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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 August 2016 (04.08.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/122441 A1

(51) International Patent Classification:
G06F 21/31 (2013.01)

(21) International Application Number:
PCT/US2015/012895

(22) International Filing Date:
26 January 2015 (26.01.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP** [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).

(72) Inventors: **WEI, Jian John**; 1822 Lexington Dr., Suite 5000, 6000, 7000, Troy, Michigan 48084 (US). **KAUR, Satwant**; 2350 Charleston Rd, Mt. View, California 94043 (US).

(74) Agents: **FEBBO, Michael** et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, CO 80528 (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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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

WO 2016/122441 A1

(54) Title: AUTHENTICATION OF A USER

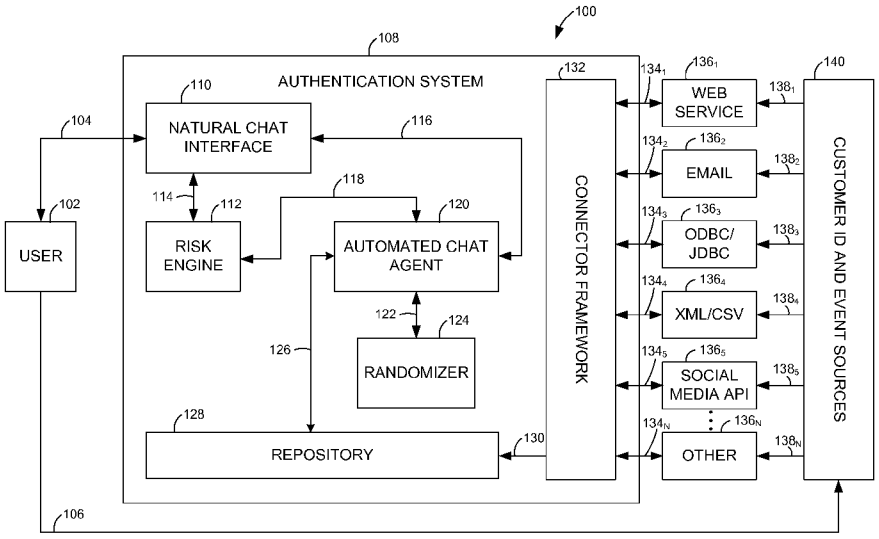

FIG. 1

(57) Abstract: One example of a system to authenticate a user receives an authentication request from a user. The authentication request includes user device data. The system determines a risk level of the user based on the user device data and generates one or more questions based on the risk level and randomly selected data records of the user. The system presents the one or more questions to the user and receives answers from the user to the one or more questions. The system authenticates the user in response to receiving a correct answer to each of the one or more questions.

AUTHENTICATION OF A USER

Background

[0001] Passwords are often used to authenticate a user prior to allowing the user access to a system, such as a computer network, a bank account, an email account, etc. To prevent brute force hacking of passwords based on language or expression dictionaries, many systems require passwords to comply with increasingly complex password schemas, such as requiring a password to be at least eight characters long, using a combination of upper and lower case letters, avoiding words used in past passwords or common expressions, and including special characters. These password schemas degrade the ability of users to remember truly unique passwords in large numbers. As a result, many users engage in unsafe password practices, such as re-using passwords across applications or sites, writing down passwords in unencrypted form, or using passwords that contain easy to remember or self-identifying information. In addition, many passwords in use do not change often. When a user is forced to change a password, the actual change is typically minimal such as appending an incremental number. Finally, once a password is stolen and a system is hacked into, until that password is reset, the hacker has authorization to execute all transactions a rightful user is empowered to execute.

Brief Description of the Drawings

[0002] Figure 1 is a block diagram illustrating one example of a system.

[0003] Figure 2 is a sequence diagram illustrating one example of the operation of the system of Figure 1.

[0004] Figure 3 is a block diagram illustrating one example of a processing system for implementing an authentication system.

[0005] Figure 4 is a flow diagram illustrating one example of a method for authenticating a user.

Detailed Description

[0006] In the following detailed description, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific examples in which the disclosure may be practiced. It is to be understood that other examples may be utilized and structural or logical changes may be made without departing from the scope of the present disclosure. The following detailed description, therefore, is not to be taken in a limiting sense, and the scope of the present disclosure is defined by the appended claims. It is to be understood that features of the various examples described herein may be combined, in part or whole, with each other, unless specifically noted otherwise.

[0007] Typical password-based authentication solutions are inherently prone to hacking since the passwords are typically unnatural, changed infrequently, and not self-healing. Accordingly, this disclosure addresses these three vulnerabilities by providing a password-less authentication mechanism that uses a real-time randomized sampling of naturally generated user information in a real-time, automated, and human chat like manner. The authentication mechanism can improve the end user experience and confidence in the authentication mechanism without users having to remember increasingly complex and different passwords.

[0008] The authentication mechanism authenticates a user based on correlating user responses to a set of questions randomly generated based on dynamic information. The dynamic information is naturally generated by the user in their

daily interactions and stored as user data records. The dynamic information can be broadly grouped into three categories including:

1. What the user knows (e.g., when he swiped his access card to enter the work place this morning).
2. What the user has (e.g., geo-location and operating system version of a user device).
3. What the person is (e.g., a singular email recipient from someone else on a given subject two days ago).

The disclosed authentication mechanism is natural, constantly changing, and self-healing.

