



(51) International Patent Classification:

G06F 16/215 (2019.01)

(21) International Application Number:

PCT/CN2019/091433

(22) International Filing Date:

15 June 2019 (15.06.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

201910501710.5 11 June 2019 (11.06.2019) CN

(71) Applicant: **BEIJING DIDI INFINITY TECHNOLOGY AND DEVELOPMENT CO., LTD.** [CN/CN]; Building 34, No. 8 Dongbeiwang West Road, Haidian District, Beijing 100193 (CN).

(72) Inventors: **ZHU, Bao**; Building 34, No. 8 Dongbeiwang West Road, Haidian District, Beijing 100193 (CN). **CHEN, Shujun**; Building 34, No. 8 Dongbeiwang West Road, Haidian District, Beijing 100193 (CN). **CUI, Dongdong**; Building 34, No. 8 Dongbeiwang West Road, Haidian District, Beijing 100193 (CN).

(74) Agent: **METIS IP (CHENGDU) LLC**; Room 808, 8th Floor, Building B7, Block D, Tianfu Jingrong Center, No.

99 West Section of Hupan Road, Tianfu New District, Chengdu, Sichuan 610213 (CN).

(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, 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, 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, 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: SYSTEMS AND METHODS FOR ANOMALY DETECTION

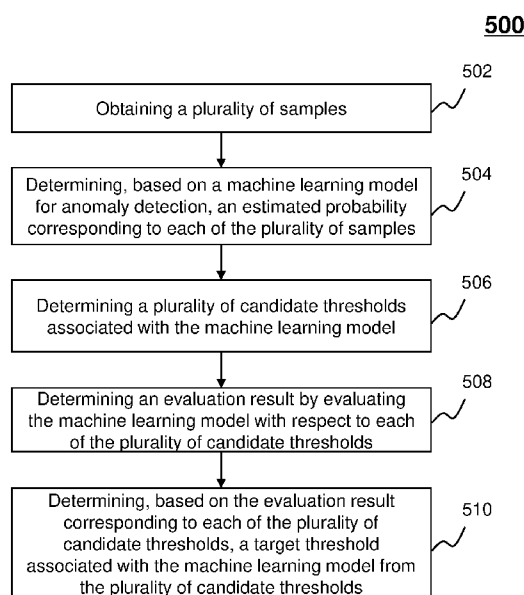


FIG. 5

(57) Abstract: Systems and methods for anomaly detection. The system may obtain a plurality of samples. Each of the plurality of samples may be associated with an event. The system may also determine an estimated probability based on a machine learning model for the anomaly detection. The system may also determine a plurality of candidate thresholds associated with the machine learning model based on estimated probabilities corresponding to at least a portion of the plurality of samples. The system may also determine an evaluation result by evaluating the machine learning model for the anomaly detection with respect to each of the plurality of candidate thresholds. The system may also determine, based on the evaluation result, a target threshold associated with the machine learning model for the anomaly detection from the plurality of candidate thresholds.

## **SYSTEMS AND METHODS FOR ANOMALY DETECTION**

### **CROSS-REFERENCE TO RELATED APPLICATIONS**

**[0001]** This application claims priority to Chinese Patent Application No. 201910501710.5 filed on June 11, 2019, the contents of which are incorporated herein by reference.

### **TECHNICAL FIELD**

**[0002]** The present disclosure generally relates to anomaly detection field, and specifically, to systems and methods for determining thresholds of a machine learning model for anomaly detection.

### **BACKGROUND**

**[0003]** Machine learning has greatly promoted the development of anomaly detection technology, which in turn expands the use of anomaly detection technology. For example, an anomaly detection technology is applied to intrusion detection, fault detection, network abnormal traffic detection, etc. Currently, unsupervised machine learning techniques are widely used for anomaly detection. Using an unsupervised machine learning model for anomaly detection, a threshold may be predetermined for determining whether an event is anomalous. At present, a threshold for an unsupervised machine learning model for anomaly detection is set by a user empirically, which may lack sufficient accuracy and or effectiveness of the threshold, which in turn may decrease accuracy of estimated results and/or effectiveness of the unsupervised machine learning model for anomaly detection. Therefore, it is desirable to develop systems and methods for determining a threshold of an unsupervised machine learning model for anomaly detection with improved accuracy and/or effectiveness.

### **SUMMARY**

**[0004]** According to an aspect of the present disclosure, a system for anomaly detection is provided. The system may include at least one storage medium storing a set of instructions and at least one processor configured to communicate with the at least one

storage medium. When executing the set of instructions, the at least one processor may be directed to cause the system to obtain a plurality of samples. Each of the plurality of samples may be associated with an event. The at least one processor may be further directed to cause the system to determine, for each of the plurality of samples, based on a machine learning model for the anomaly detection, an estimated probability that the event corresponding to the each of the plurality of samples is anomalous. The at least one processor may be further directed to cause the system to determine, based on estimated probabilities corresponding to at least a portion of the plurality of samples, a plurality of candidate thresholds associated with the machine learning model. The at least one processor may be further directed to cause the system to determine an evaluation result by evaluating the machine learning model for the anomaly detection with respect to each of the plurality of candidate thresholds. The at least one processor may be further directed to cause the system to determine, based on the evaluation result, a target threshold associated with the machine learning model for the anomaly detection from the plurality of candidate thresholds.

**[0005]** In some embodiments, the machine learning model may include at least one of a one-class support vector machine (SVM) model or an isolation forest algorithm.

**[0006]** In some embodiments, to determine, based on estimated probabilities corresponding to at least a portion of the plurality of samples, a plurality of candidate thresholds associated with the machine learning model, the at least one processor may be directed to cause the system to designate the estimated probability corresponding to each of the at least a portion of the plurality of samples as one of the plurality of candidate thresholds.

**[0007]** In some embodiments, to evaluate the machine learning model with respect to each of the plurality of candidate thresholds, the at least one processor may be directed to cause the system to determine, for each of the plurality of samples, a reference probability

corresponding to the each of the plurality of samples based on a probability estimation model. The at least one processor may be directed to cause the system to evaluate, based on the estimated probability and the reference probability, the machine learning model with respect to each of the plurality of candidate thresholds.

**[0008]** In some embodiments, to evaluate, based on the estimated probability and the reference probability, the machine learning model, the at least one processor may be directed to cause the system to determining, based on the reference probability and the estimated probability, an evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds. The at least one processor may be further directed to cause the system to evaluate, based on the evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds, the machine learning model.

**[0009]** In some embodiments, to determine, based on the reference probability and the estimated probability, an evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds, the at least one processor may be directed to cause the system to determine, based on each of the plurality of candidate thresholds and the estimated probability, an estimated label of each of the plurality of samples, the estimated label including a negative sample or a positive sample. The at least one processor may be further directed to cause the system to determine, based on the reference probability and the estimated label, the evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds.

**[0010]** In some embodiments, the at least one processor may be further directed to cause the system to ranking the reference probability of each of the plurality of samples. To determine the evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds, the at least one processor may be further directed to

cause the system to determine, based on the ranked reference probability, and the estimated label corresponding to each of the plurality of the samples, the evaluation index.

**[0011]** In some embodiments, the evaluation index of the machine learning model may include at least one of an area under curve (AUC) or a Gini coefficient.

**[0012]** In some embodiments, to determine, based on the evaluation result, a target threshold associated with the machine learning model from the plurality of candidate thresholds, the at least one processor may be directed to cause the system to identify, from the plurality of candidate thresholds, a candidate threshold that corresponds to a maximum of the evaluation index. The at least one processor may be further directed to cause the system to designate the identified candidate threshold as the target threshold associated with the machine learning model.

**[0013]** In some embodiments, the at least one processor may be further directed to cause the system to obtain data associated with a specific event. The at least one processor may be further directed to cause the system to determine, based on the data associated with the specific event and the machine learning model with respect to the target threshold, whether the specific event is anomalous.

**[0014]** According to another aspect of the present disclosure, a method for anomaly detection is provided. The method may include obtaining a plurality of samples. Each of the plurality of samples may be associated with an event. The method may further include determining, for each of the plurality of samples, an estimated probability that the event corresponding to the each of the plurality of samples is anomalous based on a machine learning model for the anomaly detection. The method may further include determining, based on estimated probabilities corresponding to at least a portion of the plurality of samples, a plurality of candidate thresholds associated with the machine learning model. The method may further include determining an evaluation result by evaluating the machine learning model for the anomaly detection with respect to each of

the plurality of candidate thresholds. The method may further include determining, based on the evaluation result, a target threshold associated with the machine learning model for the anomaly detection from the plurality of candidate thresholds.

**[0015]** According to still a further aspect of the present disclosure, a non-transitory computer readable medium is provided. The non-transitory computer readable medium storing instructions, the instructions, when executed by a computer, may cause the computer to implement a method. The method may include one or more of the following operations. The method may include obtaining a plurality of samples. Each of the plurality of samples may be associated with an event. The method may further include determining, for each of the plurality of samples, an estimated probability that the event corresponding to the each of the plurality of samples is anomalous based on a machine learning model for the anomaly detection. The method may further include determining, based on estimated probabilities corresponding to at least a portion of the plurality of samples, a plurality of candidate thresholds associated with the machine learning model. The method may further include determining an evaluation result by evaluating the machine learning model for the anomaly detection with respect to each of the plurality of candidate thresholds. The method may further include determining, based on the evaluation result, a target threshold associated with the machine learning model for the anomaly detection from the plurality of candidate thresholds.

**[0016]** According to another aspect of the present disclosure, a system for anomaly detection is provided. The system may include an acquisition module, a determination module and an evaluation module. The acquisition module may be configured to obtain a plurality of samples. Each of the plurality of samples may be associated with an event. The determination module may be configured to for each of the plurality of samples, determine, based on a machine learning model for the anomaly detection, an estimated probability that the event corresponding to the each of the plurality of samples is

anomalous. The determination module may be also configured to determine, based on estimated probabilities corresponding to at least a portion of the plurality of samples, a plurality of candidate thresholds associated with the machine learning model. The evaluation module may be configured to determine an evaluation result by evaluating the machine learning model for the anomaly detection with respect to each of the plurality of candidate thresholds. The determination module may be further configured to determine, based on the evaluation result, a target threshold associated with the machine learning model for the anomaly detection from the plurality of candidate thresholds.

**[0017]** Additional features will be set forth in part in the description which follows, and in part will become apparent to those skilled in the art upon examination of the following and the accompanying drawings or may be learned by production or operation of the examples. The features of the present disclosure may be realized and attained by practice or use of various aspects of the methodologies, instrumentalities and combinations set forth in the detailed examples discussed below.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

**[0018]** The present disclosure is further described in terms of exemplary embodiments. These exemplary embodiments are described in detail with reference to the drawings. These embodiments are non-limiting exemplary embodiments, in which like reference numerals represent similar structures throughout the several views of the drawings, and wherein:

**[0019]** FIG. 1 is a schematic diagram illustrating an exemplary anomaly detection system according to some embodiments of the present disclosure;

**[0020]** FIG. 2 is a schematic diagram illustrating exemplary hardware and software components of a computing device according to some embodiments of the present disclosure;

**[0021]** FIG. 3 is a schematic diagram illustrating exemplary hardware and/or software components of a mobile device on which a terminal may be implemented according to some embodiments of the present disclosure;

**[0022]** FIG. 4 is a block diagram illustrating an exemplary processing device according to some embodiments of the present disclosure;

**[0023]** FIG. 5 is a flowchart illustrating an exemplary process for determining a threshold of a machine learning model for anomaly detection according to some embodiments of the present disclosure;

**[0024]** FIG. 6 is a flowchart illustrating an exemplary process for evaluating a machine learning model according to some embodiments of the present disclosure;

**[0025]** FIG. 7 is a flowchart illustrating an exemplary process for anomaly detection according to some embodiments of the present disclosure; and

**[0026]** FIGs. 8A-8D are schematic diagrams of exemplary anomaly detection results according to some embodiments of the present disclosure.

### **DETAILED DESCRIPTION**

**[0027]** In the following detailed description, numerous specific details are set forth by way of examples in order to provide a thorough understanding of the relevant disclosure.

However, it should be apparent to those skilled in the art that the present disclosure may be practiced without such details. In other instances, well-known methods, procedures, systems, components, and/or circuitry have been described at a relatively high-level, without detail, in order to avoid unnecessarily obscuring aspects of the present disclosure. Various modifications to the disclosed embodiments will be readily apparent to those skilled in the art, and the general principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the present disclosure. Thus, the present disclosure is not limited to the embodiments shown, but to be accorded the widest scope consistent with the claims.

