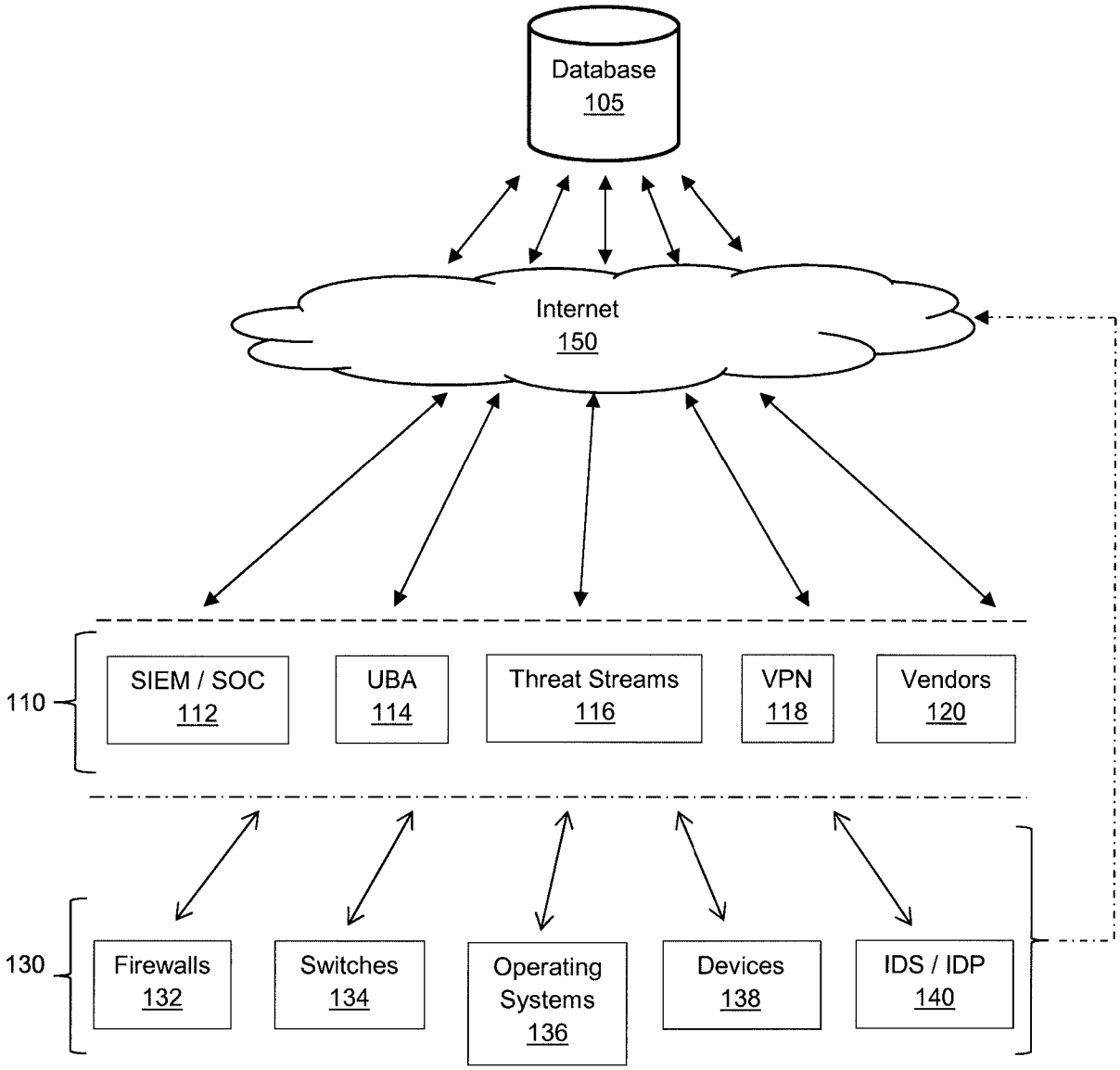
Database
105
Internet
150
110
SIEM / SOC
112
UBA
114
Threat Streams
116
VPN
118
Vendors
120
130
Firewalls
132
Switches
134
Operating
Systems
136
Devices
138
IDS / IDP
140

