



- (51) International Patent Classification:
H04L 12/58 (2006.01)
- (21) International Application Number:
PCT/US2013/037086
- (22) International Filing Date:
18 April 2013 (18.04.2013)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
61/625,984 18 April 2012 (18.04.2012) US
13/829,708 14 March 2013 (14.03.2013) US
- (71) Applicant: LIVEPERSON, INC. [US/US]; 475 10th Avenue, Fifth Floor, New York, New York 10018 (US).
- (72) Inventors: BARAK, Matan; 475 10th Avenue, Fifth Floor, New York, New York 10018 (US). LEWIS, Todd; 475 10th Avenue, Fifth Floor, New York, New York 10018 (US). MULHEARN, Justin, Robert; 475 10th Avenue, Fifth Floor, New York, New York 10018 (US).

- (74) Agents: LEZAK, Arrienne, Monique et al.; Kilpatrick Townsend & Stockton LLP, Two Embarcadero Center, Eighth Floor, San Francisco, California 94111 (US).
- (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, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: AUTHENTICATION OF SERVICE REQUESTS

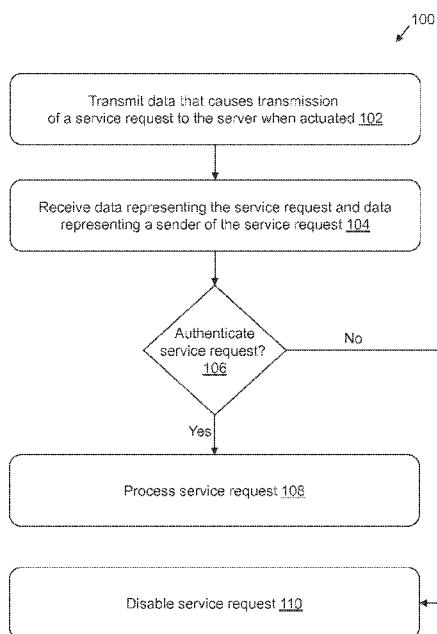


FIG. 1

(57) Abstract: Described are computer-based methods and apparatuses, including computer program products, for authentication of service requests. Data is transmitted that causes transmission of a service request to the server when actuated. Data representing the service request and data representing a sender of the service request is received. The (a) data representing the service request, data representing the sender of the service request, or both, is compared against (b) pre-defined criteria associated with the data that causes transmission of the service request. The service request from the sender is processed if the comparison authenticates the service request.



Published:

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

AUTHENTICATION OF SERVICE REQUESTS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Application No. 61/625,984, filed April 18, 2012, and entitled "Authentication of Service Requests," and to U.S. Non-Provisional Application No. 13/829,708, filed March 14, 2013, and entitled "Authentication of Service Requests," which is incorporated herein by reference in its entirety for all purposes.

[0002] This application relates to and is assigned to the same entity as the co-pending U.S. Patent Application No. 12/967,782, filed on December 14, 2010, entitled "Authentication of Service Requests Initiated From a Social Networking Site," the disclosure of which is hereby incorporated herein by reference in its entirety, and attached hereto as Appendix A. The systems and methods described herein can be used in combination with the systems and methods described in Appendix A. For example, the authentication techniques described in Appendix A can be used to authenticate users that invoke service requests, as described herein.

TECHNICAL FIELD

[0003] The technical field relates generally to computer-based methods and apparatuses, including computer program products, for authentication of service requests.

SUMMARY OF THE INVENTION

[0004] A brief summary of various exemplary embodiments is presented. Some simplifications and omissions may be made in the following summary, which is intended to highlight and introduce some aspects of the various exemplary embodiments, but not limit the scope of the invention. Detailed descriptions of a preferred exemplary embodiment adequate to allow those of ordinary skill in the art to make and use the inventive concepts will follow in the later sections.

[0005] In one aspect, a computerized method for authenticating user service requests is presented. A server transmits data that causes transmission of a service request to the server when actuated. The server receives data representing the service request and data representing a sender of the service request. The server compares (a) the data representing the service request, the data representing the sender of the service request, or both, against (b) pre-defined criteria associated with the data that causes transmission of the service request. The server processes the service request from the sender if the comparison authenticates the service request.

[0006] In other examples, any of the aspects above can include one or more of the following features. The data that causes transmission of a service request to the server when actuated comprises an HTTP link.

[0007] The techniques, which include both methods and apparatuses, described herein can provide one or more of the following advantages. Website links, such as HTTP links, can be authenticated based on the user that invoked the link, as well as pre-defined criteria for the link, such as an expiration time, a number of users that can invoke the link, and/or the like. Data received about service requests and/or the users that invoke the service requests can be used to appropriately tailor the service request for each user.

[0008] Other aspects and advantages of the present invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, illustrating the principles of the invention by way of example only.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The foregoing and other aspects, features, and advantages of the present invention, as well as the invention itself, will be more fully understood from the following description of various embodiments, when read together with the accompanying drawings.

[0010] FIG. 1 is a flow chart showing an exemplary method for processing a service request.

DETAILED DESCRIPTION

[0011] In general, computerized systems and methods are provided for creating links (e.g., web page links, such as HTML links) that can be authenticated by a server. Data

about the links and/or the user(s) that invoke the links can be used to authenticate the link based on pre-defined criteria stored for the link. The service request links can be configured based on the pre-defined criteria. For example, the service request links can expire based on the pre-defined criteria such that the links can be invoked only for a predetermined period of time, can only be invoked by a predetermined number of users, can only be invoked by particular users (e.g., based on profile data of the user), etc. This data can be used to navigate the invoking user to the proper location (e.g., to a service request (such as chat or video), or to a particular web page).

[0012] FIG. 1 is a flow chart showing an exemplary method 100 for processing a service request. At step 102, the server transmits data that causes transmission of a service request to the server when actuated. At step 104, the server receives data representing the service request and data representing a sender of the service request. At step 106, the server authenticates the service request. If the server authenticates the service request at step 106, the method proceeds to step 108, and the server processes the service request. If the server does not authenticate the service request at step 106, the method proceeds to step 110, and the server disables the service request.

[0013] Referring to step 102, the data that causes transmission of a service request to the server when actuated can be, for example, an HTTP link. For example, the link, when actuated (and authenticated as described with respect to step 106 below) can initiate any type of a service request, such as online text chat, audio chat, presentation of a support page (e.g., frequently asked questions), presentation of a coupon, video chat, and/or other types of service requests. The server can send service requests to a remote user for help with navigating a web page, to a remote user in response to a social media message (e.g., in response to a Twitter tweet or a Facebook post), to a remote user by email, a data messaging service (e.g., short messaging service (SMS)), etc. As is described further below, administrators of the server (and related components) can set pre-defined criteria for the service request (e.g., for an HTML link) that configure when the service request can be invoked (e.g., a time expiration).

[0014] Referring to step 104, the data representing the service request can include, for example, data about the service request (e.g., about an HTML link), and/or data about the user that invoked the service request (e.g., about the user that clicked the HTML link). For example, if the server transmits an HTML link to a web page, the data representing the service request can include identifying data for the service request

(e.g., so the system can identify which service request was invoked), a number of times the HTML link was invoked prior to the current invocation (e.g., a number of times the link was clicked), an amount of time the HTML link has been on the web page, and/or other data about the service request.

[0015] Referring further to step 104, the data representing a sender of the service request can include data about the party that invoked the service request. For example, this data may include social networking information, as described in Appendix A (e.g., a user profile for the user from the social networking site).

[0016] Referring to step 106, the server authenticates the service request. For example, unless certain properties of the service request are satisfied (e.g., a time limit has not expired, a pre-set number of users have not already invoked the service request, the invoking user matches pre-defined criteria (e.g., the service request was sent to the user, the user is a follower of a social networking site, located in a particular geographic location, and/or the link)), then the server will not authenticate the service request.

[0017] Referring further to step 106, the server can compare the data received at step 104 with stored data for the service request. For example, in some embodiments the server compares (a) the data representing the service request, the data representing the sender of the service request, or both, against (b) pre-defined criteria associated with the data the server transmitted in step 102. For example, the pre-defined criteria can be defined by the system administrator. For example, for an HTTP link, the administrator can set a number of times the link can be clicked before the link expires (e.g., can no longer be clicked by a user to invoke the service request), an amount of time the link is active until the link expires, required social networking profile information (e.g., indicative of the originator, such as geographical location and/or other user profile information), etc.

[0018] Referring further to step 106, if the server authenticates the service request such that the pre-defined criteria are satisfied (e.g., if the time limit associated with the service request has not expired, if the maximum number of users has not invoked the service request, if the social networking data associated with the user that invoked the request matches the pre-defined criteria, etc.), the server processes the service request at step 108. The server can process the service request by setting up the service request, such as by transmitting a coupon to the sender, setting up an online chat with the

sender, setting up a video chat with the sender, sending the user to a help page, and/or setting up any other type of service request.

[0019] If the server determines the service request is not authenticated (e.g., if the time limit associated with the service request expired, if the maximum number of users already invoked the service request, if the social networking data associated with the user that invoked the request does not match the pre-defined criteria, etc.), then the server disables the service request at step 110. For example, the server may transmit back to the sender an HTTP error page, a blank page, a page that indicates the link expired and therefore will not be completed, etc.

[0020] The authentication allows administrators and agents of the server to create and/or reconnect service requests (e.g., click-to-chat links) that can be limited to a number of users, time expirations, social networking attributes of the sender, etc. For example, if an agent is communicating with a user via online chat and the conversation is dropped, the server can create a link that allows the visitor to return back to the agent he was chatting with, but will only work based on pre-defined criteria associated with the link (e.g., a set number of clicks, time expiration, etc.). The link itself can be sent to the visitor as a regular HTTP link, as SMS, email, or via the original chat itself.

[0021] As an example, assume an agent is engaged in a service request with a user (e.g., online chat), and the agent needs to re-boot their computer. The agent can send the user a link so agent can be re-connected with the user after the reboot to resume their conversation. Advantageously, while the server can transmit a link that allows the user to re-engage the service request, the system can use pre-defined criteria to ensure only the same user can re-engage the service request (e.g., based on social networking data), and that the agent is still connected to the system (e.g., limit the link's active time to one hour).

