(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 July 2016 (21.07.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/115141 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2016/013058

(22) International Filing Date:
12 January 2016 (12.01.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201510019448.2 14 January 2015 (14.01.2015) CN

(71) Applicant: **ALIBABA GROUP HOLDING LIMITED** [—/US]; Fourth Floor, One Capital Place, P.O. Box 847, George Town, Grand Cayman (KY).

(72) Inventors: **WANG, Wei**; Alibaba Group Legal Department, 5/F, Building 3, No. 969 West Wen Yi Road, Yu Hang District, Hangzhou, 311121 (CN). **LIN, Shumin**; Alibaba Group Legal Department, 5/F, Building 3, No. 969 West Wen Yi Road, Yu Hang District, Hangzhou, 311121 (CN).

(74) Agent: **CHEN, Weiguo**; Finnegan, Henderson, Farabow, Garrett & Dunner LLP, 901 New York Avenue, NW, Washington, DC 20001-4413 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: METHODS, SYSTEMS, AND APPARATUS FOR IDENTIFYING RISKS IN ONLINE TRANSACTIONS

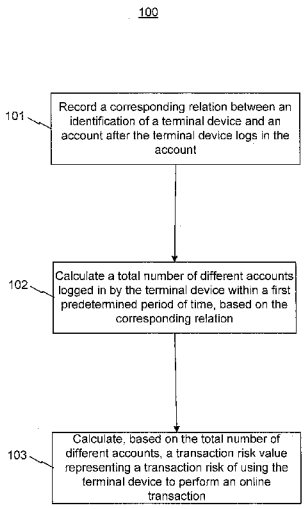

Fig. 1

(57) Abstract: A method for identifying risks in online transactions is provided. The method includes recording a corresponding relation between an identification of a terminal device and an account after the terminal device logs in the account, calculating a total number of different accounts logged in by the terminal device within a first predetermined period of time, based on the corresponding relation, and calculating, based on the total number of different accounts, a transaction risk value representing a transaction risk of using the terminal device to perform an online transaction.

WO 2016/115141 A1

METHODS, SYSTEMS, AND APPARATUS FOR IDENTIFYING RISKS IN ONLINE TRANSACTIONS

CROSS REFERENCE TO RELATED APPLICATION

[001] The present application claims the benefits of priority to Chinese Application No. 201510019448.2, filed January 14, 2015, the entire contents of which are incorporated herein by reference.

TECHNICAL FIELD

[001] The present application relates to computer network technologies, and more particularly, to methods, systems, and apparatus for identifying risks in online transactions.

BACKGROUND

[002] Nowadays electronic commerce (e-commerce), as a new way of shopping, has been generally accepted and widely used. As a result, internet-based transactions have become more frequent. In addition, as smart mobile devices become popular, more people have started using internet-accessible (mobile) device terminals to perform transactions, which may become the most dominant way for payment in the near future.

[003] Meanwhile, as the total transaction amount conducted over the internet grows, transaction security becomes an issue. Due to possibilities of hacking or many other ways of illegally taking possession of other people's assets online, it has been extremely challenging for online payment and finance service providers to preemptively identify all potential threats. It is therefore important to develop technologies that can secure online transactions and eliminate potential breaches.

[004] Existing online transaction security practices of traditional financial organizations usually involve authenticating an identification of an account by using a security digital certificate. This causes burden to users and is often user unfriendly.

SUMMARY

[005] One aspect of the present disclosure is directed to a method for identifying risks in online transactions. The method includes recording a corresponding relation between an identification of a terminal device and an account after the terminal device logs in the account, calculating a total number of different accounts logged in by the terminal device within a first predetermined period of time, based on the corresponding relation, and calculating, based on the total number of different accounts, a transaction risk value representing a transaction risk of using the terminal device to perform an online transaction.

[006] Another aspect of the present disclosure is directed to an apparatus for identifying risks in online transactions. The apparatus includes a recording module configured to record an identification of the terminal device and a corresponding relation between the identification and an account after the terminal device logs in the account, a total number of different accounts statistic module configured to calculate a total number of different accounts logged in by the terminal device within a first predetermined period of time, based on the corresponding relation, and a transaction risk calculation module configured to calculate, based on the total number of different accounts, a transaction risk value representing a transaction risk of using the terminal device to perform an online transaction.

[007] Additional objects and advantages of the present disclosure will be set forth in part in the following detailed description, and in part will be obvious from the description, or may be learned by practice of the present disclosure. The objects

and advantages of the present disclosure will be realized and attained by means of the elements and combinations particularly pointed out in the appended claims.

[008] It is to be understood that the foregoing general description and the following detailed description are exemplary and explanatory only, and are not restrictive of the invention, as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[009] The accompanying drawings, which constitute a part of this specification, illustrate several embodiments and, together with the description, serve to explain the disclosed principles.

[010] FIG. 1 is a flow diagram illustrating a method for identifying risks in online transactions, according to an exemplary embodiment.

[011] FIG. 2 is a flow diagram illustrating another method for identifying risks in online transactions according to an exemplary embodiment.

[012] FIG. 3 is a graphical representation illustrating a function for identifying risks in online transactions, according to an exemplary embodiment.

[013] FIG. 4 is a graphical representation illustrating another function for identifying risks in online transactions, according to an exemplary embodiment.

[014] FIG. 5 is a graphical representation illustrating another function for identifying risks in online transactions, according to an exemplary embodiment.

[015] FIG. 6 is a flow diagram illustrating another method for identifying risks in online transactions, according to an exemplary embodiment.

[016] FIG. 7 is a block diagram illustrating an apparatus for identifying risks in online transactions, according to an exemplary embodiment.

[017] FIG. 8 is a block diagram illustrating another apparatus for identifying risks in online transactions, according to an exemplary embodiment.

[018] Fig. 9 is a block diagram illustrating another apparatus for identifying risks in online transactions, according to an exemplary embodiment.

DETAILED DESCRIPTION

[019] Reference will now be made in detail to exemplary embodiments of the invention, examples of which are illustrated in the accompanying drawings. The following description refers to the accompanying drawings in which the same numbers in different drawings represent the same or similar elements unless otherwise represented. The implementations set forth in the following description of exemplary embodiments consistent with the present invention do not represent all implementations consistent with the invention. Instead, they are merely examples of systems and methods consistent with aspects related to the invention as recited in the appended claims.

[020] Consistent with some embodiments, the present disclosure provides a method for online transaction risk identification based on a computer system. FIG. 1 is a flow diagram of the method 100 for online transaction risk identification based on a computer system.

[021] As shown in FIG. 1, for example, the method for online transaction risk identification based on a computer system includes the following steps:

[022] Step 101: collect and/or record a corresponding relation between an identification of a terminal device and an account after the terminal device logs in the account. The recording may be achieved via a webpage (e.g., a browser) or a mobile device.

[023] The identification of the terminal device may be implemented in various forms, as long as it can uniquely identify one terminal device, for example, a Media Access Control (MAC) address, a User Machine Identification (UMID) code, a

Terminal Identification (TID) code, an identifier allocated to the terminal device by an application (APP) installed on the terminal device, a Subscriber Identity Module (SIM) card number, a processor identifier, a main board identifier, etc..

[024] The terms of the MAC address, the UMID code, and the TID code are explained as follows:

[025] MAC Address: Media Access Control address, or called a hardware address, is used for defining a location of a network device. In a network protocol OSI model, the Layer 3 Network Layer is responsible for IP address, whereas the Layer 2 Data Link Layer is responsible for MAC address. Thus, one host has one IP address, whereas each network location has a unique MAC address.

