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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 October 2022 (20.10.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/220902 A1

(51) International Patent Classification:
G06N 3/08 (2006.01) *G06N 3/04* (2006.01)

(21) International Application Number:
PCT/US2022/013768

(22) International Filing Date:
25 January 2022 (25.01.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
17/231,015 15 April 2021 (15.04.2021) US

(71) Applicant: **SALESFORCE.COM, INC.** [US/US]; 415 Mission Street, 3rd Floor, San Francisco, CA 94105 (US).

(72) Inventors: **ARPIT, Devansh**; 415 Mission Street, 3rd Floor, San Francisco, CA 94105 (US). **WANG, Huan**; 415 Mission Street, 3rd Floor, San Francisco, CA 94105 (US). **XIONG, Caiming**; 415 Mission Street, 3rd Floor, San Francisco, CA 94105 (US).

(74) Agent: **FARN, Michael, W.** et al.; Fenwick & West LLP, Silicon Valley Center, 801 California Street, Mountain View, CA 94041 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, ST, 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).

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

(54) **Title:** NEURAL NETWORK BASED ANOMALY DETECTION FOR TIME-SERIES DATA

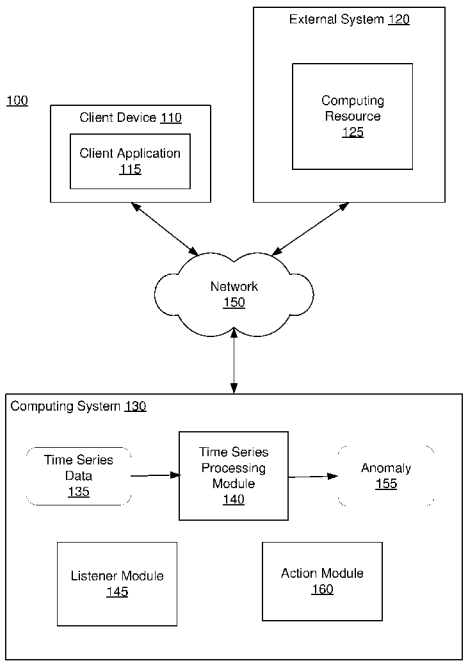

FIG. 1

(57) **Abstract:** A system uses a neural network to detect anomalies in time series data. The system trains the neural network for a fixed number of iterations using data from a time window of the time series. The system uses the loss value at the end of the fixed number of iterations for identifying anomalies in the time series data. For a time window, the system initializes the neural network to random values and trains the neural network for a fixed number of iterations using the data of the time window. After the fixed number of iterations, the system compares the loss values for various data points to a threshold value. Data points having loss value exceeding a threshold are identified as anomalous data points.

WO 2022/220902 A1

NEURAL NETWORK BASED ANOMALY DETECTION FOR TIME-SERIES DATA

BACKGROUND

FIELD OF ART

[0001] The disclosure relates to analysis of time series data in general and more specifically to using neural networks for identification of anomalies in time series data.

DESCRIPTION OF THE RELATED ART

[0002] Time-series data is generated and processed in several contexts. Examples of time series data include sensor data, data generated by instrumented software that monitors utilization of resources such as processing resources, memory resources, storage resources, network resources, application usage data, and so on. Anomaly detection is typically performed to identify issues with systems that generate time series data. For example, anomalies in computing resource utilization may be an indication of server failure that is likely to happen in near future. Similarly, anomalies in network resource utilization may be an indication of network failure that is likely to happen in near future. Accurate and timely detection of anomalies in time series data allows such failures to be predicted in advance so that preventive actions can be taken.

[0003] Various techniques are used for anomaly detection including, clustering analysis, random forest techniques, and machine learning based models, for example, neural networks. Conventional neural network based techniques for anomaly detection require large amount of training data and significant computing resources for training the neural network. Furthermore, if the characteristics of the time series data being analyzed are different from the time series data used for training the neural networks, the neural network based techniques have low accuracy.

BRIEF DESCRIPTION OF DRAWINGS

[0004] The disclosed embodiments have other advantages and features which will be

more readily apparent from the detailed description, the appended claims, and the accompanying figures (or drawings). A brief introduction of the figures is below.

[0005] Figure (FIG.) 1 is a block diagram of a system environment including a computing system for performing time series analysis, in accordance with an embodiment

[0006] FIG. 2 shows an example time series data and corresponding output of anomaly detection, in accordance with an embodiment.

[0007] FIG. 3 illustrates the system architecture of a time series processing module, in accordance with an embodiment.

[0008] FIG. 4 illustrates a neural network architecture used for anomaly detection, in accordance with an embodiment.

[0009] FIG. 5 illustrates the process of anomaly detection, in accordance with an embodiment.

[0010] FIG. 6 shows a flowchart illustrating the process of anomaly detection, according to an embodiment.

[0011] FIG. 7 is a high-level block diagram illustrating an example computer for implementing the client device and/or the computing system of FIG. 1.

[0012] The Figures (FIGS.) and the following description describe certain embodiments by way of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles described herein. Reference will now be made in detail to several embodiments, examples of which are illustrated in the accompanying figures.

DETAILED DESCRIPTION

[0013] A system performs anomaly detection for time series data using machine learning based models, for example, neural networks. The system trains the neural network for a fixed number of iterations using data from a time window of the time series. The system uses the loss value at the end of the fixed number of iterations for identifying anomalies in the time series data. The loss value may represent a difference between the predicted data value and the actual data value of the time-series corresponding to the time value. For example, the system compares the loss value to a predetermined threshold value. The system uses the loss value to adjust parameters of the neural network, for example, using back propagation. The system also uses the loss values determined during the training phase to determine whether a data point of the time series represents an anomaly. If the loss value for a time point exceeds

the threshold value, the system determines that the time value corresponds to an anomaly. In an embodiment, the anomaly is a point anomaly. The system performs the above steps for a new time interval. The system reinitializes the neural network for the new time interval and repeats the above steps.

[0014] Conventionally a neural network is trained using training dataset and the trained neural network is used at inference time to predict results. In contrast, the system according to various embodiments, determines anomalies during the training phase rather than through use of a trained neural network for making predictions.

[0015] The system trains the neural network using data within a time window and detects anomalies for data points within the time window based on the loss value determined during the time window. Conventional systems train a neural network until convergence, for example, until the loss value reaches below a threshold value. In contrast, the system according to various embodiments trains the neural network for a fixed number of iterations. After the fixed number of iterations, the system compares the loss values for data points within the time window with a threshold value. The system identifies data points having loss value exceeding the threshold value as anomalous data points. The system repeats the process for subsequent time intervals.

[0016] When the process is repeated for the next time window, the system discards the neural network trained using data of the previous time window. Accordingly, for each time window the system reinitializes the neural network, for example, using random values. Accordingly, the system does not train the neural network for future use as a predictor at inference time. The system simply runs the training process for using the loss determined during the training process for identifying point anomalies. After the anomalies are detected for a time window during the training phase of the neural network, the system discards the neural network and reinitializes the neural network using random values for the next time interval.

[0017] Furthermore, the system performs training of the neural network for a fixed number of iterations. Conventionally, the training of a neural network is performed until some convergence criteria is met, for example, until a loss value is below a threshold indicating convergence is reached. The system does not attempt to reach convergence but uses the training dynamics to determine anomalies. Accordingly, the system does not aim to generate a fully trained neural network.

