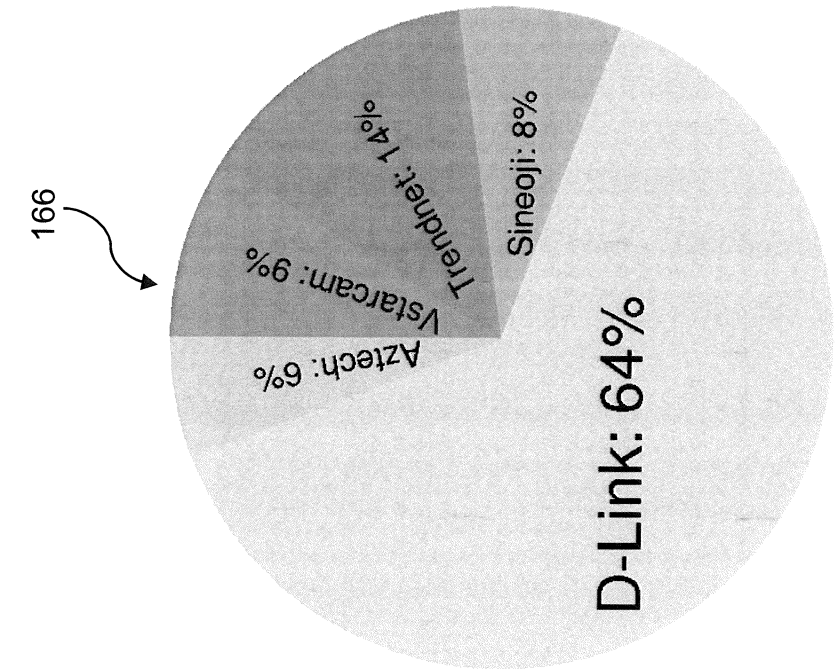

162
Apr 2017
Aug 2017
Jan 2018
Aug 2018
Persirai 19 Apr 2017
Hajime 21 Apr 2017
Satori 2 15 Sep 2017
Bricker Bot 22 Sep 2017
Mirai 21 Apr 2017
Satori 1 22 Apr 2017
IoT Reaper 21 Sep 2017
Owari 23 Apr 2018
Hakai 29 May 2018
Sora 25 Apr 2018
Seraph 6 Jul 2018

