



(51) International Patent Classification:
G06F 17/30 (2006.01)

(21) International Application Number:
PCT/CN2013/084317

(22) International Filing Date:
26 September 2013 (26.09.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201210393872.X 17 October 2012 (17.10.2012) CN

(71) Applicant: TENCENT TECHNOLOGY (SHENZHEN)
COMPANY LIMITED [CN/CN]; Room 403, East Block
2, SEG Park, Zhenxing Road, Futian District, Shenzhen,
Guangdong 518044 (CN).

(72) Inventors: ZENG, Fansheng; Room 403, East Block 2,
SEG Park, Zhenxing Road, Futian District, Shenzhen,
Guangdong 518044 (CN). GAO, Bin; Room 403, East
Block 2, SEG Park, Zhenxing Road, Futian District, Shen-
zhen, Guangdong 518044 (CN).

(74) Agent: DEQI INTELLECTUAL PROPERTY LAW
CORPORATION; 7/F, Xueyuan International Tower, No.
1 Zhichun Road, Haidian District, Beijing 100083 (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, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM,
ZW.

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

Published:

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

(54) Title: METHOD AND APPARATUS FOR PROCESSING WEBPAGE

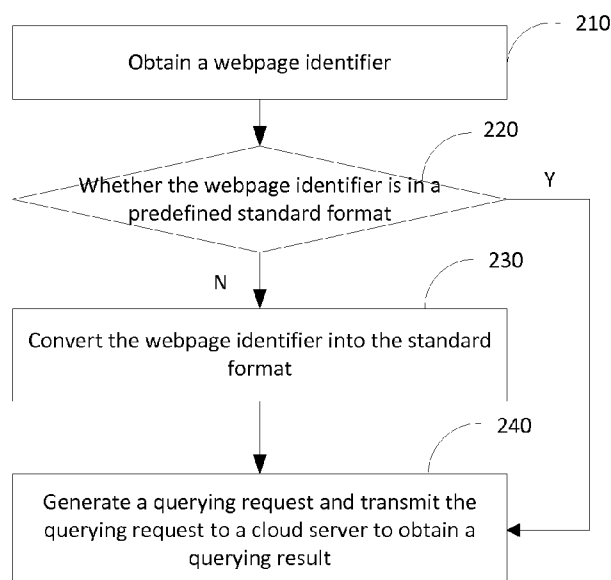


FIG. 2

(57) Abstract: A method for processing a webpage, comprises: obtaining, by a user device, a webpage identifier; determining, by the user device, whether the webpage identifier is in a predefined standard format; if the webpage identifier is not in the predefined standard format, converting, by the user device, the webpage identifier into a webpage identifier in the predefined standard format; generating, by the user device, a querying request and transmitting the querying request to a cloud server to receive a querying result, wherein the querying request comprises the webpage identifier in the standard format, the querying request comprises information indicating whether the webpage identifier is malicious.

METHOD AND APPARATUS FOR PROCESSING WEBPAGE

PRIORITY STATEMENT

[0001] This application claims the benefit of Chinese Patent Application No. 201210393872.X, filed on October 17, 2012, the disclosure of which is incorporated herein in its entirety by reference.

FIELD

[0002] The present disclosure relates to Internet techniques, and more particularly, to a method and an apparatus for processing a webpage.

BACKGROUND

[0003] With the popularization of the Internet, users use the Internet more and more frequently. Therefore, it is required to ensure the security of users' computers on the Internet.

[0004] Each webpage on the Internet has a unique webpage identifier, generally referred to as a Uniform/Universal Resource Locator (URL) address, a web address or a website address. When the user logs in on the Internet, malicious webpage identifiers usually emerge. These malicious webpage identifiers usually force the user to visit some webpages through modifying a browser homepage of the user's computer, or adding a desktop shortcut, or forbidding restoring to factory configurations or deleting them. These malicious webpage identifiers generally direct to advertisement websites, virus websites or some other undesirable websites, which affects normal browsing of the user and threatens the security of the user's computer.

SUMMARY

[0005] According to an example of the present disclosure, a method for processing a webpage is provided. The method includes:

- obtaining, by a user device, a webpage identifier;

- determining, by the user device, whether the webpage identifier is in a predefined standard format; if the webpage identifier is not in the predefined standard format, converting, by the user device, the webpage identifier into a webpage identifier in the predefined standard format; and

- generating, by the user device, a querying request and transmitting the querying

request to a cloud server to receive a querying result; wherein the querying request comprises the webpage identifier in the standard format, the querying result comprises information indicating whether the webpage identifier is malicious.

[0006] According to another example of the present disclosure, a method for processing a webpage is provided. The method includes:

- receiving, by a cloud server, a querying request transmitted by a user device, wherein the querying request comprises a webpage identifier;

- determining, by the cloud server, whether the webpage identifier in the querying request is malicious; and

- generating, by the cloud server, a querying result and transmitting the querying result to the user device, wherein the querying result comprises information indicating whether the webpage identifier is malicious.

[0007] According to still another example of the present disclosure, a user device for processing a webpage is provided. The cloud server includes:

- one or more processors;

- memory; and

- one or more program modules stored in the memory and to be executed by the one or more processors, the one or more program modules comprise:

- a webpage identifier obtaining module, to obtain a webpage identifier;

- a format determining module, to determine whether the webpage identifier obtained by the webpage identifier obtaining module is in a predefined standard format;

- a format converting module, to convert the webpage identifier into a webpage identifier in the standard format if the format determining module determines that the webpage identifier is not in the standard format; and

- a querying module, to generate a querying request and transmit the querying request to a cloud server to obtain a querying result; wherein the querying request comprises the webpage identifier; the querying result comprises information indicating whether the webpage identifier is malicious.

[0008] According to yet another example of the present disclosure, a cloud server for processing a webpage is provided. The user device includes:

- one or more processors;

- memory; and

- one or more program modules stored in the memory and to be executed by the one or more processors, the one or more program modules comprise:

a querying request receiving module, to receive a querying request transmitted by a user device, wherein the querying request comprises a webpage identifier;

a malicious webpage determining module, to determine whether the webpage identifier in the querying request is malicious;

a querying result generating module, to generate a querying result, wherein the querying result comprises information indicating whether the webpage identifier in the querying request is malicious; and

a querying result transmitting module, to transmit the querying result to the user device.

