EVENT PROCESSING METHOD AND SYSTEM, AND STORAGE MEDIUM

TECHNICAL FIELD

[0001] This specification relates to the field of Internet technologies, and in particular, to an event processing method and system, and a storage medium.

BACKGROUND

[0002] With increasing popularity of e-commerce and Internet services, how to perform risk prevention and control on an event triggered by a user over the Internet is an important means to maintain normal and effective running of the Internet.

[0003] In a related technology, a risk prevention and control method for a marketing activity in a marketing scenario is used as an example, and can be divided into a risk prevention and control method before the marketing activity goes online and a risk prevention and control method after the marketing activity goes online. The risk prevention and control method before the marketing activity goes online is to perform risk estimation on the marketing activity based on historical data before the marketing activity goes online. There is a disadvantage that there is a large difference between an estimation result and actual performance. In other words, there is low accuracy. The risk prevention and control method after the marketing activity goes online is to manually observe and analyze data of the online marketing activity after the marketing activity goes online. There are disadvantages that a large quantity of manpower resources are consumed, accuracy is not high due to a subjective factor, and it is difficult to control a fund loss due to data transmission hysteresis.

[0004] It should be noted that, content of the related technology is merely information known to the inventor, and neither means that the information has entered a public domain before an application date of this specification, nor means that the information can become a conventional technology of this specification.

SUMMARY

[0005] This specification provides an event processing method and system, and a storage medium, to avoid at least one of the above-mentioned technical problems.

[0006] According to a first aspect, this specification provides an event processing method, including: determining, in response to that a target event is triggered, a first risk level corresponding to a first time period including a trigger moment of the target event; determining a target risk control policy based on the first risk level, where risk control policies determined based on different risk levels have different prevention and control efforts; and performing risk identification on the target event based on the target risk control policy, to determine whether the target event is a risk event.

[0007] According to a second aspect, this specification provides an event processing system, including: at least one storage medium, storing at least one instruction set, to perform event processing; and at least one processor, communicatively connected to the at least one storage medium, where when running, the at least one processor reads the at least one instruction set, and performs the following operations based on an indication of the at least one instruction set: determining, in response to that a target event is triggered, a first risk level corresponding to a first time period including a trigger moment of the target event; determining a target risk control policy based on the first risk level, where risk control policies determined based on different risk levels have different prevention and control efforts; and performing risk identification on the target event based on the target risk control policy, to determine whether the target event is a risk event.

[0008] According to a third aspect, this specification provides a computer-readable non-transitory storage medium. The computer-readable non-transitory storage medium stores at least one instruction set, and when the at least one instruction set is executed by at least one processor, the method according to any implementation of the first aspect is implemented.

[0009] According to a fourth aspect, this specification provides a computer program product, including a computer program. When the computer program is executed by a processor, the method according to any implementation of the first aspect is implemented.

[0010] It can be learned from the above-mentioned technical solutions that this specification provides an event processing method and system, and a storage medium. The method includes: determining, in response to that a target event is triggered, a first risk level corresponding to a first

time period including a trigger moment of the target event; determining a target risk control policy based on the first risk level, where risk control policies determined based on different risk levels have different prevention and control efforts; and performing risk identification on the target event based on the target risk control policy, to determine whether the target event is a risk event. In other words, in this embodiment, the processing system can detect an event online in real time, and when the target event is detected, determine the first risk level corresponding to the target event, to determine the target risk control policy determined based on the first risk level, so as to determine, based on the target risk control policy, whether the target event is a risk event. In this way, a real-time detection function for determining the risk event is implemented, a disadvantage of risk control hysteresis in a related technology is avoided, automatic risk control is implemented, manual complexity and subjective processing are avoided, and there is relatively higher efficiency and accuracy.

[0011] Other functions of the event processing method and system, and the storage medium provided in this specification are partially listed in the following descriptions. Based on the descriptions, content described by using the following numbers and examples is clear to a person of ordinary skill in the art. Creative aspects of the event processing method and system, and the storage medium provided in this specification can be fully explained by practice or by using the methods, apparatuses, and combinations described in the following detailed examples.

BRIEF DESCRIPTION OF DRAWINGS

[0012] To describe the technical solutions in the embodiments of this specification more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments. Clearly, the accompanying drawings in the following descriptions show merely some embodiments of this specification, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0013] FIG. 1 is a schematic diagram of an application scenario of an event processing method according to an embodiment of this specification;

[0014] FIG. 2 is a diagram of a hardware structure of a computing device according to an embodiment of this specification;

[0015] FIG. 3 is a schematic diagram of an event processing method according to an

embodiment of this specification;

[0016] FIG. 4 is a schematic diagram of determining a first risk level corresponding to a first time period including a trigger moment of a target event according to an embodiment of this specification;

[0017] FIG. 5 is a schematic diagram of an event processing method according to another embodiment of this specification; and

[0018] FIG. 6 is a schematic diagram of an event processing method according to another embodiment of this specification.

DESCRIPTION OF EMBODIMENTS

[0019] Example embodiments are described in detail here, and examples of the example embodiments are presented in the accompanying drawings. When the following description relates to the accompanying drawings, unless specified otherwise, same numbers in different accompanying drawings represent same or similar elements. Implementations described in the following example embodiments do not represent all implementations consistent with the present specification. On the contrary, the embodiments are merely examples of apparatuses and methods that are described in the appended claims in details and consistent with some aspects of the present specification.

[0020] It should be understood that the terms "include" and "have" in the embodiments of this specification and any variants thereof are intended to cover the non-exclusive inclusion, for example, a product or device that includes a series of components are not necessarily limited to those components that are clearly listed, but may include other components that are not clearly listed or inherent to such product or device.

[0021] In the embodiments of this specification, the term "and/or" describes an association relationship between associated objects and indicates that three relationships may exist. For example, "A and/or B" may indicate the following three cases: Only A exists, both A and B exist, and only B exists. The character "/" generally indicates an "or" relationship between the associated objects.

[0022] In the embodiments of this specification, the term "a plurality of" refers to two or more, and other quantifiers are similar to this term.

[0023] The terms "first", "second", "third", etc. in this specification are used to distinguish between similar or same objects or entities, and do not necessarily mean limiting a specific order or sequence, unless otherwise indicated. It should be understood that the terms used in such a way is interchangeable in appropriate cases, for example, can be implemented in an order other than those illustrated or described in the embodiments of this specification.

[0024] The term "unit/module" used in this specification means any known or later developed hardware, software, firmware, artificial intelligence, fuzzy logic, or a combination of hardware code or/and a combination of software code, and can perform functions related to the element.

[0025] To facilitate readers' understanding of this specification, at least some terms in this specification are explained below:

[0026] A marketing activity is a marketing activity specified by a merchant or a platform to attract a user, for example, a discount activity or a buy-and-get activity. The platform can be a social platform, an e-commerce platform, etc.

[0027] Marketing funds are funds provided by a merchant or a platform to subsidize a user to attract the user to participate in a marketing activity.

[0028] A subsidy rate is a ratio of an amount subsidized by the merchant/platform in the marketing activity to a transaction amount.

[0029] A write-off rate is a ratio of a quantity of coupons actually written off in a marketing activity launched by a merchant to a quantity of issued coupons. For example, when the marketing activity is a discount activity, the write-off rate can be understood as a ratio of a quantity of actually written-off coupons to a quantity of issued coupons in discount coupons issued by the merchant.

[0030] A black market is short for a black market, and is a network illegal behavior implemented by using an Internet technology.

[0031] A KYC user is a user who may have a risk and therefore for which a customer information check needs to be performed in fields such as the financial field, the banking field, or the securities transaction field.

[0032] To facilitate readers' understanding of this specification, application scenarios and related technologies of this specification are described below.

[0033] An event processing method provided in this specification can be applied to a scenario in which real-time risk prevention and control needs to be performed on an event. For example, whether an event is a marketing cheating event is identified in a marketing activity scenario,

whether a transaction event is a risk transaction is identified in a transaction scenario, and whether a payment event is an illegal fund transfer event is identified in a payment scenario. Examples are not listed one by one here.

[0034] For example, that the event processing method in this specification is applied to the marketing activity scenario is used as an example. A to-be-processed event can correspond to a request event generated because a user requests to participate in a marketing activity.

