

RISK DETECTION SYSTEM AND RISK DETECTION METHOD

This application claims priority to Taiwan Patent Application No. 109119205 filed on June 8, 2020, which is hereby incorporated by reference in its entirety.

5

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] Embodiments of the present invention relate to a risk detection system and a risk detection method. More specifically, embodiments of the present invention relate to a risk detection system links to a user interface of a network service system and a risk detection method.

10

Descriptions of the Related Art

[0002] Network services (e.g., applying for network accounts, conducting transactions, searching for data, opening accounts in network banks) often suffer from incidents such as identity/credit card theft or the like, which cause serious losses to service users, service providers, or banks. Therefore, in order to reduce risks of network services, service providers or banks often have to carry out identity verification or risk detection on customers through a verification system before further deciding whether to provide the network services. However, the traditional verification system must spend a lot of time and manpower to carry out identity verification or risk detection, which will reduce the efficiency of network services and further affect the customer's service experience. Accordingly, an urgent need exists in the art to

15

20

improve the efficiency of the traditional verification system.

SUMMARY OF THE INVENTION

[0003] In order to solve at least the aforesaid problems, an embodiment of the present invention provides a risk detection system linking to a user interface of a network service system. The risk detection system comprises a risk database and a risk detection module which are electrically connected to each other. The risk detection module may be configured to: store at least one detection condition and corresponded predefined information corresponding to the at least one detection condition; receive input data related to a service from the user interface after the input data is inputted by a user via the user interface but before the input data is transmitted to a verification system; detect whether the input data meets the at least one detection condition according to the risk database; when determining that the input data does not meet any of the at least one detection condition, transmit first detection result data to the network service system so that the network service system transmits the first detection result data and the input data to the verification system; and when determining that the input data meets any of the at least one detection condition, generate and transmit the corresponded predefined information, which corresponds to the detection condition, to the user interface to request reply data from the user, detect whether the input data coordinated with the reply data meets the at least one detection condition according to the risk database after receiving the reply data, and transmit second detection result data to the network service system so that the network service system transmits the second detection result data and the input data to the verification system.

[0004] In order to solve at least the aforesaid problems, an embodiment of the present invention further provides a risk detection method. The risk detection method comprises: receiving, by a risk detection module of a risk detection system, input data related to a service from a user interface of a network service system after the input data is inputted by a user via the user interface but before the input data is transmitted to a verification system, wherein the risk detection system links to the user interface, and the risk detection module stores at least one detection condition and corresponded predefined information corresponding to the at least one detection condition; detecting, by the risk detection module, whether the input data meets the at least one detection condition according to a risk database of the risk detection system; when determining that the input data does not meet any of the at least one detection condition, transmitting, by the risk detection module, first detection result data to the network service system so that the network service system transmits the first detection result data and the input data to the verification system; and when determining that the input data meets any of the at least one detection condition, generating and transmitting, by the risk detection module, the corresponded predefined information, which corresponds to the detection condition, to the user interface to request reply data from the user, detecting whether the input data coordinated with the reply data meets the at least one detection condition according to the risk database after receiving the reply data, and transmitting second detection result data to the network service system so that the network service system transmits the second detection result data and the input data to the verification system.

[0005] According to the embodiments of the present invention, before the network

service system transmits the input data of the user (i.e., the customer) to the traditional verification system for traditional verification, the risk detection module first obtains the input data of the user, and then detect the risk of the input data according to a pre-established risk database in a short time. Next, the risk detection module transmits the pre-detected result data to the network service system, so that the network service system transmits the pre-detected result data along with the input data to the traditional verification system. By detecting the input data in advance at the network service system end (i.e., the front end), the processing time required for traditional verification of the input data at the subsequent verification system end (i.e., the back end) can be effectively reduced or omitted, so that the efficiency of network service can be improved, and the service experience of the customer can be further improved.