[0022] As another example, assume an agent is busy but wants to talk (e.g., online chat, video chat, voice chat) with a user, and the agent determines the best time for a chat is between 4-5 PM EST. The agent (via the server) can send the user a link that is valid only from 4-5 PM (e.g., if the user clicks the link between 4-5 PM, the server will process the service request, otherwise the server will not process the service request). For example, if the user clicks the link outside of the 4-5 PM window, then the server can redirect the user to a landing page.

[0023] As another example, the server can use the links to initiate a call sequence. For example, the agent may be available for a call before 5 PM that day. The server can send the user a link that is valid only until 5 PM (e.g., if the user clicks the link any time before 5 PM that day, the server will process the service request, otherwise the server will not process the service request). If properly invoked, the server will initiate a call sequence between the user and the agent.

[0024] As another example, the server can use the links for an advertisement campaign (e.g., for marketing content). The server can send links such that the first users that click the link (e.g., the first 100 users) get a special discount (e.g., are presented with a coupon). As another example, the link can be used to keep track of a number of times people scan a bar code to keep track of how many users scan the code. The user can then be presented with a coupon related to the bar code, establish a service request (e.g., chat), and/or the like.

[0025] As another example, the validation can validate the sender that invokes the service request (e.g., to verify the sender). For example, social networking parameters (e.g., a profile page) can be used to verify the sender (e.g., if the request is transmitted from a social networking site). For example, a company may monitor tweets posted to Twitter. The company may see a tweet that states "I don't like the services of Company." The Company can use the server (e.g., manually or automatically) to send a link to the author of the tweet to invoke a service request. For example, the link can be used to invoke a chat with a Company representative (via online chat, video chat, etc.) to discuss their dislikes of the Company, to send the user to a support page to help explain the Company's services, etc. The link, once clicked, can navigate the user to any type of service request channel (such as chat, video, a support page, etc.) based on the time the link exists, the number of clicks, and/or the social parameters of the user (e.g., who the user is, and what the user's location is, etc.). As an example, the social parameters can be used to navigate visitors from Europe to a European chat page, visitors from the US to a US chat page, etc. The social networking parameters can be used to tailor how the service request channels are invoked for each particular user.

[0026] The above-described techniques can be implemented in digital and/or analog electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. The implementation can be as a computer program product, i.e., a computer program tangibly embodied in a machine-readable storage device, for execution by, or

to control the operation of, a data processing apparatus, e.g., a programmable processor, a computer, and/or multiple computers. A computer program can be written in any form of computer or programming language, including source code, compiled code, interpreted code and/or machine code, and the computer program can be deployed in any form, including as a stand-alone program or as a subroutine, element, or other unit suitable for use in a computing environment. A computer program can be deployed to be executed on one computer or on multiple computers at one or more sites.

[0027] Method steps can be performed by one or more processors executing a computer program to perform functions of the invention by operating on input data and/or generating output data. Method steps can also be performed by, and an apparatus can be implemented as, special purpose logic circuitry, e.g., a FPGA (field programmable gate array), a FPAA (field-programmable analog array), a CPLD (complex programmable logic device), a PSoC (Programmable System-on-Chip), ASIP (application-specific instruction-set processor), or an ASIC (application-specific integrated circuit). Subroutines can refer to portions of the computer program and/or the processor/special circuitry that implement one or more functions.

[0028] Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any kind of digital or analog computer. Generally, a processor receives instructions and data from a read-only memory or a random access memory or both. The essential elements of a computer are a processor for executing instructions and one or more memory devices for storing instructions and/or data. Memory devices, such as a cache, can be used to temporarily store data. Memory devices can also be used for long-term data storage. Generally, a computer also includes, or is operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data, e.g., magnetic, magneto-optical disks, or optical disks. A computer can also be operatively coupled to a communications network in order to receive instructions and/or data from the network and/or to transfer instructions and/or data to the network. Computer-readable storage devices suitable for embodying computer program instructions and data include all forms of volatile and non-volatile memory, including by way of example semiconductor memory devices, e.g., DRAM, SRAM, EPROM, EEPROM, and flash memory devices; magnetic disks, e.g., internal hard disks or removable disks; magneto-optical disks; and optical disks, e.g., CD, DVD, HD-

DVD, and Blu-ray disks. The processor and the memory can be supplemented by and/or incorporated in special purpose logic circuitry.

[0029] To provide for interaction with a user, the above described techniques can be implemented on a computer in communication with a display device, e.g., a CRT (cathode ray tube), plasma, or LCD (liquid crystal display) monitor, for displaying information to the user and a keyboard and a pointing device, e.g., a mouse, a trackball, a touchpad, or a motion sensor, by which the user can provide input to the computer (e.g., interact with a user interface element). Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback, e.g., visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, and/or tactile input. The above described techniques can also be implemented on mobile devices (e.g., a smartphone, a personal digital assistant device, a cellular telephone, a laptop).

[0030] The above described techniques can be implemented in a distributed computing system that includes a back-end component. The back-end component can, for example, be a data server, a middleware component, and/or an application server. The above described techniques can be implemented in a distributed computing system that includes a front-end component. The front-end component can, for example, be a client computer having a graphical user interface, a Web browser through which a user can interact with an example implementation, and/or other graphical user interfaces for a transmitting device. The above described techniques can be implemented in a distributed computing system that includes any combination of such back-end, middleware, or front-end components.

[0031] The computing system can include clients and servers. A client and a server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[0032] The components of the computing system can be interconnected by any form or medium of digital or analog data communication (e.g., a communication network). Examples of communication networks include circuit-based and packet-based networks. Packet-based networks can include, for example, the Internet, a carrier internet protocol (IP) network (e.g., local area network (LAN), wide area network (WAN), campus area

network (CAN), metropolitan area network (MAN), home area network (HAN), a private IP network, an IP private branch exchange (IPBX), a wireless network (e.g., radio access network (RAN), 802.11 network, 802.16 network, general packet radio service (GPRS) network, HiperLAN), and/or other packet-based networks. Circuit-based networks can include, for example, the public switched telephone network (PSTN), a private branch exchange (PBX), a wireless network (e.g., RAN, bluetooth, code-division multiple access (CDMA) network, time division multiple access (TDMA) network, global system for mobile communications (GSM) network), and/or other circuit-based networks.

[0033] Devices of the computing system and/or computing devices can include, for example, a computer, a computer with a browser device, a telephone, an IP phone, a mobile device (e.g., cellular phone, personal digital assistant (PDA) device, laptop computer, electronic mail device, iPhone available from Apple®), a server, a rack with one or more processing cards, special purpose circuitry, and/or other communication devices. The browser device includes, for example, a computer (e.g., desktop computer, laptop computer) with a world wide web browser (e.g., Microsoft® Internet Explorer® available from Microsoft Corporation, Mozilla® Firefox available from Mozilla Corporation, Chrome available from Google®, Safari available from Apple®, etc.). A mobile computing device includes, for example, a Blackberry®. IP phones include, for example, a Cisco® Unified IP Phone 7985G available from Cisco System, Inc, and/or a Cisco® Unified Wireless Phone 7920 available from Cisco System, Inc.

[0034] One skilled in the art will realize the invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. The foregoing embodiments are therefore to be considered in all respects illustrative rather than limiting of the invention described herein. Scope of the invention is thus indicated by the appended claims, rather than by the foregoing description, and all changes that come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

[0035] What is claimed is:

AUTHENTICATION OF SERVICE REQUESTS INITIATED FROM A SOCIAL NETWORKING SITE

FIELD OF THE INVENTION

[0001] The present invention relates generally to computer-based methods and apparatuses, including computer program products, for authentication of service requests initiated from a social networking site.

BACKGROUND

[0002] With the advent of social networking sites (e.g., Facebook, Twitter, MySpace, LinkedIn, and other social networking sites), it has become increasingly common for people to publicly share information. Social networking sites typically allow a user to create and maintain their own unique user profile that contains personal information about themselves (e.g., their name, residence, hobbies, etc.). Once a user becomes a member of a social networking site, the user can communicate with other users of the social networking site (e.g., with a specific individual, with a group of individuals, or with all users of the social networking site).

[0003] A user can send messages or post updates to one or more other users (for example, at their own volition, or in response to a previous message or update from themselves or another user). These updates can include any type of information, often being limited only by the user's imagination. Some messages include status updates that describe what the user is currently doing at the time of the status update, or what the user intends to do in the near future. Some updates express a user's satisfaction (or dissatisfaction) with a product or experience. Some updates ask questions to other users of the social networking site. Depending on the context, it is desirable to monitor the content of the messages or updates and to allow the user or people (e.g., associated with the user in some way, such as a friend of the user, a contact of the user, members of the same group of the user) to initiate service requests.

SUMMARY OF THE INVENTION

[0004] The techniques described herein provide computerized methods, apparatuses, and computer program products for authentication of service requests initiated from a social networking site. Such authentication facilitates, for example, provisioning service requests to users of the social networking site only upon authorization of the requesting users.

[0005] In one embodiment, the invention features a computerized method for authenticating user service requests from a social networking site. The method includes monitoring, at a server, data representing messages posted at a social networking server. The method includes storing, by the server, data representing a selected message and an originator of the selected message. The method includes transmitting, from the server, data representing a reply to the originator of the selected message for posting at the social networking server, the reply including data that causes transmission of a service request to the server when actuated. The method includes receiving, at the server, data representing the service request and a sender of the service request. The method includes retrieving, by the server, data representing a user profile of the sender of the service request from the social networking server. The method includes comparing, by the server, one or more attributes of the user profile of the sender against one or more attributes of the stored data representing the originator of the selected message in order to verify the one or more attributes of the user profile. The method includes processing, by the server, the service request from the sender if the one or more attributes of the user profile of the sender match the one or more attributes of the stored data representing the originator of the selected message.

[0006] In another embodiment, the invention features a computer program product, tangibly embodied in a non-transitory computer readable medium. The computer program product includes instructions being configured to cause a data processing apparatus to monitor data representing messages posted at a social networking server. The computer program product includes instructions being configured to cause a data processing apparatus to store data representing a selected message and an originator of the selected message. The computer program product includes instructions being configured to cause a data processing apparatus to transmit data representing a reply to the originator of the selected message for posting at the social networking server, the reply including data that

causes transmission of a service request to the server when actuated. The computer program product includes instructions being configured to cause a data processing apparatus to receive data representing the service request and a sender of the service request. The computer program product includes instructions being configured to cause a data processing apparatus to retrieve data representing a user profile of the sender of the service request from the social networking server. The computer program product includes instructions being configured to cause a data processing apparatus to compare one or more attributes of the user profile of the sender against one or more attributes of the stored data representing the originator of the selected message in order to verify the one or more attributes of the user profile. The computer program product includes instructions being configured to cause a data processing apparatus to process the service request from the sender if the one or more attributes of the user profile of the sender match the one or more attributes of the stored data representing the originator of the selected message.

