FUND SECURITY DETECTION METHOD AND APPARATUS IN SERVICE FIELD, AND COMPUTER SYSTEM

TECHNICAL FIELD

[0001] One or more embodiments of this specification relate to the field of computer technologies, and in particular, to a fund security detection method and apparatus in a service field, and a computer system.

BACKGROUND

[0002] In some service fields, as services progress, a large amount of service field data, for example, merchant charging data, user transaction data, and transaction data between enterprises, is generated on a service platform. The service field data or the transaction data involves changes in funds, and risk control needs to be performed to discover a fund security risk on the service platform in a timely manner and make an alarm. In addition, the service field data on the service platform includes privacy data, and privacy protection needs to be performed during use.

[0003] Currently, an improved solution is expected to more effectively detect fund security on the service platform.

SUMMARY

[0004] One or more embodiments of this specification describe a fund security detection method and apparatus in a service field, and a computer system, to more effectively perform security detection on fund security on a service platform. Specific technical solutions are as follows:

[0005] According to a first aspect, an embodiment provides a fund security detection method in a service field, including: obtaining fund transaction data generated on an online platform at a current moment, and determining current time series data corresponding to a current time period based on the fund transaction data; obtaining historical time series data corresponding to each of a plurality of historical time periods, where any historical time series data is determined based on fund transaction data in a corresponding historical time period; determining fluctuation trend data

corresponding to a plurality of pieces of historical time series data; comparing the current time series data with the fluctuation trend data; and determining, based on a comparison result, whether there is a fund security risk in the current time period.

[0006] According to a second aspect, an embodiment provides a computer system, including a storage, a processor, and a computer program stored in the storage and capable of running on the processor. When the processor executes the program, the following steps are implemented: obtaining fund transaction data generated on an online platform at a current moment, and determining current time series data corresponding to a current time period based on the fund transaction data; obtaining historical time series data corresponding to each of a plurality of historical time periods, where any historical time series data is determined based on fund transaction data in a corresponding historical time period; determining fluctuation trend data corresponding to a plurality of pieces of historical time series data; comparing the current time series data with the fluctuation trend data; and determining, based on a comparison result, whether there is a fund security risk in the current time period.

[0007] According to a third aspect, an embodiment provides a fund security detection apparatus in a service field, including: an online data obtaining module, configured to: obtain fund transaction data generated on an online platform at a current moment, and determine current time series data corresponding to a current time period based on the fund transaction data; a historical data obtaining module, configured to obtain historical time series data corresponding to each of a plurality of historical time periods, where any historical time series data is determined based on fund transaction data in a corresponding historical time period; a fluctuation trend determining module, configured to determine fluctuation trend data corresponding to a plurality of pieces of historical time series data; a module for comparing two types of data, configured to compare the current time series data with the fluctuation trend data; and a fund security determining module, configured to determine, based on a comparison result, whether there is a fund security risk in the current time period.

[0008] According to a fourth aspect, an embodiment provides a computer-readable nonvolatile storage medium. The storage medium stores a computer program, and when the computer program is executed by a processor, the method according to any implementation of the first aspect is implemented.

[0009] In the method and the apparatus provided in the embodiments of the specification,

security comparison is performed between current time series data on an online platform in a current time period and fluctuation trend data reflected by a plurality of pieces of historical time series data, so that more effective fund security detection can be performed on service field data generated on the online platform. A fluctuation trend of historical time series data in a time period can better reflect stability of service field data. Therefore, when the current time series data corresponding to fund transaction data at a current moment does not match the fluctuation trend, it is highly probably that there is a fund security problem. Therefore, the above method can more effectively perform security detection on fund security on the service platform.

BRIEF DESCRIPTION OF DRAWINGS

[0010] To describe the technical solutions in the embodiments of the present invention 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 the present invention, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0011] FIG. 1 is a schematic diagram of an implementation scenario of an embodiment disclosed in this specification;

[0012] FIG. 2 is a schematic flowchart of a fund security detection method according to an embodiment;

[0013] FIG. 3A is a schematic diagram of a principle of a fluctuation detection warning;

[0014] FIG. 3B is a schematic diagram of a principle of a drop to zero detection warning;

[0015] FIG. 4 is a schematic flowchart of another fund security detection method according to an embodiment;

[0016] FIG. 5 is a schematic block diagram of a fund security detection apparatus in a service field according to an embodiment; and

[0017] FIG. 6 is a schematic diagram of a structure of a computer system according to an embodiment.

DESCRIPTION OF EMBODIMENTS

[0018] The solutions provided in this specification are described below with reference to the

accompanying drawings.

[0019] In a service field, online services on a service platform generate a large amount of service field data. The service field data is data related to funds and transactions, and is also referred to as fund transaction data. User privacy data included in the fund transaction data is obtained after a user consent is sought. Fund transaction data is generated on the online service platform every day. The fund transaction data involves different service lines, and is generated by different objects in different transaction methods. To perform fund security detection on the fund transaction data, security detection is performed when each transaction is generated on the online service platform. For example, it can be detected whether an amount of the transaction exceeds a limit and whether a fund receiver involved in the transaction is a risky user. In this detection manner, fund security can be detected to some extent.

[0020] To perform more effective fund security detection, an embodiment of this specification provides a fund security detection method. FIG. 1 is a schematic diagram of an implementation scenario of an embodiment disclosed in this specification. An online service platform (briefly referred to as an online platform below) and a detection device are included. The online platform is a platform for executing services. In a service execution process, a plurality of pieces of fund transaction data are generated on the online platform in real time. The fund transaction data is service field data. The online platform can send the fund transaction data generated in real time to the detection device. The detection device receives the fund transaction data sent by the online platform, performs fund security detection based on the fund transaction data, and gives a warning when a security risk is detected. In addition, there can be various configurations, including a data access configuration, a detection configuration, an alarm configuration, a noise reduction configuration, and the like, for the detection device. Detection warnings given by the detection device include a fluctuation detection warning and a drop to zero detection warning.