[0009] With the proliferation of sensors and devices, and the resulting increasing human system interactions on a daily basis, by automating the inquiry process and randomizing the question generation, real-time authentication can be enabled based on a constantly improving knowledge base over a vast number of data sources. By asking a user for information the user already has, knows, or possesses, and then matching that information to the knowledge already available in the knowledge base, the user can be authenticated without using a password. Since the questions are generated in real-time, and the underlying knowledge base evolve dynamically, a hacker's success with one authenticated session does not provide assurance for success in future sessions. The system may be configured and changed dynamically in how the questions are generated and in the thresholds for accepting the answers, thereby further increasing the security of the system.

[0010] Figure 1 is a block diagram illustrating one example of a system 100. System 100 includes a user 102, an authentication system 108, information sources 136_1-136_N, where "N" is any suitable number of information sources, and customer identity and event sources 140. Authentication system 108 includes a natural chat interface 110, a risk engine 112, an automated chat agent 120, a randomizer 124, a repository 128, and a connector framework 132.

[0011] User 102 is communicatively coupled to natural chat interface 110 through a communication path 104 (e.g., a computer network, a cellular telephone network, the Internet) and to customer identity and event sources 140

through a link 106 (e.g., interactions). Natural chat interface 110 is communicatively coupled to risk engine 112 through a communication path 114 and to automated chat agent 120 through a communication path 116. Risk engine 112 is commutatively coupled to automated chat agent 120 through a communication path 118. Automated chat agent 120 is communicatively coupled to randomizer 124 through a communication path 122 and to repository 128 through a communication path 126. Repository 128 is communicatively coupled to connector framework 132 through a communication path 130.

[0012] Connector framework 132 is communicatively coupled to information sources 136_1-136_N through communication paths 134_1-134_N, respectively. Information sources 136_1-136_N are communicatively coupled to customer identity and event sources 140 through links 138_1-138_N (e.g., interactions with user 102), respectively. In this example, information sources 136_1-136_N include a web service 136_1, an email system 136_2, an Open Database Connectivity (ODBC) and/or Java Database Connectivity (JDBC) system 136_3, Extensible Markup Language (XML) and/or Comma-Separated Values (CSV) data sources 136_4, a social media Application Programming Interface (API) 136_5, and other suitable data sources such as indicated at 136_N. While specific examples of information sources are illustrated in Figure 1, any other suitable information sources may be used, such as building access systems, climate control systems, etc.

[0013] Natural chat interface 110 provides a user interface for interacting with user 102 via a user device (e.g., computer, smart phone, tablet), such as through a browser installed on the user device. In response to a user requesting access (e.g., login or authentication request) to a system, natural chat interface 110 captures user profile data from the user device, such as the operating system (OS) of the user device, the browser being used by the user, the geo-location of the user device, and/or the user device type. In one example, the user profile data is included in the authentication request. Natural chat interface 110 sends the user profile data to risk engine 112 for evaluation and ultimately presents to the user a set of questions generated by automated chat agent 120 based on the evaluated risk. Natural chat interface 110

captures the user's answers to the questions for evaluation by automated chat agent 120.

[0014] Risk engine 112 compares the user profile data received from the user device to historical user profile data previously captured by authentication system 108 during previous requests for access and determines a risk level. For example, for a user that usually accesses the system from Michigan, using an HP Slate 7 Extreme, on Android 4.4.2., if the user conforms to this pattern, risk engine 112 would deem the access request to be low risk. In this case, low risk will lead to automated chat agent 120 generating a smaller number of questions covering events over a more recent span of time. If, however, the user deviates from the usual pattern and attempts to access the system from California on a Nexus 7 using an older Android version of 4.3, risk engine 112 would deem the access request as high risk based on the degree of deviation to the usual pattern. In this case, high risk will lead to automated chat agent 120 generating a larger number of questions covering events over a greater span of time.

[0015] The total deviation of the user profile data from the historical user profile data may be calculated by summing the Relative Standard Deviation (RSD) for each risk factor (e.g., OS, browser, geo-location, device type). The risk threshold may then be grouped for example into the following risk categories:

1. Low Risk (e.g., within 1 sigma of normal distribution)
2. Medium Risk (e.g., within 2-4 sigma of normal distribution)
3. High Risk (e.g., within 5-6 sigma of normal distribution)

where the normal distribution is determined from the historical user profile data. The threshold in sigma for each risk category may be configured based on a configuration file, table, or other suitable method.

[0016] Based on the risk factor, risk engine 112 determines the number and difficultly of the questions to be asked. In one example, a configurable mapping based on the sigma value of the user access request dictates the number of questions to ask, how far to go back in time with events, the mix of question types, and the threshold of correct answers for authentication. A low sigma value signifies that the user access request is similar to past user access

requests in terms of OS, browser, geo-location, and device type. A sample configuration based on the sigma value is illustrated in the following table:

Sigma	Question Count	Earliest Time	Question Mix	Threshold of Correct Answer Percentage for Authorization
<1	1	3 days before	1 Type	100%
2	2	7 days before	2 Types	100%
3	4	14 days before	4 Types	75%
4	8	28 days before	8 Types	75%
>5	16	56 days before	16 Types	80%

[0017] Once risk engine 112 determines the sigma value, risk engine 112 uses the configuration table to set the question count, question time span, question mix, and threshold of correct answers based on the sigma value. Risk engine 112 sends the question count, question time span, question mix, and threshold of correct answers to automated chat agent 120.