In the case where the input data is detected in advance, when it is detected that the input data meets any of at least one detection condition (which represents that the probability that the user cannot pass the traditional verification at the back end may be high), the risk detection module will further propose corresponded predefined information to the user and request reply data, detect the input data according to the risk database and the reply data, and transmit the second detection result data. In addition to reducing the burden of manual inspection required when adopting the traditional verification system, the present invention can also reduce the misjudgment rate through the above-mentioned double detection. Also, the present invention can expand the source of information by setting the risk database at the front end with a lower level of information security risk demand, thereby acquiring the latest risk events in a more real-time manner to prevent illegal acts such as theft and fraud which are constantly changing.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] The attached drawings may assist in explaining various embodiments of the present invention, in which:

5 **FIG. 1** is a block diagram illustrating a risk detection system according to some embodiments of the present invention;

FIG. 2 is a flowchart diagram illustrating the operation of a risk detection system according to some embodiments of the present invention;

FIG. 3A is a schematic view illustrating the operation of an establishment module according to some embodiments of the present invention;

10 **FIG. 3B** is a schematic view illustrating the operation of a relationship graph engine according to some embodiments of the present invention;

FIG. 4 is a schematic view illustrating a correspondence relationship between a detection condition and corresponded predefined information according to some embodiments of the present invention; and

15 **FIG. 5** is a schematic view illustrating a risk detection method according to some embodiments of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

[0007] In the following description, the present invention will be explained with reference to embodiments thereof; however, these embodiments are not intended to limit the present invention to the operations, environment, applications, structures, processes, or steps described in these embodiments. For ease of description, contents that are not directly related

20

to the embodiments of the present invention or that can be appreciated without special explanation will be omitted from depiction herein and in the attached drawings. Dimensions of elements and proportional relationships among individual elements in the attached drawings are only exemplary examples but not intended to limit the scope claimed in the present invention. Unless stated particularly, same (or similar) reference numerals may correspond to same (or similar) elements in the following description. The number of each element described below may be one or more in the case where it can be implemented, unless otherwise specified.

[0008] Terms used in the present disclosure are only used for describing the embodiments and are not intended to limit the scope claimed in the present invention. Singular forms “a” and “an” are also intended to include the plural forms unless the context clearly indicates otherwise. Terms “comprising” , “including” and the like indicate the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence of one or more other features, integers, steps, operations, elements, components, and/or combinations thereof. The term “and/or” includes any and all combinations of one or more associated listed items.

[0009] **FIG. 1** is a block diagram illustrating a risk detection system according to some embodiments of the present invention. However, the content shown in **FIG. 1** is only for purpose of illustrating embodiments of the present invention, and is not for purpose of limiting the scope claimed in the present invention. Referring to **FIG. 1**, the risk detection system **11** may link to a user interface **121** of a network service system **12**, and the network service system

12 may provide various network services, e.g., transaction services and account opening services, to a user which is marked **USR**. The network service system **12** may link to a verification system **13**. The risk detection system **11** may comprise a risk database **112** and a risk detection module **111** electrically connected to each other (directly or indirectly). The risk
5 detection module **111** may store at least one detection condition **R1** and data **C0** to be confirmed corresponding to the at least one detection condition **R1**. In some embodiments, in addition to the risk database **112** and the risk detection module **111**, the risk detection system **11** may optionally comprise an establishment module **113** for the risk database **112** and a relationship graph engine **114**. The establishment module **113** and the relationship graph engine **114** may
10 be electrically connected (directly or indirectly) to the risk database **112**. The risk detection module **111**, the establishment module **113**, and the relationship graph engine **114** may be implemented through appropriate hardware, firmware, and software, wherein the hardware may comprise elements such as a processor, a memory, an input/output interface, and a network interface, while the software and firmware may comprise programs, algorithms or the like
15 required for respective functions thereof.