[0021] This embodiment is described below in detail with reference to FIG. 2.

[0022] FIG. 2 is a schematic flowchart of a fund security detection method according to an embodiment. The method is performed by a detection device. The detection device can be implemented by any apparatus, device, platform, device cluster, or the like that has computing and processing capabilities. During specific implementation, the detection device can be implemented by another device independent of the online service platform in FIG. 1, or can be implemented by a device or a module inside the online service platform. The method includes the following steps.

[0023] Step S210: The detection device obtains fund transaction data generated on an online platform at a current moment t1, and determines current time series data D1 corresponding to a current time period T1 based on the fund transaction data.

[0024] A time period is preset specified duration. For example, the time period can be one day, two days, three days, one week, two weeks, three weeks, or one month. There is a time sequence between a plurality of time periods. For example, if one day is used as a time period, May 1 and May 2 are different time periods, and May 2 is a time period after May 1. When one week is used as a time period, a time period from May 6 to May 12 is a time period before a time period from May 13 to May 19.

[0025] On a time-period basis, a large amount of fund transaction data continuously generated on the online platform can be accumulated or averaged. In this way, the obtained data is arranged in a time sequence, that is, time series data corresponding to different time periods is formed. The time series data has a time series attribute. A plurality of pieces of time series data can form a time series. The time series is a series formed by arranging values of a same statistical indicator in a time sequence. For example, if one day is used as a time period, time series data on May 1, time series data on May 2, and time series data on May 3 can be obtained.

[0026] The above current moment t1 is relative to a historical moment. The historical moment is a moment before the current moment t1, and is a moment earlier than the current moment t1. When receiving the fund transaction data that is at the current moment t1 and that is sent by the online platform, the detection device can accumulate or average all fund transaction data in the current time period when the current time period arrives, to obtain time series data corresponding to the current time period T1 as the current time series data D1. All the fund transaction data in the current time period T1 includes the fund transaction data at the current moment t1. The above accumulation or averaging operation can be replaced with another operation, for example, an operation of calculating a median or a mode.

[0027] The fund transaction data is described below. One piece of fund transaction data can include a plurality of fields and field values of the plurality of fields. For example, these fields can include a service line, a merchant identity (ID), a user ID, a transaction currency, a transaction method, a transaction indicator, an amount, and a transaction time. The service line can include, for example, an international service and a domestic service. The merchant ID and the user ID are objects involved in a transaction. The transaction indicator is an actual service name of the

transaction amount, for example, can include an amount charged by a merchant and an amount transferred by the merchant to another party. The transaction method includes an online transaction, an offline transaction, and the like.

[0028] The online platform can periodically send a fund transaction data table to the detection device. Each row in the fund transaction data table is one piece of fund transaction data. The above current moment t1 can be a generation moment of the fund transaction data table. When receiving the fund transaction data table sent by the online platform, the detection device can accumulate or average data in the current time period T1 based on data in the fund transaction data table, to obtain the current time series data D1.

[0029] This accumulation or averaging operation can be accumulating or averaging target fields in the fund transaction data. For example, transaction amount field values in the fund transaction data can be accumulated. Alternatively, other data in the fund transaction data can be accumulated or averaged. For example, quantities of transactions in the current time period T1 can be accumulated. A data object for accumulation or averaging can further include transaction duration and the like. The data object for accumulation or averaging is not limited to the above listed data objects. The accumulation operation or the averaging operation can be selected based on specific service requirements and configurations.

[0030] That is, the time series data (including the current time series data and the historical time series data) can be an accumulated value of the amounts, an accumulated value of the quantities of transactions, an accumulated value or an average of the transaction duration, or the like. For example, when a day is used as a time unit, charge amounts of a merchant in a day can be accumulated. For example, if a merchant executes 10000 transactions on May 1, and an amount of a single transaction is approximately 10 yuan, transaction amounts of the 10000 transactions of the merchant on May 1 are accumulated to obtain a total transaction amount of 100000 yuan; or quantities of transactions of the merchant on May 1 can be accumulated to obtain 10000 transactions. Examples of a plurality of pieces of fund transaction data are recorded in Table 1.

Table 1

Service line	Merchant ID	Transaction currency	Transaction method	Charge amount	Transaction time
Domestic service	x1	RMB	Online payment	10 yuan	10:20 on May 1, 2025
Domestic service	x2	RMB	Online payment	11 yuan	12:45 on May 1, 2025
International service	x3	RMB	Online payment	8 yuan	19:50 on May 1, 2025
...	...	...	...	...	...

[0031] The fund transaction data table obtained by the detection device at the current moment t1 can be similar to the fund transaction data in Table 1. In addition, the fund transaction data table can include a type such as a full table and an incremental table. The full table is a table including fund transaction data at all times, and the incremental table is a table including only newly added fund transaction data.

[0032] The detection device can filter the data in the fund transaction data table based on the data access configuration. The data access configuration includes a preset filtering field. The detection device can filter, based on the preset filtering field, field data included in the fund transaction data generated at the current moment t1, and determine the current time series data corresponding to the current time period T1 based on selected data. Specifically, for the selected data, all data that belongs to the current time period T1 can be accumulated or averaged, to obtain the current time series data D1 corresponding to the current time period T1.

[0033] The filtering field in the data access configuration can be a field in the fund transaction data, for example, can include filtering for a service line, an object, a transaction indicator, and a transaction method. The filtering field can further include setting of a time period. For example, filtering can be performed at a granularity of a day, week, or month. For example, when a day is used as a time period, fund transaction data in a day can be selected to perform an accumulation or averaging operation. Through data access filtering, filtering of a service line, an object scenario, and a time granularity can be implemented in this embodiment, to process target data.