[0035] Correspondingly, for the request event triggered by the user, an event processing system can perform the event processing method in this specification, to determine and perform risk prevention and control processing (which can be briefly referred to as risk control processing) on the request event based on a risk control policy corresponding to the request event. For example, the event processing system performs risk identification on the request event, to determine whether the request event is a risk event, and further, when the request event is a risk event, blocks the request event, and outputs prompt information corresponding to the blocking to the user.

[0036] For example, the event processing system performs risk identification on the request event, to determine whether the request event is a get the best deal event that a black market registers a large amount of accounts, etc. to participate in the marketing activity. If yes, the event processing system blocks the request event, for example, rejects a request of the user to participate in the marketing activity, and sends prompt information to the user to prompt the user that the request of the user is rejected. In some cases, the event processing system can further selectively inform the user of a reason why the user is rejected to participate in the marketing activity.

[0037] It can be understood that, to avoid tedious descriptions, for a principle that the event processing method in this specification is applied to another scenario such as a transaction scenario or a payment scenario, references can be made to the descriptions of the marketing activity scenario in the above-mentioned example. Details are omitted here for simplicity. In addition, it should be noted that the above-mentioned application scenario is merely a part of a plurality of use scenarios provided in this specification. A person skilled in the art should understand that, that the event processing method described in this specification is applied to another use scenario also falls within the protection scope of this specification.

[0038] With reference to the above-mentioned descriptions of the application scenario, an event that is of the user and that is generated based on the Internet is, for example, an event of requesting to participate in the marketing activity in the marketing activity scenario, an event of

requesting to participate in a transaction in the transaction scenario, or an event of requesting to participate in payment in the payment scenario. To avoid generating an Internet risk, a system in a corresponding scenario needs to perform risk control processing on a corresponding event, for example, risk identification and risk coping when a risk event is determined through risk identification.

[0039] For ease of understanding of a reader, in this specification, a marketing activity scenario is mainly used as an example, to describe related technologies in this specification in detail. For another scenario, references can be made to descriptions of the marketing activity scenario.

[0040] For example, any merchant or platform can launch a marketing activity, for example, subsidize a user to promote a transaction, to maintain an old user and obtain a new user. In addition, the marketing activity can have various activity content, activity types, etc. For example, the marketing activity can be a coupon, a transaction discount activity, a peer-to-peer promotion activity, or a lottery activity.

[0041] However, in a process of the marketing activity, the platform may not only attract an ordinary consumer to participate, but also attract a black market to participate in the activity by registering a large quantity of accounts, etc., to get the best deal and implement cash realization. Consequently, although the platform has spent a large amount of marketing funds, real development of a service cannot be promoted actually.

[0042] To avoid the above-mentioned disadvantage, the platform can deploy a corresponding risk control method, for example, a risk prevention and control method, to prevent the above-mentioned marketing cheating risk in the risk prevention and control method. For example, the platform can deploy a risk control policy system. The risk prevention and control method is implemented based on the risk control policy system. To be specific, the platform can prevent the above-mentioned marketing cheating risks by using the risk control policy system.

[0043] Based on an applicable time, the risk prevention and control method can include a risk prevention and control method before the marketing activity goes online and a risk prevention and control method after the marketing activity goes online. The risk prevention and control method before the marketing activity goes online is to estimate, before the marketing activity goes online, a risk after content, etc. of the marketing activity goes online, and then perform risk prevention and control by properly designing a rule of the marketing activity. The risk prevention and control method after the marketing activity goes online is to detect data of the marketing activity after the

marketing activity goes online, to realize risk prevention and control.

[0044] However, the risk prevention and control method before the marketing activity goes online is to estimate, based on data of a historical similar marketing activity, a risk after a current marketing activity goes online. Usually, there is a relatively large difference between an estimation result and actual performance of the marketing activity. Unless there is a clear high-risk marketing activity, it is difficult to pr-estimate actual risk performance after the marketing activity goes online. Consequently, it is difficult to effectively perform prevention and control.

[0045] An evaluation method after the marketing activities go online is mainly that after the marketing activity goes online, a worker observes and analyzes data of the online marketing activity. An extremely large quantity of manpower resources are consumed, and it is very difficult to implement long-time continuous observation and analysis. In addition, because the marketing activity has been online and there is data transmission hysteresis, if troubleshooting is started when a data abnormality is found, it is too late, the black market has gained a huge profit, and a large amount of funds are usually lost.

[0046] It should be noted that, content of the related technology is merely information known to the inventor, and neither means that the information has entered a public domain before an application date of this specification, nor means that the information can become a conventional technology of this specification.

[0047] To avoid at least one of the above-mentioned problems, this specification provides a creative technical concept: An event is detected online in real time. When a target event is detected, a dynamic risk level is determined in real time, and risk control processing is performed on the target event based on a target risk control policy corresponding to the dynamic risk level. For example, risk identification is performed on the target event, to determine whether the target event is a risk event. Further, when the target event is a risk event, the target event can be blocked, and when the target event is not a risk event, an operation corresponding to the target event is allowed to be performed.

[0048] Relatively, based on the above-mentioned technical concept, timeliness of risk control processing is improved in a real-time manner, to avoid risk control processing hysteresis in the related technology, and real-time automatic risk control processing is performed, to avoid manual complexity and subjective risk control processing, and improve accuracy and reliability of risk control processing.

[0049] FIG. 1 is a schematic diagram of an application scenario of an event processing method according to an embodiment of this specification. The event processing method in this specification can be applied to an application scenario 100 shown in FIG. 1. As shown in FIG. 1, the application scenario 100 can include a target user 101, a client 102, a server 103, and a network 104.

[0050] The target user 101 can be a user who triggers an event. To be specific, the target user 101 can perform an event triggering operation on the client 102.

[0051] For example, with reference to the above-mentioned descriptions of the application scenario, if the application scenario is a marketing activity scenario, the target user 101 is a user who initiates a request event of participating in a marketing activity; if the application scenario is a transaction scenario, the target user 101 is a user who initiates a transaction request; and if the application scenario is a payment scenario, the target user 101 is a user who initiates a payment request.

[0052] The client 102 can be a device that responds to a triggering operation of the target user 102. In some embodiments, the event processing method provided in this specification can be performed on the client 102. In this case, the client 102 can store data or instructions for performing the event processing method, and can execute or be configured to execute the data or the instructions. The client 102 can include a hardware device with a data information processing function and a necessary program needed to drive the hardware device to work.

[0053] For example, when the client 102 detects that the target user 102 triggers a specific event, the client 102 can perform the event processing method in this specification, to perform risk control processing on the event.

[0054] The client 102 can include a mobile device, a tablet, a laptop computer, a device built in a motor vehicle or similar content, or any combination thereof. In some embodiments, the mobile device can include a smart home device, a smart mobile device, a virtual reality device, an augmented reality device or a similar device, or any combination thereof. In some embodiments, the smart home apparatus can include a smart television, a desktop computer, or any combination. In some embodiments, the smart mobile device can include a smartphone, a personal digital assistant, a game device, a navigation device, or any combination thereof. In some embodiments, the apparatus built in the motor vehicle can include a vehicle-mounted computer, a vehicle-mounted television, etc. In some embodiments, the client 102 can include an event collection

device, configured to collect the event initiated by the target user 101.

[0055] In some embodiments, one or more applications (app) can be installed on the client 102. The app can provide the target user 101 with a capability and an interface for interacting with the outside through the network 104. The app includes but is not limited to a web browser app program, a search app program, a chat app program, a shopping app program, a video app program, a financial app program, an instant messaging tool, a mailbox client, social platform software, etc. In some embodiments, a target app can be installed on the client 102. The target app can collect, for the client 102, the event initiated by the target user 101.

[0056] As shown in FIG. 1, the client 102 can be communicatively connected to the server 103. The server 103 can communicate with one client 102, or can communicate with a plurality of clients 102. In some embodiments, the client 102 can interact with the server 103 through the network 104, to receive or send a message, etc.

[0057] The server 103 can be a server that provides various services. For example, in the marketing activity scenario, the server 103 can be a back-end server that provides a marketing risk control service for the client 102; in the transaction scenario, the server 103 can be a back-end server that provides a transaction risk control service for the client 102; and in the payment scenario, the server 103 can be a back-end server that provides a payment risk control service for the client 102. The server 103 can be a local server, or can be a cloud server.

