(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 February 2016 (04.02.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/018266 A1

(51) International Patent Classification:
G06F 15/16 (2006.01) *G06N 7/02* (2006.01)

(21) International Application Number:
PCT/US2014/048705

(22) International Filing Date:
29 July 2014 (29.07.2014)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 11445 Compaq Center Drive W., Houston, Texas 77070 (US).

(72) Inventor: **IVANOV, Plamen V.**; 258 Okolovrasten Pat, Str., 1766 Sofia (BG).

(74) Agents: **FEBBO, Michael A.** et al.; Hewlett-Packard Company, Intellectual Property Administration, 3404 E. Harmony Road, Mail Stop 35, Fort Collins, Colorado 80528 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

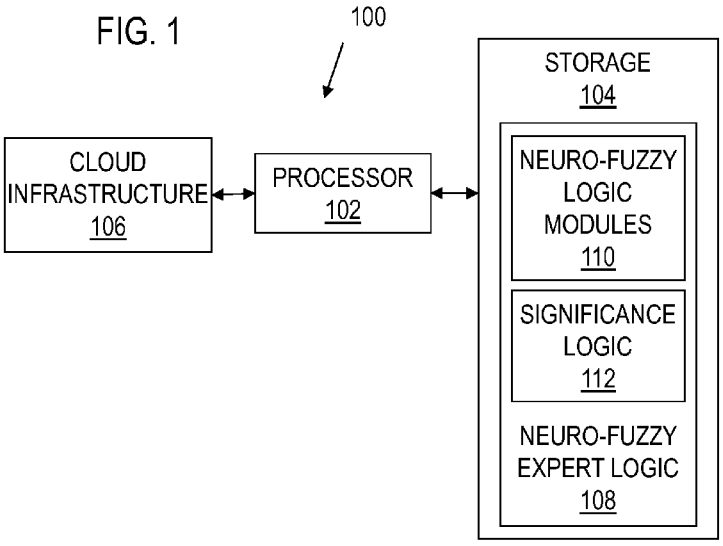
Published:

— *with international search report (Art. 21(3))*

WO 2016/018266 A1

(54) Title: CLOUD INFRASTRUCTURE EVENT ANALYSIS

FIG. 1



(57) Abstract: In one example, neuro-fuzzy expert system logic analyzes and assigns significance values to events occurring in a cloud infrastructure. The logic includes event significance logic and a plurality of neuro-fuzzy logic modules. Each of the logic modules includes fuzzy logic to determine a fuzzy value of an effect of a detected event on the cloud infrastructure. The event significance logic includes neuro-fuzzy logic to determine, based on the values of the effects of the detected event determined by the plurality of neuro-fuzzy logic modules, a value indicative of significance of the event to the cloud infrastructure.

CLOUD INFRASTRUCTURE EVENT ANALYSIS

BACKGROUND

[0001] As cloud-based services proliferate, the number of events generated in the cloud infrastructure is increasing significantly. To effectively manage cloud-based services, the status of the underlying infrastructure should be monitored and abnormal behavior and deviation from normal or expected service/infrastructure component states should be detected and analyzed. Based on the results of analysis, the appropriate control actions can be applied to prevent or restore services disruptions.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] For a detailed description of various examples, reference will now be made to the accompanying drawings in which:

[0003] Figures 1 and 2 show block diagrams of system that applies neuro-fuzzy logic to analyze events in a cloud infrastructure in accordance with principles disclosed herein;

[0004] Figure 3 shows neuro-fuzzy logic arranged to determine the significance of an event in cloud infrastructure in accordance with principles disclosed herein;

[0005] Figures 4A-4F shows examples of fuzzy values applied in a system for analyzing events in a cloud infrastructure in accordance with principles disclosed herein;

[0006] Figure 5 shows an arrangement of logic layers in neuro-fuzzy logic for analyzing events in a cloud infrastructure in accordance with principles disclosed herein;

[0007] Figure 6 shows a flow diagram for a method for applying neuro-fuzzy logic to analyze events in a cloud infrastructure in accordance with principles disclosed herein; and

[0008] Figure 7 shows a flow diagram for a method for training neuro-fuzzy logic to analyze events in a cloud infrastructure in accordance with principles disclosed herein.

DETAILED DESCRIPTION

[0009] Certain terms are used throughout the following description and claims to refer to particular system components. As one skilled in the art will appreciate, different companies may refer to a component by different names. This document does not intend to distinguish between components that differ in name but not function. In the following discussion and in the claims, the terms "including" and "comprising" are used in an open-ended fashion, and thus should be interpreted to mean "including, but not limited to… ." The recitation "based on" is intended to mean "based at least in part on." Therefore, if *X* is based on *Y*, *X* may be based on *Y* and any number of other factors.

[0010] An event can be defined as any detectable or discernible occurrence that has significance for the management of an information technology (IT) infrastructure or the delivery of IT service. Events are evaluated to determine the impact a deviation in operation resulting from the event might cause to services.

[0011] Because cloud infrastructure and services are complex, when applied in the cloud context, conventional event analysis methods are subject to a variety of deficiencies. Correlation engines employed in conventional methodologies apply predefined rules and criteria to event analysis. The rules and analysis criteria require continuous tuning, and system experts must be available to provide tuning information and services. Similarly, application of an incorrect level of filtering can result in a flood of insignificant events or misclassification of important events.

[0012] The event analysis system disclosed herein includes a neuro-fuzzy expert system that analyzes and categorizes events based on event significance. Neuro-fuzzy expert systems represent fuzzy logic in a neural structure that provides the flexible reasoning of fuzzy logic with the structure and trainability of neural networks. The system disclosed herein analyzes events using previously defined and implemented expert knowledge including fuzzy variables, fuzzy rules, fuzzy inference engines, and fuzzy defuzzification methods. Additionally the system can be trained, thereby eliminating or minimizing the need for constantly available experts that gather and implement expert knowledge, tune and optimize the system.

[0013] Figures 1 and 2 show block diagrams of a system 100 that applies neuro-fuzzy logic to analyze events in a cloud infrastructure in accordance with principles disclosed herein. The system 100 includes a processor 102 coupled to a cloud infrastructure 106 and storage 104. Some implementations of the system 100 may include a plurality of processors 102. The cloud infrastructure 106 may include a plurality of servers, storage systems, and other device interconnected by a communication network, such as a wide area network, the internet, etc. The servers may provide various services to devices and users that access the cloud infrastructure 106. Events occurring in the cloud infrastructure 106 are detected, and the processor 102 is notified. In some implementations the processor 102 may detect events occurring in the cloud infrastructure 106.

[0014] The processor 102 may be a general-purpose microprocessor, a digital signal processor, a microcontroller, or other device capable of executing instructions retrieved from a computer-readable storage medium. Processor architectures generally include execution units (e.g., fixed point, floating point, integer, etc.), storage (e.g., registers, memory, etc.), instruction decoding, instruction and data fetching logic, peripherals (e.g., interrupt controllers, timers, direct memory access controllers, etc.), input/output systems (e.g., serial ports, parallel ports, etc.) and various other components and sub-systems.

[0015] The storage 104 is communicatively coupled to the processor 102. The storage 104 is a non-transitory computer-readable storage medium suitable for storing instructions that are retrieved and executed by the processor 102 to perform the functions disclosed herein. The storage 104 may include volatile storage such as random access memory, non-volatile storage (e.g., a hard drive, an optical storage device (e.g., CD or DVD), FLASH storage, read-only-memory), or combinations thereof. In some implementations, the processor 102 and the storage 104 may be embodied in a computer, such as a server computer, a rack-mount computer, etc.

[0016] Processors execute instructions. Instructions alone are incapable of performing a function. Therefore, in the present disclosure, any reference to a function performed by instructions, or to instructions performing a function is

simply a shorthand means for stating that the function is performed by the processor 102 executing the instructions.

[0017] The storage 104 includes neuro-fuzzy expert logic 108 and event preprocessing logic 208. The event pre-processing logic 208 includes instructions that are executed by the processor 102 to process events occurring in the cloud infrastructure prior to analysis by the neuro-fuzzy expert logic 108. The neuro-fuzzy expert logic 108 is executable by the processor 102 to analyze and assign significance values to events occurring in the cloud infrastructure 106. The neuro-fuzzy expert logic 108 includes neuro-fuzzy logic modules 110 and event significance logic 112. The neuro-fuzzy logic modules 110 includes event potential logic 202, event seriousness logic 204, and event magnitude logic 206, each of which includes fuzzy logic that is executable by the processor 102 to determine a fuzzy value of an effect of a detected event on the cloud infrastructure 106. The event significance logic 112 includes neuro-fuzzy logic executable by the processor 102 to determine, based on the values of the effects of the detected event determined by the neuro-fuzzy logic modules 110, a value indicative of significance of the event to the cloud infrastructure 106 and services provided thereby.