[0009] A non-transitory computer-readable storage medium including a set of instructions for processing a webpage, the set of instructions to direct at least one processor to perform acts of:

obtaining a webpage identifier;

determining whether the webpage identifier is in a predefined standard format; if the webpage identifier is not in the predefined standard format, converting the webpage identifier into a webpage identifier in the predefined standard format; and

generating a querying request and transmitting the querying request to a cloud server to receive a querying result; wherein the querying request comprises the webpage identifier in the standard format, the querying result comprises information indicating whether the webpage identifier is malicious.

[0010] A non-transitory computer-readable storage medium including a set of instructions for processing a webpage, the set of instructions to direct at least one processor to perform acts of:

receiving a querying request transmitted by a user device, wherein the querying request comprises a webpage identifier;

determining whether the webpage identifier in the querying request is malicious; and

generating a querying result and transmitting the querying result to the user device, wherein the querying result comprises information indicating whether the webpage identifier is malicious.

[0011] Other aspects or embodiments of the present disclosure can be understood by those skilled in the art in light of the description, the claims, and the drawings of the present disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Features of the present disclosure are illustrated by way of example and not limited in the following figures, in which like numerals indicate like elements, in which:

[0013] FIG. 1 is a schematic diagram illustrating an example of a user device and a cloud server for executing the method of the present disclosure.

[0014] FIG. 2 is a flowchart illustrating a method for processing a webpage at a user device side according to an example of the present disclosure.

[0015] FIG. 3 is a flowchart illustrating a method for processing a webpage at a user device side according to another example of the present disclosure.

[0016] FIG. 4 is a flowchart illustrating a method for processing a webpage at a user device side according to still another example of the present disclosure.

[0017] FIG. 5 is a flowchart illustrating a method for processing a webpage at a cloud server side according to an example of the present disclosure.

[0018] FIG. 6 is a schematic diagram illustrating a structure of a user device according to an example of the present disclosure.

[0019] FIG. 7 is a schematic diagram illustrating a structure of a user device according to another example of the present disclosure.

[0020] FIG. 8 is a schematic diagram illustrating a structure of a user device according to still another example of the present disclosure.

[0021] FIG. 9 is a schematic diagram illustrating a structure of a user device according to yet another example of the present disclosure.

[0022] FIG. 10 is a schematic diagram illustrating a cloud server according to an example of the present disclosure.

DETAILED DESCRIPTION

[0023] The present disclosure will be described in further detail hereinafter with reference to accompanying drawings and examples to make the technical solution and merits therein clearer.

[0024] For simplicity and illustrative purposes, the present disclosure is described by referring to examples. In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure. It will be readily apparent however, that the present disclosure may be practiced without

limitation to these specific details. In other instances, some methods and structures have not been described in detail so as not to unnecessarily obscure the present disclosure. As used herein, the term “includes” means includes but not limited to, the term “including” means including but not limited to. The term “based on” means based at least in part on. In addition, the terms “a” and “an” are intended to denote at least one of a particular element.

[0025] Conventional systems can find and deal with malicious program such as troy horse and virus through real-time protection and file scanning. The malicious program usually directs to advertisement websites, virus websites or other undesirable websites. Although the malicious program can be removed, the malicious webpage identifiers of the malicious websites are not removed. It is difficult for the security software to recognize whether the malicious webpage identifiers are configured by the user or by the malicious program. And the user will still visit the websites directed by the malicious webpage identifiers. The reason is that conventional security software lacks the ability of recognizing and processing the malicious webpage identifiers. In addition, the real-time protection function also cannot effectively recognize webpage addresses not in standard formats. Thus, the malicious webpage identifiers in the computer cannot be removed thoroughly.

[0026] In various examples of the present disclosure, a webpage identifier is obtained. It is determined whether the webpage identifier is in a predefined standard format. If not, the obtained webpage identifier is converted into the standard format. A querying request is generated and transmitted to a cloud server to obtain a querying result. The querying request includes the webpage identifier in the standard format and the querying result includes information indicating whether the webpage identifier is malicious.

[0027] FIG. 1 is a schematic diagram illustrating an example of a user device and a cloud server which may execute the method of the present disclosure. As shown in FIG. 1, a user device 110 and a cloud server 120 may be computing devices capable of executing methods and apparatuses of present disclosure. The user device 110 may, for example, be a device such as a personal desktop computer or a portable device, such as a laptop computer, a tablet computer, a cellular telephone, or a smart phone.

[0028] The user device 110 may include one or more non-transitory processor-readable storage media 151 and one or more processors 152 in communication with the non-transitory processor-readable storage media 151. The user

device 110 may include or may execute an operating system 121 and an application 122 executable by a processor to implement the methods provided by the present disclosure.

[0029] The cloud server 120 in FIG. 1 represents a computer system that is made available to the user device 110. The cloud server 120 may include one or more non-transitory processor-readable storage media 141 and one or more processors 142 in communication with the non-transitory processor-readable storage media 141. The cloud server 120 may include or may execute an operating system 131 and an application 132 executable by a processor to implement the methods provided by the present disclosure.

[0030] The non-transitory processor-readable storage media 151 and 141 may be a RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of non-transitory storage medium known in the art.

[0031] FIG. 2 is a schematic diagram illustrating a method for processing a webpage at a user device side according to an example of the present disclosure. FIG. 2 is a simplified diagram according to one embodiment of the present invention. This diagram is merely an example, which should not unduly limit the scope of the claims. One of ordinary skill in the art would recognize many variations, alternatives, and modifications. As shown in FIG. 2, the method includes the following.

[0032] At block 210, a webpage identifier is obtained.

[0033] In this example, the webpage identifier may be a URL webpage address or other webpage identifiers, if only a webpage can be obtained according to the webpage identifier.

[0034] In a practical application, the webpage identifier may be obtained through any one of the following two manners.

[0035] In a first manner, it is determined whether a webpage open instruction is received. If the webpage open instruction is received, the webpage identifier of the webpage being opened is obtained when the webpage is opened. This manner collects the URL address through monitoring a browser, which reduces a collecting area and a collecting difficulty, and improves effectiveness of the collecting of the URL.

[0036] In a second manner, a predetermined area of the user device is scanned to obtain the webpage identifier, wherein the predetermined area stores the webpage identifier. In this manner, when the scanning is performed, URL address relevant items are traversed and attributes are allocated to the URLs according to their positions in a

system. For example, URLs in a network favorite folder may be omitted, whereas URLs emerged on desktop and start menu should be scanned thoroughly.