[0058] In some embodiments, the event processing method can be performed on the server 103. In this case, the server 103 can store data or instructions for performing the event processing method described in this specification, and can execute or be configured to execute the data or the instructions. The server 103 can include a hardware device with a data information processing function and a necessary program needed for driving the hardware device to work.

[0059] For example, the target user 101 can initiate an event to the server 103 by performing a touch operation on the client 102. Correspondingly, when detecting that the event is triggered, the server 103 can perform the event processing method in this specification, to perform risk control processing on the event.

[0060] The network 104 is a medium configured to provide a communication connection between the client 102 and the server 103. The network 104 can facilitate exchange of information or data. As shown in FIG. 1, the client 102 and the server 103 can be separately connected to the network 104, and transmit information or data to each other through the network 104.

[0061] The network 104 can be any type of wired or wireless network, or can be a combination thereof. For example, the network 104 can include a cable network, a wired network, an optical fiber network, a telecommunication network, an intranet, the internet, a local area network (LAN), a wide area network (WAN), a wireless local area network (WLAN), a metropolitan area network (MAN), a public switched telephone network (PSTN), a Bluetooth networkTM, a short-range wireless network (ZigBeeTM), a near field communication (NFC) network, or a similar network. The network 104 can include one or more network access points. For example, the network 104 can include a wired or wireless network access point, for example, a base station or an Internet switching point. Through the access point, one or more components of the client 102 and the server 103 can be connected to the network 104 to exchange data or information.

[0062] Quantities of clients 102, servers 103, and networks 104 in FIG. 1 are merely examples. There can be any quantity of clients 102, servers 103, and networks 104 based on implementation needs. In addition, the event processing method provided in this specification can be completely performed on the client 102, can be completely performed on the server 103, or can be partially performed on the client 102 and partially performed on the server 103.

[0063] In other words, FIG. 1 and the above-mentioned descriptions for FIG. 1 are merely used to describe an example of an application scenario to which the event processing method in this specification may be applied, and cannot be understood as a limitation on the application scenario.

[0064] FIG. 2 is a diagram of a hardware structure of a computing device 200 according to an embodiment of this specification. The computing device 200 can perform an event processing method described in this specification. The event processing method is described in another part of this specification. The computing device 200 can correspond to the client 102 shown in FIG. 1, can correspond to the server 103 shown in FIG. 1, or can correspond to an event processing system provided in this specification.

[0065] As shown in FIG. 2, the computing device 200 can include at least one storage medium 203 and at least one processor 202. In some embodiments, the computing device 200 can further include a communication port 204 and an internal communication bus 201. The computing device 200 can further include an I/O component 205.

[0066] The internal communication bus 201 can be connected to different system components. For example, the internal communication bus 201 can be connected to the storage medium 203,

the processor 202, the communication port 204, and the I/O component 205.

[0067] The I/O component 205 supports input/output between the computing device 200 and other components.

[0068] The communication port 204 is used for data communication between the computing device 200 and the outside. For example, the communication port 204 can be used for data communication between the computing device 200 and a network 104. The communication port 204 can be a wired communication port, or can be a wireless communication port.

[0069] The storage medium 203 can include a data storage apparatus. The data storage apparatus can be a non-transitory storage medium, or can be a transitory storage medium. For example, the data storage apparatus can include one or more of a disk 2031, a read-only storage medium (ROM) 2032, or a random access storage medium (RAM) 2033. The storage medium 203 further includes at least one instruction set stored in the data storage apparatus. The instruction set includes computer program code, and the computer program code can include a program, a routine, an object, a component, a data structure, a process, a module, etc. for performing the event processing method provided in this specification.

[0070] The at least one processor 202 can be communicatively connected to the at least one storage medium 203. The at least one processor 202 is configured to execute the at least one instruction set. When the computing device 200 runs, the at least one processor 202 reads the at least one instruction set, and performs, based on an indication of the at least one instruction set, the event processing method provided in this specification. The processor 202 can perform all steps included in the event processing method. The processor 202 can be in a form of one or more processors. In some embodiments, the processor 202 can include one or more hardware processors, for example, a microcontroller, a microprocessor, a reduced instruction set computer (RISC), an application-specific integrated circuit (ASIC), an application-specific instruction set processor (ASIP), a central processing unit (CPU), a graphics processing unit (GPU), a physical processing unit (PPU), a microcontroller unit, a digital signal processor (DSP), a field programmable gate array (FPGA), an advanced RISC machine (ARM), a programmable logic device (PLD), any circuit or processor that can perform one or more functions, or any combination thereof.

[0071] To merely describe a problem, only one processor 202 is shown in the computing device 200 in the accompanying drawings. However, it should be noted that, the computing device 200 in this specification can further include a plurality of processors. Therefore, the operations

and/or method steps disclosed in this specification can be performed by one processor, or can be jointly performed by a plurality of processors. For example, if the processor 202 in the computing device 200 described in this specification performs step A and step B, it should be understood as that step A and step B can be jointly or separately performed by two different processors 202 (for example, a first processor performs step A, and a second processor performs step B, or a first processor and a second processor jointly perform step A and step B).

[0072] FIG. 3 is a schematic diagram of an event processing method according to an embodiment of this specification. As shown in FIG. 3, the method includes S301 to S303.

[0073] S301: Determine, in response to that a target event is triggered, a first risk level corresponding to a first time period including a trigger moment of the target event.

[0074] For example, this embodiment can be executed by an event processing system (briefly referred to as a processing system below), and the processing system can be a server, can be a terminal device, can be a processor, can be a chip, etc. Details are not listed one by one here.

[0075] If the processing system is a server, the processing system can be an independent server, or can be a cluster server, or can be a cloud server, or can be a local server. This is not limited in this embodiment.

[0076] For example, with reference to the application scenario shown in FIG. 1, the processing system can be the client 102 shown in FIG. 1, can be the server 103 shown in FIG. 1, or can be a system including the client 102 and the server 103 shown in FIG. 1. For another example, with reference to the computing device 200 shown in FIG. 2, the processing system can be the computing device 200 shown in FIG. 2. Specifically, the processor 202 can read an instruction set stored in a local storage medium of the processor 202, and then perform the event processing method based on a stipulation of the instruction set.

[0077] S301 can be understood as follows: The processing system performs real-time detection on an event; and when the target event is detected, obtains the trigger moment of the target event, determines a time period including the trigger moment, where the time period is referred to as the first time period for ease of distinguishing, and obtains a risk level corresponding to the first time period, where the risk level is referred to as the first risk level for ease of distinguishing.

[0078] Duration of the first time period can be determined by the processing system based on an application scenario, a requirement, a historical record, a manner such as an experiment, etc. This is not limited in this embodiment.

[0079] For example, for an application scenario in which a risk is relatively large, the duration of the first time period can be relatively short; on the contrary, for an application scenario in which a risk is relatively small, the duration of the first time period can be relatively long. For another example, for a requirement with relatively strong timeliness, the duration of the first time period can be relatively short; on the contrary, for a requirement with relatively weak timeliness, the duration of the first time period can be relatively long. For still another example, for an application scenario in which a risk degree changes frequently, the duration of the first time period can be relatively short; on the contrary, for an application scenario in which a risk degree changes infrequently, the duration of the first time period can be relatively long.

[0080] In some embodiments, the target event can be one of the following: a transaction event triggered by a target user; a payment event triggered by the target user; and an event that the target user requests to participate in a marketing activity.

[0081] For example, with reference to the above-mentioned example, the event processing method in this specification can be applied to different application scenarios such as a transaction scenario, a payment scenario, and a marketing activity scenario. Correspondingly, different application scenarios correspond to different target events. For example, in the transaction scenario, the target event is a transaction event triggered by the target user due to a transaction requirement; in the payment scenario, the target event is a payment event triggered by the target user due to a payment requirement; and in the marketing activity scenario, the target event is an event triggered by the target user for a requirement for participating in the marketing activity.

[0082] In other words, the event processing method in this embodiment can be applied to different application scenarios, and different application scenarios correspond to different target events. That is, the event processing method in this specification has a relatively strong generalization capability, and has general applicability.

[0083] For ease of understanding of a reader, S301 is described in detail with reference to FIG. 1, the marketing activity scenario, and the target event in the marketing activity scenario. For descriptions of another application scenario, references can be made to this example. Details are omitted for simplicity.

[0084] For example, the application scenario is the marketing activity scenario, and the processing system is the server 103.