[0007] In another embodiment, the invention features an apparatus for authenticating user service requests from a social networking site. The apparatus includes a database configured to store data representing a selected message and an originator of the selected message. The apparatus includes a server in communication with the database with a processor and memory configured to monitor data representing messages posted at a social networking server. The server is configured to transmit data representing a reply to the originator of the selected message for posting at the social networking server, the reply including data that causes transmission of a service request to the server when actuated. The server is configured to receive data representing the service request and a sender of the service request. The server is configured to retrieve data representing a user profile of the sender of the service request from the social networking server. The server is configured to compare one or more attributes of the user profile of the sender against one or more attributes of the stored data representing the originator of the selected message in order to verify the one or more attributes of the user profile. The server is configured to process the service request from the sender if the one or more attributes of the user profile of the sender match the one or more attributes of the stored data representing the originator of the selected message.

[0008] In other examples, any of the aspects above can include one or more of the following features. The service request can be a request to initiate a chat session. Comparing can include comparing a person attribute in the user profile to a person attribute in the stored data representing the originator to determine whether the sender is the originator of the selected message. Comparing can include comparing a follower attribute in the user profile to a follower attribute in the stored data representing the originator to determine whether the sender is a follower of the originator of the selected message.

[0009] In some examples, comparing includes comparing a location attribute in the user profile to a location attribute in the stored data representing the originator to determine whether the sender is in a same location as the originator of the selected message. Retrieving the data representing a user profile can include transmitting data representing an access authorization to the sender of the service request for authorization to retrieve the data representing the user profile, and receiving data representing a response to the access authorization, the response including data indicative of the sender providing access authorization.

[0010] In other examples, processing the service request includes transmitting a request to a chat server to establish a chat between the sender of the service request and a third party. Data representing a second user profile of the originator of the selected message can be retrieved from a second social networking server. Data representing the reply can be transmitted to the originator at the second social networking server. An aggregated social media profile for the originator including the second user profile and the data representing the selected message and the originator of the selected message can be stored.

[0011] In some examples, the social networking server provides a social networking service to users, the social networking service including a social networking service provided by a social networking site selected from the group consisting of twitter.com, facebook.com, myspace.com, or any combination thereof. The service request can be an advertisement request, a support request, a voice call request, or any combination thereof.

[0012] In other examples, the social networking server provides a social networking service to users, the social networking service including a social networking service provided by a social networking site selected from the group consisting of twitter.com, facebook.com, myspace.com, or any combination thereof. The server can include a user

interface configured to display the data representing messages posted at the social networking server.

[0013] The techniques, which include both methods and apparatuses, described herein can provide one or more of the following advantages. Information can be retrieved from social networking sites based on keywords and reacted to as desired (e.g., by a predefined set of rules). If, for example, a message posted by an originating user includes one or more keywords of interest, a response (e.g., posted reply message) can be sent to the originator of the message that includes invocable data to initiate a service request by a user of the social networking site (e.g., by the originator or other users of the social networking site). Once initiated, the system can authenticate the initiator of the service request (e.g., based on a user profile of the initiator) to verify that, for example, the service request is only granted to a desired audience of the social networking site (e.g., to verify that the initiator profile matches the originator profile, or the initiator profile is related to the originator profile). Advantageously, services such as advertisements, chat services, live help, and other services can be provided to a targeted group of users of social networking sites.

[0014] Social media profiles can be created for users of the social networking site that includes account information for the users aggregated across a plurality of social networking sites to which the user belongs (e.g., for users that post messages that are responded to by the system described herein). The aggregated social media profile can be used to respond to an originator of a message at any one of the originator's many social media services. Advantageously, the targeted group of users for the services is spread across multiple social networking sites.

[0015] Other aspects and advantages of the present invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, illustrating the principles of the invention by way of example only.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] The foregoing and other aspects, features, and advantages of the present invention, as well as the invention itself, will be more fully understood from the following description of various embodiments, when read together with the accompanying drawings.

[0017] FIG. 1 is a diagram showing an exemplary system for implementing service requests for a social networking site;

[0018] FIGS. 2A and 2B are diagrams of an exemplary social networking page for a social networking site according to the present invention;

[0019] FIG. 3 is a flow chart showing an exemplary method for processing a service request; and

[0020] FIG. 4 is a flow chart showing an exemplary method for authenticating a service request.

DETAILED DESCRIPTION

[0021] In general overview, computerized systems and methods are provided for provisioning services to authenticated users of social networking services provided by social networking sites. Social networking sites (or social media) can be monitored so that messages of interest (e.g., posted by users of the social networking sites) are responded to and provided with invocable data to initiate a service request. The actuator of the service request (which can be the originator of the identified message or another user of the social networking site) is authenticated before providing the actuator with the service associated with the service request. In some examples, the user profile (or data profile, e.g., which is requested from the social networking site) associated with the actuator of the service request is compared against the stored data for the associated identified message (e.g., a user profile for the user that initiated the associated identified message) to authenticate one or more attributes between the originator of the identified message and the actuator of the service request.

[0022] FIG. 1 is an exemplary diagram showing an exemplary system 100 for implementing service requests for a social networking site. The system 100 includes a social networking server 102. The social networking server 102 is in communication with a plurality of user devices 104A through 104N (collectively referred to herein as user devices 104). The social networking server 102 is also in communication with a monitoring server 106, which includes a database 108. The monitoring server 106 is also in communication with user devices 104. Application server 110 is in communication with user devices 104 and the monitoring server 106. The computerized elements of system 100

can be in communication using, for example, the internet, cellular links, and/or any other type of data or voice communication.

[0023] The social networking server 102 can be, for example, a single web server with a processor and memory, or a plurality of web servers configured to provide a social networking service to the user devices 104. The social networking services can include, for example, providing computerized services for the user to maintain or update their profile with the social networking site, providing computerized services that facilitate communication with other users of the social networking site, providing computerized services for posting communications or messages, and other services offered through social networking sites. The social networking services can include those service provided by, for example, twitter.com, facebook.com, myspace.com, or linkedin.com. The social networking site provides an application programming interface (API) that facilitates monitoring keywords in messages or other data used within the social networking service (e.g., which can be viewed by user devices 104). Although the following description is directed to an embodiment involving the social networking site twitter.com, the described computerized systems and methods are not so limited and can be applied to other social networking sites, such as facebook.com, myspace.com, or linkedin.com.

[0024] The API is an interface implemented by the social networking site that enables other software programs (e.g., a program executed by the monitoring server 106) to interact with the social networking site. The social networking site provides services through the API, and the API allows the other software programs to access the services. For example, the API services can include services to monitor keywords contained within user communications posted in the social networking site, services to post communications (e.g., messages) to users of the social networking site, or services to obtain information about users of the social networking site (e.g., user profile information).

[0025] The user devices 104 are computing devices with a processor and memory that can interact with the social networking site. For example, the user devices 104 can include desktop computers, laptop computers, tablet PCs, and/or smart phones. A user of a social networking site can use a user device 104 to log into the social networking site and to use the provided social networking services. A user can use any user device 104; they profile

information for a user can be determined independently for a user from the actual user device 104.

[0026] The monitoring server 106 is a computing device having a processor and memory that uses the API for the social networking site to monitor one or more configurable keywords. For example, a computer hardware company that specializes in selling computer hard drives may want to automatically monitor user posts (or messages) to the social networking server 102 to identify posts that includes keywords or phrases related to their business. Advantageously, the monitoring server 106 can receive information based on the keywords and react to the keywords as desired (e.g., if a question is posted from a user device 104 about "hard drives," the monitoring server can transmit a link to the user device 104 that, when invoked, establishes a chat connection with a person who is knowledgeable about hard drives and who can answer the question transmitted from the user device 104).

[0027] For example, the Twitter social networking site provides an API that allows the monitoring server 106 to monitor keywords contained within tweets. A tweet is a posted message that is viewable by users of the twitter.com site. The monitoring server 106 can interface with the twitter social networking site using the API (e.g., by subscribing to a service through the API, such a notification service that pushes information to programs that implement certain functions of the API) with one or more keywords to receive notifications that the keyword is being tweeted, the number of tweets that include the keyword, the number of followers that can see the tweet, and/or other pertinent information. When the monitoring server 106 identifies a keyword, the monitoring server 106 can send a reply tweet to the user that posted the tweet containing the keyword. The database 108 is configured to store data representing selected messages or tweets (e.g., those that contain the monitored keyword) and an originator of the selected message (e.g., which user device 104 transmitted the selected message to the social networking server 102).

[0028] The monitoring server 106 can be in communication with an operator terminal (not shown) that includes a graphical user interface configured to display the data representing messages posted at the social networking server 102. For example, the monitoring server 106 can display information about the identified messages that include the one or more

monitored keywords. The information about the messages can include, for example, the date of the message, the number of followers of the user that posted the message (e.g., people who are subscribed to see the particular message and any related messages), the number of friends of the posting user (e.g., the number of people the posting user has established a relationship with in the social networking site), the geographical location of the posting user (e.g., to the country level, state level, city level, etc.), an identifier for the message, a token for the message (e.g., an Open Authorization (OAuth) token), the source of the message (e.g., the user posted the message via the web, via a mobile device, etc.), the content of the message, the number of messages related to the posted message (e.g., the number of messages in the message string that contained the posted message, such as the count of tweets), the user image associated with the posting user (e.g., a picture of the user), the name of the posting user, a user name associated with the posting user in the social networking site (e.g., a screen name for the user), and/or other information gleaned from the message (e.g., based on the posted message itself, a user profile associated with the posting user, or other information from the social networking site).

[0029] An operator can view the graphical user interface provided by the operator terminal to decide how to respond to the identified message/post. For example, the operator may decide not to respond to the identified message based on one or more criteria associated with the identified message (e.g., geographical area, message content, etc.). Or the operator can decide to send a response to the identified message. This process is described in further detail with respect to FIG. 3.

