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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 January 2014 (23.01.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/012471 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/CN2013/079376

(22) International Filing Date:
15 July 2013 (15.07.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201210247230.9 17 July 2012 (17.07.2012) CN

(71) Applicant: **TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED** [CN/CN]; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN).

(72) Inventors: **DONG, Wenhui**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN). **SHAO, Fudong**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN).

(74) Agent: **BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY AGENCY CO., LTD.**; A-1-102, He Jing Yuan, Ji Men Li, Xueyuan Road, Haidian District, Beijing 100088 (CN).

(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, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, 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,

[Continued on next page]

(54) Title: METHOD, SYSTEM AND CLIENT TERMINAL FOR DETECTION OF PHISHING WEBSITES

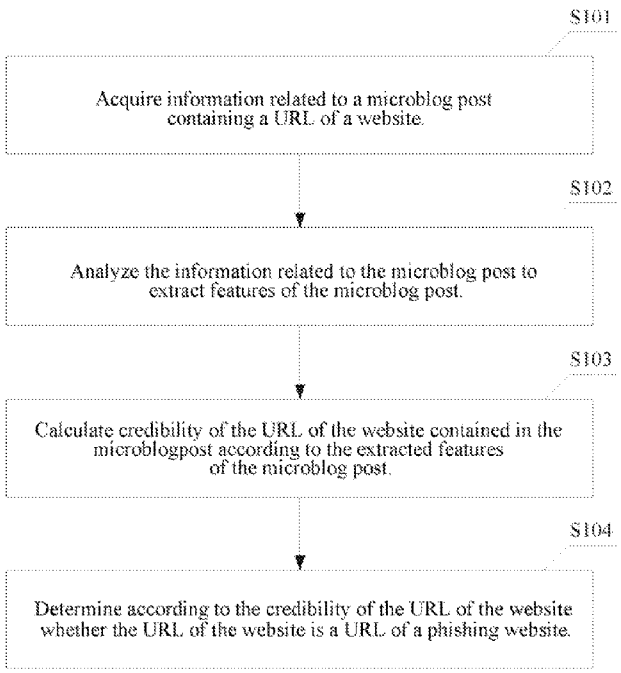

FIG. 1

(57) Abstract: One aspect of the present invention relates to a method for detecting a phishing website. The method includes acquiring information related to a microblog post containing a uniform resource locator (URL) of a website; analyzing the information related to the microblog post to extract features of the microblog post; calculating credibility of the URL of the website contained in the microblog post according to the extracted features of the microblog post; and determining according to the credibility of the URL of the website whether the URL of the website is a URL of a phishing website.

WO 2014/012471 A1

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))*

METHOD, SYSTEM AND CLIENT TERMINAL FOR DETECTION OF PHISHING WEBSITES

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the priority to Chinese Patent Application No. 201210247230.9, filed July 17, 2012 in the State Intellectual Property Office of P.R. China, which is hereby incorporated herein in its entirety by reference.

FIELD OF THE INVENTION

The present invention relates generally to the field of Internet, and more particularly to method, system and client terminal for detection of a phishing website.

BACKGROUND OF THE INVENTION

With popularization of the Internet, more and more users use the Internet to communicate with each other and conduct business transactions. Accordingly, Internet services such as e-commerce and e-bank are developed. When accessing a website, a user needs to input information such as an account and a password. Only when the input information such as the account and password is correct, can the user log in to the website to perform online operations. The account and password of the user are a unique identifier for the user to log in to such websites to perform operations. Once someone steals the account and password of the user and impersonates the user to log in to the website, the interests of the user may be affected. At present, some malicious parties use a phishing website to display a webpage similar to a legitimate website to a user, lure the user into inputting the account and password, and steal the account and password of the user. A phishing website refers to a counterfeit website which is configured by a malicious party through various means to mimic the uniform resource locator (URL) and webpage content of a legitimate website for the purpose of stealing private data such as accounts and passwords of users.

In addition, as indicated by "The 29th Statistical Survey Report on the Internet

Development in China" released by the China Internet Network Information Center, up to the end of December, 2011, the number of microblog users has reached 250 millions, the number of microblog accounts registered on various websites is about 800 millions, and the number of microblog messages posted each day has reached 200 millions. The microblog has become one of important network services in daily life, is increasingly penetrating into the social life, and has become an important way for people to acquire information (for example, a URL of a website). However, a URL of a website contained in a microblog post may be a URL of a phishing website, and it cannot be determined in the prior art whether a URL of a website contained in a microblog post is a URL of a phishing website, resulting in inconvenience for users.

Therefore, a heretofore unaddressed need exists in the art to address the aforementioned deficiencies and inadequacies.

SUMMARY OF THE INVENTION

One of the objectives of the present invention is to provide method, system and client terminal for detecting a phishing website, so as to solve the problem in the prior art that it cannot be determined whether a URL of a website contained in a microblog post is a URL of a phishing website.