[0018] Automated chat agent 120 generates a number of questions as indicated by the question count, question time span, and question mix from risk engine 112. Automated chat agent 120 generates questions and evaluates the match between the answers and the corresponding event information. The degree of match between the answers and the corresponding event information may be configured to result in authorization of access to the system, more questions being presented to the user before access to the system is granted, or blocking of access to the system.

[0019] Automated chat agent 120 may generate questions based on information about what the user has, what the user knows, and what the user is. These three general categories are further divided by event types, such as by the source of the information (e.g., each information source 136_1-136_N provides a different event type). Example information for each category is as follows:

A. Information on what the user has (i.e., user ownership data):

1. Serial number of the company issued device (e.g. laptop)
2. Model of cell phone that was last used to access company network (e.g. HTC One)
3. Brand and model number of home internet enabled thermostats
4. Last 4 digits of credit card number

5. Year home house was built

B. The information on what the user knows (i.e., user knowledge data):

1. When he entered which office yesterday
2. Who he / she reports up to
3. When he joined the company
4. Rating from the last performance review
5. Where he/she lived before
6. Whom he/she sent an email to on a given subject

C. Information on what the user is (i.e., user inherence data):

1. Biometric marker
2. Name of parent
3. Date of birth
4. Place of birth
5. Citizenship

[0020] In one example, automated chat agent 120 implements two loops, a first loop by event type and a second loop by question count. For each pass through the first loop, randomizer 124 generates a number between 0 and 1, which is multiplied by the question mix count. The resulting number is rounded up and used as an index to randomly select an event type. For the second loop, which is a sub-loop of the first loop, randomizer 124 generates a number between 0 and 1, which is multiplied by the question count. The resulting number is rounded up and used as an index to randomly select a particular event from the event type randomly selected in the first loop. For each particular event selected, a question is generated for presentation to the user with the particular event data providing the correct answer to the question for comparison to the user's answer to the question.

[0021] Randomizer 124 generates random numbers to be used to randomly select past event information as the basis for questions to be generated by automated chat agent 120. Therefore, even if a hacker gains access to some confidential information of the user, the hacker will still be unable to gain guaranteed access to the system since the hacker will not know which event information will be selected for each access request.

[0022] Repository 128 is a knowledge base where the event information data of the users is stored. The data stored in repository 128 is normalized, indexed, and classified by type for selection by automated chat agent 120. In one example, repository 128 is implemented by a Storage Area Network (SAN) or other suitable data storage system.

[0023] Connector framework 132 enables information from customer identity and event sources 140 to flow into repository 128 through information sources 136_1-136_N. The data may flow into repository 128 synchronously and/or asynchronously. Connector framework 132 receives, normalizes, and indexes the data for storage in repository 128. As a user interacts with information sources 136_1-136_N, repository 128 is updated with new user records such that repository 128 provides a dynamic knowledge base.

[0024] Figure 2 is a sequence diagram illustrating one example of the operation 200 of authentication system 100 of Figure 1. The operation of system 100 involves user 102, natural chat interface 110, risk engine 112, randomizer 124, repository 128, and automated chat agent 120. To begin, user 102 logs on (i.e., requests access) to natural chat interface 110 as indicated by LOGON() at 202. Natural chat interface 110 initiates a user device dump to capture user profile data such as the OS, geo-location, device type, and browser information as indicated by DEVICE_DUMP() at 204. Natural chat interface 110 sends the user profile data to risk engine 112 for analysis as indicated by RISK_PROFILE() at 206. Risk engine 112 determines a risk profile based on a comparison of the user profile data to the historical user profile data and informs automated chat agent 120 on the number of questions and degree of difficulty of the questions to generate as indicated by START_CHAT() at 208.

[0025] Automated chat agent 120 calls upon randomizer 124 to generate a random number as indicated by GET_RNDM#() at 210. Based on the random number, automated chat agent 120 randomly selects a set of event information from repository 128 as indicated by RTRV_INFO(RNDM_#) at 212. Automated chat agent 120 selects a particular event from the event information as indicated by GET_INFO_TYPE() at 214 and generates a question as indicated by GEN_QUESTION() at 216 based on the selected event information. Automated

chat agent 120 sends the generated questions to natural chat interface 110 as indicated by ASK_QUESTION() at 218.

[0026] Natural chat interface 110 presents the questions to user 102, who reads the questions as indicated by RD_QUESTION() at 220. User 102 provides answers to the questions that are captured by natural chat interface 120 as indicated by CPTR_ANSWER() at 222. Natural chat interface 110 passes the answers to automated chat agent 120 for evaluation as indicated by EVALUATE_MATCH() at 224. Automated chat agent 120 evaluates the match between the user's answers and the underlying event information to grant authorization as indicated by AUTHORIZE() as 226, to ask additional questions prior to granting access to the system, or to block access to the system.

[0027] Figure 3 is a block diagram illustrating one example of a processing system 300 for implementing an authentication system. In one example, processing system 300 is used to implement system 100 previously described and illustrated with reference to Figure 1. Processing system 300 includes a processor 302, a memory 306, input devices 320, and output devices 322. Processor 302, memory 306, input devices 320, and output devices 322 are communicatively coupled to each other through a communication path 304 (e.g., a bus).

