RISK IDENTIFICATION METHOD, CLIENT DEVICE, AND RISK IDENTIFICATION SYSTEM

TECHNICAL FIELD

[0001] The present application relates to the field of computer technologies, and in particular, to a risk identification method, a client device, and a risk identification system.

BACKGROUND

[0002] With the rapid development of the Internet financial industry, financial services, products, and transaction types are increasing, which also leads to higher service risks. Therefore, Internet service risks need to be controlled.

[0003] In an existing risk control system, a centralized server cluster processing method is usually used, and risk identification and control are performed after a server device receives data. In this method, numerous server resources are consumed for data storage, data calculation, and risk analysis, and calculation costs and hardware costs of a server cluster are huge too.

SUMMARY

[0004] An implementation of the present application provides a risk identification method, to reduce server device costs in the existing technology, consumption of the server device, and storage costs of risk identification and control.

[0005] An implementation of the present application further provides a client device, to reduce server device costs in the existing technology, consumption of the server device, and storage costs of risk identification and control.

[0006] An implementation of the present application further provides a risk identification system, to reduce device server device costs in the existing technology, consumption of the server device, and storage costs and calculation analysis costs of risk identification and control.

[0007] An implementation of the present application further provides a second risk identification system, to reduce device sever devices costs in the existing technology, consumption of the server device, and storage costs of risk identification and control.

[0008] An implementation of the present application further provides a third risk identification system, to reduce device server device costs in the existing technology, consumption of the server device, and storage costs of risk identification and control.

[0009] The following technical solutions are used in the implementations of the present application:

[0010] An implementation of the present application provides a risk identification method, including: receiving, by a client device, a risk identification request sent based on a service operation request, where the service operation request includes service data; obtaining, by the client device, service data corresponding to the risk identification request; and determining whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or service indicator data stored in the client device, where the service indicator data is determined based on the service data.

[0011] An implementation of the present application further provides a client device, including: a request receiving module, configured to receive a risk identification request sent based on a service operation request, where the service operation request includes service data; a data acquisition module, configured to obtain service data corresponding to the risk identification request; an indicator storage module, configured to store service indicator data determined based on the service data; and a risk identification module, configured to determine whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or the service indicator data.

[0012] An implementation of the present application further provides a risk identification system, including: a client device, configured to receive a risk identification request sent based on a service operation request, where the service operation request includes service data; obtain service data corresponding to the risk identification request; and determine whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or service indicator data stored in the client device, where the service indicator data is determined based on the service data; and a server device, configured to send

the risk identification rule or the risk identification model to the client device by using a data channel, where the risk identification rule or the risk identification model is used to determine whether the service operation request is risky; and receive the service indicator data stored in the client device by using the data channel.

[0013] An implementation of the present application further provides a second risk identification system, including: a client device, configured to receive a risk identification request sent based on a service operation request, where the service operation request includes service data; obtain service data corresponding to the risk identification request; and receive, by using a data channel, a result that is determined by the server device, of whether the service operation request is risky; and a server device, configured to receive service indicator data stored in the client device by using the data channel; determine whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or the service indicator data stored in the client device, where the service indicator data is determined based on the service data; and send, to the client device by using the data channel, the result that is determined by the server device, of whether the service operation request is risky.

[0014] An implementation of the present application further provides a third risk identification system, including: a client device, configured to receive a risk identification request sent based on a service operation request, where the service operation request includes service data; obtain service data corresponding to the risk identification request; and receive, by using a data channel, a result that is determined by a cloud risk identification device, of whether the service operation request is risky; the cloud risk identification device, configured to determine whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or service indicator data stored in the client device, where the service indicator data is determined based on the service data; and a server device, configured to receive the service indicator data stored in the client device by using the data channel; send the service indicator data to the cloud risk identification device; and send the risk identification rule or the risk identification model to the cloud risk identification device.

[0015] At least one of the previously described technical solutions adopted in the implementations of the present application can achieve the following beneficial effects:

[0016] In the implementations of the present application, when data used for risk identification is being stored, the service indicator data is determined based on the raw service data, and the service indicator data is stored in the client device. As the service indicator data used for risk identification is stored in the client device, storage costs of the server device can be reduced. In addition, as massive raw service data is converted into the service indicator data for storage, the overall storage costs are reduced. Even if the service indicator data is synchronized to the server device for storage, storage costs of the server device are still lower than those in the existing technology.