[0037] In this example, for the URL addresses in the user device, different attributes may be allocated for them according to their positions. In other words, a lenient policy may be adopted for positions familiar to the user, whereas a strict policy may be adopted for positions usually utilized by malicious software.

[0038] At block 220, it is determined whether the obtained webpage identifier is in a predefined standard format, if yes, block 240 is performed; otherwise, block 230 is performed.

[0039] At block 230, the webpage identifier is converted into a webpage identifier in the standard format.

[0040] In particular, a protocol header identifier such as “http://”, “https://” and “www.” is deleted from the URL address. A protocol tail identifier such as “/” is also deleted from the URL address. For example, a URL address “http://www.xxx.com/yyy/” will be converted into the standard format “xxx.com/yyy”. In this example, the obtained webpage identifier is converted into the standard format, which reduce the difficulty for determining whether the webpage identifier is malicious and improves an accuracy ratio of the determination.

[0041] At block 240, a querying request is generated and transmitted to the cloud server, so as to obtain a querying result.

[0042] The querying request includes the webpage identifier in the standard format. The querying result includes information indicating whether the webpage identifier is malicious.

[0043] Through the above blocks 210 to 240, the user device obtains the webpage identifier and converts the webpage identifier into the standard format if the webpage identifier is not in the standard format. The user device transmits the webpage identifier in the standard format to the cloud server which determines whether the webpage identifier is malicious. The method is able to recognize the webpage identifier effectively. The efficiency for removing the malicious webpage identifier in the user device is improved and the security of the user device is protected.

[0044] FIG. 3 is a flowchart illustrating a method for processing a webpage according to another example of the present disclosure. In the method as shown in FIG. 3, blocks 310, 320, 330 and 360 are respectively the same with blocks 210 to 240 in FIG. 2. Different from FIG. 2, after block 330, the method as shown in FIG. 3 further includes

the following.

[0045] At block 340, it is determined whether a current network situation meets a predefined condition for transmitting the querying request to the cloud server, if yes, block 360 is performed; otherwise, block 350 is performed.

[0046] In this block, if the network situation is not good or it is unable to connect to the Internet, it is determined that the predefined condition is not met.

[0047] At block 350, the obtained webpage identifier is saved in the user device.

[0048] FIG. 4 is a flowchart illustrating a method for processing a webpage according to another example of the present disclosure. In the method as shown in FIG. 4, blocks 410 to 440 are respectively the same with blocks 210 to 240 in FIG. 2. Different from FIG. 2, after block 440, the method as shown in FIG. 4 further includes the following.

[0049] At block 450, the querying result is received from the cloud server. It is determined whether the webpage identifier is malicious. If yes, block 460 is performed; otherwise, the method ends.

[0050] At block 460, prompt information is generated for the user. Access to the webpage identifier is blocked, or the webpage identifier is removed or repaired.

[0051] FIG. 5 is a flowchart illustrating a method for processing a webpage at a cloud server side according to an example of the present disclosure. FIG. 5 is a simplified diagram according to one embodiment of the present invention. This diagram is merely an example, which should not unduly limit the scope of the claims. One of ordinary skill in the art would recognize many variations, alternatives, and modifications.

[0052] At block 501, malicious webpage identifiers and/or a malicious webpage identifier determining rule are stored in advance.

[0053] At block 502, a querying request transmitted by a user device is received, wherein the querying request includes a webpage identifier.

[0054] At block 503, it is determined whether the webpage identifier in the querying request is a malicious webpage identifier; if yes, block 504 is performed; otherwise, the method ends.

[0055] In this example, there are two manners for determining whether the webpage identifier in the querying request is a malicious webpage identifier.

[0056] In a first manner, the webpage identifier in the querying request is compared with malicious webpage identifiers stored in the cloud server. If the webpage identifier in the querying request is the same with one of the malicious webpage identifiers stored in the cloud server, it is determined that the webpage identifier in the querying request

is a malicious webpage identifier.

[0057] In a second manner, it is determined whether the webpage identifier in the querying request meets the malicious webpage identifier determining rule stored in the cloud server. If the webpage identifier in the querying request meets the malicious webpage identifier determining rule stored in the cloud server, it is determined that the webpage identifier in the querying request is a malicious webpage identifier.

[0058] For example, the determining rule may include: whether a querying times of the webpage identifier in the querying request reaches a predefined determining times, if yes, it is determined that the webpage identifier in the querying request is a malicious webpage identifier. In a practical application, the cloud server may sort webpage identifiers according to their querying times. The webpage identifier with a largest querying times ranks in the first. Then, the cloud server may determine that webpage identifiers rank in, e.g. first five are malicious webpage identifiers. In one example, the determination on whether the webpage identifier is malicious may also be performed by a manager.

[0059] At block 504, a querying result is generated and information indicating whether the webpage identifier in the querying request is a malicious webpage identifier is added in the querying result.

[0060] At block 505, the generated querying result is transmitted to the user device.

[0061] FIG. 6 is a schematic diagram illustrating a user device for processing a webpage according to an example of the present disclosure. As shown in FIG. 6, the user device includes a webpage identifier obtaining module 61, a format determining module 62, a format converting module 63, and a querying module 64.

[0062] The webpage identifier obtaining module 61 obtains a webpage identifier of a webpage.

[0063] In a practical application, the webpage identifier obtaining module 61 may scan a predetermined area of the user device to obtain the webpage identifier, wherein the predetermined area stores the webpage identifier.

[0064] The format determining module 62 determines whether the webpage identifier obtained by the webpage identifier obtaining module 61 is in a predefined standard format. If not, the format converting module 63 converts the webpage identifier into the standard format.

[0065] The querying module 64 generates a querying request and transmits the querying request to a cloud server to obtain a querying result. The querying request

includes the webpage identifier in the standard format. The querying result includes information indicating whether the webpage identifier is malicious.

[0066] FIG. 7 is a schematic diagram illustrating a user device for processing a webpage according to another example of the present disclosure. Compared with the user device as shown in FIG. 6, the user device as shown in FIG. 7 further includes a detecting module 65. The detecting module 65 detects whether a webpage open instruction is received, if the detecting module 65 detects that the webpage open instruction is received, the webpage identifier obtaining module 61 obtains the webpage identifier of the webpage.

[0067] Functions and operations of other modules in FIG. 7 are similar to those of corresponding modules as shown in FIG. 6 and will not be repeated herein.