**[0028]** The terminology used herein is for the purpose of describing particular example embodiments only and is not intended to be limiting. As used herein, the singular forms “a,” “an,” and “the” may be intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms “comprise,” “comprises,” and/or “comprising,” “include,” “includes,” and/or “including,” when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

**[0029]** It will be understood that the term “system,” “engine,” “unit,” “module,” and/or “block” used herein are one method to distinguish different components, elements, parts, section or assembly of different level in ascending order. However, the terms may be displaced by another expression if they achieve the same purpose.

**[0030]** Generally, the word “module,” “unit,” or “block,” as used herein, refers to logic embodied in hardware or firmware, or to a collection of software instructions. A module, a unit, or a block described herein may be implemented as software and/or hardware and may be stored in any type of non-transitory computer-readable medium or another storage device. In some embodiments, a software module/unit/block may be compiled and linked into an executable program. It will be appreciated that software modules can be callable from other modules/units/blocks or from themselves, and/or may be invoked in response to detected events or interrupts. Software modules/units/blocks configured for execution on computing devices may be provided on a computer-readable medium, such as a compact disc, a digital video disc, a flash drive, a magnetic disc, or any other tangible medium, or as a digital download (and can be originally stored in a compressed or installable format that needs installation, decompression, or decryption prior to execution). Such software code may be stored, partially or fully, on a storage device of the executing computing device, for execution by the computing device. Software instructions may be embedded

in firmware, such as an erasable programmable read-only memory (EPROM). It will be further appreciated that hardware modules/units/blocks may be included in connected logic components, such as gates and flip-flops, and/or can be included of programmable units, such as programmable gate arrays or processors. The modules/units/blocks or computing device functionality described herein may be implemented as software modules/units/blocks, but may be represented in hardware or firmware. In general, the modules/units/blocks described herein refer to logical modules/units/blocks that may be combined with other modules/units/blocks or divided into sub-modules/sub-units/sub-blocks despite their physical organization or storage. The description may be applicable to a system, an engine, or a portion thereof.

**[0031]** It will be understood that when a unit, engine, module or block is referred to as being “on,” “connected to,” or “coupled to,” another unit, engine, module, or block, it may be directly on, connected or coupled to, or communicate with the other unit, engine, module, or block, or an intervening unit, engine, module, or block may be present, unless the context clearly indicates otherwise. As used herein, the term “and/or” includes any and all combinations of one or more of the associated listed items.

**[0032]** These and other features, and characteristics of the present disclosure, as well as the methods of operation and functions of the related elements of structure and the combination of parts and economies of manufacture, may become more apparent upon consideration of the following description with reference to the accompanying drawings, all of which form a part of this disclosure. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only and are not intended to limit the scope of the present disclosure. It is understood that the drawings are not to scale.

**[0033]** The flowcharts used in the present disclosure illustrate operations that systems implement according to some embodiments in the present disclosure. It is to be

expressly understood the operations of the flowchart may be implemented not in order. Conversely, the operations may be implemented in inverted order, or simultaneously. Moreover, one or more other operations may be added to the flowcharts. One or more operations may be removed from the flowcharts.

**[0034]** Embodiments of the present disclosure may be applied to different transportation systems including but not limited to land transportation, sea transportation, air transportation, space transportation, or the like, or any combination thereof. A vehicle of the transportation systems may include a rickshaw, travel tool, taxi, chauffeured car, hitch, bus, rail transportation (e.g., a train, a bullet train, high-speed rail, and subway), ship, airplane, spaceship, hot-air balloon, driverless vehicle, or the like, or any combination thereof. The transportation system may also include any transportation system that applies management and/or distribution, for example, a system for sending and/or receiving an express.

**[0035]** The application scenarios of different embodiments of the present disclosure may include but not limited to one or more webpages, browser plugins and/or extensions, client terminals, custom systems, intracompany analysis systems, artificial intelligence robots, or the like, or any combination thereof. It should be understood that application scenarios of the system and method disclosed herein are only some examples or embodiments. Those having ordinary skills in the art, without further creative efforts, may apply these drawings to other application scenarios, for example, another similar server.

**[0036]** The term “passenger,” “requester,” “requestor,” “service requester,” “service requestor” and “customer” in the present disclosure are used interchangeably to refer to an individual, an entity or a tool that may request or order a service. Also, the term “driver,” “provider,” “service provider,” and “supplier” in the present disclosure are used interchangeably to refer to an individual, an entity or a tool that may provide a service or facilitate the providing of the service. The term “user” in the present disclosure may refer

to an individual, an entity or a tool that may request a service, order a service, provide a service, or facilitate the providing of the service. For example, the user may be a requester, a passenger, a driver, an operator, or the like, or any combination thereof. In the present disclosure, “requester” and “requester terminal” may be used interchangeably, and “provider” and “provider terminal” may be used interchangeably.

**[0037]** The term “request,” “service,” “service request,” and “order” in the present disclosure are used interchangeably to refer to a request that may be initiated by a passenger, a requester, a service requester, a customer, a driver, a provider, a service provider, a supplier, or the like, or any combination thereof. The service request may be accepted by any one of a passenger, a requester, a service requester, a customer, a driver, a provider, a service provider, or a supplier. The service request may be chargeable or free.

**[0038]** Some embodiments of the present disclosure provide systems and methods for determining or predicting whether an event is anomalous using a model. The model may be a machine learning model. The model may be used with a target threshold that may serve as a classifier. The model may be used to predict or determine whether an event is anomalous. For instance, the model may predict or determine a probability that an event is anomalous, and then by comparing the probability with the target threshold determine/designate the event as anomalous or not.

**[0039]** Some embodiments of the present disclosure provide systems and methods for determining a model and a target threshold with respect to the model for anomaly detection that is used to determine or predict whether an event is anomalous. The target threshold may be determined using a plurality of samples associated with different events each of whose anomaly status (whether an event is anomalous or not) is unknown or known. Estimated probabilities corresponding to the plurality of samples may be determined. Further, a plurality of candidate thresholds associated with a machine

learning model for anomaly detection may be determined. Then an evaluation result may be determined by evaluating the machine learning model, with respect to each of the plurality of candidate thresholds, for detecting anomaly of the samples. A target threshold associated with the machine learning model from the plurality of candidate thresholds may be determined based on the evaluation result. Accordingly, the plurality of candidate thresholds may be applied to a machine learning model for anomaly detection to assess the accuracy and/or effectiveness of the candidate thresholds for the machine learning model in anomaly detection. The target threshold may then be determined from the plurality of candidate thresholds by evaluating the machine learning model with respect to each of the plurality of candidate thresholds, which may further improve the accuracy and/or effectiveness of the machine learning model. The systems and methods for anomaly detection according to some embodiments of the present disclosure may reduce or avoid the need to rely on the experience of an individual to select a threshold for a machine learning model for anomaly detection.

**[0040]** FIG. 1 is a schematic diagram illustrating an exemplary anomaly detection system 100 according to some embodiments of the present disclosure. The anomaly detection system 100 may be a platform for data and/or information processing, for example, training a machine learning model for anomaly detection and/or data classification, such as image classification, text classification, etc. The anomaly detection system 100 may be applied in intrusion detection, fault detection, network abnormal traffic detection, fraud detection, behavior abnormal detection, or the like, or a combination thereof. An anomaly may be also referred to as an outlier, a novelty, a noise, a deviation, an exception, etc. As used herein, an anomaly refers to an action or an event that is determined to be unusual or abnormal in view of known or inferred conditions. For example, for a network subscribe platform (e.g., a video broadcast platform, a social network platform, etc.), the anomaly may include a network quality anomaly, a user access anomaly, a server anomaly, etc.

As another example, for an online transport service platform (e.g., an online taxi-hailing service platform), the anomaly may include an order anomaly, a driver behavior anomaly, a passenger behavior anomaly, a route anomaly, etc.

**[0041]** The anomaly detection system 100 may include a data exchange port 101, a data transmitting port 102, a server 110, and storage 120. In some embodiments, the anomaly detection system 100 may interact with a data providing system 130 and a service providing system 140 via the data exchange port 101 and the data transmitting port 102, respectively. For example, anomaly detection system 100 may access information and/or data stored in the data providing system 130 via the data exchange port 101. As another example, the server 110 may send information and/or data to a service providing system 140 via the data transmitting port 102.

**[0042]** The server 110 may process information and/or data relating to anomaly detection. In some embodiments, the server 110 may be a single server, or a server group. The server group may be centralized, or distributed (e.g., the server 110 may be a distributed system). In some embodiments, the server 110 may be implemented on a cloud platform. Merely by way of example, the cloud platform may include a private cloud, a public cloud, a hybrid cloud, a community cloud, a distributed cloud, an inter-cloud, a multi-cloud, or the like, or any combination thereof. In some embodiments, the server 110 may be implemented on a computing device having one or more components illustrated in FIG. 2 in the present disclosure.

**[0043]** In some embodiments, the server 110 may include a processing device 112. The processing device 112 may process information and/or data relating to anomaly detection to perform one or more functions described in the present disclosure. For example, the processing device 112 may receive a machine learning model for anomaly detection from the data providing system 130 and a sample set from the service providing system 140. The processing device 112 may determine a target threshold for the machine learning

model for anomaly detection based on the sample set. As another example, the processing device 112 may estimate whether a specific sample received from the service providing system 140 is anomalous based on the target threshold using the machine learning model for anomaly detection. The target threshold may be updated from time to time, e.g., periodically or not, based on a sample set that is at least partially different from the original sample set from which the original target threshold is determined. For instance, the target threshold may be updated based on a sample set including new samples that are not in the original sample set, samples whose anomaly is assessed using the machine learning model in connection with the original target threshold or a target threshold of a prior version, or the like, or a combination thereof. As still another example, the processing device 112 may transmit a signal including the estimated result to the service providing system 140. In some embodiments, the determination and/or updating of the target threshold may be performed on a processing device, while the application of a machine learning model in connection with the target threshold may be performed on a different processing device. In some embodiments, the determination and/or updating of the target threshold and/or the corresponding machine learning model may be performed on a processing device of a system different than the anomaly detection system 100 or a server different than the server 110 on which the application of a machine learning model in connection with the target threshold is performed. For instance, the determination and/or updating of the target threshold and/or the machine learning model may be performed on a first system of a vendor who provides and/or maintains such a machine learning model, including the target threshold, and/or has access to training samples used to determine and/or update the target threshold and/or the machine learning model, while anomaly detection of an event based on the provided machine learning model, including the target threshold, may be performed on a second system of a client of the vendor. In some embodiments, the determination and/or

updating of the target threshold and/or the machine learning model may be performed online in response to a request for anomaly detection of an event. In some embodiments, the determination and/or updating of the target threshold and/or the machine learning model may be performed offline. In some embodiments, the processing device 112 may include one or more processors (e.g., single-core processor(s) or multi-core processor(s)). Merely by way of example, the processing device 112 may include a central processing unit (CPU), an application-specific integrated circuit (ASIC), an application-specific instruction-set processor (ASIP), a graphics processing unit (GPU), a physics processing unit (PPU), a digital signal processor (DSP), a field programmable gate array (FPGA), a programmable logic device (PLD), a controller, a microcontroller unit, a reduced instruction-set computer (RISC), a microprocessor, or the like, or any combination thereof.

**[0044]** The storage 120 may store data and/or instructions related to content identification and/or data classification. In some embodiments, the storage 120 may store data obtained/acquired from the data providing system 130 and/or the service providing system 140. In some embodiments, the storage 120 may store data and/or instructions that the server 110 may execute or use to perform exemplary methods described in the present disclosure. In some embodiments, the storage 120 may include a mass storage device, a removable storage device, a volatile read-and-write memory, a read-only memory (ROM), or the like, or any combination thereof. Exemplary mass storage devices may include a magnetic disk, an optical disk, a solid-state drive, etc. Exemplary removable storage devices may include a flash drive, a floppy disk, an optical disk, a memory card, a zip disk, a magnetic tape, etc. Exemplary volatile read-and-write memory may include a random access memory (RAM). Exemplary RAM may include a dynamic RAM (DRAM), a double data rate synchronous dynamic RAM (DDR SDRAM), a static RAM (SRAM), a thyristor RAM (T-RAM), and a zero-capacitor RAM (Z-RAM), etc. Exemplary ROM may include a mask ROM (MROM), a programmable ROM (PROM), an erasable programmable ROM

(PEROM), an electrically erasable programmable ROM (EEPROM), a compact disk ROM (CD-ROM), and a digital versatile disk ROM, etc. In some embodiments, the storage 120 may be implemented on a cloud platform. Merely by way of example, the cloud platform may include a private cloud, a public cloud, a hybrid cloud, a community cloud, a distributed cloud, an inter-cloud, a multi-cloud, or the like, or any combination thereof.