[0018] The event potential logic 202 analyzes event information generated by the event preprocessing logic 208 to determine the potential impact of the detected event on the cloud infrastructure 106. The event seriousness logic 204 analyzes event information generated by the event preprocessing logic 208 to determine the seriousness of the effect of the detected event on the cloud infrastructure 106. The event magnitude logic 206 analyzes event information generated by the event preprocessing logic 208 to determine the magnitude of effect of the event on the cloud infrastructure 106.

[0019] The storage 104 also includes training logic 210. The training logic 210 tunes the neuro-fuzzy expert logic 108 to analyze events occurring in the cloud infrastructure 106. A method applied by the training logic 210 to train the neuro-fuzzy expert logic 108 is disclosed herein.

[0020] Figure 3 shows an arrangement of the neuro-fuzzy expert logic 108. The event potential logic 202, event seriousness logic 204, and event magnitude

logic 206 receive and apply fuzzy logic processing to input values I1.1 to I3.3 provided by the event preprocessing logic 208. Some implementations of the neuro-fuzzy expert logic 108 may process a different number and/or different types of input values than those described herein. The event significance logic 112 receives fuzzy event potential, event seriousness, and event magnitude values from the event potential logic 202, event seriousness logic 204, and event magnitude logic 206, and applies fuzzy logic to generate event significance output values O1 and O2 based on the event potential, event seriousness, and event magnitude values.

[0021] The inputs (I1.1, I1.2, and I1.3) to the event potential logic 202 include information related to the impact of the event on the cloud infrastructure 106. Input value I1.1 may establish the number of events similar to the event currently being analyzed that have occurred in the cloud infrastructure 106, and represent a value of previous similarity impact. Similarity can be determined, for example, based on categorization of the events and/or components impacted. Input value I1.2 may establish the number of components of the cloud infrastructure 106 affected by previously occurring events similar to the event currently being analyzed, and represent a value of previous infrastructure impact. Input value I1.3 may establish the number of services provided by the cloud infrastructure 106 affected by previously occurring events similar to the event currently being analyzed, and represent a value of previous business impact.

[0022] The inputs (I2.1, I2.2, and I2.3) to the event seriousness logic 204 include information related to the seriousness of an effect of the event on the cloud infrastructure 106. Input value I2.1 may establish the number of users affected by the current event, and represent a value of customer impact. Input value I2.2 may establish the urgency of the services affected by the event (e.g., based on predetermined service level requirements of the services), and represent a value of service level impact. Input value I2.3 may establish the level of utilization (e.g., not exceeding (low), reaching (medium), exceeding (high) a threshold) of component affected by the event, and represent a value of component impact.

[0023] The inputs (I3.1, I3.2, and I3.3) to the event magnitude logic 206 include information related to the magnitude of an effect of the event on the cloud infrastructure 106. Input value I3.1 may establish the number of components of the cloud infrastructure 106 affected by the current event, and represent a value of current infrastructure impact. Input value I3.2 may establish the number of services provided by the cloud infrastructure 106 affected by the event, and represent a value of current business impact. Input value I3.3 may establish the number of similar events currently detected in the cloud infrastructure 106, and represent a value of current similarity impact.

[0024] Each of the inputs I1.1-I3.1 are fuzzy input variables whose values (linguistically defined using words such as 'Low', 'Medium' or 'High') are modeled with fuzzy numbers using triangular, sinusoidal or trapezoidal membership functions. Each of these membership functions can be opened for training and tuned automatically by the training logic 210. Figures 4A-4D shows examples of fuzzy input values that may be applied in the system 100. In the examples of Figures 4A-4D values are expressed as "low," "medium," or "high" using various membership functions. In each of Figs. 4A-4E, the vertical axis represents degree of membership in a fuzzy set (e.g., small, medium, large), and the vertical axis represents the value evaluated for fuzzy set membership. Values evaluated for fuzzy set membership may be normalized as shown in Figs. 4A-4E, but normalization is not a requirement.

[0025] Event analysis result values O1 and O2 may be fuzzy and crisp (defuzzified) values respectively. The result O1 represents fuzzy event significance and may be modeled with fuzzy numbers using triangular, sinusoidal or trapezoidal membership functions. Figures 4E and 4F show examples of fuzzy output values that may be provided by the system 100. In the examples of Figures 4E-4F, output values are expressed as "informational," "warning," or "exception" using various membership functions. Events having informational significance may not require action, but may be stored for future reference. Events having warning significance can be classified as notifications and may need attention, but may not require immediate attention. Events having exception significance may be further investigated and resolved with a higher degree of

urgency than events having warning significance. The crisp result value O2 can be used, for example, to sort events within a significance level.

[0026] Based on output values O1 and/or O2, a significance of the events can be determined. For example, events can be classified by their significance level according to fuzzy value O1 (e.g., “informational,” “warning,” or “exception”) and, subsequently, the event can be graded using the crisp value O2. Thus, the fuzzy output value O1 can be used to determine a class or category for each event and the crisp value O2 can be used to index the event in that class or category. The crisp value O2 can also be used to further affect the determined class or category, such that an event can be reclassified into a neighboring class or category if the crisp value O2 exceeds or falls below a certain threshold.

[0027] The outputs of the significance logic 112 can be passed a management system that manages the events based on the level of significance, provides the analysis results to a human operator and/or automatically manages the events to maintain operation and performance of the cloud infrastructure 106.

[0028] Figure 5 shows an arrangement of logic layers 500 in neuro-fuzzy logic for analyzing events in a cloud infrastructure in accordance with principles disclosed herein. The logic arrangement of Figure 5 is applicable to each of the event potential logic 202, event seriousness logic 204, event magnitude logic 206, and event significance logic 112. Accordingly, each of the event potential logic 202, event seriousness logic 204, event magnitude logic 206, and event significance logic 112 may include five neural network layers as shown in Figure 5. The neural network layers 500 include an input values layer 502, an input terms layer 504, a fuzzy rules layer 506, an output terms layer 508, and an output values layer 510.

[0029] The input values layer 502 includes crisp input value nodes 502-1, 502-2, and 502-3 that provide received input values to the input terms layer 504. Each input value nodes 502-1, 502-2, and 502-3 provide an input value to three input term nodes. Input value layer 502-1 provides an input value to input term nodes 504-1, 504-2, and 504-3. Input value layer 502-2 provides an input value to input term nodes 504-4, 504-5, and 504-6. Input value layer 502-3 provides an input value to input term nodes 504-7, 504-8, and 504-9. Some

implementations may provide a different number of input value nodes, input term nodes, and/or connections therebetween. The input term layer 504 fuzzifies the crisp input values received from the input values layer 502. For example, nodes 504-1, 504-4, and 504-7 may represent a low value subrange, nodes 504-2, 504-5, and 504-8 may represent, for example, a medium value subrange, and nodes 504-3, 504-6, and 504-7 may represent a high value subrange.

[0030] The rules layer 506 includes the fuzzy rules nodes 506-1 to 506-27. In some implementations, the rules layer 506 may include a different number of rules. Each of the rules nodes 506-1 to 506-27 may receive all of the fuzzy term values generated by the input terms layer 504, and process the fuzzy term values in accordance with predetermined neuro-fuzzy expert rule logic to assess the term values. Each of the rules 506 includes a weight value that represents the weight or strength of the rule relative to the other rules 506. Some implementations may include an inference engine that specifies a hierarchy for application of the rules 506-1 to 506-27.

[0031] The output terms layer 508 receives results of rule processing by the rules 506 and evaluates the results to produce fuzzy output terms 508-1, 508-2, 508-3. The results of each rule 506 can be combined in different ways, such as using one of a maximum method, a bounded sum method, and a normalized sum method and other suitable methods. Also, the membership degrees of all members of the resulting fuzzy set can be analyzed in order to derive a further approximation of a fuzzy output value. Output terms 508-1, 508-2, and 508-3 may represent, for example, low, medium, and high value subranges respectively. The fuzzy output terms (fuzzy set) generated by the output terms layer 508 are provided to the output values layer 510. The output values layer 510 may generate from the output term values, the fuzzy output value 510-1.