[0028] Processor 302 includes a Central Processing Unit (CPU) or another suitable processor. In one example, memory 306 stores machine readable instructions executed by processor 302 for operating processing system 300. Memory 306 includes any suitable combination of volatile and/or non-volatile memory, such as combinations of Random Access Memory (RAM), Read-Only Memory (ROM), flash memory, and/or other suitable memory.

[0029] Memory 306 stores repository 314 for use by processing system 300. Memory 306 also stores instructions to be executed by processor 302 including instructions for a natural chat interface 308, a risk engine 310, a randomizer 312, an automated chat agent 316, and a connector framework 318. Processor 302 executes instructions of natural chat interface 308 to implement natural chat interface 110 previously described and illustrated with reference to Figures 1 and 2. Processor 302 executes instructions of risk engine 310 to implement risk

engine 112 previously described and illustrated with reference to Figures 1 and 2. Processor 302 executes instructions of randomizer 312 to implement randomizer 124 previously described and illustrated with reference to Figures 1 and 2. Processor 302 executes instructions of automated chat agent 316 to implement automated chat agent 120 previously described and illustrated with reference to Figures 1 and 2. Processor 302 executes instructions of connector framework 318 to implement connector framework 132 previously described and illustrated with reference to Figure 1.

[0030] Input devices 320 may include a keyboard, mouse, data ports, network adapters, and/or other suitable devices for inputting information into processing system 300. Input devices 320 may also be used to receive the data to be stored in repository 314 and to receive data from a user such as the user profile data and the user's answers to questions. Output devices 322 may include a monitor, speakers, data ports, network adapters, and/or other suitable devices for outputting information from processing system 300. In one example, output devices 316 are used to provide data to a user, such as the questions presented to the user in response to an access request.

[0031] Figure 4 is a flow diagram illustrating one example of a method 400 for authenticating a user. At 402, an authentication request is received from a user from a user device. At 404, device data about the user device is retrieved. Retrieving the device data may include retrieving a geolocation, a device type, and an operating system version of the user device. At 406, a risk level of the user is determined based on the device data. At 408, user records are randomly selected from a repository based on the risk level. At 410, one or more questions are generated based on the selected user records. In one example, a greater number of questions are generated in response to a higher risk level and a lesser number of questions are generated in response to a lower risk level.

[0032] At 412, the user is asked the one or more questions. At 414, answers to the one or more questions are received from the user. In one example, the received answers are evaluated to determine a degree of match to the correct answer to each of the one or more questions. At 416, the user is authenticated

in response to receiving a correct answer to each of the one or more questions. In one example, the user is authenticated in response to the degree of match for each of the one or more questions exceeding a threshold value. The method may also include collecting user data from a plurality of different sources of different types, normalizing the collected user data, and storing the normalized user data in the repository.

[0033] Although specific examples have been illustrated and described herein, a variety of alternate and/or equivalent implementations may be substituted for the specific examples shown and described without departing from the scope of the present disclosure. This application is intended to cover any adaptations or variations of the specific examples discussed herein. Therefore, it is intended that this disclosure be limited only by the claims and the equivalents thereof.

CLAIMS

1. A system comprising:

a processor; and

a memory communicatively coupled to the memory, the memory storing user data records and instructions executable by the processor to:

receive an authentication request from a user, the authentication request including user device data;

determine a risk level of the user based on the user device data;

generate one or more questions based on the risk level and randomly selected data records of the user;

present the one or more questions to the user;

receive answers from the user to the one or more questions; and

authenticate the user in response to receiving a correct answer to each of the one or more questions.

2. The system of claim 1, wherein a number of questions generated increases as the risk level increases.

3. The system of claim 1, wherein the user data records comprise user knowledge data, user ownership data, and user inherence data.

4. The system of claim 1, wherein the memory stores instructions executable by the processor to:

collect user data from a plurality of different sources;

normalize the collected user data; and

store the normalized user data in the memory as user data records.

5. The system of claim 4, wherein the plurality of difference sources include access control systems, web services, email, database systems, and social media.

6. A system comprising:

a processing system comprising:

a natural chat interface to receive user device data, present questions to a user, and receive answers to the questions in response to a user authentication request;

a risk engine to determine a risk level based on received user device data and to determine a number of questions to be presented to the user based on the risk level;

a randomizer to randomly select event information for questions to be presented to the user;

a repository to store the event information;

an automated chat agent to generate the questions presented to the user, evaluate the received answers to the questions, and authenticate the user based on the evaluation; and

a connector framework to collect event information and store the collected event information in the repository.

7. The system of claim 6, wherein the risk engine determines the risk level based on a relative standard deviation for each of a number of risk factors compared to a pattern of the user over previous authentication requests.

8. The system of claim 6, wherein the connector framework collects event information indicating what the user knows, what the user has, and what the user is.

9. The system of claim 6, wherein the automated chat agent blocks access to the user in response to the evaluation of the received answers indicating incorrect answers.

10. The system of claim 6, wherein the automated chat agent generates additional questions in response to the evaluation of the received answers indicating a portion of the received answers are incorrect.