BRIEF DESCRIPTION OF DRAWINGS

[0017] The accompanying drawings described here are intended to provide a further understanding of the present application, and constitute a part of the present application. The illustrative implementations of the present application and descriptions thereof are intended to describe the present application, and do not constitute limitations on the present application. In the accompanying drawings:

[0018] FIG. 1 shows a typical system to which a risk identification method is applied, according to the present application;

[0019] FIG. 2 is a schematic flowchart illustrating a risk identification method, according to an implementation of the present application;

[0020] FIG. 3 is a schematic structural diagram illustrating a risk identification device, according to an implementation of the present application;

[0021] FIG. 4 is a schematic structural diagram illustrating a second risk identification device, according to an implementation of the present application;

[0022] FIG. 5 is an architectural diagram illustrating a risk identification system, according to an implementation of the present application;

[0023] FIG. 6 is an architectural diagram illustrating a second risk identification system, according to an implementation of the present application;

[0024] FIG. 7 is an architectural diagram illustrating a third risk identification system, according to an implementation of the present application; and

[0025] FIG. 8 is an architectural diagram illustrating a fourth risk identification system, according to an implementation of the present application.

DESCRIPTION OF IMPLEMENTATIONS

[0026] To make the objectives, technical solutions, and advantages of the present application clearer, the following clearly and comprehensively describes the technical solutions of the present application with reference to the implementations of the present application and corresponding accompanying drawings. Apparently, the described implementations are merely some but not all of the implementations of the present application. All other implementations obtained by a person of ordinary skill in the art based on the implementations of the present application without creative efforts shall fall within the protection scope of the present application.

[0027] The technical solutions provided in the implementations of the present application are described in detail below with reference to the accompanying drawings.

[0028] FIG. 1 shows a typical system in practice, according to an implementation of the present application. The system includes a client device and a server device, and data is synchronized between the client device and the server device by using a data channel.

[0029] Referring to FIG. 2, a risk identification method provided in this application includes the following steps.

[0030] S101: A client device receives a risk identification request sent based on a service operation request, where the service operation request includes service data.

[0031] S102: The client device obtains service data corresponding to the risk identification request.

[0032] In actual applications, the service operation request is usually sent by a user. After the client receives the service operation request, the client starts a risk identification program to send the risk identification request, if the service operation request belongs to a high risk operation type. The client device can obtain the service data corresponding to the risk identification request based on the risk identification request. To be specific, the client device extracts the service data from the service operation request associated with the risk identification request. For example, the user sends a payment request, and the payment request is a high risk operation type. Therefore, the client device starts the risk identification program to extract service data of a payment service from the payment request, such as login information of the user, hardware environment information and/or software environment information of

the client device used by the user, payment account information and/or password information, a current payment amount, and payee information.

[0033] In the existing technology, the raw service data usually needs to be sent to a server device and stored in the server device for risk identification and control. In this implementation of the present application, risk identification can be implemented without storing the raw service data in the server device. Certainly, in consideration of data backup, the raw service data can be sent to the server device for storage or can be stored in the client device if the service operation request is completed, a network is idle, or storage space of the server device is sufficient. Technical effects of the present application are not affected.

[0034] S103: Determine whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or service indicator data stored in the client device, where the service indicator data is determined based on the service data.

[0035] In the process of performing step S103 to determine whether the service operation request is risky, the service indicator data needs to be calculated based on the service data and analysis and determining need to be performed based on the service data and/or the service indicator data. The previously described calculation step can be performed by the client device or the server device, and the analysis and determining step can be performed by the client device or the server device. Different calculation methods and content in the calculation step can be performed by the client device or the server device, or can be partially performed by the client and partially performed by the server device. Different content analysis and determining processes in the analysis and determining step can be performed by the client device or the server device, or can be partially performed by the client and partially performed by the server device. Implementations are not limited in the present application. For example, in an implementation shown in FIG. 8, data storage and calculation can be performed by the client device, and analysis and processing are performed by the server device.

[0036] A series of statistical calculations can be performed based on the service data to obtain the service indicator data. The service indicator data can represent a historical status of the service operation request corresponding to the service data within a specified time period. A series of statistical values of data generated by the service operation request in a predetermined time window can be calculated. For

example, the statistics values can be a count value (COUNT), a sum value (SUM), a first value (FIRST), a last value (LAST), a distinction value (DISTINCT), an average value (AVG), a standard deviation (STDEV), a variance (VAR), a maximum value (MAX), and/or a minimum value (MIN) of an amount or time, and the time window can be one hour, twelve hours, or seven days. For example, calculating "COUNT, successful payment within one hour" means that the number of successful payments times by the client device and the account within the last hour is calculated. Information about the client device and information about the payment account can be from the service data extracted from the service operation request. For another example, calculating "SUM, payment amount within 24 hours" means that the total amount of successful payments by the client device and the account within the last 24 hours is calculated. Information about the client device, information about the payment account, and an amount of each successful payment within 24 hours (related to the service operation request within 24 hours) can be from the service data extracted from the service operation request. A person skilled in the art can understand that, in the first method, the raw service data in the predetermined time window can be stored, and the corresponding raw service data is used to calculate the service indicator data. In the second method, the raw service data is not stored, and when new service data is generated, the service indicator data is recalculated based on the new service data, and the service indicator data is updated. For example, a value of the "COUNT, successful payment within one hour" can be updated over time during each successful payment. In terms of reducing storage costs, the second method is better.

