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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 October 2014 (16.10.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/166266 A1

(51) International Patent Classification:
G06F 21/56 (2013.01)

(21) International Application Number:
PCT/CN2013/088489

(22) International Filing Date:
4 December 2013 (04.12.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201310119396.7 8 April 2013 (08.04.2013) 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) Inventor: **NIE, Zixiao**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN).

(74) Agent: **SHENPAT INTELLECTUAL PROPERTY AGENCY**; Room 1521, West Block, Guomao Building, Shenzhen, Guangdong 518014 (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, IR, 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: FILE SCANNING METHOD AND SYSTEM, CLIENT AND SERVER

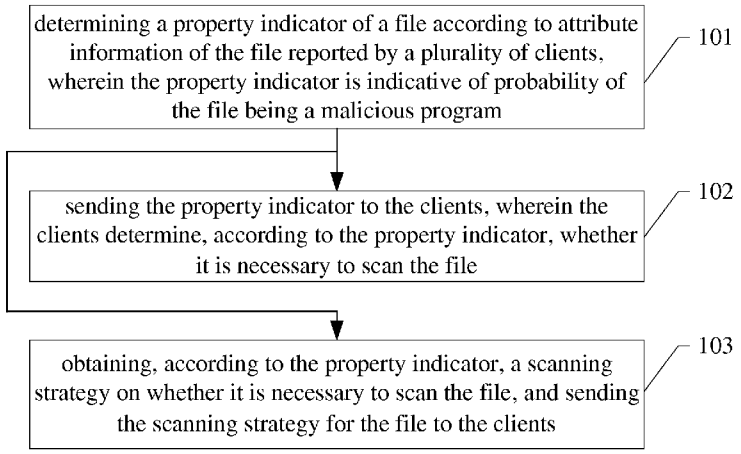

Fig. 2

(57) Abstract: A file scanning method and a file scanning system, a client and a server are disclosed. The server determines, by comprehensive consideration of the attribute information of the file reported by a plurality of clients, the property indicator of the file, i.e., the probability of the file being a malicious program; and the server sends the property indicator to the clients, wherein the clients determine, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, or the server directly determines, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and sends the scanning strategy to the clients. Then, the clients scan the file in accordance with the scanning strategy for the file, and only the file which has a higher probability to be a malicious program will be scanned.

WO 2014/166266 A1

FILE SCANNING METHOD AND SYSTEM, CLIENT AND SERVER

[0001] The present application claims the priority to Chinese Patent Application No. 201310119396.7, entitled as "FILE SCANNING METHOD AND SYSTEM, CLIENT AND SERVER", filed on April 8, 2013 with State Intellectual Property Office of People's Republic of China, which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] The present disclosure relates to communication technology and in particular to a file scanning method, a file scanning system, a client and a server.

BACKGROUND

[0003] With the development of information technology, the relation between the human life and computers becomes tighter and tighter. To avoid the rapid development of trojans and viruses, by employing a real-time file monitoring system, the virus can be found timely, and the danger can be avoided.

[0004] Presently, with the real-time file monitoring system, the file operation event in the system can be monitored in real time in accordance with a determined strategy. When a file operation event is monitored, a virus scanning engine is activated, and then a scanning, an intercepting and an anti-virus operation are performed based on the result from the scanning engine. However, the amount of the file operation events in the system is huge, and the occurrence of viruses is an event with relatively lower probability, so that the benefit from the real-time file monitoring system is poor.

SUMMARY

[0005] The present disclosure provides a file scanning method, a file scanning system, a client and a server, whereby the amount of the files to be scanned in file defense is decreased, and the effect on the other operations of the system is reduced.

[0006] It is provided a file scanning method in an embodiment of the disclosure, the file scanning method including:

determining a property indicator of a file according to attribute information of the file reported by a plurality of clients, wherein the property indicator is indicative of probability of the file being a malicious program; and

sending the property indicator to the clients, wherein the clients determine, according to the property indicator, whether it is necessary to scan the file; or obtaining, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and sending the scanning strategy for the file to the clients.

[0007] It is further provided a file scanning method in an embodiment of the disclosure, which includes:

reporting attribute information of a file to a server;

receiving from the server a scanning strategy on whether it is necessary to scan the file, wherein the scanning strategy is returned by the server according to the attribute information of the file reported by a plurality of clients; or receiving from the server a property indicator of the file, obtaining, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, wherein the property indicator is returned by the server according to the attribute information of the file reported by the plurality of clients.

[0008] It is further provided a server in an embodiment of the disclosure, which includes:

a property indicator determining unit, configured to determine a property indicator of a file according to attribute information of the file reported by a plurality of clients, where the property indicator is indicative of probability of the file being a malicious program; and

a sending unit, configured to send the property indicator to the clients, wherein the clients determine, according to the property indicator, whether it is necessary to scan the file; or to obtain, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and to send the

scanning strategy for the file to the clients.

[0009] It is further provided a client in an embodiment of the disclosure, which includes:

an attribute reporting unit, configured to report attribute information of a file to a server; and

a file scanning unit, configured to receive from the server a scanning strategy on whether it is necessary to scan the file, wherein the scanning strategy is returned by the server according to the attribute information of the file reported by a plurality of clients; or configured to receive from the server a property indicator of the file, to obtain, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, wherein the property indicator is returned by the server according to the attribute information of the file reported by the plurality of clients.

[0010] It is further provided a file scanning system in an embodiment of the disclosure, which includes a plurality of clients and a server,

wherein the server includes:

a property indicator determining unit, configured to determine a property indicator of a file according to attribute information of the file, wherein the property indicator is indicative of probability of the file being a malicious program; and

a sending unit, configured to send the property indicator to the clients, wherein the clients determine, according to the property indicator, whether it is necessary to scan the file; or to obtain, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and to send the scanning strategy for the file to the clients, and

the client includes:

an attribute reporting unit, configured to report the attribute information of the file to a server; and

a file scanning unit, configured to receive from the server a scanning

strategy on whether it is necessary to scan the file, wherein the scanning strategy is returned by the server according to the attribute information of the file reported by a plurality of clients; or configured to receive from the server a property indicator of the file, to obtain, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, wherein the property indicator is returned by the server according to the attribute information of the file reported by the plurality of clients.

[0011] It can be seen that in the embodiment of the disclosure, during the file real-time protection, the server determines, by comprehensive consideration of the attribute information of the file reported by a plurality of clients, the property indicator of the file, i.e., the probability of the file being a malicious program; and the server sends the property indicator to the clients, wherein the clients determine, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, or the server directly determines, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and sends the scanning strategy to the clients. Then, the clients scan the file in accordance with the scanning strategy for the file, and only the file which has a higher probability to be a malicious program will be scanned. Therefore, the amount of the files to be scanned during the protection can be decreased, the spent time is shortened, and the influence on the other operations in the server is reduced.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] In order to illustrate the technical solutions according to the embodiments of the present disclosure or in the prior art more clearly, drawings used in the description will be described briefly hereinafter. Apparently, the drawings described hereinafter are only some embodiments of the present disclosure, and other drawings may be obtained by those skilled in the art according to those drawings without creative labor.

[0013] Figure 1 is a schematic structural diagram of a file scanning system according to an embodiment of the disclosure;

[0014] Figure 2 is a flow chart of a file scanning method performed by a server according to an embodiment of the disclosure;

[0015] Figure 3a is a flow chart of a file scanning method performed by a server according to another embodiment of the disclosure;

[0016] Figure 3b is a flow chart of a file scanning method performed by a server according to yet another embodiment of the disclosure;

[0017] Figure 4 is a flow chart of a file scanning method performed by a client according to an embodiment of the disclosure;

[0018] Figure 5 is a schematic structural diagram of a server according to an embodiment of the disclosure;

[0019] Figure 6 is a schematic structural diagram of a server according to another embodiment of the disclosure;

[0020] Figure 7 a schematic structural diagram of a server according to yet another embodiment of the disclosure;

[0021] Figure 8 is a schematic structural diagram of a client according to an embodiment of the disclosure; and

[0022] Figure 9 is a schematic structural diagram of a client according to another embodiment of the disclosure.

DETAILED DESCRIPTION

[0023] Hereinafter, the technical solutions in the embodiments of the present disclosure will be described clearly and completely in conjunction with the drawings. Obviously, the described embodiments are only some of the embodiments of the present disclosure, but not all the embodiments. All the other embodiments obtained by those skilled in the art based on the embodiments in the present disclosure without creative labor will fall within the scope of protection of the present disclosure.

[0024] It is provided a file scanning method in an embodiment of the disclosure. The file scanning method is generally applied in a system as shown in Figure 1.

The system includes a server and a plurality of clients. The method in this embodiment is the method performed by the server of the system, and as shown by the flow chart in Figure 2, the method includes the following steps 101 to 103.

[0025] Step 101, determining a property indicator of the file according to the received attribute information of the file reported by a plurality of clients, wherein the property indicator is indicative of probability of the file being a malicious program, and then proceeding to step 102 or 103.

[0026] The attribute information is the information for describing the file, and may include, but not limited to, at least one of path information of the file, i.e., store address information of the file, loading information of the file, i.e., information during the loading of the file into a memory, releasing information of the file, i.e. information during the releasing of the file, a black-white attribute of the file, i.e., information on whether the file is a malicious program, context information of a program corresponding to the file (i.e., information of a parent procedure) and the like.