11. A method comprising:

receiving an authentication request from a user from a user device;

retrieving device data about the user device;

determining a risk level of the user based on the device data;

randomly selecting user records from a repository based on the risk level;

generating one or more questions based on the selected user records;

asking the one or more questions of the user;

receiving answers from the user to the one or more questions; and

authenticating the user in response to receiving a correct answer to each of the one or more questions.

12. The method of claim 11, wherein retrieving the device data comprises retrieving a geolocation, a device type, and an operating system version of the user device.

13. The method of claim 11, further comprising:

collecting user data from a plurality of different sources of different types;

normalizing the collected user data; and

storing the normalized user data in the repository.

14. The method of claim 11, further comprising:

evaluating the received answers to determine a degree of match to the correct answer to each of the one or more questions; and

authenticating the user in response to the degree of match for each of the one or more questions exceeding a threshold value.

15. The method of claim 11, wherein generating the one or more questions based on the selected user records comprises generating a greater number of

questions in response to a higher risk level and a lesser number of questions in response to a lower risk level.

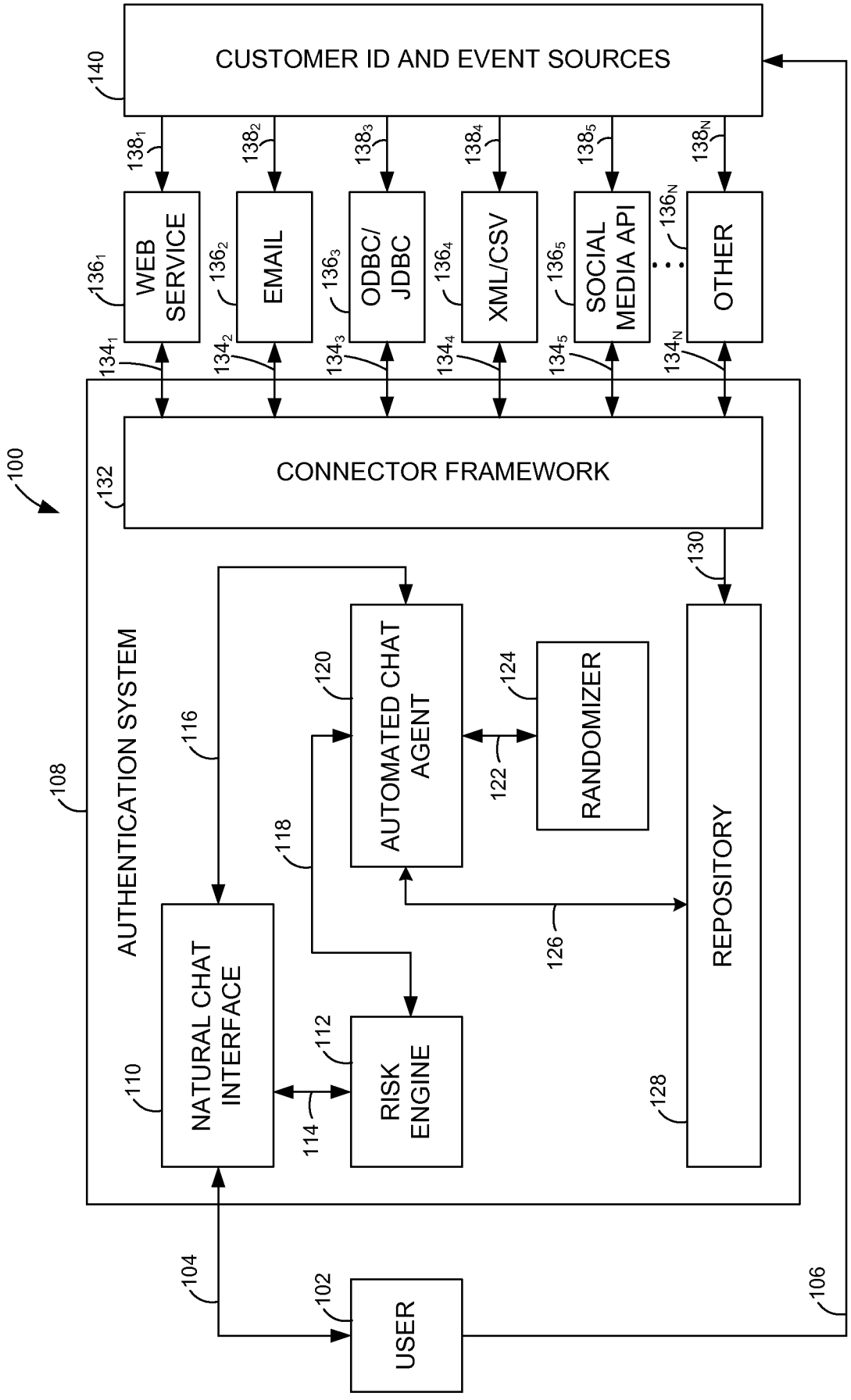
CUSTOMER ID AND EVENT SOURCES
140
138_1
138_2
138_3
138_4
138_5
138_N
WEB SERVICE
EMAIL
ODBC/ JDBC
XML/CSV
SOCIAL MEDIA API
OTHER
136_1
136_2
136_3
136_4
136_5
136_N
134_1
134_2
134_3
134_4
134_5
134_N
CONNECTOR FRAMEWORK
132
100
130
AUTHENTICATION SYSTEM
108
116
120
AUTOMATED CHAT AGENT
124
RANDOMIZER
122
118
REPOSITORY
126
NATURAL CHAT INTERFACE
110
112
RISK ENGINE
114
128
104
102
USER
106

