

METHOD AND APPARATUS FOR IDENTIFYING RISKY BEHAVIOR

Technical Field

The present application relates to the field of computer technologies, and in particular, to a method and an apparatus for identifying a network risky behavior.

Related Art

With development of the Internet, network behaviors of people interweave more frequently. Conceptually, a network behavior refers to a process of acquiring, sending, or transmitting network data by each network individual in the network, which generally includes: information query, file downloading, mail sending, and the like. In addition to normal network behaviors, abnormal network behaviors conducted by network individuals intentionally or unintentionally, such as browsing information irrelevant to work by a company employee during work or illegally querying an expense history by network customer service staff, may cause loss. To deal with the above problem, a risk monitoring system for monitoring a network risky behavior comes into being.

At present, a conventional risk monitoring system, by constructing a rule engine, extracts and analyzes characteristics of network behaviors that conform to definitions of rules, thereby identifying risks of network behaviors. However, the rules employed by the rule engine usually have vulnerabilities, and it is necessary to continuously add rules to remedy the vulnerabilities of the rules. This may definitely increase the workload of developers, and the efficiency is low. In addition, the rule engine itself needs to consume extra computer resources, thus causing burden to a computer system.

Summary of the Invention

Embodiments of the present application provide a method and an apparatus for identifying a risky behavior to solve the problem of low efficiency in the prior art caused by remedying a rule vulnerability during identification of a network behavior risk, and the problem that a rule engine consumes extra computer resources.

The method for identifying a risky behavior provided in the embodiments of the present application includes:

acquiring behavior data of a user;

determining a risk coefficient of a specific behavior link in the behavior data; and

judging, according to the risk coefficient, whether the specific behavior link is risky.

The apparatus for identifying a risky behavior provided in the embodiments of the present application includes:

an acquisition module configured to acquire behavior data of a user;

a determination module configured to determine a risk coefficient of a specific behavior link in the behavior data; and

a judgment module configured to judge, according to the risk coefficient, whether the specific behavior link is risky.

The at least one technical solution employed in the embodiments of the present application can achieve the following beneficial effects:

In the embodiments of the present application, behavior data of a user is acquired, and a specific behavior link is selected from the behavior data; a risk coefficient of the specific behavior link in the behavior data is determined by means of calculations, and finally, it is determined, according to the risk coefficient, whether the specific behavior link is risky. Compared with the rule engine manner, in the foregoing process, it is unnecessary to remedy a rule vulnerability manually, thus improving the efficiency of behavior risk identification. In addition, the foregoing process avoids the disadvantage that the rule engine consumes extra computer resources, thus alleviating burden of a computer system.

Brief Description of the Accompanying Drawings

The accompanying drawings described here are used to provide further understanding of the present application and constitute a part of the present application. The schematic embodiments of the present application and the description thereof are used to illustrate the present application, but do not constitute improper limitations to the present application. In the drawings:

FIG. 1 shows a process of a method for identifying a risky behavior according to an embodiment of the present application;

FIG. 2 shows a process of selecting a specific behavior link from behavior data in a method for identifying a risky behavior according to an embodiment of the present application;

FIG. 3 shows a process of determining a short-term risk coefficient in a method for identifying a risky behavior according to an embodiment of the present application;

FIG. 4 shows a process of determining a historical risk coefficient in a method for identifying a risky behavior according to an embodiment of the present application;

FIG. 5 shows a process of determining a team risk coefficient in a method for identifying a risky behavior according to an embodiment of the present application;

FIG. 6 shows a process of judging whether a specific behavior link is risky in a method for identifying a risky behavior according to an embodiment of the present application; and

FIG. 7 is a schematic structural diagram of an apparatus for identifying a risky behavior according to an embodiment of the present application.

Detailed Description

In order to make the objectives, technical solutions, and advantages of the present application clearer, the technical solutions of the present application are described clearly and completely below with reference to the specific embodiments of the present application and the corresponding drawings. Apparently, the described embodiments are merely some of rather than all of the embodiments of the present application. Based on the embodiments in the present application, all other embodiments obtained by those of ordinary skill in the art without paying creative efforts all belong to the protection scope of the present application.

FIG. 1 shows a process of a method for identifying a risky behavior according to an embodiment of the present application, which includes the following steps:

S11: Behavior data of a user is acquired.