[0068] FIG. 8 is a schematic diagram illustrating a user device for processing a webpage according to still another example of the present disclosure. Compared with the user device as shown in FIG. 7, the user device as shown in FIG. 8 further includes a network situation determining module 66 and a storage module 67. The network situation determining module 66 determines whether a current network situation meets a predefined condition for transmitting the querying request to the cloud server. If the network situation determining module 66 determines that the current network situation does not meet the predefined condition, the storage module 67 stores the webpage identifier in the user device. If the network situation determining module 66 determines that the network situation meets the predefined condition, the querying module 64 generates the querying request and transmits the querying request to the cloud server to obtain the querying result.

[0069] Functions and operations of other modules in FIG. 8 are similar to those of corresponding modules as shown in FIG. 7 and will not be repeated herein.

[0070] FIG. 9 is a schematic diagram illustrating a user device for processing a webpage according to yet another example of the present disclosure. Compared with the user device as shown in FIG. 8, the user device as shown in FIG. 9 further includes a webpage identifier determining module 68 and a processing module 69. The webpage identifier determining module 68 receives the querying result returned by the cloud server and determines whether the webpage identifier is malicious according to the querying result. If the webpage identifier determining module 68 determines that the webpage identifier is malicious, the processing module 69 generates prompt information for the user and processes the webpage identifier, e.g., block access to the

webpage identifier or delete the webpage identifier.

[0071] FIG. 10 is a schematic diagram illustrating a structure of a cloud server for processing a webpage according to an example of the present disclosure. FIG. 10 is a simplified diagram according to one embodiment of the present invention. This diagram is merely an example, which should not unduly limit the scope of the claims. One of ordinary skill in the art would recognize many variations, alternatives, and modifications.

[0072] As shown in FIG. 10, the cloud server includes: a querying request receiving module 1001, a malicious webpage determining module 1002, a querying result generating module 1003 and a querying result transmitting module 1004.

[0073] The querying request receiving module 1001 receives a querying request transmitted by a user device, wherein the querying request includes a webpage identifier. The malicious webpage determining module 1002 determines whether the webpage identifier in the querying request is a malicious webpage identifier.

[0074] In a practical application, the malicious webpage determining module 1002 includes a comparing unit 1021 and/or a standard matching unit 1022.

[0075] The comparing unit 1021 compares the webpage identifier in the querying request with malicious webpage identifiers stored in the cloud server. If the webpage identifier is the same with one of the malicious webpage identifiers stored in the cloud server, the malicious webpage determining module 1002 determines that the webpage identifier in the querying request is malicious.

[0076] The standard matching unit 1022 determines whether the webpage identifier in the querying request meets a malicious webpage identifier determining rule stored in the cloud server. If yes, the malicious webpage determining module 1002 determines that the webpage identifier in the querying request is malicious. The determining rule includes: a querying times of the webpage identifier in the querying request reaches a predefined determining times.

[0077] The querying result generating module 1003 generates a querying result and adds information indicating whether the webpage identifier in the querying request is malicious in the querying result. The querying result transmitting module 54 transmits the querying result to the user device.

[0078] In examples of the present disclosure, the user device obtains the webpage identifier, converts the webpage identifier into the standard format and transmits the webpage identifier in the standard format to the cloud server which determines whether

the webpage identifier is malicious. The solution of the present disclosure effectively identifies the obtained webpage identifier, improves removing efficiency of malicious webpage identifiers in the user device and improves security performance of the user device.

[0079] What has been described and illustrated herein is a preferred example of the disclosure along with some of its variations. The terms, descriptions and figures used herein are set forth by way of illustration only and are not meant as limitations. Many variations are possible within the spirit and scope of the disclosure, which is intended to be defined by the following claims -- and their equivalents -- in which all terms are meant in their broadest reasonable sense unless otherwise indicated.

CLAIMS

1. A method for processing a webpage, comprising:
 - obtaining, by a user device, a webpage identifier;
 - determining, by the user device, whether the webpage identifier is in a predefined standard format; if the webpage identifier is not in the predefined standard format, converting, by the user device, the webpage identifier into a webpage identifier in the predefined standard format; and
 - generating, by the user device, a querying request and transmitting the querying request to a cloud server to receive a querying result; wherein the querying request comprises the webpage identifier in the standard format, the querying result comprises information indicating whether the webpage identifier is malicious.
2. The method of claim 1, wherein the obtaining the webpage identifier comprises:
 - detecting, by the user device, whether a webpage open instruction is received; and
 - if the webpage open instruction is received, obtaining, by the user device, the webpage identifier of the webpage being opened when the webpage is opened.
3. The method of claim 1, wherein the obtaining the webpage identifier comprises:
 - scanning, by the user device, a predefined area of the user device to obtain the webpage identifier, wherein the predefined area stores the webpage identifier.
4. The method of claim 1, further comprising:
 - before generating the querying request and transmitting the querying request to the cloud server, determining, by the user device, whether a current network situation meets a predefined condition for transmitting the querying request to the cloud server;
 - if the current network situation does not meet the predefined condition, storing the webpage identifier in the user device; and
 - if the current network situation meets the predefined condition, performing the process of generating the querying request and transmitting the querying request to the cloud server.

5. The method of claim 1, further comprising:
receiving, by the user device, the querying result;
determining, by the user device, whether the webpage identifier is malicious according to the querying result; and
if the webpage identifier is malicious, generating prompt information for a user and processing the webpage identifier.

6. The method of any one of claim 1 to 5, wherein the webpage identifier is a webpage address.

7. A method for processing a webpage, comprising:
receiving, by a cloud server, a querying request transmitted by a user device, wherein the querying request comprises a webpage identifier;
determining, by the cloud server, whether the webpage identifier in the querying request is malicious; and
generating, by the cloud server, a querying result and transmitting the querying result to the user device, wherein the querying result comprises information indicating whether the webpage identifier is malicious.

8. The method of claim 7, wherein the determining whether the webpage identifier in the querying request is malicious comprises:
comparing, by the cloud server, the webpage identifier in the querying request with malicious webpage identifiers which are stored in the cloud server in advance, if the webpage identifier in the querying request is the same with one of the malicious webpage identifiers stored in the cloud server, determining, by the cloud server, that the webpage identifier in the querying request is malicious.