In one aspect, the present invention relates to a method for detecting a phishing website. In one embodiment, the method includes acquiring information related to a microblog post containing a uniform resource locator (URL) of a website;analyzing the information related to the microblog post to extract features of the microblog post; calculating credibility of the URL of the website contained in the microblog post according to the extracted features of the microblog post; and determining according to the credibility of the URL of the website whether the URL of the website is a URL of a phishing website.

In another aspect, the present invention provides a system for detecting a phishing website. In one embodiment, the system includes an acquisition module, configured to acquire information related to a microblog post containing a uniform resource locator (URL) of a website; an analysis module, configured to analyze the information related to

the microblog post to extract features of the microblog post; a calculation module, configured to calculate credibility of the URL of the website contained in the microblog post according to the extracted features of the microblog post; and a determining module, configured to determine according to the credibility of the URL of the website whether the URL of the website is a URL of a phishing website.

In yet another aspect, the present invention provides a client terminal, including the foregoing system for detecting a phishing website.

In a further aspect, the present invention relates to a non-transitory computer-readable medium storing instructions which, when executed by one or more processors, cause the system to perform the above method for detecting a phishing website.

In the present invention, information related to a microblog post containing a URL of a website is acquired, features of the microblog post are extracted from the information related to the microblog post, and credibility of the URL of the website contained in the microblog post is calculated according to the extracted features of the microblog post, so as to determine whether the URL of the website is a URL of a phishing website. Therefore, the present invention solves the problem in the prior art that it cannot be determined whether a URL of a website contained in a microblog post is a URL of a phishing website, thereby providing convenience for users.

These and other aspects of the present invention will become apparent from the following description of the preferred embodiment taken in conjunction with the following drawings, although variations and modifications therein may be affected without departing from the spirit and scope of the novel concepts of the disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings illustrate one or more embodiments of the invention and, together with the written description, serve to explain the principles of the invention. Wherever possible, the same reference numbers are used throughout the drawings to refer to the same or like elements of an embodiment. The drawings do not limit the present invention to the specific embodiments disclosed and described herein. The drawings are

not necessarily to scale, emphasis instead being placed upon clearly illustrating the principles of the invention.

FIG. 1 is a flowchart of a method for detecting a phishing website according to one embodiment of the present invention;

FIG. 2 is a functional block diagram of a system for detecting a phishing website according to one embodiment of the present invention;

FIG. 3 is a flowchart of a method for detecting a phishing website according to one embodiment of the present invention; and

FIG. 4 is a functional block diagram of a system for detecting a phishing website according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The following description is merely illustrative in nature and is in no way intended to limit the disclosure, its application, or uses. The broad teachings of the disclosure can be implemented in a variety of forms. Therefore, while this disclosure includes particular examples, the true scope of the disclosure should not be so limited since other modifications will become apparent upon a study of the drawings, the specification, and the following claims. For purposes of clarity, the same reference numbers will be used in the drawings to identify similar elements.

The terms used in this specification generally have their ordinary meanings in the art, within the context of the disclosure, and in the specific context where each term is used. Certain terms that are used to describe the disclosure are discussed below, or elsewhere in the specification, to provide additional guidance to the practitioner regarding the description of the disclosure. The use of examples anywhere in this specification, including examples of any terms discussed herein, is illustrative only, and in no way limits the scope and meaning of the disclosure or of any exemplified term. Likewise, the disclosure is not limited to various embodiments given in this specification.

As used in the description herein and throughout the claims that follow, the meaning of “a”, “an”, and “the” includes plural reference unless the context clearly dictates

otherwise. Also, as used in the description herein and throughout the claims that follow, the meaning of "in" includes "in" and "on" unless the context clearly dictates otherwise.

As used herein, the terms "comprising," "including," "having," "containing," "involving," and the like are to be understood to be open-ended, i.e., to mean including but not limited to.

As used herein, the phrase "at least one of A, B, and C" should be construed to mean a logical (A or B or C), using a non-exclusive logical OR. It should be understood that one or more steps within a method may be executed in different order (or concurrently) without altering the principles of the present disclosure.

As used herein, the term "module" may refer to, be part of, or include an Application Specific Integrated Circuit (ASIC); an electronic circuit; a combinational logic circuit; a field programmable gate array (FPGA); a processor (shared, dedicated, or group) that executes code; other suitable hardware components that provide the described functionality; or a combination of some or all of the above, such as in a system-on-chip. The term module may include memory (shared, dedicated, or group) that stores code executed by the processor.

The term "code", as used herein, may include software, firmware, and/or microcode, and may refer to programs, routines, functions, classes, and/or objects. The term "shared", as used herein, means that some or all code from multiple modules may be executed using a single (shared) processor. In addition, some or all code from multiple modules may be stored by a single (shared) memory. The term "group", as used herein, means that some or all code from a single module may be executed using a group of processors. In addition, some or all code from a single module may be stored using a group of memories.

The systems and methods described herein may be implemented by one or more computer programs executed by one or more processors. The computer programs include processor-executable instructions that are stored on a non-transitory tangible computer readable medium. The computer programs may also include stored data. Non-limiting examples of the non-transitory tangible computer readable medium are nonvolatile

memory, magnetic storage, and optical storage.