[026] UMID Code: User Machine Identification code is used for providing an accurate authentication service on an identification of a user machine.

[027] TID Code: Terminal Identification is used for providing an accurate identification service on a user's App environment.

[028] For example, to control risks, web browsers or cell phone clients can collect user device's finger print information, and encode the information for storage and recording (in which the internet generally uses, for example, MAC address, UMID code, TID code, etc.). The user's operation (which is not limited to a transaction) corresponding to an event in a system, and all relevant information involved in the event, such as a user name, an operation name, a device code of the device used (such as MAC address, UMID code, or TID code, etc.), and so on, can be recorded and stored.

[029] Step 102: calculate a total number of different accounts logged in by the terminal device within a first predetermined period of time, based on the corresponding relation(s).

[030] Step 103: calculate, based on the total number of different accounts, a transaction risk value representing a transaction risk of using the terminal device to perform an online transaction.

[031] Once the transaction risk value is calculated, it not only can be used for online transaction, but also can be used for creating an online transaction blacklist, making credit assessment, and so on. For example, when the transaction risk value is used for creating an online transaction blacklist, for a plurality of terminal devices, a transaction risk value is respectively calculated for each of the terminal devices by using the method disclosed in the embodiments of the present disclosure; next, an identification of each terminal device with a transaction risk value higher than a preset threshold is obtained; and then, an online transaction blacklist is created. Thus, the terminal devices listed in the backlist will be rejected when performing online transactions.

[032] In this embodiment, by means of information analysis and data modeling on internet terminal devices used in online transactions, the system can identify a risk value in the online transactions and fund management, and that can help guarantee users' fund security in online shopping or financing during the users' normal usage.

[033] Consistent with some other embodiments, the present disclosure provides a method for online transaction risk identification based on a computer system. FIG. 2 is a flow diagram of the method 200 for online transaction risk identification based on a computer system.

[034] In these embodiments, besides a total number of different accounts, the computer system may further analyze a total number of logins of the terminal device within one time period, a total transaction amount, a time duration from the

first login to a current time, thereby obtaining a more accurate transaction risk value. For example:

[035] Before Step 103, the method further includes the following steps:

[036] Step 1021: calculate a total number of logins at the terminal device within a second predetermined period of time;

[037] Step 1022: acquire a time duration between a first login at the terminal device and a current time;

[038] Step 1023: calculate a total transaction amount within a third predetermined period of time.

[039] Correspondingly, Step 103 further includes a Sub-step 1031: calculate a transaction risk value representing a transaction risk of using the terminal device to perform an online transaction, based on the total number of different accounts and at least one of the total number of logins, the time duration, or the total transaction amount.

[040] For example, the above Step 1021 to Step 1023 are not indispensable. Instead, they may be executed depending upon the total number of logins, the time duration, or the total transaction amount selected in any combination with the total number of different accounts. Moreover, the sequence thereof may not be fixed either. Therefore, any combination of the above steps and the execution sequence thereof all fall within the protection scope of the present application.

[041] In this embodiment, besides the total number of different accounts, the system may further analyze the total number of logins of the terminal device within one time period, the total transaction amount, and the time duration from the first login to a current time, so that the obtained transaction risk value is more accurate.

[042] In addition, the method can further control the risks by performing a short message service (SMS) code authentication on each transaction, or making strict authority control on the terminal devices without installing digital certificates.

[043] Consistent with some other embodiments, the present disclosure provides another method for online transaction risk identification based on a computer system. In these embodiments, the computer system may comprehensively consider the total number of different accounts of the terminal device, the total number of logins and the total transaction amount circulated within one time period, and the time duration from the first login to a current time, and may further considering a different weight of each of the above factors in calculating the transaction risk value, so that the calculated transaction risk value is more proper for the actual situation. For example:

[044] In Step 1031, calculate a transaction risk value based on Equation (1).

[045]
$$Score = \frac{a_1 \cdot f_1(\mathrm{F}) + a_2 \cdot f_2(\mathrm{R}) + a_3 \cdot f_3(\mathrm{M})}{b \cdot f_0(\mathrm{U})} \quad (1)$$

[046] In Equation (1), $f_1(\mathrm{F})$ and a_1 respectively represent a function of a total number of logins F and a weight thereof, $f_2(\mathrm{R})$ and a_2 respectively represent a function of a time duration R and a weight thereof, $f_3(\mathrm{M})$ and a_3 respectively represent a function of a total transaction amount M and a weight thereof, and $f_0(\mathrm{U})$ and b respectively represent a function of a total number of different accounts U and a weight thereof. In applications, when a certain factor is more important compared with the other factors, its weight can be set correspondingly. In one exemplary embodiment, a_1, a_2, a_3, and b are all 1, and $f_1(\mathrm{F})$, $f_2(\mathrm{R})$, and $f_3(\mathrm{M})$ are all normalization functions.

[047] For example, the total number of different accounts on a certain device is can be for example 1 to 2, which is reasonable. If the device has too many accounts, it indicates that the device has a poor privacy feature, and even has a risk of being used maliciously.

[048] For example, in the step of calculating the transaction risk value based on Equation (1), $f_0(\mathrm{U})$ is an exponential function $f_0(\mathrm{U}) = \mathrm{pow}(1.2, \mathrm{U}-1)$, in which U represents a total number of different accounts, 1.2 is a base of the exponential function, and U-1 is an exponent of the exponential function.

[049] As an example, $f_0(\mathrm{U})$ may also be represented in other ways, which can also represent that the device has a lower risk when the total number of different accounts falls within a certain scope, for example, but not limited to, $f_0(\mathrm{U}) = ax^2 + bx + c$.

[050] In addition, the statistic data shows, the login activities of terminal devices fall within a certain scope; if the terminal device has a too low total number of logins, it implies that the terminal device is not frequently used, and if the terminal device has a too high total number of logins, it implies that the terminal device may be maliciously used.

[051] Considering the above situations, for example, the step of calculating the transaction risk value based on Equation (1) may further include a following sub-step:

[052] using a Chi-square distribution density curve function $f_k(x) = \frac{(1/2)^{k/2}}{\Gamma(k/2)} x^{k/2-1} e^{-x/2}$ to perform normalization on the total number of logins.

[053] In this case, in Equation (1), $f_1(\mathrm{F})$ is $f_{1k}(F)=\frac{(1/2)^{k/2}}{\Gamma(k/2)}F^{k/2-1}e^{-F/2}$;

[054] wherein, k represents a degree of freedom, F represents a total number of logins, and Γ represents Gamma function.

[055] In one embodiment, it sets the degree of freedom k=3, and statistically collects a total number of logins on the terminal device by users within 90 days, and a normalization curve is shown in FIG. 3. When the users' total number of logins reaches about 90 times, the normalization risk value approaches 1.0, whereas when the total number of logins becomes lower or higher, the corresponding normalization risk value becomes smaller.

[056] The normalization of the total number of logins may be performed in other ways, for example, but not limited to, $f_1(F)=\frac{1}{\sigma\sqrt{2\pi}}e^{\frac{(F-\mu)^2}{2\sigma^2}}$.

[057] The step of calculating the transaction risk value based on Equation (1) may further include the following sub-step:

using a logic equation $f(x)=\frac{2}{1+e^{-ax}}-1$ to perform normalization on the time duration.

[058] In this case, in Equation (1), $f_2(\mathrm{R})$ is $f_2(\mathrm{R})=\frac{2}{1+e^{-aR}}-1$;

where, a parameter a is determined by $f_2^{'}(R=0)=K*f_2^{'}\left(R=R\_P\right)$,

$R\_P=75$ quantile, and $K=100$.