[0085] The client 102 can be a shopping app program, and an e-commerce platform initiates,

by using the shopping app program, a marketing activity, for example, a marketing activity in which a discount coupon is issued. The target user 101 can perform a coupon receiving operation on the shopping app program. The coupon receiving operation is to trigger the target event. In other words, the target event is a target event in which the target user 101 initiates, to the server 103 by using the shopping app program, a request to participate in the marketing activity, and is specifically a target event in which coupon receiving is initiated to the server 103 by using the shopping app program. A time at which the target user 101 performs the coupon receiving operation on the shopping app program is 11:30.

[0086] Correspondingly, the server 103 determines a first time period including 11:30 for the coupon receiving operation of the target user 101, and the first time period can be determined based on a magnitude of a risk of the marketing activity of the discount coupon.

[0087] The server 103 can use the trigger time as a start point, backtrack a period of time, and determine the time period as the first time period.

[0088] For example, if the risk is relatively high, the first time period can be a time period between 11:20 and 11:30; and if the risk is relatively low, the first time period can be a time period between 11:00 and 11:30. For example, when the server 103 determines that the first time period is a time period between 11:00 and 11:30, a risk level corresponding to 11:00 and 11:30 can be determined, and the risk level is referred to as the first risk level.

[0089] Alternatively, the server 103 can pre-divide the time period, to determine, when the trigger time is obtained, a specific time period including the trigger time, so as to determine that the time period including the trigger time is the first time period.

[0090] For example, if the risk is relatively high, the first time period can be a time period between 11:00 and 12:00; and if the risk is relatively low, the first time period can be a time period between 10:00 and 12:00. For example, the server 103 can determine that 11:30 belongs to the time period from 10:00 to 12:00, determine that the first time period is the time period from 10:00 to 12:00, and determine a risk level corresponding to the time period from 10:00 to 12:00. The risk level is referred to as the first risk level.

[0091] With reference to the above-mentioned example, it can be learned that the processing system can determine the first time period in at least two manners. A first manner is that the processing system uses the trigger time as the start point, backtracks the period of time, and uses the period of time as the first time period. In a second manner, the processing system pre-divides

the time period, and determines that the time period including the trigger time is the first time period.

[0092] For the first time period determined in different manners, the processing system can determine the first risk level in different manners. For example, for a first manner, the processing system can determine the first risk level through computation with reference to online data collected in the first time period; and for a second manner, the processing system can determine the first risk level based on a preset correspondence between a time period and a risk level.

[0093] For example, the first manner of determining the first time period is used as an example. In some embodiments, an end moment of the first time period is the trigger moment of the target event. With reference to FIG. 4, the determining a first risk level corresponding to a first time period including a trigger moment of the target event in S301 can include S3011 and S3012:

[0094] S3011: Obtain event information of a plurality of historical events triggered in the first time period.

[0095] Each historical event has corresponding event information, and event information of any two historical events may be the same or different.

[0096] Any historical event is an event that is triggered in the first time period and whose trigger time is earlier than the trigger moment of the target event. For example, with reference to the above-mentioned example, if the first time period is a time period between 11:00 and 11:30, the historical event is an event that occurs after 11:00 and before 11:30.

[0097] Event information of any historical event is related data of a corresponding historical event in the application scenario. For example, if the application scenario is the marketing activity scenario, the event information can include related information of a user who executes the historical event, a type of a coupon received by the user, an amount consumed due to coupon receiving, etc. For another example, if the application scenario is the transaction scenario, the event information can include a transaction amount, related information of a transaction user, etc.

[0098] In some embodiments, the processing system can include an awareness platform, or referred to as a data platform, to obtain corresponding data. For example, the awareness platform performs S3011, to obtain the event information of the plurality of historical events triggered in the first time period.

[0099] S3012: Determine the first risk level corresponding to the first time period based on the event information of the plurality of historical events.

[0100] For example, when the processing system obtains the event information of the plurality of historical events, the first risk level corresponding to the first time period can be determined with reference to the event information corresponding to each historical event.

[0101] In some embodiments, the processing system can further include a real-time risk element computing platform, or referred to as a risk element computing module, etc., to be connected to the awareness platform to obtain event information of a plurality of historical events that is transmitted by the awareness platform, so as to compute the first risk level.

[0102] In a possible technical solution, the processing system can further include a feature platform. The feature platform is separately connected to the awareness platform and the real-time risk element computing platform, to obtain the event information of the plurality of historical events transmitted by the awareness platform, determine a risk feature, for example, a feature vector, corresponding to the event information of the plurality of historical events, and transmit the feature vector to the real-time risk element computing platform. Correspondingly, the real-time risk element computing platform computes the feature vector, to obtain the first risk level.

[0103] With reference to S3011 and S3012, it can be learned that in this embodiment, the processing system determines the first risk level with reference to event information of each historical event, to implement real-time evaluation on the risk level. In addition, the first risk level is obtained based on the event information of the plurality of historical events in the first time period, the first risk level can accurately represent a risk level corresponding to the target event at a current moment. In other words, validity and reliability of the first risk level can be improved.

[0104] In some embodiments, with reference to FIG. 4, it can be learned that S3012 can include S30121 and S30122.

[0105] S30121: Determine a current index value corresponding to at least one preset risk control index based on the event information of the plurality of historical events.

[0106] Similarly, content and a quantity of preset risk control indexes can be separately determined by the processing system based on an application scenario, a requirement, a historical record, a manner such as an experiment, etc. This is not limited in this embodiment. For example, for a scenario in which a precision requirement is relatively high, there can be a plurality of preset risk control indexes. For another example, for the marketing activity scenario, the preset risk control index can include one or more of the following: a write-off rate, a subsidy rate, a proportion of KYC users, etc.

[0107] In some embodiments, the processing system can select one or more risk control indexes from the plurality of risk control indexes as at least one preset risk control index, to avoid tedious computation and relatively ensure accuracy of subsequently determining the first risk level.

[0108] S30122: Determine the first risk level corresponding to the first time period based on the current index value corresponding to the at least one preset risk control index and a preset mapping relationship, where the preset mapping relationship is used to represent a correspondence between an index value corresponding to the at least one preset risk control index and a risk level.

[0109] Similarly, the processing system can determine the correspondence between an index value and a risk level based on the application scenario, the requirement, the historical record, the manner such as the experiment, etc., to construct the preset mapping relationship. Correspondingly, in actual applications, when obtaining the index value, the processing system can determine the corresponding risk level based on a manner of querying the preset mapping relationship.

[0110] For example, it is assumed that the at least one preset risk control index is one preset risk control index, for example, is the write-off rate. In this case, after computing a value of the write-off rate, the processing system can query the preset mapping relationship, to obtain a risk level corresponding to the value of the write-off rate, and determine the risk level as the first risk level.

[0111] For example, it is assumed that the at least one preset risk control index is two preset risk control indexes, for example, the write-off rate and the subsidy rate. In this case, after separately computing the value of the write-off rate and a value of the subsidy rate, the processing system queries the preset mapping relationship, to obtain a risk level corresponding to the value of the write-off rate, and obtain a risk level corresponding to the value of the subsidy rate. Then, the processing system can determine the first risk level based on two risk levels, and a specific manner of determining the first risk level is not limited. For example, the first risk level can be determined based on the application scenario, the requirement, the historical record, the manner such as the experiment, etc. For example, the processing system can determine a risk level with a higher risk from the two risk levels, and determine the risk level with a higher risk as the first risk level. For another example, the processing system can determine a risk level with a lower risk from the two risk levels, and determine the risk level with a lower risk as the first risk level. For still another example, the processing system can determine an average risk level of the two risk levels, and determine the average risk level as the first risk level.

[0112] In the above-mentioned example, when there are two preset risk control indexes (for example, the write-off rate and the subsidy rate), the preset mapping relationship can be shown in Table 1. In this case, after separately computing the value of the write-off rate and the value of the subsidy rate, the processing system can query the mapping relationship shown in Table 1 based on the value of the write-off rate and the value of the subsidy rate, to obtain the first risk level.

Table 1

Write-off rate	Subsidy rate	Risk level
[x1, x2)	[y1, y2)	Risk level 1
[x2, x3)	[y2, y3)	Risk level 2
...	...	...