[0037] A series of feature calculation can be performed based on the service data to obtain the service indicator data. A frequency feature of the service operation request and/or a running environment feature of the client device can be calculated, and the running environment feature of the client device can include a running software environment and a running hardware environment of the client device. For example, a frequency of performing a payment operation by the client device can be calculated (alternatively, the number of payment operations by the client device in the predetermined time window can be calculated), a frequency of performing a payment operation by an account in the client device can be calculated, and an attenuation degree of a battery of the client device can be calculated.

[0038] It is worthwhile to note that the service indicator data is calculated based on the service data. During specific implementation, the calculation process can be

performed by the client device or the server device. If the service indicator data is calculated by the client device, the client device obtains the service indicator data through calculation based on the service data. Further, the client device reports the calculated service indicator data to the server device by using a data channel. Correspondingly, the server device receives, by using the data channel, the service indicator data calculated by the client device based on the service data. Calculation is performed by the client device to reduce calculation costs of the server device. After calculation is completed by the client device, the service indicator data is stored in the client device, and can be reported to the server device by using the data channel, to synchronize the service indicator data between the server device and the client device. If the service indicator data is calculated by the server device, the client device first reports the service data to the server device by using the data channel, and then the client device receives, by using the data channel, the service indicator data calculated by the server device based on the service data. Correspondingly, the server device receives, by using the data channel, the service data reported by the client device. The service device calculates the service indicator data based on the service data, and then sends the service indicator data to the client device by using the data channel. In this method, the client device does not need to calculate the service indicator data, so that a design of the client device can be simplified. Also, the client device can receive, by using the data channel, the service indicator data calculated by the server device, to synchronize the service indicator data between the client device and the server device.

[0039] When performing step S103 of determining whether the service operation request is risky based on the risk identification rule or the risk identification model, and the service data and/or the service indicator data stored in the client device, the client device can directly perform logic analysis and/or probability analysis on the service data and/or the service indicator data, and determine whether the service operation request is risky based on a result of the logic analysis and/or the probability analysis. In this method, the client device can detect an abnormal service operation request in time through analysis, to better identify, prevent, and control risks. Details are as follows:

[0040] The client device performs logic analysis on the service data and/or the service indicator data based on the risk identification rule, and determines whether the service operation request is risky based on a result of the logic analysis; or the client device performs logic analysis and/or probability analysis on the service data and/or

the service indicator data based on the risk identification model, and determines whether the service operation request is risky based on a result of the logic analysis and/or the probability analysis.

[0041] In addition, optionally, the client device can receive, by using a data channel, a result of logic analysis and/or probability analysis performed by the server device on the service data and/or the service indicator data, and determines whether the service operation request is risky based on the result of the logic analysis and/or the probability analysis. If there is no information about the service data or the service indicator data in the server device, before receiving the analysis result of the server device, the client device further needs to send the service data and/or the service indicator data to the server device by using the data channel. The method of sending the data to the server device for analysis can simplify a design of the client device, and the client device can identify risks based on the analysis result of the server device. Details are as follows:

[0042] The client device receives, based on the risk identification rule and by using a data channel, a result of logic analysis performed by the server device on the service data and/or the service indicator data, and determines whether the service operation request is risky based on a result of the logic analysis; or the client device receives, based on the risk identification model and by using a data channel, a result of logic analysis and/or probability analysis performed by the server device on the service data and/or the service indicator data, and determines whether the service operation request is risky based on a result of the logic analysis and/or the probability analysis.

[0043] Probability analysis can be performed on the service data and/or the service indicator data by using the risk identification model to obtain a risk probability, and whether there is a risk can be determined based on the risk probability.