[0018] As a result, the process used for detecting anomalies in time series data is computationally efficient as the neural network is trained only for a few iterations and not

until convergence. The accuracy of the techniques disclosed is either better or at least as good as other techniques that fully train the neural networks. Accordingly, the system achieves high accuracy with fewer computational resources. Therefore, the disclosed techniques improve the computational efficiency of the process of detecting anomalies in time series data and provide a technological advantage over conventional techniques.

OVERALL SYSTEM ENVIRONMENT

[0019] FIG. 1 is a block diagram of a system environment including a computing system for performing time series analysis, in accordance with an embodiment. The system environment 100 shown in FIG. 1 comprises a computing system 130, client device 110, an external system 120, and a network 150. In alternative configurations, different and/or additional components may be included in the system environment 100. The computing system 130 may be an online system or a system working offline, for example, by performing batch processing for performing anomaly detection.

[0020] The computing system 130 includes a time series processing module 140, a listener module 145, and an action module 160. The listener module 145 receives time series data 135 from one or more sources, for example, external systems 120. The time series processing module 140 performs anomaly detection on the time series data 135 to detect anomalies, for example point anomalies 155. The action module 160 takes an action based on the detected anomaly 155, for example, by sending an alert message to a user or taking an automated remedial action. In some embodiments, the computing system 130 itself may be the source of time series data.

[0021] FIG. 2 shows an example time series data and corresponding output of anomaly detection performed by the time series processing module 140, in accordance with an embodiment. The chart 210 represents the time series data 135 received by the listener module 140 and provided as input to the time series processing module 140. The time series processing module 140 outputs scores indicating occurrence of anomalies in the time series data shown in chart 210. Example scores determined based on the time series data of chart 210 are shown as chart 220. As shown in FIG. 2, the computing system 130 determines occurrence of an anomaly 155 if the scores generated by the time series processing module 140 exceed a predetermined threshold, for example, score increases at point 225 based on a point anomaly detected in time series data at point 215.

[0022] Anomaly detection may be performed for system maintenance, for example, to detect system problems in advance. For example, anomalies in computing resource utilization may be an indication of server failure that may happen in near future. Similarly,

anomalies in network resource utilization may be an indication of network failure that may happen in near future. Therefore, accurate and timely detection of anomalies if important for such time series data analysis.

[0023] The computing system 130 receives time series data 135 from sources, for example, from the external system 120. For example, the external system 120 includes computing resources 125 that generate time series data. Examples of computing resources including memory resources, processing resources, storage resources, network resources, and so on. The external system 120 may execute instrumented software that generates time series data representing resource usage of one or more resources. For example, the external system 120 may execute instrumented software that monitors the network usage and reports metrics indicating network usage on a periodic basis. The reported data represents a time series 135 that is received by the computing system 130. The time series processing module 140 may detect anomalies 155 that represent potential issues with a computing resource, for example, a potential failure that is likely to occur. The action module 160 may take appropriate action responsive to detection of the anomaly 155, for example, by sending an alert to a system administrator or by taking an automatic remedial action, for example, by allocating additional computing resources for a task or process if the system determines that the anomaly 155 indicates shortage of a particular computing resource allocated for the task or process. For example, the computing system 130 may determine that a point anomaly detected in a time series representing network usage indicates lack of sufficient network resources for a communication channel, the action module 160 may reallocate network resources to provide additional network bandwidth to the communication channel. As another example, the time series data may represent a number of pages swapped by a process and the anomaly 155 may be caused by an increase in the number of pages swapped indicating a shortage of storage resources. The action module 160 in response to detection of the anomaly 155 may allocate additional storage to the process.

[0024] Time series data 135 may be reported by other sources for example, sensors that monitor some real-world data and report it on a periodic basis, for example, temperature, pressure, weight, light intensity, and so on. For example, a sensor may monitor temperature or pressure of an industrial process that performs a chemical reaction and report it on a periodic basis as time series data 135. The action module 160 may perform an action that controls the industrial process in response to detection of the anomaly 155, for example, by controlling the industrial process to adjust the rate the chemical reaction.

[0025] The time series data 135 may represent user actions, for example, user interactions

with an online system. For example, the computing system 130 may monitor user interactions with an online system to detect anomalies in the user interaction. The point anomaly may be an indication of a change in user behavior or an issue with the online system receiving the user interactions. The action module 160 may take appropriate action based on detection of a point anomaly 155, for example, by sending an alert message to a user. The alert message may provide a recommendation of an action that the user may take to adjust the online system parameters in response to the anomaly detection. For example, if the anomaly 155 is determined as an indication of increase in demand for a specific product, the online system may initiate an online campaign for the product to provide additional users with information describing the product.

[0026] FIG. 1 shows a single instance of various components such as external system, client devices, and so on. However, there may be multiple instances of each of these components. For example, there may be several computing systems 130 and dozens or hundreds of client devices110 or external system 120 in communication with each computing system 130. The figures use like reference numerals to identify like elements. A letter after a reference numeral, such as "110a," indicates that the text refers specifically to the element having that particular reference numeral. A reference numeral in the text without a following letter, such as "110," refers to any or all of the elements in the figures bearing that reference numeral.

[0027] The client devices 110 are computing devices such as smartphones with an operating system such as ANDROID® or APPLE® IOS®, tablet computers, laptop computers, desktop computers, electronic stereos in automobiles or other vehicles, or any other type of network-enabled device on which digital content may be listened to or otherwise experienced. Typical client devices 110 include the hardware and software needed to connect to the network 150 (e.g., via Wifi and/or 4G or other wireless telecommunication standards).

[0028] The network 150 provides a communication infrastructure between the client devices 110, external systems 120, and computing system 130. The network 150 is typically the Internet, but may be any network, including but not limited to a Local Area Network (LAN), a Metropolitan Area Network (MAN), a Wide Area Network (WAN), a mobile wired or wireless network, a private network, or a virtual private network. Portions of the network 150 may be provided by links using communications technologies including WiFi based on the IEEE 802.11 standard, the BLUETOOTH short range standard, and the Wireless Universal Serial Bus (USB) standard.

SYSTEM ARCHITECTURE

[0029] FIG. 3 illustrates the system architecture of a time series processing module, in accordance with an embodiment. The time series processing module 140 comprises an anomaly detection module 310 and a time series database 360. The time series processing module 140 may perform various types of processing of the time series data including anomaly detection. The anomaly detection module 310 performs anomaly detection of time series data stored in time series database 360. The anomaly detection module 310 comprises a neural network 320, a loss determination module 340, a training module 330, and a threshold determination module 350. Conventional components such as network interfaces, security functions, load balancers, failover servers, management and network operation consoles, and the like are not shown so as to not obscure the details of the system architecture.

[0030] In an embodiment, the neural network 320 is a multi-layer perceptron. FIG. 4 illustrates a neural network architecture used for anomaly detection, in accordance with an embodiment. FIG. 4 shows an example neural network 400 that includes an input layer 410, one or more hidden layers 420, and an output layer 430. The input layer 410 is configured to receive a time value as input and the output layer 430 is configured to predict a data value corresponding to the input time value.

[0031] The loss determination module 340 determines a loss value based on the predictions of a neural network being trained. The loss value represents a difference between the predicted data value and the corresponding known data value of the time-series corresponding to the time value. For example, if the time series data value is D1 for a time value T1, the neural network predicts a value D1' and determines the loss value as based on a difference between D1' and D1. The loss value may be determined using any of various possible metrics, for example, root mean square, mean absolute value, and so on.

[0032] The training module 330 performs the training process of a neural network. The training module 330 initializes the neural network, for example, by setting the parameters of the neural network to random values. The training module 330 predicts values of the time series data using the neural network and determines the loss values by invoking the loss determination module 340. The training module 330 adjusts the parameters of the neural network based on the loss value, for example, using back propagation, to minimize the loss value.