**[0045]** In some embodiments, the storage 120 may be connected to or communicate with the server 110. The server 110 may access data or instructions stored in the storage 120 directly or via a network. In some embodiments, the storage 120 may be a part of the server 110.

**[0046]** The data providing system 130 may provide data and/or information related to anomaly detection and/or data classification. The data and/or information may include images, text files, voice segments, web pages, video recordings, user requests, programs, applications, algorithms, instructions, computer codes, or the like, or a combination thereof. In some embodiments, the data providing system 130 may provide the data and/or information to the server 110 and/or the storage 120 of the anomaly detection system 100 for processing (e.g., train a machine learning model for anomaly detection). In some embodiments, the data providing system 130 may provide the data and/or information to the service providing system 140 for generating a service response relating to the anomaly detection and/or data classification.

**[0047]** In some embodiments, the service providing system 140 may be configured to provide online services, such as an anomaly detection service, an online to offline service (e.g., a taxi service, a carpooling service, a food delivery service, a party organization service, an express service, etc.), an unmanned driving service, a medical service, a map-based service (e.g., a route planning service), a live chatting service, a query service, a Q&A service, etc. The service providing system 140 may generate service responses, for

example, by inputting the data and/or information received from a user and/or the data providing system 130 into a machine learning model for anomaly detection.

**[0048]** In some embodiments, the data providing system 130 and/or the service providing system 140 may be a device, a platform, or other entity interacting with the anomaly detection system. In some embodiments, the data providing system 130 may be implemented in a device with data acquisition and/or data storage, such as a mobile device 130-1, a tablet computer 130-2, a laptop computer 130-3, a server 130-4, a storage device (not shown), or the like, or any combination thereof. In some embodiments, the service providing system 140 may also be implemented in a device with data processing, such as a mobile device 140-1, a tablet computer 140-2, a laptop computer 140-3, and a server 140-4, or the like, or any combination thereof. In some embodiments, the mobile devices 130-1 and 140-1 may include a smart home device, a wearable device, a smart mobile device, a virtual reality device, an augmented reality device, or the like, or any combination thereof. In some embodiments, the smart home device may include a smart lighting device, a control device of an intelligent electrical apparatus, a smart monitoring device, a smart television, a smart video camera, an interphone, or the like, or any combination thereof. In some embodiments, the wearable device may include a smart bracelet, a smart footgear, a smart glass, a smart helmet, a smart watch, a smart clothing, a smart backpack, a smart accessory, or the like, or any combination thereof. In some embodiments, the smart mobile device may include a smartphone, a personal digital assistant (PDA), a gaming device, a navigation device, a point of sale (POS) device, or the like, or any combination thereof. In some embodiments, the virtual reality device and/or the augmented reality device may include a virtual reality helmet, a virtual reality glass, a virtual reality patch, an augmented reality helmet, an augmented reality glass, an augmented reality patch, or the like, or any combination thereof. For example, the virtual reality device and/or the augmented reality device may include a Google Glass, an Oculus

Rift, a HoloLens, a Gear VR, etc. In some embodiments, the servers 130-4 and 140-4 may include a database server, a file server, a mail server, a web server, an application server, a computing server, a media server, a communication server, etc.

**[0049]** In some embodiments, the data providing system 130 may be a device with data processing technology for preprocessing acquired or stored information (e.g., identifying images from stored information). In some embodiments, the service providing system 140 may be a device for data processing, for example, train an identification model using a cleaned dataset received from the server 110. In some embodiments, the service providing system 140 may directly communicate with the data providing system 130 via a network 150-3. For example, the service providing system 140 may receive a dataset from the data providing system 130, and perform an anomaly detection on the dataset based on a machine learning model for anomaly detection.

**[0050]** In some embodiments, any two systems of the anomaly detection system 100, the data providing system 130, and the service providing system 140 may be integrated into a device or a platform. For example, both the data providing system 130 and the service providing system 140 may be implemented in a mobile device of a user. In some embodiments, the anomaly detection system 100, the data providing system 130, and the service providing system 140 may be integrated into a device or a platform. For example, the anomaly detection system 100, the data providing system 130, and the service providing system 140 may be implemented in a computing device including a server and a user interface.

**[0051]** Networks 150-1 through 150-3 may facilitate exchange of information and/or data. In some embodiments, one or more components in the anomaly detection system (e.g., the server 110 and/or the storage 120) may send and/or receive information and/or data to/from the data providing system 130 and/or the service providing system 140 via the networks 150-1 through 150-3. For example, the server 110 may obtain/acquire datasets

for anomaly detection from the data providing system 130 via the network 150-1. As another example, the server 110 may transmit/output estimated result for anomaly detection to the service providing system 140 via the network 150-2. In some embodiments, the networks 150-1 through 150-3 may be any type of wired or wireless networks, or combination thereof. Merely by way of example, the networks 150 may include a cable network, a wireline network, an optical fiber network, a telecommunications network, an intranet, an Internet, a local area network (LAN), a wide area network (WAN), a wireless local area network (WLAN), a metropolitan area network (MAN), a wide area network (WAN), a public telephone switched network (PSTN), a Bluetooth™ network, a ZigBee™ network, a near field communication (NFC) network, a global system for mobile communications (GSM) network, a code-division multiple access (CDMA) network, a time-division multiple access (TDMA) network, a general packet radio service (GPRS) network, an enhanced data rate for GSM evolution (EDGE) network, a wideband code division multiple access (WCDMA) network, a high speed downlink packet access (HSDPA) network, a long term evolution (LTE) network, a user datagram protocol (UDP) network, a transmission control protocol/Internet protocol (TCP/IP) network, a short message service (SMS) network, a wireless application protocol (WAP) network, a ultra wide band (UWB) network, an infrared ray, or the like, or any combination thereof.

**[0052]** FIG. 2 illustrates a schematic diagram of an exemplary computing device 200 according to some embodiments of the present disclosure. The computing device 200 may be a computer, such as the server 110 in FIG. 1 and/or a computer with specific functions, configured to implement any particular system according to some embodiments of the present disclosure. The computing device 200 may be configured to implement any component that performs one or more functions disclosed in the present disclosure. For example, the server 110 (e.g., the processing device 112) may be implemented in hardware devices, software programs, firmware, or any combination thereof of a computer

like the computing device 200. For brevity, FIG. 2 depicts only one computing device. In some embodiments, the functions of the computing device may be implemented by a group of similar platforms in a distributed mode to disperse the processing load of the system.

**[0053]** The computing device 200 may include a communication terminal 250 that may connect with a network that may implement the data communication. The computing device 200 may also include a processor 220 that is configured to execute instructions and includes one or more processors. The schematic computer platform may include an internal communication bus 210, different types of program storage units and data storage units (e.g., a hard disk 270, a read-only memory (ROM) 230, a random-access memory (RAM) 240), various data files applicable to computer processing and/or communication, and some program instructions executed possibly by the processor 220. The computing device 200 may also include an I/O device 260 that may support the input and output of data flows between the computing device 200 and other components. Moreover, the computing device 200 may receive programs and data via the communication network.

**[0054]** FIG. 3 is a schematic diagram illustrating exemplary hardware and/or software components of an exemplary mobile device on which a service system (e.g., the anomaly detection system 122, the data providing system 130 and/or the service providing system 140) may be implemented according to some embodiments of the present disclosure. As illustrated in FIG. 3, the mobile device 300 may include, a communication platform 310, a display 320, a graphics processing unit (GPU) 330, a central processing unit (CPU) 340, an I/O 350, a memory 360, a mobile operating system (OS) 370, application (s), and a storage 390. In some embodiments, any other suitable component, including but not limited to a system bus or a controller (not shown), may also be included in the mobile device 300.

**[0055]** In some embodiments, the mobile operating system 370 (e.g., iOS™, Android™, Windows Phone™, etc.) and one or more applications 380 may be loaded into the memory 360 from the storage 390 in order to be executed by the CPU 340. The applications 380 may include a browser or any other suitable mobile apps for receiving and rendering information relating to image processing or other information from the Anomaly detection system 100. User interactions with the information stream may be achieved via the I/O 350 and provided to the storage device 120, the server 110 and/or other components of the Anomaly detection system 100. In some embodiments, the mobile device 300 may be an exemplary embodiment corresponding to a terminal associated with, the anomaly detection system 100, the data providing system 130 and/or the service providing system 140.

**[0056]** To implement various modules, units, and their functionalities described in the present disclosure, computer hardware platforms may be used as the hardware platform(s) for one or more of the elements described herein. A computer with user interface elements may be used to implement a personal computer (PC) or any other type of work station or terminal device. A computer may also act as a system if appropriately programmed.

**[0057]** FIG. 4 is a block diagram illustrating an exemplary processing device 112 according to some embodiments of the present disclosure. The processing device 112 may include an acquisition module 410, a determination module 420, an evaluation module 430, and a storage module 440.

**[0058]** The acquisition module 410 may be configured to obtain data for anomaly detection. For example, the acquisition module 410 may obtain a plurality of samples. Each of the plurality of samples may be associated with an event. As used herein, an event may be defined by information and/or data that indicating something has happened at a specific time or time period. As another example, the acquisition module 410 may

also obtain data associated with a specific event. In some embodiments, the specific event may be an event associated with one of the plurality of samples. The data associated with the specific event may be one of the plurality of samples. The data associated with the specific event may include one or more features that characterizes the specific event as described elsewhere in the present disclosure. As still another example, the acquisition module 410 may be configured to obtain a model, such as a machine learning model for anomaly detection, a probability estimation model, etc.

**[0059]** The determination module 420 may be configured to determine an estimated probability for each of the plurality of samples based on a machine learning model for anomaly detection. Each of the plurality of samples may correspond to an estimated probability. The determination module 420 may further determine a plurality of candidate thresholds associated with the machine learning model based on the estimated probabilities of the plurality of samples. The determination module 420 may also determine a target threshold associated with the machine learning model from the plurality of candidate thresholds based on an evaluation result corresponding to each of the plurality of candidate thresholds. The determination module 420 may determine whether the specific event is anomalous based on the data associated with the specific event and the machine learning model with the target threshold.

**[0060]** The evaluation module 430 may be configured to determine the evaluation result by evaluating the machine learning model for anomaly detection with respect to each of the plurality of candidate thresholds. The evaluation module 430 may evaluate the machine learning model with respect to each of the plurality of candidate thresholds according to one or more evaluation indexes. The evaluation result may be denoted by one or more values of the one or more evaluation indexes.

**[0061]** The storage module 440 may be configured to store information. The information may include programs, software, algorithms, data, text, number, images and some other

information. For example, the information may include data which may define an event indicating something has happened at a specific time or time period, etc. As another example, the information may include a machine learning model for anomaly detection.

**[0062]** It should be noted that the above description of the processing device 112 provided for the purposes of illustration, and is not intended to limit the scope of the present disclosure. For persons having ordinary skills in the art, multiple variations and modifications may be made under the teachings of the present disclosure. However, those variations and modifications do not depart from the scope of the present disclosure. In some embodiments, any module mentioned above may be implemented in two or more separate units. For example, the functions of determination module 420 may be implemented in two separate units, one of which is configured to determine an estimated probability corresponding to each of the plurality of samples, and the other is configured to determine candidate thresholds associated with the machine learning model. In some embodiments, the processing device 112 may further include one or more additional modules (e.g., a storage module). Additionally or alternatively, one or more modules mentioned above may be omitted.

**[0063]** FIG. 5 is a flowchart illustrating an exemplary process 500 for determining a threshold of a machine learning model for anomaly detection according to some embodiments of the present disclosure. At least a portion of process 500 may be implemented on the computing device 200 as illustrated in FIG. 2 or the mobile device 300 as illustrated in FIG. 3. In some embodiments, one or more operations of process 500 may be implemented in the anomaly detection system 100 as illustrated in FIG. 1. In some embodiments, one or more operations in the process 500 may be stored in a storage device (e.g., the storage 120, the ROM 230, the RAM 240, the storage 390) as a form of instructions, and invoked and/or executed by the server 110 (e.g., the processing device 112 in the server 110, or the processor 220 of the computing device 200) or the

CPU 340 of the mobile device 300. In some embodiments, the instructions may be transmitted in the form of electronic current or electrical signals.

**[0064]** In 502, the processing device 112 (e.g., the acquisition module 410) may obtain a plurality of samples. Each of the plurality of samples may be associated with an event. The plurality of samples may be obtained by the acquisition module 410 from a storage device (e.g., the storage device 120, the ROM 230, the RAM 240, the storage 390) as described elsewhere in the present disclosure. As used herein, an event may be defined by information and/or data that indicating something has happened at a specific time or within a specific time period. For example, for an online taxi-hailing platform, the event may include logging in the online taxi-hailing platform, initiating a service request, dispatching a service request, picking up a passenger, transporting a passenger to a destination along a predetermined route, a communication between a driver and a passenger on a route, a communication between a client terminal and a server associated with the online taxi-hailing platform, or the like, or a combination thereof.