FIG. 1

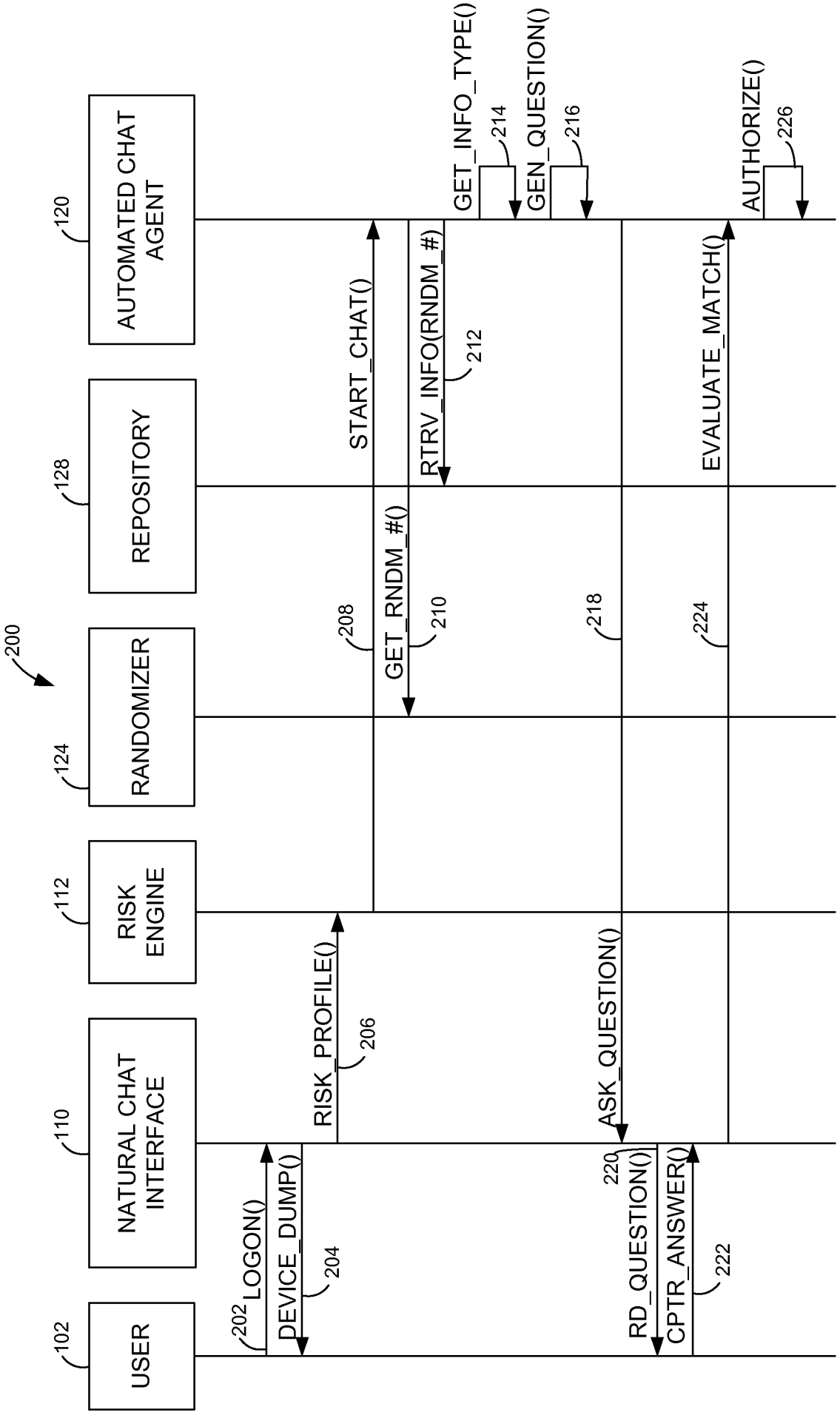
200
USER
102
NATURAL CHAT INTERFACE
110
RISK ENGINE
112
RANDOMIZER
124
REPOSITORY
128
AUTOMATED CHAT AGENT
120
LOGON()
202
DEVICE_DUMP()
204
RISK_PROFILE()
206
GET_RNDM_#()
208
RTRV_INFO(RNDM_#)
210
212
START_CHAT()
GET_INFO_TYPE()
214
GEN_QUESTION()
216
218
ASK_QUESTION()
220
RD_QUESTION()
CPTR_ANSWER()
222
224
EVALUATE_MATCH()
AUTHORIZE()
226