9. The method of claim 7, wherein the determining whether the webpage identifier in the querying request is malicious comprises:
determining, by the cloud server, whether the webpage identifier in the querying request meets a malicious webpage identifier determining rule which is stored in the cloud server in advance, if the webpage identifier in the querying request meets the malicious webpage identifier determining rule, determining, by the cloud server, that

the webpage identifier in the querying request is malicious.

10. The method of claim 9, wherein the malicious webpage identifier determining rule comprises: a querying times of the webpage identifier in the querying request reaches a predefined determining times.

11. A user device, comprising:

one or more processors;

memory; and

one or more program modules stored in the memory and to be executed by the one or more processors, the one or more program modules comprise:

a webpage identifier obtaining module, to obtain a webpage identifier;

a format determining module, to determine whether the webpage identifier obtained by the webpage identifier obtaining module is in a predefined standard format;

a format converting module, to convert the webpage identifier into a webpage identifier in the standard format if the format determining module determines that the webpage identifier is not in the standard format; and

a querying module, to generate a querying request and transmit the querying request to a cloud server to obtain a querying result; wherein the querying request comprises the webpage identifier; the querying result comprises information indicating whether the webpage identifier is malicious.

12. The user device of claim 11, wherein the one or more program modules further comprise:

a detecting module, to detect whether a webpage open instruction is received; and

the webpage identifier obtaining module is further to obtain, if the detecting module detects that the webpage open instruction is received and when a webpage is opened, the webpage identifier of the webpage being opened.

13. The user device of claim 11, the webpage identifier obtaining module is further to scan a predefined area of the user device to obtain the webpage identifier, wherein the predefined area stores the webpage identifier.

14. The user device of claim 11, wherein the one or more program modules further

comprise:

a network situation determining module, to determine whether a current network situation meets a predefined condition for transmitting the querying request to the cloud server;

a storage module, to store the webpage identifier in the user device if the network situation determining module determines that the current network situation does not meet the predefined condition; and

the querying module is further to generate the querying request and transmit the querying request to the cloud server if the network situation determining module determines that the current network situation meets the predefined condition.

15. The user device of claim 11, wherein the one or more program modules further comprise:

a webpage identifier determining module, to receive the querying result and determine whether the webpage identifier is malicious according to the querying result; and

a processing module, to generating prompt information for a user and process the webpage identifier if the webpage identifier determining module determines that the webpage identifier is malicious.

16. A cloud server, comprising:

one or more processors;

memory; and

one or more program modules stored in the memory and to be executed by the one or more processors, the one or more program modules comprise:

a querying request receiving module, to receive a querying request transmitted by a user device, wherein the querying request comprises a webpage identifier;

a malicious webpage determining module, to determine whether the webpage identifier in the querying request is malicious;

a querying result generating module, to generate a querying result, wherein the querying result comprises information indicating whether the webpage identifier in the querying request is malicious; and

a querying result transmitting module, to transmit the querying result to the user device.

17. The cloud server of claim 16, wherein the malicious webpage determining module further comprises:

a comparing unit, to compare the webpage identifier in the querying request with malicious webpage identifiers which are stored in the cloud server in advance; and

the malicious webpage determining module is to determine that the webpage identifier in the querying request is malicious if the webpage identifier in the querying request is the same with one of the malicious webpage identifier stored in the cloud server.

18. The cloud server of claim 16, wherein the malicious webpage determining module further comprises:

a standard matching unit, to determine whether the webpage identifier in the querying request meets a malicious webpage identifier determining rule which is stored in the cloud server in advance; and

the malicious webpage determining module is further to determine that the webpage identifier in the querying request is malicious if the standard matching unit determines that the webpage identifier in the querying request meets the malicious webpage identifier determining rule.

19. The cloud server of claim 18, wherein the malicious webpage identifier determining rule comprises:

a querying times of the webpage identifier in the querying request reaches a predefined determining times.

20. A non-transitory computer-readable storage medium comprising a set of instructions for processing a webpage, the set of instructions to direct at least one processor to perform acts of:

obtaining a webpage identifier;

determining whether the webpage identifier is in a predefined standard format; if the webpage identifier is not in the predefined standard format, converting the webpage identifier into a webpage identifier in the predefined standard format; and

generating a querying request and transmitting the querying request to a cloud server to receive a querying result; wherein the querying request comprises the

webpage identifier in the standard format, the querying result comprises information indicating whether the webpage identifier is malicious.

21. A non-transitory computer-readable storage medium comprising a set of instructions for processing a webpage, the set of instructions to direct at least one processor to perform acts of:

receiving a querying request transmitted by a user device, wherein the querying request comprises a webpage identifier;

determining whether the webpage identifier in the querying request is malicious;
and

generating a querying result and transmitting the querying result to the user device, wherein the querying result comprises information indicating whether the webpage identifier is malicious.