The description will be made as to the embodiments of the present invention in conjunction with the accompanying drawings in FIGS. 1-4. It should be understood that specific embodiments described herein are merely intended to explain the present invention, but not intended to limit the present invention. In accordance with the purposes of this invention, as embodied and broadly described herein, this invention, in one aspect, relates to method, system and client terminal for detection of phishing websites.

Referring to FIG. 1, a flowchart of a method for detecting a phishing website is shown according to a first embodiment of the present invention. In one embodiment, the method includes the following steps:

At step S101: information related to a microblog post containing a URL of a website is acquired.

In one embodiment, the information related to the microblog post includes functional features, social networking features and propagation features.

At step S102: the information related to the microblog post is analyzed so as to extract features of the microblog post.

In one embodiment, the features of the microblog post include functional features, social networking features and propagation features of the microblog post.

At step S103: credibility of the URL of the website contained in the microblog post is calculated according to the extracted features of the microblog post.

At step S104: whether the URL of the website is a URL of a phishing website is determined according to the credibility of the URL of the website.

Referring to FIG. 2, a system for detecting a phishing website is shown according to one embodiment of the present invention. The system includes an acquisition module 11, an analysis module 12, a calculation module 13, and a determining module 14.

The acquisition module 11 is configured to acquire information related to a microblog post containing a URL of a website. In the exemplary embodiment, the information related to the microblog post includes functional features, social networking features and propagation features.

The analysis module 12 is configured to analyze the information related to the microblog post to extract features of the microblog post. In this embodiment, the features of the microblog post include functional features, social networking features and propagation features of the microblog post.

The calculation module 13 is configured to calculate credibility of the URL of the website contained in the microblog post according to the extracted features of the microblog post.

The determining module 14 is configured to determine according to the credibility of the URL of the website whether the URL of the website is a URL of a phishing website.

Referring to FIG. 3, a flowchart of a method for detecting a phishing website is shown according to another embodiment of the present invention. The method includes the following steps:

At step S201: information related to a microblog post containing a URL of a website is acquired.

In one embodiment, the information related to the microblog post includes functional features, social networking features and propagation features, where the functional features include the length of the microblog post, content of the microblog post, and the like; the social networking features include an identity of a microblog poster, whether real name authentication is passed, the age of the microblog poster, microblog account registration time, a microblog level, the number of microblog posts (original posts and re-posts), the number of followers or fans, information about followers or fans, an activity status, and the like; and the propagation features include the number of re-posts and comments, features of re-posters and commenters, and the like.

At step S202: noise reduction is performed on the information related to the microblog post.

At step S203: the information related to the microblog post after the noise reduction is analyzed to extract features of the microblog post.

In one embodiment, the features of the microblog post include functional features, social networking features and propagation features of the microblog post.

At step S204: credibility of the URL of the website contained in the microblog post is calculated according to the extracted features of the microblog post.

Assuming that the credibility of the URL of the website is c, c is comprehensively determined according to functional features, social networking features and propagation features based on a preset weight ratio, where the functional features, the social networking features and the propagation features are comprehensively determined according to a plurality of different functional feature descriptors corresponding to the functional features, the social networking features and the propagation features based on a preset weight ratio, respectively.

Specifically, $c = \{(f,p_f), (s,p_s), (d,p_d)\}$, where,

f represents functional features, $f = \{(f_1,p_{f1}), (f_2,p_{f2}), (f_3,p_{f3}), ..., (f_n,p_{fn})\}$, f_i represents a functional feature descriptor, $i=\{1, 2, 3, ..., n\}$, n represents the number of functional feature descriptors, and p_{fi} represents a weight of the functional feature descriptor f_i;

p_f represents weights of the functional features f;

for example, f_1 represents the length of the microblog post, and f_2 represents existence of certain words or emotional words; p_{f1} represents a weight of the length of the microblog post, and p_{f2} represents a weight of existence of certain words or emotional words;

s represents social networking features, $s = \{(s_1,p_{s1}), (s_2,p_{s2}), (s_3,p_{s3}), ..., (s_n,p_{sn})\}$, s_i represents a social networking feature descriptor, $i=\{1, 2, 3, ..., n\}$, n represents the number of social networking feature descriptors, and p_{si} represents a weight of the social networking feature descriptor S_i;

p_s represents weights of the social networking features s;

for example, S_1 represents an identity of a microblog poster, S_2 represents real name authentication, S_3 represents age, S_4 represents microblog account registration time, S_5 represents a microblog level, S_6 represents the number of microblog posts (original posts and re-posts), S_7 represents the number of followers or fans, S_8 represents information about followers or fans, and S_9 represents an activity status;

p_{s1} represents a weight of the identity of the microblog poster, p_{s2} represents a weight of real name authentication, p_{s3} represents a weight of age, p_{s4} represents a weight of the microblog account registration time, p_{s5} represents a weight of the microblog level, p_{s6} represents a weight of the number of microblog posts (original posts and re-posts), p_{s7} represents a weight of the number of followers or fans, p_{s8} represents a weight of the information about followers or fans, and p_{s9} represents a weight of the activity status;

d represents propagation features, $d = \{(d_1,p_{d1}), (d_2,p_{d2}), (d_3,p_{d3}), ..., (d_n,p_{dn})\}$, d_i represents a propagation feature descriptor, $i=\{1, 2, 3, ..., n\}$, n represents the number of propagation feature descriptors, and p_{di} represents a weight of the propagation feature descriptor d_i;

p_d represents weights of the propagation features d;

for example, d_1 represents the number of re-posts and comments, and d_2 represents features of re-posters and commenters; p_{d1} represents a weight of the number of re-posts and comments, and p_{d2} represents a weight of the features of re-posters and commenters.