[0027] It can be understood that each client scans periodically or time to time the file stored locally, and reports the attribute information of the file to the server. The client may determine, according to a preset attribute reporting strategy, which attribute information of the file is to be reported by the client, where the preset attribute reporting strategy can include the prescription of reporting which attribute information of the file in which case; or the client may make the decision according to the instruction information sent from the server. In this case, the server can send instruction information to the clients for instructing to the clients which attribute information of the file is to be reported, and further, the instruction information can instruct the client that in which case the client needs to report the attribute information of the file.

[0028] For a same file, the storing manner on different clients may be different, and then the attribute information of the file reported by the clients may be different. In this embodiment, the server gathers different attribute information of the same file reported by the plurality of clients, and determines the

probability of the file being a malicious program. The property indicator of the file can be determined in the following two ways.

[0029] (1) If the attribute information of the file reported by each client corresponds to only one attribute, i.e., any one of the foregoing attribute information, for example, each client sends the black-white attribute of the file, the server can determine the property indicator of the file in the following steps A1 to B1, and the flow chart is shown in Figure 3a.

[0030] A1: determining for each one of the plurality of clients, according to the attribute information of the file reported by each client, whether the file is a malicious program. Specifically, it is to determine whether the attribute information of the file reported by each client conforms to a preset strategy, i.e., the attribute information of the file reported by each client conforms to the attribute information for determining the file as a malicious program. If the attribute information of the file reported by one client conforms to the preset strategy, the file is a malicious program; otherwise, the file is not a malicious program.

[0031] B1: Determining the property indicator of the file by a ratio of the number of clients for which the file is determined as the malicious program to the total number of the plurality of clients. For example, according to the attribute information of the file reported by M clients, the server determines that for N clients that the file is determined as the malicious program, thus the obtained property indicator of the file is N/M.

[0032] (2) If the attribute information of the file reported by each client corresponds to multiple attributes, i.e., multiple types of the foregoing attribute information, for example, each client reports the black-white attribute of the file and the path information of the file, the server can determine the property indicator of the file in the following steps A2 to C2, and the flow chart is shown in Figure 3b.

[0033] A2: determining by the server, for each one of the plurality of clients, according to the information corresponding to the multiple attributes reported by each client, whether the file is a malicious program with respect to each of the

multiple attributes respectively. Specifically, the server determines whether the information corresponding to each attribute reported by each client conforms to a preset strategy, i.e., the attribute information corresponding to each attribute reported by each client conforms to the attribute information for determining the file as a malicious program. If a preset strategy for an attribute is met, the file is a malicious program with respect to this attribute. In this way, whether the file is a malicious program with respect to the respective attributes may be obtained for each client.

[0034] B2: Determining, for each of the multiple attributes of the file, a probability ratio of the file being a malicious program with respect to the attribute by a ratio of the clients for which the file is determined as the malicious program with respect to the attribute to the total number of the plurality of clients.

[0035] C2: determining the property indicator of the file by a sum of the respective probability ratios of the file being a malicious program with respect to the multiple attributes, or determining the property indicator of the file by a sum of weighted probability ratios of the file being a malicious program with respect to the multiple attributes, where the weighted probability ratios are products of the respective probability ratios multiplying with corresponding weights.

[0036] For example, each client reports attribute information corresponding to two attributes of the file, e.g., information of an attribute a and information of an attribute b, the server firstly obtains for respective clients first information on whether the file is a malicious program with respect to the attribute a according to the information of the attribute a reported from each client, i.e., the server determines respectively whether the information of the attribute a reported from each client is in accordance with a first preset strategy and obtains the first information for respective clients, for example, it is determined that there are n1 clients for which the file is a malicious program with respect to the attribute a; and the server obtains for respective clients second information on whether the file is a malicious program with respect to the attribute b according to the information of the attribute b of the file reported from each client, i.e., the server

determines for respective clients whether the information of the attribute b reported from each client is in accordance with a second preset strategy, and obtains the second information for respective clients, for example, it is determined that there are n2 clients for which the file is a malicious program with respect to the attribute b.

[0037] Then, the server determines, for the attribute a, a ratio of the number n1 of the clients for which the file is determined as a malicious program to the total number m of the plurality of clients, namely n1/m, as the probability ratio of the file being a malicious program with respect to the attribute a; and determines, for the attribute b, the number n2 of the clients for which the file is determined as a malicious program by the total number m of the plurality of clients, namely n2/m, as the probability ratio of the file being a malicious program with respect to the attribute b is.

[0038] Finally, the probability ratios of the file being a malicious program obtained with respect to the respective attributes are added to obtain the property indicator of the file, i.e., (n1/m)+(n2/m); alternatively, the probability ratios of the file being a malicious program obtained with respect to the respective attributes are multiplied with corresponding weight values (which are x1 and x2, respectively), and then the products are added to obtain the property indicator of the file, i.e., x1*(n1/m)+x2*(n2/m). Each weight value can be set by the user based on experience. If the information of one attribute of the file is relatively more important for determining whether the file is a malicious program, the weight value corresponding to this attribute can be set as greater.

[0039] Step 102, sending the property indicator to the clients, wherein the clients determine, according to the property indicator, whether it is necessary to scan the file. Accordingly, the clients may scan the file when it is necessary.

[0040] Step 103, obtaining, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and sending the scanning strategy for the file to the clients. Accordingly, the clients may scan the file respectively according to the scanning strategy.

[0041] When it is determined whether it is necessary for the clients to scan the

file, the property indicator can be compared with a preset value. If it is determined that the property indicator is greater than the preset value, it indicates that the file has a greater probability to be a malicious program, and it is necessary for the clients to scan the file. If the property indicator is less than or equal to the preset value, it indicates that the file has a less probability to be a malicious program, and it is unnecessary for the clients to scan the file.

[0042] It is to be noted that the server can continuously perform the steps 101 and 102, or the steps 101 and 103, for updating the information on whether it is necessary for the clients to scan the file.

[0043] It can be seen that in the embodiment of the disclosure, during the file real-time protection, the server determines, by comprehensive consideration of the attribute information of the file reported by a plurality of clients, the property indicator of the file, i.e., the probability of the file being a malicious program; and the server sends the property indicator to the clients, wherein the clients determine, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, or the server directly determines, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and sends the scanning strategy to the clients. Then, the clients scan the file in accordance with the scanning strategy for the file, and only the file which has a higher probability to be a malicious program will be scanned. Therefore, the amount of the files to be scanned during the protection can be decreased, the spent time is shortened, and the influence on the other operations in the server is reduced.

[0044] It is provided another file scanning method in an embodiment of the disclosure, which is generally applied in a system as shown in Figure 1. The method in this embodiment is the method performed by a client in the system, and as shown by the flow chart in Figure 4, the method includes the following steps 201 to 203.

[0045] Step 201, reporting attribute information of a file to a server, and then proceeding to step 202 or 203.

[0046] The attribute information may include, but not limited to, at least one of

path information of the file, loading information of the file, releasing information of the file, a black-white attribute of the file, context information of a program corresponding to the file and the like.

[0047] The client may determine, according to a preset attribute reporting strategy, which attribute information of the file is to be reported by the client, where the preset attribute reporting strategy can include the prescription of reporting which attribute information of the file in which case; or the client may make the decision according to the instruction information sent from the server. In this case, the client can receive instruction information sent from the server for instructing to the client which attribute information of the file is to be reported, and further, the instruction information can instruct the client that in which case the client needs to report the attribute information of the file.

[0048] Step 202, receiving from the server a scanning strategy on whether it is necessary to scan the file, where the scanning strategy is returned by the server according to the attribute information of the file reported by a plurality of clients. After step 202 is performed by the client, the server can obtain the scanning strategy of the file and send the scanning strategy to the client using steps 101 and 103 in the above embodiment, and then the client can perform the scanning in accordance with the obtained scanning strategy.

[0049] Step 203, receiving from the server a property indicator of the file, obtaining, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, where the property indicator is returned by the server according to the attribute information of the file reported by the plurality of clients. After the client performs step 201, the server can obtain the property indicator using steps 101 to 102 and send the property indicator to the client. In this case, the client further needs to obtain the scanning strategy of the file according to the property indicator. Specifically, the client can determine whether the property indicator is greater than a preset value. If the property indicator is greater than the preset value, it is necessary for the client to scan the file. And if the property indicator is not greater than the preset value, it is unnecessary for the client to scan the file. Thus, the client performs the scanning

in accordance with the obtained scanning strategy.

[0050] It can be seen that in the embodiment of the disclosure, during the file real-time protection, the clients report the attribute information of the file to the server; the server determines, by comprehensive consideration of the attribute information of the file reported by a plurality of clients, the property indicator of the file, i.e., the probability of the file being a malicious program; and the server sends the property indicator to the clients, wherein the clients determine, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, or the server directly determines, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and sends the scanning strategy to the clients. Then, the clients scan the file in accordance with the scanning strategy for the file, and only the file which has a higher probability to be a malicious program will be scanned. Therefore, the amount of the files to be scanned during the protection can be decreased, the spent time is shortened, and the influence on the other operations in the server is reduced.

[0051] It is further provided a server in an embodiment of the disclosure, and units of the server can scan the file in accordance with the flow chart shown in Figure 2, so as to perform real-time protection on the file according to the scanning. Figure 5 shows a schematic structural diagram of the server according to this embodiment, which includes a property indicator determining unit 11 and a sending unit 12.