1/7

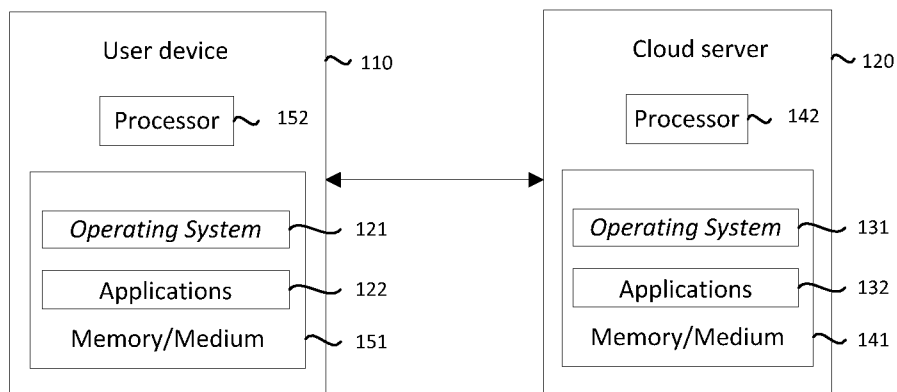


FIG. 1

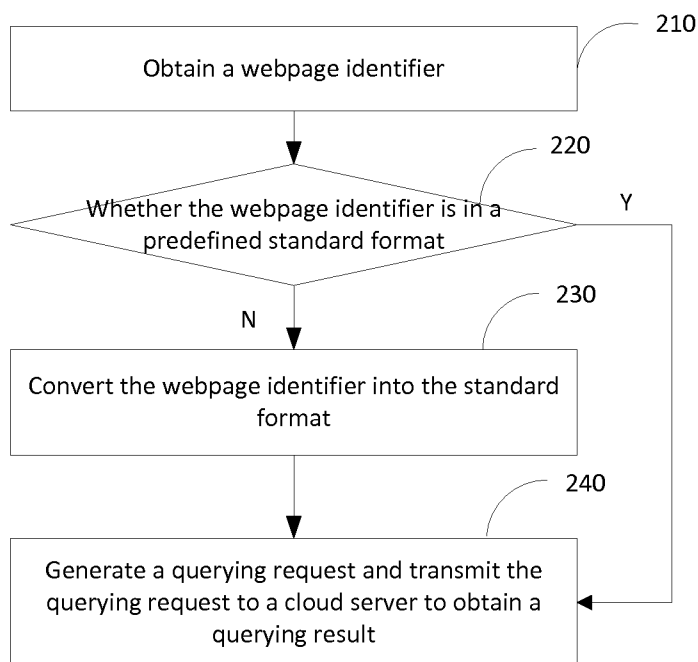


FIG. 2

2/7

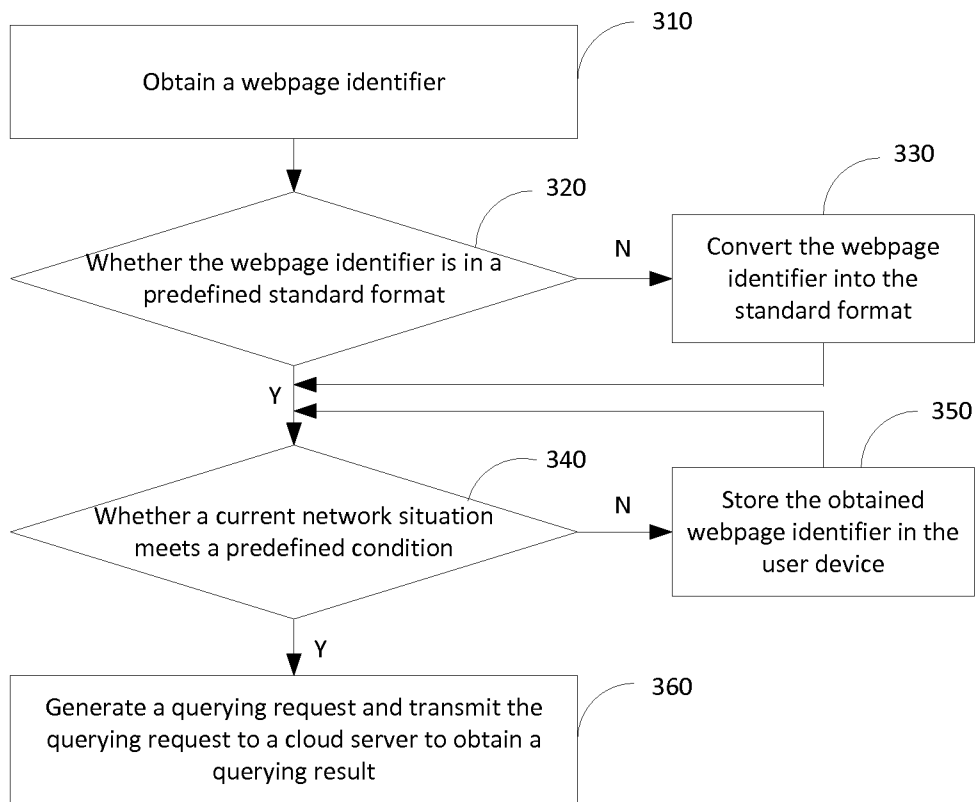


FIG. 3

3/7

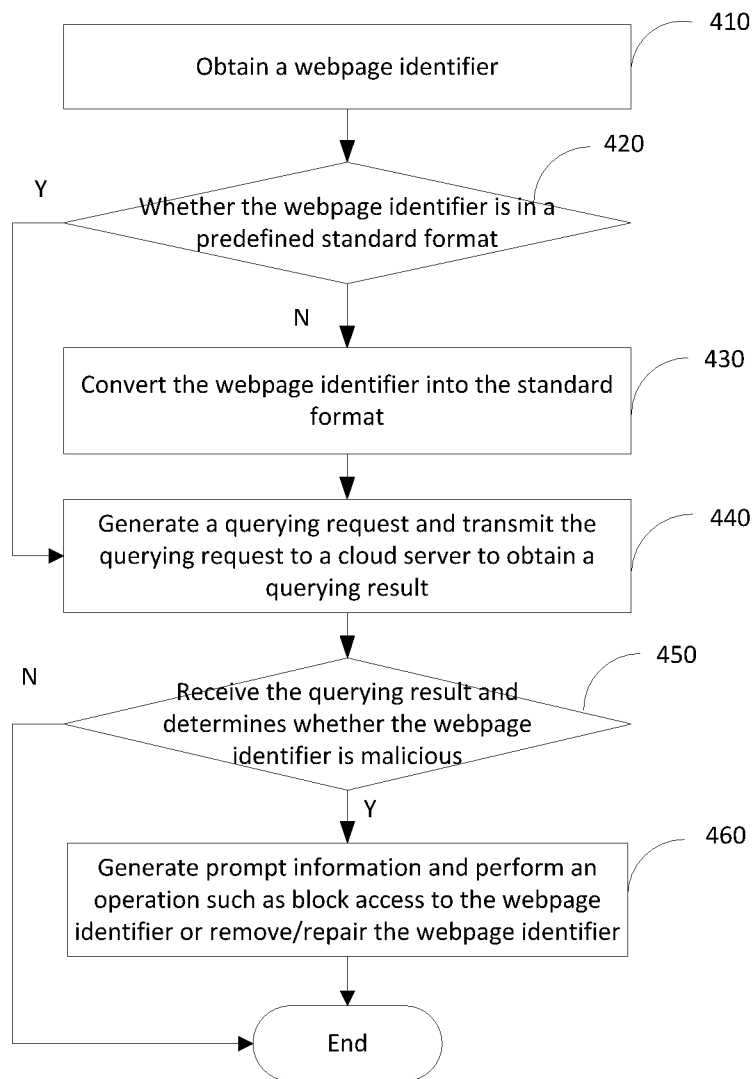


FIG. 4

4/7

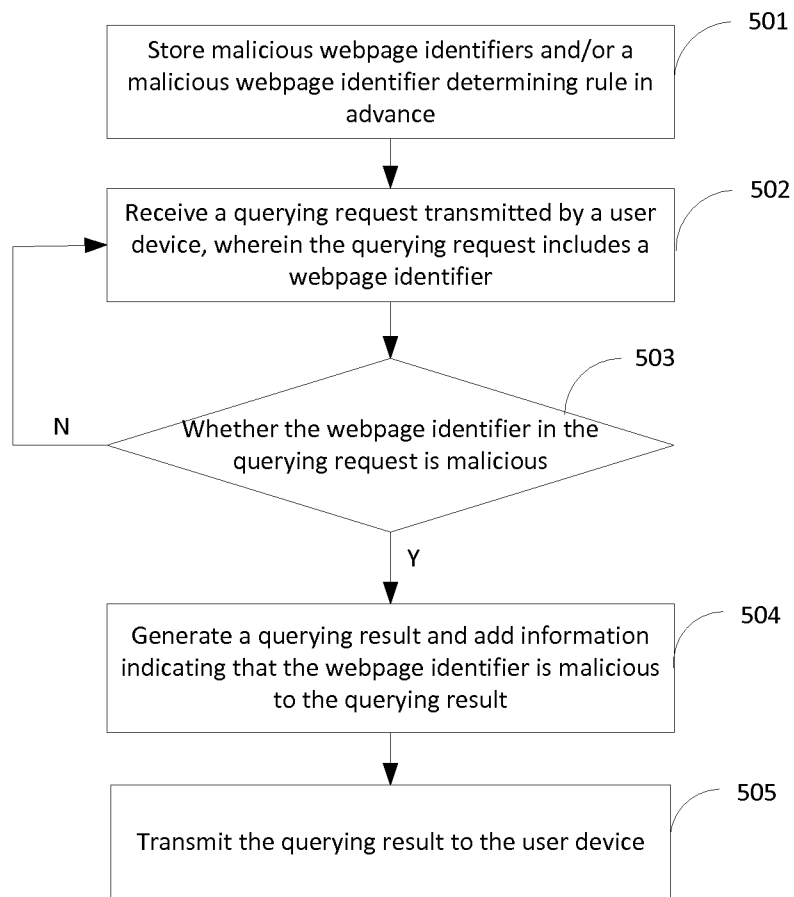


FIG. 5

5/7

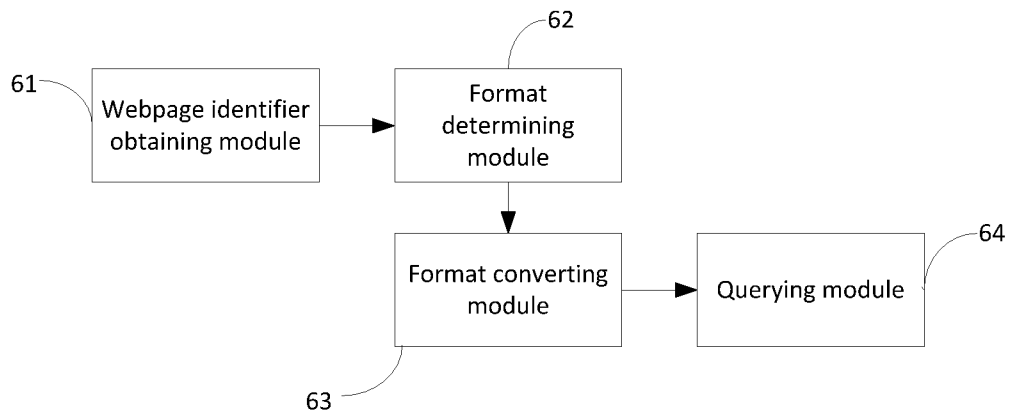


FIG. 6

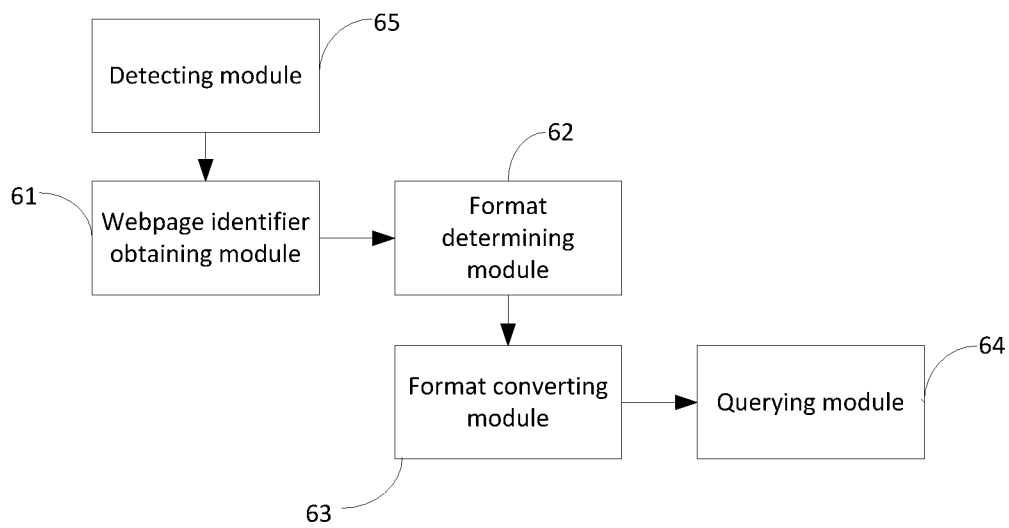


FIG. 7

6/7

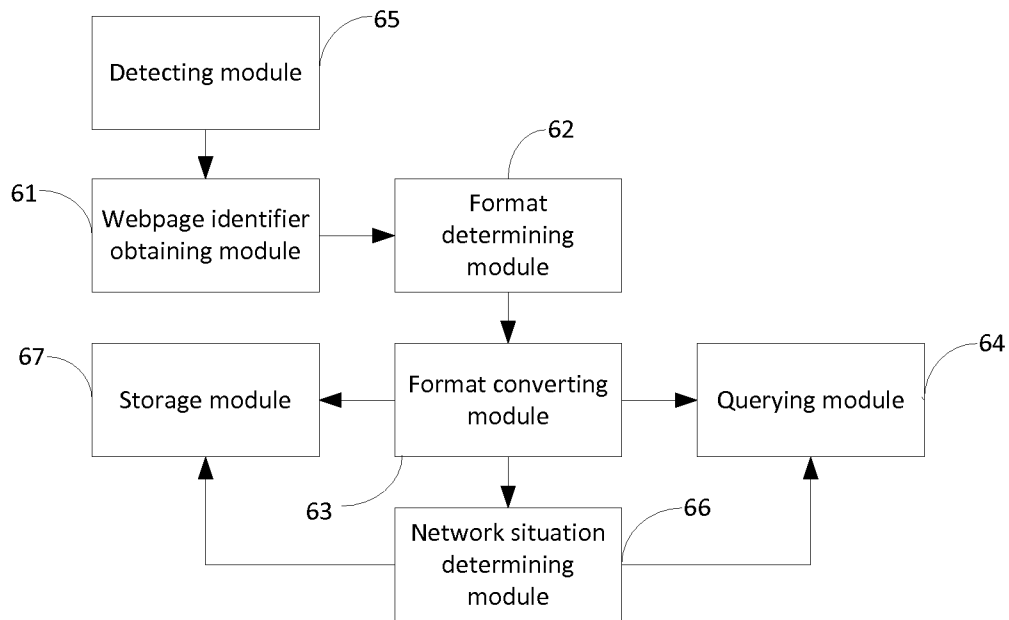


FIG. 8

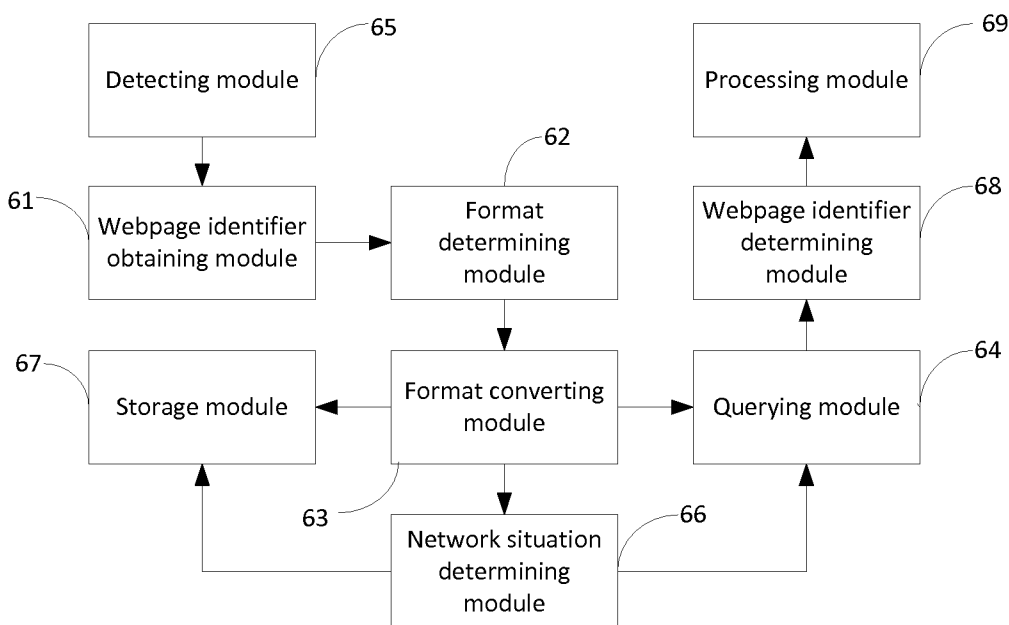


FIG. 9

7/7

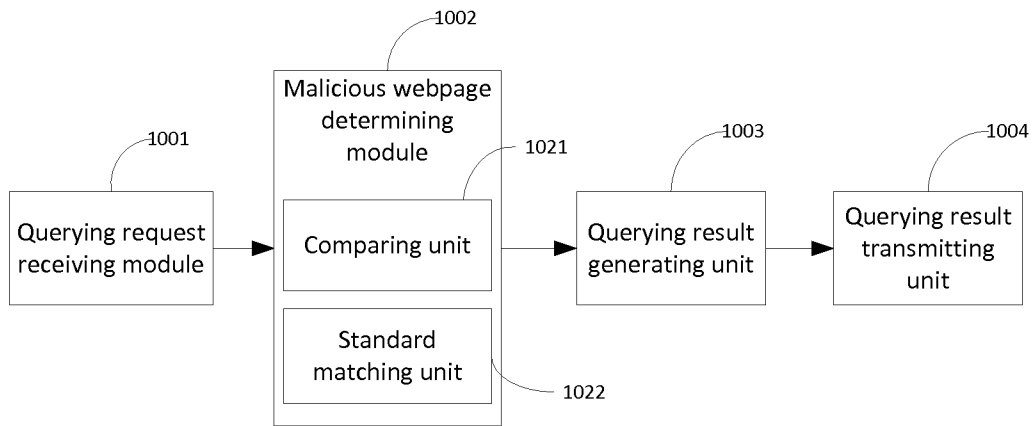


FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/084317

A. CLASSIFICATION OF SUBJECT MATTER