At step S205: whether the URL of the website is a URL of a phishing website is determined according to the credibility of the URL of the website.

When the credibility c of the URL of the website is $\geq T_w$, it is determined that the URL of the website is credible, where T_w is a preset credible threshold.

When the credibility c of the URL of the website is $\leq T_B$, it is determined that the URL of the website is non-credible, and it is determined that the URL of the website is a URL of a phishing website, where T_B is a preset non-credible threshold.

When the credibility c of the URL of the website satisfies $T_w > c > T_B$, it is determined that the URL of the website is unknown.

The preset non-credible threshold T_B and the preset credible threshold T_w are obtained in the following manner:

selecting keywords (such as bank and taobao) that are frequently used in phishing, collecting microblog posts containing URLs by using the keywords to form a data set, performing word segmentation and data formatting on the data set, and extracting functional features, social networking features and propagation features;

manually marking credible results of the URLs in the data set, and grouping a training set and a test set at a ratio of 4:1 at random; and

training and testing classification models by means of cross-checking, where the classification models may be supervised learning models such as SVM, decision trees, and Bayes networks, and according to the experiment in the paper "Information Credibility on Twitter" by Carlos Castillo et al., a high accuracy can be obtained by a J48 decision tree; and defining the probability from the root node of the decision tree to a non-credible class leaf node and the probability from the root node of the decision tree to a credible class leaf node as a non-credible threshold and a credible threshold respectively, thereby obtaining the preset non-credible threshold T_B and the preset credible threshold T_w.

Referring to FIG. 4, a system for detecting a phishing website is shown another embodiment of the present invention. The system includes an acquisition module 21, a noise reduction module 22, an analysis module 23, a calculation module 24, and a determining module 25.

The acquisition module 21 is used for acquiring information related to a microblog post containing a URL of a website. In the fourth embodiment of the present invention, the information related to the microblog post includes functional features, social networking features and propagation features, where the functional features include the length of the microblog post, content of the microblog post, and the like; the social networking features include an identity of a microblog poster, whether real name authentication is passed, the age of the microblog poster, microblog account registration time, a microblog level, the number of microblog posts (original posts and re-posts), the number of followers or fans, information about followers or fans, an activity status, and the like; and the propagation features include the number of re-posts and comments, features of re-posters and commenters, and the like.

The noise reduction module 22 is used for performing noise reduction on the information related to the microblog post.

The analysis module 23 is used for analyzing the information related to the microblog post after the noise reduction to extract features of the microblog post. In the

fourth embodiment of the present invention, the features of the microblog post include functional features, social networking features and propagation features of the microblog post.

The calculation module 24 is used for calculating credibility of the URL of the website contained in the microblog post according to the extracted features of the microblog post.

Assuming that the credibility of the URL of the website is c, c is comprehensively determined according to functional features, social networking features and propagation features based on a preset weight ratio, where the functional features, the social networking features and the propagation features are comprehensively determined according to a plurality of different functional feature descriptors corresponding to the functional features, the social networking features and the propagation features based on a preset weight ratio, respectively.

Specifically, $c = \{(f,p_f), (s,p_s), (d,p_d)\}$, where,

f represents functional features, $f = \{(f_1,p_{f1}), (f_2,p_{f2}), (f_3,p_{f3}), ..., (f_n,p_{fn})\}$, f_i represents a functional feature descriptor, $i=\{1, 2, 3, ..., n\}$, n represents the number of functional feature descriptors, and p_{fi} represents a weight of the functional feature descriptor f_i;

p_f represents weights of the functional features f;

for example, f_1 represents the length of the microblog post, and f_2 represents existence of certain words or emotional words; p_{f1} represents a weight of the length of the microblog post, and p_{f2} represents a weight of existence of certain words or emotional words;

s represents social networking features, $s = \{(s_1,p_{s1}), (s_2,p_{s2}), (s_3,p_{s3}), ..., (s_n,p_{sn})\}$, s_i represents a social networking feature descriptor, $i = \{1, 2, 3, ..., n\}$, n represents the number of social networking feature descriptors, and p_{si} represents a weight of the social networking feature descriptor S_i;

p_s represents weights of the social networking features s;

for example, S_1 represents an identity of a microblog poster, S_2 represents real name

authentication, S_3 represents age, S_4 represents microblog account registration time, S_5 represents a microblog level, S_6 represents the number of microblog posts (original posts and re-posts), S_7 represents the number of followers or fans, S_8 represents information about followers or fans, and S_9 represents an activity status;