[0034] In this embodiment, by performing the operation in step S210, data can be processed and detected on the time-period basis, so that the data can be macroscopically detected and processed. Compared with that in a manner of performing security detection each time a transaction is generated, fund security can be macroscopically grasped.

[0035] Step S220: Obtain historical time series data D2 corresponding to each of a plurality of historical time periods T2. Any historical time series data D2 is determined based on fund transaction data in a corresponding historical time period T2. The plurality of historical time periods T2 can be obtained from historical data stored in the detection device.

[0036] A quantity of historical time periods T2 can also be referred to as a detection step, and can be preset. In addition, the historical time periods T2 can be determined based on the current time period and the preset detection step, that is, the obtained historical time series data is historical time series data corresponding to each of a plurality of historical time periods in the preset detection step before the current time period.

[0037] For example, if the current time period is May 1, and the preset detection step can be 10 days, the historical time periods T2 can include historical time series data corresponding to each of 10 days from April 30 to April 21.

[0038] Each piece of historical time series data is obtained in a manner in step S210. That is, each piece of historical time series data is obtained by accumulating or averaging all fund transaction data in a corresponding historical time period.

[0039] The detection device can obtain a configuration parameter such as the preset detection step by using the detection configuration.

[0040] Step S230: Determine fluctuation trend data TR corresponding to a plurality of pieces of historical time series data D2.

[0041] During implementation of this step, the fluctuation trend data TR can be determined by using a statistical value corresponding to the plurality of pieces of historical time series data D2. For example, an average μ and a standard deviation σ of the plurality of pieces of historical time series data D2 can be calculated, and the corresponding fluctuation trend data TR can be determined based on the average μ and the standard deviation σ.

[0042] As mentioned in the above content, the time series data (including the current time series data D1 and the historical time series data D2) can be a value obtained by accumulating or averaging the transaction amounts, the quantities of transactions, or the transaction duration.

Values of the plurality of pieces of historical time series data D2 fluctuate. To find instructive data from these values, the fluctuation trend data can be determined based on some methods.

[0043] For example, the fluctuation trend data TR can be set to include an upper threshold limit U and a lower threshold limit L of data fluctuation. The upper threshold limit U and the lower threshold limit L can be determined based on a range obtained by adding n times the standard deviation σ to the average μ and subtracting n times the standard deviation σ from the average μ. Here, n can be 1, 2, 3, 4, or the like. For example, the upper threshold limit is $U=\mu+3\sigma$, and the lower threshold limit is $L=\mu-3\sigma$. Based on the above manner, the upper threshold limit U and the lower threshold limit L can be determined in another similar manner. The upper threshold limit U and the lower threshold limit L can alternatively be represented in a form of a piecewise function or another function, and are not limited to being represented by using a linear function. The fluctuation trend data is not limited to setting of the upper threshold limit U and the lower threshold limit L, and other setting can be performed. For example, a fluctuation rate can be calculated as the fluctuation trend data by using the average μ and the standard deviation σ. Alternatively, a trend line can be obtained by determining a target high point and low point from the plurality of pieces of historical time series data.

[0044] Step S240: Compare the current time series data D1 with the fluctuation trend data TR, to obtain a comparison result.

[0045] Step S250: Determine, based on the comparison result, whether there is a fund security risk in the current time period T1, to obtain a fund security risk result.

[0046] When the fluctuation trend data TR includes the upper threshold limit U and the lower threshold limit L, it can be determined whether the current time series data D1 exceeds a range including the upper threshold limit U and the lower threshold limit L. The comparison result can include that the current time series data D1 exceeds the range including the upper threshold limit U and the lower threshold limit L and the current time series data D1 does not exceed the range including the upper threshold limit U and the lower threshold limit L. When the current time series data D1 exceeds the range including the upper threshold limit U and the lower threshold limit L, the following case is included: A value of the current time series data D1 is greater than the upper threshold limit U, or a value of the current time series data D1 is less than the lower threshold limit L. When the current time series data D1 does not exceed the range including the upper threshold limit U and the lower threshold limit L, the following case is included: A value of the current time

series data D1 is greater than or equal to the lower threshold limit L, and the value of the current time series data D1 is less than or equal to the upper threshold limit U.

[0047] When the comparison result indicates that the current time series data D1 exceeds the range including the upper threshold limit U and the lower threshold limit L, it is determined that there is a fund security risk in the current time period T1. The detection device can send an alarm notification to the online service platform when determining that there is a fund security risk. When the comparison result indicates that the current time series data D1 does not exceed the range including the upper threshold limit U and the lower threshold limit L, it indicates that there is no fund security risk in the current time period T1.

[0048] FIG. 3A is a schematic diagram of a principle of a fluctuation detection warning. A horizontal axis of a coordinate system represents a time, and a vertical axis represents time series data. A time and a value of each of the plurality of pieces of historical time series data D2 are respectively used as a horizontal coordinate value and a vertical coordinate value, are marked in the coordinate system, and are represented by using small circles. Fluctuation of the historical time series data can be seen from FIG. 3A. The upper threshold limit U and the lower threshold limit L are separately marked in the coordinate system. It can be seen that the upper threshold limit U and the lower threshold limit L are approximately distributed on upper and lower sides of the plurality of pieces of historical time series data D2. When the current time series data D1 is obtained, it can be found that the value of D1 exceeds the upper threshold limit U. In this case, an alarm can be made. The fluctuation trend data TR is calculated by using historical time series data D1 in the detection step. In addition, as time goes by, the detection step also moves to the right. That is, a historical time period is determined based on the current time period, and updated historical time series data can be used. The updated historical time series data has higher reference value, and therefore detection can be more accurate.