[0030] The application server 110 provides one or more services to the user devices 104. The service can include, for example, a chat service (e.g., between the user device 104 and a third party, such as a person knowledgeable about a question posed from the user device 104), an advertisement service (e.g., advertisements related to the keywords of the user's message), a support service (e.g., documents or links to documents related to the user's message), and/or a voice service (e.g., the service facilitates a call between the user and a third party, such as a person knowledgeable about a question posted from the user device 104). For example, as will be further described below, the monitoring server 106 can, through the API, post a message in reply to a posted message, the posted message containing a link (e.g., a URL). The link, once invoked by a user device 104, initiates a

service with the application server 110. The monitoring server 106 can authenticate the user device 104 before providing the service to the user (e.g., as described with reference to FIG. 4 below based on a data/user profile associated with the user device 104).

[0031] FIGS. 2A and 2B are diagrams of exemplary social networking pages 200A and 200B, respectively, for a social networking site according to the present invention. Social networking page 200A includes posted messages 202A through 202N (collectively posted messages 202). Posted message 202A includes a logo 204, username user_one 206, content 208 (i.e., "My computer has been very slow lately"), and posting information 210 (i.e., "8 minutes ago via web"). The username user_one 206 indicates which user posted the message 202A (e.g., a user of a user device 104). This is advantageous, for example, to tell users apart when multiple user devices 104 are posting messages for a particular message thread or message board. The content 208 is the text that the posting user user_one 206 entered for the posted message 202A. The posting information 210 indicates how long ago user_one 206 posted the message 202A (i.e., 8 minutes ago) and how user_one 206 posted the message (i.e., via the web).

[0032] Posted message 202N includes a logo 212, username user_one 206, content 214 (i.e., "What is the best kind of computer hard drive to buy?"), and posting information 216 (i.e., "7 minutes ago via web"). Posted messages 202 are used for illustrative purposes only and are not intended to be limiting. One skilled in the art can appreciate that the information contained within the posted messages 202 can be modified without departing from the spirit of the techniques described herein.

[0033] Referring to FIG. 1, user_one 206 (where "user_one" is a screen name representative of user device 104 or of an operator of the user device 104) posted message 202A to the social networking server 102. One minute later user_one 206 posted the posted (using a user device 104) message 202N to the social networking server 102. User_one 206 can configure his account with the social networking site to control which other users can see posted messages 202A and 202N. There can be posted messages by other users between posted messages 202A and 202N (e.g., a different user device 104 can post a message in response to posted message 202A). For example, all people following the posts on social networking page 200A can see posted message 202A and can choose to post a message in response. Similarly, for example, any person that user_one 206 has

established a relationship within the social networking site (e.g., friends) can view the posted message 202A, and/or any user device 104 can view posted message 202A.

[0034] The social networking page 200B in FIG. 2B includes posted messages 202A and 202N from FIG. 2A and also includes posted message 202N+1. Posted message 202N+1 includes a logo 218, username auto_reply 220, content 222 (i.e., "What do you want to know about hard drives?"), a link 224 that causes transmission of a service request to the monitoring server 106, and posting information 226 (i.e., "5 minutes ago via API in response to user_one"). The posting information 226 indicates that posted message 202N+1 was posted by auto_reply 220 (e.g., a user with the screen name "auto_reply," which may correspond to an individual user or a company) five minutes ago via an API (e.g., an API to the social networking site provided by social networking server 102, which allows messages to be posted in response to a user's message) in response to the posted message 202N by user_one 206. Message 202N+1 will be discussed in further detail with respect to FIG. 3 below. The posted message 202N+1 can be transmitted automatically (e.g., by the monitoring server 106 based on rules stored in the database 108) or manually (e.g., by an operator of the monitoring server 106).

[0035] FIG. 3 is an exemplary flow chart showing an exemplary method 300 for processing a service request. Referring to FIG. 1, at step 302 the monitoring server 106 monitors data representing messages posted at the social networking server 102. At step 304, the monitoring server 106 stores data representing a selected message and an originator of the selected message. At step 306, the monitoring server 106 transmits data representing a reply to the originator of the selected message (e.g., to the originating user device 104) for posting at the social networking server 102. The reply includes data that causes transmission of a service request to the monitoring server 106 when actuated. At step 308, the monitoring server 106 receives data representing the service request and a sender of the service request (e.g., which user device 104 actuated the data that causes transmission of the service request).

[0036] At step 310, the monitoring sever 106 determines whether to verify one or more attributes of the sender of the service request. For example, the monitoring server 106 can determine whether or not to verify attributes of the sender based on the data of the sender (e.g., the attributes in the data). In some examples, the monitoring server 106 can be

configured (e.g., via a stored variable) to automatically verify, or not verify, the attributes of the sender. If the monitoring server 106 is configured to verify one or more attributes, the method 300 proceeds to step 400 of FIG. 4. If the monitoring server is not configured to verify the attributes of the sender, the method 300 proceeds to step 312 and the monitoring server processes the service request.

[0037] Referring to step 302, the monitoring server 106 monitors data representing messages posted at the social networking server 102. For example, users of the social networking site Twitter post tweets to the social networking server 102. The monitoring server 106 accesses information about these posted tweets (messages) from the social networking server 102 using, for example, an API provided by Twitter. The monitoring server 106 can be configured to store particular information (or attributes) from the social networking server 102 using the API. The monitoring server 106 can use the acquired information to determine whether to engage the user that posted the message. In some examples, the monitoring server 106 presents a graphical user interface that displays the acquired information to an operator that decides how to respond to the message (e.g., not to respond or to respond).

[0038] For example, referring to FIG. 2A, a computer company that sells hard drives can configure the monitoring server 106 to monitor messages posted to social networking server 102 for particular keywords related to hard drives. For example, the monitoring server 106 can be configured to monitor the content of messages posted at social networking server 102 for the keywords "hard drive" and "buy." Advantageously, if a message includes these keywords, the monitoring server 106 can take appropriate action such that a message is transmitted in response to the posted message (e.g., to provide a link that, once clicked, facilitates setting up a chat session between the user and a third party to help the user with purchasing a hard drive, or to provide an advertisement for hard drives that are provided by the computer company). An exemplary social media monitoring tool is the tracx platform provided by tracx of Hoboken, NJ.

[0039] Referring to step 304, the monitoring server 106 can store data for a selected message if the selected message includes data (e.g., keywords in the message content, a particular user name, a posting time of the message, etc.) that the monitoring server 106 is configured to identify in the posted messages. For example, continuing with the computer

company example described above with respect to step 302, if the monitoring server 106 identifies a message that includes one or more of the keywords “hard drive” and/or “buy,” the monitoring server 106 can store data indicative of the message and/or the originator of the message in database 108. Advantageously, the stored data for the message and/or the originating user can be used to authenticate the requestor of a service request associated with the message.

[0040] Referring to step 306, the monitoring server 106 transmits a reply to the originator of the selected message. For example, referring to FIG. 2B, the monitoring server 106 transmits message 202N+1 to user_one 206, using the social networking server 102, in response to message 202N posted by user_one 206. Message 202N+1 includes content 222 and link 224 that causes transmission of a service request to the monitoring server 106. For example, link 224 can be a chat invitation (e.g., an invitation to a two-way chat between the user device 104 and a second device). If a user of a user device 104 clicks the link 224, the user device 104 can be redirected to the application server 110 to open up a chat (which is described in further detail with respect to step 312 below).

[0041] Referring further to step 306, some social networking sites provide constraints on who can respond to a posted message. The monitoring server 106 can transmit the reply (e.g., using the API for the social networking site) in such a way that it complies with the social networking site constraints and still responds to the user’s posted message. For example, when using Twitter there may not be a way to send a twitter message to a user device 104 if the posting party (e.g., the monitoring server 106) is not following the tweets that included the identified message. Continuing with the computer company example, if the monitoring server 106 is not following the account of user_one 206 (e.g., not following the tweets of user_one 206), then the monitoring server 106 can not send user_one 206 a direct message. To comply with these social networking site constraints, the monitoring server 106 can, for example, send a public tweet and/or send a comment (e.g., a single message to tweeter or a broadcast message to everyone following the tweet).

[0042] Referring to step 308, the monitoring server 106 receives data representing the service request. For example, the monitoring server 106 receives data indicative of a user of a user device 104 clicking on the link 224. Depending on the social networking site (and/or how a user configures their account with the social networking site), there may not

be any guarantee that the user to whom the monitoring server 106 transmitted message 202N+1 is also the same user that clicked on the link 224. For example, if one or more users are following the message chain of user_one 206 that includes messages 202A, 202N and 202N+1, then not only can user_one 206 click the link 224, but so can any of the other users that are viewing the social networking page 200B. In some examples, any user of the social networking site can view the social networking page 200B (and therefore any user can click the link 224). Therefore, in some embodiments it may be desirable to verify attributes of the sender (e.g., to verify the attributes of the user profile for the user that clicked link 224) to determine whether that the monitoring server 106 will provide the service to the sender. The verification process is described in further detail with respect to FIG. 4.

[0043] Referring to step 312, the monitoring server 106 processes the service request. For example, the service request can be a request to initiate a service provided by application server 110. For example, the application server 110 can be a chat server, and the service request can be a request to initiate a chat session between the user that initiated the service request and a second user (e.g., through the application server). The monitoring server 106 can process the service request to chat by transmitting a request to application server 110 to establish a chat between the sender of the service request and a third party. Returning to the computer company example, if user_one 206 clicks on link 224, the monitoring server 106 can instruct the application server 110 to set up a chat session between the initiating user and an expert from the computer company. The expert can be, for example, an expert in the field of computer hard drives. Advantageously, this allows the initiating user to have a chat with the expert about hard drives. Such chat conversations allow the initiating user to have live-time discussions to learn information and/or answer any questions they have about a particular topic.

[0044] In some examples, the expert is matched up with the initiating user based on one or more criteria. For example, the application server 110 can select the expert based on one or more skills (e.g., technology advisors, social media agents, etc.). Advantageously, the monitoring server (and/or the application server 110) can direct the initiating user to the person who will help the most. In some examples, the expert is selected based on the content of the messages (e.g., messages that contain certain keywords related to the

company, keywords indicative of questions (e.g., “why” or “?”), etc.). While the monitoring server 106 can select the expert based on the content of the messages, the monitoring server 106 can also select the user based on other criteria (e.g., the initiating user’s social media profile). For example, as described above, the monitoring server 106 can select the expert based on other information known about the messages such as, for example, the date of the message, the number of followers or friends, geographical location, etc.