[0052] The server may receive attribute information of the file reported by a plurality of clients. The attribute information may include, but not limited to, at least one of path information of the file, loading information of the file, releasing information of the file, a black-white attribute of the file, context information of a program corresponding to the file and the like.

[0053] The property indicator determining unit 11 is configured to determine a property indicator of the file according to the attribute information of the file reported by a plurality of clients, where the property indicator is indicative of probability of the file being a malicious program.

[0054] The sending unit 12 is configured to send the property indicator determined by the property indicator determining unit 11 to the clients, wherein the clients determine according to the property indicator whether it is necessary to scan the file. Alternatively, the sending unit 12 is configured to obtain, according to the property indicator determined by the property indicator determining unit 11, a scanning strategy on whether it is necessary to scan the file, and to send the scanning strategy for the file to the clients.

[0055] If the sending unit 12 needs to send the scanning strategy for the file to the clients, the sending unit can determine, when obtaining the scanning strategy of the file according to the property indicator, whether the property indicator is greater than a preset value. If the property indicator is greater than the preset value, it is necessary for the clients to scan the file. And if the property indicator is not greater than the preset value, it is unnecessary for the clients to scan the file. Thereby, the scanning strategy for the file is obtained.

[0056] It can be seen that in the server according to this embodiment of the disclosure, during the file real-time protection, the property indicator determining unit 11 determines, by comprehensive consideration of the attribute information of the file reported by a plurality of clients, the property indicator of the file, i.e., the probability of the file being a malicious program; and the sending unit 12 sends the property indicator to the clients, wherein the clients determine according to the property indicator a scanning strategy on whether it is necessary to scan the file, or the sending unit 12 directly determines, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and sends the scanning strategy to the clients. Then, the clients scan the file in accordance with the scanning strategy, and only the file which has a higher probability to be a malicious program will be scanned. Therefore, the amount of the files to be scanned during the protection can be decreased, the spent time is shortened, and the influence on the other operations in the server is reduced.

[0057] Referring to Figure 6, in a specific embodiment, in addition to the structure as shown in Figure 5, the server may further include an instruction

sending unit 13, and the property indicator determining unit 11 can be implemented by a malicious program determining unit 110 and a calculating unit 111.

[0058] The instruction sending unit 13 is configured to send instruction information to the plurality of clients, wherein the instruction information is indicative of the attribute information of the file to be reported by the clients.

[0059] The malicious program determining unit 110 is configured to, if the attribute information of the file reported by the clients includes information corresponding to one attribute, determine for each one of the plurality of clients, according to the attribute information of the file reported by each one of the plurality of clients, whether the file is a malicious program.

[0060] The calculating unit 111 is configured to determine the property indicator of the file by a ratio of the number of clients for which the file is determined as the malicious program to the total number of the plurality of clients, according to the information obtained by the malicious program determining unit 110.

[0061] In another specific embodiment, the malicious program determining unit 110 is further configured to, if the attribute information of the file reported by the clients corresponds to multiple attributes, determine, for each one of the plurality of clients, according to the information corresponding to the multiple attributes reported by each client, whether the file is a malicious program with respect to each of the multiple attributes respectively. The calculating unit 111 is further configured to determine, for each of the multiple attributes of the file, a probability ratio of the file being a malicious program with respect to the attribute by a ratio of the clients for which the file is determined as the malicious program with respect to the attribute to the total number of the plurality of clients; and to determine the property indicator of the file by a sum of the respective probability ratios of the file being a malicious program with respect to the multiple attributes, or to determine the property indicator of the file by a sum of weighted probability ratios of the file being a malicious program with respect to the multiple attributes, where the weighted probability ratios are products of

the respective probability ratios multiplying with corresponding weights.

[0062] In this embodiment, the instruction sending unit 13 sends the instruction information to the plurality of clients, and indicates to the clients the attribute of the file to be reported by the clients. Upon receiving the attribute information of the file reported by the plurality of clients, the malicious program determining unit 110 of the property indicator determining unit 11 determines for each one of the plurality of clients whether the file is a malicious program. Then the calculating unit 111 calculates the property indicator according to the information obtained by the malicious program determining unit 110. Finally, the sending unit 12 sends the scanning strategy for the file to the clients according to the calculating result from the calculating unit 111, or sends the calculating result from the calculating unit 111 to the clients.

[0063] In the following, the illustration is made by mainly taking the application of the file scanning method according to the embodiment of the disclosure as shown in Figure 2 in a server as an example. Reference is made to Figure 7, which shows a schematic structural diagram of a server according to an embodiment of the disclosure.

[0064] Specifically, the server can include a Radio Frequency (RF) circuit 20, a storage 21 including one or more computer readable storage medium, a wireless fidelity (WiFi) module 22, i.e., a communication module of a short-distance wireless transmission technology, a processor 23 including one or more processing cores, a power supply 24 and the like. It can be understood by those skilled in the art that the structure of the server shown in Figure 7 is not intended to limit the server, more or less components than shown in Figure may be included in the server, some components may be combined, or the components may be in another arrangement.

[0065] The RF circuit 20 can be configured to receive and send information, or receive and send signals during a phone call. Generally, the RF circuit 20 includes, but not limited to, an antenna, at least one amplifier, a tuner, one or more oscillators, a transceiver, a coupler, a Low Noiser Amplifier (LNA), a duplexer and the like. Further, the RF circuit 20 can communicate with a

network or other devices via wireless communication. The wireless communication may be performed according to any communication standard or protocol, including but not limited to Global System of Mobile communication (GSM), General Packet Radio Service (GPRS), Code Division Multiple Access (CDMA), Wideband Code Division Multiple Access (WCDMA), Long Term Evolution (LTE), e-mail, Short Messaging Service (SMS), and the like.

[0066] The storage 21 can be configured to store software program(s) and module(s). By running the software program(s) and module(s) stored in the storage 21, the processor 23 performs various function applications and data processing. The storage 21 can generally include a program storage area and a data storage area, where the program storage area may store an operating system, an application program required for at least one function (e.g., a function of playing audio, a function of displaying image, etc.), and the like. The data storage area can store the data (such as a preset attribute reporting strategy) created based on the usage of the server, and the like. Further, the storage 21 may include a high-speed random access memory, a non-volatile memory such as at least one magnetic disk storage, flash storage device, or other volatile solid-state storage device. Accordingly, the storage 21 may further include a storage controller for providing the processor 23 with the access to the storage 21.

[0067] The processor 23, as a control center of the server, is connected to various portions of the whole server via various interfaces and wires. By running or executing the software program(s) and/or module(s) stored in the storage 21, and invoking the data stored in the storage 21, the processor 23 performs various functions of the terminal and processes the data, so as to monitor the whole server. Optionally, the processor 23 may include one or more processing core. Preferably, the processor 23 can be integrated with an application processor and a modem processor, where the application processor is generally responsive of processing involved with the operating system, the applications, etc. and the modem processor is generally responsive of processing involved with the wireless communication. It can be understood that it is also possible that the above modem processor is not integrated in the processor 23.

[0068] The server further includes a power supply 24 (such as a battery) for supplying power to various components. Preferably, the power supply 24 can be logically connected to the processor 23 via a power supply managing system, so as to manage the functions such as charging, discharging and power consumption managing. The power supply 24 may further include one ore more DC or AC power supply, a recharging system, a power supply failure detecting circuit, power supply converter or inverter, power supply state indicator, and any other assembly.

[0069] Although it is not specified, the server may further include other modules, which will not be described in detail here. In this embodiment, after the attribute information of the file reported by a plurality of clients is received by the RF circuit 20 of the server, the processor 23 implements various functions by loading executable files corresponding to one or more processes of an application into the storage 21 and running the application stored in the storage 21 by the processor 23, where the functions include the following.

[0070] According to the attribute information of the file reported by the plurality of clients, the property indicator of the file is determined, for indicating the probability of the file being a malicious program. The attribute information of the file includes, but not limited to, at least one of path information of the file, loading information of the file, releasing information of the file, a black-white attribute of the file, context information of a program corresponding to the file and the like.

[0071] The RF circuit 20 is controlled to send the property indicator to the clients, wherein the clients determine according to the property indicator whether it is necessary to scan the file and perform the scanning, or a scanning strategy on whether it is necessary to scan the file is obtained according to the property indicator, and the RF circuit 20 is controlled to send the scanning strategy for the file to the clients for instructing the clients to scan in accordance with the scanning strategy.

[0072] Further, when determining the property indicator, if the attribute information of the file reported by the clients corresponds to one attribute, the

processor 23 can obtain, according to the attribute information of the file reported by the each one of the plurality of clients, whether the file is a malicious program; and determine the property indicator of the file by a ratio of the number of clients for which the file is determined as the malicious program to the total number of the plurality of clients. When determining the property indicator, if the attribute information of the file reported by the clients corresponds to multiple attributes, the processor 23 can obtain, for each one of the plurality of clients, according to the information corresponding to the multiple attributes reported by each client, whether the file is a malicious program with respect to each of the multiple attributes respectively; determining for each of the multiple attributes of the file, a probability ratio of the file being a malicious program with respect to the attribute by a ratio of the clients for which the file is determined as the malicious program to the total number of the plurality of clients; and determining the property indicator of the file by a sum of the respective probability ratios of the file being a malicious program with respect to the multiple attributes, or determining the property indicator of the file by a sum of weighted probability ratios of the file being a malicious program with respect to the multiple attributes, wherein the weighted probability ratios are products of the respective probability ratios multiplying with corresponding weights.