[0044] Logical analysis can be performed on the service data and/or the service indicator data by using the service data and/or the service indicator data, and the predetermined risk identification rule or the risk identification model. The risk identification rule can be understood as a logical expression, and a status value (true or false) of the logical expression corresponds to a result of whether there is a risk. The service data and/or the service indicator data can be understood as specific values in the previously described logical expression. Example 1: The risk identification rule is predetermined as: (current amount + daily accumulated amount < 200) AND

(accumulated payment amount of seven days > 1w): Risk-free

[0045] In the risk identification rule, a value of the "current amount" is from the service operation request that is used for determining whether there is a risk, that is, the current service data; values of the "daily accumulated amount" and the "accumulated payment amount of seven days" are from the service indicator data, and both the service data and the service indicator data are used for analysis in this rule. Output of the logical expression (current amount + daily accumulated amount < 200) AND (accumulated payment amount of seven days > 1w)) is a determined status value "true" or "false". If the output of the logical expression is "true" in this rule, it indicates that the service operation request is risk-free.

[0046] Example 2: The risk identification rule is predetermined as: (current amount > 1w) OR (current account is not in the risk-free list): Risky

[0047] In the above risk identification rule, a value of the "current sum" is from the current service data, and information about the "current account" is from the current service data. Therefore, logic analysis is performed based on only the service data in this rule. When it is determined (the current account is not in the risk-free list), the "risk-free list" needs to be known in addition to the "current account". Detailed descriptions will be provided when describing configuration data sent by the server device by using the data channel below.

[0048] Example 3: The risk identification rule is predetermined as: (daily accumulated amount > 2000) AND (payment times within one hour > 3) AND (variance of a payment amount within one hour: < 0.3): Risky

[0049] In the above risk identification rule, values of the "daily accumulated amount", the "payment times within one hour", and the "variance of a payment amount within one hour" are from the service indicator data. Logic analysis is performed based on only the service indicator data in this rule. When output of the logical expression in this rule is "true", it indicates that the service operation request is risky.

[0050] In this implementation, the risk identification rule, the risk-free list, and/or the risk identification model that are used when logical analysis or probability analysis is performed to determine whether there is a risk, can all be the configuration data, and service indicator update data can also belongs to the configuration data. The configuration data can be sent by the server device by using the data channel, and the client device receives and stores the configuration data. The configuration data is

combined with the service data and/or the service indicator data, to determine whether the service operation request is risky. The configuration data can also be obtained by the client device through training. In a preferred implementation, data is synchronized between the client device and the server device periodically or sporadically. Data such as the service indicator data, the service indicator update data, the risk identification rule, the risk-free list, and the risk identification model are stored in both the server device and the client device. During specific implementation, a network communication mode PUSH can be used, that is, a communication mode in which the server device sends a notification to the client device. In this case, the server device actively instructs the client device to update data stored in the client device when detecting that the data needs to be updated. The data here includes various types of data that need to be synchronized. Alternatively, a network communication mode PULL can be used, that is, a communication mode in which the client device obtains data from the server device. In this case, when the client device receives a notification from the server device or local data of the client needs to be updated, the client actively obtains the updated data from the server device.

[0051] In the previously described implementations and the best combinations, after it is determined whether the service operation request is risky, the method in the present application further includes the following: determining a processing method for the service operation request based on a risk identification result of whether the service operation request is risky. There are multiple processing methods for the service operation request. The client device directly executes the service operation request if the service operation request is risk-free. An operation permission of the service operation request needs to be restricted if the service operation request is risky. The client directly restricts the operation permission of the service operation request if the service operation request is risky. Alternatively, the client receives, by using the data channel, a request sent by the server device that is used for restricting the operation permission of the service operation request if the service operation request is risky, and further restricts the operation permission of the service operation request. Further, after the operation permission of the service operation request is restricted, the restriction on the operation permission of the service operation request can be removed after a risk is excluded. The restriction on the operation permission of the service operation request is removed if restriction removal verification information fed back for a restriction removal verification request is received, and the restriction

removal verification request can be sent by the client device or the server device.

[0052] The present application further provides a client device. Referring to FIG. 3, the client device includes the following: a request receiving module 101, configured to receive a risk identification request sent based on a service operation request, where the service operation request includes service data; a data acquisition module 102, configured to obtain service data corresponding to the risk identification request; an indicator storage module 103, configured to store service indicator data determined based on the service data; and a risk identification module 105, configured to determine whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or the service indicator data.

[0053] Preferably, the client device can further include the following: a configuration data storage module 104, configured to receive and store configuration data synchronized by using a data channel, where the configuration data is combined with the service data and/or the service indicator data, to determine whether the service operation request is risky.

[0054] Further, the configuration data storage module 104 includes the following: a rule storage unit 1041, configured to store the risk identification rule that is used to determine whether the service operation request is risky; a list storage unit 1042, configured to store information associated with hardware environment information and software environment information of the client device and/or account information in the client device; and a model storage unit 1043, configured to store the risk identification model that is used to determine whether the service operation request is risky.