FIGURE 1

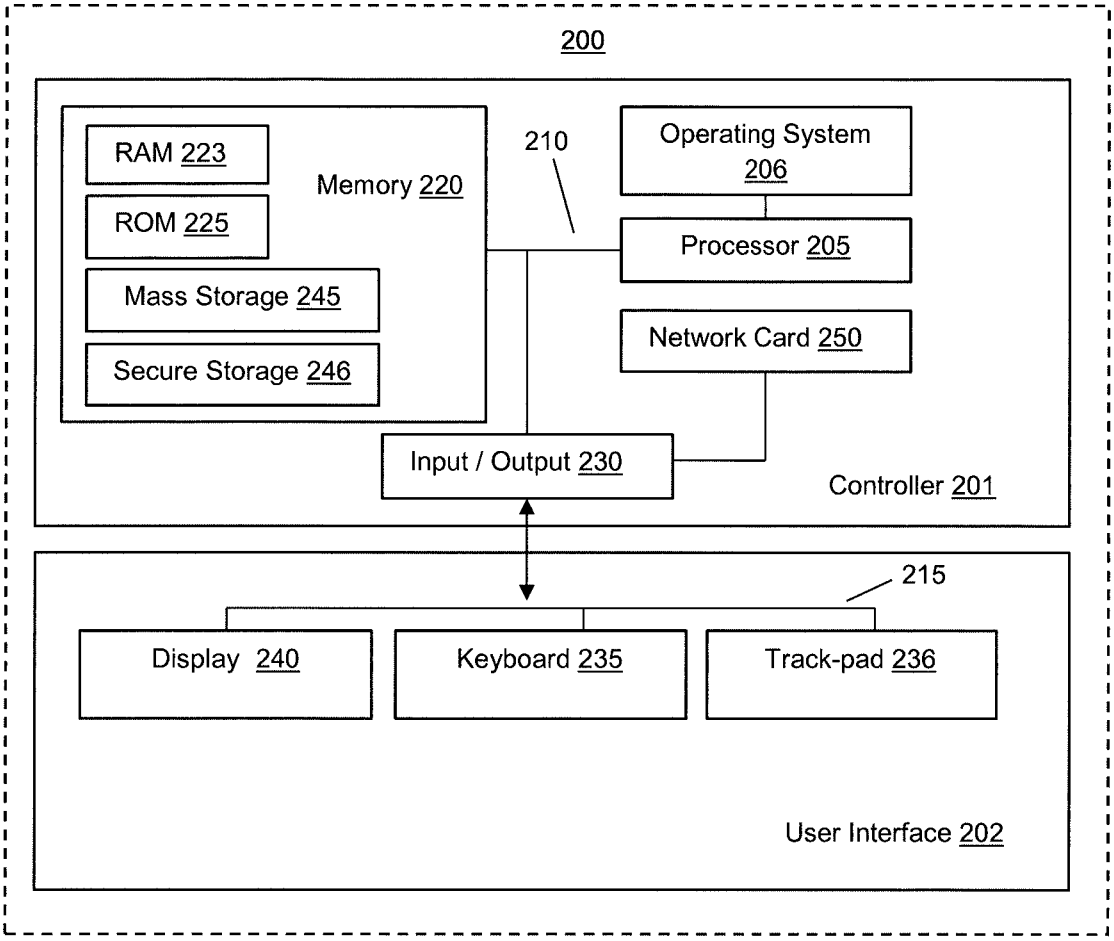
200
RAM 223
ROM 225
Mass Storage 245
Secure Storage 246
Memory 220
210
Operating System 206
Processor 205
Network Card 250
Input / Output 230
Controller 201
215
Display 240
Keyboard 235
Track-pad 236
User Interface 202