[0073] To obtain the scanning strategy on whether it is necessary to scan the file, it can be determined whether the property indicator is greater than a preset value. If the property indicator is greater than the preset value, it is necessary for the clients to scan the file. And if the property indicator is not greater than the preset value, it is unnecessary for the clients to scan the file.

[0074] To control the attribute information of the file reported by the client, the processor 23 can further control the RF circuit 20 to send instruction information to the plurality of clients, where the instruction information is indicative of the attribute information of the file to be reported by the clients.

[0075] It is further provided a client in an embodiment of the disclosure. The units of the client according to this embodiment can scan the file using the

method shown in Figure 3. Figure 8 shows a schematic structural diagram of the client, which includes an attribute reporting unit 31 and a file scanning unit 32.

[0076] The attribute reporting unit 31 is configured to report to a server the attribute information of the file gathered by the gathering unit 30.

[0077] The attribute information of the file here may include, but not limited to, at least one of path information of the file, loading information of the file, releasing information of the file, a black-white attribute of the file, context information of a program corresponding to the file and the like.

[0078] The client may determine, according to the preset attribute reporting strategy in the client, which attribute information of the file can be gathered, where the preset attribute reporting strategy can include the prescription of reporting which attribute information of the file in which case. The client can also determine, according to the instruction information sent from the server, which attribute information is to be gathered. In this case, the client further includes an instruction receiving unit (not shown in Figure 8) for receiving the instruction information sent from the server. The instruction information is indicative of the attribute information of the file to be reported by the clients.

[0079] The file scanning unit 32 is configured to receive from the server a scanning strategy on whether it is necessary to scan the file, where the scanning strategy is returned from the server according to the attribute information of the file reported by a plurality of clients via the attribute reporting unit 31. Alternatively, the file scanning unit 32 is configured to receive from the server a property indicator of the file, to obtain, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, wherein the property indicator is returned from the server according to the attribute information of the file reported by the plurality of clients via the attribute reporting unit 31.

[0080] Specifically, after the file scanning unit 32 receives the property indicator sent from the server, it can be determined whether the property indicator is greater than a preset value. If the property indicator is greater than the preset value, it is necessary for the client to scan the file. And if the property

indicator is not greater than the preset value, it is unnecessary for the client to scan the file. Thus, the scanning strategy for the file is obtained.

[0081] It can be seen that in the embodiment of the disclosure, during the file real-time protection, the client sends the attribute information of the file to the server, the server determines, by comprehensive consideration of the attribute information of the file reported by a plurality of clients, the property indicator of the file, i.e., the probability of the file being a malicious program; and the server sends the property indicator to the clients, wherein the clients determine, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, or the server directly determines, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and sends the scanning strategy to the clients. Then, the file scanning unit 32 in the clients scans the file in accordance with the scanning strategy, and only the file which has a higher probability to be a malicious program will be scanned. Therefore, the amount of the files to be scanned during the protection can be decreased, the spent time is shortened, and the influence on the other operations in the server is reduced.

[0082] The illustration is given by mainly taking the application of the file scanning method according to the embodiment of the disclosure as shown in Figure 3 in a terminal as an example. The terminal may include an intelligent telephone, a tablet, an electronic book reader, a Moving Picture Experts Group Audio Layer III (MP3) player, a Moving Picture Experts Group Audio Layer IV (MP4) player, a laptop portable computer, a desktop computer and the like.

[0083] Reference is made to Figure 9, which shows a schematic structural diagram of a terminal according to an embodiment of the disclosure.

[0084] Specifically, the terminal can include a Radio Frequency (RF) circuit 40, a storage 41 including one or more computer readable storage medium, an inputting unit 42, a displaying unit 43, a sensor 44, an audio circuit 45, a wireless fidelity (WiFi) module 46, a processor 47 including one or more processing cores, a power supply 48 and the like. It can be understood by those skilled in the art that the structure of the terminal shown in Figure 9 is not

intended to limit the terminal, more or less components than shown in Figure 9 may be included in the terminal, some components may be combined, or the components may be in another arrangement.

[0085] The RF circuit 40 can be configured to receive and send information, or receive and send signals during the phone call. Particularly, after receiving the downlink information from the base station, the RF circuit 40 sends the downlink information to one or more processors 47 for processing. Further, the RF circuit 40 sends the uplink data to the base station. Generally, the RF circuit 40 includes, but not limited to, an antenna, at least one amplifiers, a tuner, one or more oscillators, a Subscriber Identify Module (SIM) card, a transceiver, a coupler, a Low Noise Amplifier (LNA), a duplexer and the like. Further, the RF circuit 40 can communicate with a network or other devices via wireless communication. The wireless communication may be performed according to any communication standard or protocol, including but not limited to Global System of Mobile communication (GSM), General Packet Radio Service (GPRS), Code Division Multiple Access (CDMA), Wideband Code Division Multiple Access (WCDMA), Long Term Evolution (LTE), e-mail, Short Messaging Service (SMS), and the like.

[0086] The storage 41 can be configured to store software program(s) and module(s). By running the software program(s) and module(s) stored in the storage 41, the processor 47 performs various function applications and data processing. The storage 41 can generally include a program storage area and a data storage area. The program storage area can store an operation system, an application program necessary for at least one function (such as audio playing function, and image playing function), and the like. The data storage area can store the data (such as audio data and telephone dictionary) created according to the usage of the terminal, and the like. Further, the storage 41 may include a high-speed random access memory, a non-volatile memory such as at least one disk storage device, flash storage device, or other volatile solid-state storage device. Accordingly, the storage 41 may further include a storage controller for providing the processor 47 and the inputting unit 42 with the access to the storage 41.

[0087] The inputting unit 42 can be configured to receive the input number or character information, and generate keyboard, mouse, operating lever, optical or track ball signal input related to the user setting and the function control. Specifically, in an embodiment, the inputting unit 42 may include a touch-sensitive surface 421 and other inputting devices 422. The touch-sensitive surface 421, also referred to as a touch screen or touch panel, can capture the touch operation performed by the user nearby or on the touch-sensitive surface (such as the operation of the user on the touch-sensitive surface 421 or nearby the touch-sensitive surface 421 using a finger, a stylus or any suitable object or accessory), and drive a corresponding connecting device according to a preset program. Optionally, the touch-sensitive surface 421 may include two components, i.e., a touch detecting device and a touch controller. The touch detecting device detects the touch position of the user, detects a signal caused by the touch operation, and sends the signal to the touch controller. The touch controller receives the touch information from the touch detecting device, converts the touch information into coordinates of the touch position, sends the coordinates to the processor 47, and receives a command sent from the processor 47 and executes the command. Further, the touch-sensitive surface 421 can be implemented in various manners, such as resistive, capacitive, infrared and surface acoustic wave. In addition to the touch-sensitive surface 421, the inputting unit 42 may further include other inputting devices 422. Specifically, the other inputting devices 422 may include, but not limited to, one or more of a physical keyboard, a function key, (such as a volume controlling key and a switching key), a track ball, a mouse, an operating rod and the like.

[0088] The displaying unit 43 can be configured to display the information input from the user, the information provided to the user, and various graphic user interface of the terminal. The graphic user interface of the terminal can be composed of image, text, icon, video or any composition thereof. The displaying unit 43 may include a displaying panel 431. Optionally, the displaying panel 431 can be configured by a Liquid Crystal Display (LCD), an Organic Light-Emitting Diode (OLED) and the like. Further, the playing panel 431 can be covered by the touch-sensitive surface 421. Upon detecting the touch

operation on or nearby the touch-sensitive surface 421, the touch-sensitive surface 421 sends the touch information to the processor 47 for determining the type of the touch event. Then the processor 47 provides corresponding visual output on the displaying panel 431 according to the type of the touch event. Although in Figure 9 the touch-sensitive surface 421 and the displaying panel 431 perform the inputting function and the outputting function as two separate components, in some embodiments, the touch-sensitive surface 421 and the displaying panel 431 can be integrated to achieve the inputting function and the outputting function.

[0089] The terminal may also include at least one sensor 44, such as an optical sensor, a motion sensor and any other sensor. Specifically, the optical sensor may include an ambient light sensor and a proximity sensor. The ambient light sensor can adjust the brightness of the displaying panel 431 according to the intensity of ambient lights. The proximity sensor can turn off the displaying panel 431 and/or the backlight when the terminal moves nearby the ear. As one kind of the motion sensor, a gravity acceleration sensor can detect the values of the accelerations in various directions (generally three axes) and detect the value and direction of the gravity when remaining stationary. The gravity acceleration sensor may be applied in an application for recognizing posture of a mobile phone (for example, switching between landscape and portrait, relevant games, magnetometer pose calibration), a function related to vibration recognition (for example, a pedometer, knocking), etc.; in addition, other sensors, e.g., a gyroscope, a barometer, a hygrometer, a thermometer, an infrared sensor, etc. may be further provided in the terminal, the description of which is omitted herein.

[0090] The audio circuit 45, the speaker 451 and the microphone 452 can provide the audio interface between the user and the terminal. The audio circuit 45 can send the electrical signal converted from the received audio data to the speaker 451 and a voice signal is converted from the electric signal and is output by the speaker 451. In another aspect, the microphone 452 converts the collected sound signal into an electrical signal, the audio circuit 45 receives the electrical signal and converts the electrical signal into audio data to be output to the

processor 47 for processing. The processed audio data is sent to for example another terminal via the RF circuit 40. Alternatively, the audio data is output to the storage 41 for further processing. The audio circuit 45 may further include an earplug jack for providing the communication between an external earphone and the terminal.