[0033] The threshold determination module 350 determines the threshold value used for determining the point anomalies. The anomaly detection module 310 compares loss values of

the neural network with the threshold value determined by the threshold determination module 350 to determine whether a point anomaly exists at a time value in the time series data. In an embodiment, the threshold determination module 350 adjusts a threshold value based on comparison of anomalies identified and known anomalies. For example, the point anomalies may be presented to a user to receive feedback describing whether the point anomalies were identified accurately.

[0034] If the anomaly detection module 310 receives feedback indicating that one or more known point anomalies were not detected by the anomaly detection module 310, the threshold value may be reduced so that point anomalies similar to the missed point anomalies can be identified subsequently. If the anomaly detection module 310 receives feedback indicating that one or more known point anomalies were identified by the anomaly detection module 310 but were not actual point anomalies, the threshold value may be increased so that point anomalies similar to the spurious point anomalies previously identified get filtered out subsequently and are not detected. The threshold determination module 350 uses the adjusted threshold value for identifying anomalies for subsequent time windows.

ANOMALY DETECTION PROCESS

[0035] FIG. 5 illustrates the process of anomaly detection, in accordance with an embodiment. As shown in FIG. 5, the time series data 135 includes time values 510 and data values 520. For example, the time series data 135 may be represented as a sequence of tuples (T_n, D_n) where T_n represents a time value 510 and D_n represents a data value 520. The neural network 320 receives time values 510 as input and predicts data values 530. The loss determination module 320 receives as input the predicted data value 530 and the actual data value 520 of the time series and determines a loss value that is used as feedback for adjusting the parameters of the neural network. The loss values are used by the anomaly detection module 310 for determining anomalies 540 by comparing the loss values against a threshold value.

[0036] FIG. 6 shows a flowchart illustrating the process of anomaly detection, according to an embodiment. The steps described herein may be performed in an order different from that indicated herein. Furthermore, each step may be performed by a module different from that indicated herein.

[0037] The time series processing module 140 receives 610 a time-series comprising a sequence of data values. Each data value of the time series is associated with a time value. The time series processing module 140 processes different time windows of the time series data to determine point anomalies in each time window. A time window represents a range

of time values. Accordingly, the time series processing module 140 trains a neural network based on data values of the time window and detects point values within the time window based on the loss values determined during the training phase of the neural network based on the time series data of the time window. The time series processing module 140 repeats the following steps for each time window.

[0038] The time series processing module 140 identifies 620 a time window representing a range of time values. The time series processing module 140 initializes the neural network 630 for the time window. The time series processing module 140 trains the neural network for a predetermined number of iterations, by repeating the following steps 660, 670, and 680. For each iteration, the time series processing module 140 repeats the steps 660 and 670 for time values within the time window. For a time value of the time window, the time series processing module 140 executes 660 the neural network to predict a data value for the time value. The time series processing module 140 determines 670 a loss value based on the predicted data value. After repeating the steps 660 and 670 for a set of time values of the time window, the time series processing module 140 determines an aggregate loss value across the set of time values.

[0039] The time series processing module 140 adjusts 680 parameters of the neural network based on the aggregate loss value. The steps of determining the aggregate loss value and adjusting the parameters of the neural network are repeated for each iteration. After the predetermined number of iterations, the time series processing module 140 identifies 690 point anomalies in the time window as follows. If a loss value corresponding to a particular time value within the time window exceeds a threshold, the time series processing module 140 identifies the corresponding data value as an anomaly. The computing system 130 may store information describing the data values identified as point anomalies. The action module 160 may take actions based on the identified point anomalies, for example, sending an alert message to a user describing a point anomaly, sending the information describing the point anomaly for displaying via a user interface, recommending a remedial action based on the point anomaly, or performing a remedial action based on the point anomaly.

[0040] The time series processing module 140 initializes the neural network for each time window and discards the neural network at the end of processing of the time window. The neural network may be initialized by setting the parameter values of the neural network to random values. Accordingly, the time series processing module 140 performs the steps of training the neural network but does not use the trained neural network for any processing. The time series processing module 140 uses the loss value determined during the training

process to detect point anomalies in the time series data of the time window and then repeats the process for the next time window. Furthermore, the time series processing module 140 trains the neural network for a predetermined number of iterations rather than training the neural network until an aggregate loss value is below a threshold value. The predetermined number of iterations may be configurable by a user or set to a default value. The predetermined number of iterations is set to a value that is less than the number of iterations required to ensure that the aggregate loss value reaches below a threshold value. This ensures that the anomaly detection process is executed efficiently since the goal of the time series processing module 140 is not to generate a trained model that can be used at inference time for making predictions but only to go through a partial training process so that the loss value during the partial training process can be used to identify the point anomalies.

PERFORMANCE IMPROVEMENT

[0041] Experimental data shows improvement in performance obtained by using the techniques disclosed herein. The following table shows F1 scores obtained by executing various models on different datasets. The F1 score is calculated as F1 = 2*precision*recall/(precision+recall). Each column represents a particular dataset and each row represents a particular model. The disclosed techniques were compared against other models including WinStats, ISF, RRCF (robust random cut forest), and Prophet. The first row represents the data for a system according to an embodiment as disclosed and the remaining rows represent other models that do not use the techniques disclosed, for example, (1) WinStats (Window statistics) a technique that uses statistics of data in the time series to determine which specific points are anomalous, (2) ISF (isolation forest): a technique based on decision tree algorithm, (3) RRCF (robust random cut forest): a technique similar to isolation forest but modified to work on streaming data, and (3) Prophet: a regression model based approach.

	Yahoo A1	Yahoo A2	Yahoo A3	Yahoo A4	IOps	NAB all	Average
Disclosed System (no retraining)	0.48	0.72	0.89	0.59	0.28	0.22	**0.53**
WinStats (retrain daily)	**0.49**	0.63	0.10	0.15	**0.35**	**0.25**	0.33

ISF (retrain 7d)	0.30	0.46	0.58	0.23	0.32	0.21	0.35
RRCF (retrain 7d)	0.26	0.47	0.42	0.16	0.29	0.20	0.30
Prophet (retrain 7d)	0.27	0.66	**0.97**	0.43	0.04	0.16	0.42

TABLE I

[0042] As shown in the table above, the F1 scores of the system based on the disclosed techniques performed either better than all the models tested or close to the best model although the system predicts the anomaly without requiring any retraining. For example, the "average" column at the end represents the average performance of all the models for various data sets and shows that the average performance of the system as disclosed is better than all the models that were studied. Accordingly, the system disclosed is efficient computationally since it requires significantly fewer computing resources used in training of the model compared to other techniques while performing at least as well as the other techniques or better. The average performance of the disclosed techniques across all data sets was better than all the other techniques tested.

COMPUTER ARCHITECTURE

[0043] FIG. 7 is a high-level block diagram illustrating an example computer for implementing the client device and/or the computing system of FIG. 1. The computer 700 includes at least one processor 702 coupled to a chipset 704. The chipset 704 includes a memory controller hub 720 and an input/output (I/O) controller hub 722. A memory 706 and a graphics adapter 712 are coupled to the memory controller hub 720, and a display 718 is coupled to the graphics adapter 712. A storage device 708, an input device 714, and network adapter 716 are coupled to the I/O controller hub 722. Other embodiments of the computer 700 have different architectures.