FIGURE 2

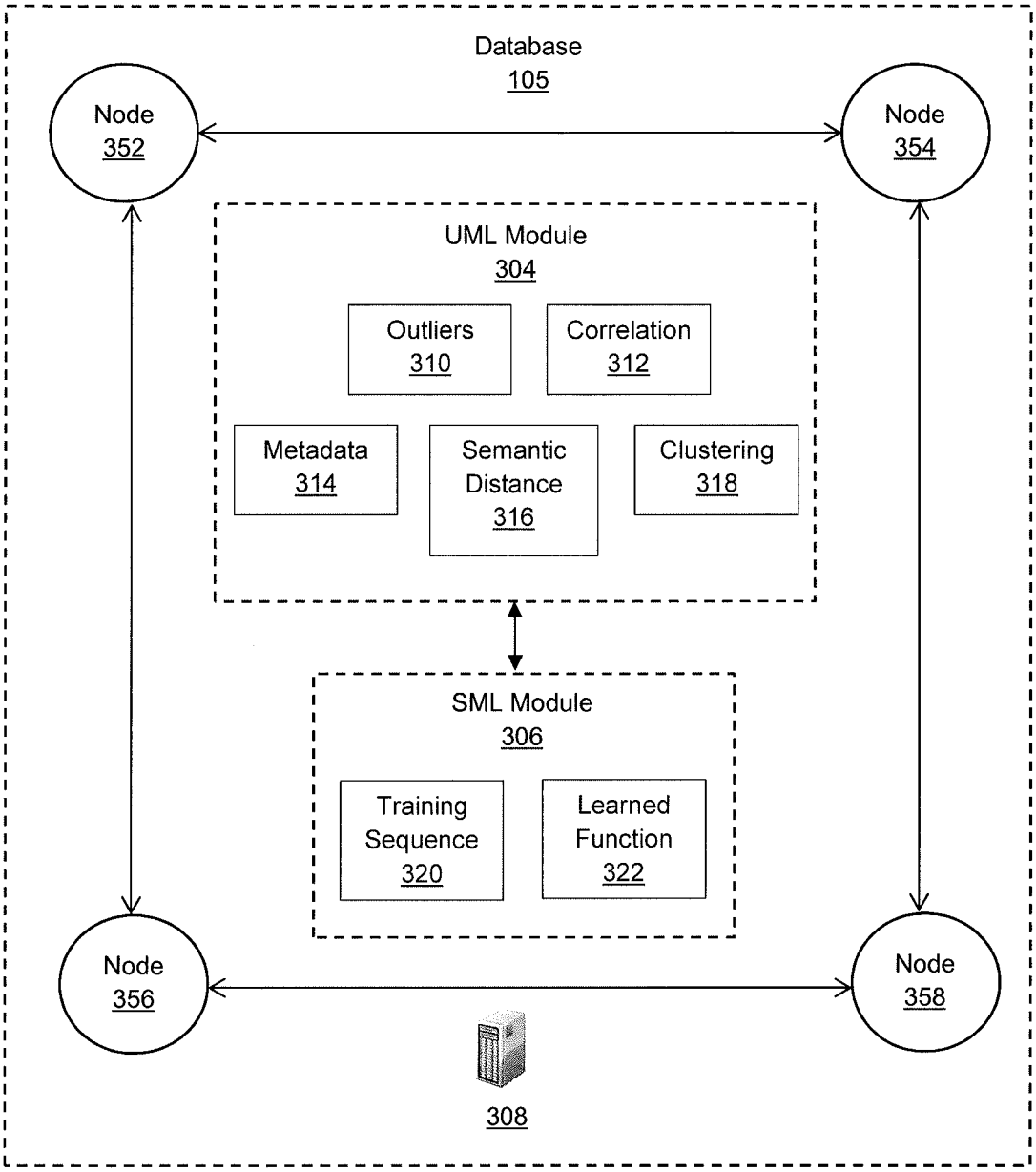
Database
105
Node
352
Node
354
UML Module
304
Outliers
310
Correlation
312
Metadata
314
Semantic
Distance
316
Clustering
318
SML Module
306
Training
Sequence
320
Learned
Function
322
Node
356
Node
358
308

