

RULE DETECTION METHOD, COMPUTER SYSTEM, AND READABLE STORAGE MEDIUM

TECHNICAL FIELD

[0001] This specification relates to the field of computer technologies, and in particular, to a
5 rule detection method, a computer system, and a readable storage medium.

BACKGROUND

[0002] Currently, a corresponding marketing rule usually needs to be configured for execution
of an online service, to provide a user with rich service experience. For example, a marketing rule
such as "spend 100 and get 50% off for a product A" can be configured for an online marketing
10 activity of the product A, so that the user can purchase the product A at a more affordable price.

[0003] To ensure normal service experience of the user, the marketing rule needs to be detected
before the marketing rule goes online, to ensure normal use of the marketing rule. However,
because many marketing rules are actually configured, a worker needs to spend a large amount of
time to complete detection of the marketing rules. In addition, a plurality of marketing rules can
15 be used together in actual applications. In this case, the worker can detect the plurality of marketing
rules only when a logical relationship between the marketing rules is accurately sorted out.
Consequently, there is a very high capability requirement for the worker, and a detection error
inevitably occurs.

[0004] Therefore, how to accurately detect the marketing rule is an urgent problem to be
20 resolved.

SUMMARY

[0005] This specification provides a rule detection method, a computer system, and a readable
storage medium, to partially resolve the above-mentioned problems in the conventional technology.

[0006] This specification provides a rule detection method, including: obtaining a to-be-
25 detected rule, where several subrules and a combination manner between the subrules are recorded

in the to-be-detected rule; predicting, based on the several subrules and the combination manner, traffic that needs to be hit by the to-be-detected rule, and querying, from preset historical traffic data, historical traffic data actually hit by the to-be-detected rule; and detecting the to-be-detected rule based on the historical traffic data actually hit by the to-be-detected rule and the predicted traffic that needs to be hit by the to-be-detected rule.

[0007] This specification provides a computer system. The computer system includes a memory, a processor, and a computer program that is stored in the memory and that is capable of running on the processor, and when executing the program, the processor implements the following steps: obtaining a to-be-detected rule, where several subrules and a combination manner between the subrules are recorded in the to-be-detected rule; predicting, based on the several subrules and the combination manner, traffic that needs to be hit by the to-be-detected rule, and querying, from preset historical traffic data, historical traffic data actually hit by the to-be-detected rule; and detecting the to-be-detected rule based on the historical traffic data actually hit by the to-be-detected rule and the predicted traffic that needs to be hit by the to-be-detected rule.

[0008] This specification provides a readable storage medium. The storage medium stores a computer program, and when the computer program is executed by a processor, the rule detection method is implemented.

[0009] The above-mentioned at least one technical solution used in this specification can achieve the following beneficial effects:

[0010] In the rule detection method provided in the embodiments of this specification, after a to-be-detected rule is obtained, historical traffic data that can be actually hit by the to-be-detected rule can be determined based on historical traffic data, and then whether the to-be-detected rule is mismatched is detected based on a combination manner between subrules included in the to-be-detected rule and the historical traffic data that can be actually hit by the to-be-detected rule. In this manner, detection efficiency can be greatly improved, and time of rule detection can be reduced. In addition, rule detection accuracy can be effectively improved.

BRIEF DESCRIPTION OF DRAWINGS

[0011] The accompanying drawings described herein are used to provide a further understanding of this specification and constitute a part of this specification. The example

embodiments of this specification and descriptions thereof are used to explain this specification, and do not constitute an improper limitation on this specification. In the accompanying drawings:

[0012] FIG. 1 is a schematic flowchart of a rule detection method according to an embodiment of this specification;

5 [0013] FIG. 2 is a detailed flowchart of rule detection according to an embodiment of this specification; and

[0014] FIG. 3 is a schematic structural diagram of a computer system according to an embodiment of this specification.

DESCRIPTION OF EMBODIMENTS

10 [0015] To make the objectives, technical solutions, and advantages of this specification clearer, the following clearly and comprehensively describes the technical solutions of this specification with reference to specific embodiments and accompanying drawings of this specification. Clearly, the described embodiments are merely some but not all of embodiments of this specification. All other embodiments obtained by a person of ordinary skill in the art based on the embodiment of
15 this specification without creative efforts shall fall within the protection scope of this specification.

[0016] The following describes in detail the technical solutions provided in the embodiments of this specification with reference to the accompanying drawings.

[0017] FIG. 1 is a schematic flowchart of a rule detection method according to this specification. The method includes the following steps.

20 [0018] S101: Obtain a to-be-detected rule, where several subrules and a combination manner between the subrules are recorded in the to-be-detected rule.

[0019] In actual applications, corresponding marketing rules can be used for various services. The marketing rules are usually configured by a worker based on actual requirements and experience, to provide a user with better service experience.

25 [0020] The marketing rules need to be detected before the marketing rules actually go online, to ensure that the marketing rules do not become abnormal in actual use. In this embodiment of this specification, a marketing rule that needs to be detected before the marketing rule goes online can be referred to as a to-be-detected rule.

[0021] The to-be-detected rule can actually include several subrules. The subrules can be

combined in a specific combination manner, to obtain the to-be-detected rule.

[0022] The combination manner mentioned herein is mainly used to reflect an "or" or "and" logical operation relationship between the subrules. For example, it is assumed that the to-be-detected rule includes a subrule 1 and a subrule 2, the subrule 1 is that a coupon can be used at a merchant A, a merchant B, or a merchant C, and the subrule 2 is that a 20% off coupon can be used when a total settlement price exceeds 200. A combination manner between the subrule 1 and the subrule 2 is an "and" combination manner. Traffic that needs to be hit by the to-be-detected rule needs to be traffic of using a 20% off coupon when a total settlement price at the merchant A, the merchant B, or the merchant C exceeds 200.