[059] In one embodiment, a normalization curve of the time duration is shown in FIG. 4, and as the time duration from the first login of the terminal device to a current time increases, the normalization risk value presents a growing trend.

[060] In addition, in some embodiments of the present disclosure, the normalization of the time duration may be performed in other ways, for example, but not limited to, $f_2(\mathrm{R}) = \frac{R - R_{\min}}{R_{\max} - R_{\min}}$.

[061] The step of calculating the transaction risk value based on Equation (1) may further include the following sub-step:

using a logic equation $f(x) = \frac{2}{1+e^{-ax}} - 1$ to perform normalization on the total transaction amount.

[062] In this case, in Equation (1), $f_3(\mathrm{M})$ is $f_3(\mathrm{M}) = \frac{2}{1+e^{-aM}} - 1$;

where, a parameter a is determined by $f_3'(\mathrm{M}=0) = K * f_3'\left(M = M\_P\right)$, $M\_P = 99$ quantile, and $K = 100$.

[063] In one embodiment, a normalization curve of the total transaction amount is shown in FIG. 5, and as the total transaction amount circulating in the terminal device increases, the normalization risk value presents a growing trend.

[064] In addition, in some embodiments of the present disclosure, the normalization of the total transaction amount may be performed in other ways, for example, but not limited to, $f_3(\mathrm{M}) = \frac{\mathrm{M} - \mathrm{M}_{\min}}{\mathrm{M}_{\max} - \mathrm{M}_{\min}}$.

[065] Consistent with some other embodiments of the present disclosure, an online transaction method is provided. FIG. 6 is a flow diagram of the online transaction method 600.

[066] For example, as shown in FIG. 6, the online transaction method includes the following steps:

[067] Step 601: calculate a transaction risk value of each terminal device involved in one transaction by using the methods provided in the above-described embodiments.

[068] Step 602: if the transaction risk value of one terminal device is higher than a preset threshold, reject the online transaction; otherwise, proceed the online transaction.

[069] As an example, the calculated transaction risk value may fall within a scope of 0~3. If the calculated transaction risk value is 3, the transaction is permitted. If the calculated transaction risk value is 2, other additional authentication modes can be added. If the calculated transaction risk value is 1, manual auditing may be requested. If the calculated transaction risk value is 0, the transaction may be rejected. The relation between the score of the transaction risk value and its corresponding operation authority can be set in other ways depending upon the requirements of the actual situations, which is not limited herein.

[070] In this embodiment, based on the transaction risk value of each terminal device, the computer system controls the authority of the terminal device in performing online transactions, and that can effectively control the risks.

[071] The method embodiments of the present disclosure can be implemented in a form of software, hardware, firmware, and so on. Regardless that the present disclosure is implemented in a form of software, hardware, or firmware, instruction codes can be stored in any type of computer accessible storage (for example, permanent or erasable, volatile or non-volatile, solid or non-solid, fixed or replaceable medium, etc.). Similarly, the storage may be, for example, Programmable Array Logic (PAL), Random Access Memory (RAM), Programmable Read Only Memory (PROM), Read-Only Memory (ROM), Electrically Erasable

Programmable ROM (EEPROM), magnetic disc, optical disc, Digital Versatile Disc, (DVD), etc.

[072] Consistent with some embodiments of the present disclosure, an apparatus for online transaction risk identification based on a computer system is provided. FIG. 7 is a block diagram of the apparatus 700 for online transaction risk identification based on a computer system. For example, as shown in FIG. 7, the apparatus for online transaction risk identification based on a computer system may include a recording module 701, for recording a corresponding relation between an identification of a terminal device and an account after the terminal device logs in the account, a total number of different accounts statistic module 702, for calculating a total number of different accounts logged in by the terminal device within a first predetermined period of time, based on the corresponding relation, and a transaction risk calculation module 703, for calculating, based on the total number of different accounts, a transaction risk value representing a transaction risk of using the terminal device to perform an online transaction. The apparatus 700 can implement the above-described methods. The detailed steps of the methods are not repeated here.

[073] By means of information analysis and data modeling on terminal devices on the Internet used in online transactions, the apparatus can identify a risk value in the online transactions and fund management, and that can help guarantee users' fund security in online shopping or financing during the users' normal usage.

[074] Consistent with some other embodiments of the present disclosure, an apparatus for online transaction risk identification based on a computer system is provided. FIG. 8 is a block diagram of the apparatus 800 for online transaction risk identification.

[075] According to some embodiments, the apparatus 800, as shown in FIG. 8, besides a total number of different accounts, can further analyze a total number of logins of the terminal device within one time period, a total transaction amount, and a time duration from the first login to a current time, thereby obtaining a more accurate transaction risk value.

[076] To implement these functions, the apparatus 800 may further include the following modules:

a total number of logins statistic module 801, for calculating a total number of logins at the terminal device within a second predetermined period of time;

a time duration acquisition module 802, for acquiring a time duration between a first login at the terminal device and a current time; and

a total transaction amount statistic module 803, for calculating a total transaction amount within a third predetermined period of time.

[077] Correspondingly, the transaction risk calculation module 703 may calculate a transaction risk value based on the total number of different accounts and at least one of the total number of logins, the time duration, or the total transaction amount.

[078] The apparatus 800 can implement the above-described methods. The detailed steps of the methods are not repeated here.

[079] In some other embodiments, the apparatus 700 and 800 described above may comprehensively consider the total number of different accounts of the terminal device, the total number of logins within one time period, the time duration from the first login to a current time, and the total transaction amount circulating within one time period, and further consider a different weight of each of the above

factors in calculating the transaction risk value, so that the calculated transaction risk value is more proper for the actual situation.

[080] For example, the transaction risk value may be calculated in the transaction risk calculation module based on Equation (1).

[081]
$$Score = \frac{a_1 \cdot f_1(\mathrm{F}) + a_2 \cdot f_2(\mathrm{R}) + a_3 \cdot f_3(\mathrm{M})}{b \cdot f_0(\mathrm{U})} \quad (1)$$

[082] $f_1(\mathrm{F})$ and a_1 respectively represent a function of a total number of logins F and a weight thereof, $f_2(\mathrm{R})$ and a_2 respectively represent a function of a time duration R and a weight thereof, $f_3(\mathrm{M})$ and a_3 respectively represent a function of a total transaction amount M and a weight thereof, and $f_0(\mathrm{U})$ and b respectively represent a function of a total number of different accounts U and a weight thereof.

[083] For example, in the step of calculating the transaction risk value based on Equation (1), $f_0(\mathrm{U})$ is an exponential function $f_0(\mathrm{U}) = \mathrm{pow}(1.2, \mathrm{U}-1)$, in which U represents the total number of different accounts, 1.2 is a base of the exponential function, and U-1 is an exponent of the exponential function.

[084] The transaction risk calculation module may further include a total number of logins normalization sub-module, which uses a Chi-square distribution density curve function to perform normalization on the total number of logins.

[085] In Equation (1), $f_1(\mathrm{F})$ is $f_{1k}(F) = \frac{(1/2)^{k/2}}{\Gamma(k/2)} F^{k/2-1} e^{-F/2}$, where k represents a degree of freedom, F represents a total number of logins, and Γ represents Gamma function.

[086] The transaction risk calculation module may further include a time duration normalization sub-module, for using a logic equation $f(x)=\frac{2}{1+e^{-ax}}-1$ to perform normalization on the time duration.

[087] In Equation (1), $f_2(\mathrm{R})$ is $f_2(\mathrm{R})=\frac{2}{1+e^{-aR}}-1$, where a parameter a is determined by: $f_2^{'}(R=0)=K*f_2^{'}\left(R=R\_P\right)$, $R\_P=75$ quantile, and $K=100$.