[0055] Preferably, the risk identification module 105 can include the following: a calculation unit 1051, configured to calculate the service indicator data based on the service data.

[0056] Preferably, the risk identification module 105 can include the following: an analysis unit 1052, configured to perform logic analysis and/or probability analysis on the service data and/or the service indicator data based on the risk identification rule or the risk identification model, and determine whether the service operation request is risky based on a result of the logic analysis and/or the probability analysis.

[0057] Preferably, the client device can further include the following: a processing module 107, configured to determine a processing method for the service operation

request based on a risk identification result of whether the service operation request is risky.

[0058] FIG. 4 is a schematic structural diagram illustrating a client device, according to a preferred implementation. The device includes a request receiving module 101, a data acquisition module 102, an indicator storage module 103, a configuration data storage module 104, a risk identification module 105, and a processing module 107. The processing module 107 depends on the risk identification module 105. The risk identification module 105 depends on the indicator storage module 102 and the configuration data storage module 104. The indicator storage module 102 depends on the data acquisition module 101. The configuration data storage module 104 depends on configuration data sent by a server device that is obtained by using a data channel. The risk identification module 105 includes a calculation unit 1051 and an analysis unit 1052. The calculation unit 1051 can include a statistical calculation subunit and a feature calculation subunit, and the statistical calculation subunit and the feature calculation subunit are respectively configured to perform statistical calculation and feature calculation. The analysis unit 1052 can include a probability analysis subunit and a logic analysis subunit, and the probability analysis subunit and the logic analysis subunit are respectively configured to perform probability analysis and logic analysis. Principles and implementation methods of the statistical calculation, the feature calculation, the probability analysis, and the logic analysis are described in detail in the previously described implementations of the risk identification method, and details are omitted here for simplicity. In this implementation, raw service data based acquisition, storage, calculation, and analysis are all performed by the client device to implement data-based risk prevention and control and reduce the times of interaction with the server device and a data volume, thereby reducing costs of risk identification and processing by the server device. In addition, because data calculation and analysis are both performed by the client device, a user can perceive and process an abnormal service operation in time, to implement risk prevention and control. Furthermore, the client device performs data analysis to determine whether there is a risk, thereby facilitating calculation of complex data. The configuration data such as service indicator update data, a risk identification rule, a risk-free list, and a risk identification model are obtained from the server device by using the data channel, so that an identification capability of the client device can be better ensured during calculation and analysis.

[0059] FIG. 5 shows a risk identification system, according to an implementation of the present application. The risk identification system includes a client device and a server device.

[0060] The client device includes the following: a request receiving module, configured to receive a risk identification request sent based on a service operation request, where the service operation request includes service data; a data acquisition module, configured to obtain service data corresponding to the risk identification request; an indicator storage module, configured to store service indicator data determined based on the service data; and a risk identification module, configured to determine whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or the service indicator data stored in the client device.

[0061] The server device includes the following: a sending module, configured to send the risk identification rule or the risk identification model to the client device by using a data channel, where the risk identification rule or the risk identification model is used to determine whether the service operation request is risky; and a receiving module, configured to receive the service indicator data stored in the client device by using the data channel.

[0062] In the schematic block diagram shown in FIG. 5, the client device completes a series of operations such as obtaining, calculating, storing, analyzing, and processing the service data. In FIG. 5, a storage engine is configured to store data, including the service indicator data (stored in the indicator storage module) calculated by the client device based on the service data, and a rule (corresponding to the previous risk identification rule and stored in the rule storage module), a list (corresponding to the previous risk-free list and stored in the list storage module), and a model (corresponding to the previous risk identification model and stored in the model storage module) that are obtained by the client device from a management back end (corresponding to the server device) by using the data channel. After obtaining the service data, the client device starts a calculation engine to perform statistical calculation and feature calculation, stores a calculation result such as the service indicator data in the indicator storage module, and synchronizes the service indicator data to the management back end by using the data channel. An analysis engine performs logic analysis and/or probability analysis on the service data and/or the service indicator data based on the risk identification rule or the risk identification

model, and determines whether the service operation request is risky based on an analysis result. Further, a processing engine can process the service operation request based on a risk identification result, including freezing processing (corresponding to restricting the operation permission of the service operation request) and restriction removal processing (corresponding to removing the restriction on the operation permission of the service operation request).

[0063] FIG. 6 shows a second risk identification system, according to an implementation of the present application. The second risk identification system includes a client device and a server device.