[0023] In this embodiment of this specification, the to-be-detected rule can be determined and obtained in a plurality of manners. For example, a new marketing rule or a modified marketing rule can be perceived in real time by subscribing to a change notification of a marketing rule table, and the perceived new marketing rule or modified marketing rule is a to-be-detected rule. For another example, a corresponding listener can be set to listen to a change situation of the marketing rule in real time. After the listener obtains a new marketing rule or a modified marketing rule through listening, the new marketing rule or the modified marketing rule can be determined, and a change message is sent based on a rule identifier corresponding to the marketing rule, to determine and obtain a to-be-detected rule based on the change message.

[0024] In this embodiment of this specification, the rule detection method can be performed by a terminal device such as a desktop computer, or certainly, can be a client or a server installed on the terminal device. For ease of description, in this embodiment of this specification, only an example that the server serves as an execution body is used to describe the rule detection method provided in this embodiment of this specification.

[0025] S102: Predict, based on the several subrules and the combination manner, the traffic that needs to be hit by the to-be-detected rule, and query, from preset historical traffic data, historical traffic data actually hit by the to-be-detected rule.

[0026] Regardless of whether the to-be-detected rule is mismatched, the specific traffic that needs to be hit by the to-be-detected rule can be reflected actually based on the combination manner between the several subrules included in the to-be-detected rule. Therefore, the server can predict, based on the combination manner, the traffic that needs to be hit by the to-be-detected rule.

[0027] In this embodiment of this specification, the predicted traffic that needs to be hit by the

to-be-detected rule is not necessarily predicted traffic actually hit by the to-be-detected rule, but mainly reflects some features of the traffic that needs to be hit by the to-be-detected rule. The features can be mainly reflected in two aspects: One is to indicate a value range of a field value included in the traffic that needs to be hit by the to-be-detected rule, and the other is to indicate a specific field value that needs to exist and a specific field value that does not need to exist in the traffic that needs to be hit by the to-be-detected rule.

[0028] There are two aspects mainly because in actual applications, the subrules included in the to-be-detected rule can be classified into two categories. One is a value type rule. The value type rule is mainly used to reflect a range to which a marketing rule is applicable. For example, when a cumulative shopping amount exceeds 500, 30% off is got for all products. Such a marketing rule is a value type rule. The other one is an enumeration type rule. The enumeration type rule is mainly used to reflect an individual to which a marketing rule is applicable. For example, a voucher can be used if shopping is performed at the merchant A, the merchant B, or the merchant C. Such a marketing rule is an enumeration type rule.

[0029] For the value type rule, the server can predict, based on a field value used in each subrule in the to-be-detected rule and a comparison symbol corresponding to the field value, a maximum value and a minimum value of a field value existing in the traffic that needs to be hit by the to-be-detected rule, to enter a value range of the field value existing in the traffic that needs to be hit by the to-be-detected rule.

[0030] For example, if the to-be-detected rule includes a subrule a and a subrule b, the subrule a and the subrule b each are a value type rule, the subrule a is that a coupon a cannot be used if a settlement amount is less than 30, the subrule b is that the coupon a cannot be used if a settlement amount exceeds 200, and a combination manner between the subrule a and the subrule b is an "and" manner, a value range of a settlement amount for which the coupon a can be used and that is included in the actually hit traffic predicted by the server is from 30 to 200.

[0031] For the enumeration type rule, the server can determine a first set and a second set based on the several subrules included in the to-be-detected rule and the combination manner between the subrules.

[0032] The first set includes a field value included in historical traffic data that needs to be hit by the to-be-detected rule and that is predicted by the server, and the second set includes a field value included in historical traffic data that cannot be hit by the to-be-detected rule and that is

predicted by the server.

[0033] For example, it is assumed that the to-be-detected rule includes a subrule c and a subrule d, the subrule c and the subrule d each are an enumeration type rule, the subrule c is that a coupon V can be used for consumption at the merchant A, the merchant B, or the merchant C, the subrule d is that the coupon V can be used for consumption at the merchant A or a merchant D, a combination manner between the subrule c and the subrule d is an "or" combination manner, and there is a merchant E and a merchant F in addition to the merchant A, the merchant B, the merchant C, and the merchant D. Field values included in the historical traffic data that needs to be hit by the to-be-detected rule and that is predicted by the server are the merchant A, the merchant B, the merchant C, and the merchant D. The field values of the four merchants form the first set. Field values included in the historical traffic data that cannot be hit by the to-be-detected rule and that is predicted by the server is the merchant E and the merchant F. The field values of the two merchants form the second set.

[0034] Subsequently, the server can detect the to-be-detected rule based on the first set, the second set, or the value range. Specific content is described in detail in subsequent step S103.

[0035] In this embodiment of this specification, the server further needs to query, from a preset database, the historical traffic data actually hit by the to-be-detected rule. The database can store full historical traffic data. The server can extract the field value included in each subrule in the to-be-detected rule and the combination manner between the subrules. Then, a query script such as a SQL query script is constructed based on the field value and the combination manner. The server can query, from the database based on the constructed query script, the historical traffic data actually hit by the to-be-detected rule.

[0036] S103: Detect the to-be-detected rule based on the historical traffic data actually hit by the to-be-detected rule and the predicted traffic that needs to be hit by the to-be-detected rule.

[0037] In actual applications, a plurality of workers may be responsible for configuring a marketing rule of the same service. However, because too many marketing rules are configured, or the workers do not notify each other of marketing rules configured by the workers, the configured marketing rules may be inevitably mismatched.