[0049] The detection can be referred to as fluctuation detection, that is, the current time series data is detected based on the fluctuation trend data. Through the detection, an abnormality of a sudden increase or decrease in values can be detected. The fluctuation trend data can also be referred to as a water level baseline. The water level baseline is a specific description of a specific service indicator arranged in a time dimension. By using the water level baseline as a reference, an abnormality can be more accurately detected from a large amount of time series data.

[0050] For example, if a merchant charges many times in a day, for example, the merchant

charges 10000 times, and 10 yuan is charged each time, a result is clearly proper when security check is performed on a single 10-yuan transaction. However, if a total charge amount in a day reaches 100000 yuan, it is likely that the amount is an improper value exceeding the upper threshold limit. By using the method in this embodiment, it can be determined that there is a fund risk, and the online service platform is alarmed.

[0051] In addition to fluctuation abnormality detection, drop to zero detection is also a data abnormality, and is also a dangerous situation that requires an alarm.

[0052] To improve effectiveness of fund security detection, an embodiment of this specification further provides a fund security detection method. The method is obtained based on the embodiment in FIG. 2. FIG. 4 is a schematic flowchart of another fund security detection method according to an embodiment. The method includes the following steps.

[0053] Step S410: A detection device obtains fund transaction data generated on an online platform at a current moment t1, and determines current time series data D1 corresponding to a current time period T1 based on the fund transaction data.

[0054] Step S420: Obtain historical time series data D2 corresponding to each of a plurality of historical time periods T2.

[0055] Steps S410 and S420 are respectively the same as steps S210 and S220. For specific descriptions, references can be made to the embodiment in FIG. 2. Details are omitted here for simplicity.

[0056] Step S430: After the historical time series data corresponding to each of the plurality of historical time periods T2 is obtained, determine whether a value of the current time series data D1 is 0. When the value of the current time series data D1 is 0, the following first determining is performed: determining whether historical time series data D2 in a first quantity, that is, m1, of historical time periods T2 before the current time period T1 is 0; and determining, based on a determining result of the first determining, whether there is a data drop to zero risk, to obtain a drop to zero risk result. When the current time series data D1 is not 0, the first determining is not performed.

[0057] The first quantity, that is, m1, of historical time periods T2 are m1 consecutive time periods, and can be time periods consecutive to (that is, immediately adjacent to) the current time period. The first quantity m1 can be preset, and can be used as a parameter in a detection configuration. A value of the first quantity m1 can be set based on experience, for example, can be

set to a relatively small value such as 0, 1, 2, or 3. When m1 is set to 0, the first determining is not performed.

[0058] The determining result of the first determining includes yes and no. When the determining result is yes, that is, it is determined that all of values of m1 pieces of historical time series data D2 are 0, it indicates that there are a plurality of pieces of consecutive historical time series data D2 that are 0. This case is an abnormal phenomenon, it can be determined that there is a drop to zero risk, and a drop to zero alarm is made, that is, a drop to zero alarm notification is sent. When the determining result is no, that is, it is determined that some of values of m1 pieces of historical time series data D2 are 0 or none of values of m1 pieces of historical time series data D2 are 0, it indicates that a current case of a drop to 0 is not an abnormal case, and it is determined that there is no drop to zero risk.

[0059] To more accurately determine the drop to zero risk, when step S430 is performed and the determining result of the first determining is yes, that is, when a value of time series data in several consecutive time periods is 0, the following second determining can continue to be performed: determining whether historical time series data D2 in a second quantity, that is, m2, of historical time periods before the first quantity, that is, m1, of historical time periods is not 0; and when a determining result of the second determining is yes, determining that there is a data drop to zero risk, to obtain a drop to zero risk result.

[0060] The second quantity, that is, m2, of historical time periods are m2 consecutive time periods, and can be time periods consecutive to (that is, immediately adjacent to) to the first quantity, that is, m1, of historical time periods. The second quantity m2 can be preset, and can be used as a parameter in the detection configuration. A value of the second quantity m2 can be set based on experience, and can be set to a value greater than the first quantity m1.

[0061] The determining result of the second determining includes yes and no. When the determining result is yes, that is, it is determined that none of values of m2 pieces of historical time series data D2 are 0, it indicates that there are currently a plurality of pieces of consecutive time series data that are 0, and a plurality of pieces of consecutive historical time series data before the plurality of pieces of consecutive time series data are not 0. This case is an abnormal phenomenon, it can be determined that there is a drop to zero risk, and a drop to zero alarm is made, that is, a drop to zero alarm notification is sent to the online service platform. When the determining result is no, that is, it is determined that some of values of m2 pieces of historical time

series data D2 are 0 or all of values of m2 pieces of historical time series data D2 are 0, it indicates that a current case of a drop to 0 is not an abnormal case, and it is determined that there is no drop to zero risk.

[0062] It can be understood that it is more likely that a case in which there is no drop to zero in a consecutive time period and then there is a drop to zero in several consecutive days is an abnormal case. Therefore, the first determining and the second determining are performed, to reduce noise, reduce incorrect drop to zero reporting, and achieve higher accuracy of drop to zero risk detection.

[0063] FIG. 3B is a schematic diagram of a principle of a drop to zero detection warning. A horizontal axis of a coordinate system represents a time unit, that is, day, and a vertical axis represents time series data. A time and a value of each of the plurality of pieces of historical time series data D2 are respectively used as a horizontal coordinate value and a vertical coordinate value, are marked in the coordinate system, and are represented by using small circles. When data including the current time series data D1 in a drop to zero step is 0, it indicates that there is a drop to zero in several consecutive days. When historical time series data D2 in a detection step before the drop to zero step is not 0, a drop to zero warning can be given in the current time period. The drop to zero step is the above first quantity, that is, m1, of time periods, and the detection step is the above second quantity, that is, m2, of time periods.