**[0065]** As used herein, a sample associated with an event may be also referred to as sample data. The sample may be in the form of an image, a video, text, etc. A sample associated with a specific event may include and/or represent one or more features that characterize the specific event. In some embodiments, the one or more features associated with the specific event may be presented as a feature vector (e.g., a multi-dimensional vector). Each dimension of the feature vector may represent a feature of the specific event. For example, in an online taxi-hailing platform, an event may include transporting a passenger to a destination along a predetermined route. The sample data (e.g., one or more features) associated with the event may include a start location, a start time, a destination, an estimated time of arrival, a real-time location, a travel trajectory (e.g., the whole length of the travel trajectory, the whole travel time of the travel trajectory, the length of a road segment in the travel trajectory, the travel time of a road segment in

the travel trajectory, etc.), or the like, or any combination thereof. In some embodiments, the plurality of samples may form a sample set. The sample set may be denoted as  $[\vec{x}_1, \vec{x}_2, \vec{x}_3, \dots, \vec{x}_n]$ . An element  $\vec{x}_i$  in the sample set may represent a sample. A sample may correspond to a multi-dimensional feature vector denoted as  $[f_1, f_2, f_3, \dots]$  that represents one or more features of the event. For example, in an online taxi-hailing platform, if an event includes transporting a passenger to a destination along a predetermined route,  $f_1$  may represent the start location,  $f_2$  may represent the destination, and  $f_3$  may represent the travel trajectory.

**[0066]** In 504, the processing device 112 (e.g., the determination module 420) may determine an estimated probability for each of the plurality of samples based on a machine learning model for anomaly detection. Each of the plurality of samples may correspond to an estimated probability. As used herein, the estimated probability of a specific sample determined based on the machine learning model for anomaly detection may refer to a possibility that the event corresponding to the specific sample is anomalous. The smaller the value of the estimated probability is, the higher the possibility that the event is anomalous may be. In some embodiments, the machine learning model for anomaly detection may be configured to generate and/or output the estimated probability of an event using the sample corresponding to the event. For example, the processing device 112 may input a specific sample into the machine learning model for anomaly detection. The machine learning model for anomaly detection may generate and output the estimated probability of an event associated with the specific sample using the inputted specific sample.

**[0067]** The machine learning model for anomaly detection may be obtained by the acquisition module 410 from the data providing system 130, the storage 120, the service providing system 140, or any other storage device as described elsewhere in the present disclosure. The machine learning model for anomaly detection may include an

unsupervised machine learning model, a semi-unsupervised machine learning model, etc. Exemplary unsupervised machine learning models may include using a classification-based algorithm, a statistical distribution-based algorithm, a proximity-based algorithm, a density-based algorithm, a cluster-based algorithm, a tree-based algorithm, etc. For example, the classification-based algorithm may include using a neural network model, a Bayesian network model, a one-class support vector machine (SVM) model, a robust SVM, a one-class kernel fisher discriminants model, etc. The statistical distribution-based algorithm may include using a Gaussian model, a robust regression model, etc. The proximity-based algorithm may include a K-nearest neighbor (KNN) algorithm, an outlier detection using in-degree number (ODIN) algorithm, etc. The density-based algorithm may include a local outlier factor (LOF) algorithm, a connectivity-based outlier factor (COF) algorithm, etc. The tree-based algorithm may include an isolation forest (iForest) algorithm, an interpretable hierarchical clustering unsupervised decision tree (IHCUDT) algorithm, etc. The cluster-based algorithm may include a share nearest neighbor (SNN) clustering algorithm, a wave cluster algorithm, K-means clustering algorithm, a self-organizing maps algorithm, an expectation maximization (EM) algorithm, etc. Exemplary semi-unsupervised machine learning models may include using a Markovian model, a finite state automata (FSA) model, a hidden Markov model (HMM), a probabilistic suffix trees (SMT) model, etc.

**[0068]** In 506, the processing device 112 (e.g., the determination module 420) may determine a plurality of candidate thresholds associated with the machine learning model. A candidate threshold associated with the machine learning model for anomaly detection may be configured to determine whether an event is anomalous. For example, if an estimated probability of an event determined using the machine learning model for anomaly detection is greater than the candidate threshold, the processing device 112 may determine that the event is anomalous when using the candidate threshold.

**[0069]** In some embodiments, the processing device 112 (e.g., the determination module 420) may determine at least a portion of the plurality of candidate thresholds based on the estimated probability determined in operation 504. For example, the processing device 112 may determine a portion or all of the plurality of candidate thresholds based on estimated probabilities corresponding to at least a portion of the plurality of samples. Further, the processing device 112 may designate each of the estimated probabilities corresponding to at least a portion of the plurality of samples as one of the plurality of candidate thresholds. As a further example, the processing device 112 may rank the estimated probability corresponding to each of the plurality of samples (e.g., in an ascending order or a descending order). The processing device 112 may determine a portion or all of the plurality of candidate thresholds based on the ranked estimated probabilities of the plurality samples. An estimated probability ranked as, e.g., the top, the bottom, the medium of the ranked estimated probabilities may be designated as a candidate threshold. As still another example, the processing device 112 may designate one or more estimated probabilities of at least a portion of the plurality samples within a certain range as one or more candidate thresholds. In some embodiments, the processing device 112 may designate the estimated probability corresponding to each of the plurality of samples as one of the plurality of candidate thresholds.

**[0070]** In some embodiments, the processing device 112 may determine at least a portion of the plurality of candidate thresholds using a probability estimation model. Further, the processing device 112 may determine a reference probability corresponding to each of the plurality of samples using the probability estimation model. The reference probability corresponding to a specific sample of the plurality of samples may be used to measure and/or assess similarity between the specific sample and one or more other samples of the plurality of samples. The greater the reference probability corresponding to the specific sample is, the higher the similarity between the specific sample and the one or

more other samples of the plurality of samples may be. The processing device 112 may determine a portion or all of the plurality of candidate thresholds based on reference probabilities corresponding to at least a portion of the plurality of samples. For example, the processing device 112 may designate each of reference probabilities corresponding to a portion of the plurality of samples as one of the plurality of candidate thresholds. As another example, the processing device 112 may designate each of reference probabilities corresponding to all the plurality of samples as one of the plurality of candidate thresholds. Exemplary probability estimation models may include using a parametric estimation algorithm, a Bayes algorithm, a non-parametric estimation algorithm, etc. For example, the parametric estimation algorithm may include a maximum likelihood algorithm. The non-parametric estimation algorithm may include a histogram probability estimation algorithm, a kernel density estimation algorithm, etc.

**[0071]** In some embodiments, at least a portion of the plurality of candidate thresholds may be set by a user or according to a default setting of the anomaly detection system 100.

**[0072]** In 508, the processing device 112 (e.g., the evaluation module 430) may determine an evaluation result by evaluating the machine learning model for anomaly detection with respect to each of the plurality of candidate thresholds. In some embodiments, the processing device 112 may evaluate the machine learning model with respect to each of the plurality of candidate thresholds according to one or more evaluation indexes. The evaluation result may be denoted by one or more values of the one or more evaluation indexes. Exemplary evaluation indexes of the machine learning model for anomaly detection may include an area under curve (AUC), a Gini coefficient, or the like, or any combination thereof. An evaluation index may be used to measure and/or indicate the accuracy of estimation results of the machine learning model for anomaly detection. For example, the greater the value of AUC of the machine learning model for

anomaly detection with respect to a candidate threshold, the greater the accuracy of estimation results of the machine learning model for anomaly detection may be.

**[0073]** The processing device 112 may determine the value of an evaluation index of the machine learning model for anomaly detection with respect to a specific candidate threshold using the plurality of samples. For example, the processing device 112 may determine a reference probability corresponding to each of the plurality of samples using a probability estimation model as described elsewhere in the present disclosure. The processing device 112 may determine the value of the evaluation index using the estimated probability and the reference probability corresponding to each of the plurality of samples. For the specific candidate threshold, the processing device 112 may designate a label to each of the plurality of samples based on the specific candidate threshold and the estimated probability corresponding to each of the plurality of samples. The label may include a positive sample or a negative sample. For example, the processing device 112 may designate a positive sample to a sample if the estimated probability corresponding to the sample exceeds the specific candidate threshold. The processing device 112 may designate a negative sample to a sample if the estimated probability corresponding to the sample is smaller than the specific candidate threshold. The processing device 112 may determine an evaluation index corresponding to the specific candidate threshold based on the label and the reference probability corresponding to each of the plurality of samples. More descriptions for determining the evaluation result may be found elsewhere in the present disclosure (e.g., FIG. 6 and the descriptions thereof).

**[0074]** In 510, the processing device 112 (e.g., the determination module 420) may determine a target threshold associated with the machine learning model from the plurality of candidate thresholds based on the evaluation result corresponding to each of the plurality of candidate thresholds. In some embodiments, the processing device 112 may

compare the evaluation result corresponding to each of the plurality of candidate thresholds. Each of the plurality of candidate thresholds may correspond to an evaluation result, i.e., a value of an evaluation index. The processing device 112 may determine the target threshold based on the comparison. The processing device 112 may compare the values of an evaluation index (e.g., AUC) of the machine learning model with respect to the plurality of candidate thresholds. The processing device 112 may designate a candidate threshold that corresponds the maximum or maximum of the values of the evaluation index (e.g., AUC) of the machine learning model with respect to the plurality of candidate thresholds as the target threshold. As another example, the processing device 112 may determine at least two candidate thresholds from the plurality of candidate thresholds. The values of the evaluation index (e.g., AUC) of the machine learning model corresponding to the at least two candidate thresholds may be greater than or smaller than values of the evaluation index corresponding to other candidate thresholds of the plurality of candidate thresholds. The processing device 112 may designate an average of the at least two candidate thresholds as the target threshold.

**[0075]** It should be noted that the above description regarding the process 500 is merely provided for the purposes of illustration, and not intended to limit the scope of the present disclosure. For persons having ordinary skills in the art, multiple variations and modifications may be made under the teachings of the present disclosure. However, those variations and modifications do not depart from the scope of the present disclosure. In some embodiments, one or more operations may be omitted and/or one or more additional operations may be added. For example, operation 510 may be combined into operation 502. Operation 512 and operation 514 may be omitted. As another example, one or more operation in process 600 may be added into the process 500 to determine an evaluation result of the machine learning model. In some embodiments, in operation 514, if the estimated probability corresponding to the specific event equals the target threshold,

the determination module 420 may determine that the specific event is anomalous or normal. In some embodiments, process 500 may also include performing an anomaly detection on the plurality of samples based on the machine learning model for anomaly detection with the target threshold. For example, the processing device 112 may determine one or more anomalies from the plurality of samples using the machine learning model for anomaly detection with the target threshold. In some embodiments, a target machine learning model may be determined based on samples each of whose anomaly status is known, and one or more operations illustrated in FIG. 5 may be omitted. For instance, operation 504 may be omitted.

**[0076]** FIG. 6 is a flowchart illustrating an exemplary process for evaluating a machine learning model according to some embodiments of the present disclosure. At least a portion of process 600 may be implemented on the computing device 200 as illustrated in FIG. 2 or the mobile device 300 as illustrated in FIG. 3. In some embodiments, one or more operations of process 600 may be implemented in the anomaly detection system 100 as illustrated in FIG. 1. In some embodiments, one or more operations in the process 600 may be stored in a storage device (e.g., the storage 120, the ROM 230, the RAM 240, the storage 390) as a form of instructions, and invoked and/or executed by the server 110 (e.g., the processing device 112 in the server 110, or the processor 220 of the computing device 200) or the CPU 340 of the mobile device 300. In some embodiments, the instructions may be transmitted in the form of electronic current or electrical signals. Operation 508 may be performed according to process 600 as described in FIG. 6.

**[0077]** In 602, the processing device 112 (e.g., the evaluation module 430) may determine a reference probability corresponding to each of a plurality of samples based on a probability estimation model. The plurality of samples may be obtained as described in connection with 502. For example, a sample may be associated with an event. The sample may include one or more features (e.g., a feature vector) that characterize the

event. The reference probability corresponding to a specific sample of the plurality of samples may be used to measure and/or indicate a similarity between the specific sample and other samples of the plurality of samples. The greater the reference probability corresponding to a specific sample is, the larger the similarity between the specific sample and other samples of the plurality of samples may be.