[0038] For example, if a marketing rule includes two enumeration type rules: a subrule i and a subrule j, the subrule i is that a coupon H can be used for consumption at the merchant A, the merchant B, or the merchant C, the subrule j is that the coupon H cannot be used for consumption

at the merchant A or the merchant D, and a combination manner between the subrule i and the subrule j is an "or" manner, the historical traffic data actually hit by the to-be-detected rule needs to include traffic of the merchant A, traffic of the merchant B, and traffic of the merchant C. However, it can be clearly learned that the actually hit historical traffic data of the merchant A
5 clearly conflicts with the subrule j. In this case, a mismatch is clear.

[0039] The server can detect the to-be-detected rule based on the actually hit historical traffic data and the predicted traffic that needs to be hit by the to-be-detected rule in step S102, to effectively detect the mismatch.

[0040] Specifically, if the to-be-detected rule includes an enumeration type subrule, the to-be-
10 detected rule can be detected based on the first set and/or the second set determined above. If it is determined that field values included in the historical traffic data actually hit by the to-be-detected rule are all hit in the first set, it can be determined that the to-be-detected rule does not become abnormal; or if it is determined that field values included in the historical traffic data actually hit
15 by the to-be-detected rule are partially hit in the second set, it can be determined that the to-be-detected rule is abnormal; or if it is determined that field values included in the historical traffic data actually hit by the to-be-detected rule are partially hit in the first set, but are not hit in the second set, it can be determined that the to-be-detected rule does not become abnormal. Other cases are not described herein one by one by using examples.

[0041] If the to-be-detected rule includes a value type subrule, the server can detect the to-be-
20 detected rule based on the determined value range. To be specific, the server can count field values included in the actually hit historical traffic data, and determine a fall situation of the field values within the data range. If it is determined that most or some of the field values fall within the value range, it can be determined that the to-be-detected rule does not become abnormal; or if it is determined that some or none of the field values falls within the value range, it can be determined
25 that the to-be-detected rule is abnormal.

[0042] In this embodiment of this specification, the server can input, into a preset detection model, the historical traffic data actually hit by the to-be-detected rule and reference data determined based on the predicted traffic that needs to be hit by the to-be-detected rule, to complete detection of the to-be-detected rule through the preset detection model.

[0043] The reference data mentioned herein can be data such as the first set, the second set,
30 and the value range of the field value included in the historical traffic data that needs to be hit by

the to-be-detected rule.

[0044] The detection model can combine parameter data and the historical traffic data actually hit by the to-be-detected rule, to determine whether the to-be-detected rule is abnormal.

[0045] In actual applications, there can be a plurality of cases in which the to-be-detected rule is abnormal. Therefore, in this embodiment of this specification, a plurality of detection models can be set, and different detection models can detect the to-be-detected rule based on different detection policies.

[0046] The plurality of actually set detection modules can include a full traffic drop to zero alarm model, a partial drop to zero alarm model, a list failure alarm model, a traffic amplification or reduction alarm model, and a service line-specific alarm model.

[0047] The full traffic drop to zero alarm model is mainly used to determine whether the to-be-detected rule does not hit any historical traffic data.

[0048] The partial drop to zero alarm model is mainly used to determine whether only some field values used in the to-be-detected rule are used in the historical traffic data actually hit by the to-be-detected rule. For example, it is assumed that the to-be-detected rule includes a subrule A and a subrule B, the subrule A is that a coupon can be used at the merchant A or the merchant B, the subrule B is that a coupon can be used at the merchant C or the merchant G, and a combination manner between the two subrules is an "or" relationship. In a normal case, the historical traffic data that needs to be hit by the to-be-detected rule needs to include historical traffic data of the merchant A, historical traffic data of the merchant B, historical traffic data of the merchant C, and historical traffic data of a merchant G. However, the historical traffic data actually hit by the to-be-detected rule includes only the historical traffic data of the merchant A, the historical traffic data of the merchant B, and the historical traffic data of the merchant C, and does not include the historical traffic data of the merchant G. In this case, traffic partially drops to zero.

[0049] The list failure alarm model is mainly used to determine a hit situation of the field value included in the actually hit historical traffic data in the first set and the second set, and determine, based on the hit situation, whether the to-be-detected rule has a list failure. For example, if the field value included in the actually hit historical traffic data is partially hit in the second set, it can be determined that the to-be-detected rule has a list failure.

[0050] The traffic abnormal amplification or reduction alarm model is mainly used to determine whether an amount of historical traffic data actually hit by the to-be-detected rule is too

large or too small.

[0051] The service line-specific alarm model is mainly used to detect the to-be-detected rule based on a detection policy specified based on an actual requirement of a service line including the to-be-detected rule. The service line including the to-be-detected rule can be understood as a service line for which the to-be-detected rule is deployed.

[0052] Therefore, the server can input, into all detection models, the historical traffic data actually hit by the to-be-detected rule and the reference data. Each detection model detects the to-be-detected rule based on a detection policy used by the detection model, to determine whether the to-be-detected rule has different types of abnormalities.

[0053] In this embodiment of this specification, the server can input different data into different detection models. For example, for the full traffic drop to zero alarm model, the server can input, into the full traffic drop to zero alarm model, the to-be-detected rule and the historical traffic data actually hit by the to-be-detected rule, to determine whether full traffic of the to-be-detected rule drops to zero. For another example, for the list failure alarm model, the server can input the to-be-detected rule, the historical traffic data actually hit by the to-be-detected rule, the first set, the second set, and the value range into each list failure alarm model, to determine whether there is a wrong combination manner between the subrules in the to-be-detected rule.

[0054] After a detection result for the to-be-detected rule is determined in the above-mentioned manner, the server can further input the detection result into a preset alarm model, to give an alarm based on an alarm result output by the alarm model.