FIGURE 3

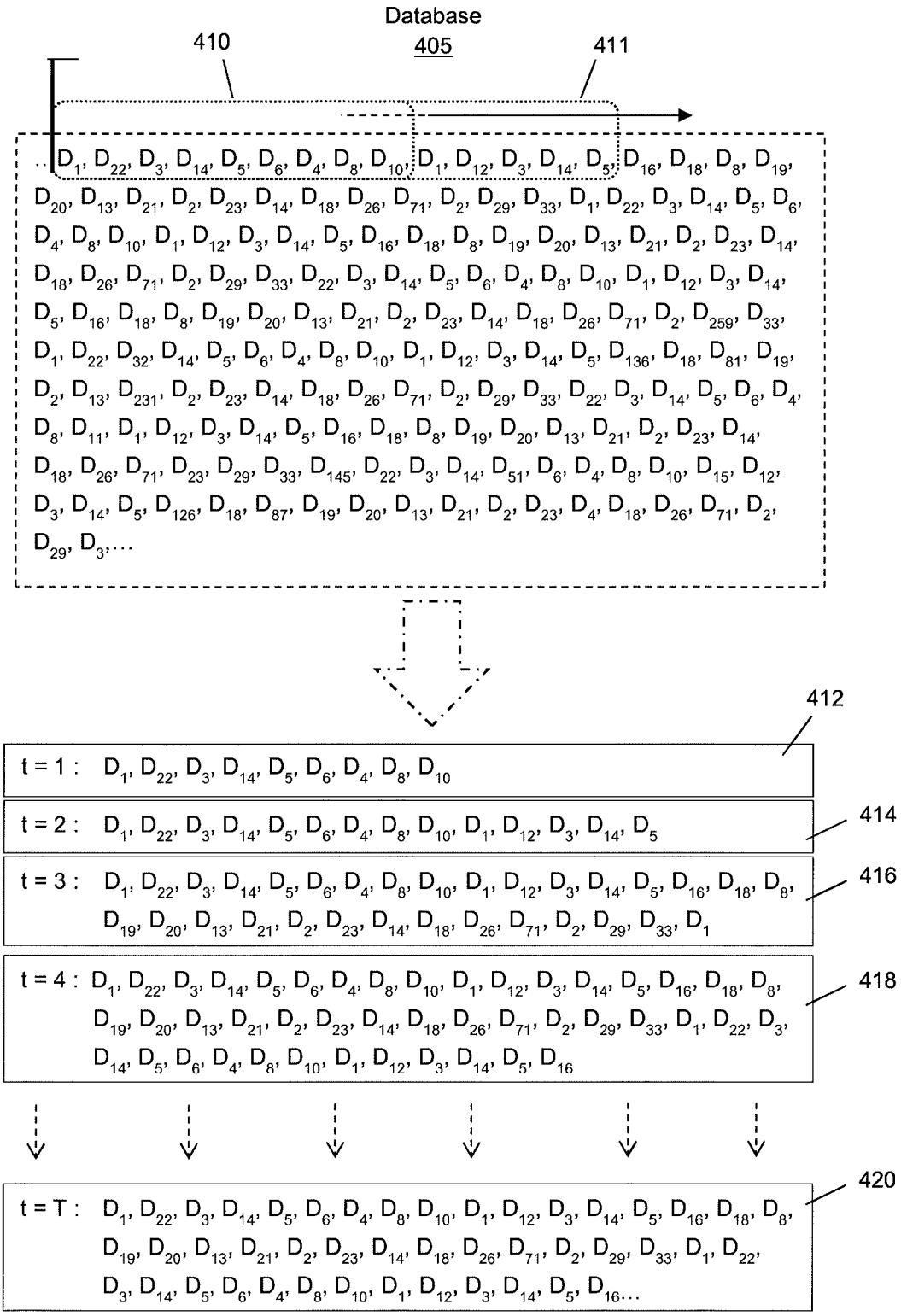
Database
405
410
411
.. D1, D22, D3, D14, D5, D6, D4, D8, D10, D1, D12, D3, D14, D5, D16, D18, D8, D19, D20, D13, D21, D2, D23, D14, D18, D26, D71, D2, D29, D33, D1, D22, D3, D14, D5, D6, D4, D8, D10, D1, D12, D3, D14, D5, D16, D18, D8, D19, D20, D13, D21, D2, D23, D14, D18, D26, D71, D2, D29, D33, D22, D3, D14, D5, D6, D4, D8, D10, D1, D12, D3, D14, D5, D16, D18, D8, D19, D20, D13, D21, D2, D23, D14, D18, D26, D71, D2, D259, D33, D1, D22, D32, D14, D5, D6, D4, D8, D10, D1, D12, D3, D14, D5, D136, D18, D81, D19, D2, D13, D231, D2, D23, D14, D18, D26, D71, D2, D29, D33, D22, D3, D14, D5, D6, D4, D8, D11, D1, D12, D3, D14, D5, D16, D18, D8, D19, D20, D13, D21, D2, D23, D14, D18, D26, D71, D23, D29, D33, D145, D22, D3, D14, D51, D6, D4, D8, D10, D15, D12, D3, D14, D5, D126, D18, D87, D19, D20, D13, D21, D2, D23, D4, D18, D26, D71, D2, D29, D3,...
412
t = 1 : D1, D22, D3, D14, D5, D6, D4, D8, D10
414
t = 2 : D1, D22, D3, D14, D5, D6, D4, D8, D10, D1, D12, D3, D14, D5
416
t = 3 : D1, D22, D3, D14, D5, D6, D4, D8, D10, D1, D12, D3, D14, D5, D16, D18, D8, D19, D20, D13, D21, D2, D23, D14, D18, D26, D71, D2, D29, D33, D1
418
t = 4 : D1, D22, D3, D14, D5, D6, D4, D8, D10, D1, D12, D3, D14, D5, D16, D18, D8, D19, D20, D13, D21, D2, D23, D14, D18, D26, D71, D2, D29, D33, D1, D22, D3, D14, D5, D6, D4, D8, D10, D1, D12, D3, D14, D5, D16
420
t = T : D1, D22, D3, D14, D5, D6, D4, D8, D10, D1, D12, D3, D14, D5, D16, D18, D8, D19, D20, D13, D21, D2, D23, D14, D18, D26, D71, D2, D29, D33, D1, D22, D3, D14, D5, D6, D4, D8, D10, D1, D12, D3, D14, D5, D16...