FIG. 2

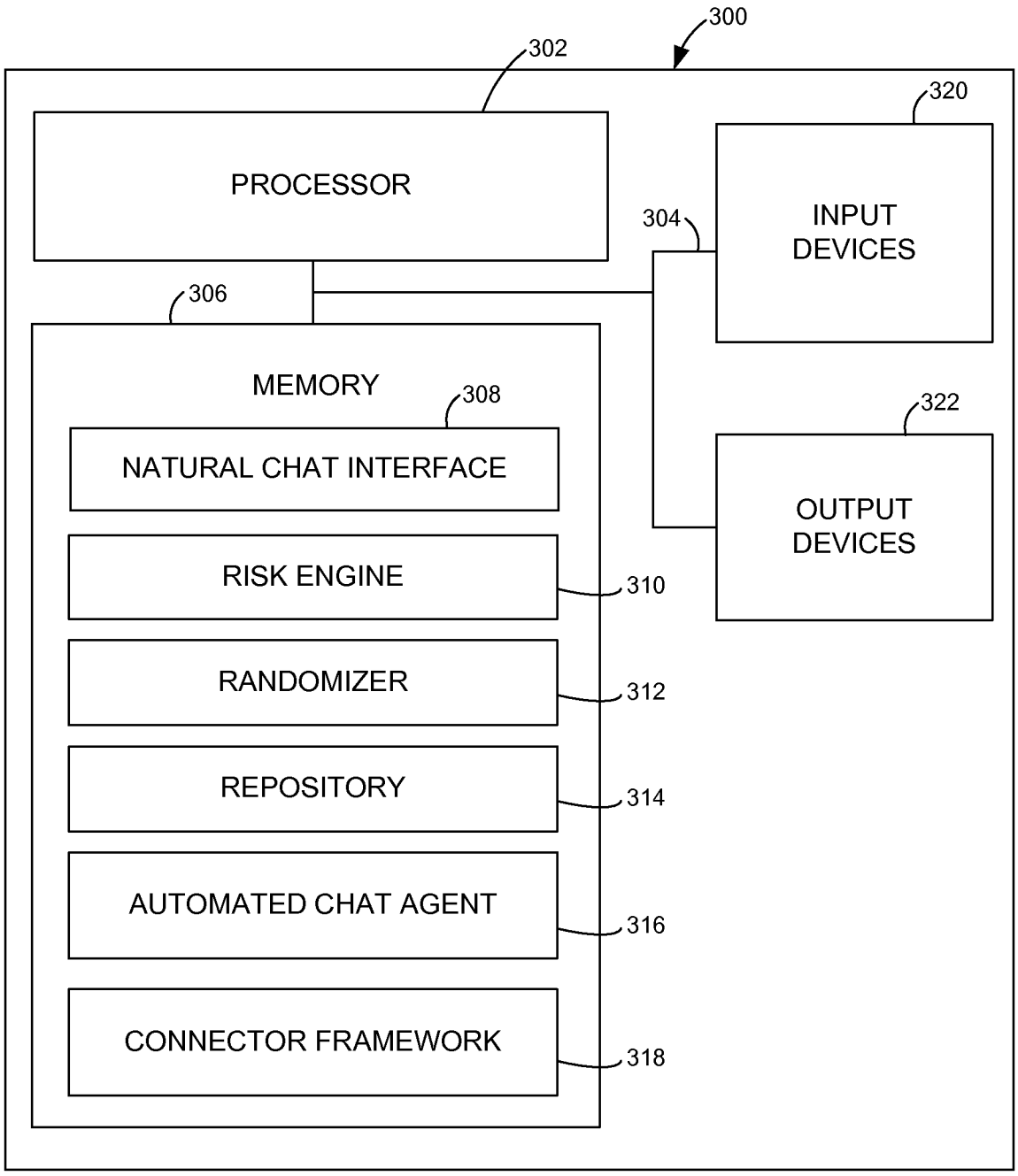
300
302
PROCESSOR
320
INPUT DEVICES
304
306
MEMORY
308
NATURAL CHAT INTERFACE
322
OUTPUT DEVICES
RISK ENGINE
310
RANDOMIZER
312
REPOSITORY
314
AUTOMATED CHAT AGENT
316
CONNECTOR FRAMEWORK
318