[0045] While the term “expert” is used to describe the second person of the chat conversation, this term is used to not only to represent a person with particular knowledge about a field (e.g., a person knowledgeable about computer hard drives), but can also be used to refer to any person who can help the initiating user (e.g., by answering questions, directing them to other websites, providing information, etc.).

[0046] In some examples, the service request is an advertisement request. For example, the content of message 202N+1 can direct a viewer to click the link 224 for a coupon. In some examples, the service request is a support request. In some examples, the service request is a voice call request. For example, the service request can include data indicative of a phone number for the requesting user and a request that the requesting user be called at the phone number. In some examples, the user is presented with a dialog box (e.g., as a web page or as an applet) that allows the user to provide their contact information.

[0047] FIG. 4 is a flow chart showing an exemplary method 400 for authenticating a service request. Method 400 provides for Open Authorization (OAuth), where the monitoring server 106 can authenticate the sender of the service request without the sender providing additional information (e.g., a username and/or password). At step 402, the monitoring server 106 retrieves data representing a user profile of the sender of the service request from the social networking server 102 (e.g., retrieves the profile of the sender identified in the data obtained in step 308 of FIG. 3). At step 404, the monitoring server 106 compares one or more attributes of the user profile of the sender against one or more attributes of the stored data representing the originator of the selected message in order to verify the one or more attributes of the user profile. At step 406, the monitoring server 106 determines whether the compared attributes match. If the one or more attributes match, the method proceeds to step 408 and the monitoring server 106 processes the service request.

If the one or more attributes do not match, the monitoring server 106 proceeds to step 410 and does not process the service request and optionally can provide a default response (e.g., presentation of a company home web page).

[0048] Referring to step 402, the monitoring server 106 can retrieve data representing the sender from the social networking server 102 using, for example, an API provided by the social networking site that is being provided by the social networking server. The monitoring server 106 may request authorization from the sender of the service request before retrieving data about the sender. For example, the monitoring server 106 can transmit an authorization request to the sender (e.g., via a pop-up dialog box, a web page, etc.). The authorization request can be, for example, data representing an access authorization to retrieve the data representing the requesting user's profile from the social networking server 102. The authorization request has a mechanism (e.g., graphical interface buttons, check boxes, etc.) for the sender to indicate either that they do or do not authorize the monitoring server 106 to retrieve data from the social networking sever 102 about them. When the user operates the mechanism, the monitoring server 106 receives data representing a response to the access authorization. If the monitoring server 106 receives data indicative of a denial from the sender, then the monitoring server 106 can terminate method 400 and not retrieve data representing the user from the social networking server 102. If the monitoring server 106 receives data indicative of the sender providing access authorization, then the monitoring server 106 is authorized to request information from the social networking server 102 (e.g., the sender's user profile).

[0049] In some examples, the authorization request is embedded in the social networking site. In some examples, when the requesting user clicks link 224, the link 224 can redirect the user to a servlet that prompts the user with the authorization request (e.g., a Java servlet, or some other protocol by which the monitoring server 106 can respond to the HTTP request). This request can be a request to begin the OAuth stage of method 400. If the monitoring server 106 receives authorization, the monitoring server can request any appropriate information from the social networking server 102 (e.g., the user profile). The monitoring server 106 can retrieve stored information for the originator of the selected message from database 108 (e.g., which was stored in step 304 of method 300). The information retrieved from the social networking server 102 can include, for example, any

information that the monitoring server 106 can use to verify the user profile against the originator of the selected message. For example, the information retrieved from the social networking server 102 can include the date of the message, the number of followers of the user, the number of friends of the user, the user's geographical location, an identifier for the message, a token for the message, the source of the message, the content of the message, the number of messages related to the posted message, the user's image, the name of the user, a user name associated with the user, and/or other information gleaned from the message.

[0050] Referring to steps 404 and 406, the monitoring server 106 can verify one or more attributes of the user profile and the originator of the selected message. In some examples, the monitoring server 106 can verify that the originator of the message is the sender of the service request. For example, the monitoring server 106 can compare a person attribute in the user profile to a person attribute in the stored data representing the originator to determine whether the sender is the originator of the selected message. If the person attributes match, then the monitoring server 106 successfully validated that the sender is the originator of the selected message. For example, referring to FIG. 2B, user_one 206 posted message 202N, and this information is stored in the database 108. The stored information includes a person attribute indicative of user_one 206. If the user_one 206 clicked the link 224 in message 202N+1, then the monitoring server 106 will receive a person attribute indicative of user_one 206 in response to its request for information about the sender of the service request. Since the person attribute for the originator of message 202N is the same as the person attribute for the sender of the service request, the monitoring server 106 can identify that the same user clicked the link 224. Advantageously, the monitoring server 106 can process the service request (e.g., step 408) since the service request was effected by an intended recipient of the service request.

[0051] In some examples, the monitoring server 106 can verify one or more attributes between the user profile and the originator of the selected message that are not unique to the originator of the selected message. For example, the one or more attributes can be shared by a group of people (e.g., and the monitoring server 106 can be configured to engage with members of the particular group). Advantageously, the monitoring server 106 need not verify that the service request was effected by the same user that posted the

message, but can verify other characteristics, such as characteristics of user profiles. For example, the monitoring server can verify whether there is any relationship between the originator of the message and the sender of the service request (e.g., if they are friends in the social networking site), whether they are located within a same geographical area, whether they share one or more common interests or hobbies, and/or other attributes. For example, the monitoring server 106 can verify the sender of the service request is a follower of the originator of the selected message. The monitoring server 106 can compare a follower attribute in the user profile to a follower attribute in the stored data representing the originator to determine whether the sender is a follower of the originator of the selected message. Advantageously, by performing such comparisons, the monitoring server 106 can determine that the sender of the service request is likely to share one or more attributes or characteristics with the originator of the message, and therefore is likely to be a proper audience for the service request.

[0052] In some examples, the monitoring server 106 verifies the sender of the service request is in the same geographical location as the originator of the message. For example, the monitoring server 106 can compare a location attribute in the user profile to a location attribute in the stored data representing the originator to determine whether the sender is in a same location as the originator of the selected message. Advantageously, by comparing the location information, the monitoring server 106 can verify that, for example, targeted advertisements are provided to appropriate recipients.

[0053] Advantageously, the monitoring server 106 can determine if the sender of the service request is the same person as the originator of the selected message based on, for example, a user ID, date, time, location (e.g., the location of the message, based on packet information and geographical location information), and any other attributes relevant to identifying the sender of the service request. Advantageously, because the monitoring server 106 has stored data for the selected message, the monitoring server 106 is not limited to matching the identity of the sender and the originator. As another example, the monitoring server 106 can determine whether the sender of the service request is a "friend" of the selected message. For example, the monitoring server 106 can determine whether the sender has some relationship in the social network to the originator of the selected message (e.g., as indicated between their user profiles). As an illustrative example, the

monitoring server 106 can use an identification field in the originator's profile and use the identification field to get all the followers of the originator (e.g., via the social networking site's API). The monitoring server 106 can perform a basic search of the retrieved list of followers to determine whether the sender of the service request is a follower of the originator of the stored message.

[0054] Referring to step 408, after the sender of the service request is authenticated, the sender can be redirected based on their user profile. For example, the sender can be redirected to a chat session with an expert. The application server 110 can select the expert based on one or more skills of the expert (e.g., technology advisors, social media agents, etc.) based on the sender's user profile. For example, as described above, the monitoring server 106 can select the expert based on the number of followers or friends in the sender's user profile, the geographical location in the user's profile, etc.

[0055] Referring to step 410, the monitoring server 106 can perform other actions even though the monitoring server 106 does not process the service request. For example, the sender of the service request can be directed to a particular web page (e.g., a landing page). For example, the sender can be directed to a default advertisement, a web page that explains the authentication process, a web page that explains why the sender was not provided with the service request, and/or the like.

[0056] In some examples, the monitoring server 106 can monitor a first social networking site and respond to messages posted at the first social networking site through a second social networking site. For example, referring to method 300 in FIG. 3, the monitoring server 106 can monitor data indicative of messages posted at social networking server 102. The monitoring server 106 can retrieve data representing a second user profile of the originator of the selected message from a second social networking server (e.g., from a different social networking server than social networking server 102, which is not shown in FIG. 1). Referring to step 306, the monitoring server 106 can transmit data representing the reply to the originator at the second social networking server (e.g., and not through the social networking server 102).

[0057] For example, the monitoring server 106 can monitor tweets posted to Twitter (e.g., via the Twitter API). If the monitoring server 106 desires to respond to a tweet (e.g., the

tweet includes one or more keywords of interest), the monitoring server 106 can identify one or more additional social networking sites that the originator of the selected message belongs to (e.g., other social networking sites where the originator has an account). For example, the monitoring server 106 can determine that the originator has a Facebook account. The monitoring server 106 can transmit a reply (based on the originator's tweet) to the originator via Facebook instead of through Twitter.

[0058] In some examples, the monitoring server 106 stores an aggregated social media profile for the originator comprising any other user profiles (or information) for the originator at other social media services. The monitoring server 106 can also store the data representing the selected message and the originator of the selected message in the aggregated social media profile. Advantageously, the monitoring server 106 can use the aggregated social media profile to respond to the originator at any one of its many social media services. The social media server 102 can provide multiple social networking sites, a single social media server 102 can provide a single social networking site, or any combination thereof. The social networking site can include Twitter, Facebook, Myspace, LinkedIn, and/or any other social networking service.

[0059] The above-described computerized methods and apparatuses can be implemented in digital and/or analog electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. The implementation can be as a computer program product, i.e., a computer program tangibly embodied in a machine-readable storage device, for execution by, or to control the operation of, a data processing apparatus, e.g., a programmable processor, a computer, and/or multiple computers. A computer program can be written in any form of computer or programming language, including source code, compiled code, interpreted code and/or machine code, and the computer program can be deployed in any form, including as a stand-alone program or as a subroutine, element, or other unit suitable for use in a computing environment. A computer program can be deployed to be executed on one computer or on multiple computers at one or more sites.