[0113] With reference to S30121 and S30122, it can be learned that, in this embodiment, the processing system can first compute the current index value, and determine the first risk level with reference to the current index value and the preset mapping relationship, so that the first risk level is aligned with the current index value. Because the current index value is further aligned with the event information, the first risk level is highly aligned with the event information. Therefore, the first risk level can be associated with an actual situation, and validity and reliability of the first risk level can be improved.

[0114] The second manner of determining the first time period is used as an example. In some embodiments, the processing system can pre-divide each time period, pre-construct a correspondence between a time period and a risk level, and when the trigger time of the target event is obtained, determine a time period including the trigger time, where the time period is the first time period, and query the correspondence, to determine the risk level corresponding to the first time period, where the risk level is the first risk level.

[0115] For example, for an application scenario in which risk levels present a specific rule in terms of time, the processing system can construct the correspondence based on the time and the rule of the risk levels. For example, generally, there is a medium risk level from 8:00 to 10:00, and there is a medium risk level from 10:00 to 12:00. When the trigger time is 11:30, the processing system determines a time period (namely, the first time period) from 10:00 to 12:00 including the trigger time, and determines that a risk level corresponding to the time period is the medium risk

level.

[0116] A risk level division manner is not limited in this specification. For example, in some scenarios, the risk level can be divided into a high risk level, a medium risk level, and a low risk level. For another example, in some scenarios, the risk level can be divided into a high risk level and a low risk level. For another example, in some scenarios, the risk level can be further divided into an extremely high risk level, a high risk level, a medium risk level, a low risk level, and an extremely low risk level.

[0117] S302: Determine a target risk control policy based on the first risk level, where risk control policies determined based on different risk levels have different prevention and control efforts.

[0118] For example, with reference to the above-mentioned example, the processing system can further include a policy hierarchical platform (or referred to as a policy layer module) and a policy scheduling platform that are connected to each other, and the policy scheduling platform is further connected to the real-time risk element computing platform. A plurality of risk control policies are stored on the policy hierarchical platform. The policy scheduling platform receives the first risk level transmitted by the real-time risk element computing platform, and determines and invokes the target risk control policy from the policy hierarchical platform based on the first risk level.

[0119] The risk control policy can be one or more policies used for prevention and control risk, can be a policy packet, can be a policy set, etc.

[0120] Different risk levels correspond to different risk control policies, and risk control policies of different risk levels have different risk prevention and control efforts or strength. For example, a higher risk level corresponds to more prevention and control efforts of a risk control policy; on the contrary, a lower risk level corresponds to less prevention and control efforts of a risk control policy.

[0121] It should be noted that any risk control policy can include a plurality of policies used for risk prevention and control, such as a high-risk tightening policy, a packet blocking policy, or a data missing proportion blocking policy.

[0122] The high-risk tightening policy can be understood as follows: When the risk level is relatively high, an event can be blocked in a relatively strict risk prevention and control manner, for example, at a higher blocking level. The high-risk tightening policy can be performing

tightening from a single dimension, or can be performing tightening from a plurality of dimensions. The single dimension can be a dimension of newly registered user information, or can be a dimension of an object (for example, a product) corresponding to the event, a dimension of an internet protocol (IP) address, etc. Correspondingly, the plurality of dimensions can be a combination of at least two single dimensions.

[0123] The packet blocking policy can be understood as that different blocking levels are used for group users of different risk levels. For example, the blocking level can be relatively high for a group user with a relatively high risk level; on the contrary, the blocking level can be relatively low for a group user with a relatively low risk level.

[0124] The data missing proportion blocking policy can be understood as that the processing system can obtain data of a user who initiates an event, and the processing system can block the event if the data of the user is missing and a missing proportion is relatively high. Similarly, in this embodiment, a standard in which the processing system determines whether the missing proportion is high or low is not limited, and can be determined by the processing system based on the application scenario, the requirement, the historical record, the manner such as the experiment, etc.

[0125] In this embodiment, any risk control policy can include a plurality of different policies such as the high-risk tightening policy, the packet blocking policy, and the data missing proportion blocking policy, to avoid disadvantages such as low flexibility and low accuracy that are caused by a single threshold risk control policy, and improve flexibility and diversity of risk control processing.

[0126] It should be noted that when the first risk level is determined, the processing system can determine the target risk control policy in different manners with reference to the first risk level. For example, if the first risk level is determined by the processing system in an online real-time manner, the processing system can also determine the target risk control policy in an online single-dimensional manner. For another example, the processing system can determine the target risk control policy in an online and offline multi-dimensional manner.

[0127] For example, the processing system determines the target risk control policy in the online single-dimensional manner. In some embodiments, S302 can include: using a risk control policy corresponding to the first risk level in a plurality of preset risk control policies as the target risk control policy.

[0128] For example, different risk levels correspond to different risk control policies, there is a one-to-one correspondence between the plurality of preset risk control policies and a plurality of preset risk levels, and the risk control policy corresponding to the first risk level in the plurality of preset risk control policies is the target risk control policy.

[0129] Correspondingly, the processing system determines the risk control policy corresponding to the first risk level from the plurality of preset risk control policies, and determines the risk control policy as the target risk control policy.

[0130] In this embodiment, the processing system determines the target risk control policy in the online single-dimensional manner, to implement real-time dynamic switching of the risk control policy, and improve efficiency and convenience of determining the target risk control policy.

[0131] For example, the processing system determines the target risk control policy in the online and offline multi-dimensional manner. In some embodiments, S302 can include step 1 to step 3.

[0132] Step 1: Obtain a second risk level corresponding to a second time period including the trigger moment of the target event, where the second risk level is determined based on event information of a historical event that occurs in a third time period, the second time period includes the first time period, and the third time period is before the second time period.

[0133] For example, the second risk level is determined in an offline manner, and is specifically determined based on the event information of the historical event that occurs in the third time period. For the historical event that occurs in the third time period and content of the event information of the historical event that occurs in the third time period, references can be made to the descriptions of the plurality of historical events triggered in the first time period and the event information of the plurality of historical events triggered in the first time period in the above-mentioned example. Details are omitted here for simplicity.

[0134] The processing system can periodically perform periodic risk backtracking on event information of a historical event in an offline computing manner, and determine a second risk level corresponding to a next period based on a risk backtracking result. For example, duration of the period can be one day. To be specific, risk backtracking on event information of a historical event that occurs on the T^{th} day is triggered at 24:00 on the T^{th} day. A risk backtracking result is used as a second risk level corresponding to the $(T+1)^{th}$ day.

[0135] For example, with reference to the above-mentioned example, the processing system can further include a risk offline platform, or referred to as a risk backtracking platform, and is separately connected to the data platform and the policy scheduling platform. The risk offline platform obtains corresponding data from the data platform to compute a corresponding risk level for risk backtracking, and transmits the second risk level obtained through risk backtracking to the policy scheduling platform. The policy scheduling platform schedules the corresponding risk control policy from the policy hierarchical platform in combination with the first risk level provided by the real-time risk element computing platform and the second risk level provided by the risk offline platform.

[0136] For example, if the trigger moment of the target event is 9 o'clock on April 15, the first time period can be 8 o'clock to 9 o'clock on April 15, the second time period can be April 15, and the third time period can be April 14.

[0137] The processing system can determine a second risk level corresponding to April 15 (namely, the second time period) based on event information of a historical event that occurs on April 14 (namely, the third time period). In some embodiments, for a specific manner of determining the second risk level, references can be made to the descriptions of determining the first risk level in the above-mentioned example. Details are omitted here for simplicity. In some other embodiments, the processing system can alternatively determine the second risk level based on each risk level, on April 14, obtained through online real-time detection, for example, determine the second risk level based on an average algorithm, a maximum risk level selection policy, a minimum risk level selection policy, and a maximum risk level quantity selection policy.

[0138] Correspondingly, the processing system can store the second risk level, to invoke the second risk level in an online real-time detection process.

[0139] It can be understood that, obtaining of the second risk level is described by using the processing system as an example. The second risk level can alternatively be determined by another system (for example, an offline data processing system), and the second risk level is transmitted to the processing system, so that the processing system invokes the second risk level online.

[0140] Step 2: Determine a target risk level based on the first risk level and the second risk level.

[0141] Similarly, a manner in which the processing system determines the target risk level is not limited in this embodiment, and can be determined by the processing system based on the

application scenario, the requirement, the historical record, the manner such as the experiment, etc.