[0032] Some implementations of the output values layer 510 may also generate, from the output term values, a crisp (defuzzified) output value 510-2. The crisp value 510-2 can refer to a numerical or real value which can be derived by a defuzzification of the fuzzy set and its membership degrees. In order to determine the crisp value the geometry and shape of the membership functions

of the resulting fuzzy set can be analyzed and superimposed to derive a numerical value, for example, from a centroid resulting from the superimposed functions.

[0033] Figure 6 shows a flow diagram for a method 600 for applying neuro-fuzzy logic to analyze events in a cloud infrastructure in accordance with principles disclosed herein. Though depicted sequentially as a matter of convenience, at least some of the actions shown can be performed in a different order and/or performed in parallel. Additionally, some embodiments may perform only some of the actions shown. In some embodiments, at least some of the operations of the method 600, as well as other operations described herein, can be implemented as instructions stored in the storage 104 and executed by the processor 102.

[0034] In block 602, the cloud infrastructure 106 is operating to service requests and provide services to users. The event analysis system comprising the processor 102 is executing the instructions retrieved from the storage 104 to analyze events occurring in the cloud infrastructure 106, and an event is detected in the cloud infrastructure 106. The event preprocessing logic 208 processes the event and generates input values related to the detected event for processing by the neuro-fuzzy expert logic 108.

[0035] The event potential logic 202, event seriousness logic 204, and event magnitude logic 206 process the input values using neuro-fuzzy logic to determine values of event potential impact on the cloud infrastructure 106, seriousness of the event to the cloud infrastructure 106, and magnitude of the effect of the event on the cloud infrastructure 106.

[0036] In block 604, neuro-fuzzy logic is applied to determine effects of the event on the cloud infrastructure 106. More specifically, the event potential logic 202, event seriousness logic 204, and event magnitude logic 206 provide fuzzy result values for potential impact, seriousness, and magnitude of the event to the event significance logic 112.

[0037] In block 606, the event significance logic 112 applies neuro-fuzzy logic to the received input values and determines a fuzzy value representing significance of the event to the cloud infrastructure 106 and operation thereof. A crisp value of event significance may also be generated by the event significance logic 112.

The determined values of event significance may be provided to a management system that handles the event in accordance with the determined significance.

[0038] Figure 7 shows a flow diagram for a method for training neuro-fuzzy logic to analyze events in a cloud infrastructure in accordance with principles disclosed herein. Though depicted sequentially as a matter of convenience, at least some of the actions shown can be performed in a different order and/or performed in parallel. Additionally, some embodiments may perform only some of the actions shown. In some embodiments, at least some of the operations of the method 700, as well as other operations described herein, can be implemented as instructions stored in the storage 104 and executed by the processor 102.

[0039] At initiation of the method 700, the event potential logic 202, event seriousness logic 204, event magnitude logic 206, and event significance logic may be untrained. The logic to be trained includes defined fuzzy input variables, membership functions of fuzzy input terms, fuzzy rules, fuzzy rule blocks, fuzzy output variables, membership functions of the fuzzy output values terms, etc. as disclosed herein. In block 702, neural network training data is acquired. The training data includes representative sets of input and out values. The training data can be obtained from daily operations of the system 100 or similar systems, input from human experts, etc. The training data may be modified by a human expert to eliminate irrelevant and insignificant values.

[0040] In block 704, the training data is applied to the neuro-fuzzy expert logic 108. The training uses a backpropagation technique that compares the results computed by the neuro-fuzzy expert logic 108 to results provided in the training data, and computes the deviation. Based on the deviation, the neural-fuzzy network weights of the fuzzy rules 506 are modified or membership functions of the fuzzy input terms 504 or fuzzy output terms 508 are adjusted. Weights associated with each of the rules 506 may be changed by starting from the output neurons and going backward through the network to the input neurons. The training executes these operations until the average error is no more than a predefined threshold value. During the training, rules found to be redundant or unnecessary may be deleted.

[0041] In block 706, after completion of training, the neuro-fuzzy expert logic 108 is validated by testing the logic 108 with sample data and analyzing the results. If the results are not satisfactory (validation fails in block 708), then training may be repeated until acceptable results are achieved. The neuro-fuzzy expert logic 108 may be optimized by manually changing one or more parameters of the logic.

[0042] If the trained system is deemed valid, then, in block 710, the neuro-fuzzy expert logic 108 can be applied to analyze events in the system 100. During operation the processed input and calculated output values can be stored for use as training data.

[0043] The training method 700 can be executed on a daily basis or as needed at any specified time interval. By training on a daily or regular basis, the neuro-fuzzy expert logic 108 can be continually and automatically tuned and updated.

[0044] The above discussion is meant to be illustrative of the principles and various embodiments of the present invention. Numerous variations and modifications will become apparent to those skilled in the art once the above disclosure is fully appreciated. It is intended that the following claims be interpreted to embrace all such variations and modifications.

CLAIMS

What is claimed is:

1. A system, comprising:

a processor;

neuro-fuzzy expert system logic executable by the processor to analyze and assign significance values to events occurring in a cloud infrastructure, the logic comprising:

a plurality of neuro-fuzzy logic modules, each of the logic modules comprising fuzzy logic to determine a fuzzy value of an effect of a detected event on the cloud infrastructure; and

event significance logic comprising neuro-fuzzy logic to determine, based on the values of the effects of the detected event determined by the plurality of neuro-fuzzy network modules, a value indicative of significance of the event to the cloud infrastructure.

2. The system of claim 1, wherein the plurality of neuro-fuzzy logic modules comprise:

event potential determination logic comprising fuzzy logic to determine a value of potential impact of the detected event on the cloud infrastructure;

event seriousness determination logic comprising fuzzy logic to determine a value of seriousness of the effect of the detected event on the cloud infrastructure;

event magnitude determination logic comprising fuzzy logic to determine a value of magnitude of effect of the event on the cloud infrastructure.

3. The system of claim 2, wherein the event potential determination logic is to determine the value of potential impact of the event on the cloud infrastructure based on a number of previously detected events that are similar to the detected event, a number of components previously affected by an event similar to the detected event, and a number of business services previously affected by an

event similar to the detected event; wherein the event seriousness determination logic is to determine the value of seriousness of the event based on a number of users of the cloud infrastructure currently affected by the detected event, urgency of services affected by the detected event, and current utilization levels of components affected by the detected event; wherein the event magnitude determination logic is to determine the value of magnitude of effect of the event on the cloud infrastructure based on a number of components affected by the detected event, a number of business services affected by the detected event, and a number of events similar to the detected event detected concurrently with the detected event.

4. The system of claim 1, wherein the plurality of logic modules and the event significance logic each comprises a plurality of layers, the plurality of layers comprising:

an input layer to map discrete values input to the logic module to input fuzzy term values;

a rules layer to apply fuzzy logic rules to the input fuzzy term values; and

an output layer to map output fuzzy term values generated by the rules layer to a fuzzy output value.

5. The system of claim 4, wherein each of the plurality of logic modules and the event significance logic further comprises an inference engine to specify a hierarchy for application of the fuzzy logic rules.

6. The system of claim 4, wherein the output layer is to generate a fuzzy output value and a crisp output value from the output fuzzy term values.

7. The system of claim 4, further comprising training logic to adjust the logic of the input layer, the rules layer, and the output layer of each of the plurality of logic modules and the event significance logic based on comparison of a training data set to outputs of the plurality of logic modules and the event significance logic.

8. A method, comprising:

detecting an event occurring in a cloud infrastructure;

applying neuro-fuzzy logic to determine effects of the event, the effects comprising:

a value of potential impact of the detected event on the cloud infrastructure;

a value of seriousness of the effect of the detected event on the cloud infrastructure;

a value of magnitude of effect of the event on the cloud infrastructure;

determining, via neuro-fuzzy logic, based on the value of potential impact, the value of seriousness, and the value of magnitude, a value indicative of significance of the event to the cloud infrastructure.

9. The method of claim 8, wherein the potential impact of the detected event is determined based on a number of previously detected events that are similar to the detected event, a number of components previously affected by an event similar to the detected event, and a number of business services previously affected by an event similar to the detected event.

10. The method of claim 8, wherein the value of seriousness of the event is based on a number of users of the cloud infrastructure currently affected by the detected event, urgency of services affected by the detected event, and current utilization levels of components affected by the detected event; and wherein the value of magnitude of effect of the event on the cloud infrastructure based on a number of components affected by the detected event, a number of business services affected by the detected event, and a number of events similar to the detected event detected concurrently with the detected event.