[0060] The computerized method steps can be performed by one or more processors executing a computer program to perform functions of the invention by operating on input data and/or generating output data. Method steps can also be performed by, and an apparatus can be implemented as, special purpose logic circuitry, e.g., a FPGA (field

programmable gate array), a FPAA (field-programmable analog array), a CPLD (complex programmable logic device), a PSoC (Programmable System-on-Chip), ASIP (application-specific instruction-set processor), or an ASIC (application-specific integrated circuit). Subroutines can refer to portions of the computer program and/or the processor/special circuitry that implement one or more functions.

[0061] Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any kind of digital or analog computer. Generally, a processor receives instructions and data from a read-only memory or a random access memory or both. The essential elements of a computer are a processor for executing instructions and one or more memory devices for storing instructions and/or data. Memory devices, such as a cache, can be used to temporarily store data. Memory devices can also be used for long-term data storage. Generally, a computer also includes, or is operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data, e.g., magnetic, magneto-optical disks, or optical disks. A computer can also be operatively coupled to a communications network in order to receive instructions and/or data from the network and/or to transfer instructions and/or data to the network. Computer-readable storage devices suitable for embodying computer program instructions and data include all forms of volatile and non-volatile memory, including by way of example semiconductor memory devices, e.g., DRAM, SRAM, EPROM, EEPROM, and flash memory devices; magnetic disks, e.g., internal hard disks or removable disks; magneto-optical disks; and optical disks, e.g., CD, DVD, HD-DVD, and Blu-ray disks. The processor and the memory can be supplemented by and/or incorporated in special purpose logic circuitry.

[0062] To provide for interaction with a user, the above described techniques can be implemented on a computer in communication with a display device, e.g., a CRT (cathode ray tube), plasma, or LCD (liquid crystal display) monitor, for displaying information to the user and a keyboard and a pointing device, e.g., a mouse, a trackball, a touchpad, or a motion sensor, by which the user can provide input to the computer (e.g., interact with a user interface element). Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory

feedback, e.g., visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, and/or tactile input.

[0063] The above described techniques can be implemented in a distributed computing system that includes a back-end component. The back-end component can, for example, be a data server, a middleware component, and/or an application server. The above described techniques can be implemented in a distributed computing system that includes a front-end component. The front-end component can, for example, be a client computer having a graphical user interface, a Web browser through which a user can interact with an example implementation, and/or other graphical user interfaces for a transmitting device. The above described techniques can be implemented in a distributed computing system that includes any combination of such back-end, middleware, or front-end components.

[0064] The computing system can include clients and servers. A client and a server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[0065] The components of the computing system can be interconnected by any form or medium of digital or analog data communication (e.g., a communication network). Examples of communication networks include circuit-based and packet-based networks. Packet-based networks can include, for example, the Internet, a carrier internet protocol (IP) network (e.g., local area network (LAN), wide area network (WAN), campus area network (CAN), metropolitan area network (MAN), home area network (HAN)), a private IP network, an IP private branch exchange (IPBX), a wireless network (e.g., radio access network (RAN), 802.11 network, 802.16 network, general packet radio service (GPRS) network, HiperLAN), and/or other packet-based networks. Circuit-based networks can include, for example, the public switched telephone network (PSTN), a private branch exchange (PBX), a wireless network (e.g., RAN, bluetooth, code-division multiple access (CDMA) network, time division multiple access (TDMA) network, global system for mobile communications (GSM) network), and/or other circuit-based networks.

[0066] Devices of the computing system and/or computing devices can include, for example, a computer, a computer with a browser device, a telephone, an IP phone, a mobile device (e.g., cellular phone, personal digital assistant (PDA) device, laptop computer,

electronic mail device), a server, a rack with one or more processing cards, special purpose circuitry, and/or other communication devices. The browser device includes, for example, a computer (e.g., desktop computer, laptop computer) with a world wide web browser (e.g., Microsoft® Internet Explorer® available from Microsoft Corporation, Mozilla® Firefox available from Mozilla Corporation). A mobile computing device includes, for example, a Blackberry®. IP phones include, for example, a Cisco® Unified IP Phone 7985G available from Cisco System, Inc, and/or a Cisco® Unified Wireless Phone 7920 available from Cisco System, Inc.

[0067] One skilled in the art will realize the invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. The foregoing embodiments are therefore to be considered in all respects illustrative rather than limiting of the invention described herein. Scope of the invention is thus indicated by the appended claims, rather than by the foregoing description, and all changes that come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

[0068] What is claimed is:

CLAIMS

1. A computerized method for authenticating user service requests from a social networking site, comprising:
 - monitoring, at a server, data representing messages posted at a social networking server;
 - storing, by the server, data representing a selected message and an originator of the selected message;
 - transmitting, from the server, data representing a reply to the originator of the selected message for posting at the social networking server, the reply including data that causes transmission of a service request to the server when actuated;
 - receiving, at the server, data representing the service request and a sender of the service request;
 - retrieving, by the server, data representing a user profile of the sender of the service request from the social networking server;
 - comparing, by the server, one or more attributes of the user profile of the sender against one or more attributes of the stored data representing the originator of the selected message in order to verify the one or more attributes of the user profile; and
 - processing, by the server, the service request from the sender if the one or more attributes of the user profile of the sender match the one or more attributes of the stored data representing the originator of the selected message.
2. The method of claim 1, wherein the service request is a request to initiate a chat session.
3. The method of claim 1, wherein comparing comprises comparing a person attribute in the user profile to a person attribute in the stored data representing the originator to determine whether the sender is the originator of the selected message.
4. The method of claim 1, wherein comparing comprises comparing a follower attribute in the user profile to a follower attribute in the stored data representing the originator to determine whether the sender is a follower of the originator of the selected message.

5. The method of claim 1, wherein comparing comprises comparing a location attribute in the user profile to a location attribute in the stored data representing the originator to determine whether the sender is in a same location as the originator of the selected message.
6. The method of claim 1, wherein retrieving the data representing a user profile comprises:
transmitting data representing an access authorization to the sender of the service request for authorization to retrieve the data representing the user profile; and
receiving data representing a response to the access authorization, the response comprising data indicative of the sender providing access authorization.
7. The method of claim 1, wherein processing the service request comprises transmitting a request to a chat server to establish a chat between the sender of the service request and a third party.
8. The method of claim 1, further comprising:
retrieving data representing a second user profile of the originator of the selected message from a second social networking server; and
transmitting data representing the reply to the originator at the second social networking server.
9. The method of claim 8, further comprising storing an aggregated social media profile for the originator comprising the second user profile and the data representing the selected message and the originator of the selected message.
10. The method of claim 1, wherein the social networking server provides a social networking service to users, the social networking service comprising a social networking service provided by a social networking site selected from the group consisting of twitter.com, facebook.com, myspace.com, or any combination thereof.
11. The method of claim 1, wherein the service request is an advertisement request, a support request, a voice call request, or any combination thereof.

12. A computer program product, tangibly embodied in a non-transitory computer readable medium, the computer program product including instructions being configured to cause a data processing apparatus to:

- monitor data representing messages posted at a social networking server;
- store data representing a selected message and an originator of the selected message;
- transmit data representing a reply to the originator of the selected message for posting at the social networking server, the reply including data that causes transmission of a service request to the server when actuated;

- receive data representing the service request and a sender of the service request;

- retrieve data representing a user profile of the sender of the service request from the social networking server;

- compare one or more attributes of the user profile of the sender against one or more attributes of the stored data representing the originator of the selected message in order to verify the one or more attributes of the user profile; and

- process the service request from the sender if the one or more attributes of the user profile of the sender match the one or more attributes of the stored data representing the originator of the selected message.

13. An apparatus for authenticating user service requests from a social networking site, comprising:

- a database configured to store data representing a selected message and an originator of the selected message; and

- a server in communication with the database with a processor and memory configured to:

- monitor data representing messages posted at a social networking server;
- transmit data representing a reply to the originator of the selected message for posting at the social networking server, the reply including data that causes transmission of a service request to the server when actuated;

- receive data representing the service request and a sender of the service request;

- retrieve data representing a user profile of the sender of the service request from the social networking server;

compare one or more attributes of the user profile of the sender against one or more attributes of the stored data representing the originator of the selected message in order to verify the one or more attributes of the user profile; and

process the service request from the sender if the one or more attributes of the user profile of the sender match the one or more attributes of the stored data representing the originator of the selected message.

14. The apparatus of claim 13, wherein the social networking server provides a social networking service to users, the social networking service comprising a social networking service provided by a social networking site selected from the group consisting of twitter.com, facebook.com, myspace.com, or any combination thereof.

15. The apparatus of claim 13, wherein the server comprises a user interface configured to display the data representing messages posted at the social networking server.