p_{s1} represents a weight of the identity of the microblog poster, p_{s2} represents a weight of real name authentication, p_{s3} represents a weight of age, p_{s4} represents a weight of the microblog account registration time, p_{s5} represents a weight of the microblog level, p_{s6} represents a weight of the number of microblog posts (original posts and re-posts), p_{s7} represents a weight of the number of followers or fans, p_{s8} represents a weight of the information about followers or fans, and p_{s9} represents a weight of the activity status;

d represents propagation features, $d = \{(d_1,p_{d1}), (d_2,p_{d2}), (d_3,p_{d3}), ..., (d_n,p_{dn})\}$, d_i represents a propagation feature descriptor, $i = \{1, 2, 3, ..., n\}$, n represents the number of propagation feature descriptors, and p_{di} represents a weight of the propagation feature descriptor d_i;

p_d represents weights of the propagation features d;

for example, d_1 represents the number of re-posts and comments, and d_2 represents features of re-posters and commenters; p_{d1} represents a weight of the number of re-posts and comments, and p_{d2} represents a weight of the features of re-posters and commenters.

The determining module 25 is used for determining according to the credibility of the URL of the website whether the URL of the website is a URL of a phishing website.

When the credibility c of the URL of the website is $\geq T_w$, it is determined that the URL of the website is credible, where T_w is a preset credible threshold.

When the credibility c of the URL of the website is $\leq T_B$, it is determined that the URL of the website is non-credible, and it is determined that the URL of the website is a URL of a phishing website, where T_B is a preset non-credible threshold.

When the credibility c of the URL of the website satisfies $T_w > c > T_B$, it is determined that the URL of the website is unknown.

The preset non-credible threshold T_B and the preset credible threshold T_w are obtained in the following manner:

selecting keywords (such as bank and taobao) that are frequently used in phishing, collecting microblog posts containing URLs by using the keywords to form a data set, performing word segmentation and data formatting on the data set, and extracting functional features, social networking features and propagation features;

manually marking credible results of the URLs in the data set, and grouping a training set and a test set at a ratio of 4:1 at random; and

training and testing classification models by means of cross-checking, where the classification models may be supervised learning models such as SVM, decision trees, and Bayes networks, and according to the experiment in the paper "Information Credibility on Twitter" by Carlos Castillo et al., a high accuracy can be obtained by a J48 decision tree; and defining the probability from the root node of the decision tree to a non-credible class leaf node and the probability from the root node of the decision tree to a credible class leaf node as a non-credible threshold and a credible threshold respectively, thereby obtaining the preset non-credible threshold T_B and the preset credible threshold T_w.

In the embodiments of the present invention, information related to a microblog post containing a URL of a website is acquired, features of the microblog post are extracted from the information related to the microblog post, and credibility of the URL of the website contained in the microblog post is calculated according to the extracted features of the microblog post, so as to determine whether the URL of the website is a URL of a phishing website. Therefore, the present invention solves the problem in the prior art that it cannot be determined whether a URL of a website contained in a microblog post is a URL of a phishing website, thereby providing convenience for users.

One ordinary skill in the art may understand that all or part of the steps in the preceding embodiments may be completed by hardware following instructions of a program.

Another aspect of the present invention provides a non-transitory tangible computer-readable medium storing instructions or codes which, when executed by one or more processors, cause the above system to perform the above method for detection of a phishing website. The non-transitory tangible computer-readable storage medium

includes, but not limited to, disk, CD-ROM, read-only memory (ROM), random memory (RAM), flash dive, or the likes.

The foregoing description of the exemplary embodiments of the invention has been presented only for the purposes of illustration and description and is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many modifications and variations are possible in light of the above teaching.

The embodiments were chosen and described in order to explain the principles of the invention and their practical application so as to activate others skilled in the art to utilize the invention and various embodiments and with various modifications as are suited to the particular use contemplated. Alternative embodiments will become apparent to those skilled in the art to which the present invention pertains without departing from its spirit and scope. Accordingly, the scope of the present invention is defined by the appended claims rather than the foregoing description and the exemplary embodiments described therein.

CLAIMS

What is claimed is:

1. A method for detecting a phishing website, comprising:
   (a) acquiring information related to a microblog post containing a uniform resource locator (URL) of a website;
   (b) analyzing the information related to the microblog post to extract features of the microblog post;
   (c) calculating credibility of the URL of the website contained in the microblog post according to the extracted features of the microblog post; and
   (d) determining according to the credibility of the URL of the website whether the URL of the website is a URL of a phishing website.

2. The method according to claim 1, wherein the information related to the microblog post comprises functional features, social networking features and propagation features, and wherein the features of the microblog post comprise functional features, social networking features and propagation features of the microblog post.

3. The method according to claim 2, wherein

the functional features comprise a length of the microblog post and/or content of the microblog post;

the social networking features comprise an identity of a microblog poster, whether real name authentication is passed, an age of the microblog poster, microblog account registration time, a microblog level, the number of microblog posts, the number of followers or fans, information about followers or fans and/or an activity status; and

the propagation features comprise the number of re-posts and comments and/or features of re-posters and commenters.