[088] The transaction risk calculation module may further include a total transaction amount normalization sub-module, which uses a logic equation $f(x)=\frac{2}{1+e^{-ax}}-1$ to perform normalization on the total transaction amount.

[089] In Equation (1), $f_3(\mathrm{M})$ is $f_3(\mathrm{M})=\frac{2}{1+e^{-aM}}-1$, where a parameter a is determined by $f_3^{'}(\mathrm{M}=0)=K*f_3^{'}\left(M=M\_P\right)$, $M\_P=99$ quantile, and $K=100$.

[090] FIG. 9 is a block diagram of an online transaction apparatus 900 according to some other embodiments of the present disclosure.

[091] The online transaction apparatus may include an online transaction risk identification module 901 and a transaction determination module 902. The online transaction risk identification module 901 calculates a transaction risk value of each terminal device involved in a transaction by using the apparatus described above.

[092] The transaction determination module 902 determines whether to proceed with the transaction. For example, the transaction determination module 902 may reject the online transaction, if the transaction risk value of one terminal device is higher than a preset threshold; otherwise, proceed the online transaction.

[093] In addition, in some embodiments, the calculated transaction risk value may be set with a range of 0~3. If the calculated transaction risk value is 3, the transaction is permitted. If the calculated transaction risk value is 2, other additional authentication mode may be added. If the calculated transaction risk value is 1, manual auditing may be requested. If the calculated transaction risk value is 0, the transaction may be rejected. The relation between the score of the transaction risk value and its corresponding operation authority can be set in other ways depending upon the requirements of the actual situations, which is not limited herein.

[094] In this embodiment, based on the transaction risk value of each terminal device, the apparatus controls the authority of the terminal device in performing online transactions, thereby effectively controlling the risks.

[095] The embodiments of the present disclosure use big data technologies to analyze history operation records made by thousands of network subscribers in daily shopping payment and fund management on terminal devices on the Internet, build data modeling, identify potential risks in online transactions and fund management, and provide a score associated with the risk, to guarantee network subscribers' fund security in online shopping or financing.

[096] The modules described in the apparatus embodiments of the present disclosure may be logic modules. One logic module may be one physical module, a part of one physical module, or a combination of a plurality of physical modules. In some other embodiments, the modules/units may be implemented in a form of software, hardware, firmware, or any combination of software, hardware, and firmware. For examples, the modules/units may be implemented by a processor executing software instructions stored in computer readable memories.

[097] The specification has described methods, systems, and apparatus for identifying risks in online transactions. The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. Thus, these examples are presented herein for purposes of illustration, and not limitation. For example, steps or processes disclosed herein are not limited to being performed in the order described, but may be performed in any order, and some steps may be omitted, consistent with disclosed embodiments. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments.

[098] While examples and features of disclosed principles are described herein, modifications, adaptations, and other implementations are possible without departing from the spirit and scope of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items, or meant to be limited to only the listed item or items. It must also be noted that as used herein and in the appended claims, the singular forms "a," "an," and "the" include plural references unless the context clearly dictates otherwise.

[099] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term "computer-readable medium" may include tangible items and exclude carrier waves and transient signals, i.e., be non-transitory. Examples include RAM, ROM, volatile memory, nonvolatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, Programmable Array Logic (PAL), Programmable Read Only Memory (PROM), Electrically Erasable Programmable ROM (EEPROM), magnetic disc, optical disc, and any other known physical storage media.

[0100] It will be appreciated that the present invention is not limited to the exact construction that has been described above and illustrated in the accompanying drawings, and that various modifications and changes can be made without departing from the scope thereof. It is intended that the scope of the invention should only be limited by the appended claims.

WHAT IS CLAIMED IS:

1. A method for identifying risks in online transactions, comprising:

recording a corresponding relation between an identification of a terminal device and an account after the terminal device logs in the account;

calculating a total number of different accounts logged in by the terminal device within a first predetermined period of time, based on the corresponding relation; and

calculating, based on the total number of different accounts, a transaction risk value representing a transaction risk of using the terminal device to perform an online transaction.

2. The method of claim 1, before calculating the transaction risk value, further comprising:

calculating a total number of logins by the terminal device within a second predetermined period of time,

wherein calculating the transaction risk value comprises calculating the transaction risk value further based on the total number of logins.

3. The method of claim 1, before calculating the transaction risk value, further comprising:

acquiring a time duration between a first login by the terminal device and a current time,

wherein calculating the transaction risk value comprises calculating the transaction risk value further based on the time duration.

4. The method of claim 1, before calculating the transaction risk value, further comprising:

calculating a total transaction amount within a third predetermined period of time,

wherein calculating the transaction risk value comprises calculating the transaction risk value further based on the total transaction amount.

5. The method of claim 1, before calculating the transaction risk value, further comprising:

calculating a total number of logins by the terminal device within a second predetermined period of time;

acquiring a time duration between a first login by the terminal device and a current time; and

calculating a total transaction amount within a third predetermined period of time,

wherein calculating the transaction risk value comprises calculating the transaction risk value further based on the total number of logins, the time duration, and the total transaction amount.

6. The method of claim 5, wherein calculating the transaction risk value comprises calculating the transaction risk value further based on an equation

$Score = \frac{a_1 \cdot f_1(\mathrm{F}) + a_2 \cdot f_2(\mathrm{R}) + a_3 \cdot f_3(\mathrm{M})}{b \cdot f_0(\mathrm{U})}$, with Score being the transaction risk value, F being the total number of logins, $f_1(\mathrm{F})$ being a function of the total number of logins F, a_1 being a weight of the function $f_1(\mathrm{F})$, R being the time duration, $f_2(\mathrm{R})$ being a function of the time duration R, a_2 being a weight of the function $f_2(\mathrm{R})$, M being the total transaction amount, $f_3(\mathrm{M})$ being a function of the total transaction amount M, a_3 being a weight of the function $f_3(\mathrm{M})$, U being the total number of different accounts, $f_0(\mathrm{U})$ being a function of the total number U, and b being a weight of the function $f_0(\mathrm{U})$.

7. The method of claim 6, wherein $f_0(\mathrm{U})$ is an exponential function $f_0(\mathrm{U}) = \mathrm{pow}(1.2, \mathrm{U}-1)$, 1.2 being a base of the exponential function, and U-1 being an exponent of the exponential function.

8. The method of claim 6, wherein $f_1(\mathrm{F})$ is a function $f_{1k}(F) = \frac{(1/2)^{k/2}}{\Gamma(k/2)} F^{k/2-1} e^{-F/2}$, k being a degree of freedom, and Γ being a Gamma function.

9. The method of claim 6, wherein $f_2(\mathrm{R})$ is a function $f_2(\mathrm{R}) = \frac{2}{1+e^{-aR}} - 1$, wherein a is determined by $f_2'(R=0) = K * f_2'(R = R\_P)$, $R\_P = 75$ quantile, and $K = 100$.

10. The method of claim 6, wherein $f_3(\mathrm{M})$ is a function $f_3(\mathrm{M}) = \frac{2}{1+e^{-aM}} - 1$, wherein a is determined by $f_3'(\mathrm{M}=0) = K * f_3'\left(M = M\_P\right)$, $M\_P = 99$ quantile, and $K = 100$.

11. The method of claim 1, further comprising rejecting the online transaction, if the transaction risk value exceeds a predetermined threshold.