In the embodiment of the present application, the behavior data is obtained through a network monitoring system. The network monitoring system monitors and controls computers in a network to record Internet activities (network behavior) conducted by users in the network in a time dimension. The network monitoring system includes monitoring hardware or monitoring software, and the network includes a local area network, a metropolitan area network, or a wide area network. The behavior data above is stored in a particular storage medium, and according to an actual analysis requirement, corresponding behavior data is extracted from the storage medium for analysis.

In this specification, an e-business website is taken as an example to introduce the technical solutions of the present application. Hence, the method for identifying a risky behavior is used for monitoring whether a network behavior of customer service staff of an e-business website is risky.

S12: A specific behavior link is selected from the behavior data. A behavior link refers to a combination obtained by sequentially arranging multiple behaviors according to occurrence times. As a behavior link is closer to an actual behavior intention of the user, the credibility of network behavior risk identification is improved.

FIG. 2 shows a process of selecting a specific behavior link from behavior data in a method for identifying a risky behavior according to an embodiment of the present application. In the embodiment of the present application, step S12 specifically includes the following steps:

S121: Fragment data in a specific time period is selected from behavior data.

Still taking the example in this specification, it is assumed that a network individual that needs a behavior risk analysis is a user M. In this case, fragment data of the user M in a specific time period on a particular day D is extracted from the storage medium. If the specific time period is 15 minutes, for example, 13:10 to 13:25, the fragment data refers to data about behaviors conducted by the user M in the time period of 13:10 to 13:25 on that day.

S122: Behaviors included in the fragment data are acquired.

In the foregoing example, it is assumed that in the time period of 13:10 to 13:25 on that day, behaviors conducted by the user M include a behavior X, a behavior Y, and a behavior Z.

S123: The behaviors are sorted in chronological order according to occurrence times to obtain a behavior link.

In the foregoing example, sorting is carried out in chronological order according to occurrence times of the behavior X, the behavior Y, and the behavior Z, and an obtained specific behavior link G is: behavior X→behavior Y→behavior Z.

S13: A risk coefficient of the specific behavior link in the behavior data is determined.

In the embodiment of the present application, the risk coefficient is a numerical value for expressing the degree of rareness of a specific behavior link G. Generally, if a network behavior

has a relatively high probability of occurrence, i.e., the network behavior is relatively common, it indicates that the network behavior is a normal behavior, e.g., a behavior of viewing shop information by customer service staff. If a network behavior has a relatively low probability of occurrence, i.e., the network behavior only occurs in extremely rare conditions, it indicates that the network behavior is a risky behavior, e.g., a behavior of querying expense histories of relatives and friends by customer service staff. The present application judges, according to the risk coefficient, whether a network behavior is risky.

In the embodiment of the present application, the foregoing risk coefficient includes one or more of a short-term risk coefficient a , a historical risk coefficient b , and a team risk coefficient c . Certainly, in other embodiments of the present application, the analyzed risk coefficient may not be limited to the foregoing three types. The short-term risk coefficient a refers to a degree of rareness of operating the specific behavior link G by the user M in a first time period t_1 (such as one day). The historical risk coefficient b refers to a degree of rareness of operating the specific behavior link G by the user M in a total time length t_2 of registration of the user (an interval from a registration time to a current time). If it is defined that a user population to which the user M belongs is a user group and the user group includes multiple users, the team risk coefficient c refers to a degree of rareness of operating the specific behavior link G by the user group to which the user M belongs.

Processes of determining the foregoing risk coefficients will be described in detail below:

FIG. 3 shows a process of determining a short-term risk coefficient in a method for identifying a risky behavior according to an embodiment of the present application, which specifically includes the following steps:

S131: A total number of operations s_1 that the user M operates all behavior links in a first time period t_1 is acquired.

Still taking the example in this specification, assuming that the first time period t_1 is one day, the number of all behavior links (i.e., the total number of operations s_1) conducted by the user M on that day may be counted based on behavior data of the user M on that day. In the embodiment of the present application, the total number of operations s_1 of the user M on that day is counted by using a time interval t_g that a single specific behavior link G lasts as a reference. Specifically, if t_g is 15 minutes, the total number of operations $s_1=24*60/15=96$.

S132: The number of operations s_2 that the user M operates the specific behavior link G in

the first time period t_1 is acquired.