[0055] A main purpose of the alarm model is to: for an abnormality of the to-be-detected rule, send alarm information to a terminal device used by the worker, to prompt the worker to repair the to-be-detected rule in a timely manner.

[0056] In other words, an alarm does not need to be given to the worker for all abnormalities of the to-be-detected rule. An alarm may not be given for some abnormalities based on an actual application requirement of a service.

[0057] Therefore, the alarm model actually reduces noise, that is, reduces excessive disturbance to the worker to a certain extent. In a specific implementation process, a plurality of alarm models can be set. Different alarm models can correspond to different services. A different alarm rule is set for each alarm model based on an actual requirement of a service of the alarm model.

[0058] For example, an amount of actually hit historical traffic data may be too small if it is set that historical traffic data from 11:00 p.m. to 3:00 a.m. needs to be obtained in a process of querying, from the database, the historical traffic data actually hit by the to-be-detected rule. However, because an amount of traffic generated in the period of time is usually relatively small, it may be considered that an abnormality that the amount of actually hit traffic is too small does not occur in this case, and therefore, no alarm needs to be given.

[0059] For another example, it is assumed that, for a service of a sales event, an amount of historical traffic data actually hit by a to-be-detected rule configured for the service may be too large. However, because too much traffic is generated during the sales event, it may be considered that an abnormality that the amount of actually hit traffic is too large does not occur in this case, and therefore, no alarm needs to be given.

[0060] Therefore, the server can determine a service including the to-be-detected rule as a target service, determine an alarm model corresponding to the target service from the alarm models, and input the detection result for the to-be-detected rule into the alarm model, to determine whether alarm information for the to-be-detected rule needs to be sent to the worker.

[0061] In this embodiment of this specification, different expansion coefficients or scaling coefficients can be set in the alarm model based on an actual requirement of a service. The expansion coefficient or scaling coefficient is mainly used to obtain a warning range through division. The alarm information needs to be sent to the worker if it is determined, based on the detection result for the to-be-detected rule, that traffic falls within the warning range; and the alarm information does not need to be sent to the worker if it is determined that traffic does not fall within the warning range.

[0062] For example, for whether the amount of historical traffic data actually hit by the to-be-detected rule is too large or too small, it is assumed that the warning range determined based on the expansion coefficient or scaling coefficient is less than 8000 pieces of historical traffic data or more than 12000 pieces of historical traffic data. If the amount of historical traffic data actually hit by the to-be-detected rule is 9000 pieces of historical traffic data, it can be determined that the historical traffic data actually hit by the to-be-detected rule does not fall within the warning range, and further, it can be determined that the alarm information is not sent to the worker.

[0063] In this embodiment of this specification, a basic warning range can be set based on an actual requirement of a service, and then, the basic warning range is expanded or scaled based on

the expansion coefficient or scaling coefficient, to determine an actually used warning range.

[0064] For example, if a basic warning range determined based on an actual requirement of a service A is zero to 10000 pieces and an expansion coefficient determined based on the actual requirement of the service A is 1.2, it is determined that a finally and actually used warning range is zero to 12000 pieces. Therefore, when an amount of historical traffic data actually hit by a to-be-detected rule of the service A falls within the warning range, it is determined that the amount of historical traffic data actually hit by the to-be-detected rule is too small.

[0065] For any alarm model, an alarm result can be output based on an alarm policy used by the alarm model. The server can aggregate alarm results output by these alarm models, and give an alarm based on an aggregation result. If any alarm model outputs an alarm result indicating that an alarm needs to be given, alarm information can be sent to the terminal device used by the worker. Certainly, for different types of abnormalities of the to-be-detected rule, alarm information can also be sent to terminal devices used by different workers. For example, if it is determined that the amount of historical traffic data actually hit by the to-be-detected rule is too large or too small, alarm information can be sent to a worker who specially processes such an abnormality; and if it is determined that the historical traffic data actually hit by the to-be-detected rule all drops to zero, alarm information can be sent to a worker who specially processes such an abnormality.

[0066] It can be learned from the above-mentioned method that, after the to-be-detected rule is obtained, the historical traffic data that can be actually hit by the to-be-detected rule can be determined based on the historical traffic data, and then whether the to-be-detected rule is mismatched is detected based on the combination manner between the subrules included in the to-be-detected rule and the historical traffic data that can be actually hit by the to-be-detected rule. In this manner, detection efficiency can be greatly improved, and time of rule detection can be reduced. In addition, rule detection accuracy can be effectively improved.

[0067] Before this, an alarm model for noise reduction is set to filter out unnecessary alarm information, to reduce unnecessary disturbance to the worker.

[0068] In addition, in the rule detection method provided in this embodiment of this specification, in addition to a marketing rule of a conventional online service, a marketing rule used for a cross-border payment service or a cross-border settlement service can be detected. For example, for the cross-border settlement service, an interest rate, a tax rate, etc. that are used can be specified in a marketing rule configured for the cross-border settlement service. Therefore, the

server can detect, in the above-mentioned method, information such as the interest rate and the tax rate that are configured in the to-be-detected rule, to determine whether the to-be-detected rule is configured properly.

[0069] To more clearly explain the rule detection method provided in this specification, a detailed example is used herein for description, as shown in FIG. 2.

[0070] FIG. 2 is a detailed flowchart of rule detection according to an embodiment of this specification.

[0071] It can be learned from FIG. 2 that a server listens to a change situation of a marketing rule table through a listener. After a new marketing rule or a modified marketing rule appears, the server sends a change message based on a rule identifier corresponding to the marketing rule, to obtain a to-be-detected rule. The server determines a first set and a second set based on a subrule in the obtained to-be-detected rule and a combination manner between subrules. In addition, a query script is constructed based on a field value included in each subrule in the to-be-detected rule and the combination manner between the subrules, to query, from a database based on the constructed query script, historical traffic data actually hit by the to-be-detected rule.