4. The method according to claim 1, after the step of acquiring the information related to the microblog post, further comprising

performing noise reduction on the information related to the microblog post,

wherein the step of analyzing the information related to the microblog post comprises:

analyzing the information related to the microblog post after the noise reduction.

5. The method according to claim 2, wherein the step of calculating the credibility of the URL of the website comprises:

determining c according to the functional features, the social networking features and the propagation features based on a preset weight ratio, wherein c is the credibility of the URL of the website, wherein the functional features, the social networking features and the propagation features are comprehensively determined according to a plurality of different functional feature descriptors corresponding to the functional features, the social networking features and the propagation features based on the preset weight ratio, respectively.

6. The method according to claim 5, wherein the step of determining according to the credibility of the URL of the website whether the URL of the website is a URL of a phishing website comprises:

when $c \geq T_w$, determining that the URL of the website is credible, wherein T_w is a preset credible threshold;

when $c \leq T_B$, determining that the URL of the website is non-credible, and determining that the URL of the website is a URL of a phishing website, wherein T_B is a preset non-credible threshold; and

when the credibility c of the URL of the website satisfies $T_w > c > T_B$, determining that the URL of the website is unknown.

7. A system for detecting a phishing website, comprising:

(a) an acquisition module, configured to acquire information related to a microblog post containing a uniform resource locator (URL) of a website;

(b) an analysis module, configured to analyze the information related to the microblog post to extract features of the microblog post;

(c) a calculation module, configured to for calculate credibility of the URL of the website contained in the microblog post according to the extracted features of the microblog post; and

(d) a determining module, configured to determine according to the credibility of the URL of the website whether the URL of the website is a URL of a phishing website.

8. The system according to claim 7, wherein the information related to the microblog post comprises functional features, social networking features and propagation features, and wherein the features of the microblog post comprises functional features, social networking features and propagation features of the microblog post.

9. The system according to claim 7, further comprising:

a noise reduction module, configured to perform noise reduction on the information related to the microblog post;

wherein the analysis module is configured to analyze the information related to the microblog post after the noise reduction, so as to extract functional features, social networking features and propagation features of the microblog post, respectively.

10. The system according to claim 8, wherein the calculation module is configured to determine c according to the functional features, the social networking features and the propagation features based on a preset weight ratio, wherein c is the credibility of the URL of the website, wherein the functional features, the social networking

features and the propagation features are comprehensively determined according to a plurality of different functional feature descriptors corresponding to the functional features, the social networking features and the propagation features based on the preset weight ratio, respectively.

11. The system according to claim 10, wherein the determining module is configured to:

when $c \geq T_w$, determining that the URL of the website is credible, wherein T_w is a preset credible threshold;

when $c \leq T_B$, determining that the URL of the website is non-credible, and determining that the URL of the website is a URL of a phishing website, wherein T_B is a preset non-credible threshold; and

when the credibility c of the URL of the website satisfies $T_w > c > T_B$, determining that the URL of the website is unknown.

12. A client terminal, comprising the system for detecting a phishing website according to claim 7.

13. A non-transitory computer-readable medium storing instructions which, when executed by one or more processors, cause a system to perform a method for detecting a phishing website, the method comprising:

(a) acquiring information related to a microblog post containing a uniform resource locator (URL) of a website;

(b) analyzing the information related to the microblog post to extract features of the microblog post;

(c) calculating credibility of the URL of the website contained in the microblog post according to the extracted features of the microblog post; and

(d) determining according to the credibility of the URL of the website whether the URL of the website is a URL of a phishing website.

14. The non-transitory computer-readable medium according to claim 13, wherein the information related to the microblog post comprises functional features, social networking features and propagation features, and wherein the features of the microblog post comprise functional features, social networking features and propagation features of the microblog post.

15. The non-transitory computer-readable medium according to claim 14, wherein

the functional features comprise a length of the microblog post and/or content of the microblog post;

the social networking features comprise an identity of a microblog poster, whether real name authentication is passed, an age of the microblog poster, microblog account registration time, a microblog level, the number of microblog posts, the number of followers or fans, information about followers or fans and/or an activity status; and

the propagation features comprise the number of re-posts and comments and/or features of re-posters and commenters.

16. The non-transitory computer-readable medium according to claim 13,wherein after the step of acquiring the information related to the microblog post, the method further comprises

performing noise reduction on the information related to the microblog post,

wherein the step of analyzing the information related to the microblog post comprises:

analyzing the information related to the microblog post after the noise reduction.

17. The non-transitory computer-readable medium according to claim 14, wherein the step of calculating the credibility of the URL of the website comprises:

determining c according to the functional features, the social networking features and the propagation features based on a preset weight ratio, wherein c is the credibility of the URL of the website, wherein the functional features, the social networking features and the propagation features are comprehensively determined according to a plurality of different functional feature descriptors corresponding to the functional features, the social networking features and the propagation features based on the preset weight ratio, respectively.