[0142] For example, in some embodiments, step 2 can include one of Manner 1 to Manner 3:

[0143] Manner 1: Determine the first risk level as the target risk level if the first risk level is higher than or equal to the second risk level.

[0144] For example, for an application scenario in which a risk control requirement is relatively strict, the processing system can select a higher risk level from the first risk level and the second risk level as the target risk level based on a "strict" policy, to strictly control a get the best deal behavior.

[0145] Manner 2: Determine the second risk level as the target risk level if the first risk level is higher than or equal to the second risk level.

[0146] For example, for an application scenario in which the risk control requirement is relatively loose, the processing system can select a lower risk level from the first risk level and the second risk level as the target risk level based on a "loose" policy, to avoid blocking a normal user incorrectly.

[0147] Manner 3: Select a risk level corresponding to a preset prevention and control effort requirement for the target event from the first risk level and the second risk level as the target risk level based on the preset prevention and control effort requirement.

[0148] Similarly, the preset prevention and control effort requirement can be determined by the processing system based on the application scenario, the requirement, the historical record, the manner such as the experiment, etc. This is not limited in this embodiment.

[0149] For example, if the preset prevention and control effort requirement is relatively high, the processing system can select a risk level with a higher prevention and control effort from the first risk level and the second risk level as the target risk level; on the contrary, if the preset prevention and control effort requirement is relatively low, the processing system can select a risk level with a lower prevention and control effort from the first risk level and the second risk level as the target risk level.

[0150] With reference to Manner 1 to Manner 3, it can be learned that in this embodiment, the processing system can determine the target risk level in different manners, to implement flexibility and diversity of determining the target risk level.

[0151] Step 3: Use a risk control policy corresponding to the target risk level in a plurality of preset risk control policies as the target risk control policy.

[0152] Correspondingly, when the target risk level is determined, the processing system can determine the risk control policy corresponding to the target risk level from the plurality of preset risk policies, and determine the risk control policy as the target risk control policy. For an implementation in which the processing system specifically determines the target risk control policy corresponding to the target risk level, references can be made to the descriptions that the processing system determines the target risk control policy corresponding to the first risk level in the above-mentioned example. Details are omitted here for simplicity.

[0153] With reference to step 1 to step 3, it can be learned that in this embodiment, that the processing system determines the target risk control policy in the online and offline multi-dimensional manner is equivalent to adaptively adjust the online risk level in the offline manner, to improve accuracy and reliability of determining the target risk control policy.

[0154] With reference to the above-mentioned analysis, it can be learned that, in this specification, a manner of determining the target risk control policy in the online single-dimensional manner is provided, and a manner of determining the target risk control policy in the online and offline multi-dimensional manner is provided, to implement flexibility and diversity of determining the target risk control policy. It should be noted that the above-mentioned two manners of "determining the target risk control policy in the online single-dimensional manner" and "determining the target risk control policy in the online and offline multi-dimensional manner" can be flexibly selected based on an application scenario. For example, in some cases, the former is selected, and in some cases, the latter is selected. This is not limited in this specification.

[0155] S303: Perform risk identification on the target event based on the target risk control policy, to determine whether the target event is a risk event.

[0156] With reference to the above-mentioned analysis, it can be learned that the processing system can obtain the target risk control policy by performing S301 and S302. Correspondingly, in S303, to be specific, when the target risk control policy is obtained, the processing system can perform risk control processing on the target event. For example, the processing system can determine, based on the target risk control policy, whether the target event is a risk event, to obtain a determining result of whether the target event is the risk event.

[0157] Based on S301 to S303, it can be learned that the processing system can perform online real-time detection on an event, and dynamically select the target risk control policy when the target event is detected, to determine, based on the target risk control policy, whether the target

event is a risk event, and implement a real-time detection function of the risk event. In this way, the above-mentioned disadvantage of risk control hysteresis in the related technology can be avoided, and automatic risk control is implemented. In addition, risk identification is performed based on the dynamically selected target risk control policy, to avoid manual complexity and subjective processing. In this way, there is relatively high efficiency and accuracy.

[0158] In some embodiments, as shown in FIG. 5, based on S301 to S303, the event processing method in this specification can further include S304: When it is determined that the target event is a risk event, block the target event, and output blocking prompt information to the target user.

[0159] For example, the processing system performs risk identification on the target event based on the target risk control policy, and may obtain two different identification results. One identification result represents that the target event is a risk event, and the other identification result represents that the target event is not a risk event. For different identification results, the processing system can perform processing in different manners, to implement flexibility of risk control processing.

[0160] When the identification result represents that the target event is a risk event, in this embodiment, for the identification result representing that the target event is a risk event, to prevent a merchant, a platform, etc. from being attacked by the target event, the processing system blocks the target event, and outputs the blocking prompt information, to notify the target user that the target event is blocked.

[0161] For example, with reference to the marketing activity scenario, if the identification result represents that an event in which the target user requests to participate in a marketing activity is a risk event, and if the target user may be a get the best deal user, the processing system rejects the request of the target user to participate in the marketing activity, for example, rejects the request of the target user to receive a coupon, and outputs the blocking prompt information to the target user, to notify the target user that the request of the target user to receive the coupon is rejected.

[0162] For another example, with reference to the transaction scenario, if the identification result represents that a transaction event requested by the target user is a risk event, and if the target user may be a fake account user such as brushing, the processing system rejects the request of the target user to participate in a transaction, and outputs the blocking prompt information to the target user, to notify the target user that the transaction requested by the target user is rejected.

[0163] For descriptions of another application scenario, references can be made to descriptions

of the marketing activity scenario and the transaction scenario. Examples are not listed one by one here.

[0164] When the identification result represents that the target event is not a risk event, in some embodiments, the processing system can respond to the target event, and output response success prompt information to the target user.

[0165] For example, with reference to the marketing activity scenario, if the identification result represents that the event in which the target user requests to participate in the marketing activity is not a risk event, and if the target user is a normal user who participates in the marketing activity, the processing system allows the request of the target user to participate in the marketing activity, for example, allows the request of the target user to receive a coupon and issues a coupon to the target user, and outputs the response success prompt information to the target user, to notify the target user that the target user successfully receives a coupon.

[0166] For another example, with reference to the transaction scenario, if the identification result represents that the transaction event requested by the target user is not a risk event, and if the target user is a normal transaction user, the processing system allows the request of the target user to participate in the transaction, and outputs the response success prompt information to the target user, for example, outputs a transaction information confirmation interface, to notify the target user to continue the transaction.

[0167] Similarly, for descriptions of another application scenario, references can be made to descriptions of the marketing activity scenario and the transaction scenario. Examples are not listed one by one here.

[0168] In some embodiments, based on any one of the above-mentioned examples, for example, based on S301 to S304, or based on S301 to S303, the processing system can further analyze risk control trend information from one or more risk control dimensions, and can output the risk control trend information, so that a worker performs observation or performs corresponding processing; or can output corresponding warning information when the risk control trend information satisfies a preset condition, so that the worker performs related warning analysis and response coping.

[0169] With reference to the above-mentioned example, the processing system can further include a monitoring platform. The monitoring platform can be configured to analyze the risk control trend information from one or more risk control dimensions, and can output the risk control

trend information.

[0170] For ease of understanding, an example in which the processing system analyzes the risk control trend information based on S301 to S304 is used in FIG. 6. As shown in FIG. 6, the event processing method in this specification can further include S305 and S306 based on S301 to S304:

[0171] S305: Determine risk control trend information from a plurality of risk control dimensions based on risk control data related to the target event and risk control data related to a historical event in a historical time period, where the historical time period is before the trigger moment of the target event, and the risk control trend information represents a trend in which a risk control effect changes with time.

[0172] For example, the risk control data is data related to risk prevention and control of the target event, for example, data used to represent a risk level, a blocking level for blocking the target event, and/or blocking magnitude data. Examples are not listed one by one here.

[0173] Similarly, this embodiment sets no limitation on a time length of the historical time period, and can be determined by the processing system based on the requirement, the historical record, the manner such as the experiment, etc.

[0174] Different risk control dimensions correspond to different risk control trend information. In this embodiment, the processing system can separately determine risk control trend information respectively corresponding to all the risk control dimensions from the plurality of risk control dimensions. For example, for each risk control dimension, the processing system can determine, based on corresponding risk control data, information indicating that a risk control effect in the risk control dimension changes with time.