In the foregoing example, the set first time period t_1 is one day, and thus the number of times (i.e., the number of operations s_2) that the user M operates the specific behavior link G on that day is counted. Specifically, if t_G is 15 minutes, the day is divided into several 15-minute time slices, and it is sequentially judged whether the specific behavior link G occurs in each 15-minute time slice; if yes, the number of operations s_2 is incremented by 1, and if no, the number of operations s_2 is incremented by 0, till the number of operations s_2 on that day is obtained.

S133: A ratio of the total number of operations s_1 to the number of operations s_2 is determined to obtain the short-term risk coefficient a .

In the embodiment of the present application, a formula for calculating the short-term risk coefficient a is as follows:

$$a=s_1/s_2.$$

FIG. 4 shows a process of determining a historical risk coefficient in a method for identifying a risky behavior according to an embodiment of the present application, which specifically includes the following steps:

S134: A total time length t_2 of the user M from a registration time t_0 to a current time t_a is acquired.

Still taking the example in this specification, it is assumed that the registration time t_0 of the user M in a customer service system of an e-business website is January 1st, 2014, and a current time t_a is January 1st, 2015; in this case, the total time length t_2 is 365 days.

S135: An actual time length t_3 that the user M operates the specific behavior link G is acquired.

In the embodiment of the present application, in the step of acquiring an actual time length t_3 that the user M operates the specific behavior link G, calculation is carried out on a daily basis. In this case, behavior data of the user M in the 365 days is split into 365 pieces of fragment data on a daily basis, and it is sequentially judged whether the specific behavior link G occurs in fragment data of each day; if yes, the actual time length t_3 is incremented by 1; and if no, the actual time length t_3 is incremented by 0, till the actual number of days (i.e., the actual time length t_3) that the user M operates the specific behavior link G is obtained.

S136: The historical risk coefficient b is determined according to the total time length t_2 and the actual time length t_3 .

In the embodiment of the present application, for an old user, as the user registers at an earlier time, the total time length t_2 is relatively long (such as 3 years). Assuming that the actual time length t_3 that the old user operates the specific behavior link G is 2 days, it is finally concluded that the probability of operating the specific behavior link G by the old user in the total time length t_2 is relatively low. However, for a new user, as the user registers recently, the total time length t_2 is relatively short (such as 5 days). Assuming that the actual time length t_3 that the new user operates the specific behavior link G is 2 days, it is finally concluded that the probability of operating the specific behavior link G by the new user in the total time length t_2 is relatively high. As can be seen, the difference between new and old users may affect the credibility of the historical risk coefficient b , and in order to smooth the difference between new and old users, step S136 specifically includes:

First of all, the total time length t_2 and the actual time length t_3 are smoothed to obtain a smooth total time length t_{2k} and a smooth actual time length t_{3k} . In the embodiment of the present application, the smoothing may be logarithmic processing, modulo processing, root extraction processing, or the like. Taking the logarithmic processing manner as an example, $t_{2k} = \lg t_2$; and $t_{3k} = \lg t_3$. Certainly, the base of the logarithmic processing is not limited.

Then, calculations are carried out on the smooth actual time length t_{3k} and the smooth total time length t_{2k} to obtain the historical risk coefficient b . In the embodiment of the present application, a formula for calculating the historical risk coefficient b is as follows:

$$b = (1 + t_{3k}) / (1 + t_{2k}) = (1 + \lg t_3) / (1 + \lg t_2).$$

FIG. 5 shows a process of determining a team risk coefficient in a method for identifying a risky behavior according to an embodiment of the present application, which specifically includes the following steps:

S137: A total number of users n included in a user group to which the user M belongs is determined.

Still taking the example in this specification, it is assumed that the user M is customer service staff of an e-business website. In this case, a department to which the user M belongs is the user group. It is assumed that the total number of users n included in this department is 20.

S138: An actual number of users m who have operated the specific behavior link G in a second time period t_4 is acquired in the user group.

In the foregoing example, if the second time period t_4 is one day, the step S138 is used to count the number of persons who have operated the specific behavior link G (i.e., the actual number of users m) on a particular day among the 20 persons in the department to which the user M belongs. Specifically, behavior data of the 20 persons in the department on that day is separately acquired in advance, and then it is sequentially viewed whether the 20 users have operated the specific behavior link G on that day; if yes, the actual number of users m is incremented by 1; and if no, the actual number of users m is incremented by 0, till the actual number of users m who have operated the specific behavior link G on that day is obtained.