Figure 7


166
D-Link: 64%
Sineoji: 8%
Trendnet: 14%
Vstarcam: 9%
Aztech: 6%

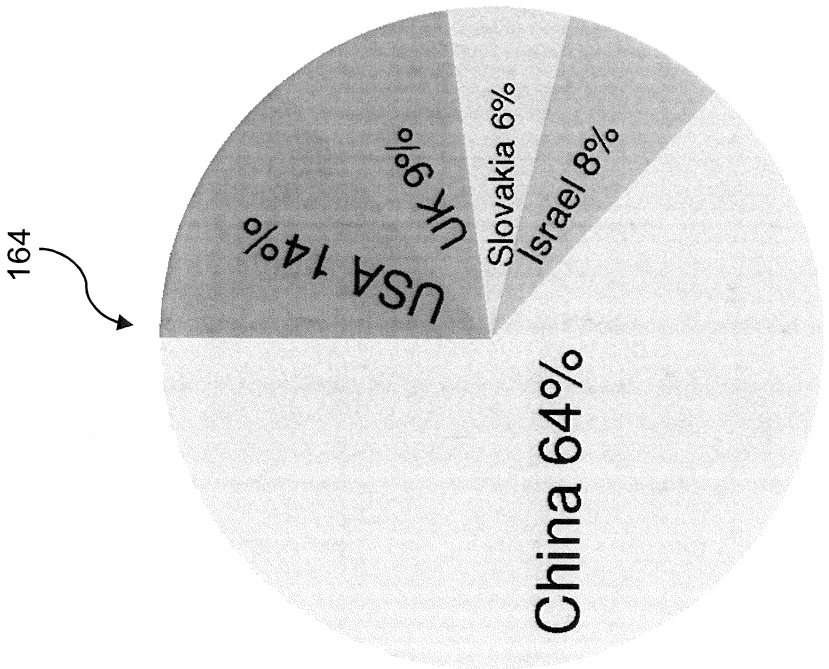

164
China 64%
USA 14%
UK 9%
Slovakia 6%
Israel 8%

Figure 8

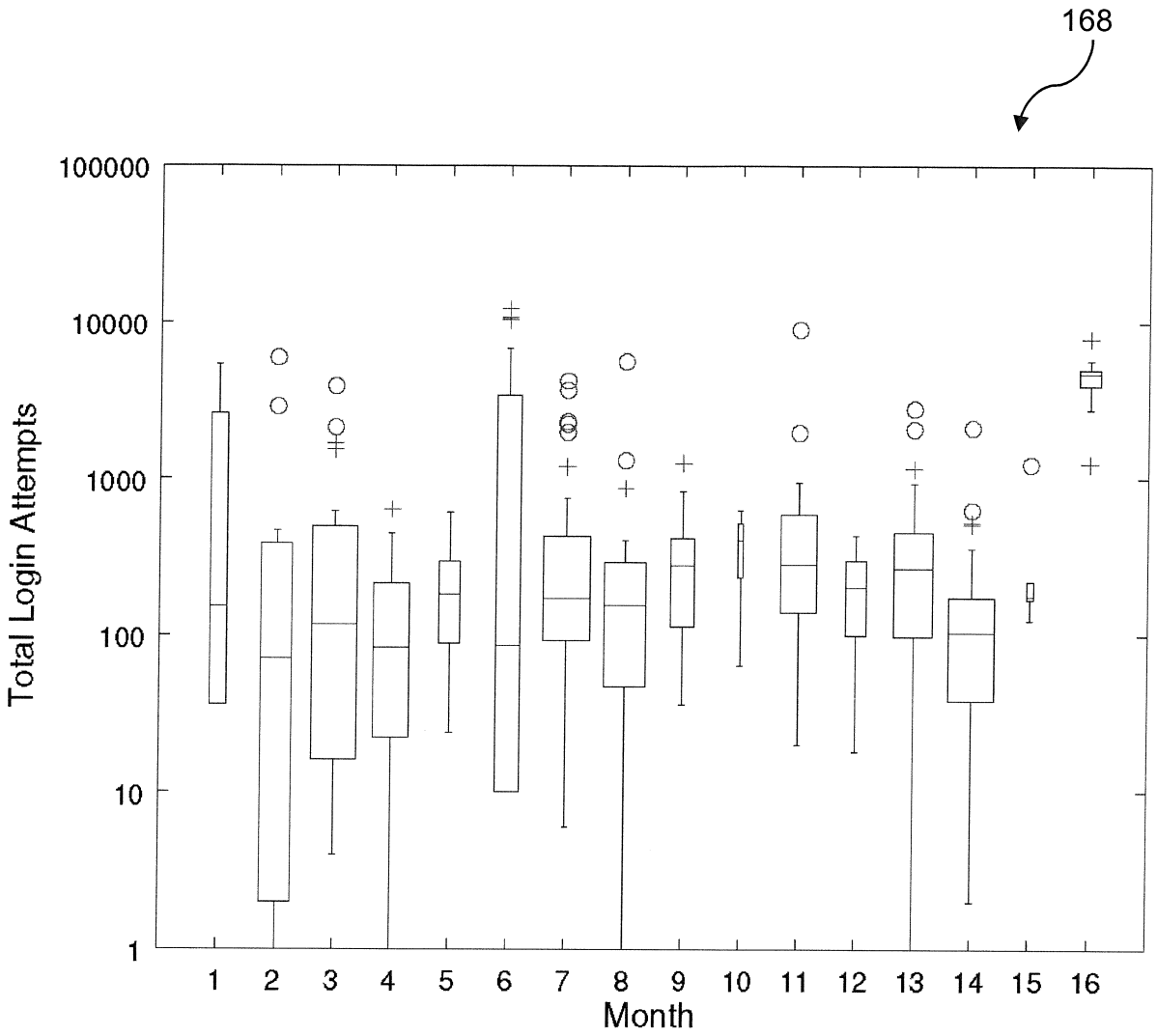

168
100000
10000
1000
100
10
1
Total Login Attempts
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
Month