[0091] WiFi is a technology for short-distance wireless transmission. Via the WiFi module 46, the terminal can help the user to receive and send an e-mail, brows a web page, access a stream media, provide the user with wireless wideband Internet access. Although the WiFi module 46 is shown in Figure 9, it can be understood that the WiFi module 46 is not an indispensable component of the terminal, and can be omitted as required without deviating from the scope of the spirit of the disclosure.

[0092] The processor 47, as a control center of the terminal, is connected various portions of the whole mobile phone via various interfaces and wires. By running or performing the software program(s) and/or module(s) stored in the storage 41 and revoking the data stored in the storage 41, the processor 47 performs various functions of the terminal and processes data, so as to monitor the whole mobile phone. Optionally, the processor 47 may include one or more processing core. Preferably, the processor 47 can be integrated with an application processor and a modem processor, where the application processor is mainly responsive of processing involved with the operating system, the user interface, the applications, etc. and the modem processor is mainly responsive of processing involved with the wireless communication. It can be understood that it is also possible that the above modem processor is not integrated in the processor 47.

[0093] The terminal further includes a power supply 48 (such as a battery) for supplying power to various components. Preferably, the power supply 48 can be logically connected to the processor 47 via a power supply managing system, so as to manage the functions such as charging, discharging and power consumption managing. The power supply 48 may further include one ore more DC or AC power supply, a recharging system, a power supply failure detecting

circuit, power supply converter or inverter, power supply state indicator, and any other assembly.

[0094] Although it is not specified, the terminal may further include a camera, a Bluetooth module and the like, for which the description is omitted. In this embodiment, the processor 47 in the terminal implements various functions by loading executable files corresponding to one or more processes of an application into the storage 41 and running the application stored in the storage 41 by the processor 47. The functions include the following.

[0095] The attribute information of the file can be gathered, for example according to the instruction information sent from the server and received by the RF circuit 40. The instruction information is indicative of the attribute information of the file to be reported by the client. The gathered attribute information of the file includes, but not limited to, at least one of path information of the file, loading information of the file, releasing information of the file, a black-white attribute of the file, context information of a program corresponding to the file and the like.

[0096] The RF circuit 40 is controlled to report the attribute information of the file to the server.

[0097] Upon receiving from the server the scanning strategy on whether it is necessary to scan the file, the RF circuit 40 scans the file in accordance with the scanning strategy, where the scanning strategy is returned from the server according to the attribute information of the file sent from the plurality of clients. Alternatively, upon receiving from the server the property indicator of the file, the RF circuit 40 obtains, according to the property indicator, the scanning strategy on whether it is necessary to scan the file and scans the file in accordance with the scanning strategy, where the property indicator is returned by the server according to the attribute information of the file reported by the plurality of clients.

[0098] To obtain, according to the property indicator, the scanning strategy on whether it is necessary to scan the file, the processor 47 can determine whether the property indicator is greater than a preset value. If the property indicator is

greater than the preset value, it is necessary for the client to scan the file. And if the property indicator is not greater than the preset value, it is unnecessary for the client to scan the file.

[0099] It is further provided a file scanning system in an embodiment of the disclosure, which includes the server as shown in Figure 5 or 6 and a plurality of clients as shown in Figure 8, and is not described in detail here.

[00100] It is further provided a file scanning system in an embodiment of the disclosure, which includes the server as shown in Figure 7 and a plurality of clients as shown in Figure 9, and is not described in detail here.

[00101] It should be understood by those skilled in the art that all or some of the steps in the methods according to the embodiments of the disclosure may be performed by a corresponding hardware instructed with a program. The program may be stored in a computer readable storage medium. The computer readable storage medium may include Read Only Memory (ROM), Random Access Memory (RAM), magnetic disk, Compact Disk, etc.

[00102] The file scanning method and file scanning method system, the client and the server according to the embodiments of the disclosure have been described in detail above. The principle and implementation of the disclosure are illustrated with specific examples, which are set forth only for the purpose of better understanding of the method and core concept of the disclosure; changes to the specific embodiments and the application scope may be made by those skilled in the art based on the spirit of the disclosure, and the specification is not intended to limit the disclosure.

WHAT IS CLAIMED IS:

1. A file scanning method, comprising:

determining a property indicator of a file according to attribute information of the file reported by a plurality of clients, wherein the property indicator is indicative of probability of the file being a malicious program; and

sending the property indicator to the clients, wherein the clients determine, according to the property indicator, whether it is necessary to scan the file; or obtaining, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and sending the scanning strategy for the file to the clients.

2. The method according to claim 1, wherein the attribute information comprises at least one of path information of the file, loading information of the file, releasing information of the file, a black-white attribute of the file and context information of a program corresponding to the file.

3. The method according to claim 1 or 2, wherein if the attribute information of the file reported by the clients corresponds to one attribute, the determining a property indicator of the file according to the attribute information of the file reported by the plurality of clients comprises:

determining for each one of the plurality of clients, according to the attribute information of the file reported by each one of the plurality of clients, whether the file is a malicious program; and

determining the property indicator of the file by a ratio of the number of clients for which the file is determined as the malicious program to the total number of the plurality of clients.

4. The method according to claim 1 or 2, wherein if the attribute information of

the file reported by the clients corresponds to multiple attributes, the determining a property indicator of the file according to the attribute information of the file reported by the plurality of clients comprises:

determining for each one of the plurality of clients, according to the attribute information corresponding to the multiple attributes reported by each client, whether the file is a malicious program with respect to each of the multiple attributes;

determining, for each of the multiple attributes of the file, a probability ratio of the file being a malicious program with respect to the attribute by a ratio of the clients for which the file is determined as the malicious program with respect to the attribute to the total number of the plurality of clients; and

determining the property indicator of the file by a sum of the respective probability ratios of the file being a malicious program with respect to the multiple attributes, or determining the property indicator of the file by a sum of weighted probability ratios of the file being a malicious program with respect to the multiple attributes, wherein the weighted probability ratios are products of the respective probability ratios multiplying with corresponding weights.

5. The method according to claim 1 or 2, wherein the obtaining, according to the property indicator, a scanning strategy on whether it is necessary to scan the file comprises:

judging whether the property indicator is greater than a preset value, determining that it is necessary for the clients to scan the file if the property indicator is greater than the preset value; determining that it is unnecessary for the clients to scan the file if the property indicator is not greater than the preset value.

6. The method according to claim 1 or 2, further comprising,

sending instruction information to the plurality of clients, wherein the instruction information is indicative of the attribute information of the file to be

reported by the clients.

7. A file scanning method, comprising:

reporting attribute information of a file to a server; and

receiving from the server a scanning strategy on whether it is necessary to scan the file, wherein the scanning strategy is returned by the server according to the attribute information of the file reported by a plurality of clients; or receiving from the server a property indicator of the file, obtaining, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, wherein the property indicator is returned by the server according to the attribute information of the file reported by the plurality of clients.

8. The method according to claim 7, wherein the attribute information comprises at least one of path information of the file, loading information of the file, releasing information of the file, a black-white attribute of the file and context information of a program corresponding to the file.

9. The method according to claim 7 or 8, wherein the obtaining, according to the property indicator, a scanning strategy on whether it is necessary to scan the file comprises:

judging whether the property indicator is greater than a preset value, determining that it is necessary for the clients to scan the file if the property indicator is greater than the preset value; determining that it is unnecessary for the clients to scan the file if the property indicator is not greater than the preset value.

10. The method according to claim 7 or 8, further comprising:

receiving instruction information sent from the server, wherein the instruction information is indicative of the attribute information of the file to be

reported by the clients.

11. A server, comprising:

a property indicator determining unit, configured to determine a property indicator of a file according to attribute information of the file reported by a plurality of clients, wherein the property indicator is indicative of probability of the file being a malicious program; and

a sending unit, configured to send the property indicator to the clients, wherein the clients determine, according to the property indicator, whether it is necessary to scan the file; or to obtain, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and to send the scanning strategy for the file to the clients.

12. The server according to claim 11, wherein the property indicator determining unit comprises:

a malicious program determining unit, configured to, if the attribute information of the file reported by the clients corresponds to one attribute, determine for each one of the plurality of clients, according to the attribute information of the file reported by each one of the plurality of clients, whether the file is a malicious program; and

a calculating unit, configured to determine the property indicator of the file by a ratio of the number of clients for which the file is determined as the malicious program to the total number of the plurality of clients.

13. The server according to claim 12, wherein

the malicious program determining unit is further configured to, if the attribute information of the file reported by the clients corresponds to multiple attributes, determine, for each one of the plurality of clients, according to the information corresponding to the multiple attributes reported by each client,

whether the file is a malicious program with respect to each of the multiple attributes respectively; and

the calculating unit is further configured to determine, for each of the multiple attributes of the file, a probability ratio of the file being a malicious program with respect to the attribute by a ratio of the clients for which the file is determined as the malicious program with respect to the attribute to the total number of the plurality of clients; and to determine the property indicator of the file by a sum of the respective probability ratios of the file being a malicious program with respect to the multiple attributes, or to determine the property indicator of the file by a sum of weighted probability ratios of the file being a malicious program with respect to the multiple attributes, wherein the weighted probability ratios are products of the respective probability ratios multiplying with corresponding weights.