11. The method of claim 8, wherein the value of potential impact, the value of seriousness, the value of magnitude, and the value indicative of significance are each determined in a different neuro-fuzzy logic module, and the method further comprises:

processing the detected event in a plurality of layers of each neuro-fuzzy logic module, the processing comprising:

mapping, in an input layer, discrete input values to input fuzzy term values;

applying, a rules layer, fuzzy logic rules to the input fuzzy term values; and

mapping, in an output layer, fuzzy term values generated by the rules layer to a fuzzy output value.

12. The method of claim 11, further comprising specifying, in an inference engine, a hierarchy for application of the fuzzy logic rules.

13. The method of claim 11, further comprising to generating, in the output layer:

a discrete output value of significance from the output fuzzy term values; and

a fuzzy output value of significance from the output fuzzy term values.

14. The method of claim 11, further comprising adjusting logic of the input layer, the rules layer, and the output layer of each neuro-fuzzy logic module and the event significance logic based on comparison of a training data set to outputs of the neuro-fuzzy logic modules.

15. A non-transitory computer-readable medium encoded with instructions that when executed cause a processor to:

provide a neuro-fuzzy expert system to analyze and assign significance values to events occurring in a cloud infrastructure;

determine a fuzzy value of an effect of a detected event on the cloud infrastructure via a plurality of neuro-fuzzy logic modules, each of the logic modules comprising fuzzy logic; and

determine, based on the determined values of the effects of the detected event, a value of significance of the event to the cloud infrastructure; and

manage the event in the cloud infrastructure based on the determined value of significance;

wherein the plurality of neuro-fuzzy logic modules comprise:

event potential determination logic comprising fuzzy logic to determine a value of potential impact of the detected event on the cloud infrastructure;

event seriousness determination logic comprising fuzzy logic to determine a value of seriousness of the effect of the detected event on the cloud infrastructure; and

event magnitude determination logic comprising fuzzy logic to determine a value of magnitude of effect of the event on the cloud infrastructure.

FIG. 1

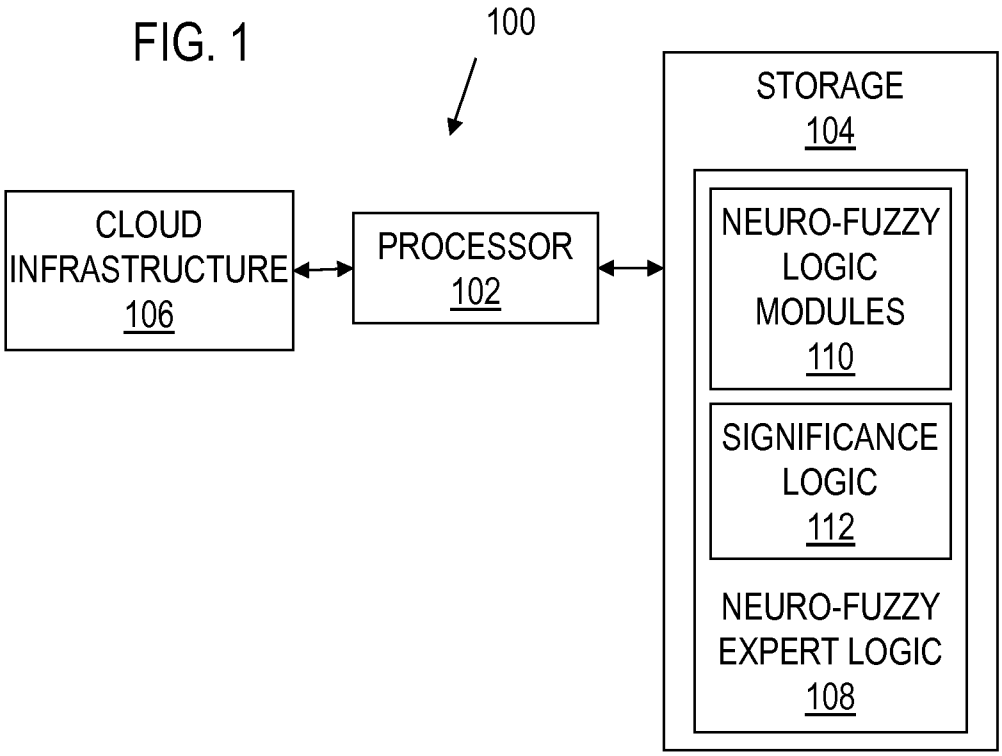

100
CLOUD INFRASTRUCTURE 106
PROCESSOR 102
STORAGE 104
NEURO-FUZZY LOGIC MODULES 110
SIGNIFICANCE LOGIC 112
NEURO-FUZZY EXPERT LOGIC 108

FIG. 2

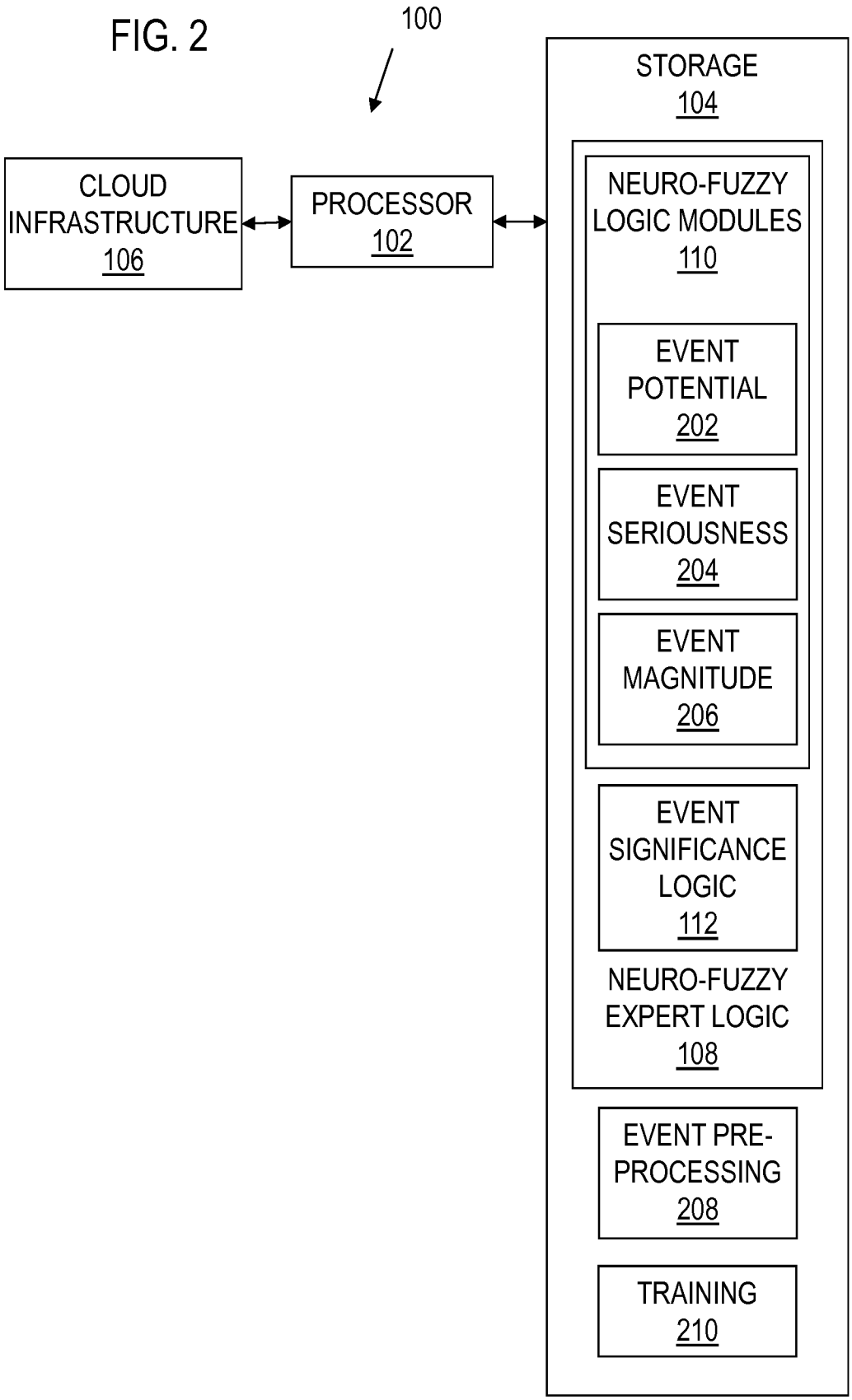
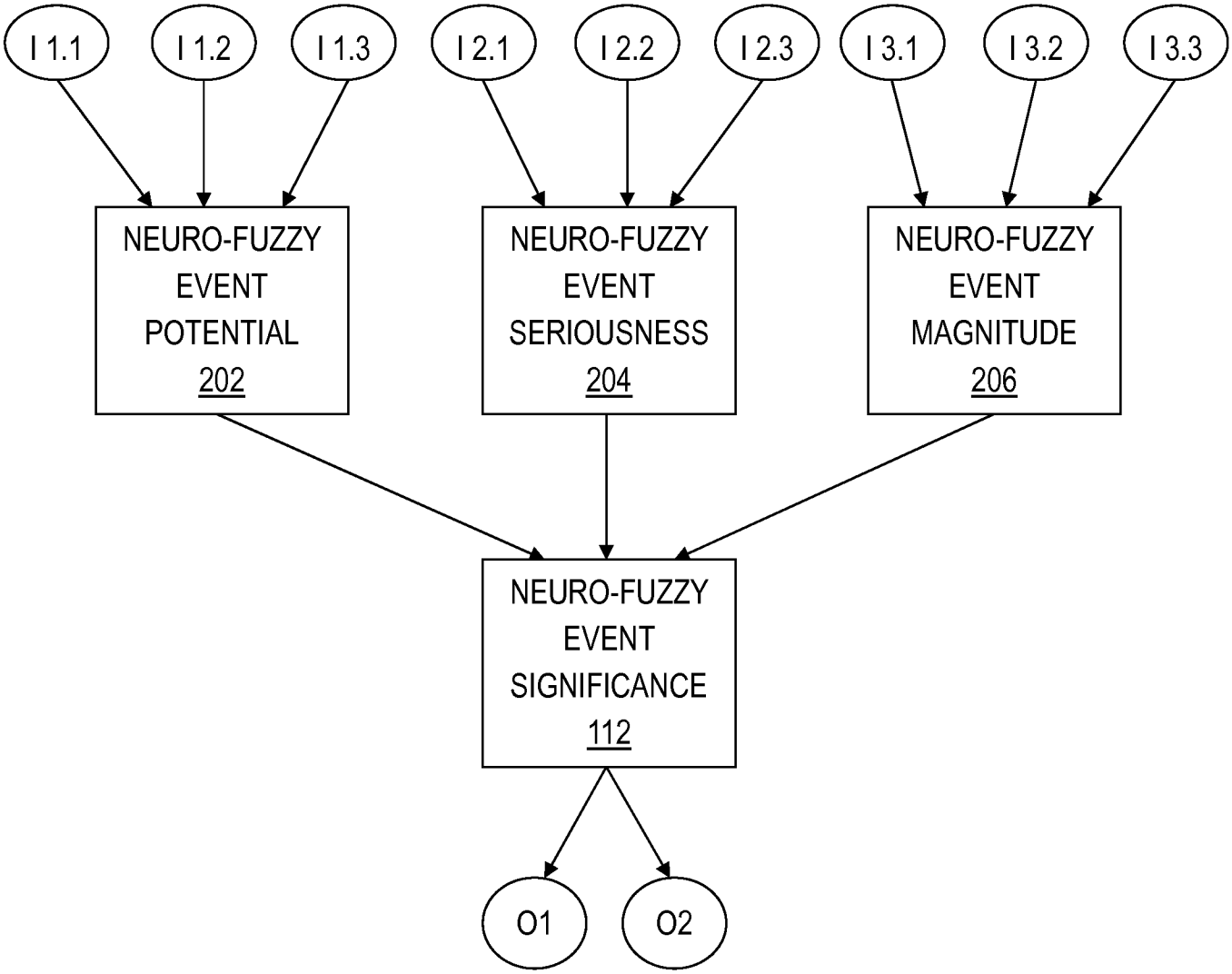