[0010] Next, the operation of the risk detection system **11** will be described with reference to **FIG. 2** to **FIG. 4**. **FIG. 2** is a flowchart diagram illustrating the operation of the risk detection system **11** according to some embodiments of the present invention, **FIG. 3A** is a schematic view illustrating the operation of an establishment module according to some
20 embodiments of the present invention, **FIG. 3B** is a schematic view illustrating the operation of a relationship graph engine according to some embodiments of the present invention, and

FIG. 4 is a schematic view illustrating a correspondence relationship between a detection condition and corresponded predefined information according to some embodiments of the present invention. However, the contents shown in **FIG. 2** to **FIG. 4** are only for purpose of illustrating embodiments of the present invention, and are not for purpose of limiting the scope claimed in the present invention.

[0011] Referring to both **FIG. 1** and **FIG. 2**, in an operation process **2** of the risk detection system **11**, first of all, the risk detection module **111** may retrieve or receive input data **D1** related to a service from the user interface **121** of the network service system **12** after the input data **D1** is inputted by a user **USR** via the user interface **121** and before the input data **D1** is transmitted to the verification system **13** (which is labeled as action **201**). Next, the risk detection module **111** may detect whether the input data **D1** meets the at least one detection condition according to the risk database **112** (labeled as action **202**) to detect whether the input data **D1** meets at least one detection condition **R1** stored in the risk detection module **111** (labeled as action **203**). In some embodiments, the network service system **12** may have a data transmission module (not shown in **FIG. 1**) to transmit the input data **D1** to the risk detection module **111** after it is detected that the user inputs the data in the field corresponding to the input data **D1** in the user interface **121** or the user changes the page of the user interface in the user interface **121**. In other embodiments, the risk detection module **111** may be disposed at the end of the network service system **12**, and directly links to the user interface **121** to retrieve the input data **D1**.

[0012] In some embodiments, the input data **D1** may be personal data of the user (e.g.,

name, position of the company, birthday, identity card number, phone number, address, related person, photo, credit card number) and data related to the service (e.g., type of commodities which are requested for transaction, quantity of commodities, transaction amount, data of a specific person, or the like).

5 **[0013]** In some embodiments, the risk database **112** has a plurality of fields for detecting whether the at least one detection condition **R1** is met. Moreover, the plurality of fields are related to at least one of the following: data of a specific person (e.g., name, company, position, birthday, identity card number, phone number, address, related person, photo of a specific person) and data of a specific event (e.g., commodity type, commodity quantity, amount, 10 average transaction amount, specific transaction website or commodity, high-priced commodity related to a transaction service, checking data related to a network bank account opening service, abnormal (stolen or fraudulent) commodity/credit card data). For example, the specific person has ever been listed on a blacklist of online transaction services, a financial unit supervision list, an international sanction list, a financial criminal record list or other lists of persons with risks, 15 or holds an important position in a specific organization or group, or has an identity as a government official or the like which is legally subject to supervision. In addition, a related person who has a kinship or business cooperation relationship with the above-mentioned specific person will also be regarded as an object with risk, so the plurality of fields required for the detection condition **R1** stored in the risk database **112** will also be related to data of the 20 related person (e.g., name, company, position, birthday, identity card number, phone number, address, related person, photo of the related person), and will be listed as one of the detection

conditions **R1**. The specific event may be an online transaction service-related event, a data leakage event, a financial report of enterprises (including board of shareholders, subsidiaries, purchase and sale, turnover), a financial crime event, a legal dispute event, financial loans or other related news events.

5 **[0014]** In some embodiments, the data corresponding to each field in the risk database **112** may be as follows: the establishment module **113** directly acquires the data corresponding to each of the plurality of fields from corresponding fields in the structured data stored in at least one public database, or performs a specific format conversion on the structured data stored in the at least one public database to generate the data corresponding to each of the plurality of
10 fields.

[0015] Taking **FIG. 3A** as an example for description, the structured data **300** may come from a public database, and the establishment module **113** may directly obtain data in fields **F21**, **F23** and **F24** of the structured data **300** (i.e., “name”, “related person” and “photo”), and directly import the obtained data into fields **F11**, **F13** and **F14** (i.e., “name”, “related person”
15 and “photo”) of the risk database **112** individually. For another example, the establishment module **113** may perform a specific format conversion (e.g., convert “birthday” into “age”) on the data (i.e., “birthday”) in the field **F22** of the structured data **300**, and then import the generated data into the field **F12** of the risk database **112**.