[0064] The client device includes the following: a request receiving module, configured to receive a risk identification request sent based on a service operation request, where the service operation request includes service data; a data acquisition module, configured to obtain service data corresponding to the risk identification request; an indicator storage module, configured to store service indicator data determined based on the service data; and a result receiving module, configured to receive, by using a data channel, a result that is determined by the server device, of whether the service operation request is risky.

[0065] The server device includes the following: a receiving module, configured to receive the service indicator data stored in the client device by using the data channel; a risk identification module, configured to determine whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or the service indicator data stored in the client device, where the service indicator data is determined based on the service data; and a sending module, configured to send, to the client device by using the data channel, the result that is determined by the server device, of whether the service operation request is risky.

[0066] In the implementation shown in FIG. 6, the client device includes only a storage engine, and a calculation engine, an analysis engine, and a processing engine are all implemented by the server device, to simplify the client device and reduce a size of a software development kit (SDK) of the client device, thereby reducing integration costs and relieving a problem such as an excessively large installation package.

[0067] FIG. 7 shows a third risk identification system, according to an implementation of the present application, including a client device, a cloud risk

identification device, and a server device.

[0068] The client device includes the following: a request receiving module, configured to receive a risk identification request sent based on a service operation request, where the service operation request includes service data; a data acquisition module, configured to obtain service data corresponding to the risk identification request; an indicator storage module, configured to store service indicator data determined based on the service data; and a result receiving module, configured to receive, by using a data channel, a result that is determined by the cloud risk identification device, of whether the service operation request is risky.

[0069] The cloud risk identification device includes the following: a risk identification module, configured to determine whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or the service indicator data stored in the client device, where the service indicator data is determined based on the service data.

[0070] The server device includes the following: a receiving module, configured to receive the service indicator data stored in the client device by using the data channel; and a sending module, configured to send the service indicator data to the cloud risk identification device, and send the risk identification rule or the risk identification model to the cloud risk identification device.

[0071] In the implementation shown in FIG. 7, a server end is divided into the cloud risk identification device and the server device, to further reduce calculation and analysis burden of the server device and reduce costs of the server end.

[0072] A person skilled in the art should understand that an implementation of the present application can be provided as a method, a system, or a computer program product. Therefore, the present application can use a form of hardware only implementations, software only implementations, or implementations with a combination of software and hardware. Moreover, the present application can use a form of a computer program product that is implemented on one or more computer-usable storage media (including but not limited to a disk memory, a CD-ROM, an optical memory, etc.) that include computer-usable program code.

[0073] The present application is described with reference to the flowcharts and/or block diagrams of the method, the device (system), and the computer program product according to the implementations of the present application. It should be understood that computer program instructions can be used to implement each process

and/or each block in the flowcharts and/or the block diagrams and a combination of a process and/or a block in the flowcharts and/or the block diagrams. These computer program instructions can be provided for a general-purpose computer, a dedicated-purpose computer, an embedded processor, or a processor of another programmable data processing device to generate a machine, so that the instructions executed by the computer or the processor of the another programmable data processing device generate an apparatus for implementing a specific function in one or more flows in the flowcharts and/or in one or more blocks in the block diagrams.

[0074] These computer program instructions can be stored in a computer readable memory that can instruct the computer or the another programmable data processing device to work in a specific way, so that the instructions stored in the computer readable memory generate an artifact that includes an instruction apparatus. The instruction apparatus implements a specific function in one or more flows in the flowcharts and/or in one or more blocks in the block diagrams.

[0075] These computer program instructions can be loaded onto the computer or the another programmable data processing device, so that a series of operations and steps are performed on the computer or the another programmable device, thereby generating computer-implemented processing. Therefore, the instructions executed on the computer or the another programmable device provide steps for implementing a specific function in one or more flows in the flowcharts and/or in one or more blocks in the block diagrams.

[0076] In a typical configuration, a computing device includes one or more processors (CPU), an input/output interface, a network interface, and a memory.

[0077] The memory can include a non-persistent memory, a random access memory (RAM), a non-volatile memory, and/or another form in a computer readable medium, for example, a read-only memory (ROM) or a flash memory (flash RAM). The memory is an example of the computer readable medium.

[0078] The computer readable medium includes persistent, non-persistent, movable, and unmovable media that can implement information storage by using any method or technology. Information can be a computer readable instruction, a data structure, a program module, or other data. An example of a computer storage medium includes but is not limited to a phase-change random access memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), another type of random access memory (RAM), a read-only memory

(ROM), an electrically erasable programmable read-only memory (EEPROM), a flash memory or another memory technology, a compact disc read-only memory (CD-ROM), a digital versatile disc (DVD) or another optical storage, a cassette magnetic tape, a tape and disk storage or another magnetic storage device or any other non-transmission media that can be configured to store information that a computing device can access. As described in the present application, the computer readable medium does not include computer readable transitory media such as a modulated data signal and a carrier.