S139: The team risk coefficient c is determined according to the total number of users n and the actual number of users m .

In the embodiment of the present application, if the user group that needs to be analyzed includes a large number of users (for example, $n=1000$), and if it is obtained that the actual number of users m who have operated the specific behavior link G on a particular day is equal to 5, at this point, it indicates that the probability that the specific behavior link G has been operated in the user group is relatively low. However, if the user group that needs to be analyzed includes a small number of users (for example, $n=10$), and if it is obtained that the actual number of users m who have operated the specific behavior link G on a particular day is equal to 5, at this point, it indicates that the probability that the specific behavior link G has been operated in the user group is relatively high. As can be seen, different numbers of users in different user groups may affect the credibility of the team risk coefficient c , and in order to smooth the different numbers of users in different user groups, step S139 specifically includes:

First of all, the total number of users n and the actual number of users m are smoothed to obtain a smooth total number of users p and a smooth actual number of users q . In the embodiment of the present application, the smoothing may be logarithmic processing, modulo processing, root extraction processing, or the like. Taking the logarithmic processing manner as an example, $p=\lg n$; and $q=\lg m$. Certainly, the base of the logarithmic processing is not limited.

Then, calculations are carried out on the smooth total number of users p and the smooth actual number of users q to obtain the team risk coefficient c . In the embodiment of the present application, a formula for calculating the team risk coefficient c is as follows:

$$c=(1+p)/(1+q)=(1+lg n)/(1+lg m).$$

S14: It is judged, according to the risk coefficient r , whether the specific behavior link G is risky.

In the embodiment of the present application, a formula for calculating the risk coefficient r is as follows:

$$r=a \times b \times c.$$

Certainly, in other embodiments of the present application, the risk coefficient $r=a+b+c$.

FIG. 6 shows a process of judging whether a specific behavior link is risky in a method for identifying a risky behavior according to an embodiment of the present application. In the embodiment of the present application, step S14 specifically includes:

S141: Risk coefficients r of behavior links are sorted in descending order.

Still taking the example in this specification, it is assumed that the extracted behavior data is all behavior links of the user M on a particular day D . In the behavior data, there are 100 pieces of monitored behavior links; in this case, risk coefficients r_1 to r_{100} of the 100 behavior links are separately determined according to the foregoing method, and then the risk coefficients r_1 to r_{100} are sorted in descending order.

S142: It is judged whether the risk coefficient r_G corresponding to the specific behavior link G is in risk ranks.

In the embodiment of the present application, a higher rank of a risk coefficient indicates a higher degree of rareness of the behavior link and a higher risk coefficient thereof. Assuming that a preset risk rank is top 3, it is judged whether the risk coefficient r_G corresponding to the specific behavior link G is ranked top 3.

S143: If yes, it is determined that the specific behavior link G is risky.

If the risk coefficient r_G corresponding to the specific behavior link G is ranked top 3, it indicates that the specific behavior link G is risky, and subsequently, the specific behavior link G may be published as a risky behavior to tell customer service staff of an e-business website not to operate the behavior link.

S144: If no, it is judged that the specific behavior link G is not risky.

If the risk coefficient r_G corresponding to the specific behavior link G is not ranked top 3, it indicates that the specific behavior link G is not risky.

FIG. 7 is a schematic structural diagram of an apparatus for identifying a risky behavior according to an embodiment of the present application. Based on the same idea, the apparatus includes:

an acquisition module 10 configured to acquire behavior data of a user;

a selection module 20 configured to select a specific behavior link from the behavior data;

a determination module 30 configured to determine a risk coefficient of the specific behavior link in the behavior data; and

a judgment module 40 configured to judge, according to the risk coefficient, whether the specific behavior link is risky.

In the embodiment of the present application, the selection module 20 is specifically configured to:

select, from the behavior data, fragment data in a specific time period;

acquire behaviors included in the fragment data; and

sort the behaviors in chronological order according to occurrence times to obtain the specific behavior link.

In the embodiment of the present application, the risk coefficient includes one or more of a short-term risk coefficient, a historical risk coefficient, and a team risk coefficient.

In the embodiment of the present application, the determination module 30 includes a short-term risk determination module 31 configured to:

acquire a total number of operations that the user operates all behavior links in a first time period;

acquire the number of operations that the user operates the specific behavior link in the first time period; and

determine a ratio of the total number of operations to the number of operations to obtain the short-term risk coefficient.