[0016] In some other embodiments, the data corresponding to each field in the risk
20 database **112** may be corresponding data generated by the establishment module **113** through performing machine recognition on unstructured data (e.g., network data or other data). In

these embodiments, a relationship graph may be built from the unstructured data through the relationship graph engine **114** (detailed steps are described later), and the establishment module **113** generates or updates data corresponding to the plurality fields in the risk database **112** according to the relationship graph. For example, when the processor (not shown) of the risk detection system **11** performs a regular comparison operation, it compares the data corresponding to the plurality of fields in the risk database **112** with the relationship graph **314**, and determines that the person A and the person B are in a parent-child relationship and the person A is a specific person in the existing risk database **112**. Then, the processor adds the name of the person B in the related person field corresponding to the person A in the risk database **112**, and newly adds a piece of data of the person B (e.g., name, company, position, birthday, identity card number, phone number, address, related person, photo). For another example, the processor determines that the person A is related to a financial crime event (e.g., a fraud event) according to the relationship graph **314**, and then the processor may add the financial crime event in the related event field of the person A in the risk database **112**.

[0017] Taking **FIG. 3B** as an example for description, the generation of the relationship graph **314** may be divided into a machine learning stage and a machine recognition stage. In the machine learning stage, unstructured data **310** to be trained (e.g., one or several paragraphs of text) may be marked to generate correlation data **311**, and the correlation data **311** mainly comprises relevance between two entities to establish an initial relationship graph. Next, a series of unstructured data **310** and the correlation data **311** are trained by a relationship graph engine **114** and a model **313** is built. The unstructured data **312** to be identified must be

marked first. For example, the developed automatic marking software is used to automatically mark the unstructured data **312** to be identified after reading the unstructured data **312** to generate the correlation data of the unstructured data **312** to be identified. Then, the unstructured data **312** to be identified and the correlation data thereof are input into the model

5 **313**. Then, the model **313** determines the relevancy between the unstructured data **312** to be identified and the correlation data thereof and the unstructured data already existing in the model **313** and the correlation data thereof according to the input data, adds the correlation data with high relevancy (and the two entities and relevance thereof) to the correlation data **311**, and gradually expands new entities and the relevance between the entities from the initial

10 relationship graph by repeating the above steps continuously to generate the relationship graph **314** with more complete data. Then, the establishment module **113** may generate or update data required for corresponding fields in the risk database **112** according to the relationship graph **314**.

[0018] In the machine learning stage, a variety of different retrieval modes may be

15 adopted to find potentially relevant text paragraphs from the network or different data sources to serve as unstructured data **310** to be trained. The retrieval mode may be, for example but not limited to: a person name retrieval mode, an enterprise name retrieval mode, a UN anti-terrorism sanction list, or real-time fraud related news. For example, in the person name retrieval mode, whether the user is a political figure or a relative thereof, whether the user is

20 listed in the anti-terrorism and UN sanction blacklist, whether the user is a person in charge of an enterprise, a director, a supervisor, and whether there is lawsuit information related to the

user may be retrieved. In the enterprise name retrieval mode, the basic information of the enterprise (shareholders, directors and supervisors, managers, investment subsidiaries), important information, whether there is lawsuit information, loans, endorsements, purchase and sale, receivables/payables may be determined. For example, a real-time fraud news is first

5 retrieved from the network, and then a specific person name and event are retrieved from a section of the real-time fraud news through automatic marking software to serve as two entities and relevance thereof so as to establish a new relationship graph or incorporate it into an existing relationship graph. Then, the specific person name and event are compared with the specific person and specific event data in the risk database. When it is determined that data

10 of the relevant specific person or specific event has already exist in the risk database, then the related person may be filled in the related person field, and when it is determined that there is no data of the relevant specific person or specific event, then the data may be added to the risk database.