**[0078]** The processing device 112 may determine a reference probability corresponding to a specific sample based on the specific sample and other samples of the plurality of samples using the probability estimation model. Exemplary probability estimation models may include using a parametric estimation algorithm, a Bayes algorithm, non-parametric estimation algorithm, etc. For example, the parametric estimation algorithm may include a maximum likelihood algorithm. The non-parametric estimation algorithm may include a histogram probability estimation algorithm, a kernel density estimation algorithm, etc.

**[0079]** In 604, the processing device 112 (e.g., the evaluation module 430) may determine an estimated label for each of the plurality of samples based on a candidate threshold and an estimated probability corresponding to each of the plurality of samples. The estimated probability may be determined as described in connection with operation 504. The candidate threshold may be determined as described in connection with operation 506.

**[0080]** The estimated probability corresponding to a specific sample may be used to measure and/or indicate a possibility that an event associated with the specific sample is anomalous. The processing device 112 may determine an estimated label corresponding to a specific sample by comparing the estimated probability corresponding to the specific sample with the candidate threshold. The estimated label may include a negative sample and a positive sample. The negative sample may indicate that an event associated with the negative sample is anomalous. The positive sample may indicate that an event associated with the positive sample is normal. In some embodiments, if the estimated

probability corresponding to the specific sample exceeds the candidate threshold, the processing device 112 may label the specific sample as a positive sample. If the estimated probability corresponding to the specific sample is smaller the candidate threshold, the processing device 112 may label the specific sample as a negative sample.

**[0081]** In 606, the processing device 112 (e.g., the evaluation module 430) may determine an evaluation index of the machine learning model with respect to the candidate threshold based on the reference probability and the estimated label corresponding to each of the plurality of samples. Exemplary evaluation indexes of the machine learning model for anomaly detection may include an area under curve (AUC), a Gini coefficient, etc. The AUC of the machine learning model for anomaly detection may be defined by a probability that when the machine learning model is used for anomaly detection, a random positive sample is ranked above a random negative sample. The greater the AUC of a machine learning model for anomaly detection is, the greater the accuracy of the machine learning model for anomaly detection estimation may be.

**[0082]** In some embodiments, the processing device 112 may rank the samples according to the reference probability from small to large. The processing device 112 may determine, statistically the probability that a positive sample is ranked above a negative sample. For example, the processing device 112 may determine the value of AUC according to the Equation (1) as below:

$$AUC = \frac{\sum I(P_{positive}, P_{negative})}{M * N} \quad (1),$$

where  $M$  refers to a count of positive samples of the plurality of samples,  $N$  refers to a count of negative samples of the plurality of samples,  $P_{positive}$  refers to a reference probability (i.e., a true score) of a positive sample,  $P_{negative}$  refers to a reference probability (i.e., a true score) of a negative sample, and  $I(P_{positive}, P_{negative})$  may be determined according to equation (2) as below:

$$I(P_{positive}, P_{negative}) = \begin{cases} 1, P_{positive} > P_{negative} \\ 0.5, P_{positive} = P_{negative} \\ 0, P_{positive} < P_{negative} \end{cases}, \quad (2)$$

**[0083]** According to Equation (1), the plurality of samples may include  $M$  positive samples and  $N$  negative samples. The processing device 112 may determine  $M * N$  sample pairs. Each of the  $M * N$  sample pairs may include a negative sample and a positive sample. The processing device 112 may comparing a reference probability corresponding to each of the negative sample and the positive sample in each of the  $M * N$  sample pairs to determine the AUC of the machine learning model for anomaly detection with respect to the candidate threshold.

**[0084]** For example, assuming that the plurality of samples include A, B, C, and D, the estimated probability of each the plurality of samples is 0.9, 0.8, 0.75, and 0.85, respectively, and the reference probability of each the plurality of samples is 0.7, 0.6, 0.8 and 0.9, respectively. The candidate threshold equals the estimated probability 0.85 of sample D. The processing device 112 may label sample A as a positive sample, sample B as a negative sample, sample C as a negative sample, and sample D as a positive sample by comparing the estimated probabilities of sample A, B, C, and D, respectively, with the candidate threshold 0.85. The processing device 112 may determine 4 sample pairs including (A, B), (A, C), (D, B), and (D, C). According to equation (2), the processing device 112 may determine  $I(A, B)$ ,  $I(A, C)$ ,  $I(D, B)$ , and  $I(D, C)$  as 1, 0, 1, and 1, respectively. According to the Equation (1), the AUC of the machine learning model for anomaly detection may be determined as  $AUC = \frac{1+0+1+1}{2*2} = 0.75$ , when designating the estimated probability 0.85 of sample D as the candidate threshold. Similarly, the processing device 112 may determine the AUCs of the machine learning

model for anomaly detection when designating estimated probabilities of samples A, B, and C as the candidate threshold, respectively.

**[0085]** The Gini coefficient of the machine learning model for anomaly detection with respect to the candidate threshold may be determined based on the AUC according to equation (3) as below:

$$Gini = 2 * AUC - 1. \quad (3)$$

**[0086]** It should be noted that the above description regarding the process 600 is merely provided for the purposes of illustration, and not intended to limit the scope of the present disclosure. For persons having ordinary skills in the art, multiple variations and modifications may be made under the teachings of the present disclosure. However, those variations and modifications do not depart from the scope of the present disclosure.

**[0087]** FIG. 7 is a flowchart illustrating an exemplary process 700 for anomaly detection according to some embodiments of the present disclosure. At least a portion of process 700 may be implemented on the computing device 200 as illustrated in FIG. 2 or the mobile device 300 as illustrated in FIG. 3. In some embodiments, one or more operations of process 700 may be implemented in the anomaly detection system 100 as illustrated in FIG. 1. In some embodiments, one or more operations in the process 500 may be stored in a storage device (e.g., the storage 120, the ROM 230, the RAM 240, the storage 390) as a form of instructions, and invoked and/or executed by the server 110 (e.g., the processing device 112 in the server 110, or the processor 220 of the computing device 200) or the CPU 340 of the mobile device 300. In some embodiments, the instructions may be transmitted in the form of electronic current or electrical signals.

**[0088]** In 702, the processing device 112 (e.g., the acquisition module 410) may obtain data associated with a specific event. In some embodiments, the specific event may be an event associated with one of the plurality of samples. The data associated with the specific event may be one of the plurality of samples. In some embodiments, the data

associated with the specific event may be obtained by the acquisition module 410 from the data providing system 130, the service providing system 140, the storage 120, etc. The data associated with the specific event may include one or more features that characterizes the specific event as described elsewhere in the present disclosure.

**[0089]** In 704, the processing device 112 (e.g., the acquisition module 410) may obtain a machine learning model for anomaly detection with a target threshold. The acquisition module 410 may obtain the machine learning model with the target threshold from the storage 120, the data providing system 130, the service providing system 140, and any other storage device as described elsewhere in the present disclosure.

**[0090]** The machine learning model for anomaly detection may include an unsupervised machine learning model, a semi-unsupervised machine learning model, etc., as described elsewhere in the present disclosure (e.g., FIG. 5, and the descriptions thereof). In some embodiments, the target threshold may be used by the machine learning model for anomaly detection to determine whether an event is anomalous based on. The target threshold may be determined according to process 500 as described in FIG. 5. The target threshold may be determined using a plurality of samples associated with different events each of whose anomaly status (whether an event is anomalous or not) is unknown. In some embodiments, the plurality of samples may include the data associated with the event obtained in operation 702. Estimated probabilities corresponding to the plurality of samples may be determined. Further, a plurality of candidate thresholds associated with a machine learning model for anomaly detection may be determined. Then an evaluation result may be determined by evaluating the machine learning model, with respect to each of the plurality of candidate thresholds, for detecting anomaly of the samples. A target threshold associated with the machine learning model from the plurality of candidate thresholds may be determined based on the evaluation result.

**[0091]** In 706, the processing device 112 (e.g., the determination module 420) may determine whether the specific event is anomalous based on the data associated with the specific event and the machine learning model with the target threshold. The processing device 112 may determine whether the specific event is anomalous by inputting the data associated with the specific event into the machine learning model. In some embodiments, the machine learning model for anomaly detection may be configured to determine and output an estimated probability corresponding to the specific event based on the inputted data associated with the specific event. Further, the determination module 420 may compare the estimated probability with the target threshold. If the estimated probability corresponding to the specific event is smaller than the target threshold, the determination module 420 may determine that the specific event is anomalous. If the estimated probability corresponding to the specific event exceeds the target threshold, the determination module 420 may determine that the event is normal. In some embodiments, the machine learning model for anomaly detection may be configured to determine an estimated probability corresponding to the specific event and determine whether the specific event is anomalous based on the inputted data associated with the specific event and the target threshold. The machine learning model for anomaly detection may be configured to output an estimated result of the specific event. For example, if the specific event is anomalous, the machine learning model for anomaly detection may output "0." If the specific event is normal, the machine learning model for anomaly detection may output "1."

**[0092]** FIGs. 8A-8D illustrate schematic diagrams of exemplary anomaly detection results according to some embodiments of the present disclosure. As shown in FIG. 8A, the horizontal axis represents the time axis. The vertical axis represents sample signals obtained over time. Curve "a" and Curve "b" represents service indicators associated with the sample signals. Curve "c" represents alarm signals that indicate an anomaly

appears. The greater a peak of curve “a” or curve “b”, the greater a possibility that an anomaly exists may be. As shown in FIG. 8A, the anomaly detection was performed using a machine learning model for anomaly detection with respect to a target threshold of about 0.1387. The AUC of the machine learning model for anomaly detection with respect to a threshold of about 0.1387 was about 0.9376. FIG. 8A shows a plurality of anomalies appeared during anomaly detection. As shown in FIG. 8B, the anomaly detection was performed using a machine learning model for anomaly detection with respect to a target threshold of about 0.1728. The AUC of the machine learning model for anomaly detection with respect to the threshold of about 0.1728 was about 0.9671. FIG. 8B shows that a plurality of anomalies appeared during anomaly detection. As shown in FIG. 8C, the anomaly detection was performed using a machine learning model for anomaly detection with respect to a threshold of about 0.5838. The AUC of the machine learning model for anomaly detection with respect to the threshold about 0.5838 was about 0.9998. FIG. 8C shows that an anomaly appeared at the time corresponding to a maximum peak “P.” As shown in FIG. 8D, the anomaly detection was performed using a machine learning model for anomaly detection with respect to a target threshold of about 0.8272. The AUC of the machine learning model for anomaly detection with respect to the threshold about 0.8272 was about 0.9980. FIG. 8D shows that at least two anomalies appeared at the time corresponding to a maximum peak “P.” Generally, one single anomaly may appear at the time corresponding to a maximum peak, e.g., peak “P.” Accordingly, the greater the AUC of a machine learning model for anomaly detection is, the greater the accuracy of the machine learning model for anomaly detection may be.

**[0093]** Having thus described the basic concepts, it may be rather apparent to those skilled in the art after reading this detailed disclosure that the foregoing detailed disclosure is intended to be presented by way of example only and is not limiting. Various alterations, improvements, and modifications may occur and are intended to those skilled

in the art, though not expressly stated herein. These alterations, improvements, and modifications are intended to be suggested by this disclosure, and are within the spirit and scope of the exemplary embodiments of this disclosure.

**[0094]** Moreover, certain terminology has been used to describe embodiments of the present disclosure. For example, the terms “one embodiment,” “an embodiment,” and/or “some embodiments” mean that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present disclosure. Therefore, it is emphasized and should be appreciated that two or more references to “an embodiment,” “one embodiment,” or “an alternative embodiment” in various portions of this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures or characteristics may be combined as suitable in one or more embodiments of the present disclosure.

**[0095]** Further, it will be appreciated by one skilled in the art, aspects of the present disclosure may be illustrated and described herein in any of a number of patentable classes or context including any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof. Accordingly, aspects of the present disclosure may be implemented entirely hardware, entirely software (including firmware, resident software, micro-code, etc.) or combining software and hardware implementation that may all generally be referred to herein as a “block,” “module,” “engine,” “unit,” “component,” or “system.” Furthermore, aspects of the present disclosure may take the form of a computer program product embodied in one or more computer readable media having computer readable program code embodied thereon.

**[0096]** A computer readable signal medium may include a propagated data signal with computer readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated signal may take any of a variety of forms, including electro-magnetic, optical, or the like, or any suitable combination thereof. A computer

readable signal medium may be any computer readable medium that is not a computer readable storage medium and that may communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device. Program code embodied on a computer readable signal medium may be transmitted using any appropriate medium, including wireless, wireline, optical fiber cable, RF, or the like, or any suitable combination of the foregoing.