100
CLOUD INFRASTRUCTURE 106
PROCESSOR 102
STORAGE 104
NEURO-FUZZY LOGIC MODULES 110
EVENT POTENTIAL 202
EVENT SERIOUSNESS 204
EVENT MAGNITUDE 206
EVENT SIGNIFICANCE LOGIC 112
NEURO-FUZZY EXPERT LOGIC 108
EVENT PRE-PROCESSING 208
TRAINING 210

FIG. 3


I 1.1
I 1.2
I 1.3
I 2.1
I 2.2
I 2.3
I 3.1
I 3.2
I 3.3
NEURO-FUZZY EVENT POTENTIAL 202
NEURO-FUZZY EVENT SERIOUSNESS 204
NEURO-FUZZY EVENT MAGNITUDE 206
NEURO-FUZZY EVENT SIGNIFICANCE 112
O1
O2

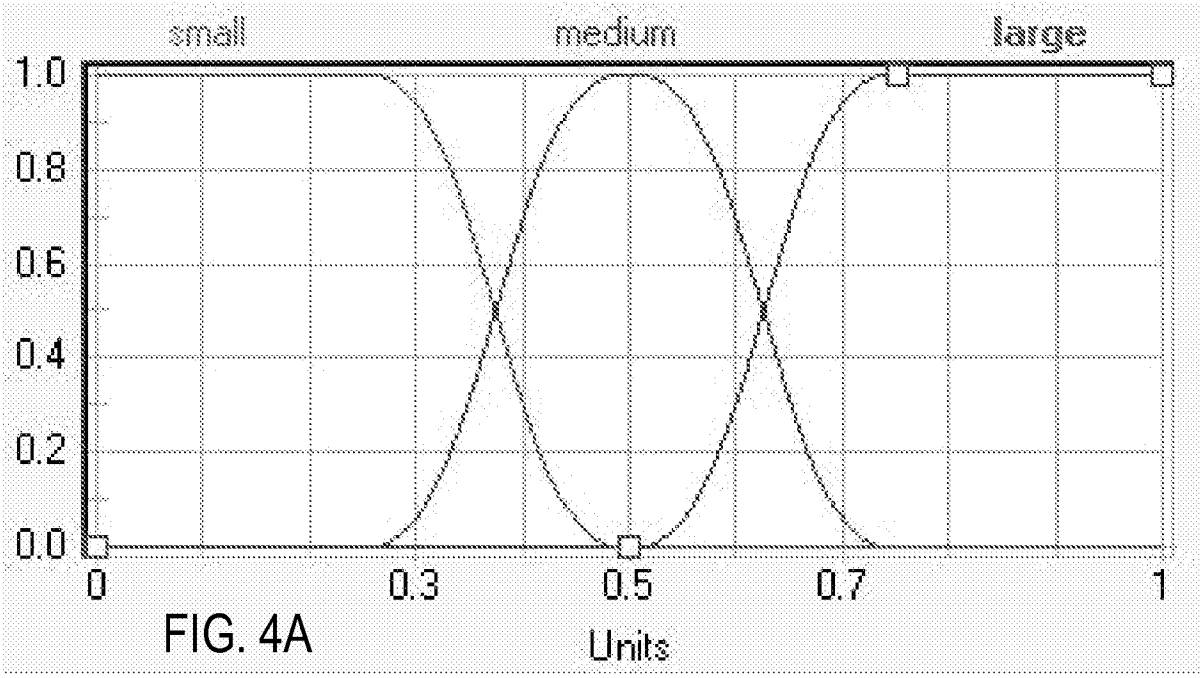

small
medium
large
1.0
0.8
0.6
0.4
0.2
0.0
0
0.3
0.5
0.7
1
Units

FIG. 4A

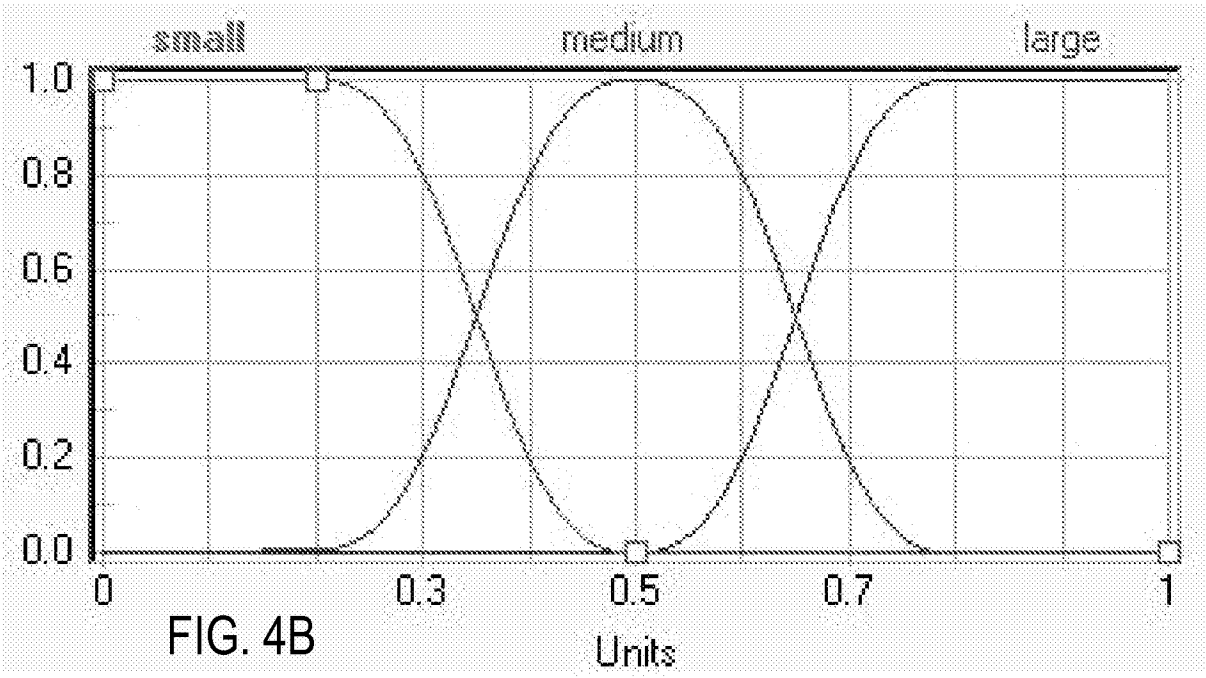

small
medium
large
1.0
0.8
0.6
0.4
0.2
0.0
0
0.3
0.5
0.7
1
Units

FIG. 4B

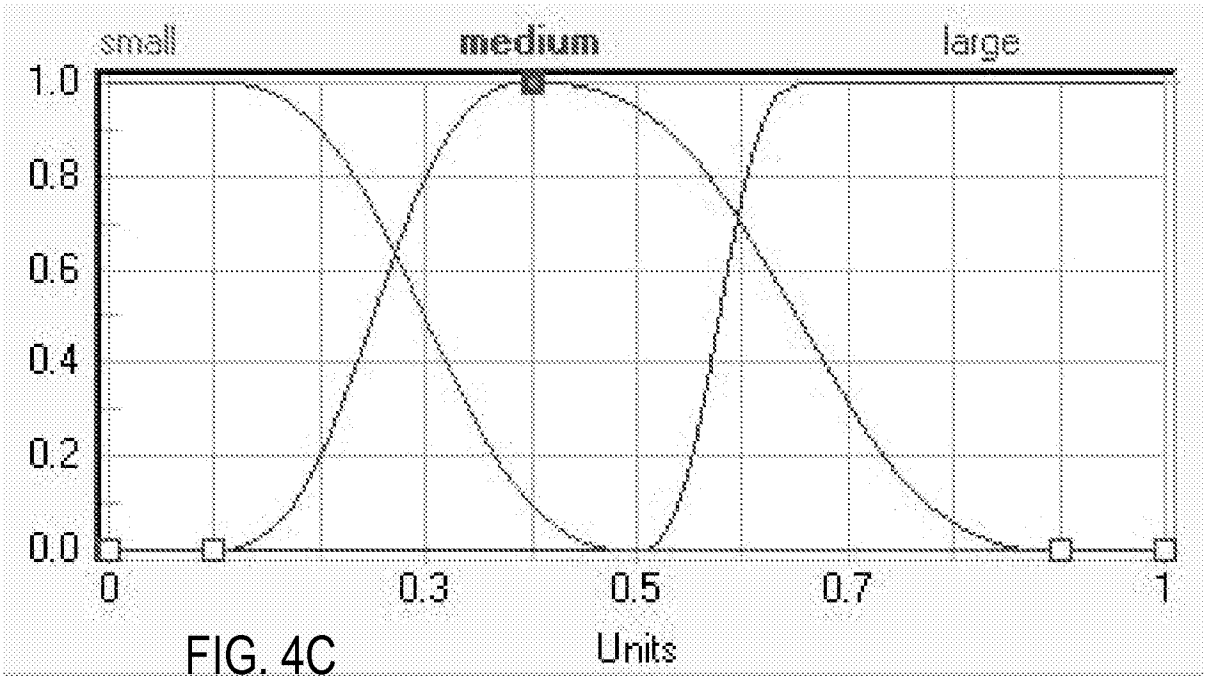

small
medium
large
1.0
0.8
0.6
0.4
0.2
0.0
0
0.3
0.5
0.7
1
Units

FIG. 4C

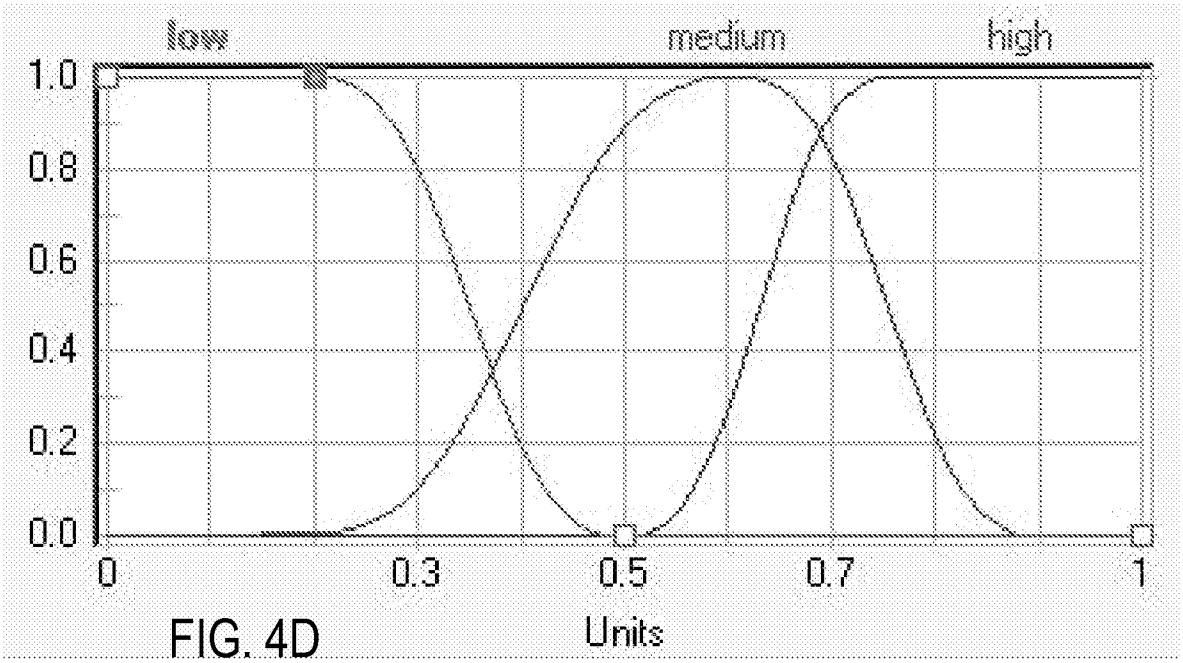

low
medium
high
1.0
0.8
0.6
0.4
0.2
0.0
0
0.3
0.5
0.7
1
Units

FIG. 4D

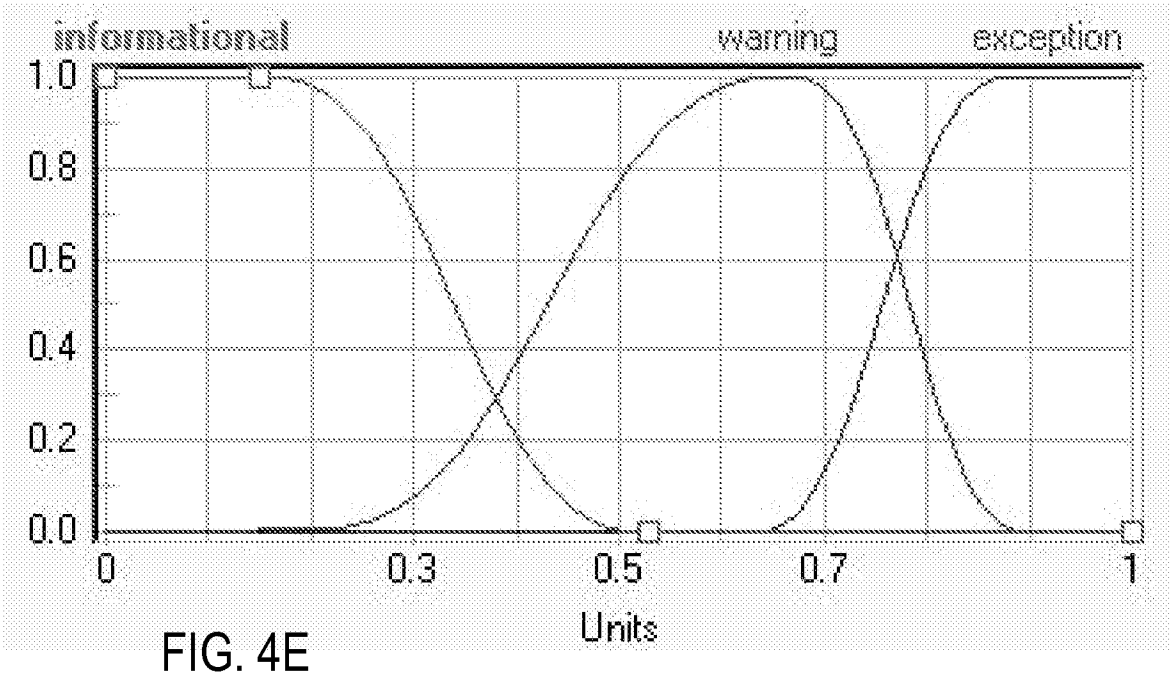