[0019] In some embodiments, data sources, data items, and graph entities of

15 unstructured data may be exemplified as follows:

Data source	Data item	Graph entity
Law data retrieval system	Criminal and civil judgement data	Name (or company name), role of parties (plaintiff, defendant ...)
Ministry of Economy business registration	Basic company data issued publicly/non-publicly in domestic	Name, company, position, investment company
Public information observation station	Information on purchase and sale, receivables and	Company, object, dealing subject

	payables of the related person	
Public information observation station	Data on enterprise financial loan and endorsement guarantee	Company, subject
Public information observation station	Important message of enterprise	Company, message gist

[0020] It should be noted that, the risk database adopted by the traditional verification system has the characteristics of having a long update period and closeness (the scope for storing data is too limited), which makes it difficult to improve the accuracy of identity verification and risk detection. The embodiment of the present invention generates or updates the risk database **112** according to structured data and unstructured data from external sources, so that the data in the risk database **112** can be more complete and get updated in time, thereby improving the accuracy of identity verification and risk detection.

[0021] With continued reference to **FIG. 2**, in action **203**, when it is detected that the input data **D1** does not meet any of the at least one detection condition **R1** (i.e., the risk probability of the user or the requested service may be low), the risk detection module **111** may perform action **204**. In the action **204**, the risk detection module **111** may transmit first detection result data **M1** to the network service system **12** so that the network service system **12** transmits the first detection result data **M1** and the input data **D1** to the verification system **13**, and ends the operation process **2** of the risk detection system **11**. In some embodiments, the first detection result data **M1** may be data such as which risk conditions have been detected and passed, or data generated by detecting which risk conditions. When the first detection

result data **M1** is transmitted to the verification system **13** along with the input data **D1**, the verification system **13** directly receives the data that has passed the first detection, or adds the generated data into the database of the verification system **13** without repeating verification.

[0022] On the other hand, in the action **203**, when it is detected that the input data **D1** meets any of the at least one detection condition **R1** (i.e., the risk probability of the user or the requested service may be high), the risk detection module **111** may perform actions **205** to **208**. In the action **205**, the risk detection module **111** may transmit the data **C0** to be confirmed corresponding to the detection condition **R1** to the user interface **121** to request the user **USR** to provide reply data **C1**.

[0023] In some embodiments, the at least one detection condition **R1** stored in the risk detection module **111** and the data **C0** to be confirmed corresponding to the at least one detection condition **R1** may be as shown in **FIG. 4**. As shown in **FIG. 4**, the detection condition **R1** may comprise: the name conforming to a specific supervision list or a related person, the photo approximating a supervision list or a related person, a service website belonging to a high-risk transaction website, the transaction amount being greater than “n” times the average transaction amount under the name (“n” may be a preset value), and the service/transaction coming from a specific domain. In addition, as shown in **FIG. 4**, the data **C0** to be confirmed corresponding to the above-mentioned detection condition **R1** may comprise: providing a photo in the high-risk database, asking the user to confirm whether the photo is himself/herself, providing the relationship between the user and the person on the supervision list and asking the user to confirm whether the relationship is true, and asking the

user whether he/she has bought a certain commodity recently.

[0024] In some embodiments, assuming that the input data **D1** is the name provided by the user **USR** itself, the risk detection module **111** determines that the input data meets the detection condition when it detects that the user's name conforms to the specific supervision list. Then, the risk detection module **111** may take out the photo of the person who meet the name in the supervision list from the risk database **112**, transmit the photo to the user interface **121** as the corresponded predefined information, and ask the user whether the photo provided is himself/herself. In other embodiments, assuming that the input data **D1** comprises a photo provided by the user **USR** itself, and the photo is analyzed by an image recognition software and determined to be a photo approximating the supervision list or the related person, then the risk detection module **111** may determine that the input data meets the detection condition **R11**, and the risk detection module **111** may transmit the data **C01** to be confirmed corresponding to the detection condition **R11** to the user interface **121** to request the user **USR** to provide reply data **C1**.