12. An apparatus for identifying risks in online transactions, comprising:

a recording module configured to record an identification of a terminal device and a corresponding relation between the identification and an account after the terminal device logs in the account;

a total number of different accounts statistic module configured to calculate a total number of different accounts logged in by the terminal device within a first predetermined period of time, based on the corresponding relation; and

a transaction risk calculation module configured to calculate, based on the total number of different accounts, a transaction risk value representing a transaction risk of using the terminal device to perform an online transaction.

13. The apparatus of claim 12, further comprising:

a total number of logins statistic module configured to calculate a total number of logins by the terminal device within a second predetermined period of time,

wherein the transaction risk calculation module is further configured to calculate the transaction risk value based on the total number of logins.

14. The apparatus of claim 12, further comprising:

a time duration acquisition module configured to acquire a time duration between a first login by the terminal device and a current time,

wherein the transaction risk calculation module is further configured to calculate the transaction risk value based on the time duration.

15. The apparatus of claim 12, further comprising:

a total transaction amount statistic module configured to calculate a total transaction amount within a third predetermined period of time,

wherein the transaction risk calculation module is further configured to calculate the transaction risk value based on the total transaction amount.

16. The apparatus of claim 12, further comprising:

a total number of logins statistic module configured to calculate a total number of logins by the terminal device within a second predetermined period of time;

a time duration acquisition module configured to acquire a time duration between a first login by the terminal device and a current time; and

a total transaction amount statistic module configured to calculate a total transaction amount within a third predetermined period of time,

wherein the transaction risk calculation module is further configured to calculate the transaction risk value based on the total number of logins, the time duration, and the total transaction amount.

17. The apparatus of claim 16, wherein the transaction risk calculation module is further configured to calculate the transaction risk value based on an equation $Score = \frac{a_1 \cdot f_1(\mathrm{F}) + a_2 \cdot f_2(\mathrm{R}) + a_3 \cdot f_3(\mathrm{M})}{b \cdot f_0(\mathrm{U})}$, with Score being the transaction risk value, F being the total number of logins, $f_1(\mathrm{F})$ being a function of the total number of logins F, a_1 being a weight of the function $f_1(\mathrm{F})$, R being the time duration, $f_2(\mathrm{R})$ being a function of the time duration R, a_2 being a weight of the function $f_2(\mathrm{R})$, M being the total transaction amount, $f_3(\mathrm{M})$ being a function of the total transaction amount M, a_3 being a weight of the function $f_3(\mathrm{M})$, U being the total number of different accounts, $f_0(\mathrm{U})$ being a function of the total number U of different accounts, and b being a weight of the function $f_0(\mathrm{U})$.

18. The apparatus of claim 17, wherein $f_0(\mathrm{U})$ is an exponential function $f_0(\mathrm{U}) = \mathrm{pow}(1.2, \mathrm{U}-1)$, 1.2 being a base of the exponential function, and U-1 being an exponent of the exponential function.

19. The apparatus of claim 17, wherein $f_1(\mathrm{F})$ is a function $f_{1k}(F) = \frac{(1/2)^{k/2}}{\Gamma(k/2)} F^{k/2-1} e^{-F/2}$, k being a degree of freedom, and Γ being a Gamma function.

20. The apparatus of claim 12, further comprising a transaction determination module configured to reject the online transaction, if the transaction risk value exceeds a predetermined threshold.

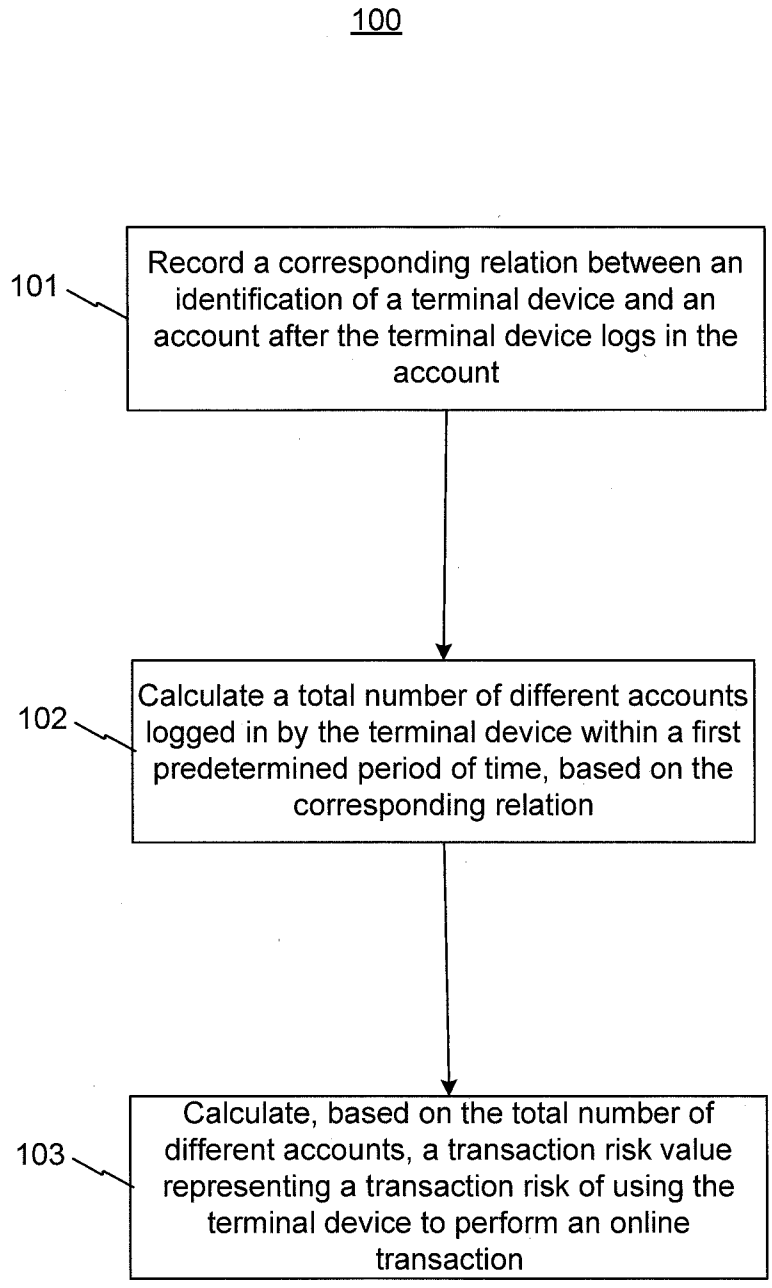
100
101
Record a corresponding relation between an identification of a terminal device and an account after the terminal device logs in the account
102
Calculate a total number of different accounts logged in by the terminal device within a first predetermined period of time, based on the corresponding relation
103
Calculate, based on the total number of different accounts, a transaction risk value representing a transaction risk of using the terminal device to perform an online transaction