**[0097]** Computer program code for carrying out operations for aspects of the present disclosure may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Scala, Smalltalk, Eiffel, JADE, Emerald, C++, C#, VB. NET, Python or the like, conventional procedural programming languages, such as the “C” programming language, Visual Basic, Fortran 1703, Perl, COBOL 1702, PHP, ABAP, dynamic programming languages such as Python, Ruby and Groovy, or other programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider) or in a cloud computing environment or offered as a service such as a software as a service (SaaS).

**[0098]** Furthermore, the recited order of processing elements or sequences, or the use of numbers, letters, or other designations, therefore, is not intended to limit the claimed processes and methods to any order except as may be specified in the claims. Although the above disclosure discusses through various examples what is currently considered to be a variety of useful embodiments of the disclosure, it is to be understood that such detail

is solely for that purpose, and that the appended claims are not limited to the disclosed embodiments, but, on the contrary, are intended to cover modifications and equivalent arrangements that are within the spirit and scope of the disclosed embodiments. For example, although the implementation of various components described above may be embodied in a hardware device, it may also be implemented as a software-only solution—e.g., an installation on an existing server or mobile device.

**[0099]** Similarly, it should be appreciated that in the foregoing description of embodiments of the present disclosure, various features are sometimes grouped together in a single embodiment, figure, or description thereof for the purpose of streamlining the disclosure aiding in the understanding of one or more of the various embodiments. This method of disclosure, however, is not to be interpreted as reflecting an intention that the claimed subject matter requires more features than are expressly recited in each claim. Rather, claimed subject matter may lie in less than all features of a single foregoing disclosed embodiment.

**WE CLAIM:**

1. A system for anomaly detection, comprising:

at least one storage medium including a set of instructions;

at least one processor in communication with the at least one storage medium, wherein when executing the set of instructions, the at least one processor is directed to cause the system to perform operations including:

obtaining a plurality of samples, each of the plurality of samples being associated with an event;

for each of the plurality of samples, determining, based on a machine learning model for the anomaly detection, an estimated probability that the event corresponding to the each of the plurality of samples is anomalous;

determining, based on estimated probabilities corresponding to at least a portion of the plurality of samples, a plurality of candidate thresholds associated with the machine learning model for the anomaly detection;

determining an evaluation result by evaluating the machine learning model for the anomaly detection with respect to each of the plurality of candidate thresholds; and

determining, based on the evaluation result, a target threshold associated with the machine learning model for the anomaly detection from the plurality of candidate thresholds.

2. The system of claim 1, wherein the machine learning model includes at least one of a one-class support vector machine (SVM) model or an isolation forest algorithm.

3. The system of claim 1 or claim 2, wherein to determine, based on estimated probabilities corresponding to at least a portion of the plurality of samples, a plurality of candidate thresholds associated with the machine learning model, the at least one

processor is directed to cause the system to perform additional operations including:

designating the estimated probability corresponding to each of the at least a portion of the plurality of samples as one of the plurality of candidate thresholds.

4. The system of any one of claims 1 to 3, wherein to evaluate the machine learning model with respect to each of the plurality of candidate thresholds, the at least one processor is directed to cause the system to perform additional operations including:

for each of the plurality of samples,

determining, based on a probability estimation model, a reference probability corresponding to the each of the plurality of samples; and

evaluating, based on the estimated probability and the reference probability, the machine learning model with respect to each of the plurality of candidate thresholds.

5. The system of claim 4, wherein to evaluate, based on the estimated probability and the reference probability, the machine learning model, the at least one processor is directed to cause the system to perform additional operations including:

determining, based on the reference probability and the estimated probability, an evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds.

6. The system of claim 5, wherein to determine, based on the reference probability and the estimated probability, an evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds, the at least one processor is directed to cause the system to perform additional operations including:

determining, based on each of the plurality of candidate thresholds and the estimated probability, an estimated label of each of the plurality of samples, the estimated label

including a negative sample or a positive sample; and

determining, based on the reference probability and the estimated label, the evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds.

7. The system of claim 6, wherein the at least one processor is further directed to cause the system to perform additional operations including:

ranking the reference probability of each of the plurality of samples, wherein determining the evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds includes:

determining, based on the ranked reference probability, and the estimated label corresponding to each of the plurality of the samples, the evaluation index.

8. The system of any one of claims 5 to 7, wherein the evaluation index of the machine learning model includes at least one of an area under curve (AUC) or a Gini coefficient.

9. The system of any one of claims 5 to 8, wherein to determine, based on the evaluation result, a target threshold associated with the machine learning model from the plurality of candidate thresholds, the at least one processor is directed to cause the system to perform additional operations including:

identifying, from the plurality of candidate thresholds, a candidate threshold that corresponds to a maximum of the evaluation index; and

designating the identified candidate threshold as the target threshold associated with the machine learning model.

10. The system of any one of claims 1 to 9, wherein the at least one processor is

directed to cause the system to perform additional operations including:

obtaining data associated with a specific event; and

determining, based on the data associated with the specific event and the machine learning model with respect to the target threshold, whether the specific event is anomalous.

11. A method for anomaly detection, comprising:

obtaining a plurality of samples, each of the plurality of samples being associated with an event;

for each of the plurality of samples, determining, based on a machine learning model for the anomaly detection, an estimated probability that the event corresponding to the each of the plurality of samples is anomalous;

determining, based on estimated probabilities corresponding to at least a portion of the plurality of samples, a plurality of candidate thresholds associated with the machine learning model;

determining an evaluation result by evaluating the machine learning model for the anomaly detection with respect to each of the plurality of candidate thresholds; and

determining, based on the evaluation result, a target threshold associated with the machine learning model for the anomaly detection from the plurality of candidate thresholds.

12. The method of claim 11, wherein the machine learning model includes at least one of a one-class support vector machine (SVM) model or an isolation forest algorithm.

13. The method of claim 11 or claim 12, wherein the determining, based on estimated probabilities corresponding to at least a portion of the plurality of samples, a plurality of

candidate thresholds associated with the machine learning model includes:

designating the estimated probability corresponding to each of the at least a portion of the plurality of samples as one of the plurality of candidate thresholds.

14. The method of any one of claims 11 to 13, wherein the evaluating the machine learning model with respect to each of the plurality of candidate thresholds includes:

for each of the plurality of samples,

determining, based on a probability estimation model, a reference probability corresponding to the each of the plurality of samples; and

evaluating, based on the estimated probability and the reference probability, the machine learning model with respect to each of the plurality of candidate thresholds.

15. The method of claim 14, wherein the evaluating, based on the estimated probability and the reference probability, the machine learning model includes:

determining, based on the reference probability and the estimated probability, an evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds; and

evaluating, based on the evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds, the machine learning model.

16. The method of claim 15, wherein the determining, based on the reference probability and the estimated probability, an evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds includes:

determining, based on each of the plurality of candidate thresholds and the estimated probability, an estimated label of each of the plurality of samples, the estimated label including a negative sample or a positive sample; and

determining, based on the reference probability and the estimated label, the evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds.

17. The method of claim 16, further comprising:

ranking the reference probability of each of the plurality of samples, wherein determining the evaluation index of the machine learning model with respect to each of the plurality of candidate thresholds includes:

determining, based on the ranked reference probability and the estimated label corresponding to each of the plurality of the samples, the evaluation index.

18. The method of any one of claims 15 to 17, wherein the evaluation index of the machine learning model includes at least one of an area under curve (AUC) or a Gini coefficient.

19. The method of any one of claims 15 to 18, wherein the determining, based on the evaluation result, a target threshold associated with the machine learning model from the plurality of candidate thresholds includes:

identifying, from the plurality of candidate thresholds, a candidate threshold that corresponds to a maximum of the evaluation index; and

designating the identified candidate threshold as the target threshold associated with the machine learning model.

20. The method of any one of claims 11 to 19, further comprising:

obtaining data associated with a specific event; and

determining, based on the data associated with the specific event and the machine

learning model with respect to the target threshold, whether the specific event is anomalous.

21. A non-transitory computer readable medium storing instructions, the instructions, when executed by at least one processor, causing the at least one processor to implement a method comprising:

- obtaining a plurality of samples, each of the plurality of samples being associated with an event;

- for each of the plurality of samples, determining, based on a machine learning model for the anomaly detection, an estimated probability that the event corresponding to the each of the plurality of samples is anomalous;

- determining, based on estimated probabilities corresponding to at least a portion of the plurality of samples, a plurality of candidate thresholds associated with the machine learning model;

- determining an evaluation result by evaluating the machine learning model for the anomaly detection with respect to each of the plurality of candidate thresholds; and

- determining, based on the evaluation result, a target threshold associated with the machine learning model for the anomaly detection from the plurality of candidate thresholds.

22. A system for anomaly detection, comprising:

- an acquisition module configured to obtain a plurality of samples, each of the plurality of samples being associated with an event;

- a determination module configured to:

- for each of the plurality of samples, determine, based on a machine learning model for the anomaly detection, an estimated probability that the event corresponding to the each

of the plurality of samples is anomalous; and

determining, based on estimated probabilities corresponding to at least a portion of the plurality of samples, a plurality of candidate thresholds associated with the machine learning model; and

an evaluation module configured to determine an evaluation result by evaluating the machine learning model for the anomaly detection with respect to each of the plurality of candidate thresholds, and wherein the determination module is further configured to:

determine, based on the evaluation result, a target threshold associated with the machine learning model for the anomaly detection from the plurality of candidate thresholds.