[0079] It is worthwhile to further note that the terms "include", "includes", or their any other variant is intended to cover a non-exclusive inclusion, so that a process, a method, a merchandise, or 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, article, or device. An element preceded by "includes a ..." does not, without more constraints, preclude the existence of additional identical elements in the process, method, merchandise, or device that includes the element.

[0080] A person skilled in the art should understand that an implementation of the present application can be provided as a method, a system, or a computer program product. Therefore, the present application can use a form of hardware only implementations, software only implementations, or implementations with a combination of software and hardware. Moreover, the present application can use a form of a computer program product that is implemented on one or more computer-usable storage media (including but not limited to a disk memory, a CD-ROM, an optical memory, etc.) that include computer-usable program code.

[0081] The previous descriptions are merely implementations of the present application, and are not intended to limit the present application. For a person skilled in the art, the present application can have various modifications and changes. Any modifications, equivalent substitutions, improvements, etc. made in the spirit and principle of the present application shall fall in the scope of the claims in the present application.

CLAIMS

What is claimed is:

1. A risk identification method, comprising the following:

receiving, by a client device, a risk identification request sent based on a service operation request, wherein the service operation request comprises service data;

obtaining, by the client device, service data corresponding to the risk identification request; and

determining whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or service indicator data stored in the client device, wherein the service indicator data is determined based on the service data.

2. The method according to claim 1, wherein that the service indicator data is determined based on the service data comprises the following:

calculating, by the client device, the service indicator data based on the service data.

3. The method according to claim 2, wherein after the calculating, by the client device, the service indicator data based on the service data, the method further comprises the following:

reporting, by the client device, the calculated service indicator data to a server device by using a data channel.

4. The method according to claim 1, wherein that the service indicator data is determined based on the service data comprises the following:

receiving, by a server device by using a data channel, the service indicator data calculated by the client device based on the service data.

5. The method according to claim 1, wherein that the service indicator data is determined based on the service data comprises the following:

reporting, by the client device, the service data to a server device by using a data channel; and

receiving, by the client device by using the data channel, the service indicator data calculated by the server device based on the service data.

6. The method according to claim 1, wherein that the service indicator data is determined based on the service data comprises the following:

receiving, by a server device by using a data channel, the service data reported by the client device;

calculating, by the server device, the service indicator data based on the service data; and

sending, by the server device, the service indicator data to the client device by using the data channel.

7. The method according to any one of claims 1 to 6, wherein the service indicator data comprises a count value, a sum value, a first value, a last value, a distinction value, an average value, a standard deviation, a variance, a maximum value, and/or a minimum value of data generated by the service operation request in a predetermined time window.

8. The method according to any one of claims 1 to 6, wherein the service indicator data comprises a frequency feature of the service operation request and/or a running environment feature of the client device.

9. The method according to claim 1, wherein the determining whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or service indicator data stored in the client device comprises the following:

performing, by the client device, logic analysis on the service data and/or the service indicator data based on the risk identification rule, and determining whether the service operation request is risky based on a result of the logic analysis; or

performing, by the client device, logic analysis and/or probability analysis on the service data and/or the service indicator data based on the risk identification model, and determining whether the service operation request is risky based on a result of the logic analysis and/or the probability analysis.

10. The method according to claim 1, wherein the determining whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or service indicator data stored in the client device comprises the following:

receiving, by the client device by using a data channel, a result of logic analysis performed by a server device on the service data and/or the service indicator data based on the risk identification rule, and determining whether the service operation request is risky based on a result of the logic analysis; or

receiving, by the client device by using a data channel, a result of logic analysis

and/or probability analysis performed by a server device on the service data and/or the service indicator data based on the risk identification model, and determining whether the service operation request is risky based on a result of the logic analysis and/or the probability analysis.

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

receiving and storing, by the client device, configuration data sent by a server device by using a data channel, wherein the configuration data is combined with the service data and/or the service indicator data, to determine whether the service operation request is risky.

12. The method according to claim 11, wherein the configuration data comprises service indicator update data, the risk identification rule, a risk-free list, and/or the risk identification model.

13. The method according to claim 1, wherein after the determining whether the service operation request is risky, the method further comprises the following:

determining a processing method for the service operation request based on a risk identification result of whether the service operation request is risky.

14. The method according to claim 13, wherein the determining a processing method for the service operation request based on a risk identification result of whether the service operation request is risky comprises the following:

restricting, by the client device, an operation permission of the service operation request if the service operation request is risky.