18. The non-transitory computer-readable medium according to claim 17, wherein the step of determining according to the credibility of the URL of the website whether the URL of the website is a URL of a phishing website comprises:

when $c \geq T_w$, determining that the URL of the website is credible, wherein T_w is a preset credible threshold;

when $c \leq T_B$, determining that the URL of the website is non-credible, and determining that the URL of the website is a URL of a phishing website, wherein T_B is a preset non-credible threshold; and

when the credibility c of the URL of the website satisfies $T_w > c > T_B$, determining that the URL of the website is unknown.

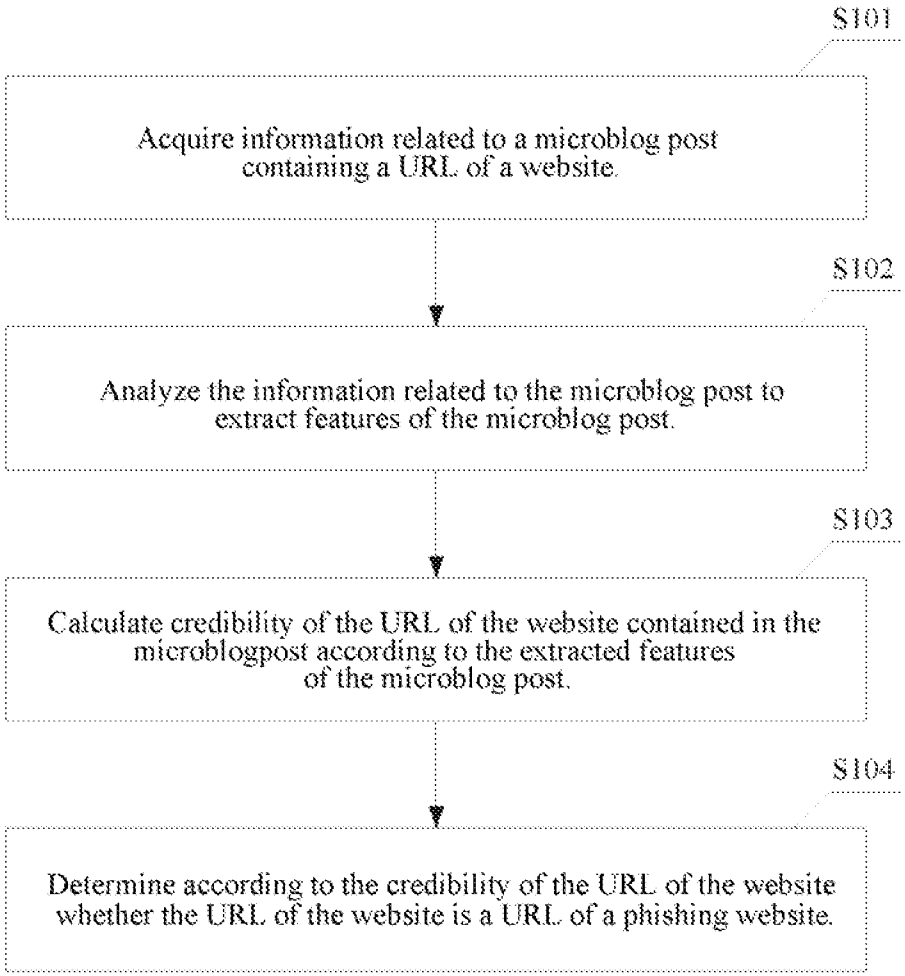
S101
Acquire information related to a microblog post containing a URL of a website.
S102
Analyze the information related to the microblog post to extract features of the microblog post.
S103
Calculate credibility of the URL of the website contained in the microblogpost according to the extracted features of the microblog post.
S104
Determine according to the credibility of the URL of the website whether the URL of the website is a URL of a phishing website.

FIG. 1

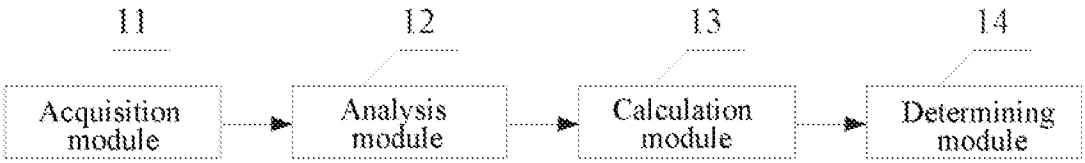
11
Acquisition module
12
Analysis module
13
Calculation module
14
Determining module