In the embodiment of the present application, the determination module 30 includes a historical risk determination module 32 configured to:

acquire a total time length for the user from a registration time to a current time;

acquire an actual time length that the user operates the specific behavior link; and

determine the historical risk coefficient according to the total time length and the actual time length.

In the embodiment of the present application, the determination module 30 includes a team risk determination module 33 configured to:

determine a total number of users included in a user group to which the user belongs;

acquire, in the user group, an actual number of users who have operated the specific behavior link in a second time period; and

determine the team risk coefficient according to the total number of users and the actual number of users.

In the embodiment of the present application, the historical risk determination module 32 includes a first smoothing unit configured to:

smooth the total time length and the actual time length to obtain a smooth total time length and a smooth actual time length; and

carry out calculations on the smooth actual time length and the smooth total time length to obtain the historical risk coefficient.

In the embodiment of the present application, the team risk determination module 33 includes a second smoothing unit configured to:

smooth the total number of users and the actual number of users to obtain a smooth total number of users and a smooth actual number of users; and

carry out calculations on the smooth total number of users and the smooth actual number of

users to obtain the team risk coefficient.

In the embodiment of the present application, the determination module 30 is specifically configured to: multiply or sum the short-term risk coefficient, the historical risk coefficient, and the team risk coefficient to obtain the risk coefficient.

In the embodiment of the present application, the judgment module 40 is specifically configured to:

sort risk coefficients of behavior links in descending order;

judge whether the risk coefficient corresponding to the specific behavior link is in risk ranks;
and

if yes, judge that the specific behavior link is risky; and if no, judge that the specific behavior link is not risky.

The method and apparatus provided in the embodiments of the present application acquire behavior data of a user, select a specific behavior link from the behavior data, determine a risk coefficient of the specific behavior link in the behavior data by means of calculations, and finally, determine, according to the risk coefficient, whether the specific behavior link is risky. Compared with the rule engine manner, in the foregoing process, it is unnecessary to remedy a rule vulnerability manually, thus improving the efficiency of behavior risk identification. In addition, the foregoing process avoids the disadvantage that the rule engine consumes extra computer resources, thus alleviating burden of a computer system.

In the embodiment of the present application, three factors: short-term (such as a particular day), history (from a registration time to a current time), and team (a user group to which the user belongs), are comprehensively considered to analyze whether a behavior of a user is risky, thus reducing the impact of some sudden factor transitions (such as service orientation adjustment of the team or job transfer of the user) on the behavior link of the user, thereby improving the accuracy and credibility of risky behavior identification.

It is worth mentioning that, the apparatus for identifying a risky behavior disclosed in this specification is generated according to the same idea based on the method for identifying a risky behavior. Therefore, the method for identifying a risky behavior may continue to use all technical features of the above apparatus for identifying a risky behavior. Details are not described here again.

It should be additionally noted that, formulas for calculating the risk coefficients in the present application are not limited to the disclosed embodiments. For example, in other embodiments, the short-term risk coefficient $a=s_2/s_1$; the historical risk coefficient $b=(1+\lg t_2)/(1+\lg t_3)$; and the team risk coefficient $c=(1+\lg m)/(1+\lg n)$. Correspondingly, during subsequent judgment of whether the behavior link is risky, risk coefficients of behavior links are sorted in ascending order to judge whether the risk coefficient corresponding to the specific behavior link is in risk ranks.

Persons skilled in the art should understand that, the embodiments of the present invention may be provided as a method, a system, or a computer program product. Therefore, the present invention may be implemented in the form of a complete hardware embodiment, a complete software embodiment, or an embodiment combining software and hardware. Moreover, the present invention may employ the form of a computer program product implemented on one or more computer usable storage media (including, but not limited to, a magnetic disk memory, a CD-ROM, an optical memory, and the like) including computer usable program code.