FIG. 3

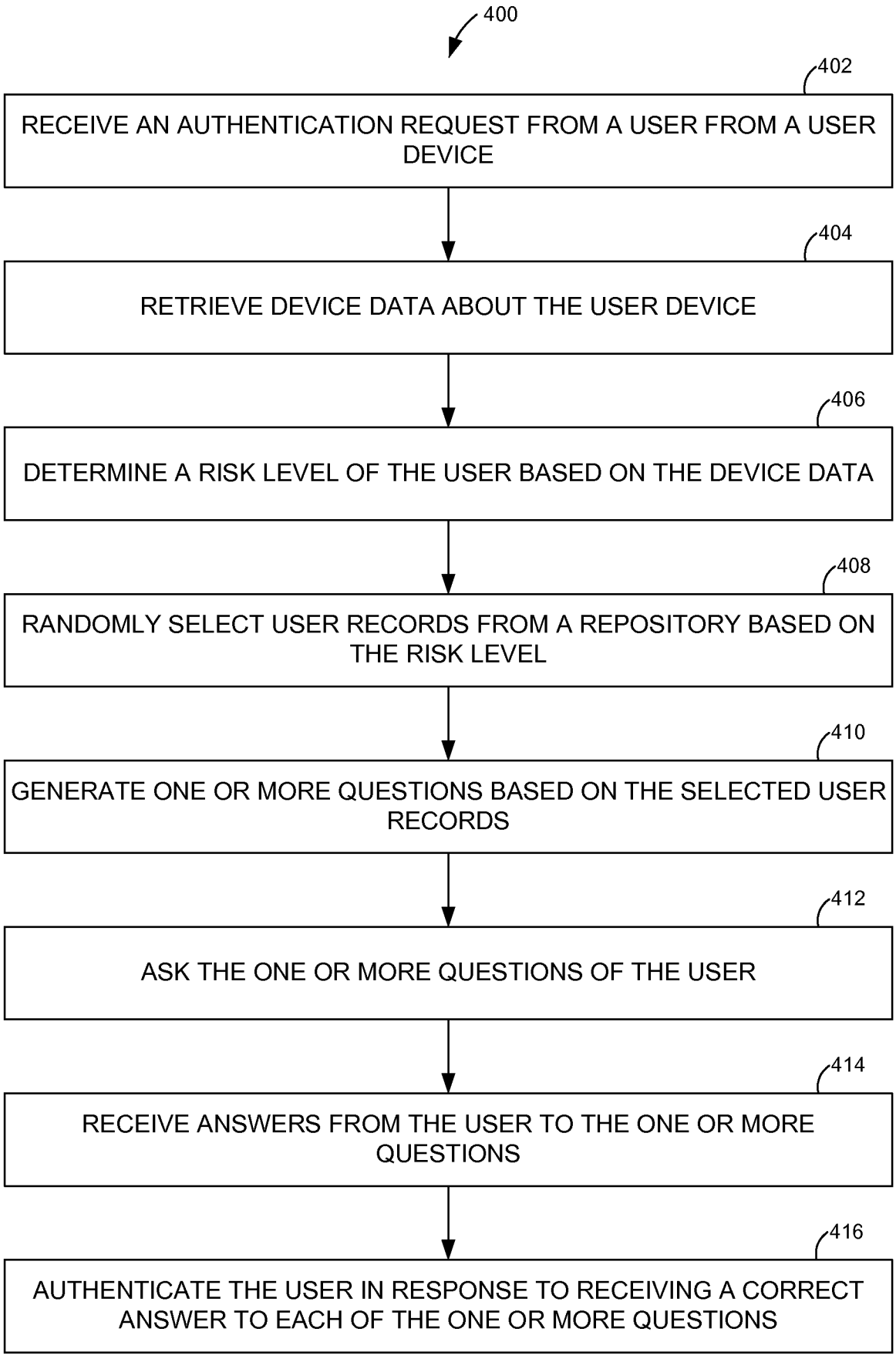
400
402
RECEIVE AN AUTHENTICATION REQUEST FROM A USER FROM A USER DEVICE
404
RETRIEVE DEVICE DATA ABOUT THE USER DEVICE
406
DETERMINE A RISK LEVEL OF THE USER BASED ON THE DEVICE DATA
408
RANDOMLY SELECT USER RECORDS FROM A REPOSITORY BASED ON THE RISK LEVEL
410
GENERATE ONE OR MORE QUESTIONS BASED ON THE SELECTED USER RECORDS
412
ASK THE ONE OR MORE QUESTIONS OF THE USER
414
RECEIVE ANSWERS FROM THE USER TO THE ONE OR MORE QUESTIONS
416
AUTHENTICATE THE USER IN RESPONSE TO RECEIVING A CORRECT ANSWER TO EACH OF THE ONE OR MORE QUESTIONS

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/012895

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/31(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F 21/31; G06F 21/40; G06F 21/20; H04L 9/32; H04L 29/06; G08B 23/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords:authenticate, risk level, question, answer, normalize

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008-0086759 A1 (CHRISTEN J. COLSON) 10 April 2008 See paragraphs [0001], [0011], [0023]-[0027], [0035]-[0040], [0047]-[0057], [0065]-[0066], [0108], [0114], [0121]-[0125]; and figure 2.	1-3,6,8-12,14-15
Y		4-5,7,13
Y	US 2014-0282977 A1 (SOCURE INC.) 18 September 2014 See paragraphs [0038], [0045], [0049]; and figure 1.	4-5,7,13
A	US 2014-0189835 A1 (PITNEY BOWES INC.) 03 July 2014 See paragraphs [0035]-[0037]; and figure 3.	1-15
A	EP 2369523 A1 (DAON HOLDINGS LIMITED) 28 September 2011 See paragraphs [0005], [0133]-[0134]; and figure 10.	1-15
A	US 8856894 B1 (CONSUMERINFO.COM, INC.) 07 October 2014 See column 11, line 34 - column 12, line 4; and figure 2.	1-15

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

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 October 2015 (22.10.2015)	**23 October 2015 (23.10.2015)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea
Facsimile No. +82-42-472-7140

Authorized officer
LEE, Dong Yun
Telephone No. +82-42-481-8734

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2015/012895

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0086759 A1	10/04/2008	CA 2664510 A1	17/04/2008
		EP 2074513 A2	01/07/2009
		EP 2074513 A4	29/02/2012
		US 2012-266227 A1	18/10/2012
		US 8239677 B2	07/08/2012
		US 8793777 B2	29/07/2014
		WO 2008-045667 A2	17/04/2008
		WO 2008-045667 A3	25/09/2008
US 2014-0282977 A1	18/09/2014	WO 2014-145431 A1	18/09/2014
US 2014-0189835 A1	03/07/2014	None	
EP 2369523 A1	28/09/2011	AU 2011-201164 A1	06/10/2011
		CA 2734206 A1	22/09/2011
		US 2011-0231911 A1	22/09/2011
		US 2013-212640 A1	15/08/2013
		US 8826030 B2	02/09/2014
US 8856894 B1	07/10/2014	None	