[0044] The storage device 708 is a non-transitory computer-readable storage medium such as a hard drive, compact disk read-only memory (CD-ROM), DVD, or a solid-state memory device. The memory 706 holds instructions and data used by the processor 702. The input interface 714 is a touch-screen interface, a mouse, track ball, or other type of pointing device, a keyboard, or some combination thereof, and is used to input data into the computer 700. In some embodiments, the computer 700 may be configured to receive input

(e.g., commands) from the input interface 714 via gestures from the user. The graphics adapter 712 displays images and other information on the display 718. The network adapter 716 couples the computer 700 to one or more computer networks.

[0045] The computer 700 is adapted to execute computer program modules for providing functionality described herein. As used herein, the term "module" refers to computer program logic used to provide the specified functionality. Thus, a module can be implemented in hardware, firmware, and/or software. In one embodiment, program modules are stored on the storage device 708, loaded into the memory 706, and executed by the processor 702.

[0046] The types of computers 700 used by the entities of FIG. 1 can vary depending upon the embodiment and the processing power required by the entity. The computers 700 can lack some of the components described above, such as graphics adapters 712, and displays 718. For example, the computing system 130 can be formed of multiple blade servers communicating through a network such as in a server farm.

ALTERNATIVE EMBODIMENTS

[0047] It is to be understood that the Figures and descriptions of the disclosed invention have been simplified to illustrate elements that are relevant for a clear understanding of the present invention, while eliminating, for the purpose of clarity, many other elements found in a typical distributed system. Those of ordinary skill in the art may recognize that other elements and/or steps are desirable and/or required in implementing the embodiments. However, because such elements and steps are well known in the art, and because they do not facilitate a better understanding of the embodiments, a discussion of such elements and steps is not provided herein. The disclosure herein is directed to all such variations and modifications to such elements and methods known to those skilled in the art.

[0048] Some portions of above description describe the embodiments in terms of algorithms and symbolic representations of operations on information. These algorithmic descriptions and representations are commonly used by those skilled in the data processing arts to convey the substance of their work effectively to others skilled in the art. These operations, while described functionally, computationally, or logically, are understood to be implemented by computer programs or equivalent electrical circuits, microcode, or the like. Furthermore, it has also proven convenient at times, to refer to these arrangements of operations as modules, without loss of generality. The described operations and their associated modules may be embodied in software, firmware, hardware, or any combinations thereof.

[0049] As used herein any reference to "one embodiment" or "an embodiment" means that a particular element, feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

[0050] Some embodiments may be described using the expression "coupled" and "connected" along with their derivatives. It should be understood that these terms are not intended as synonyms for each other. For example, some embodiments may be described using the term "connected" to indicate that two or more elements are in direct physical or electrical contact with each other. In another example, some embodiments may be described using the term "coupled" to indicate that two or more elements are in direct physical or electrical contact. The term "coupled," however, may also mean that two or more elements are not in direct contact with each other, but yet still co-operate or interact with each other. The embodiments are not limited in this context.

[0051] As used herein, the terms "comprises," "comprising," "includes," "including," "has," "having" or any other variation thereof, are intended to cover a non-exclusive inclusion. For example, a process, method, article, or apparatus that comprises a list of elements is not necessarily limited to only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. Further, unless expressly stated to the contrary, "or" refers to an inclusive or and not to an exclusive or. For example, a condition A or B is satisfied by any one of the following: A is true (or present) and B is false (or not present), A is false (or not present) and B is true (or present), and both A and B are true (or present).

[0052] In addition, use of the "a" or "an" are employed to describe elements and components of the embodiments herein. This is done merely for convenience and to give a general sense of the invention. This description should be read to include one or at least one and the singular also includes the plural unless it is obvious that it is meant otherwise.

[0053] Upon reading this disclosure, those of skill in the art will appreciate still additional alternative structural and functional designs for a system and a process for displaying charts using a distortion region through the disclosed principles herein. Thus, while particular embodiments and applications have been illustrated and described, it is to be understood that the disclosed embodiments are not limited to the precise construction and components disclosed herein. Various modifications, changes and variations, which will be apparent to those skilled in the art, may be made in the arrangement, operation and details of the method

and apparatus disclosed herein without departing from the spirit and scope defined in the appended claims.

We claim:

1. A computer implemented method for identifying anomalies in time-series data, the method comprising:

receiving a time-series comprising a sequence of data values, each data value associated with a time value;

identifying a time window representing a range of time values;

identifying anomalies of the time-series data in the time window, comprising:

initializing a neural network configured to receive an input time value and predict a data value of the time-series for the input time value;

training the neural network for a predetermined number of iterations, comprising:

for one or more time values of the time window:

executing the neural network to predict a data value for the time value, and

determining a loss value based on the predicted data value;

adjusting parameters of the neural network based on the loss values;

determining anomalies in the time window after the predetermined number of iterations comprising:

responsive to a loss value corresponding to a time value exceeding a threshold, identifying the corresponding data value as an anomaly; and

storing information describing one or more data values identified as anomalies.

2. The computer implemented method of claim 1, wherein the time anomaly is a point time anomaly.

3. The computer implemented method of claim 1, wherein initializing the neural network comprises assigning random values to parameters of the neural network.

4. The computer implemented method of claim 1, wherein the time window is a first time window, the range of time values is a first range of time values, the method comprising:

identifying a second time window representing a second range of time values;

identifying anomalies in the second time window, comprising:

reinitializing the neural network for the second time window;

training the neural network for the predetermined number of iterations using data values of the second time window; and

responsive to a loss value for a time value of the second time window exceeding

the threshold, identifying the data value for the time value as an anomaly.

5. The computer implemented method of claim 1, wherein a loss value represents a difference between the predicted data value and the data value of the time-series corresponding to the time value.

6. The computer implemented method of claim 1, wherein adjusting parameters of the neural network comprises:

determining an aggregate loss value based on the loss values corresponding to the time values of the time window; and

adjusting parameters of the neural network based on the aggregate loss value.

7. The computer implemented method of claim 1, wherein the time-series represents resource utilization of a computing resource, the method further comprising:

identifying a potential resource failure based on the identified anomalies; and

sending a message reporting the potential resource failure.

8. The computer implemented method of claim 7, wherein the computing resource is one of:

a processing resource,

a memory resource,

a network resource, or

a storage resource.

9. The computer implemented method of claim 7, wherein the time-series represents resource utilization of a computing resource, the method further comprising:

taking a remedial action for preventing the potential resource failure.

10. The computer implemented method of claim 1, wherein the neural network is a multi-layered perceptron configured to receive a scalar input and output a scalar value.

11. The computer implemented method of claim 1, further comprising.

adjusting the threshold value based on comparison of one or more anomalies identified and known anomalies; and

using the adjusted threshold value for identifying anomalies for one or more other time windows.

12. A non-transitory computer readable storage medium storing instructions that when executed by the one or more computer processors causes the one or more computer processors to:

receive a time-series comprising a sequence of data values, each data value associated with a time value;

identify a time window representing a range of time values;

identify anomalies of the time-series data in the time window, wherein the identifying causes the one or more computer processors to:

initialize a neural network configured to receive an input time value and predict a data value of the time-series for the input time value;

train the neural network for a predetermined number of iterations, wherein the training causes the one or more computer processors to:

for one or more time values of the time window:

execute the neural network to predict a data value for the time value, and

determine a loss value based on the predicted data value;

adjust parameters of the neural network based on the loss values;

determine anomalies in the time window after the predetermined number of iterations wherein the determining anomalies causes the one or more computer processors to:

responsive to a loss value corresponding to a time value exceeding a threshold, identify the corresponding data value as an anomaly; and

store information describing one or more data values identified as anomalies.