14. The server according to any one of claims 11 to 13, wherein the sending unit is configured to judge whether the property indicator is greater than a preset value, determine that it is necessary for the clients to scan the file if the property indicator is greater than the preset value; determine that it is unnecessary for the clients to scan the file if the property indicator is not greater than the preset value.

15. The server according to any one of claims 11 to 13, further comprising:

an instruction sending unit, configured to send instruction information to the plurality of clients, wherein the instruction information is indicative of the attribute information of the file to be reported by the clients.

16. A client device, comprising:

an attribute reporting unit, configured to report attribute information of a file to a server; and

a file scanning unit, configured to receive from the server a scanning strategy on whether it is necessary to scan the file, wherein the scanning strategy is returned by the server according to the attribute information of the file reported by a plurality of clients; or configured to receive from the server a property indicator of the file, to obtain, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, wherein the property indicator is returned by the server according to the attribute information of the file reported by the plurality of clients.

17. The client device according to claim 16, wherein the attribute information gathered by the gathering unit comprises at least one of path information of the file, loading information of the file, releasing information of the file, a black-white attribute of the file and context information of a program corresponding to the file.

18. The client device according to claim 16 or 17, wherein the file scanning unit is further configured to judge whether the property indicator is greater than a preset value, determine that it is necessary for the clients to scan the file if the property indicator is greater than the preset value; determine that it is unnecessary for the clients to scan the file if the property indicator is not greater than the preset value.

19. The client device according to claim 16 or 17, further comprising:

an instruction receiving unit, configured to receive instruction information sent from the server, wherein the instruction information is indicative of the attribute information of the file to be reported by the clients.

20. A file scanning system, comprising a plurality of clients according to any one of claims 16 to 19 and a server according to any one of claims 11 to 15.

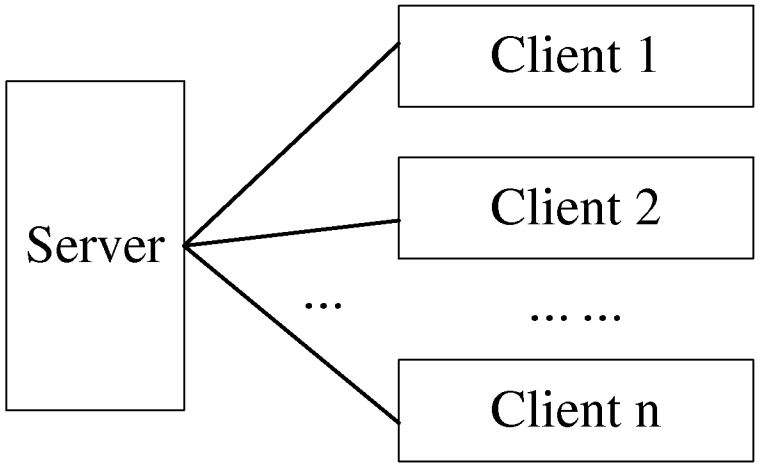
Client 1
Server
Client 2
...
... ...
Client n

Fig. 1

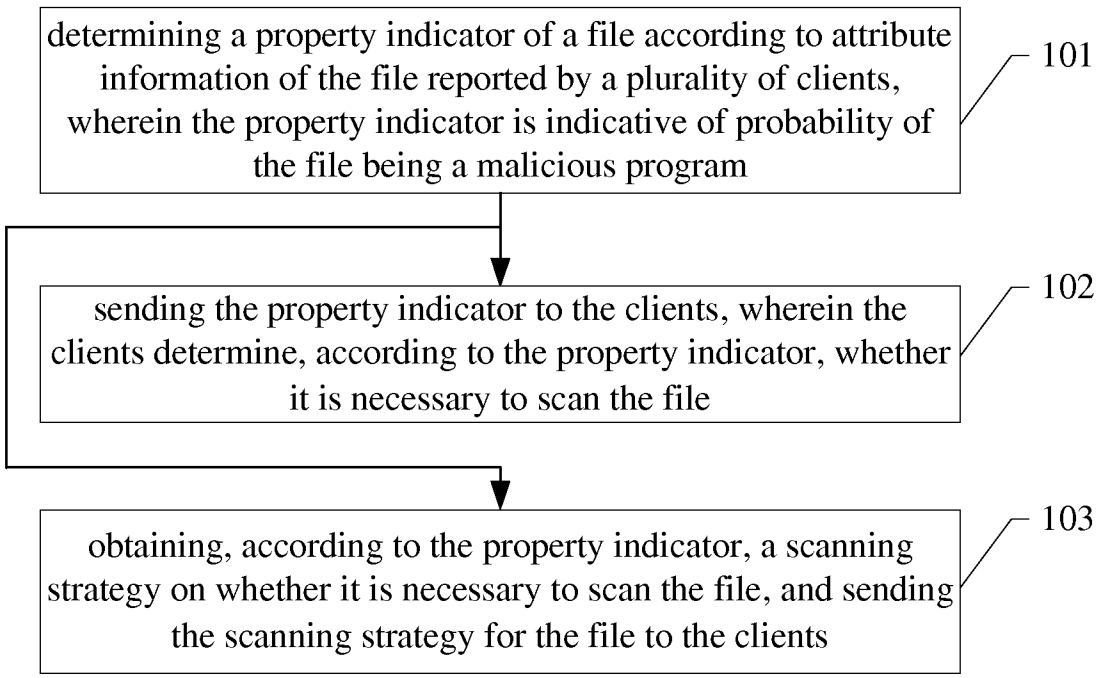
determining a property indicator of a file according to attribute information of the file reported by a plurality of clients, wherein the property indicator is indicative of probability of the file being a malicious program
101
sending the property indicator to the clients, wherein the clients determine, according to the property indicator, whether it is necessary to scan the file
102
obtaining, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and sending the scanning strategy for the file to the clients
103

Fig. 2

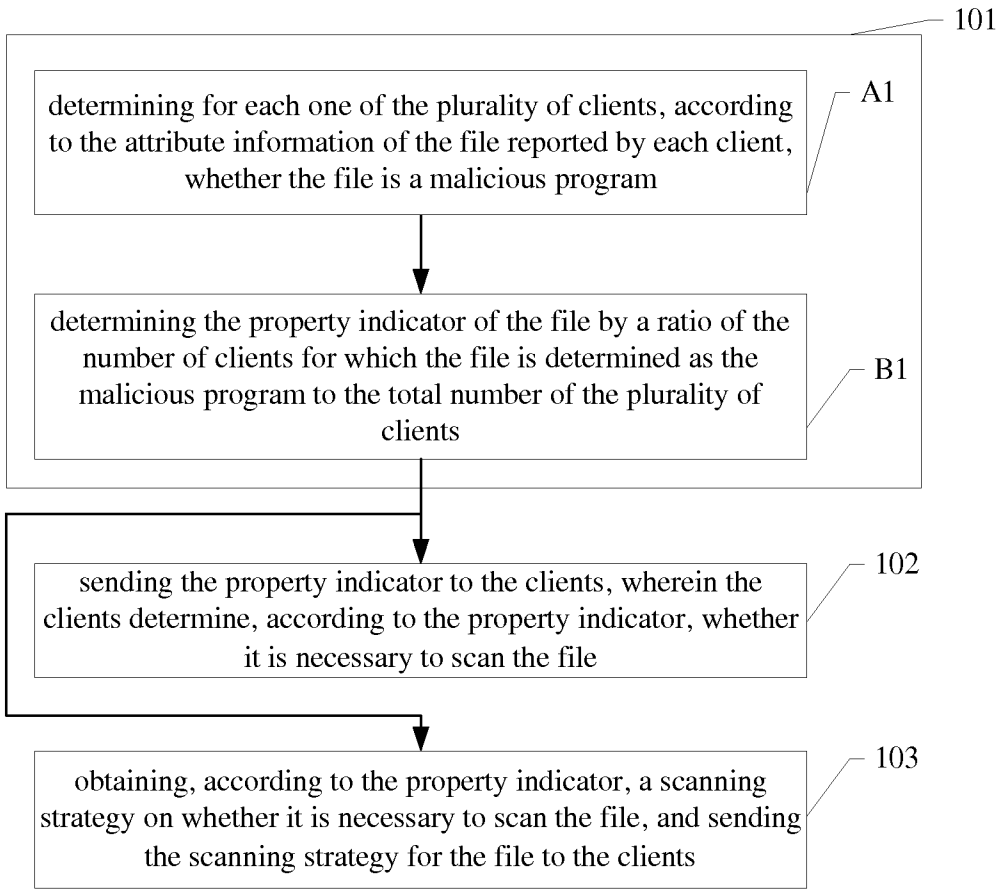
101
determining for each one of the plurality of clients, according to the attribute information of the file reported by each client, whether the file is a malicious program
A1
determining the property indicator of the file by a ratio of the number of clients for which the file is determined as the malicious program to the total number of the plurality of clients
B1
sending the property indicator to the clients, wherein the clients determine, according to the property indicator, whether it is necessary to scan the file
102
obtaining, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, and sending the scanning strategy for the file to the clients
103