[0064] In this embodiment, a drop to zero warning is given for the time series data, does not depend on real data for triggering, and is an active detection warning. That is, in this embodiment, when no transaction occurs on an object such as a merchant, a security warning can also be given, and this warning does not depend on occurrence of a transaction. For example, if a merchant has no charge transaction within two days, a problem cannot be discovered through conventional single transaction check, but a problem can be discovered through drop to zero detection in this embodiment, and a timely warning is given.

[0065] The embodiment in FIG. 4 can be used in combination with the embodiment in FIG. 2, to improve effectiveness of fund security detection.

[0066] In this specification, "first" in words such as first determining and first quantity, corresponding "second" (if present) in the specification, and the like are merely used for ease of distinguishing and description, and have no limitation meaning.

[0067] Specific embodiments of this specification are described above, and 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 a sequence different from that in the embodiments and desired results can still be achieved. In addition, the process depicted in the accompanying drawings does not necessarily need a particular sequence or consecutive sequence to achieve the desired results. In some implementations, multitasking and parallel processing are possible or may be advantageous.

[0068] FIG. 5 is a schematic block diagram of a fund security detection apparatus in a service field according to an embodiment. The apparatus embodiment corresponds to the method embodiments shown in FIG. 2 and FIG. 4. The apparatus 500 is deployed in a detection device. The apparatus 500 includes the following modules: an online data obtaining module 510, configured to: obtain fund transaction data generated on an online platform at a current moment, and determine current time series data corresponding to a current time period based on the fund transaction data; a historical data obtaining module 520, configured to obtain historical time series data corresponding to each of a plurality of historical time periods, where any historical time series data is determined based on fund transaction data in a corresponding historical time period; a fluctuation trend determining module 530, configured to determine fluctuation trend data corresponding to a plurality of pieces of historical time series data; a module for comparing two types of data 540, configured to compare the current time series data with the fluctuation trend data; and a fund security determining module 550, configured to determine, based on a comparison result, whether there is a fund security risk in the current time period.

[0069] In an implementation, that an online data obtaining module 510 determines current time series data corresponding to a current time period based on the fund transaction data includes: accumulating or averaging all fund transaction data in the current time period, to obtain the current time series data corresponding to the current time period, where all the fund transaction data in the current time period includes the fund transaction data at the current moment.

[0070] In an implementation, the historical data obtaining module 520 is specifically configured to obtain historical time series data corresponding to each of a plurality of historical time periods in a preset detection step before the current time period.

[0071] In an implementation, that an online data obtaining module 510 determines current time series data corresponding to a current time period based on the fund transaction data includes: filtering, based on a preset filtering field, field data included in the fund transaction data generated

at the current moment; and determining the current time series data corresponding to the current time period based on selected data.

[0072] In an implementation, the fluctuation trend determining module 530 includes: a calculation submodule (not shown in the figure), configured to calculate an average and a standard deviation of the plurality of pieces of historical time series data; and a determining submodule (not shown in the figure), configured to determine the corresponding fluctuation trend data based on the average and the standard deviation.

[0073] In an implementation, the fluctuation trend data includes an upper threshold limit and a lower threshold limit of data fluctuation; and the determining submodule is specifically configured to determine the upper threshold limit and the lower threshold limit based on a range obtained by adding n times the standard deviation to the average and subtracting n times the standard deviation from the average.

[0074] In an implementation, the fluctuation trend data includes an upper threshold limit and a lower threshold limit of data fluctuation; and the fund security determining module 550 is configured to: when the current time series data exceeds a range including the upper threshold limit and the lower threshold limit, determine that there is a fund security risk in the current time period.

[0075] In an implementation, the apparatus 500 further includes a value drop to zero determining module 560 and a drop to zero risk determining module 570; the value drop to zero determining module 560 is configured to: after the historical time series data corresponding to each of the plurality of historical time periods is obtained, when a value of the current time series data is 0, perform the following first determining: determining whether historical time series data in a first quantity of historical time periods before the current time period is 0; and the drop to zero risk determining module 570 is configured to determine, based on a determining result of the first determining, whether there is a data drop to zero risk.

[0076] In an implementation, the drop to zero risk determining module 570 is specifically configured to: when the determining result of the first determining is yes, perform the following second determining: determining whether historical time series data in a second quantity of historical time periods before the first quantity of historical time periods is 0; and when a determining result of the second determining is no, determine that there is a data drop to zero risk.

[0077] The apparatus embodiments correspond to the method embodiments. For specific

descriptions, references can be made to the descriptions in the method embodiments. Details are omitted here for simplicity. The apparatus embodiments are obtained based on the corresponding method embodiments, and have the same technical effects as the corresponding method embodiments. For specific descriptions, references can be made to the corresponding method embodiments.

[0078] The specification also provides a computer-readable non-transitory storage medium, wherein the storage medium stores a computer program, which, when executed by a processor, can be used to perform one or more steps of one or more methods described or illustrated herein or provides functionality described or illustrated herein. Herein, the computer-readable non-transitory storage medium or media may include one or more semiconductor-based or other integrated circuits (ICs) (such, as for example, field-programmable gate arrays (FPGAs) or application-specific ICs (ASICs)), hard disk drives (HDDs), hybrid hard drives (HHDs), optical discs, optical disc drives (ODDs), magneto-optical discs, magneto-optical drives, floppy diskettes, floppy disk drives (FDDs), magnetic tapes, solid-state drives (SSDs), RAM-drives, SECURE DIGITAL cards or drives, any other suitable computer-readable non-transitory storage media, or any suitable combination of two or more of these, where appropriate. A computer-readable non-transitory storage medium may be volatile, non-volatile, or a combination of volatile and non-volatile, where appropriate.