13. The non-transitory computer readable storage medium of claim 12, wherein the time window is a first time window, the range of time values is a first range of time values, wherein the instructions further cause the one or more computer processors to:

identify a second time window representing a second range of time values;

identify anomalies in the second time window, by causing the one or more computer processors to:

reinitialize the neural network for the second time window;

train the neural network for the predetermined number of iterations using data values of the second time window; and

responsive to a loss value for a time value of the second time window exceeding

the threshold, identify the data value for the time value as an anomaly.

14. The non-transitory computer readable storage medium of claim 12, wherein instructions for adjusting parameters of the neural network cause the one or more computer processors to:

determine an aggregate loss value based on the loss values corresponding to the time values of the time window; and

adjust parameters of the neural network based on the aggregate loss value.

15. The non-transitory computer readable storage medium of claim 12, wherein the time-series represents resource utilization of a computing resource, wherein the instructions further cause the one or more computer processors to:

identify a potential resource failure based on the identified anomalies; and

send a message reporting the potential resource failure.

16. The non-transitory computer readable storage medium of claim 12, wherein the instructions further cause the one or more computer processors to:

adjust the threshold value based on comparison of one or more anomalies identified and known anomalies; and

use the adjusted threshold value for identifying anomalies for one or more other time windows.

17. A computer system comprising:

one or more computer processors; and

non-transitory computer readable storage medium storing instructions that when executed by the one or more computer processors causes the one or more computer processors to:

receive a time-series comprising a sequence of data values, each data value associated with a time value;

identify a time window representing a range of time values;

identify anomalies of the time-series data in the time window, wherein the identifying causes the one or more computer processors to:

initialize a neural network configured to receive an input time value and predict a data value of the time-series for the input time value;

train the neural network for a predetermined number of iterations, wherein the training causes the one or more computer processors to:

for one or more time values of the time window:

execute the neural network to predict a data value for the time value, and

determine a loss value based on the predicted data value;

adjust parameters of the neural network based on the loss values;

determine anomalies in the time window after the predetermined number of iterations wherein the determining anomalies causes the one or more computer processors to:

responsive to a loss value corresponding to a time value exceeding a threshold, identify the corresponding data value as an anomaly; and

store information describing one or more data values identified as anomalies.

18. The computer system of claim 17, wherein the time window is a first time window, the range of time values is a first range of time values, wherein the instructions further cause the one or more computer processors to:

identify a second time window representing a second range of time values;

identify anomalies in the second time window, by causing the one or more computer processors to:

reinitialize the neural network for the second time window;

train the neural network for the predetermined number of iterations using data values of the second time window; and

responsive to a loss value for a time value of the second time window exceeding the threshold, identify the data value for the time value as an anomaly.

19. The computer system of claim 17, wherein instructions for adjusting parameters of the neural network cause the one or more computer processors to:

determine an aggregate loss value based on the loss values corresponding to the time values of the time window; and

adjust parameters of the neural network based on the aggregate loss value.

20. The computer system of claim 17, wherein the instructions further cause the one or more computer processors to:

adjust the threshold value based on comparison of one or more anomalies identified and

known anomalies; and

use the adjusted threshold value for identifying anomalies for one or more other time windows.

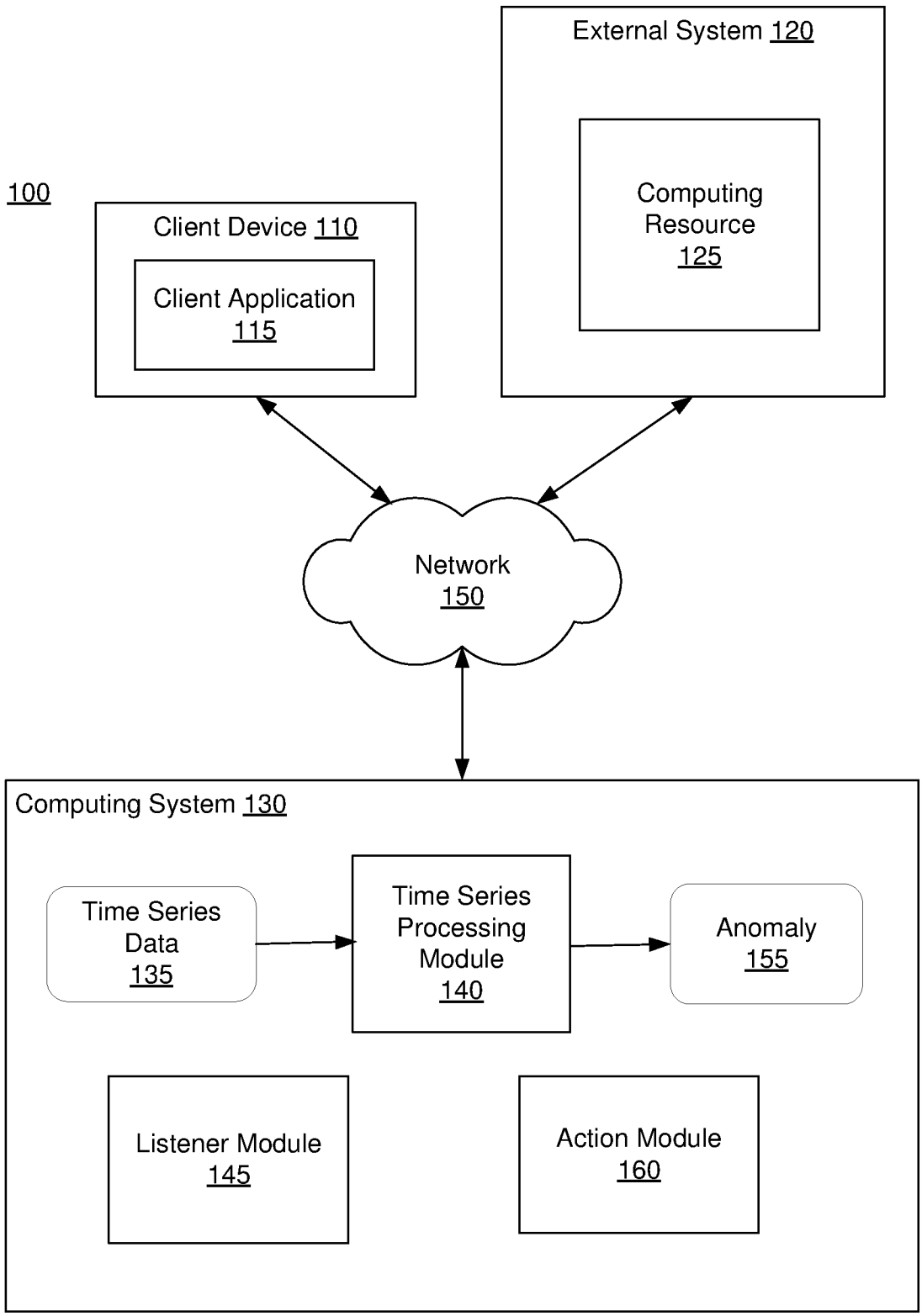
External System 120
Computing Resource 125
100
Client Device 110
Client Application 115
Network 150
Computing System 130
Time Series Data 135
Time Series Processing Module 140
Anomaly 155
Listener Module 145
Action Module 160