Fig. 3a

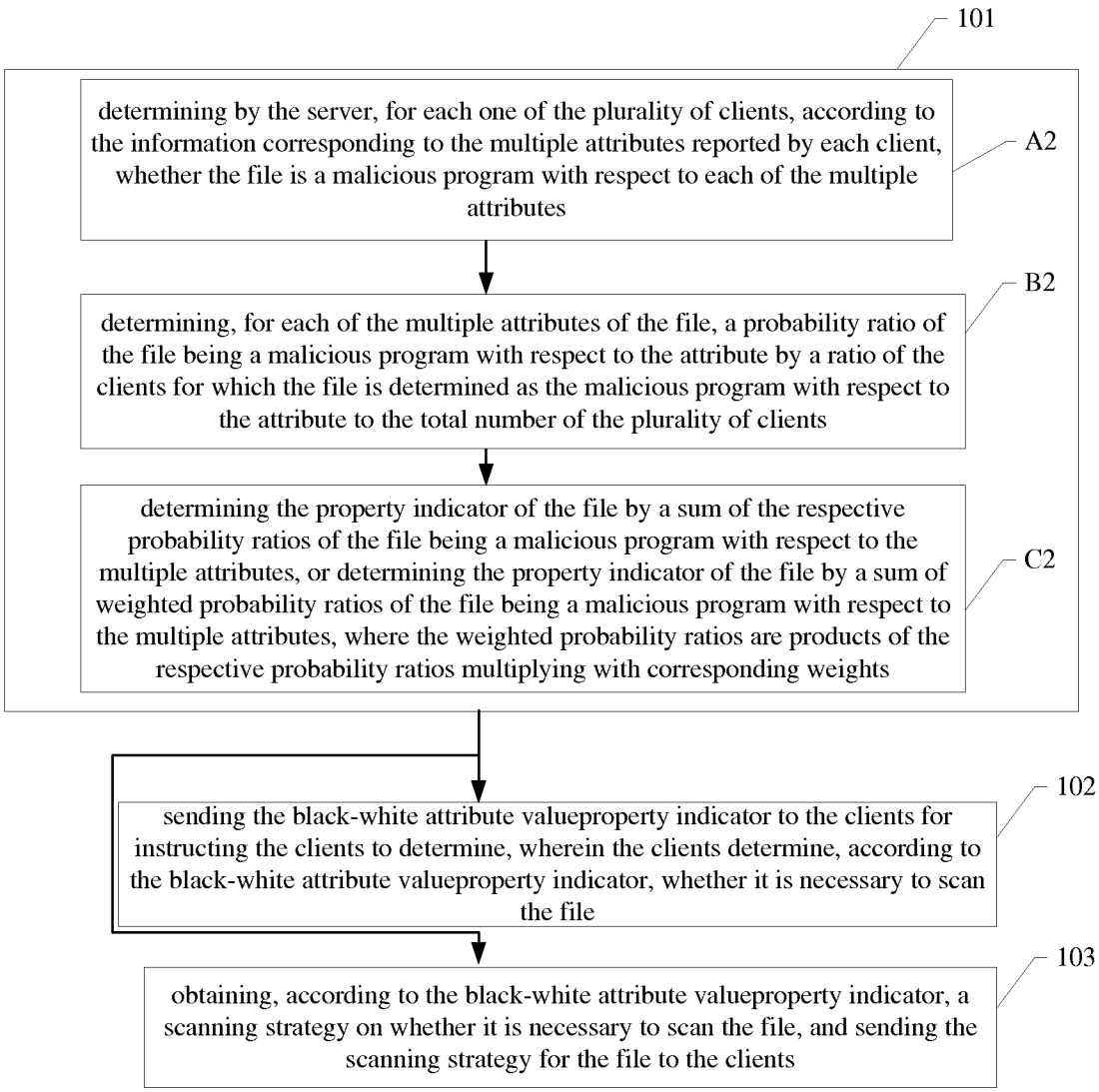
101
determining by the server, for each one of the plurality of clients, according to the information corresponding to the multiple attributes reported by each client, whether the file is a malicious program with respect to each of the multiple attributes
A2
determining, for each of the multiple attributes of the file, a probability ratio of the file being a malicious program with respect to the attribute by a ratio of the clients for which the file is determined as the malicious program with respect to the attribute to the total number of the plurality of clients
B2
determining the property indicator of the file by a sum of the respective probability ratios of the file being a malicious program with respect to the multiple attributes, or determining the property indicator of the file by a sum of weighted probability ratios of the file being a malicious program with respect to the multiple attributes, where the weighted probability ratios are products of the respective probability ratios multiplying with corresponding weights
C2
102
sending the black-white attribute valueproperty indicator to the clients for instructing the clients to determine, wherein the clients determine, according to the black-white attribute valueproperty indicator, whether it is necessary to scan the file
103
obtaining, according to the black-white attribute valueproperty indicator, a scanning strategy on whether it is necessary to scan the file, and sending the scanning strategy for the file to the clients

Fig. 3b

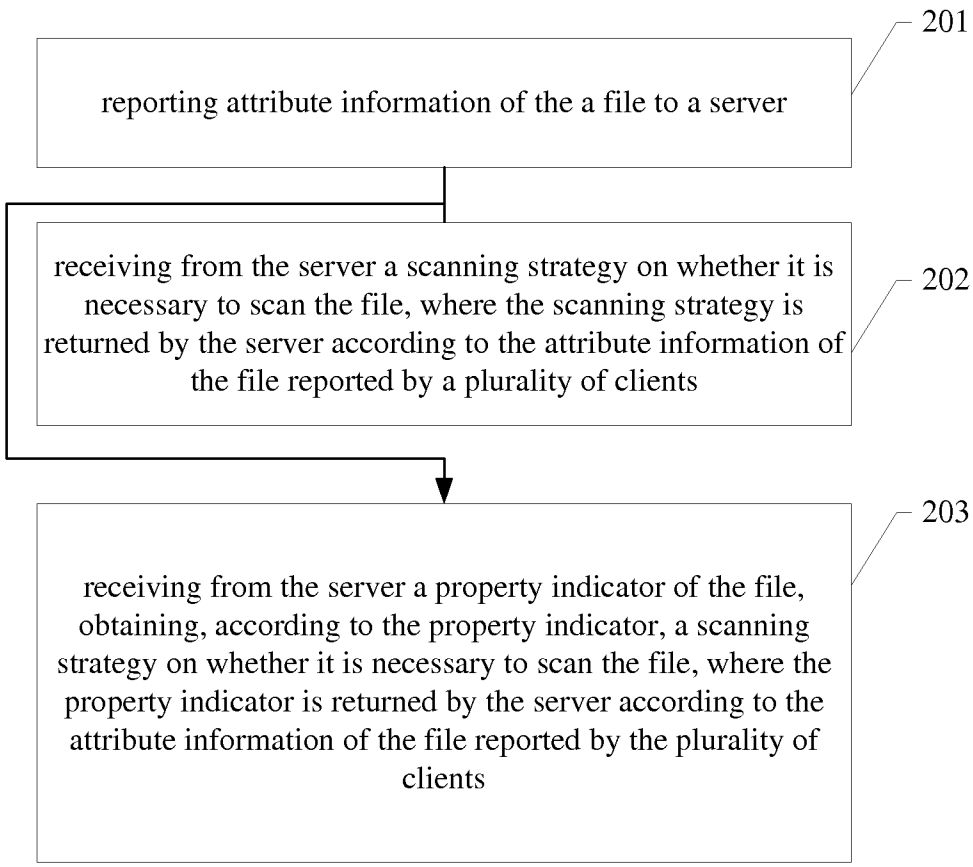
201
reporting attribute information of the a file to a server
receiving from the server a scanning strategy on whether it is necessary to scan the file, where the scanning strategy is returned by the server according to the attribute information of the file reported by a plurality of clients
202
203
receiving from the server a property indicator of the file, obtaining, according to the property indicator, a scanning strategy on whether it is necessary to scan the file, where the property indicator is returned by the server according to the attribute information of the file reported by the plurality of clients

Fig. 4

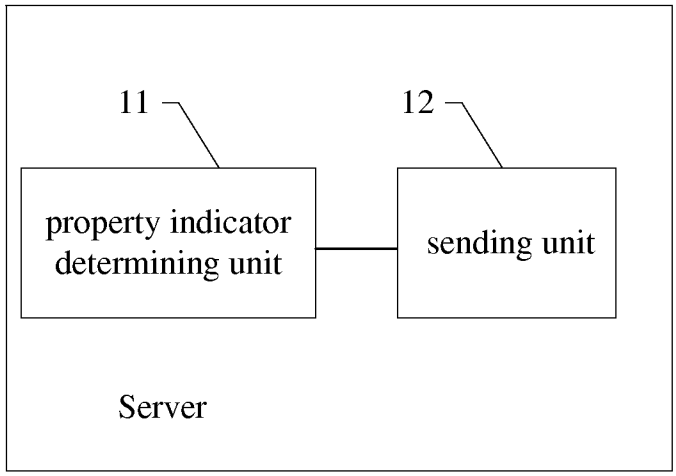
11
12
property indicator determining unit
sending unit
Server