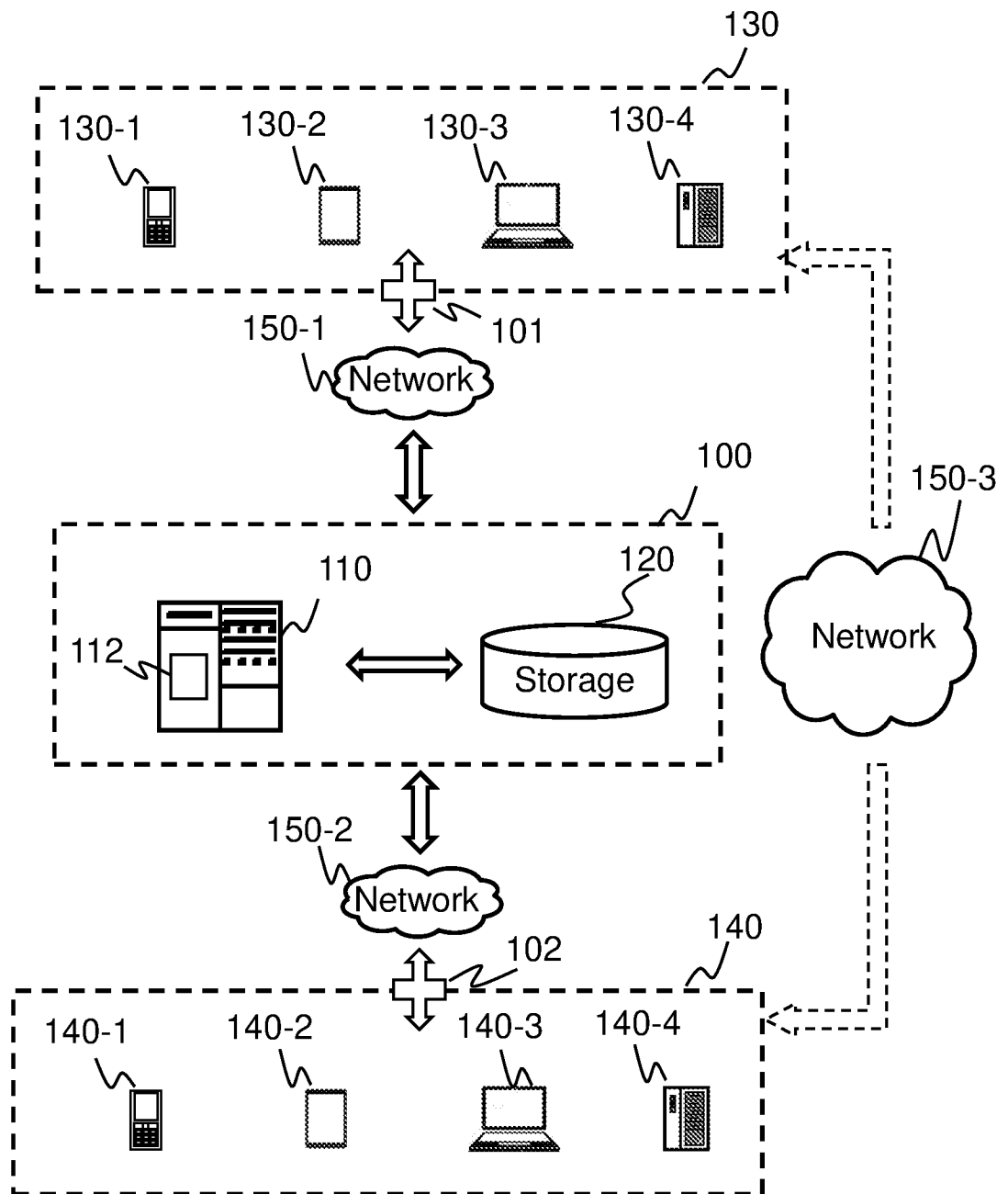
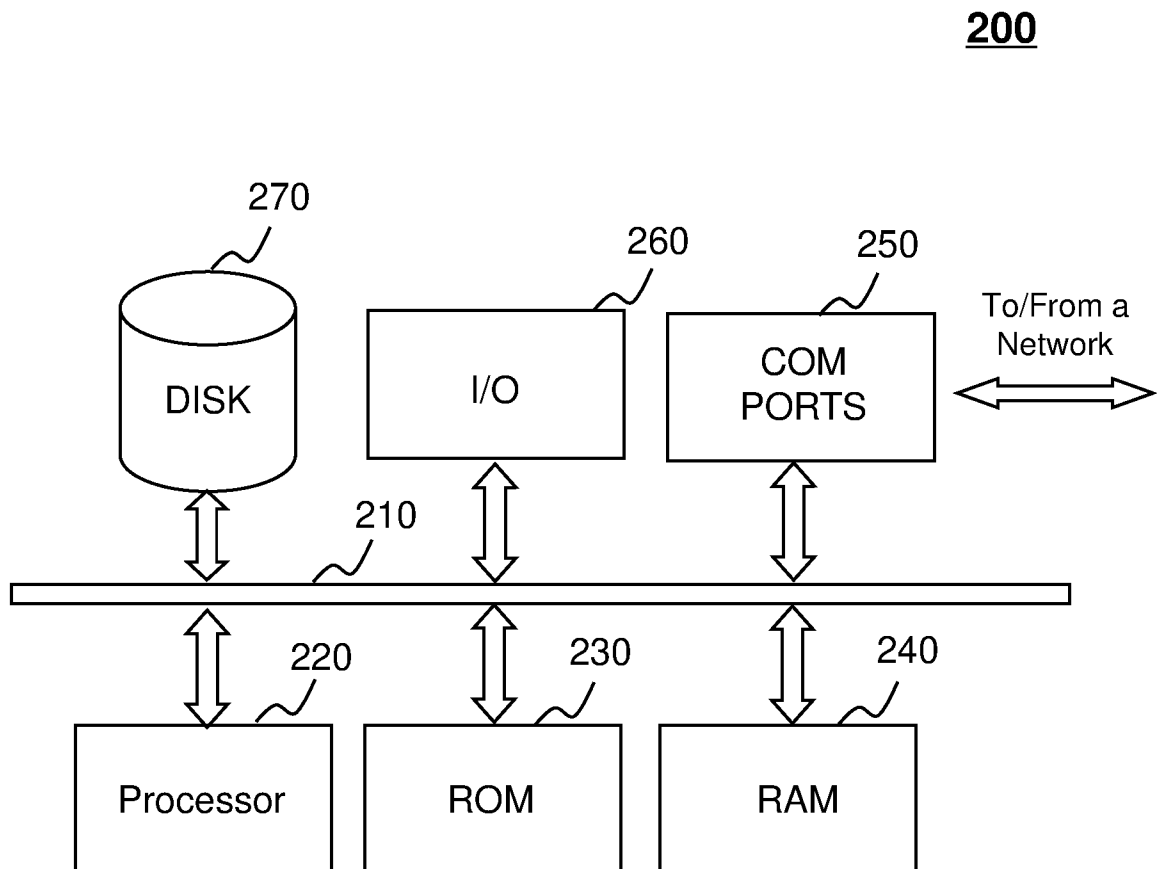
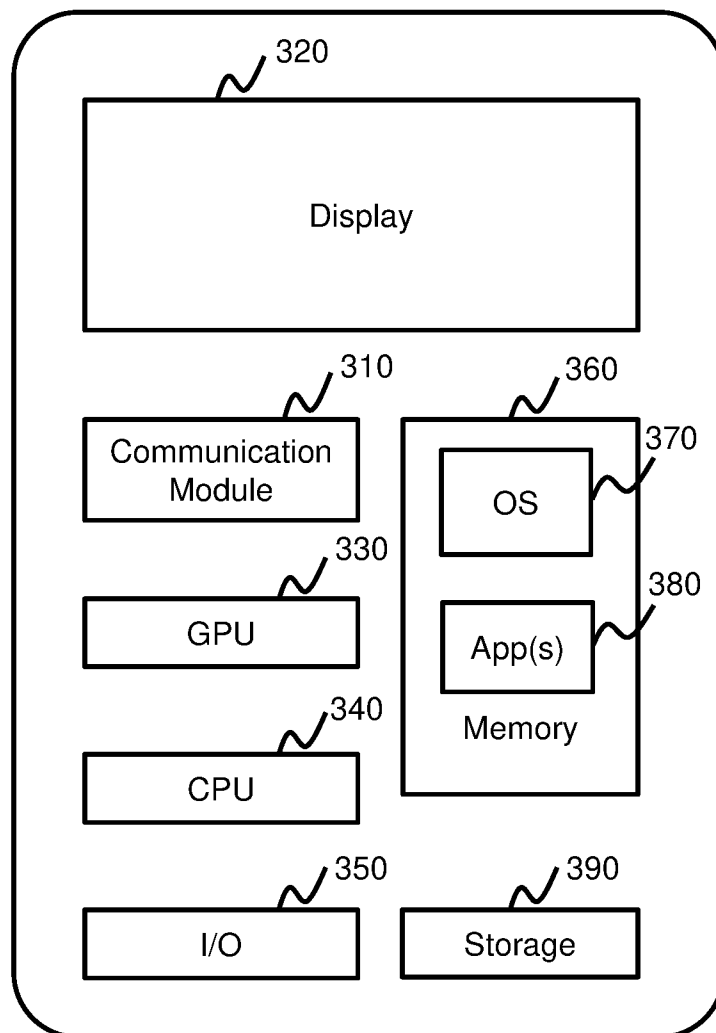