[0072] Then, the historical traffic data actually hit by the to-be-detected rule and reference data determined based on predicted traffic that needs to be hit by the to-be-detected rule are input into a preset detection model. In other words, the server inputs, into the preset detection model, the historical traffic data actually hit by the to-be-detected rule, the first set, the second set, and a value range of a field value included in the historical traffic data that needs to be hit by the to-be-detected rule. The detection model herein can be a full traffic drop to zero alarm model, a partial drop to zero alarm model, a list failure alarm model, a traffic abnormal amplification or reduction alarm model, and a service line-specific alarm model. The server further inputs, into an alarm model, a detection result that is for the to-be-detected rule and that is output by the detection model, to reduce noise of the detection result, and then aggregates all alarm information for the to-be-detected rule, to determine whether an alarm needs to be given. If yes, alarm information is pushed to a corresponding worker.

[0073] For example, it is assumed that the to-be-detected rule includes a subrule A, a subrule B, and a subrule C, the subrule A is that a coupon can be used at a merchant A or a merchant B, the subrule B is that the coupon cannot be used at the merchant B, and the subrule C is that the coupon can be used only when a payment amount is greater than 50. If subrules are combined in

a sequence of the subrule A, the subrule B, and the subrule C, a combination manner between the subrule A and the subrule B is an "or" relationship, and a combination manner between the subrule B and the subrule C is an "and" relationship, it can be determined, based on the subrule A, the subrule B, and the subrule C in the to-be-detected rule and the combination manner between the subrules, that field values included in the first set are the merchant A and the merchant B, and a field value included in the second set in the merchant B. Further, the historical traffic data that is actually hit by the to-be-detected rule and that is queried by the server from the database includes historical traffic data of the merchant A and historical traffic data of the merchant B, and a value range of a payment amount in the historical traffic data actually hit by the to-be-detected rule is 50 to 150. Based on this, the server inputs, into the preset detection model, the historical traffic data actually hit by the to-be-detected rule, the first set, the second set, the value range of the field value included in the historical traffic data that needs to be hit by the to-be-detected rule, etc. It can be learned that the value range of the payment amount in the historical traffic data actually hit by the to-be-detected rule is 50 to 150, which satisfies the value range of the field value included in the historical traffic data that needs to be hit by the to-be-detected rule. The historical traffic data actually hit by the to-be-detected rule includes the historical traffic data of the merchant B. However, in a normal case, the merchant B in the second set does not need to exist in the historical traffic data actually hit by the to-be-detected rule. It indicates that the to-be-detected rule is abnormal. Then, the server obtains the alarm information for the to-be-detected rule after inputting, into the alarm model for noise reduction, a detection result indicating that the to-be-detected rule is abnormal. Further, the server sends the alarm information for the to-be-detected rule to the worker, so that the worker corrects the to-be-detected rule based on the alarm information in a timely manner.

[0074] The specification also provides a computer-readable non-transitory storage medium, where the storage medium stores a computer program, which, when executed by a processor, can be used to perform one or more steps of one or more methods described or illustrated herein or provides functionality described or illustrated herein. Herein, the computer-readable non-transitory storage medium or media may include one or more semiconductor-based or other integrated circuits (ICs) (such, as for example, field-programmable gate arrays (FPGAs) or application-specific ICs (ASICs)), hard disk drives (HDDs), hybrid hard drives (HHDs), optical discs, optical disc drives (ODDs), magneto-optical discs, magneto-optical drives, floppy diskettes,

floppy disk drives (FDDs), magnetic tapes, solid-state drives (SSDs), RAM-drives, SECURE DIGITAL cards or drives, any other suitable computer-readable non-transitory storage media, or any suitable combination of two or more of these, where appropriate. A computer-readable non-transitory storage medium may be volatile, non-volatile, or a combination of volatile and non-volatile, where appropriate.

[0075] The specification also provides a computer system. FIG. 3 illustrates an example computer system 300. In particular embodiments, one or more computer systems 300 perform one or more steps of one or more methods described or illustrated herein. In particular embodiments, one or more computer systems 300 provide functionality described or illustrated herein. In particular embodiments, software running on one or more computer systems 300 performs one or more steps of one or more methods described or illustrated herein or provides functionality described or illustrated herein. Particular embodiments include one or more portions of one or more computer systems 300. Herein, reference to a computer system may encompass a computing device, and vice versa, where appropriate. Moreover, reference to a computer system may encompass one or more computer systems, where appropriate.

[0076] This disclosure contemplates any suitable number of computer systems 300. This disclosure contemplates computer system 300 taking any suitable physical form. As example and not by way of limitation, computer system 300 may be an embedded computer system, a system-on-chip (SOC), a single-board computer system (SBC) (such as, for example, a computer-on-module (COM) or system-on-module (SOM)), a desktop computer system, a laptop or notebook computer system, an interactive kiosk, a mainframe, a mesh of computer systems, a mobile telephone, a personal digital assistant (PDA), a server, a tablet computer system, or a combination of two or more of these. Where appropriate, computer system 300 may include one or more computer systems 300; be unitary or distributed; span multiple locations; span multiple machines; span multiple data centers; or reside in a cloud, which may include one or more cloud components in one or more networks. Where appropriate, one or more computer systems 300 may perform without substantial spatial or temporal limitation one or more steps of one or more methods described or illustrated herein. As an example and not by way of limitation, one or more computer systems 300 may perform in real time or in batch mode one or more steps of one or more methods described or illustrated herein. One or more computer systems 300 may perform at different times or at different locations one or more steps of one or more methods described or illustrated herein,

where appropriate.