FIG. 1

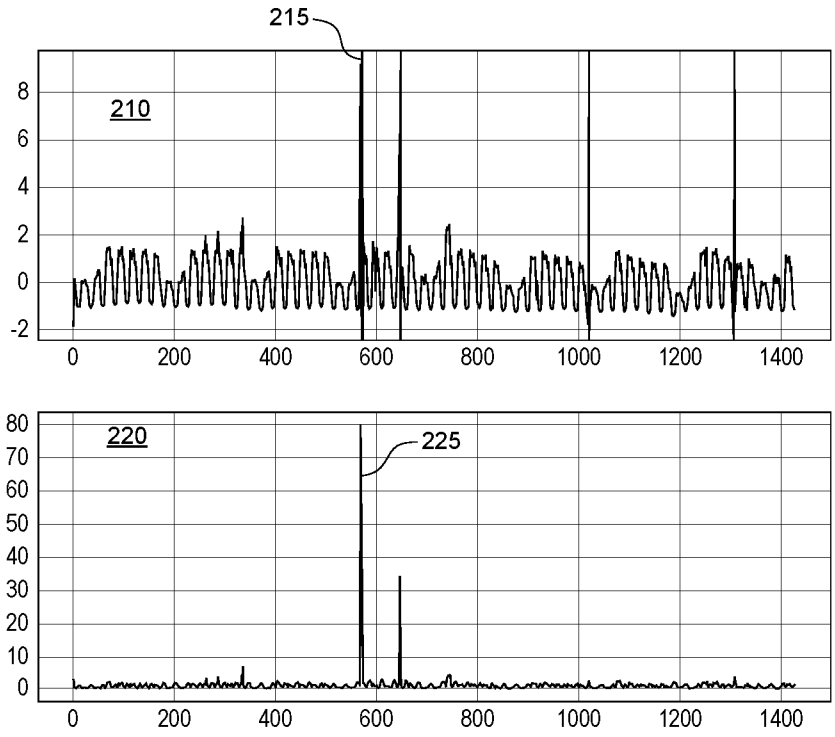
215
210
8
6
4
2
0
-2
0
200
400
600
800
1000
1200
1400
220
225
80
70
60
50
40
30
20
10
0
0
200
400
600
800
1000
1200
1400

FIG. 2

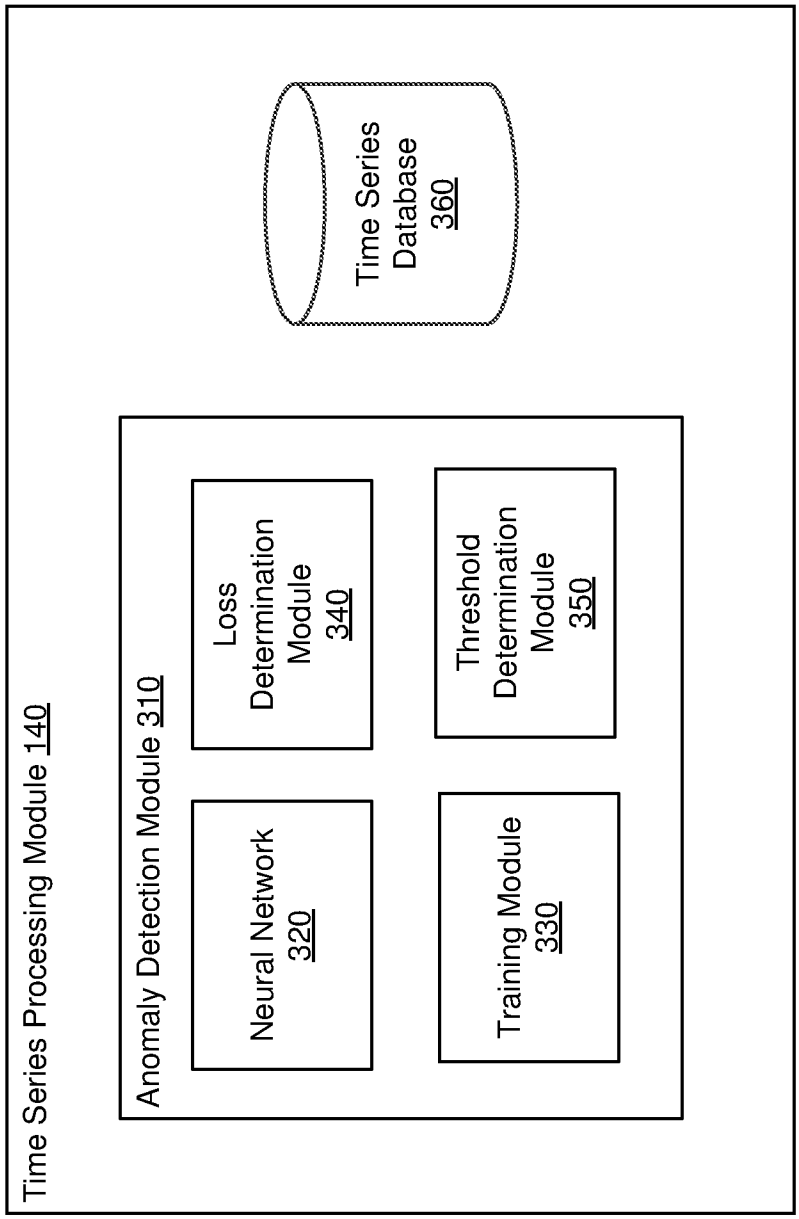
Time Series Processing Module 140
Anomaly Detection Module 310
Neural Network 320
Loss Determination Module 340
Training Module 330
Threshold Determination Module 350
Time Series Database 360