FIGURE 4

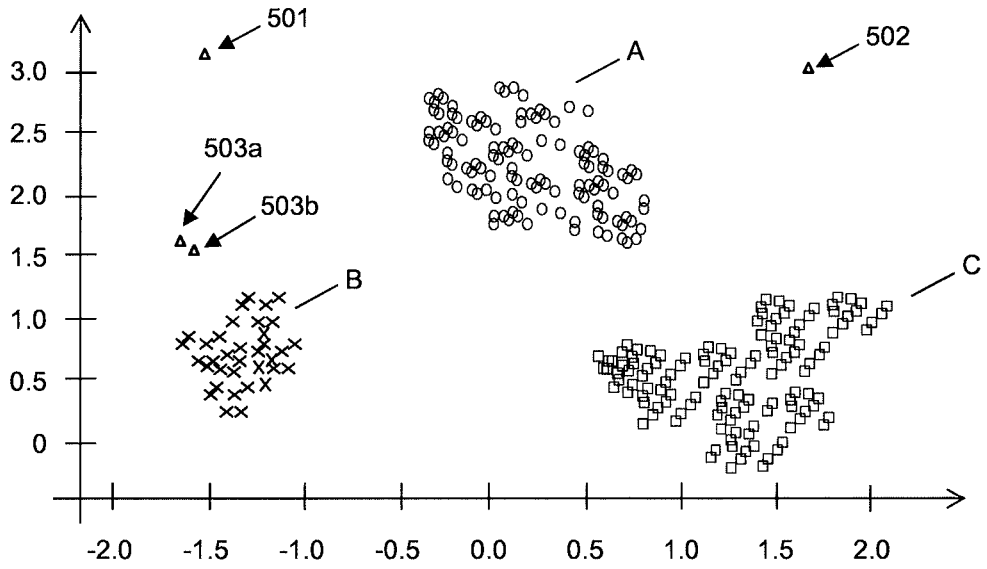

FIGURE 5a

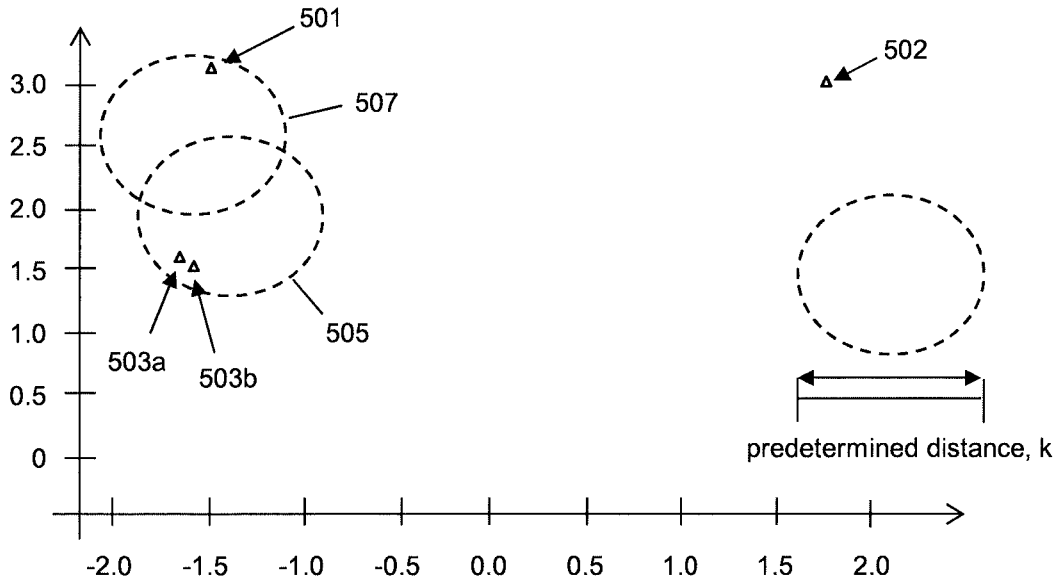

FIGURE 5b

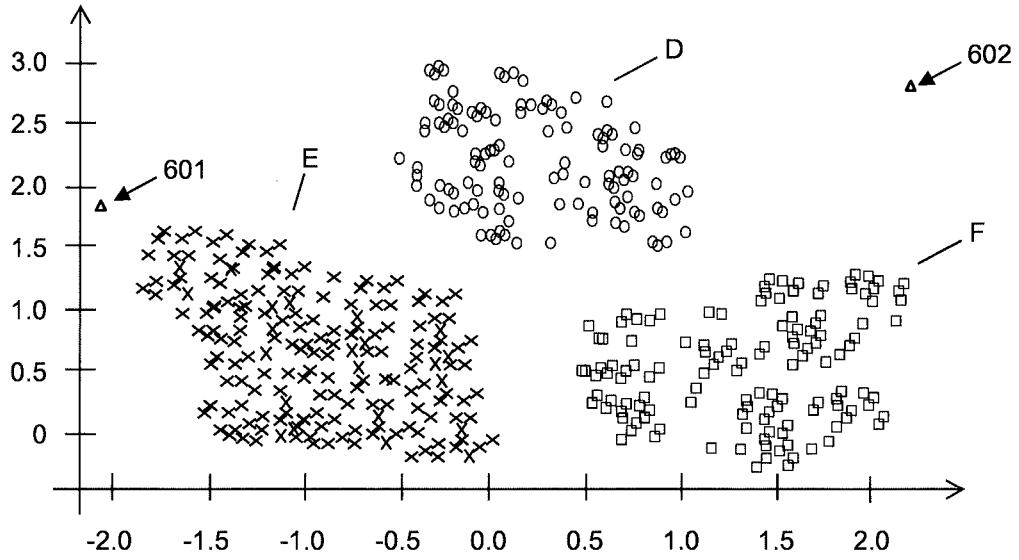

FIGURE 6

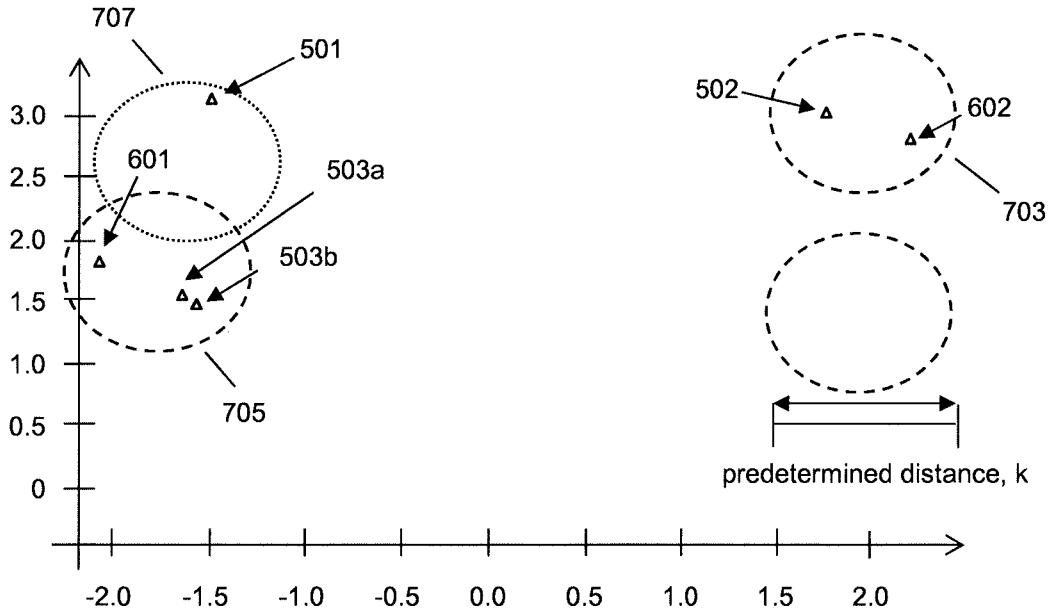

FIGURE 7