Fig. 5

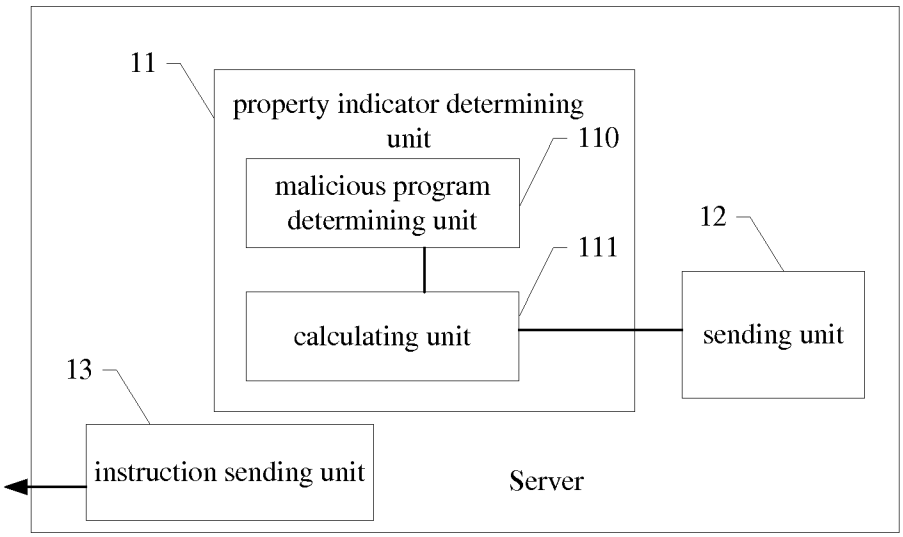
11
property indicator determining unit
110
malicious program determining unit
111
calculating unit
12
sending unit
13
instruction sending unit
Server

Fig. 6

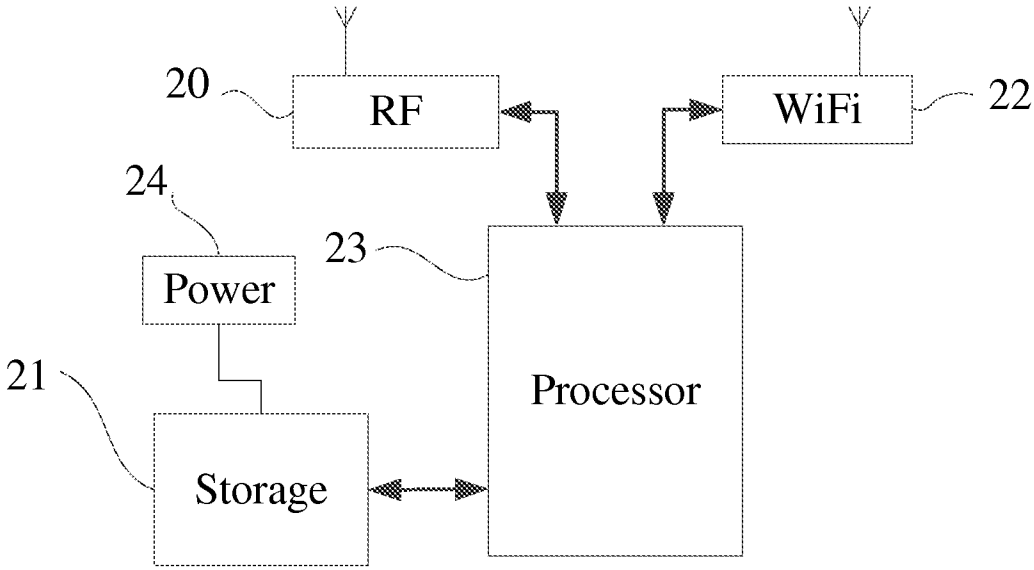
20
RF
WiFi
22
24
Power
23
Processor
21
Storage

Fig. 7

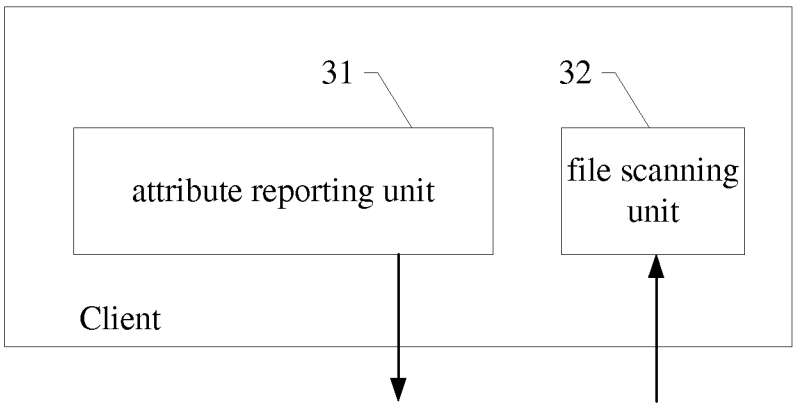
31
32
attribute reporting unit
file scanning unit
Client

Fig. 8

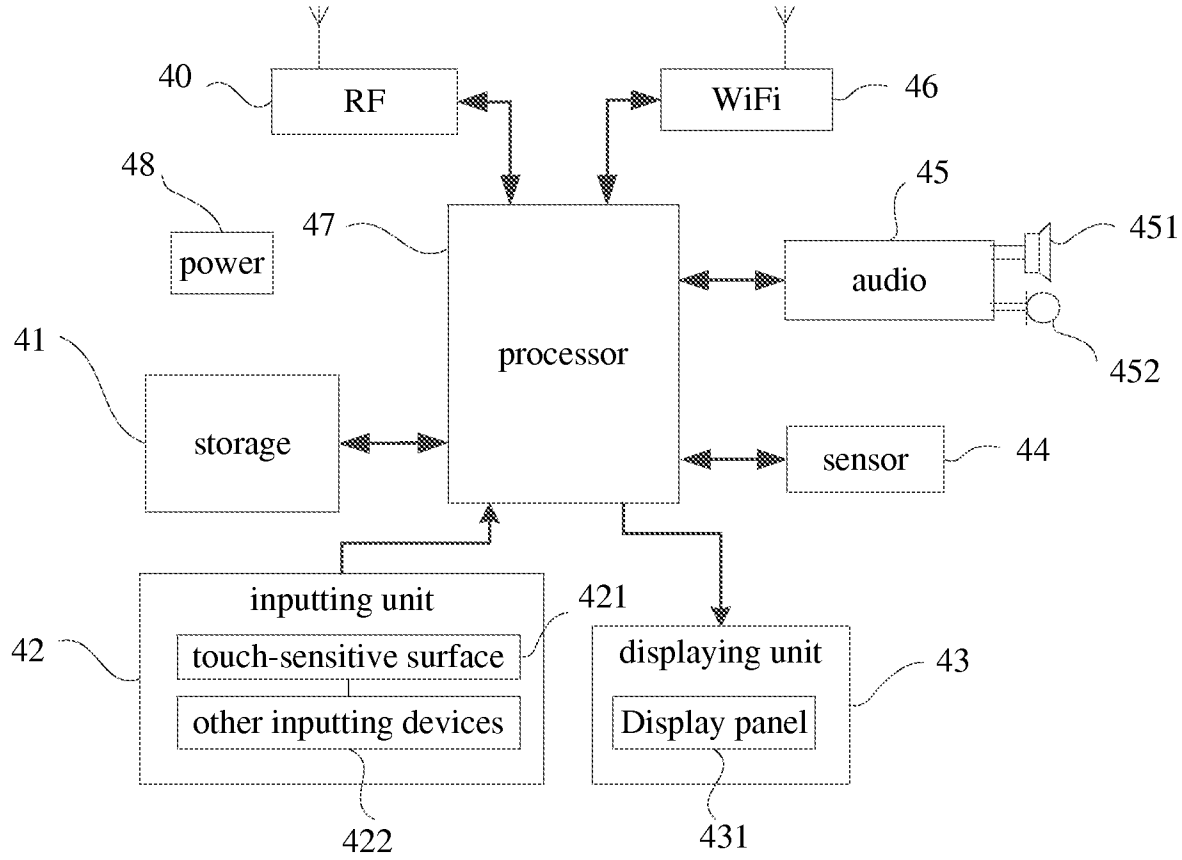
40
RF
WiFi
46
48
power
47
processor
45
audio
451
452
41
storage
sensor
44
inputting unit
421
42
touch-sensitive surface
other inputting devices
displaying unit
43
Display panel
422
431

Fig. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/088489

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56 (2013.01) 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)

CNPAT,CNKI,WPI,EPODOC scan, malicious, virus, property, attribute, black, white, probability, client, server, strategy, ratio

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN102799804A (ZHUHAI JUNTIAN ELECTRONIC TECHNOLOGY CO., LTD.) 28 Nov. 2012(28.11.2012) see description, paragraphs 0007-0040	1-20
Y	CN102799823A (BEIJING JIANGMIN NEW SCIENCE & TECHNOLOGY CO., LTD.) 28 Nov. 2012(28.11.2012) see description, paragraphs 0033-0070	1-20
A	US2010/0257609A1 (F-SECURE CORPORATION) 07 Oct. 2010(07.10.2010) the whole document	1-20
PX	CN103177217A (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) 26 Jun. 2013(26.06.2013) the whole document	1-20

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 Jan. 2014(28.01.2014)	**13 Mar. 2014 (13.03.2014)**
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 ZHAO, Xiaochun Telephone No. (86-10)62413113

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/088489

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN102799804A	28.11.2012	None	
CN102799823A	28.11.2012	None	
US2010/0257609A1	07.10.2010	GB2469117A	06.10.2010
CN103177217A	26.06.2013	None	