The present invention is described with reference to flowcharts and/or block diagrams of the method, device (system), and computer program product according to the embodiments of the present invention. It should be understood that computer program instructions may be used to implement each process and/or block in the flowcharts and/or block diagrams and a combination of a process and/or a block in the flowcharts and/or the block diagrams. These computer program instructions may be provided for a general-purpose computer, a special-purpose computer, an embedded processor, or a processor of another programmable data processing device to generate a machine, so that the instructions executed by a computer or a processor of another programmable data processing device generate an apparatus for implementing a specified function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

These computer program instructions may also be stored in a computer readable memory that can instruct the computer or another programmable data processing device to work in a particular manner, such that the instructions stored in the computer readable memory generate an article of manufacture that includes an instruction apparatus. The instruction apparatus implements a specified function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

These computer program instructions may also be loaded onto a computer or another

programmable data processing device, such that a series of operating steps are performed on the computer or another programmable device, thereby generating computer-implemented processing. Therefore, the instructions executed on the computer or another programmable device provide steps for implementing a specified function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

In a typical configuration, the computing device includes one or more processors (CPUs), an input/output interface, a network interface, and a memory.

The memory may include a volatile memory, a random access memory (RAM) and/or a non-volatile memory or the like in a computer readable medium, for example, a read-only memory (ROM) or a flash RAM. The memory is an example of the computer readable medium.

The computer readable medium includes non-volatile or volatile, and movable or non-movable media, and can implement information storage by means of any method or technology. Information may be a computer readable instruction, a data structure, and a module of a program or other data. A storage medium of a computer includes, for example, but is not limited to, a phase change memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), other types of random access memories (RAMs), a read-only memory (ROM), an electrically erasable programmable read-only memory (EEPROM), a flash memory or other memory technologies, a compact disc read-only memory (CD-ROM), a digital versatile disc (DVD) or other optical storages, a cassette tape, a magnetic tape/magnetic disk storage or other magnetic storage devices, or any other non-transmission medium, and can be used to store information accessible to the computing device. According to the definition in this text, the computer readable medium does not include transitory media, such as a modulated data signal and a carrier.

It should be further noted that, the terms "include", "comprise", or any variants thereof are intended to cover a non-exclusive inclusion, such that a process, a method, a commodity or a device that includes a series of elements not only includes such elements but also includes other elements not specified expressly, or may further include inherent elements of the process, method, commodity, or device. Without more restrictions, an element limited by the phrase "include a/an..." does not exclude other same elements existing in the process, method, commodity, or device that includes the element.

Persons skilled in the art should understand that, the embodiments of the present application may be provided as a method, a system, or a computer program product. Therefore, the present

application may be implemented in the form of a complete hardware embodiment, a complete software embodiment, or an embodiment combining software and hardware. Moreover, the present application may employ the form of a computer program product implemented on one or more computer usable storage media (including, but not limited to, a magnetic disk memory, a CD-ROM, an optical memory, and the like) including computer usable program code.

The above are merely the embodiments of the present application, which are not used to limit the present application. For persons skilled in the art, the present application may have various changes and alterations. Any modification, equivalent replacement, and improvement made in the spirit and principle of the present application should be included in the scope of the claims of the present application.

CLAIMS

What is claimed is:

1. A computer-implemented method, comprising:
 - determining behavior data of a user, wherein the behavior data describes user activities of the user using a computer network;
 - identifying a particular event chain from the behavior data, wherein the particular event chain includes one or more events of the user activities;
 - determining a risk coefficient of the particular event chain, wherein the risk coefficient expresses the degree of rareness of the particular event chain; and
 - based on the risk coefficient, determining whether the particular event chain represents a risky user behavior.
2. The computer-implemented method of claim 1, wherein identifying the particular event chain from the behavior data comprises:
 - identifying a time period;
 - based on behavior data corresponding to the time period, determining events occurred during the time period; and
 - determining the particular event chain by sorting the determined events in a chronological order.
3. The computer-implemented method of claim 1, wherein the risk coefficient comprises one or more of a short-term risk coefficient, a long-term risk coefficient, or a group risk coefficient.
4. The computer-implemented method of claim 3, wherein determining the short-term risk coefficient comprises:
 - determining a short-term time period associated with the short-term risk coefficient;
 - determining a total number of event chains the user performed in the short-term time period;
 - determining a number of times the user performed the particular event chain in the short-term time period; and

determining the short-term risk coefficient based on the total number of event chains and the number of times the user performed the particular event chain.

5. The computer-implemented method of claim 3, wherein determining the long-term risk coefficient comprises:

determining a long-term time period associated with the long-term risk coefficient;

determining a time length that the user performed the particular event chain during the long-term time period; and

determining the long-term risk coefficient based on the long-term time period and the time length for performing the particular event chain.