[0175] In some embodiments, the plurality of risk control dimensions include at least two of the following: a risk level change dimension, a risk event blocking rate change dimension, a fund loss change dimension, and a risk control index change dimension.

[0176] For ease of understanding of a reader, all the risk control dimensions are described separately.

[0177] For the risk level change dimension:

[0178] In a processing procedure of each event, the processing system can output the first risk level in real time after detecting the first risk level corresponding to the first time period including a current event. In this way, in the processing procedure of the target event, the processing system can obtain change trend information of the first risk level in the historical time period based on a

first risk level corresponding to the target event and a first risk level corresponding to each historical event in the historical time period.

[0179] For the risk event blocking rate change dimension:

[0180] In a processing procedure of each event, the processing system can output the blocking rate in real time after a blocking rate corresponding to the current event is detected. In this way, in the processing procedure of the target event, the processing system can obtain change trend information of the blocking rate in the historical time period based on a blocking rate corresponding to the target event and a blocking rate corresponding to each historical event in the historical time period.

[0181] For the fund loss change dimension:

[0182] In a processing procedure of each event, the processing system can output a fund loss corresponding to the current event in real time after detecting the fund loss. In this way, in the processing procedure of the target event, the processing system can obtain change trend information of the fund loss in the historical time period based on a fund loss corresponding to the target event and a fund loss corresponding to each historical event in the historical time period.

[0183] For the risk control index change dimension:

[0184] In a processing procedure of each event, the processing system can output a risk control index, for example, a write-off rate, corresponding to the current event in real time after detecting the risk control index. In this way, in the processing procedure of the target event, the processing system can obtain change trend information of the risk control index in the historical time period based on a risk control index corresponding to the target event and a risk control index corresponding to each historical event in the historical time period.

[0185] In this embodiment, corresponding risk control trend information is determined from at least two of the plurality of dimensions such as the risk level change dimension, the risk event blocking rate change dimension, the fund loss change dimension, and the risk control index change dimension, to implement diversity and flexibility of the determined risk control trend information. In particular, widespread trend change coverage can be implemented when risk control trend information corresponding to each risk control dimension is determined.

[0186] S306: Output the risk control trend information, and output the warning information when the risk control trend information satisfies the preset condition.

[0187] For example, when determining the risk control trend information, the processing

system can output the risk control trend information for use by the worker. In addition, the processing system can further determine whether the risk control trend information satisfies the preset condition, and output the warning information when the risk control trend information satisfies the preset condition.

[0188] With reference to the above-mentioned example, the risk control trend information is determined by the processing system from the plurality of risk control dimensions. Different risk control dimensions correspond to different risk control trend information. Correspondingly, different risk control trend information may also correspond to different preset conditions.

[0189] For example, when the risk control dimension includes the risk level change dimension, the risk control trend information can include the risk level change trend information, and the preset condition can include that the risk level change trend information represents that the risk level presents an increasing trend. Therefore, when the risk level change trend information determined by the processing system represents that the risk level presents an increasing trend, if the risk level change trend information represents that the risk level changes from a low risk level to a medium risk level and then changes to a high risk level, the processing system outputs the warning information, to attract an attention of the worker, help take a corresponding measure in a timely manner, and avoid a too high risk level.

[0190] For example, when the risk control dimension includes the risk event blocking rate change dimension, the risk control trend information can include blocking rate change trend information, and the preset condition can include that the blocking rate change trend information represents that the blocking rate represents an increasing trend. Therefore, when the blocking rate change trend information determined by the processing system represents that the blocking rate represents an increasing trend, if the blocking rate change trend information represents that the blocking rate changes from 1.0 to 1.2 and then changes to 1.5, the processing system outputs the warning information, to attract an attention of the worker, help take a corresponding measure in a timely manner, and avoid blocking a normal user due to a too high blocking rate.

[0191] Similarly, for the descriptions of risk control trend information respectively corresponding to the fund loss change dimension and the risk control index change dimension, references can be made to the above-mentioned implementation principles of the risk level change dimension and the risk event blocking rate change dimension. Details are not listed one by one here.

[0192] With reference to S305 and S306, it can be learned that in this embodiment, the processing system can determine and output the risk control trend information from the plurality of risk control dimensions with reference to the risk control data, to display the risk control trend information intuitively, so that the worker can detect real-time risk control processing, and the processing system can output the warning information based on the preset condition, to alert the worker to improve validity and reliability of risk control processing.

[0193] It should be noted that, the above-mentioned examples are merely used to describe examples of a possible implementation of the event processing method in this specification, and cannot be understood as a limitation on the implementation of the event processing method in this specification. For example, based on the above-mentioned technical concept, some of the above-mentioned technical features can be combined to obtain a new embodiment, a new technical feature can be added based on the above-mentioned example to obtain a new embodiment, some technical features can be reduced based on the above-mentioned example to obtain a new embodiment, some technical features in the above-mentioned example may be replaced with other technical features, or some technical features and orders in the above-mentioned example can be adjusted to obtain a new embodiment. Examples are not listed one by one here.

[0194] According to the above-mentioned technical concept, this specification further provides a computer-readable non-transitory storage medium. The computer-readable non-transitory storage medium stores at least one instruction set, and when the at least one instruction set is executed by a processor, steps of the event processing method described in this specification are implemented.

[0195] In some possible implementations, aspects of this specification can further be implemented in a form of a program product, including program code. When the program product runs on a computing device 200, the program code is used to enable the computing device 200 to perform steps of the event processing method described in this specification. The program product configured to implement the foregoing method can use a portable compact disc read-only memory (CD-ROM) that includes program code, and can run on the computing device 200. However, the program product in this specification is not limited thereto. In this specification, a readable storage medium can be any tangible medium that includes or stores a program, and the program can be used by or in combination with an instruction execution system. The program product can be any combination of one or more readable media. The readable medium can be a readable signal

medium or a readable storage medium. The readable storage medium can be, for example, an electrical system, apparatus, or device, a magnetic system, apparatus, or device, an optical system, apparatus, or device, an electromagnetic system, apparatus, or device, an infrared system, apparatus, or device, or a semiconductor system, apparatus, or device, or any combination thereof. More specific examples of the readable storage medium include: an electrical connection including one or more conducting wires, a portable disk, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage component, a magnetic storage component, or any proper combination thereof. The computer-readable storage medium can include a data signal propagated in a baseband or as part of a carrier, and carries readable program code. The propagated data signal can be in a plurality of forms, and includes but is not limited to an electromagnetic signal, an optical signal, or any proper combination thereof. The readable storage medium can further be any readable medium other than the readable storage medium, and the readable medium can be used to send, propagate, or transmit a program used by or in combination with an instruction execution system, apparatus, or component. The program code included in the readable storage medium can be transmitted in any proper medium, including but not limited to a wireless medium, a wired medium, optical cable, an RF medium, or any proper combination thereof. Program code for performing an operation of this specification can be written in any combination of one or more program design languages. The program design language includes an object-oriented program design language, for example, Java or C++, and further includes a conventional procedural program design language, for example, "C" language, or a similar program design language. The program code can be completely executed on the computing device 200, partially executed on the computing device 200, executed as an independent software package, partially executed on the computing device 200 and partially executed on a remote computing device, or completely executed on a remote computing device 200.

[0196] Collection, storage, use, processing, transmission, provision, disclosure, etc. of personal information (for example, personal information of a user in risk control data) of the user in the technical solutions in this specification all comply with related laws and regulations, and do not violate public order and good morals.

[0197] Specific embodiments of this specification are described above. Other embodiments

fall within the scope of the appended claims. In some cases, the actions or steps described in the claims can be performed in an order different from that in the embodiments, and the desired results can still be achieved. In addition, the process depicted in the accompanying drawings does not necessarily need a particular order or consecutive order to achieve the desired results. In some implementations, multitasking and parallel processing are possible or may be advantageous.

[0198] In conclusion, after reading the detailed disclosure, a person skilled in the art can understand that the detailed disclosure can be presented only in an example manner, and can impose no limitation. Although it is not explicitly stated here, a person skilled in the art can understand that the requirements of this specification include various proper changes, improvements, and modifications to the embodiments. These changes, improvements, and modifications are intended to be presented in this specification, and fall within the spirit and scope of the example embodiments of this specification.