FIG. 3

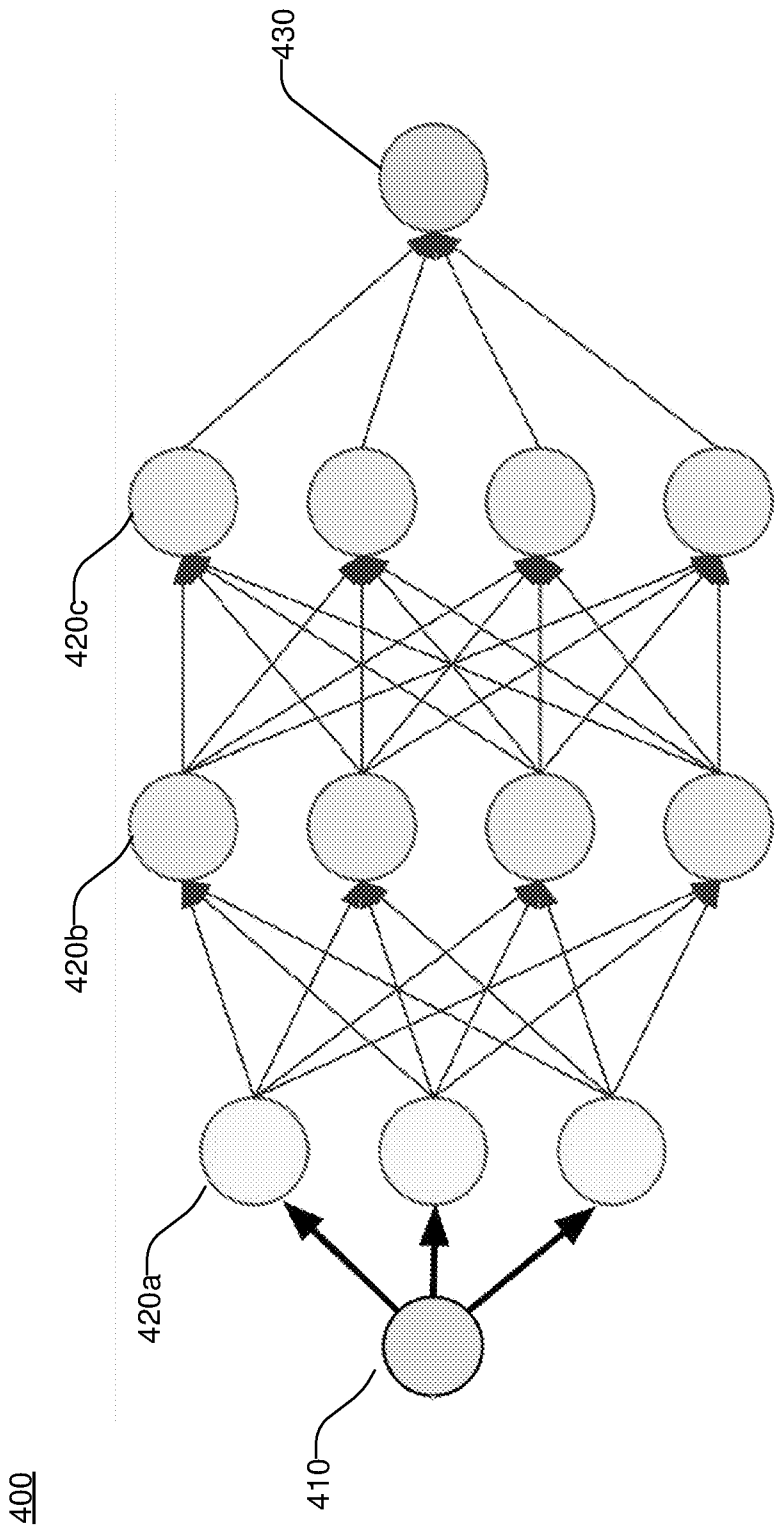

FIG. 4

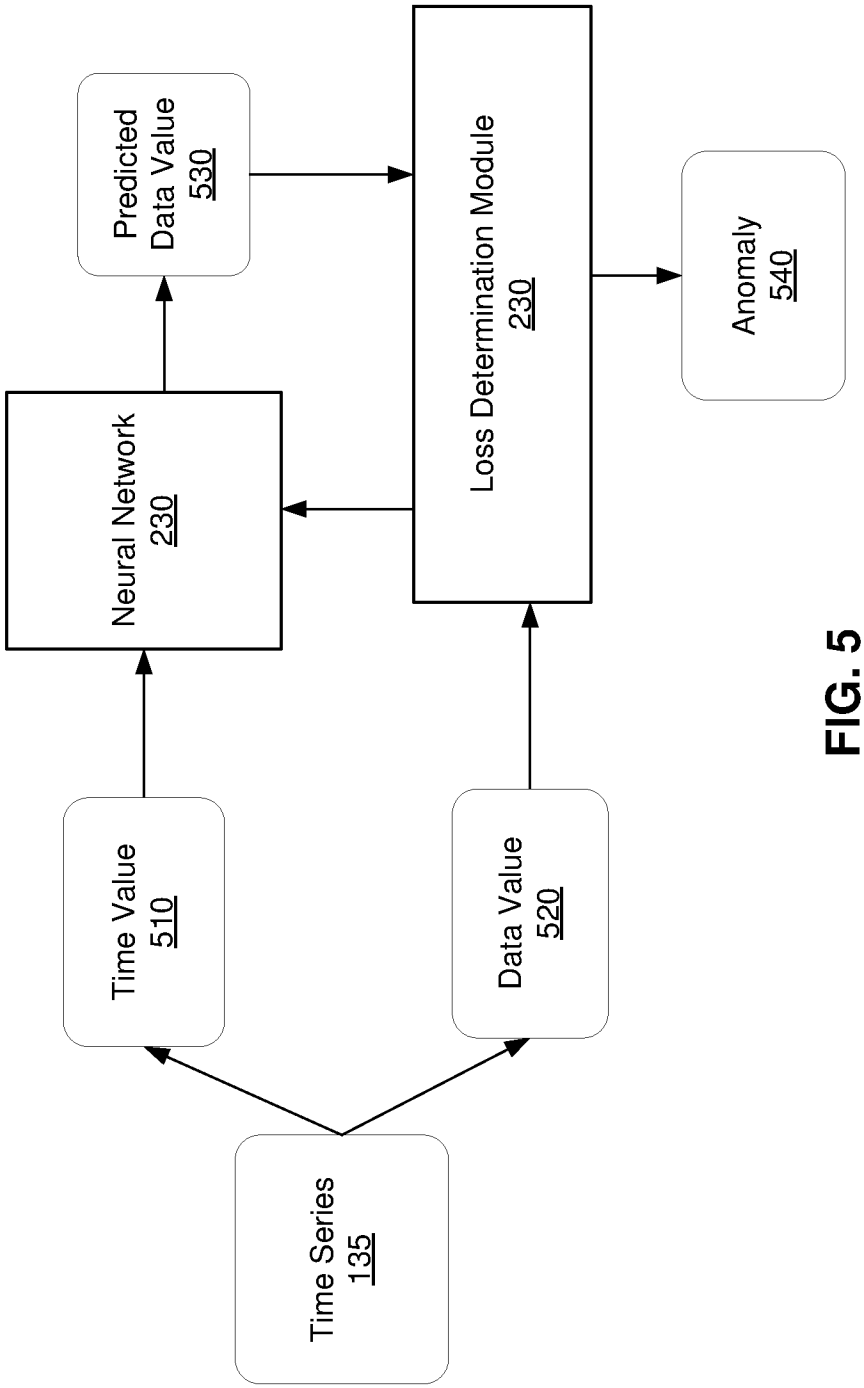
Time Series
135
Time Value
510
Data Value
520
Neural Network
230
Predicted
Data Value
530
Loss Determination Module
230
Anomaly
540