Fig. 1

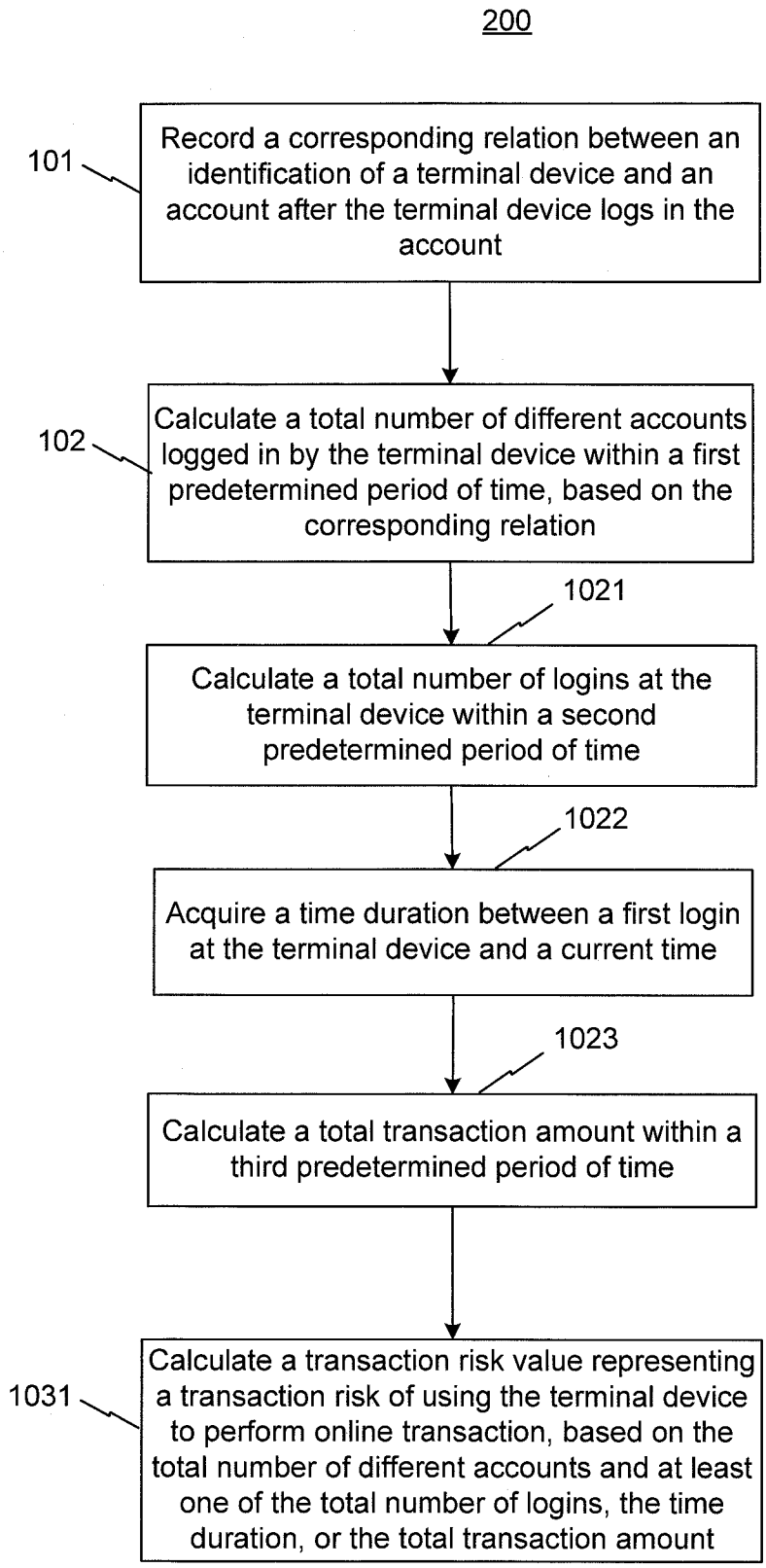
200
101
Record a corresponding relation between an identification of a terminal device and an account after the terminal device logs in the account
102
Calculate a total number of different accounts logged in by the terminal device within a first predetermined period of time, based on the corresponding relation
1021
Calculate a total number of logins at the terminal device within a second predetermined period of time
1022
Acquire a time duration between a first login at the terminal device and a current time
1023
Calculate a total transaction amount within a third predetermined period of time
1031
Calculate a transaction risk value representing a transaction risk of using the terminal device to perform online transaction, based on the total number of different accounts and at least one of the total number of logins, the time duration, or the total transaction amount