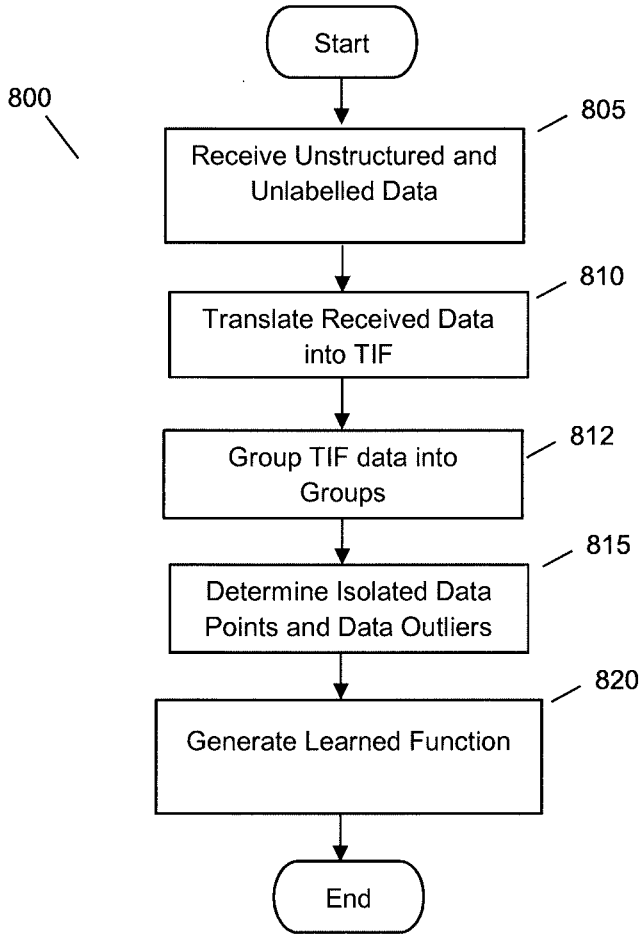
800
Start
805
Receive Unstructured and Unlabelled Data
810
Translate Received Data into TIF
812
Group TIF data into Groups
815
Determine Isolated Data Points and Data Outliers
820
Generate Learned Function
End