6. The computer-implemented method of claim 3, wherein determining the group risk coefficient comprises:

determining a total number of users in a user group associated with the user;

determining a group time period associated with the group risk coefficient;

determining a number of users in the user group that performed the particular event chain in the group time period; and

determining the group risk coefficient based on the total number of users in the user group and the number of users that performed the particular event chain.

7. The computer-implemented method of claim 1, wherein determining whether the particular event chain represents a risky user behavior comprises determining whether the risk coefficient is higher than a threshold.

8. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

determining behavior data of a user, wherein the behavior data describes user activities of the user using a computer network;

identifying a particular event chain from the behavior data, wherein the particular event chain includes one or more events of the user activities;

determining a risk coefficient of the particular event chain, wherein the risk coefficient expresses the degree of rareness of the particular event chain; and

based on the risk coefficient, determining whether the particular event chain represents a risky user behavior.

9. The non-transitory, computer-readable medium of claim 8, wherein identifying the particular event chain from the behavior data comprises:

identifying a time period;

based on behavior data corresponding to the time period, determining events occurred during the time period; and

determining the particular event chain by sorting the determined events in a chronological order.

10. The non-transitory, computer-readable medium of claim 8, wherein the risk coefficient comprises one or more of a short-term risk coefficient, a long-term risk coefficient, or a group risk coefficient.

11. The non-transitory, computer-readable medium of claim 10, wherein determining the short-term risk coefficient comprises:

determining a short-term time period associated with the short-term risk coefficient;

determining a total number of event chains the user performed in the short-term time period;

determining a number of times the user performed the particular event chain in the short-term time period; and

determining the short-term risk coefficient based on the total number of event chains and the number of times the user performed the particular event chain.

12. The non-transitory, computer-readable medium of claim 10, wherein determining the long-term risk coefficient comprises:

determining a long-term time period associated with the long-term risk coefficient;

determining a time length that the user performed the particular event chain during the long-term time period; and

determining the long-term risk coefficient based on the long-term time period and the time length for performing the particular event chain.

13. The non-transitory, computer-readable medium of claim 10, wherein determining the group risk coefficient comprises:

- determining a total number of users in a user group associated with the user;
- determining a group time period associated with the group risk coefficient;
- determining a number of users in the user group that performed the particular event chain in the group time period; and

- determining the group risk coefficient based on the total number of users in the user group and the number of users that performed the particular event chain.

14. The non-transitory, computer-readable medium of claim 8, wherein determining whether the particular event chain represents a risky user behavior comprises determining whether the risk coefficient is higher than a threshold.

15. A computer-implemented system, comprising:

- one or more computers; and

- one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing instructions that, when executed by the one or more computers, perform operations comprising:

- determining behavior data of a user, wherein the behavior data describes user activities of the user using a computer network;

- identifying a particular event chain from the behavior data, wherein the particular event chain includes one or more events of the user activities;

- determining a risk coefficient of the particular event chain, wherein the risk coefficient expresses the degree of rareness of the particular event chain; and

- based on the risk coefficient, determining whether the particular event chain represents a risky user behavior.

16. The computer-implemented system of claim 15, wherein identifying the particular event chain from the behavior data comprises:

identifying a time period;
based on behavior data corresponding to the time period, determining events occurred during the time period; and
determining the particular event chain by sorting the determined events in a chronological order.

17. The computer-implemented system of claim 15, wherein the risk coefficient comprises one or more of a short-term risk coefficient, a long-term risk coefficient, or a group risk coefficient.

18. The computer-implemented system of claim 17, wherein determining the short-term risk coefficient comprises:

determining a short-term time period associated with the short-term risk coefficient;
determining a total number of event chains the user performed in the short-term time period;
determining a number of times the user performed the particular event chain in the short-term time period; and
determining the short-term risk coefficient based on the total number of event chains and the number of times the user performed the particular event chain.

19. The computer-implemented system of claim 17, wherein determining the long-term risk coefficient comprises:

determining a long-term time period associated with the long-term risk coefficient;
determining a time length that the user performed the particular event chain during the long-term time period; and
determining the long-term risk coefficient based on the long-term time period and the time length for performing the particular event chain.

20. The computer-implemented system of claim 17, wherein determining the group risk coefficient comprises:

determining a total number of users in a user group associated with the user;
determining a group time period associated with the group risk coefficient;

determining a number of users in the user group that performed the particular event chain in the group time period; and

determining the group risk coefficient based on the total number of users in the user group and the number of users that performed the particular event chain.