Fig. 2

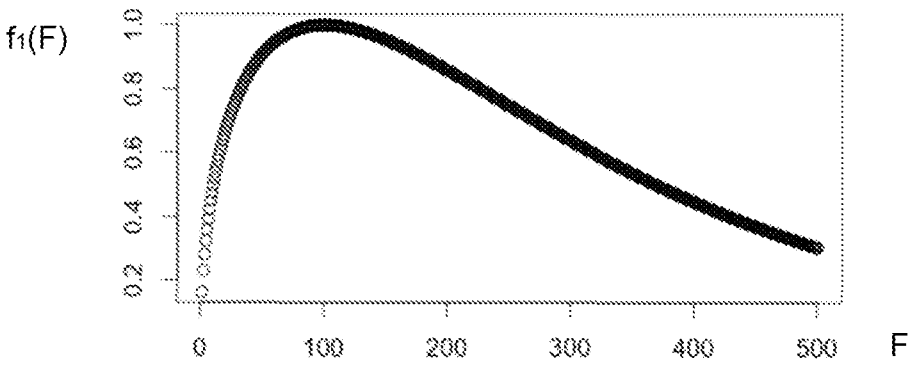

Fig. 3

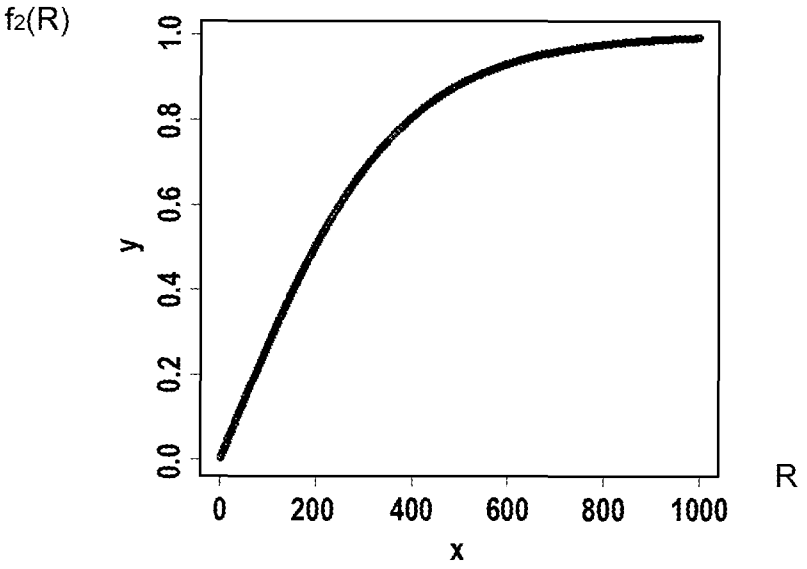

Fig. 4

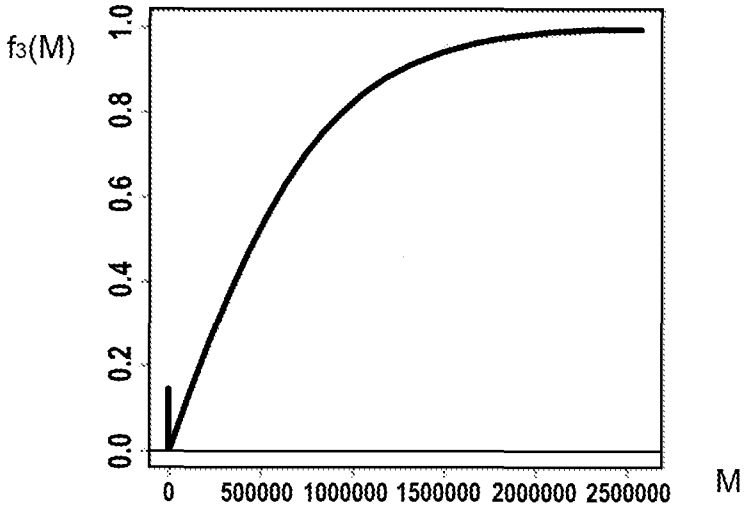

Fig. 5

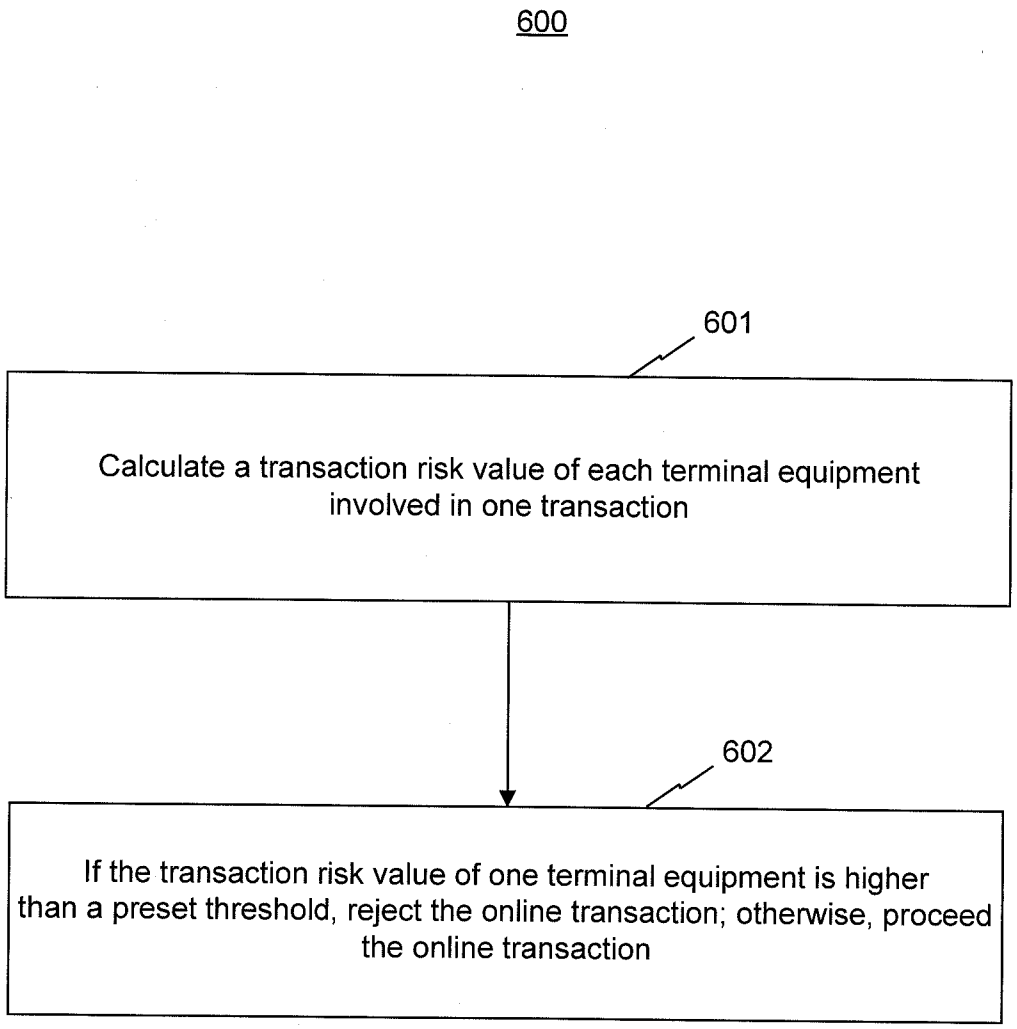
600
601
Calculate a transaction risk value of each terminal equipment involved in one transaction
602
If the transaction risk value of one terminal equipment is higher than a preset threshold, reject the online transaction; otherwise, proceed the online transaction

Fig. 6

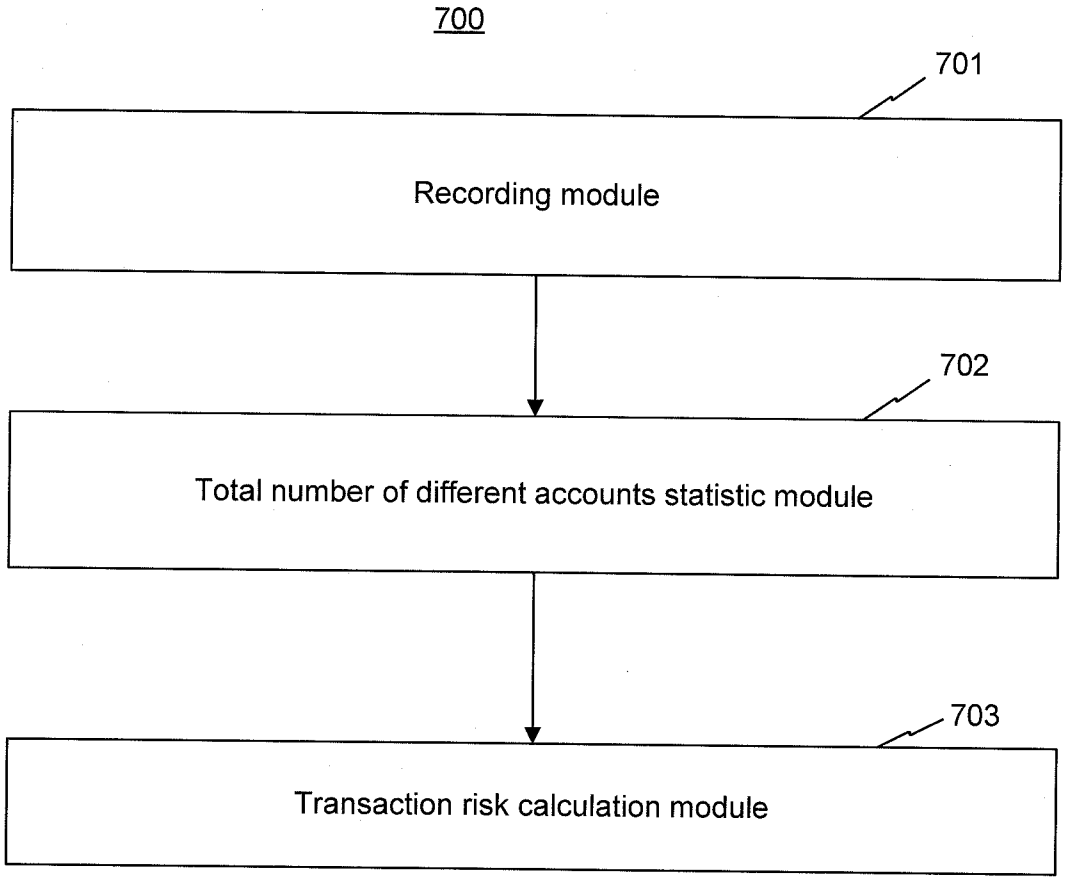
700
701
Recording module
702
Total number of different accounts statistic module
703
Transaction risk calculation module