informational
warning
exception
1.0
0.8
0.6
0.4
0.2
0.0
0
0.3
0.5
0.7
1
Units

FIG. 4E

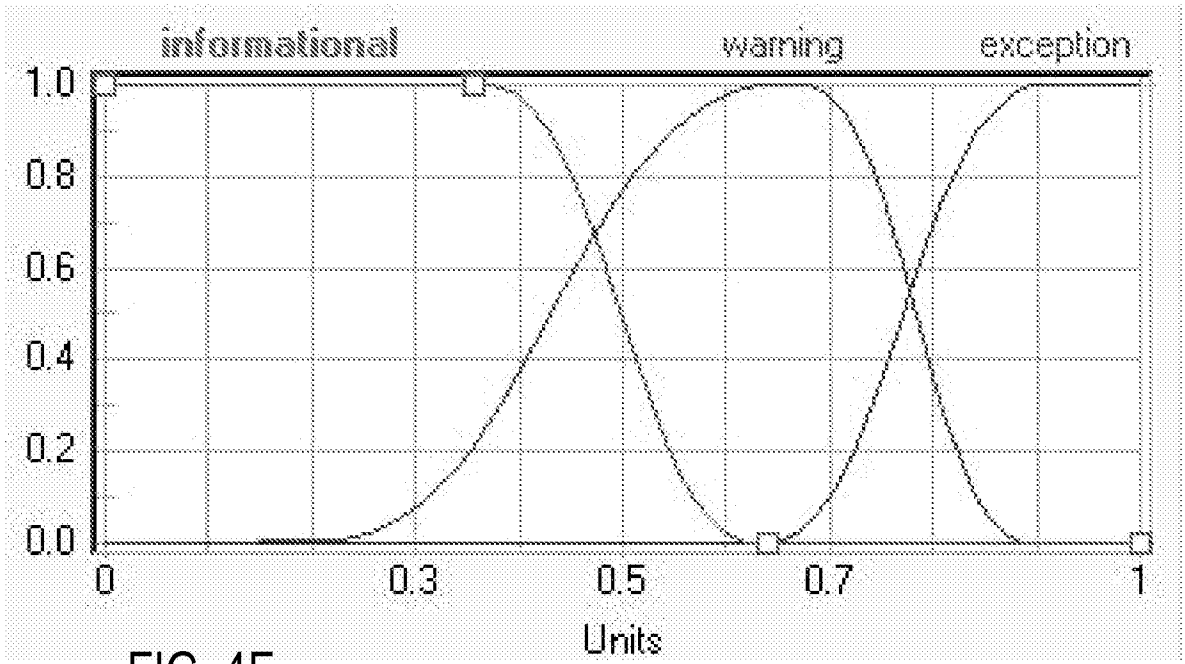

informational
warning
exception
1.0
0.8
0.6
0.4
0.2
0.0
0
0.3
0.5
0.7
1
Units

FIG. 4F

FIG. 5

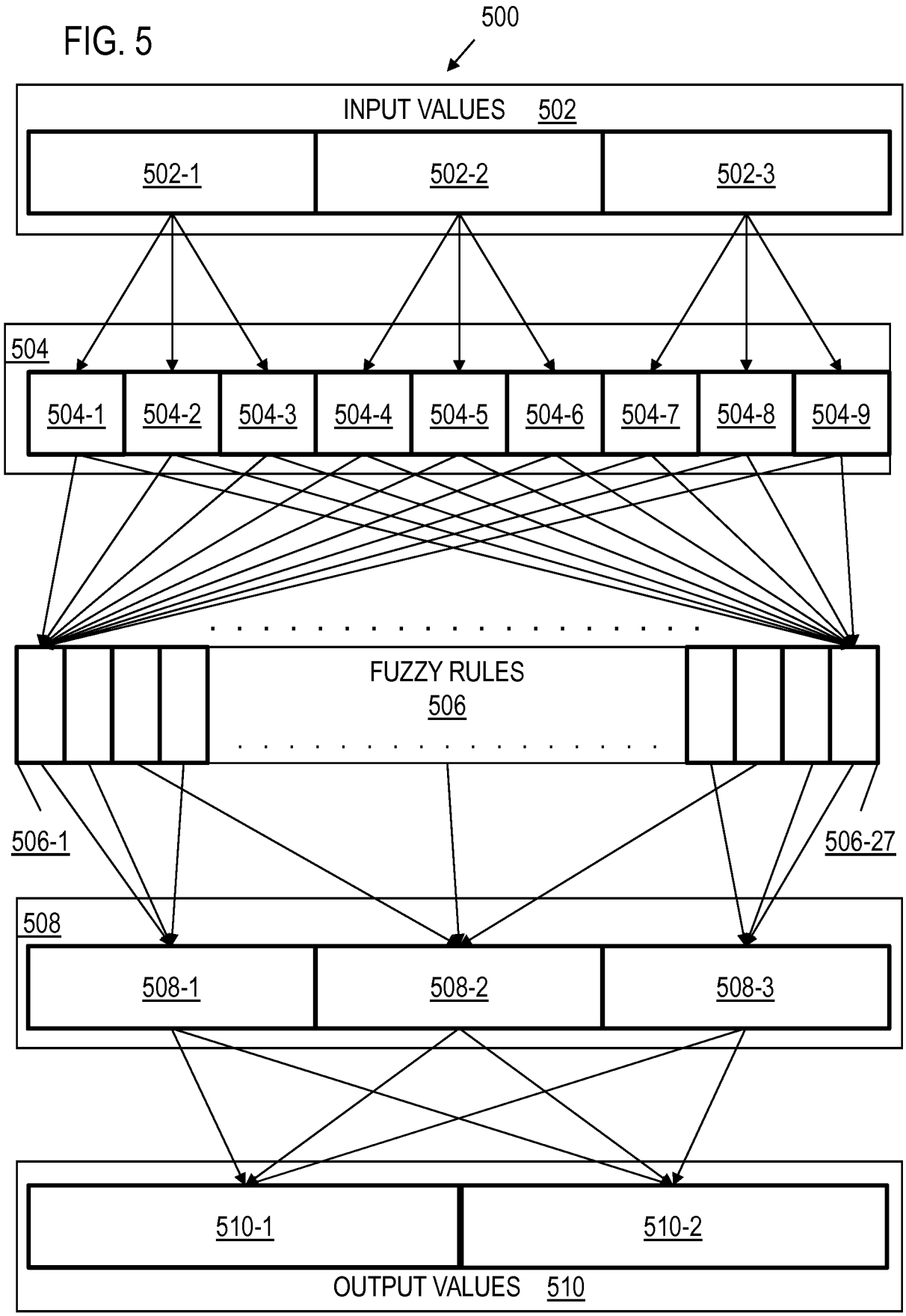

500
INPUT VALUES 502
502-1
502-2
502-3
504
504-1
504-2
504-3
504-4
504-5
504-6
504-7
504-8
504-9
FUZZY RULES
506
506-1
506-27
508
508-1
508-2
508-3
510-1
510-2
OUTPUT VALUES 510