[0077] In particular embodiments, computer system **300** includes a processor **302**, memory **304**, storage **306**, an input/output (I/O) interface **308**, a communication interface **310**, and a bus **312**. Although this disclosure describes and illustrates a particular computer system having a particular number of particular components in a particular arrangement, this disclosure contemplates any suitable computer system having any suitable number of any suitable components in any suitable arrangement.

[0078] In particular embodiments, processor **302** includes hardware for executing instructions, such as those making up a computer program. As an example and not by way of limitation, to execute instructions, processor **302** may retrieve (or fetch) the instructions from an internal register, an internal cache, memory **304**, or storage **306**; decode and execute them; and then write one or more results to an internal register, an internal cache, memory **304**, or storage **306**. In particular embodiments, processor **302** may include one or more internal caches for data, instructions, or addresses. This disclosure contemplates processor **302** including any suitable number of any suitable internal caches, where appropriate. As an example and not by way of limitation, processor **302** may include one or more instruction caches, one or more data caches, and one or more translation lookaside buffers (TLBs). Instructions in the instruction caches may be copies of instructions in memory **304** or storage **306**, and the instruction caches may speed up retrieval of those instructions by processor **302**. Data in the data caches may be copies of data of **80** in memory **304** or storage **306** for instructions executing at processor **302** to operate on; the results of previous instructions executed at processor **302** for access by subsequent instructions executing at processor **302** or for writing to memory **304** or storage **306**; or other suitable data. The data caches may speed up read or write operations by processor **302**. The TLBs may speed up virtual-address translation for processor **302**. In particular embodiments, processor **302** may include one or more internal registers for data, instructions, or addresses. This disclosure contemplates processor **302** including any suitable number of any suitable internal registers, where appropriate. Where appropriate, processor **302** may include one or more arithmetic logic units (ALUs); be a multi-core processor; or include one or more processors **302**. Although this disclosure describes and illustrates a particular processor, this disclosure contemplates any suitable processor.

[0079] In particular embodiments, memory **304** includes main memory for storing instructions for processor **302** to execute or data for processor **302** to operate on. As an example and not by

way of limitation, computer system **300** may load instructions from storage **306** or another source (such as, for example, another computer system **300**) to memory **304**. Processor **302** may then load the instructions from memory **304** to an internal register or internal cache. To execute the instructions, processor **302** may retrieve the instructions from the internal register or internal cache and decode them. During or after execution of the instructions, processor **302** may write one or more results (which may be intermediate or final results) to the internal register or internal cache. Processor **302** may then write one or more of those results to memory **304**. In particular embodiments, processor **302** executes only instructions in one or more internal registers or internal caches or in memory **304** (as opposed to storage **306** or elsewhere) and operates only on data in one or more internal registers or internal caches or in memory **304** (as opposed to storage **306** or elsewhere). One or more memory buses (which may each include an address bus and a data bus) may couple processor **302** to memory **304**. Bus **312** may include one or more memory buses, as described below. In particular embodiments, one or more memory management units (MMUs) reside between processor **302** and memory **304** and facilitate accesses to memory **304** requested by processor **302**. In particular embodiments, memory **304** includes random access memory (RAM). This RAM may be volatile memory, where appropriate. Where appropriate, this RAM may be dynamic RAM (DRAM) or static RAM (SRAM). Moreover, where appropriate, this RAM may be single-ported or multi-ported RAM. This disclosure contemplates any suitable RAM. Memory **304** may include one or more memories **304**, where appropriate. Although this disclosure describes and illustrates particular memory, this disclosure contemplates any suitable memory.

[0080] In particular embodiments, storage **306** includes mass storage for data or instructions. As an example and not by way of limitation, storage **306** may include a hard disk drive (HDD), a floppy disk drive, flash memory, an optical disc, a magneto-optical disc, magnetic tape, or a Universal Serial Bus (USB) drive or a combination of two or more of these. Storage **306** may include removable or non-removable (or fixed) media, where appropriate. Storage **306** may be internal or external to computer system **300**, where appropriate. In particular embodiments, storage **306** is non-volatile, solid-state memory. In particular embodiments, storage **306** includes read-only memory (ROM). Where appropriate, this ROM may be mask-programmed ROM, programmable ROM (PROM), erasable PROM (EPROM), electrically erasable PROM (EEPROM), electrically alterable ROM (EAROM), or flash memory or a combination of two or more of these. This disclosure contemplates mass storage **306** taking any suitable physical form. Storage **306** may

include one or more storage control units facilitating communication between processor **302** and storage **306**, where appropriate. Where appropriate, storage **306** may include one or more storages **306**. Although this disclosure describes and illustrates particular storage, this disclosure contemplates any suitable storage.

5 **[0081]** In particular embodiments, I/O interface **308** includes hardware, software, or both, providing one or more interfaces for communication between computer system **300** and one or more I/O devices. Computer system **300** may include one or more of these I/O devices, where appropriate. One or more of these I/O devices may enable communication between a person and computer system **300**. As an example and not by way of limitation, an I/O device may include a
10 keyboard, keypad, microphone, monitor, mouse, printer, scanner, speaker, still camera, stylus, tablet, touch screen, trackball, video camera, another suitable I/O device or a combination of two or more of these. An I/O device may include one or more sensors. This disclosure contemplates any suitable I/O devices and any suitable I/O interfaces **308** for them. Where appropriate, I/O interface **308** may include one or more device or software drivers enabling processor **302** to drive
15 one or more of these I/O devices. I/O interface **308** may include one or more I/O interfaces **308**, where appropriate. Although this disclosure describes and illustrates a particular I/O interface, this disclosure contemplates any suitable I/O interface.