[0079] The specification also provides a computer system. FIG. 6 illustrates an example computer system 1000. In particular embodiments, one or more computer systems 1000 perform one or more steps of one or more methods described or illustrated herein. In particular embodiments, one or more computer systems 1000 provide functionality described or illustrated herein. In particular embodiments, software running on one or more computer systems 1000 performs one or more steps of one or more methods described or illustrated herein or provides functionality described or illustrated herein. Particular embodiments include one or more portions of one or more computer systems 1000. Herein, reference to a computer system may encompass a computing device, and vice versa, where appropriate. Moreover, reference to a computer system may encompass one or more computer systems, where appropriate.

[0080] This disclosure contemplates any suitable number of computer systems 1000. This disclosure contemplates computer system 1000 taking any suitable physical form. As example and not by way of limitation, computer system 1000 may be an embedded computer system, a system-

on-chip (SOC), a single-board computer system (SBC) (such as, for example, a computer-on-module (COM) or system-on-module (SOM)), a desktop computer system, a laptop or notebook computer system, an interactive kiosk, a mainframe, a mesh of computer systems, a mobile telephone, a personal digital assistant (PDA), a server, a tablet computer system, or a combination of two or more of these. Where appropriate, computer system 1000 may include one or more computer systems 1000; be unitary or distributed; span multiple locations; span multiple machines; span multiple data centers; or reside in a cloud, which may include one or more cloud components in one or more networks. Where appropriate, one or more computer systems 1000 may perform without substantial spatial or temporal limitation one or more steps of one or more methods described or illustrated herein. As an example and not by way of limitation, one or more computer systems 1000 may perform in real time or in batch mode one or more steps of one or more methods described or illustrated herein. One or more computer systems 1000 may perform at different times or at different locations one or more steps of one or more methods described or illustrated herein, where appropriate.

[0081] In particular embodiments, computer system 1000 includes a processor 1002, memory 1004, storage 1006, an input/output (I/O) interface 1008, a communication interface 1010, and a bus 1012. Although this disclosure describes and illustrates a particular computer system having a particular number of particular components in a particular arrangement, this disclosure contemplates any suitable computer system having any suitable number of any suitable components in any suitable arrangement.

[0082] In particular embodiments, processor 1002 includes hardware for executing instructions, such as those making up a computer program. As an example and not by way of limitation, to execute instructions, processor 1002 may retrieve (or fetch) the instructions from an internal register, an internal cache, memory 1004, or storage 1006; decode and execute them; and then write one or more results to an internal register, an internal cache, memory 1004, or storage 1006. In particular embodiments, processor 1002 may include one or more internal caches for data, instructions, or addresses. This disclosure contemplates processor 1002 including any suitable number of any suitable internal caches, where appropriate. As an example and not by way of limitation, processor 1002 may include one or more instruction caches, one or more data caches, and one or more translation lookaside buffers (TLB s). Instructions in the instruction caches may be copies of instructions in memory 1004 or storage 1006, and the instruction caches may speed

up retrieval of those instructions by processor 1002. Data in the data caches may be copies of data of 80 in memory 1004 or storage 1006 for instructions executing at processor 1002 to operate on; the results of previous instructions executed at processor 1002 for access by subsequent instructions executing at processor 1002 or for writing to memory 1004 or storage 1006; or other suitable data. The data caches may speed up read or write operations by processor 1002. The TLBs may speed up virtual-address translation for processor 1002. In particular embodiments, processor 1002 may include one or more internal registers for data, instructions, or addresses. This disclosure contemplates processor 1002 including any suitable number of any suitable internal registers, where appropriate. Where appropriate, processor 1002 may include one or more arithmetic logic units (ALUs); be a multi-core processor; or include one or more processors 1002. Although this disclosure describes and illustrates a particular processor, this disclosure contemplates any suitable processor.

[0083] In particular embodiments, memory 1004 includes main memory for storing instructions for processor 1002 to execute or data for processor 1002 to operate on. As an example and not by way of limitation, computer system 1000 may load instructions from storage 1006 or another source (such as, for example, another computer system 1000) to memory 1004. Processor 1002 may then load the instructions from memory 1004 to an internal register or internal cache. To execute the instructions, processor 1002 may retrieve the instructions from the internal register or internal cache and decode them. During or after execution of the instructions, processor 1002 may write one or more results (which may be intermediate or final results) to the internal register or internal cache. Processor 1002 may then write one or more of those results to memory 1004. In particular embodiments, processor 1002 executes only instructions in one or more internal registers or internal caches or in memory 1004 (as opposed to storage 1006 or elsewhere) and operates only on data in one or more internal registers or internal caches or in memory 1004 (as opposed to storage 1006 or elsewhere). One or more memory buses (which may each include an address bus and a data bus) may couple processor 1002 to memory 1004. Bus 1012 may include one or more memory buses, as described below. In particular embodiments, one or more memory management units (MMUs) reside between processor 1002 and memory 1004 and facilitate accesses to memory 1004 requested by processor 1002. In particular embodiments, memory 1004 includes random access memory (RAM). This RAM may be volatile memory, where appropriate. Where appropriate, this RAM may be dynamic RAM (DRAM) or static RAM (SRAM). Moreover,

where appropriate, this RAM may be single-ported or multi-ported RAM. This disclosure contemplates any suitable RAM. Memory 1004 may include one or more memories 1004, where appropriate. Although this disclosure describes and illustrates particular memory, this disclosure contemplates any suitable memory.

[0084] In particular embodiments, storage 1006 includes mass storage for data or instructions. As an example and not by way of limitation, storage 1006 may include a hard disk drive (HDD), a floppy disk drive, flash memory, an optical disc, a magneto-optical disc, magnetic tape, or a Universal Serial Bus (USB) drive or a combination of two or more of these. Storage 1006 may include removable or non-removable (or fixed) media, where appropriate. Storage 1006 may be internal or external to computer system 1000, where appropriate. In particular embodiments, storage 1006 is non-volatile, solid-state memory. In particular embodiments, storage 1006 includes read-only memory (ROM). Where appropriate, this ROM may be mask-programmed ROM, programmable ROM (PROM), erasable PROM (EPROM), electrically erasable PROM (EEPROM), electrically alterable ROM (EAROM), or flash memory or a combination of two or more of these. This disclosure contemplates mass storage 1006 taking any suitable physical form. Storage 1006 may include one or more storage control units facilitating communication between processor 1002 and storage 1006, where appropriate. Where appropriate, storage 1006 may include one or more storages 1006. Although this disclosure describes and illustrates particular storage, this disclosure contemplates any suitable storage.