G06F 17/30 (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: 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)

CNABS, CNTXT, DWPI: DOMAIN NAME, WEBPAGE ADDRESS, URL, CONVERT, COUNTERFEIT, FORGE, MALICIOUS, OBTAIN, ACQUIRE, TIME, THRESHOLD

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2010110885 A1 (ALIBABA GROUP HOLDING LIMITED) 30 September 2010 (30.09.2010) see description, paragraphs 0021-0081 and figures 1-6	1-21
A	CN 102594825 A (BEIJING BAIDU NETCOM SCI&TECHNOLOGY CO.) 18 July 2012 (18.07.2012) the whole document	1-21
A	CN 102082836 A (CHINESE MOBILE GROUP SICHUAN COMPANY LIMITED) 01 June 2011 (01.06.2011) the whole document	1-21
A	US 2008172738 A1 (IBM CORPORATION) 17 July 2008 (17.07.2008) the whole document	1-21

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search
09 December 2013 (09.12.2013)

Date of mailing of the international search report
02 Jan. 2014 (02.01.2014)

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
HE,Minglun
Telephone No. (86-10)61648107

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/084317

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2010110885 A1	30.09.2010	CN 101504673 A	12.08.2009
		US 2010251380 A1	30.09.2010
		EP 2411913 A1	01.02.2012
		HK 1133720 A1	30.12.2011
		JP 2012521599 A	13.09.2012
CN 102594825 A	18.07.2012	None	
CN 102082836 A	01.06.2011	None	
US 2008172738 A1	17.07.2008	CN 101221611 A	16.07.2008