100 ↙

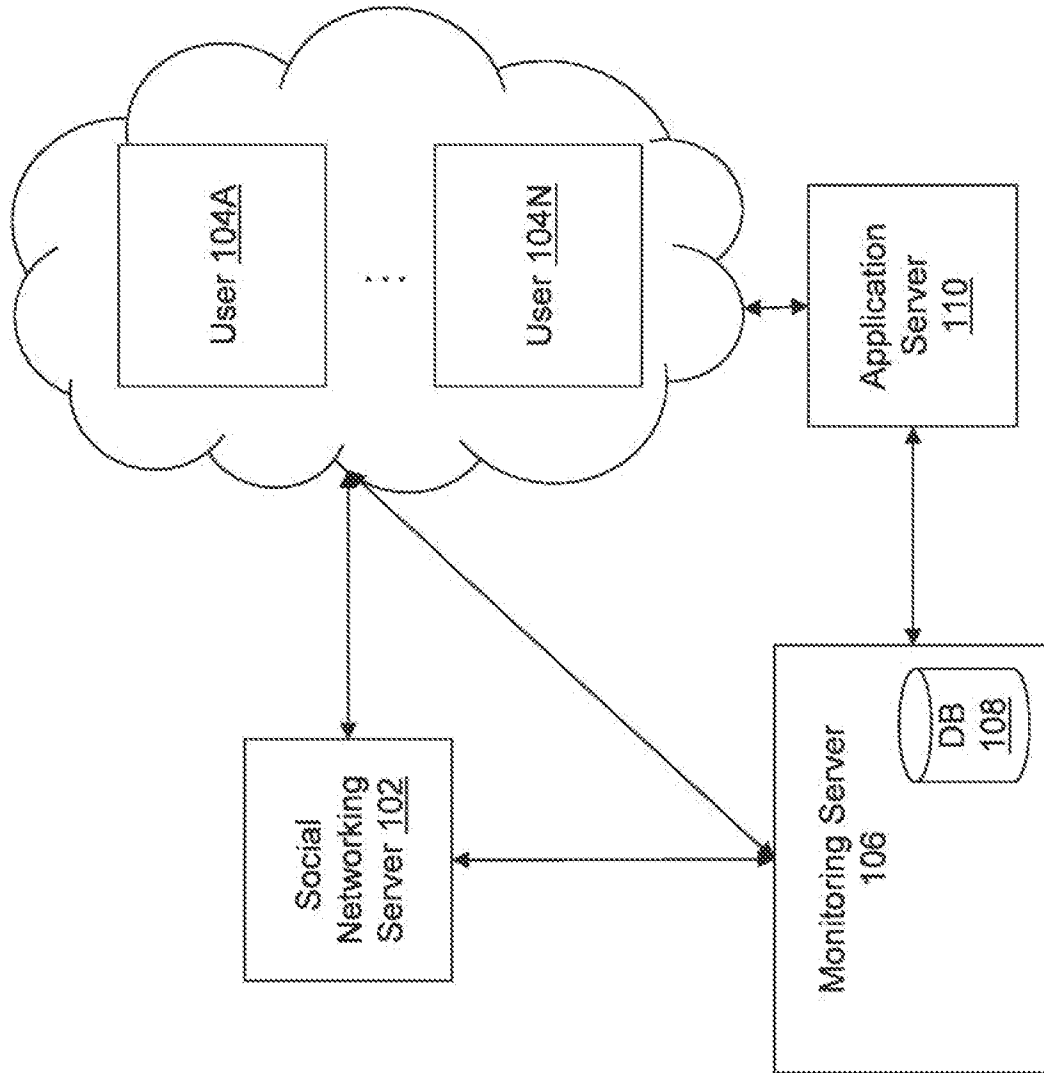


FIG. 1

2/4

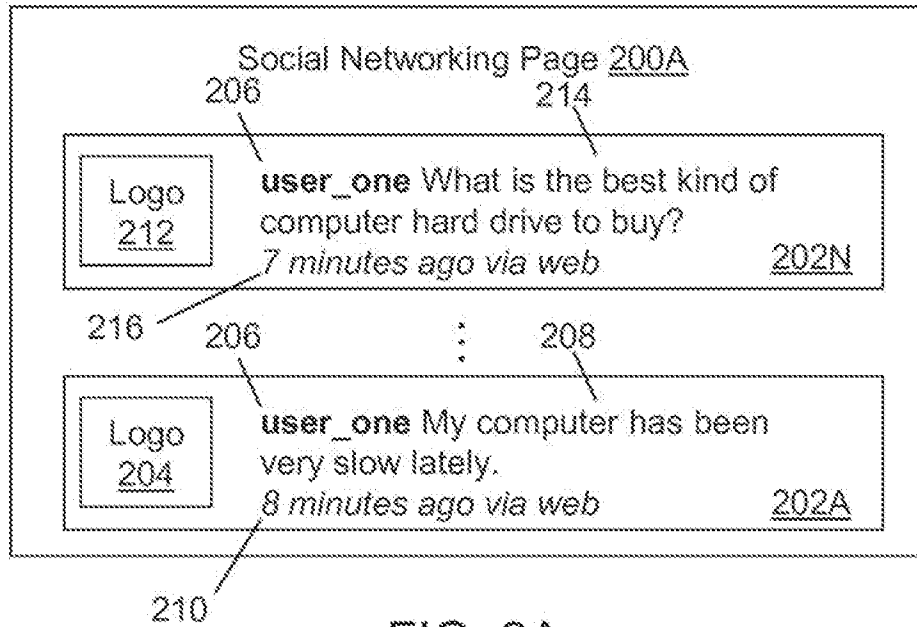


FIG. 2A

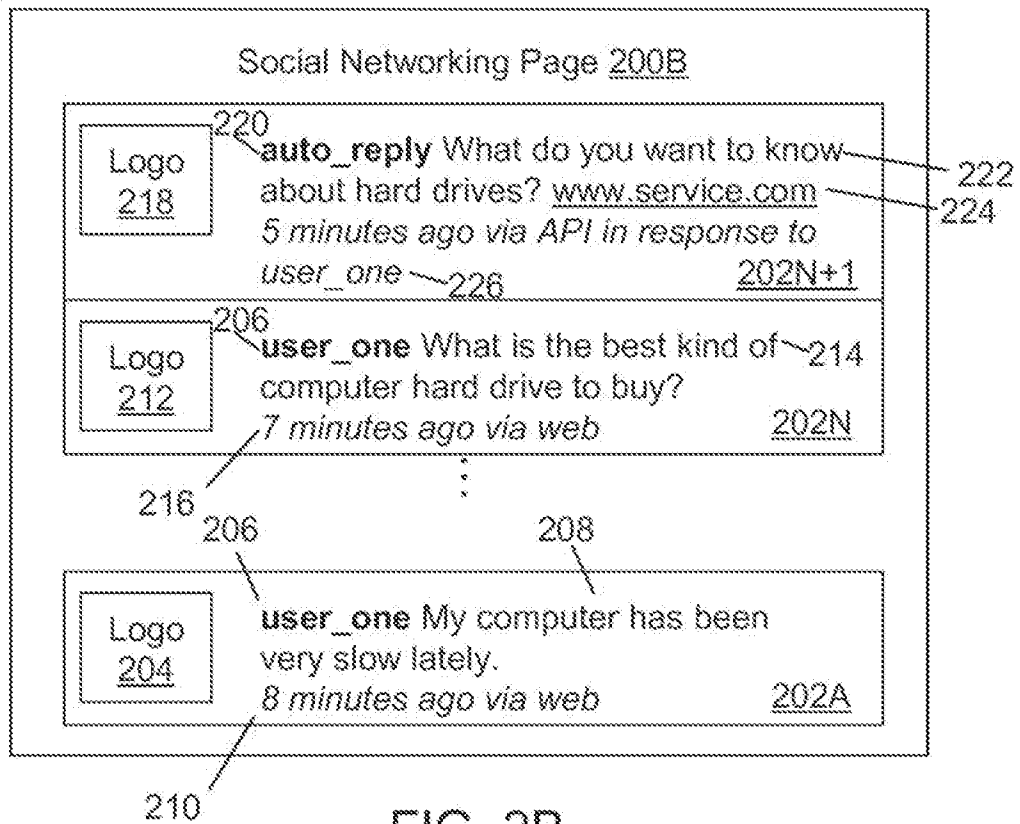


FIG. 2B

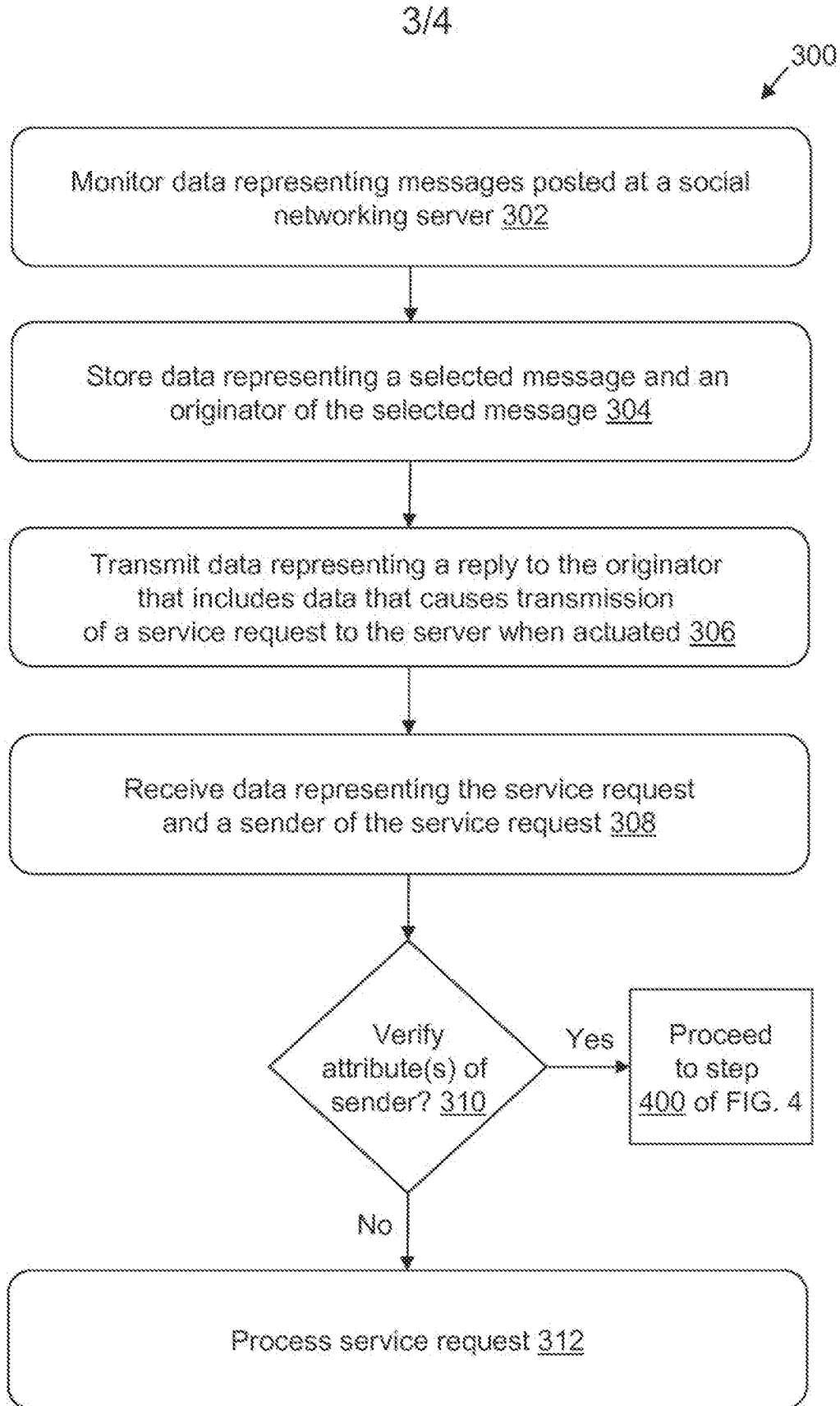


FIG. 3

4/4

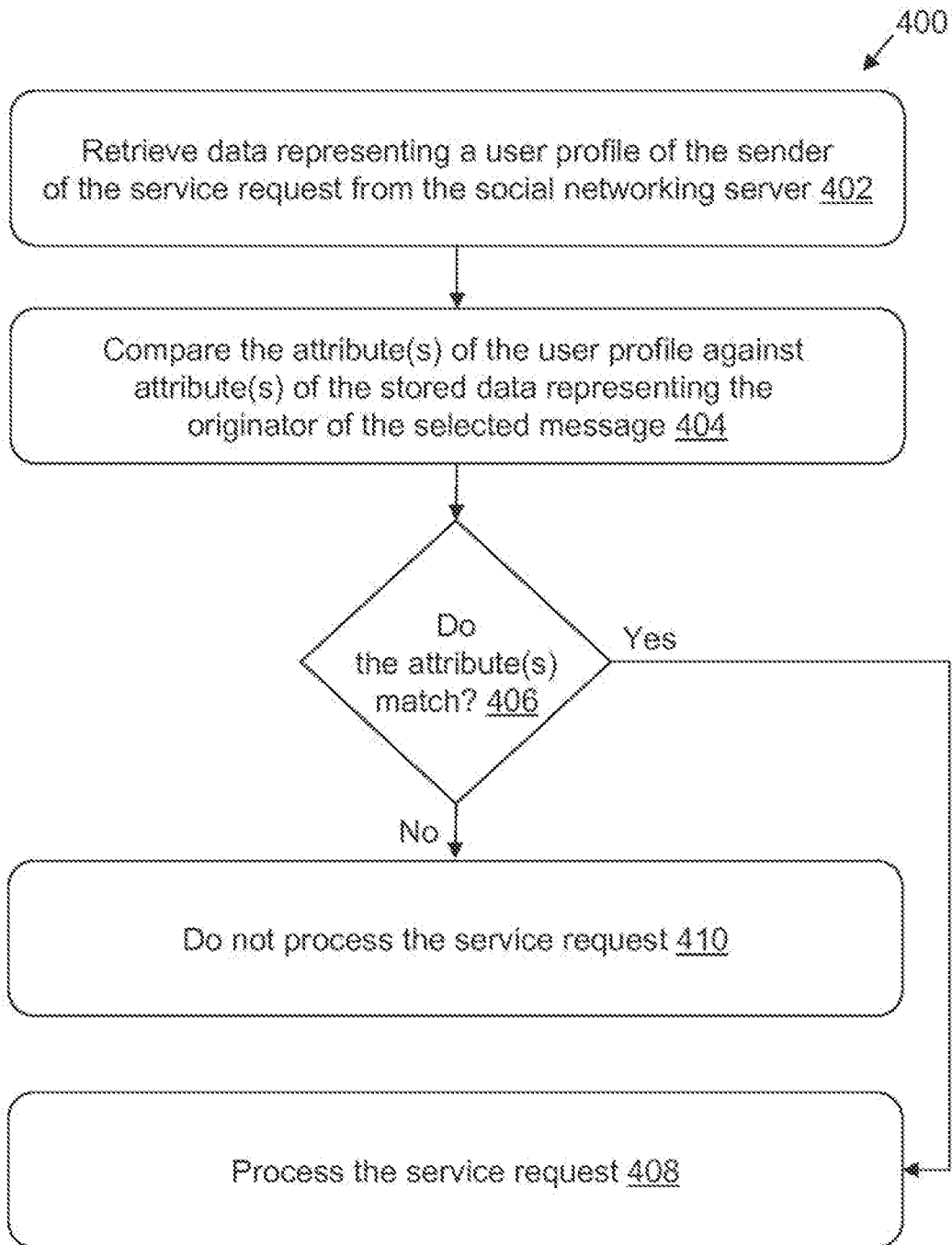


FIG. 4

CLAIMS

1. A computerized method for authenticating user service requests, comprising:
 - transmitting, from a server, data that causes transmission of a service request to the server;
 - receiving, at the server, data representing the service request and data representing a sender of the service request;
 - comparing, by the server, (a) the data representing the service request, the data representing the sender of the service request, or both, against (b) pre-defined criteria associated with the data that causes transmission of the service request; and
 - processing, by the server, the service request from the sender if the comparison authenticates the service request.

2. The method of claim 1, wherein the data that causes transmission of a service request to the server when actuated comprises an HTTP link.

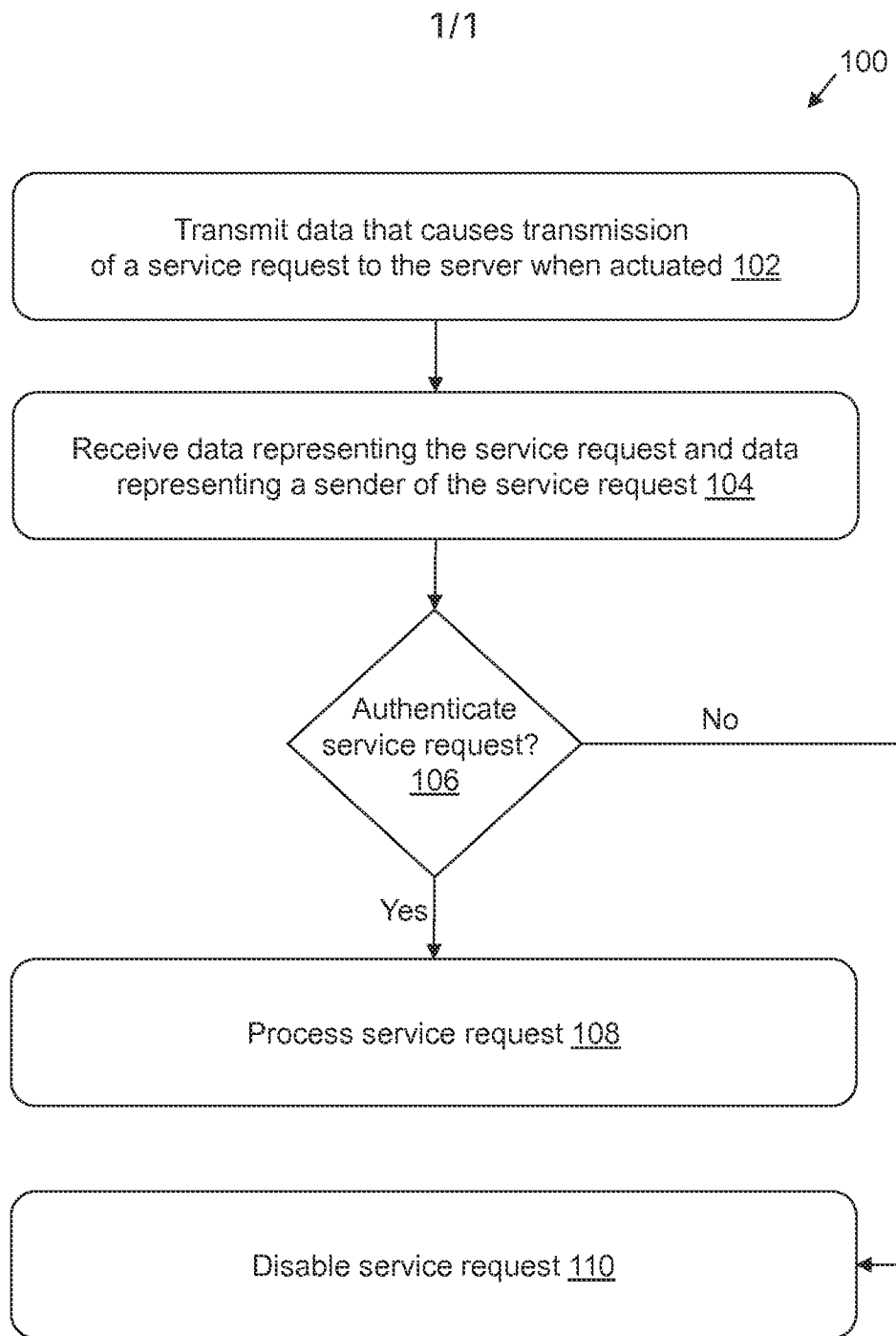


FIG. 1

INTERNATIONAL SEARCH REPORT

International application No PCT/US2013/037086

A. CLASSIFICATION OF SUBJECT MATTER
 INV. H04L12/58
 ADD.

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)
 H04L

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)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2010/144207 A2 (ALIBABA GROUP HOLDING LTD [US]; YE JUN [CN]; MO JIANXIANG [CN]) 16 December 2010 (2010-12-16) abstract figure 2	1,2