[0082] In particular embodiments, communication interface **310** includes hardware, software, or both providing one or more interfaces for communication (such as, for example, packet-based
20 communication) between computer system **300** and one or more other computer systems **300** or one or more networks. As an example and not by way of limitation, communication interface **310** may include a network interface controller (NIC) or network adapter for communicating with an Ethernet or other wire-based network or a wireless NIC (WNIC) or wireless adapter for communicating with a wireless network, such as a WI-FI network. This disclosure contemplates
25 any suitable network and any suitable communication interface **310** for it. As an example and not by way of limitation, computer system **300** may communicate with an ad hoc network, a personal area network (PAN), a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), or one or more portions of the Internet or a combination of two or more of these. One or more portions of one or more of these networks may be wired or wireless. As an example,
30 computer system **300** may communicate with a wireless PAN (WPAN) (such as, for example, a BLUETOOTH WPAN), a WI-FI network, a WI-MAX network, a cellular telephone network (such

as, for example, a Global System for Mobile Communications (GSM) network), or other suitable wireless network or a combination of two or more of these. Computer system **300** may include any suitable communication interface **310** for any of these networks, where appropriate. Communication interface **310** may include one or more communication interfaces **310**, where
5 appropriate. Although this disclosure describes and illustrates a particular communication interface, this disclosure contemplates any suitable communication interface.

[0083] In particular embodiments, bus **312** includes hardware, software, or both coupling components of computer system **300** to each other. As an example and not by way of limitation, bus **312** may include an Accelerated Graphics Port (AGP) or other graphics bus, an Enhanced
10 Industry Standard Architecture (EISA) bus, a front-side bus (FSB), a HYPERTRANSPORT (HT) interconnect, an Industry Standard Architecture (ISA) bus, an INFINIBAND interconnect, a low-pin-count (LPC) bus, a memory bus, a Micro Channel Architecture (MCA) bus, a Peripheral Component Interconnect (PCI) bus, a PCI-Express (PCIe) bus, a serial advanced technology attachment (SATA) bus, a Video Electronics Standards Association local (VLB) bus, or another
15 suitable bus or a combination of two or more of these. Bus **312** may include one or more buses **312**, where appropriate. Although this disclosure describes and illustrates a particular bus, this disclosure contemplates any suitable bus or interconnect.

[0084] It should be further noted that, the terms "include", "comprise", or any other variant thereof are intended to cover a non-exclusive inclusion, so that a process, a method, a product, or
20 a device that includes a list of elements not only includes those elements but also includes other elements which are not expressly listed, or further includes elements inherent to such process, method, product or device. Without more constraints, an element preceded by "includes a ..." does not preclude the existence of additional identical elements in the process, method, product or device that includes the element.

[0085] The embodiments of this specification are described in a progressive way. For same or
25 similar parts in the embodiments, references can be made to each other. Each embodiment focuses on a difference from another embodiment. Particularly, some system embodiments are briefly described because they are basically similar to some method embodiments. For related parts, references can be made to related descriptions in some method embodiments.

[0086] The above-mentioned descriptions are merely embodiments of this specification, and
30 are not intended to limit this specification. A person skilled in the art can make various changes

and changes to this specification. Any modification, equivalent replacement, improvement, etc. made without departing from the spirit and principle of this specification shall fall within the scope of the claims in this application.

CLAIMS

What is claimed is:

1. A rule detection method, comprising:

obtaining a to-be-detected rule, wherein several subrules and a combination manner between

5 the subrules are recorded in the to-be-detected rule;

predicting, based on the several subrules and the combination manner, traffic that needs to be hit by the to-be-detected rule, and querying, from preset historical traffic data, historical traffic data actually hit by the to-be-detected rule; and

10 detecting the to-be-detected rule based on the historical traffic data actually hit by the to-be-detected rule and the predicted traffic that needs to be hit by the to-be-detected rule.

2. The method according to claim 1, wherein the querying, from preset historical traffic data, historical traffic data actually hit by the to-be-detected rule specifically comprises:

constructing a query script based on the combination manner; and

15 querying, from the preset historical traffic data based on the query script, the historical traffic data actually hit by the to-be-detected rule.

3. The method according to claim 1, wherein the subrule comprises an enumeration type rule;

the predicting, based on the several subrules and the combination manner, traffic that needs to be hit by the to-be-detected rule specifically comprises:

20 determining a first set and a second set based on the several subrules and the combination manner, wherein the first set comprises a field value comprised in predicted historical traffic data that needs to be hit by the to-be-detected rule, and the second set comprises a field value comprised in predicted historical traffic data that cannot be hit by the to-be-detected rule; and

the detecting the to-be-detected rule based on the historical traffic data actually hit by the to-be-detected rule and the predicted traffic that needs to be hit by the to-be-detected rule specifically
25 comprises:

detecting the to-be-detected rule based on a hit situation of a field value comprised in the historical traffic data actually hit by the to-be-detected rule in the first set and/or a hit situation of the field value comprised in the historical traffic data actually hit by the to-be-detected rule in the second set.

30 4. The method according to claim 1, wherein the subrule comprises a value type rule;

the predicting, based on the several subrules and the combination manner, traffic that needs to be hit by the to-be-detected rule specifically comprises:

predicting, based on the several subrules and the combination manner, a value range of a field value comprised in historical traffic data that needs to be hit by the to-be-detected rule; and

5 the detecting the to-be-detected rule based on the historical traffic data actually hit by the to-be-detected rule and the predicted traffic that needs to be hit by the to-be-detected rule specifically comprises:

detecting the to-be-detected rule based on the value range and the historical traffic data actually hit by the to-be-detected rule.