15. The method according to claim 13, wherein the determining a processing method for the service operation request based on a risk identification result of whether the service operation request is risky comprises the following:

receiving, by the client device by using a data channel, a request sent by the server device that is used for restricting the operation permission of the service operation request if the service operation request is risky, and restricting the operation permission of the service operation request.

16. The method according to claim 14 or 15, wherein after the restricting, by the client device, an operation permission of the service operation request, the method further comprises the following:

removing the restriction on the operation permission of the service operation request if restriction removal verification information fed back for a restriction

removal verification request is received, wherein the restriction removal verification request is sent by the client device or the server device.

17. A client device, comprising the following:

a request receiving module, configured to receive a risk identification request sent based on a service operation request, wherein the service operation request comprises service data;

a data acquisition module, configured to obtain service data corresponding to the risk identification request;

an indicator storage module, configured to store service indicator data determined based on the service data; and

a risk identification module, configured to determine whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or the service indicator data.

18. The device according to claim 17, wherein the device further comprises the following:

a configuration data storage module, configured to receive and store configuration data synchronized by using a data channel, wherein the configuration data is combined with the service data and/or the service indicator data, to determine whether the service operation request is risky.

19. The device according to claim 18, wherein the configuration data storage module comprises the following:

a rule storage unit, configured to store the risk identification rule that is used to determine whether the service operation request is risky;

a list storage unit, configured to store information associated with hardware environment information and software environment information of the client device and/or account information in the client device; and

a model storage unit, configured to store the risk identification model that is used to determine whether the service operation request is risky.

20. The device according to claim 17, wherein the risk identification module comprises the following:

a calculation unit, configured to calculate the service indicator data based on the service data.

21. The device according to claim 17, wherein the risk identification module comprises the following:

an analysis unit, configured to perform logic analysis and/or probability analysis on the service data and/or the service indicator data based on the risk identification rule or the risk identification model, and determine whether the service operation request is risky based on a result of the logic analysis and/or the probability analysis.

22. The device according to claim 17, wherein the device further comprises the following:

a processing module, configured to determine a processing method for the service operation request based on a risk identification result of whether the service operation request is risky.

23. A risk identification system, comprising a client device and a server device, wherein

the client device comprises the following:

a request receiving module, configured to receive a risk identification request sent based on a service operation request, wherein the service operation request comprises service data;

a data acquisition module, configured to obtain service data corresponding to the risk identification request;

an indicator storage module, configured to store service indicator data determined based on the service data; and

a risk identification module, configured to determine whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or the service indicator data stored in the client device; and

the server device comprises the following:

a sending module, configured to send the risk identification rule or the risk identification model to the client device by using a data channel, wherein the risk identification rule or the risk identification model is used to determine whether the service operation request is risky; and

a receiving module, configured to receive the service indicator data stored in the client device by using the data channel.

24. A risk identification system, comprising a client device and a server device, wherein

the client device comprises the following:

a request receiving module, configured to receive a risk identification request

sent based on a service operation request, wherein the service operation request comprises service data;

a data acquisition module, configured to obtain service data corresponding to the risk identification request;

an indicator storage module, configured to store service indicator data determined based on the service data; and

a result receiving module, configured to receive, by using a data channel, a result that is determined by the server device, of whether the service operation request is risky; and

the server device comprises the following:

a receiving module, configured to receive the service indicator data stored in the client device by using the data channel;

a risk identification module, configured to determine whether the service operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or the service indicator data stored in the client device, wherein the service indicator data is determined based on the service data; and

a sending module, configured to send, to the client device by using the data channel, the result that is determined by the server device, of whether the service operation request is risky.

25. A risk identification system, comprising a client device, a cloud risk identification device, and a server device, wherein

the client device comprises the following:

a request receiving module, configured to receive a risk identification request sent based on a service operation request, wherein the service operation request comprises service data;

a data acquisition module, configured to obtain service data corresponding to the risk identification request;

an indicator storage module, configured to store service indicator data determined based on the service data; and

a result receiving module, configured to receive, by using a data channel, a result that is determined by the cloud risk identification device, of whether the service operation request is risky;

the cloud risk identification device comprises the following:

a risk identification module, configured to determine whether the service

operation request is risky based on a risk identification rule or a risk identification model, and the service data and/or the service indicator data stored in the client device, wherein the service indicator data is determined based on the service data; and

the server device comprises the following:

a receiving module, configured to receive the service indicator data stored in the client device by using the data channel; and

a sending module, configured to send the service indicator data to the cloud risk identification device, and send the risk identification rule or the risk identification model to the cloud risk identification device.