[0199] In addition, some terms in this specification are used to describe the embodiments of this specification. For example, "an embodiment", "embodiments", and/or "some embodiments" mean that a particular feature, structure, or feature described with reference to the embodiments can be included in at least one embodiment of this specification. Therefore, it can be emphasized and understood that two or more of "embodiments", "one embodiment", or "alternative embodiments" in each part of this specification do not necessarily indicate the same embodiment. In addition, specific features, structures, or features can be properly combined in one or more embodiments of this specification.

[0200] It should be understood that in the above-mentioned descriptions of the embodiments of this specification, to help understand a feature, for the purpose of simplifying this specification, various features are combined in a single embodiment, accompanying drawing, or description thereof in this specification. However, this does not mean that the combination of these features is necessary. It is entirely possible for a person skilled in the art to mark some devices and understand the devices as separate embodiments when reading this specification. That is, the embodiments in this specification can also be understood as an integration of a plurality of secondary embodiments. Content of each secondary embodiment is also true when features are less than all features in one of the above-mentioned disclosed embodiments.

[0201] Each patent, patent application, publication of a patent application, and other materials, for example, articles, books, instructions, publications, documents, and products, that are cited in

this specification and that are other than any document that is inconsistent or conflict with this document or that imposes limiting impact on the widest scope of the claims can be incorporated here by reference and used for all purposes now or later associated with this document. In addition, the term in this document shall prevail when there is any inconsistency or conflict between the description, definition and/or use of a related term in any material and the description, definition and/or use of a related terms in this document.

[0202] Finally, it should be understood that the principles of the implementation solutions of this specification are described in the implementation solutions of the application disclosed in this specification. Other modified embodiments also fall within the scope of this specification. Therefore, the embodiments disclosed in this specification are merely examples and not limitations. A person skilled in the art can use an alternative configuration according to the embodiments of this specification to implement the application in this specification. Therefore, the embodiments of this specification are not limited to the embodiments accurately described in the application.

CLAIMS

What is claimed is:

1. An event processing method, comprising:

determining, in response to that a target event is triggered, a first risk level corresponding to a first time period comprising a trigger moment of the target event;

determining a target risk control policy based on the first risk level, wherein risk control policies determined based on different risk levels have different prevention and control efforts; and

performing risk identification on the target event based on the target risk control policy, to determine whether the target event is a risk event.

2. The method according to claim 1, wherein the trigger moment of the target event is used as an end moment of the first time period, and the determining a first risk level corresponding to a first time period comprising a trigger moment of the target event comprises:

obtaining event information of a plurality of historical events triggered in the first time period; and

determining the first risk level corresponding to the first time period based on the event information of the plurality of historical events.

3. The method according to claim 2, wherein the determining the first risk level corresponding to the first time period based on the event information of the plurality of historical events comprises:

determining a current index value corresponding to at least one preset risk control index based on the event information of the plurality of historical events; and

determining the first risk level corresponding to the first time period based on the current index value corresponding to the at least one preset risk control index and a preset mapping relationship, wherein the preset mapping relationship is used to represent a correspondence between an index value corresponding to the at least one preset risk control index and a risk level.

4. The method according to claim 1, wherein the determining a target risk control policy based on the first risk level comprises:

obtaining a second risk level corresponding to a second time period comprising the trigger moment of the target event, wherein the second risk level is determined based on event information of a historical event that occurs in a third time period, the second time period comprises the first time period, and the third time period is before the second time period;

determining a target risk level based on the first risk level and the second risk level; and

using a risk control policy corresponding to the target risk level in a plurality of preset risk control policies as the target risk control policy.

5. The method according to claim 4, wherein the determining the target risk level based on the first risk level and the second risk level comprises one of the following:

determining the first risk level as the target risk level if the first risk level is higher than or equal to the second risk level; or

determining the second risk level as the target risk level if the first risk level is higher than or equal to the second risk level; or

selecting a risk level corresponding to a preset prevention and control effort requirement for the target event from the first risk level and the second risk level as the target risk level based on the preset prevention and control effort requirement.

6. The method according to claim 1, wherein the determining a target risk control policy based on the first risk level comprises:

using a risk control policy corresponding to the first risk level in a plurality of preset risk control policies as the target risk control policy.

7. The method according to claim 1, wherein the target event is one of the following:

a transaction event triggered by a target user;

a payment event triggered by the target user; and

an event that the target user requests to participate in a marketing activity.

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

when it is determined that the target event is a risk event, blocking the target event, and outputting blocking prompt information to the target user.

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

determining risk control trend information from a plurality of risk control dimensions based on risk control data related to the target event and risk control data related to a historical event in a historical time period, wherein the historical time period is before the trigger moment of the target event, and the risk control trend information represents a trend in which a risk control effect changes with time; and

outputting the risk control trend information, and outputting warning information when the risk control trend information satisfies a preset condition.

10. The method according to claim 9, wherein the plurality of risk control dimensions comprise at least two of the following:

a risk level change dimension;

a risk event blocking rate change dimension;

a fund loss change dimension; and

a risk control index change dimension.

11. An event processing system, comprising:

at least one storage medium, storing at least one instruction set, to perform event processing; and

at least one processor, communicatively connected to the at least one storage medium, wherein when running, the at least one processor reads the at least one instruction set, and performs the following operations based on an indication of the at least one instruction set:

determining, in response to that a target event is triggered, a first risk level corresponding to a first time period comprising a trigger moment of the target event;

determining a target risk control policy based on the first risk level, wherein risk control policies determined based on different risk levels have different prevention and control efforts; and

performing risk identification on the target event based on the target risk control policy, to determine whether the target event is a risk event.

12. The processing system according to claim 11, wherein to determine the first risk level corresponding to the first time period comprising the trigger moment of the target event, the at least one processor performs the following operations:

obtaining event information of a plurality of historical events triggered in the first time period; and

determining the first risk level corresponding to the first time period based on the event information of the plurality of historical events.

13. The processing system according to claim 12, wherein to determine the first risk level corresponding to the first time period, the at least one processor performs the following operations:

determining a current index value corresponding to at least one preset risk control index based on the event information of the plurality of historical events; and

determining the first risk level corresponding to the first time period based on the current index value corresponding to the at least one preset risk control index and a preset mapping

relationship, wherein the preset mapping relationship is used to represent a correspondence between an index value corresponding to the at least one preset risk control index and a risk level.

14. The processing system according to claim 11, wherein to determine the target risk control policy, the at least one processor performs the following operations:

obtaining a second risk level corresponding to a second time period comprising the trigger moment of the target event, wherein the second risk level is determined based on event information of a historical event that occurs in a third time period, the second time period comprises the first time period, and the third time period is before the second time period;

determining a target risk level based on the first risk level and the second risk level; and

using a risk control policy corresponding to the target risk level in a plurality of preset risk control policies as the target risk control policy.

15. The processing system according to claim 14, wherein to determine the target risk level, the at least one processor performs one of the following:

determining the first risk level as the target risk level if the first risk level is higher than or equal to the second risk level; or

determining the second risk level as the target risk level if the first risk level is higher than or equal to the second risk level; or

selecting a risk level corresponding to a preset prevention and control effort requirement for the target event from the first risk level and the second risk level as the target risk level based on the preset prevention and control effort requirement.

16. The processing system according to claim 11, wherein to determine the target risk control policy, the at least one processor performs the following operations:

using a risk control policy corresponding to the first risk level in a plurality of preset risk control policies as the target risk control policy.

17. The processing system according to claim 11, wherein the target event is one of the following:

a transaction event triggered by a target user;

a payment event triggered by the target user; and

an event that the target user requests to participate in a marketing activity.

18. The processing system according to claim 17, wherein the at least one processor performs the following operation:

when it is determined that the target event is a risk event, blocking the target event, and outputting blocking prompt information to the target user.

19. The processing system according to claim 11, wherein the at least one processor performs the following operations:

determining risk control trend information from a plurality of risk control dimensions based on risk control data related to the target event and risk control data related to a historical event in a historical time period, wherein the historical time period is before the trigger moment of the target event, and the risk control trend information represents a trend in which a risk control effect changes with time; and

outputting the risk control trend information, and outputting warning information when the risk control trend information satisfies a preset condition.

20. A computer-readable non-transitory storage medium, wherein the computer-readable non-transitory storage medium stores at least one instruction set, and when the at least one instruction set is executed by at least one processor, the method according to any one of claims 1 to 10 is implemented.