Fig. 7

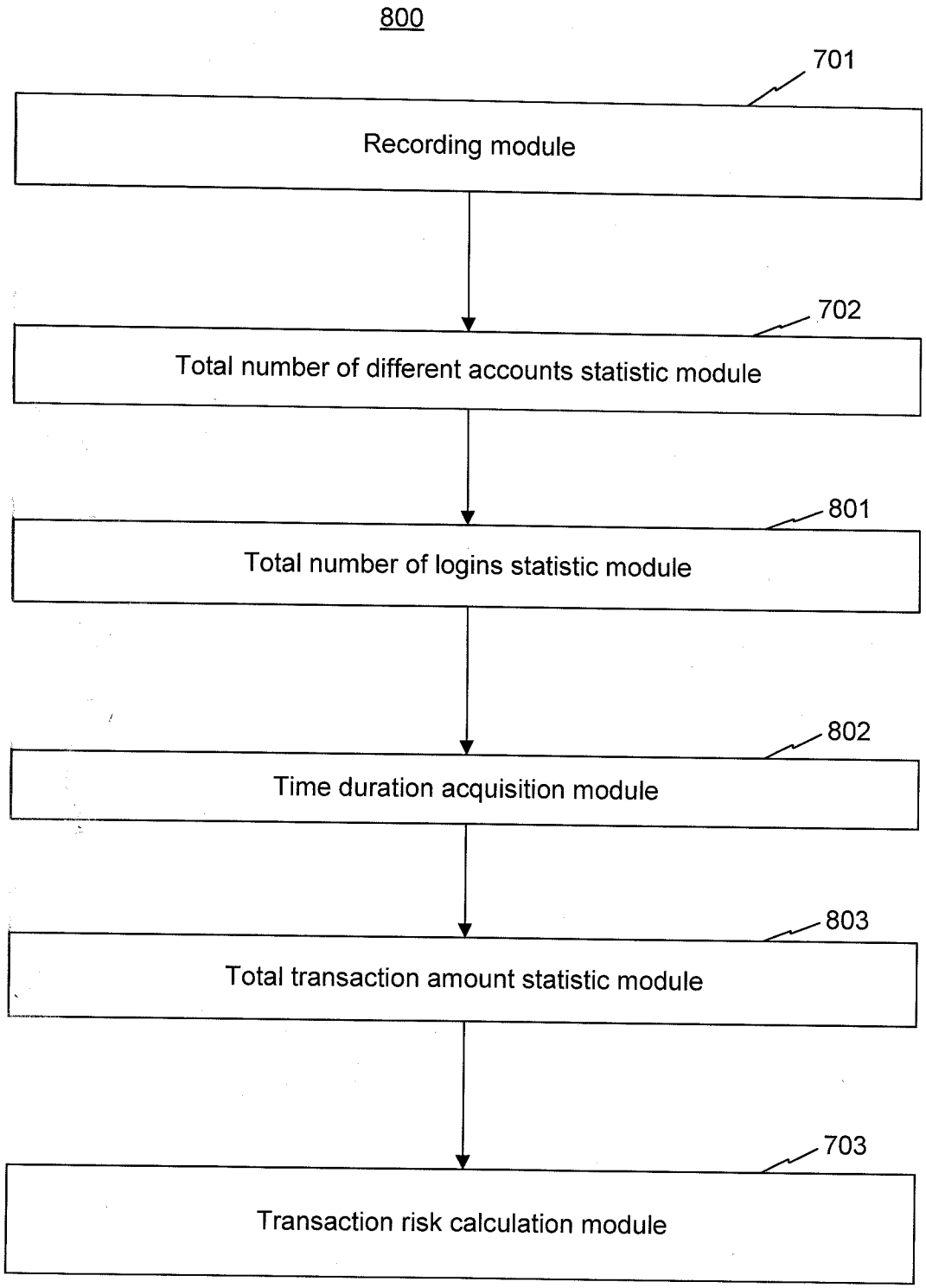
800
701
Recording module
702
Total number of different accounts statistic module
801
Total number of logins statistic module
802
Time duration acquisition module
803
Total transaction amount statistic module
703
Transaction risk calculation module

Fig. 8

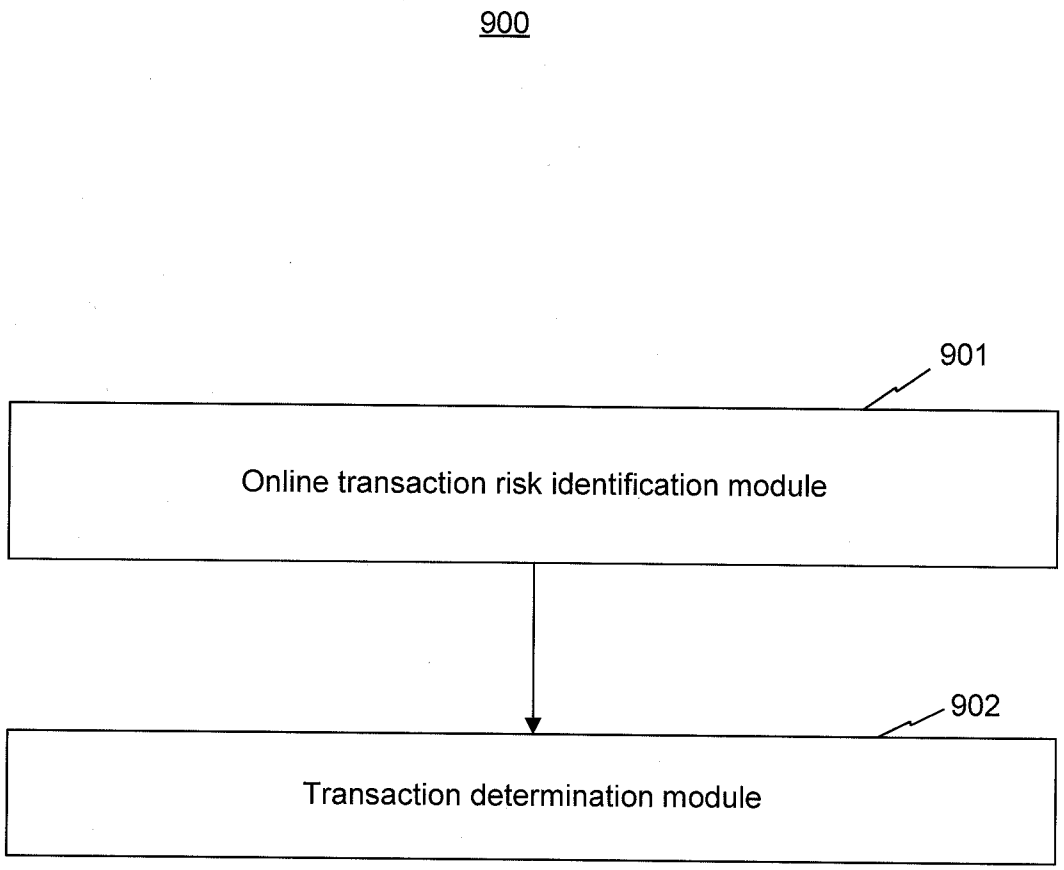
900
901
Online transaction risk identification module
902
Transaction determination module

Fig. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/013058

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/32 (2016.01)
CPC - H04L 9/32 (2016.01)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - H04L 9/00; 32; 29/06 (2016.01)
CPC - H04L 9/32; 63/00; 08; 0876 (2016.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 713/168; 713/189; 726/22; 726/26 (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Orbit, Google Patents, Google Scholar, Google
Search terms used: account, login, device, risk, transaction

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2013/0239182 A1 (IOVATION INC) 12 September 2013 (12.09.2013) entire document	1, 2, 11-13, 20 --- 3-10, 14-19
Y	US 8,452,980 B1 (BLACK et al) 28 May 2013 (28.05.2013) entire document	3, 5-10, 14, 16-19
Y	US 2008/0195528 A1 (KEITHLEY) 14 August 2008 (14.08.2008) entire document	4-10, 15-19
A	US 2012/0109821 A1 (BARBOUR et al) 03 May 2012 (03.05.2012) entire document	1-20
A	US 2011/0191200 A1 (BAYER et al) 04 August 2011 (04.08.2011) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 February 2016	11 MAR 2016
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-8300	Authorized officer Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774