[0025] With continued reference to **FIG. 2**, after receiving the data **C0** to be confirmed, the user **USR** may input the reply data **C1** to respond to the data **C0** to be confirmed on the user interface **121**, and the risk detection module **111** may receive the reply data **C1** of the user **USR** from the user interface **121** (labeled as action **206**). In some embodiments, the data **C0** to be confirmed is presented in the original display page in the user interface **121**, or in another display page generated by the user interface **121** when switching pages, or presented in a pop-up window, and the user may input the reply data **C1** into the response field in the display page

of the user interface or the response field in the pop-up window.

[0026] Next, in action **207**, the risk detection module **111** detects whether the input data **D1** coordinated with the reply data **C1** meets the at least one detection condition **R1** according to the risk database **112**. When the action **207** is completed, the risk detection module **111** may execute action **208**, i.e., transmit the second detection result data **M2** to the network service system **12** according to the second detection result, so that the network service system **12** transmits the second detection result data **M2** and the input data **D1** to the verification system **13**, and ends the operation process **2** of the risk detection system **11**.

[0027] In some embodiments, when the second detection result is that the input data **D1** does not meet any of the at least one detection condition **R1**, then the second detection result data **M2** may be detection result data. When the second detection result is that the input data **D1** still meets the at least one detection condition **R1**, then the second detection result data **M2** may comprise the detection condition that is met in the first detection, the corresponded predefined information, the reply data and the detection condition that is met in the second detection. Taking **FIG. 4** as an example, the second detection result data **M2** will comprise the detection condition **R11** that is met in the first detection, the data **C01** to be confirmed, the reply data **C1** provided by the user for the data **C01** to be confirmed, and the detection condition **R11** that is met in the second detection.

[0028] **FIG. 5** is a schematic view illustrating a risk detection method according to some embodiments of the present invention. However, the content shown in **FIG. 5** is only for purpose of illustrating embodiments of the present invention, and is not for purpose of limiting

the scope claimed in the present invention.

[0029] Referring to **FIG. 5**, the risk detection method **5** may comprise the following steps: receiving, by a risk detection module of a risk detection system, input data related to a service from a user interface of a network service system after the input data is inputted by a user via the user interface but before the input data is transmitted to a verification system (labeled as step **501**), wherein the risk detection system links to the user interface, and the risk detection module stores at least one detection condition and corresponded predefined information corresponding to the at least one detection condition; detecting, by the risk detection module, whether the input data meets the at least one detection condition according to a risk database of the risk detection system (labeled as step **502**); when determining that the input data does not meet any of the at least one detection condition, transmitting, by the risk detection module, first detection result data to the network service system so that the network service system transmits the first detection result data and the input data to the verification system (labeled as step **503**); and when determining that the input data meets any of the at least one detection condition, generating and transmitting, by the risk detection module, the corresponded predefined information, which corresponds to the met detection condition, to the user interface to request reply data from the user, detecting whether the input data coordinated with the reply data meets the at least one detection condition according to the risk database after receiving the reply data, and transmitting second detection result data to the network service system so that the network service system transmits the second detection result data and the input data to the verification system (labeled as step **504**).

[0030] In some embodiments, the risk database has a plurality of fields for detecting whether the at least one detection condition is met, and in addition to the steps **501** to **504**, the risk detection method **5** may further comprise the following step: directly acquiring, by an establishment module, data corresponding to each of the plurality of fields of the risk database
5 from corresponding field of structured data stored in at least one public database, or performing a specific format conversion on the structured data stored in the at least one public database to generate the data corresponding to each of the plurality of fields of the risk database.