FIG. 6

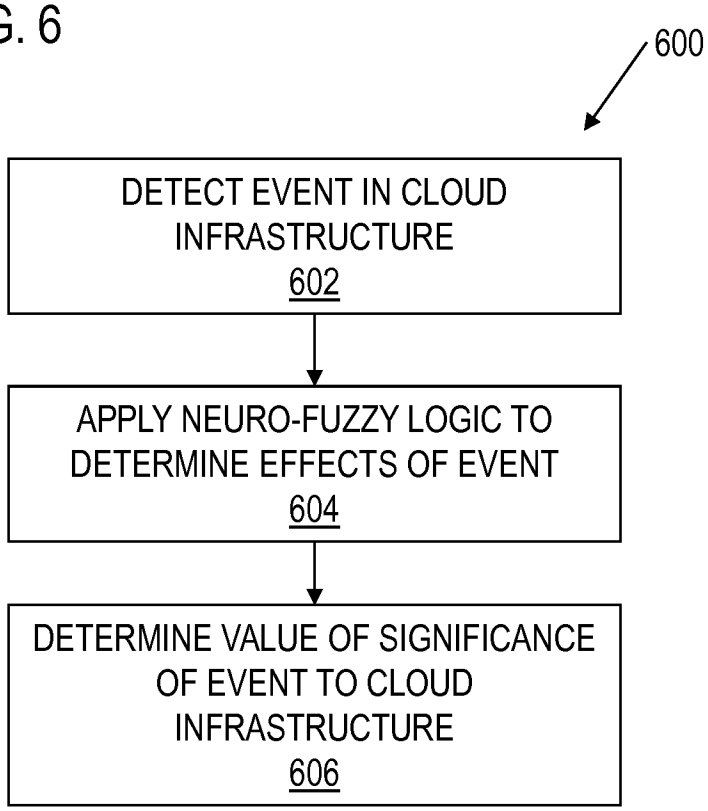
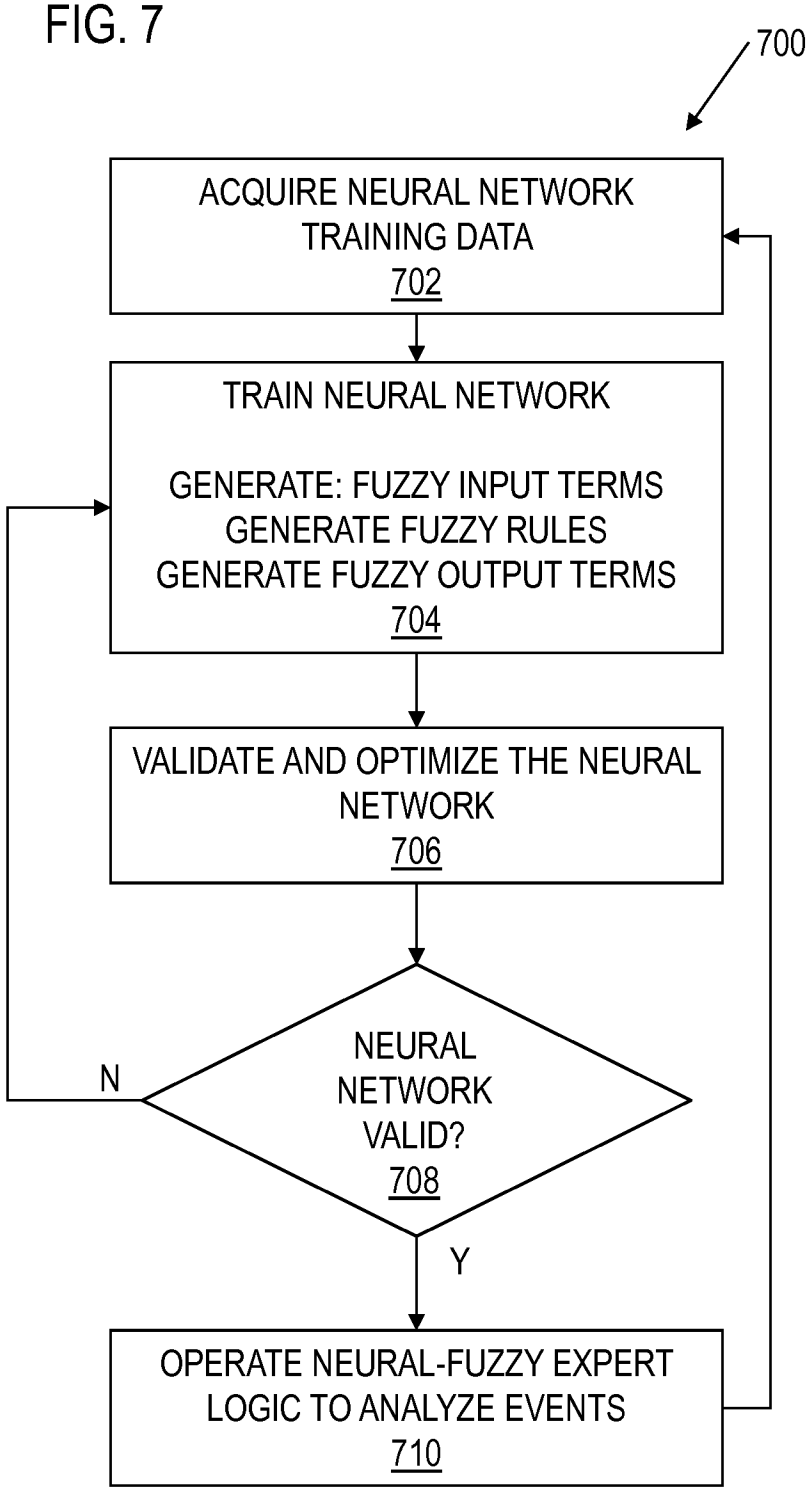

600
DETECT EVENT IN CLOUD INFRASTRUCTURE
602
APPLY NEURO-FUZZY LOGIC TO DETERMINE EFFECTS OF EVENT
604
DETERMINE VALUE OF SIGNIFICANCE OF EVENT TO CLOUD INFRASTRUCTURE
606

FIG. 7


700
ACQUIRE NEURAL NETWORK TRAINING DATA
702
TRAIN NEURAL NETWORK
GENERATE: FUZZY INPUT TERMS
GENERATE FUZZY RULES
GENERATE FUZZY OUTPUT TERMS
704
VALIDATE AND OPTIMIZE THE NEURAL NETWORK
706
NEURAL NETWORK VALID?
708
N
Y
OPERATE NEURAL-FUZZY EXPERT LOGIC TO ANALYZE EVENTS
710

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/048705

A. CLASSIFICATION OF SUBJECT MATTER

G06F 15/16(2006.01)i, G06N 7/02(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F 15/16; H04J 1/16; G06F 15/173; H04J 3/14; H04L 29/08; G06F 21/55; G06F 15/18; G06N 7/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: cloud, infrastructure, event, fuzzy

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2013-0305080 A1 (MICHAEL MAN BEHRENDT et al.) 14 November 2013 See abstract; paragraphs [0032]-[0052]; and figures 1-7.	1-15
A	US 2014-0075557 A1 (IGOR BALABINE et al.) 13 March 2014 See abstract; paragraphs [0046]-[0066]; claims 3-4; and figures 1-2.	1-15
A	US 2014-0095623 A1 (REX WIIG et al.) 03 April 2014 See abstract; paragraphs [0086]-[0091]; and figures 7A-7C.	1-15
A	US 06067287 A (CHUNG-JU; CHANG et al.) 23 May 2000 See abstract; column 5, line 28 - column 7, line 6; and figures 1-2.	1-15

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 April 2015 (21.04.2015)	**22 April 2015 (22.04.2015)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea
Facsimile No. ++82 42 472 7140

Authorized officer
CHOI, Jeong Kwon
Telephone No. +82-42-481-8507

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2014/048705

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013-0305080 A1	14/11/2013	US 8949676 B2	03/02/2015
US 2014-0075557 A1	13/03/2014	CA 2854883 A1	16/05/2013
		CN 104115463 A	22/10/2014
		EP 2777226 A1	17/09/2014
		JP 2015-502060 A	19/01/2015
		KR 10-2014-0106547 A	03/09/2014
		US 2013-0117847 A1	09/05/2013
		WO 2013-070631 A1	16/05/2013
		WO 2014-110293 A1	17/07/2014
US 2014-0095623 A1	03/04/2014	None	
US 06067287 A	23/05/2000	None	