FIG. 5

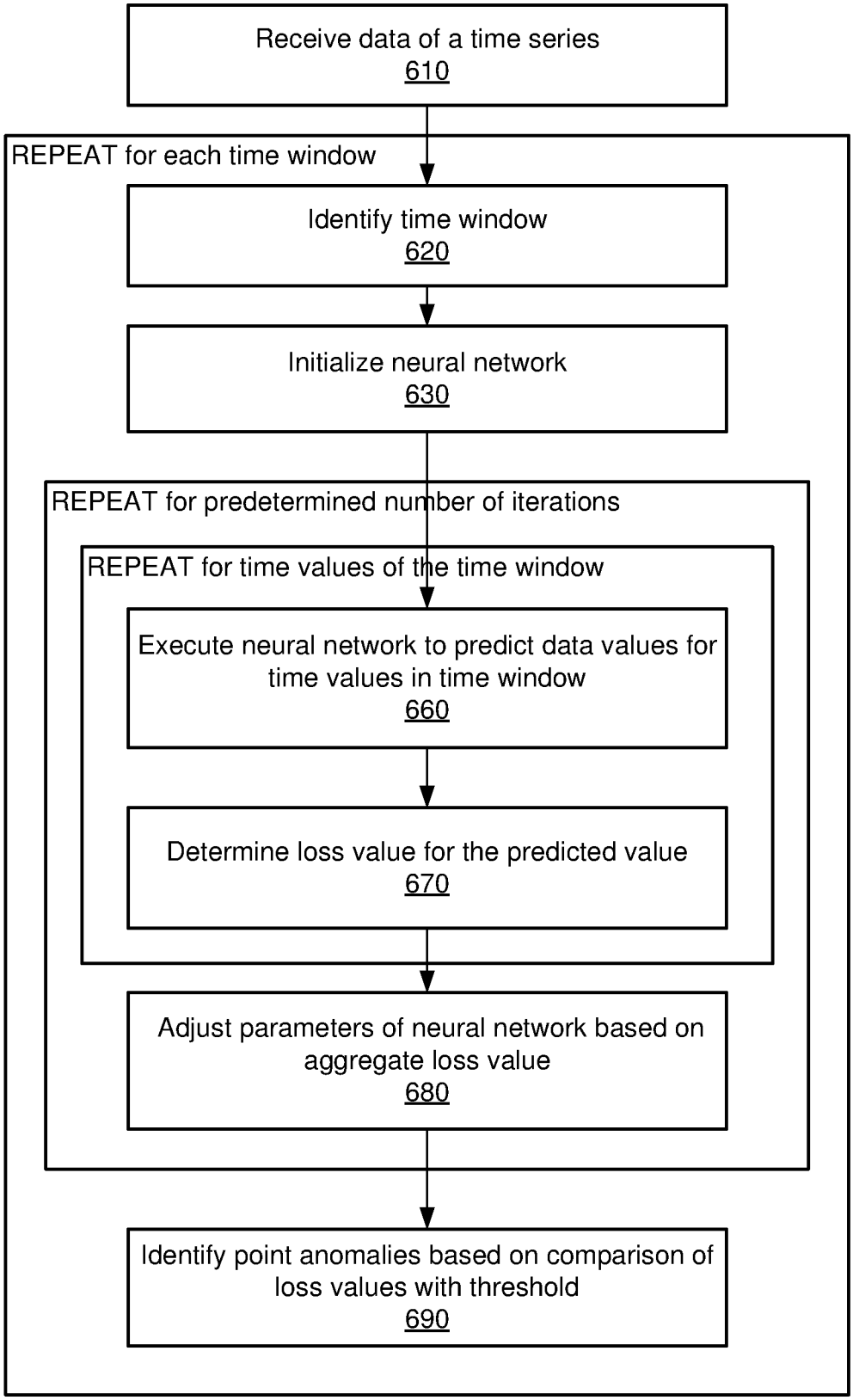
Receive data of a time series
610
REPEAT for each time window
Identify time window
620
Initialize neural network
630
REPEAT for predetermined number of iterations
REPEAT for time values of the time window
Execute neural network to predict data values for time values in time window
660
Determine loss value for the predicted value
670
Adjust parameters of neural network based on aggregate loss value
680
Identify point anomalies based on comparison of loss values with threshold
690

FIG. 6

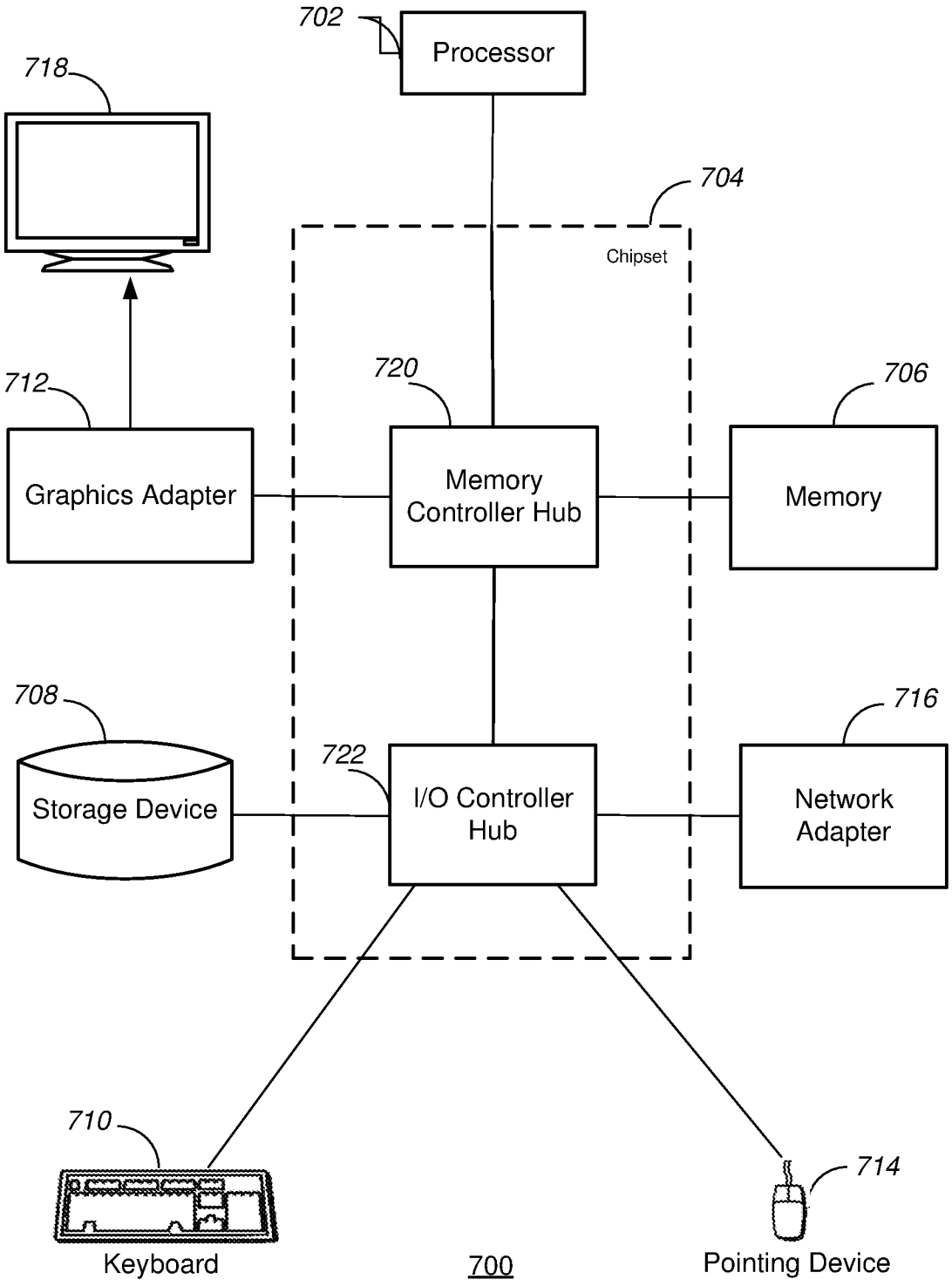
702
Processor
718
704
Chipset
712
720
706
Graphics Adapter
Memory Controller Hub
Memory
708
716
722
Storage Device
I/O Controller Hub
Network Adapter
710
714
Keyboard
700
Pointing Device

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/013768

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06N3/08 G06N3/04
ADD.

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)
G06N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/382361 A1 (CHANDRASEKHAR VIKRAM [US] ET AL) 3 December 2020 (2020-12-03) paragraph [0013] - paragraph [0017] paragraph [0021] paragraph [0050] - paragraph [0051] paragraph [0074] - paragraph [0097] paragraph [0104] - paragraph [0141] paragraph [0147]; figures 1-8	1-20
A	MOHAMMAD BRAEI ET AL: "Anomaly Detection in Univariate Time-series: A Survey on the State-of-the-Art", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 1 April 2020 (2020-04-01), XP081633976, the whole document	1-20

☐ 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
13 May 2022	24/05/2022

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Cilia, Elisa

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2022/013768

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2020382361 A1	03-12-2020	CN 114128226 A	01-03-2022
		EP 3921980 A1	15-12-2021
		KR 20220003513 A	10-01-2022
		US 2020382361 A1	03-12-2020
		WO 2020242275 A1	03-12-2020