FIGURE 8

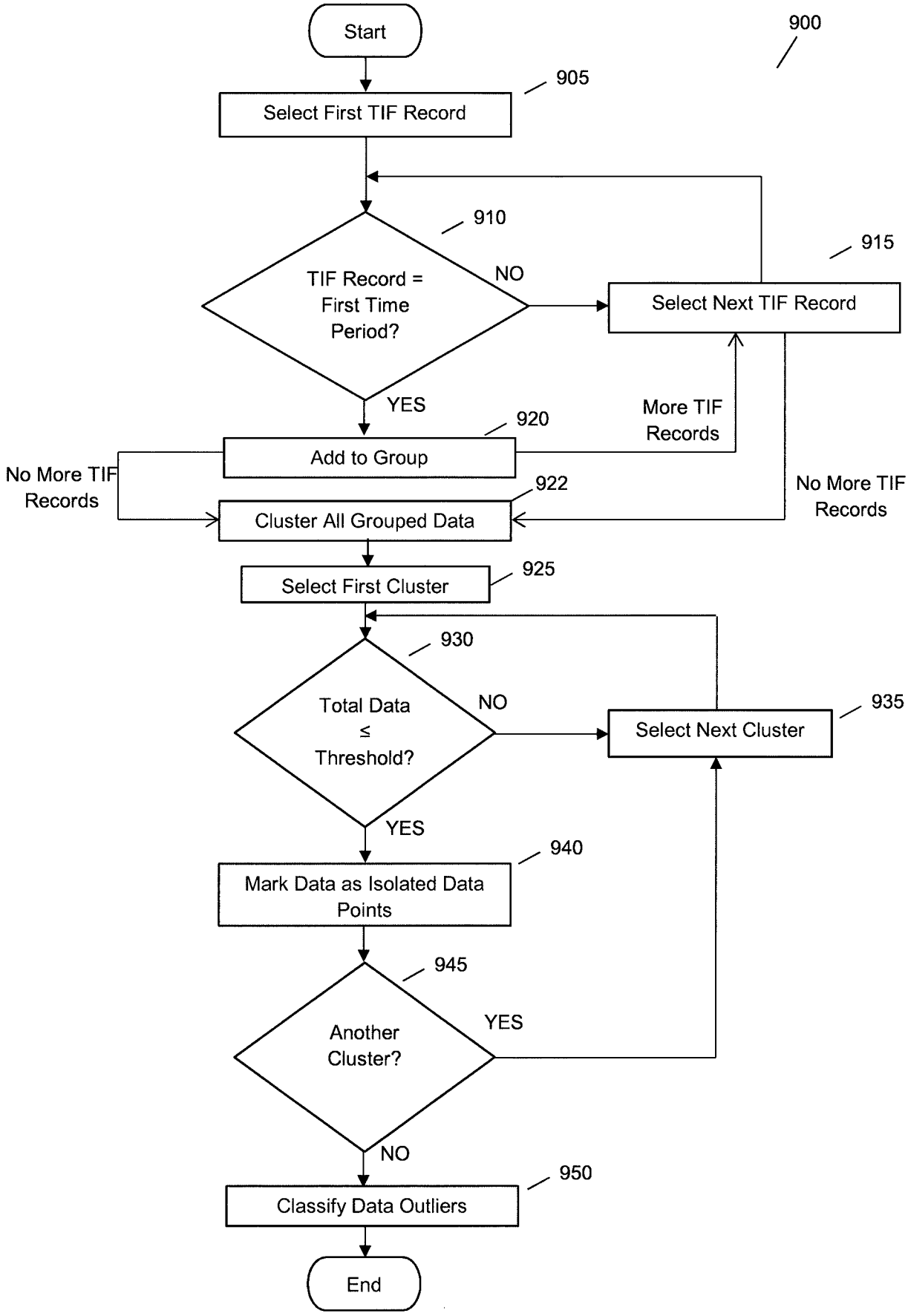
Start
900
905
Select First TIF Record
910
TIF Record = First Time Period?
NO
915
Select Next TIF Record
YES
More TIF Records
920
Add to Group
No More TIF Records
922
No More TIF Records
Cluster All Grouped Data
925
Select First Cluster
930
Total Data ≤ Threshold?
NO
935
Select Next Cluster
YES
940
Mark Data as Isolated Data Points
945
Another Cluster?
YES
NO
950
Classify Data Outliers
End

FIGURE 9