FIG. 1

**FIG. 2**

**300****FIG. 3**

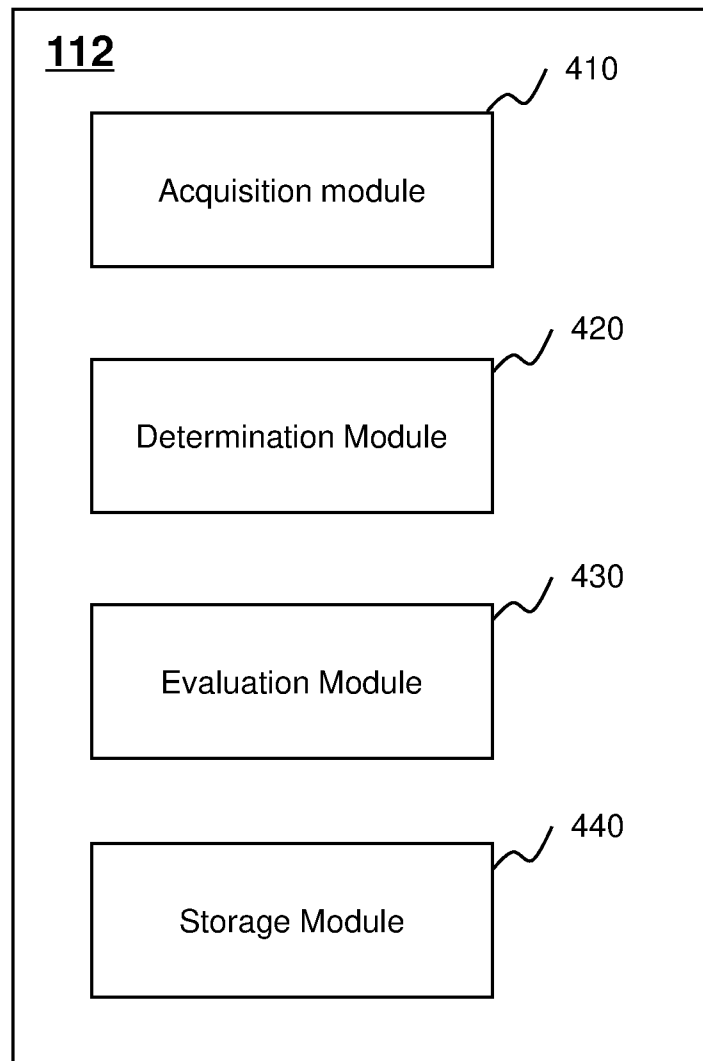


FIG. 4

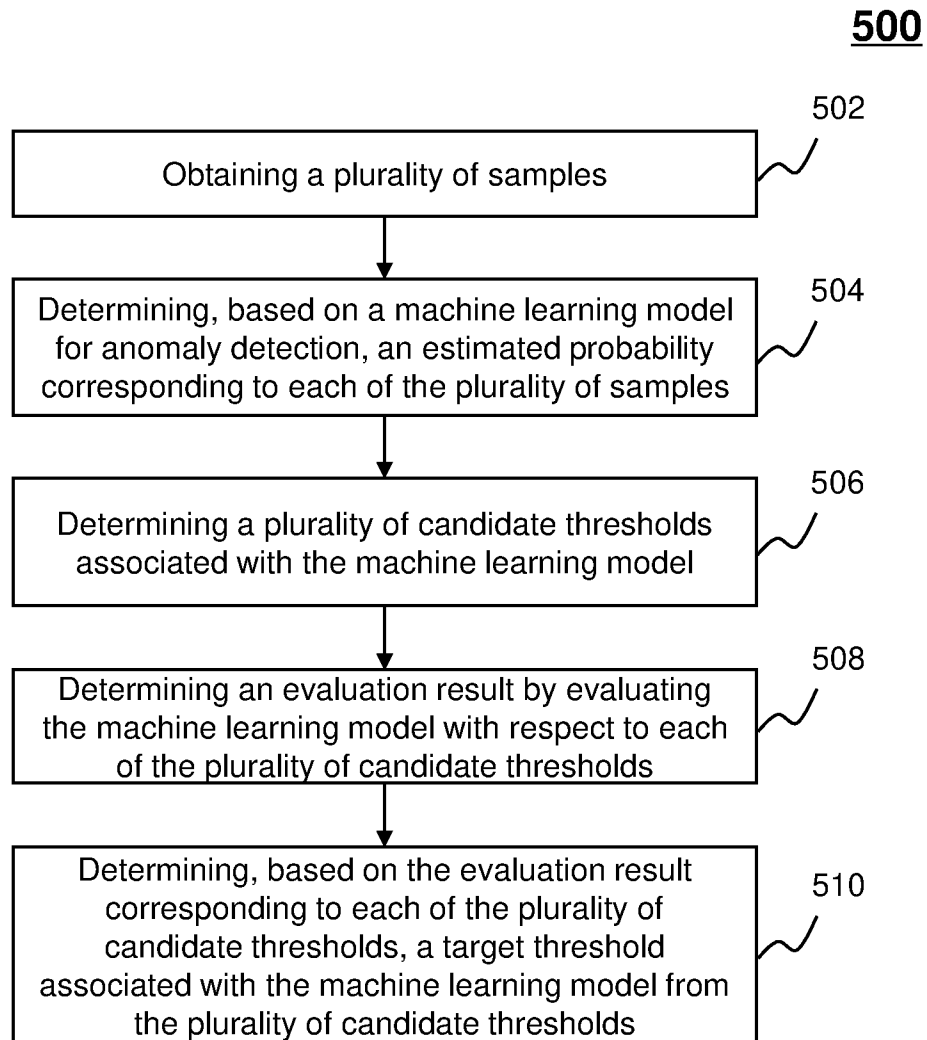


FIG. 5

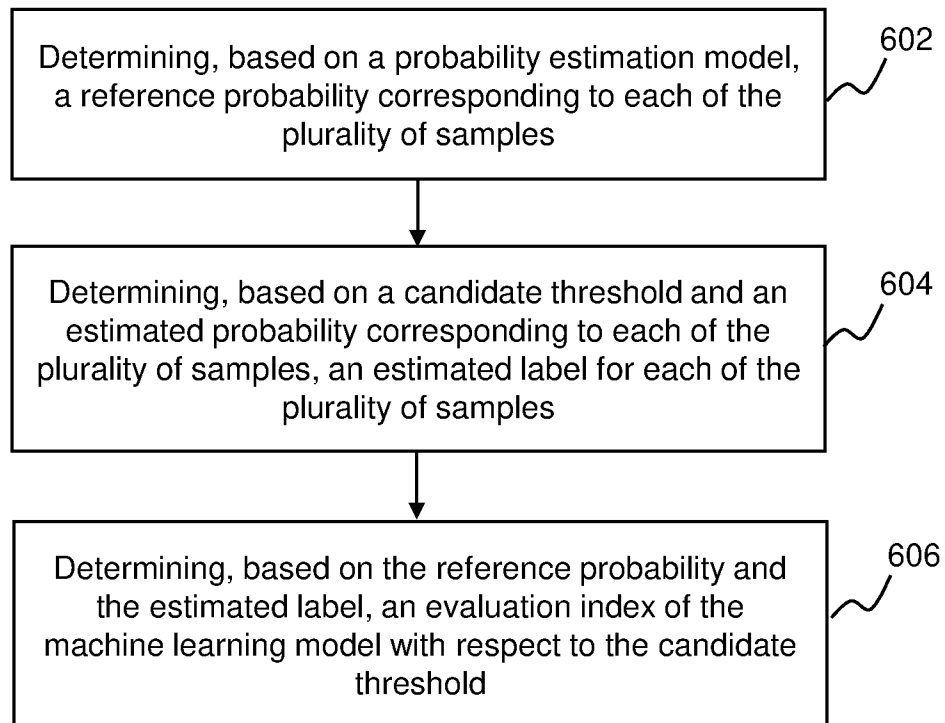
**600**

FIG. 6

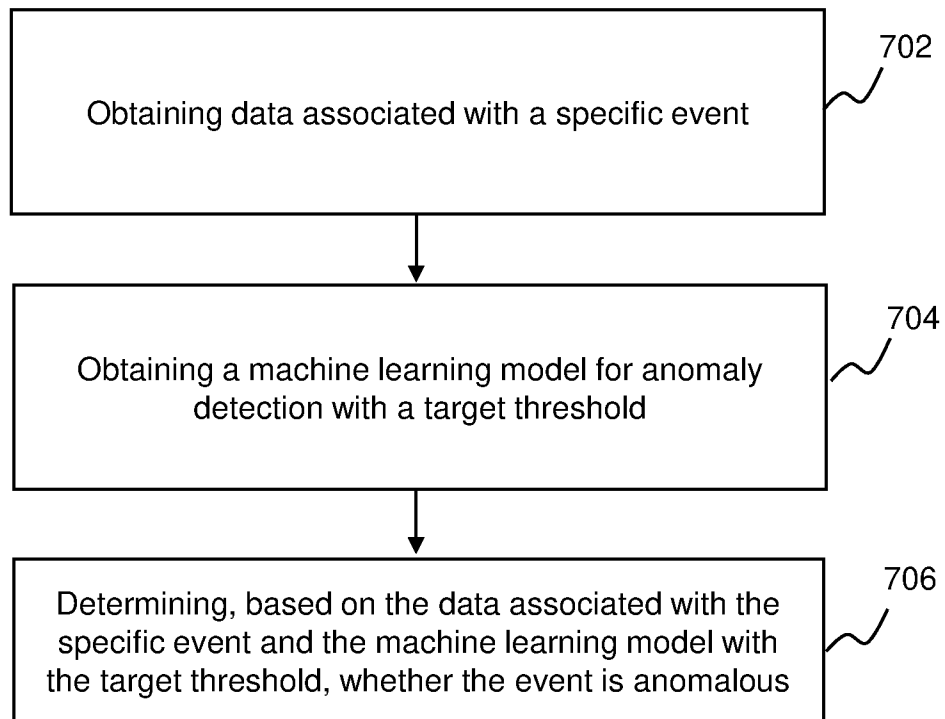
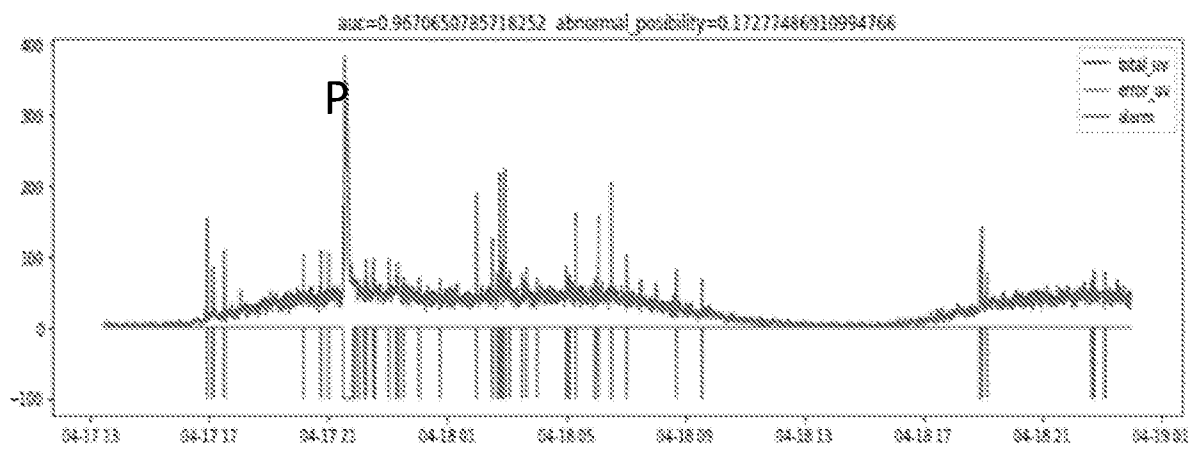
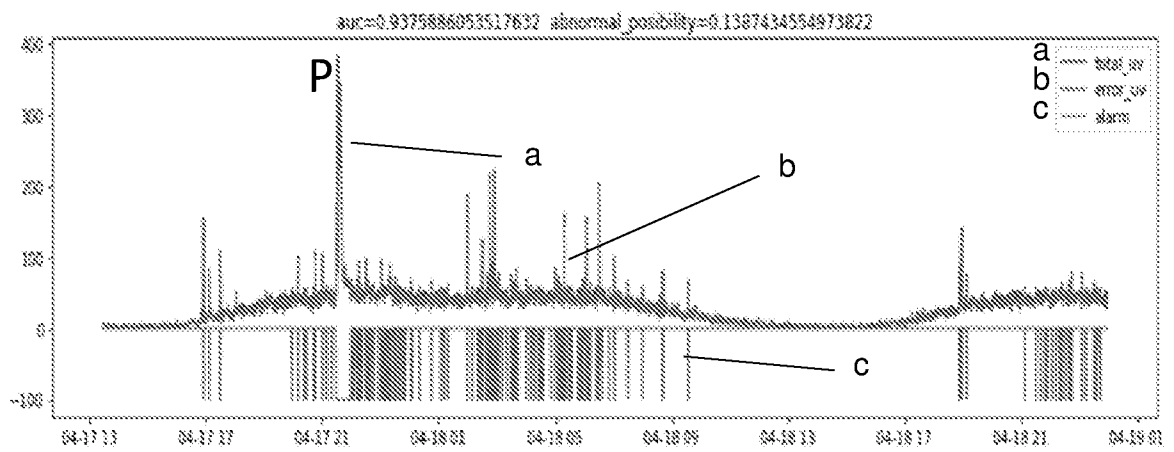
**700**

FIG. 7



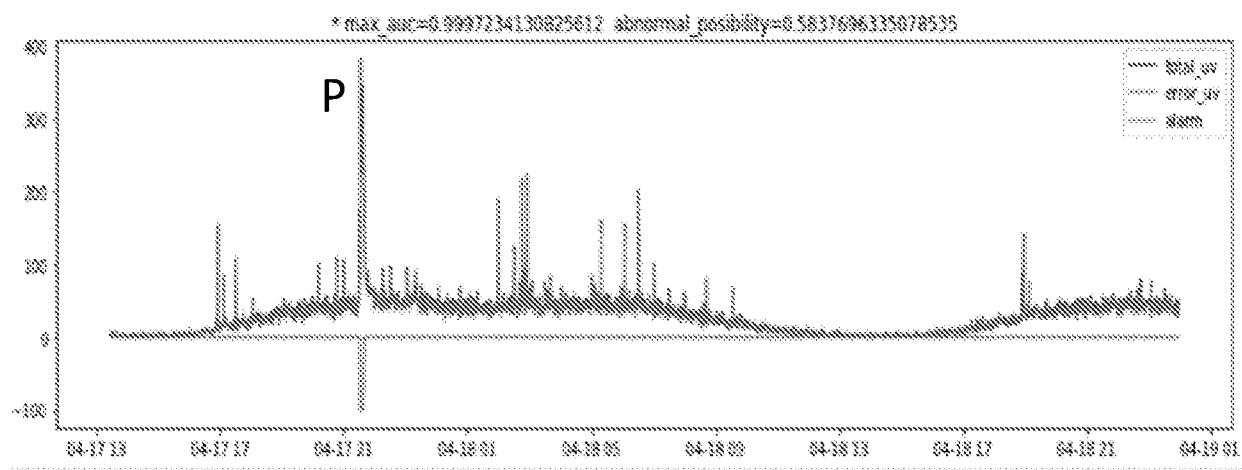


FIG. 8C

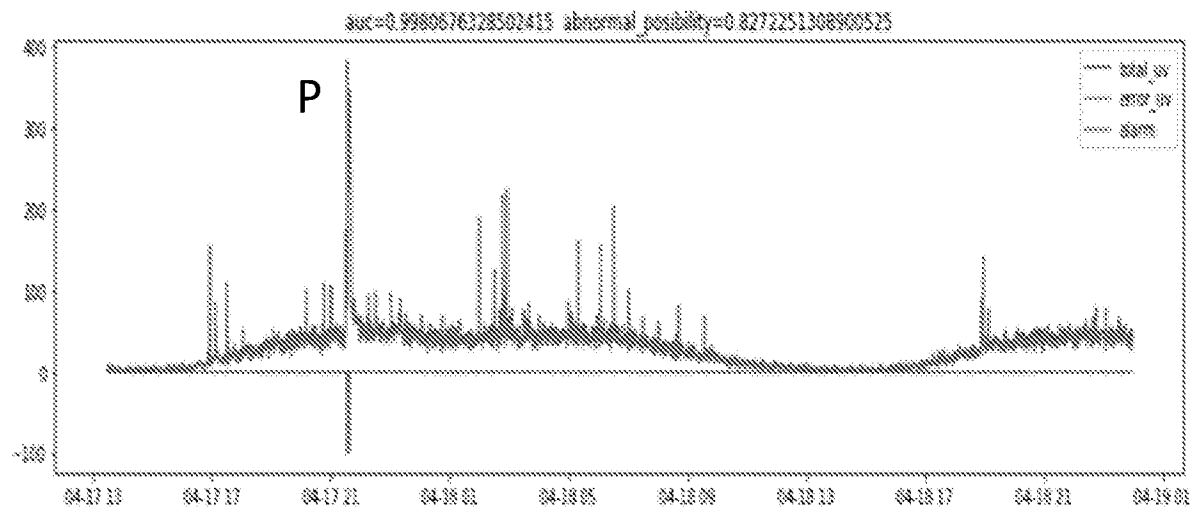


FIG. 8D

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/091433

**A. CLASSIFICATION OF SUBJECT MATTER**

G06F 16/215(2019.01)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

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)

WPI, EPODOC, CNKI, CNPAT: sample, event, machine, learning, model, anomaly, probability, candidate, threshold, svm

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                               | Relevant to claim No. |
|-----------|----------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| X         | CN 109522304 A (CHINA UNITED NETWORK COMMUNICATIONS CORP.) 26 March 2019 (2019-03-26)<br>paragraphs [0038]-[0045], [0087]-[0108] | 1-22                  |
| A         | US 2018096261 A1 (INTEL CORPORATION) 05 April 2018 (2018-04-05)<br>the whole document                                            | 1-22                  |
| A         | US 2018247220 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 30 August 2018 (2018-08-30)<br>the whole document                 | 1-22                  |



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

17 February 2020

Date of mailing of the international search report

10 March 2020

Name and mailing address of the ISA/CN

National Intellectual Property Administration, PRC  
6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing  
100088  
China

Authorized officer

HU, Ping

Facsimile No. (86-10)62019451

Telephone No. 86-(10)-53961335

**INTERNATIONAL SEARCH REPORT**  
**Information on patent family members**

International application No.

**PCT/CN2019/091433**

| Patent document<br>cited in search report |            |    | Publication date<br>(day/month/year) | Patent family member(s) |            |    | Publication date<br>(day/month/year) |
|-------------------------------------------|------------|----|--------------------------------------|-------------------------|------------|----|--------------------------------------|
| CN                                        | 109522304  | A  | 26 March 2019                        | None                    |            |    |                                      |
| US                                        | 2018096261 | A1 | 05 April 2018                        | WO                      | 2018063701 | A1 | 05 April 2018                        |
| US                                        | 2018247220 | A1 | 30 August 2018                       | None                    |            |    |                                      |