[0031] In some embodiments, the risk database has a plurality of fields for detecting whether the at least one detection condition is met, and the plurality of fields are related to at
10 least one of the following: data of a specific person, and data of a specific event. Moreover, in addition to the steps **501** to **504**, the risk detection method **5** may further comprise the following step: directly acquiring, by an establishment module, data corresponding to each of the plurality of fields of the risk database from corresponding field of structured data stored in at least one public database, or performing a specific format conversion on the structured data
15 stored in the at least one public database to generate the data corresponding to each of the plurality of fields of the risk database.

[0032] In some embodiments, the risk database has a plurality of fields for detecting whether the at least one detection condition is met, and in addition to the steps **501** to **504**, the risk detection method **5** may further comprise the following step: performing, by an
20 establishment module, machine recognition on unstructured data to generate data corresponding to each of the plurality of fields of the risk database.

[0033] In some embodiments, the risk database has a plurality of fields for detecting whether the at least one detection condition is met, and in addition to the steps **501** to **504**, the risk detection method **5** may further comprise the following steps: establishing a relationship graph of unstructured data by a relationship graph engine; and performing, by an establishment module, machine recognition on the unstructured data to generate data corresponding to each of the plurality of fields of the risk database. The machine recognition performed by the establishment module is to generate or update the data corresponding to each of the plurality of fields in the risk database according to the relationship graph.

[0034] In some embodiments, the risk database has a plurality of fields for detecting whether the at least one detection condition is met, and in addition to the steps **501** to **504**, the risk detection method **5** may further comprise the following steps: establishing a relationship graph of unstructured data by a relationship graph engine; and performing, by an establishment module, machine recognition on the unstructured data to generate data corresponding to each of the plurality of fields of the risk database. The machine recognition performed by the establishment module is to generate or update the data corresponding to each of the plurality of fields in the risk database according to the relationship graph, and the relationship graph engine retrieves the unstructured data to establish the relationship graph according to at least two of a name of a specific person, a name of a specific enterprise, and a specific event as well as relevance therebetween.

[0035] In some embodiments, the second detection result data comprises a detection condition that is met in the first detection, the corresponded predefined information, the reply

data, and a detection condition that is met in the second detection.

[0036] In some embodiments, the corresponded predefined information is presented in a display page of the user interface or presented in a pop-up window.

[0037] Each embodiment of risk detection method **5** essentially corresponds to a certain
5 embodiment of the risk detection system **11**. Therefore, a person having ordinary skill in the art can still directly appreciate the embodiments of the risk detection method **5** that are not described in detail according to the above description for the risk detection system **11**.

[0038] The above disclosure is related to the detailed technical contents and inventive features thereof. A person having ordinary skill in the art may proceed with a variety of
10 modifications and replacements based on the disclosures and suggestions of the invention as described without departing from the characteristics thereof. Nevertheless, although such modifications and replacements are not fully disclosed in the above descriptions, they have substantially been covered in the following claims as appended.

What is claimed is:

1. A risk detection system linking to a user interface of a network service system, the risk detection system comprising:

a risk database; and

a risk detection module electrically connected to the risk database, being configured to:

store at least one detection condition and corresponded predefined information;

receive, from the user interface, input data related to a service after the input data is

inputted by a user via the user interface but before the input data is transmitted

to a verification system;

detect whether the input data meets the at least one detection condition according to

the risk database;

when determining that the input data does not meet any of the at least one detection

condition, transmit first detection result data to the network service system so

that the network service system transmits the first detection result data and the

input data to the verification system; and

when determining that the input data meets any of the at least one detection condition,

generate and transmit the corresponded predefined information to the user

interface so as to request reply data from the user,

detect whether the input data coordinated with the reply data meets the at least

one detection condition according to the risk database after receiving the

reply data, and
transmit second detection result data to the network service system and then
the network service system transmits the second detection result data and the
input data to the verification system.

2. The risk detection system of Claim 1, wherein the risk database has a plurality of fields for detecting whether the at least one detection condition is met, and the risk detection system further comprises an establishment module electrically connected to the risk database and configured to: directly acquire data corresponding to each of the plurality of fields of the risk database from corresponding field of structured data stored in at least one public database; or perform a specific format conversion on the structured data stored in the at least one public database to generate the data corresponding to each of the plurality of fields of the risk database.