Figure 9A

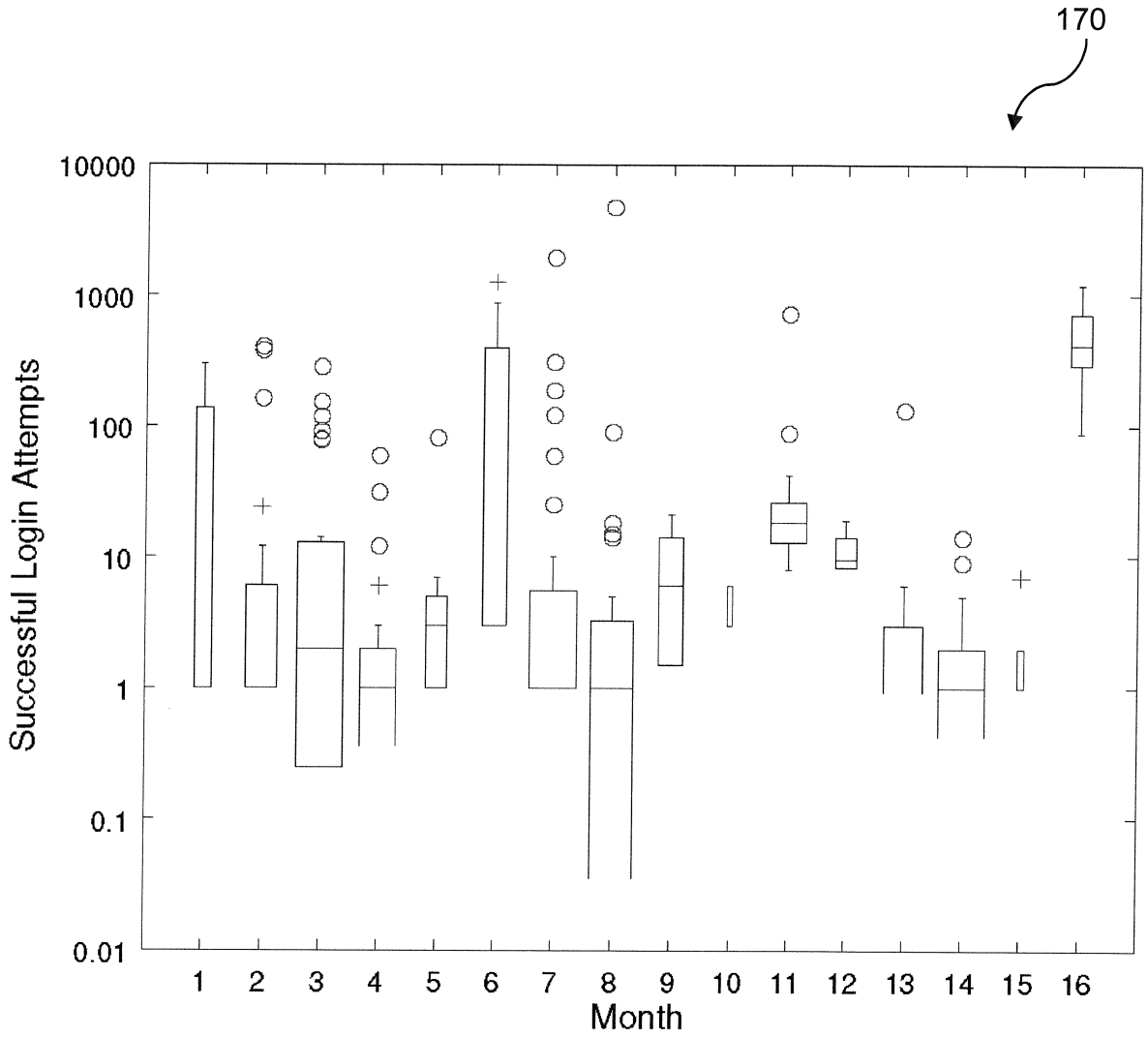

170
10000
1000
100
10
1
0.1
0.01
Successful Login Attempts
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
Month

Figure 9B