[0085] In particular embodiments, I/O interface 1008 includes hardware, software, or both, providing one or more interfaces for communication between computer system 1000 and one or more I/O devices. Computer system 1000 may include one or more of these I/O devices, where appropriate. One or more of these I/O devices may enable communication between a person and computer system 1000. As an example and not by way of limitation, an I/O device may include a keyboard, keypad, microphone, monitor, mouse, printer, scanner, speaker, still camera, stylus, tablet, touch screen, trackball, video camera, another suitable I/O device or a combination of two or more of these. An I/O device may include one or more sensors. This disclosure contemplates any suitable I/O devices and any suitable I/O interfaces 1008 for them. Where appropriate, I/O interface 1008 may include one or more device or software drivers enabling processor 1002 to drive one or more of these I/O devices. I/O interface 1008 may include one or more I/O interfaces 1008, where appropriate. Although this disclosure describes and illustrates a particular I/O

interface, this disclosure contemplates any suitable I/O interface.

[0086] In particular embodiments, communication interface 1010 includes hardware, software, or both providing one or more interfaces for communication (such as, for example, packet-based communication) between computer system 1000 and one or more other computer systems 1000 or one or more networks. As an example and not by way of limitation, communication interface 1010 may include a network interface controller (NIC) or network adapter for communicating with an Ethernet or other wire-based network or a wireless NIC (WNIC) or wireless adapter for communicating with a wireless network, such as a WI-FI network. This disclosure contemplates any suitable network and any suitable communication interface 1010 for it. As an example and not by way of limitation, computer system 1000 may communicate with an ad hoc network, a personal area network (PAN), a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), or one or more portions of the Internet or a combination of two or more of these. One or more portions of one or more of these networks may be wired or wireless. As an example, computer system 1000 may communicate with a wireless PAN (WPAN) (such as, for example, a BLUETOOTH WPAN), a WI-FI network, a WI-MAX network, a cellular telephone network (such as, for example, a Global System for Mobile Communications (GSM) network), or other suitable wireless network or a combination of two or more of these. Computer system 1000 may include any suitable communication interface 1010 for any of these networks, where appropriate. Communication interface 1010 may include one or more communication interfaces 1010, where appropriate. Although this disclosure describes and illustrates a particular communication interface, this disclosure contemplates any suitable communication interface.

[0087] In particular embodiments, bus 1012 includes hardware, software, or both coupling components of computer system 1000 to each other. As an example and not by way of limitation, bus 1012 may include an Accelerated Graphics Port (AGP) or other graphics bus, an Enhanced Industry Standard Architecture (EISA) bus, a front-side bus (FSB), a HYPERTRANSPORT (HT) interconnect, an Industry Standard Architecture (ISA) bus, an INFINIBAND interconnect, a low-pin-count (LPC) bus, a memory bus, a Micro Channel Architecture (MCA) bus, a Peripheral Component Interconnect (PCI) bus, a PCI-Express (PCIe) bus, a serial advanced technology attachment (SATA) bus, a Video Electronics Standards Association local (VLB) bus, or another suitable bus or a combination of two or more of these. Bus 1012 may include one or more buses 1012, where appropriate. Although this disclosure describes and illustrates a particular bus, this

disclosure contemplates any suitable bus or interconnect.

[0088] The embodiments of this specification are described in a progressive manner. For same or similar parts in the embodiments, mutual references can be made to the embodiments. Each embodiment focuses on a difference from other embodiments. In particular, the embodiments of the storage medium and the computing device are basically similar to the method embodiments, and therefore are described briefly. For related parts, references can be made to some descriptions in the method embodiments.

[0089] A person skilled in the art should be aware that in the above one or more examples, functions described in the embodiments of this specification can be implemented by hardware, software, firmware, or any combination thereof. When being implemented by software, these functions can be stored in a computer-readable medium or transmitted as one or more instructions or code on a computer-readable medium.

[0090] The objectives, technical solutions, and beneficial effects of the embodiments of the present invention are further described in detail in the specific implementations described above. It should be understood that the above descriptions are merely specific implementations of the embodiments of the present invention, and are not intended to limit the protection scope of the present invention. Any modification, equivalent replacement, improvement, and the like made based on the technical solutions of the present invention shall fall within the protection scope of the present invention.

CLAIMS

What is claimed is:

1. A fund security detection method in a service field, comprising:

obtaining fund transaction data generated on an online platform at a current moment, and determining current time series data corresponding to a current time period based on the fund transaction data;

obtaining historical time series data corresponding to each of a plurality of historical time periods, wherein any historical time series data is determined based on fund transaction data in a corresponding historical time period;

determining fluctuation trend data corresponding to a plurality of pieces of historical time series data;

comparing the current time series data with the fluctuation trend data; and

determining, based on a comparison result, whether there is a fund security risk in the current time period.

2. The method according to claim 1, wherein the step of determining current time series data corresponding to a current time period based on the fund transaction data comprises:

accumulating or averaging all fund transaction data in the current time period, to obtain the current time series data corresponding to the current time period, wherein all the fund transaction data in the current time period comprises the fund transaction data at the current moment.

3. The method according to claim 1, wherein the step of obtaining historical time series data corresponding to each of a plurality of historical time periods comprises:

obtaining historical time series data corresponding to each of a plurality of historical time periods in a preset detection step before the current time period.