3. The risk detection system of Claim 2, wherein the plurality of fields are related to at least one of the following: data of a specific person, and data of a specific event.

4. The risk detection system of Claim 1, wherein the risk database has a plurality of fields for detecting whether the at least one detection condition is met, the risk detection system further comprises an establishment module, and data corresponding to each of the plurality of fields of the risk database is generated by the establishment module through performing machine recognition on unstructured data.

5. The risk detection system of Claim 4, wherein the risk detection system further comprises a relationship graph engine electrically connected to the establishment module and configured to establish a relationship graph of the unstructured data, and the machine recognition performed by the establishment module is to generate or update the data corresponding to each of the plurality of fields of the risk database according to the relationship graph.

6. The risk detection system of Claim 5, wherein the relationship graph engine retrieves the unstructured data to establish the relationship graph according to at least two of a name of a specific person, a name of a specific enterprise, and a specific event as well as relevance therebetween.

7. The risk detection system of Claim 1, wherein the second detection result data comprises a detection condition that is met in the first detection, the corresponded predefined information, the reply data, and a detection condition that is met in the second detection.

8. The risk detection system of Claim 1, wherein the corresponded predefined information is presented in a display page of the user interface or presented in a pop-up window.

9. A risk detection method, comprising:

receiving, by a risk detection module of a risk detection system, input data related to a service from a user interface of a network service system after the input data is

inputted by a user via the user interface but before the input data is transmitted to a verification system, wherein the risk detection system links to the user interface, and the risk detection module stores at least one detection condition and corresponded predefined information corresponding to the at least one detection condition;

detecting, by the risk detection module, whether the input data meets the at least one detection condition according to a risk database of the risk detection system;

when determining that the input data does not meet any of the at least one detection condition, transmitting, by the risk detection module, first detection result data to the network service system so that the network service system transmits the first detection result data and the input data to the verification system; and

when determining that the input data meets any of the at least one detection condition, generating and transmitting, by the risk detection module, the corresponded predefined information, which corresponds to the met detection condition, to the user interface to request reply data from the user,

detecting whether the input data coordinated with the reply data meets the at least one detection condition according to the risk database after receiving the reply data, and

transmitting second detection result data to the network service system so that the network service system transmits the second detection result data and the input data to the verification system.

10. The risk detection method of Claim 9, wherein the risk database has a plurality of fields for detecting whether the at least one detection condition is met, and the risk detection method further comprises:

directly acquiring, by an establishment module, data corresponding to each of the plurality of fields of the risk database from corresponding field of structured data stored in at least one public database; or

performing, by the establishment module, a specific format conversion on the structured data stored in the at least one public database to generate the data corresponding to each of the plurality of fields of the risk database.

11. The risk detection method of Claim 10, wherein the plurality of fields are related to at least one of the following: data of a specific person, and data of a specific event.

12. The risk detection method of Claim 9, wherein the risk database has a plurality of fields for detecting whether the at least one detection condition is met, and the risk detection method further comprises: performing, by an establishment module, machine recognition on unstructured data to generate data corresponding to each of the plurality of fields of the risk database.

13. The risk detection method of Claim 12, wherein the risk detection method further comprises:

establishing, by a relationship graph engine, a relationship graph of the unstructured data;

and

wherein the machine recognition performed by the establishment module is to generate or update the data corresponding to each of the plurality of fields in the risk database according to the relationship graph.

14. The risk detection method of Claim 13, wherein the relationship graph engine retrieves the unstructured data to establish the relationship graph according to at least two of a name of a specific person, a name of a specific enterprise, and a specific event as well as relevance therebetween.

15. The risk detection method of Claim 9, wherein the second detection result data comprises a detection condition that is met in the first detection, the corresponded predefined information, the reply data, and a detection condition that is met in the second detection.

16. The risk detection method of Claim 9, wherein the corresponded predefined information is presented in a display page of the user interface or presented in a pop-up window.