10 5. The method according to claim 1, wherein the detecting the to-be-detected rule based on the historical traffic data actually hit by the to-be-detected rule and the predicted traffic that needs to be hit by the to-be-detected rule specifically comprises:

inputting, into a preset detection model, the historical traffic data actually hit by the to-be-detected rule and reference data determined based on the predicted traffic that needs to be hit by the to-be-detected rule, to detect the to-be-detected rule based on a detection result output by the detection model.

6. The method according to claim 5, wherein the inputting, into a preset detection model, the historical traffic data actually hit by the to-be-detected rule and reference data determined based on the predicted traffic that needs to be hit by the to-be-detected rule, to detect the to-be-detected rule based on a detection result output by the detection model specifically comprises:

inputting, into all preset detection models, the historical traffic data actually hit by the to-be-detected rule and the reference data determined based on the predicted traffic that needs to be hit by the to-be-detected rule, to detect the to-be-detected rule based on a detection result output by each detection model, wherein different detection models detect the to-be-detected model based on different detection policies.

7. The method according to claim 1, wherein the method further comprises:

inputting a detection result for the to-be-detected rule into a preset alarm model, to give an alarm based on an alarm result output by the alarm model.

8. The method according to claim 7, wherein the inputting a detection result for the to-be-detected rule into a preset alarm model, to give an alarm based on an alarm result output by the alarm model specifically comprises:

determining a service comprising the to-be-detected rule as a target service; and

inputting the detection result for the to-be-detected rule into an alarm model corresponding to the target service, to give an alarm based on an alarm result output by the alarm model corresponding to the target service.

5 9. A computer system, wherein the computer system comprises a memory, a processor, and a computer program that is stored in the memory and that is capable of running on the processor, and when executing the program, the processor implements the following steps:

obtaining a to-be-detected rule, wherein several subrules and a combination manner between the subrules are recorded in the to-be-detected rule;

10 predicting, based on the several subrules and the combination manner, traffic that needs to be hit by the to-be-detected rule, and querying, from preset historical traffic data, historical traffic data actually hit by the to-be-detected rule; and

detecting the to-be-detected rule based on the historical traffic data actually hit by the to-be-detected rule and the predicted traffic that needs to be hit by the to-be-detected rule.

15 10. The computer system according to claim 9, wherein the querying, from preset historical traffic data, historical traffic data actually hit by the to-be-detected rule specifically comprises:

constructing a query script based on the combination manner; and

querying, from the preset historical traffic data based on the query script, the historical traffic data actually hit by the to-be-detected rule.

20 11. The computer system according to claim 9, wherein the subrule comprises an enumeration type rule;

the predicting, based on the several subrules and the combination manner, traffic that needs to be hit by the to-be-detected rule specifically comprises:

25 determining a first set and a second set based on the several subrules and the combination manner, wherein the first set comprises a field value comprised in predicted historical traffic data that needs to be hit by the to-be-detected rule, and the second set comprises a field value comprised in predicted historical traffic data that cannot be hit by the to-be-detected rule; and

the detecting the to-be-detected rule based on the historical traffic data actually hit by the to-be-detected rule and the predicted traffic that needs to be hit by the to-be-detected rule specifically
30 comprises:

detecting the to-be-detected rule based on a hit situation of a field value comprised in the

historical traffic data actually hit by the to-be-detected rule in the first set and/or a hit situation of the field value comprised in the historical traffic data actually hit by the to-be-detected rule in the second set.

12. The computer system according to claim 9, wherein the subrule comprises a value type
5 rule;

the predicting, based on the several subrules and the combination manner, traffic that needs to be hit by the to-be-detected rule specifically comprises:

predicting, based on the several subrules and the combination manner, a value range of a field value comprised in historical traffic data that needs to be hit by the to-be-detected rule; and

10 the detecting the to-be-detected rule based on the historical traffic data actually hit by the to-be-detected rule and the predicted traffic that needs to be hit by the to-be-detected rule specifically comprises:

detecting the to-be-detected rule based on the value range and the historical traffic data actually hit by the to-be-detected rule.

15 13. The computer system according to claim 9, wherein the detecting the to-be-detected rule based on the historical traffic data actually hit by the to-be-detected rule and the predicted traffic that needs to be hit by the to-be-detected rule specifically comprises:

inputting, into a preset detection model, the historical traffic data actually hit by the to-be-detected rule and reference data determined based on the predicted traffic that needs to be hit by
20 the to-be-detected rule, to detect the to-be-detected rule based on a detection result output by the detection model.

14. The computer system according to claim 13, wherein the inputting, into a preset detection model, the historical traffic data actually hit by the to-be-detected rule and reference data determined based on the predicted traffic that needs to be hit by the to-be-detected rule, to detect
25 the to-be-detected rule based on a detection result output by the detection model specifically comprises:

inputting, into all preset detection models, the historical traffic data actually hit by the to-be-detected rule and the reference data determined based on the predicted traffic that needs to be hit by the to-be-detected rule, to detect the to-be-detected rule based on a detection result output by
30 each detection model, wherein different detection models detect the to-be-detected model based on different detection policies.

15. The computer system according to claim 9, wherein the computer system is further configured to input a detection result for the to-be-detected rule into a preset alarm model, to give an alarm based on an alarm result output by the alarm model.

16. The computer system according to claim 15, wherein the inputting a detection result for
5 the to-be-detected rule into a preset alarm model, to give an alarm based on an alarm result output by the alarm model specifically comprises:

determining a service comprising the to-be-detected rule as a target service; and

inputting the detection result for the to-be-detected rule into an alarm model corresponding
to the target service, to give an alarm based on an alarm result output by the alarm model
10 corresponding to the target service.

17. A computer-readable storage medium, wherein the storage medium stores a computer program, and when the computer program is executed by a processor, the method according to any one of claims 1 to 8 is implemented.