4. The method according to claim 1, wherein the step of determining current time series data corresponding to a current time period based on the fund transaction data comprises:

filtering, based on a preset filtering field, field data comprised in the fund transaction data generated at the current moment; and

determining the current time series data corresponding to the current time period based on selected data.

5. The method according to claim 1, wherein the step of determining fluctuation trend data

corresponding to a plurality of pieces of historical time series data comprises:

calculating an average and a standard deviation of the plurality of pieces of historical time series data; and

determining the corresponding fluctuation trend data based on the average and the standard deviation.

6. The method according to claim 5, wherein the fluctuation trend data comprises an upper threshold limit and a lower threshold limit of data fluctuation; and the step of determining the corresponding fluctuation trend data based on the average and the standard deviation comprises:

determining the upper threshold limit and the lower threshold limit based on a range obtained by adding n times the standard deviation to the average and subtracting n times the standard deviation from the average.

7. The method according to claim 1, wherein the fluctuation trend data comprises an upper threshold limit and a lower threshold limit of data fluctuation; and

the step of determining, based on a comparison result, whether there is a fund security risk in the current time period comprises:

when the current time series data exceeds a range comprising the upper threshold limit and the lower threshold limit, determining that there is a fund security risk in the current time period.

8. The method according to claim 1, after the obtaining historical time series data corresponding to each of a plurality of historical time periods, further comprising:

when a value of the current time series data is 0, performing the following first determining: determining whether historical time series data in a first quantity of historical time periods before the current time period is 0; and

determining, based on a determining result of the first determining, whether there is a data drop to zero risk.

9. The method according to claim 8, wherein the step of determining, based on a determining result of the first determining, whether there is a data drop to zero risk comprises:

when the determining result of the first determining is yes, performing the following second determining: determining whether historical time series data in a second quantity of historical time periods before the first quantity of historical time periods is 0; and

when a determining result of the second determining is no, determining that there is a data drop to zero risk.

10. A computer system, comprising a storage, a processor, and a computer program stored in the storage and capable of running on the processor, wherein when the processor executes the program, the following steps are implemented:

obtaining fund transaction data generated on an online platform at a current moment, and determining current time series data corresponding to a current time period based on the fund transaction data;

obtaining historical time series data corresponding to each of a plurality of historical time periods, wherein any historical time series data is determined based on fund transaction data in a corresponding historical time period;

determining fluctuation trend data corresponding to a plurality of pieces of historical time series data;

comparing the current time series data with the fluctuation trend data; and

determining, based on a comparison result, whether there is a fund security risk in the current time period.

11. The computer system according to claim 10, wherein the step of determining current time series data corresponding to a current time period based on the fund transaction data comprises:

accumulating or averaging all fund transaction data in the current time period, to obtain the current time series data corresponding to the current time period, wherein all the fund transaction data in the current time period comprises the fund transaction data at the current moment.

12. The computer system according to claim 10, wherein the step of obtaining historical time series data corresponding to each of a plurality of historical time periods comprises:

obtaining historical time series data corresponding to each of a plurality of historical time periods in a preset detection step before the current time period.

13. The computer system according to claim 10, wherein the step of determining current time series data corresponding to a current time period based on the fund transaction data comprises:

filtering, based on a preset filtering field, field data comprised in the fund transaction data generated at the current moment; and

determining the current time series data corresponding to the current time period based on selected data.

14. The computer system according to claim 10, wherein the step of determining fluctuation trend data corresponding to a plurality of pieces of historical time series data comprises:

calculating an average and a standard deviation of the plurality of pieces of historical time series data; and

determining the corresponding fluctuation trend data based on the average and the standard deviation.

15. The computer system according to claim 14, wherein the fluctuation trend data comprises an upper threshold limit and a lower threshold limit of data fluctuation; and the step of determining the corresponding fluctuation trend data based on the average and the standard deviation comprises:

determining the upper threshold limit and the lower threshold limit based on a range obtained by adding n times the standard deviation to the average and subtracting n times the standard deviation from the average.

16. The computer system according to claim 10, wherein the fluctuation trend data comprises an upper threshold limit and a lower threshold limit of data fluctuation; and the step of determining, based on a comparison result, whether there is a fund security risk in the current time period comprises:

when the current time series data exceeds a range comprising the upper threshold limit and the lower threshold limit, determining that there is a fund security risk in the current time period.

17. The computer system according to claim 10, after the obtaining historical time series data corresponding to each of a plurality of historical time periods, further comprising:

when a value of the current time series data is 0, performing the following first determining: determining whether historical time series data in a first quantity of historical time periods before the current time period is 0; and

determining, based on a determining result of the first determining, whether there is a data drop to zero risk.

18. The computer system according to claim 17, wherein the step of determining, based on a determining result of the first determining, whether there is a data drop to zero risk comprises:

when the determining result of the first determining is yes, performing the following second determining: determining whether historical time series data in a second quantity of historical time periods before the first quantity of historical time periods is 0; and

when a determining result of the second determining is no, determining that there is a data drop to zero risk.

19. A fund security detection apparatus in a service field, comprising:

an online data obtaining module, configured to: obtain fund transaction data generated on an online platform at a current moment, and determine current time series data corresponding to a current time period based on the fund transaction data;

a historical data obtaining module, configured to obtain historical time series data corresponding to each of a plurality of historical time periods, wherein any historical time series data is determined based on fund transaction data in a corresponding historical time period;

a fluctuation trend determining module, configured to determine fluctuation trend data corresponding to a plurality of pieces of historical time series data;

a module for comparing two types of data, configured to compare the current time series data with the fluctuation trend data; and

a fund security determining module, configured to determine, based on a comparison result, whether there is a fund security risk in the current time period.

20. A computer-readable nonvolatile storage medium, wherein the storage medium stores a computer program, and when the computer program is executed by a processor, the method according to any one of claims 1 to 9 is implemented.