FIG. 2

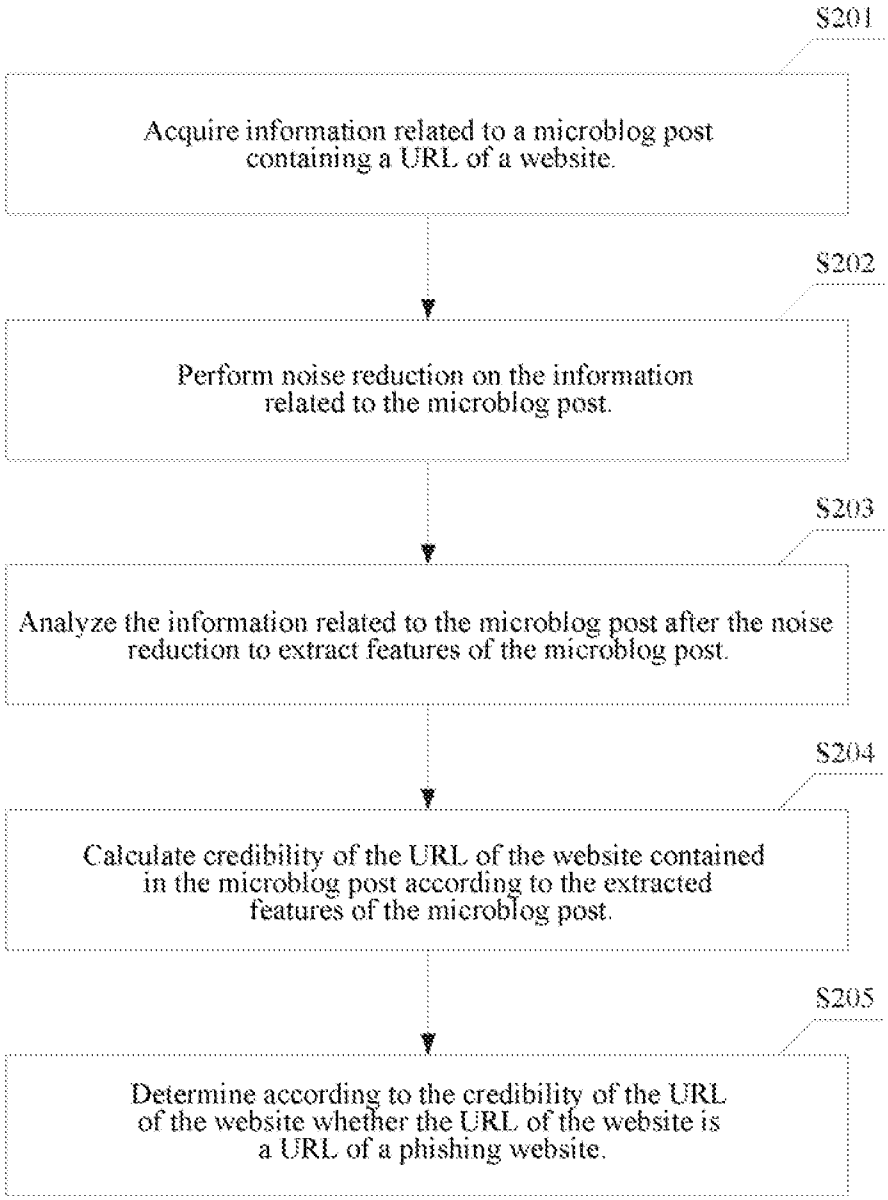
S201
Acquire information related to a microblog post containing a URL of a website.
S202
Perform noise reduction on the information related to the microblog post.
S203
Analyze the information related to the microblog post after the noise reduction to extract features of the microblog post.
S204
Calculate credibility of the URL of the website contained in the microblog post according to the extracted features of the microblog post.
S205
Determine according to the credibility of the URL of the website whether the URL of the website is a URL of a phishing website.

FIG. 3

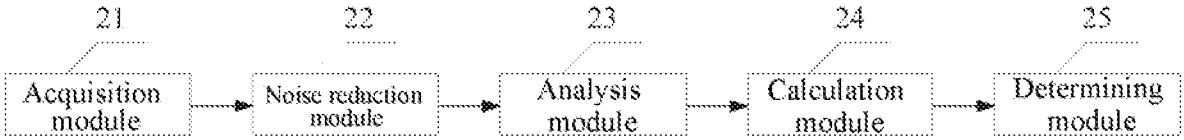
21
Acquisition module
22
Noise reduction module
23
Analysis module
24
Calculation module
25
Determining module

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/079376

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

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: H04L; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: microblog, phishing, URL, link, tweets, website, credibility, analyze

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2010042687 A1 (YAHOO! INC.) 08 February 2010 (08.02.2010) paragraphs [0024] to [0038], claims 1-10	1-18
A	CN 102231745 A (SHENGDA COMPUTER SHANGHAI CO., LTD.) 02 November 2011 (02.11.2011) the whole document	1-18
A	CN 102279875 A (CHENGDU HUAWEI SYMANTEC TECHNOLOGY LTD.) 14 December 2011 (14.12.2011) the whole document	1-18
A	CN 102355469 A (BEILONG KNET BEIJING TECHNOLOGY CO., LTD.) 15 February 2012 (15.02.2012) the whole document	1-18
A	CN 102571485 A (UNIVERSITY OF SHANGHAI JIAOTON) 11 July 2012 (11.07.2012) the whole document	1-18

☐ 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
27 September 2013 (27.09.2013)	**24 Oct. 2013 (24.10.2013)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer WU,Ping Telephone No. (86-10)62414065

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/079376

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US 2010042687 A1	08.02.2010	US 2010043071 A1	18.02.2010
CN 102231745 A	02.11.2011	None	
CN 102279875 A	14.12.2011	None	
CN 102355469 A	15.02.2012	None	
CN 102571485 A	11.07.2012	None	