X	----- FR 2 950 214 A1 (ALCATEL LUCENT [FR]) 18 March 2011 (2011-03-18) abstract figure 5	1,2
X	----- US 2011/270926 A1 (BOYD JOHN [US] ET AL) 3 November 2011 (2011-11-03) abstract figure 2	1,2
	----- -/--	

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

* Special categories of cited documents :

<p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"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)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"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</p> <p>"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</p> <p>"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</p> <p>"&" document member of the same patent family</p>
---	---

Date of the actual completion of the international search 8 July 2013	Date of mailing of the international search report 12/07/2013
---	---

Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer <p style="text-align: center; font-size: 1.2em;">Poggio, Francesca</p>
--	--

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2013/037086

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/138298 A1 (ALFRED JOSEPH ANDERSON [US] ET AL) 9 June 2011 (2011-06-09) abstract figure 3 -----	1,2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2013/037086

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 2010144207	A2	16-12-2010	CN 101572607 A	04-11-2009
			EP 2441029 A2	18-04-2012
			HK 1136722 A1	16-03-2012
			JP 2012532359 A	13-12-2012
			US 2011113101 A1	12-05-2011
			WO 2010144207 A2	16-12-2010

FR 2950214	A1	18-03-2011	NONE	

US 2011270926	A1	03-11-2011	NONE	

US 2011138298	A1	09-06-2011	NONE	
