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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
01 November 2018 (01.11.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/200129 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *G06F 21/32* (2013.01)

(21) International Application Number:
PCT/US2018/025586

(22) International Filing Date:
30 March 2018 (30.03.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/496,451 25 April 2017 (25.04.2017) US

(71) Applicant: **T-MOBILE USA, INC.** [US/US]; 12920 SE 38th Street, Bellevue, Washington 98006-1350 (US).

(72) Inventor: **OBAIDI, Ahmad Arash**; c/o T-Mobile USA, Inc., 12920 SE 38th Street, Bellevue, Washington 98006-1350 (US).

(74) Agent: **ABDALLA, Nabil A.**; Han Santos, PLLC, 500 Union Street, Suite 800, Seattle, Washington 98101 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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.

(54) Title: MULTI-FACTOR AND CONTEXT SENSITIVE BIOMETRIC AUTHENTICATION SYSTEM

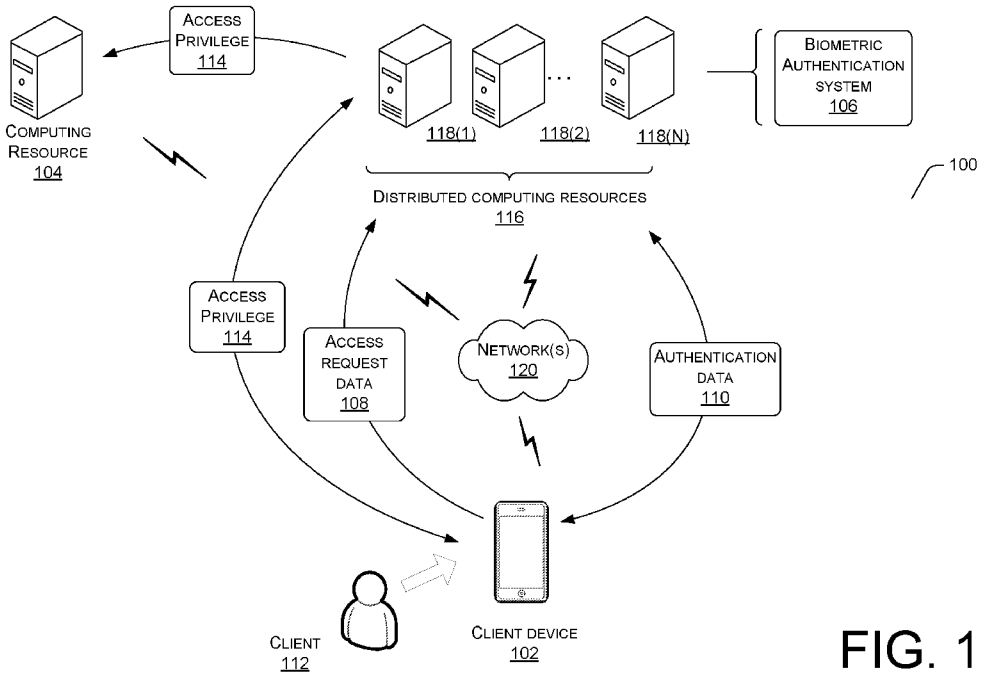

FIG. 1

(57) Abstract: This disclosure describes techniques that facilitate granting an access privilege to a client device based on selectively authenticating biometric data. Particularly, a biometric authentication system may generate an authentication policy that authenticates a client identity via biometric authentication protocols. The authentication policy may be based on a security policy of the computing resource associated with the access privilege. The biometric authentication protocols may be based on a kinematic behavior, body chemistry, or physical features of the client. Each biometric authentication protocol may be assigned an authentication score that reflects a confidence that a biometric sample used to gain an access privilege does in fact correspond to the client. Further, an authentication policy may include a random selection of biometric authentication protocols that comply with a security policy of the computing resource. An authentication policy may be further based on a client disposition, environmental conditions of the client device, or both.

WO 2018/200129 A1

[Continued on next page]

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

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

MULTI-FACTOR AND CONTEXT SENSITIVE BIOMETRIC AUTHENTICATION SYSTEM

BACKGROUND

[0001] An authentication of an individual via a biometrics can be particularly based on a measurement of one or more biometric samples. However, at times, environmental conditions or a disposition of a client can make it difficult to process biometrics because of ambient light conditions, noise level, temperature, or moisture. That is, a biometric authentication protocol that is premised on authenticating an image of a client iris, facial profile, or finger-print may be difficult to capture in a brightly lit or a dimly lit environment. Similarly, a biometric authentication protocol that is premised on voice recognition of a client may be difficult to capture in a noise filled environment.

[0002] Accordingly, an effectiveness of a biometric authentication protocol may be constrained by the environmental conditions surrounding the client device that is capturing a biometric sample.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] The detailed description is set forth with reference to the accompanying figures. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The use of the same reference numbers in different figures indicates similar or identical items or features.

[0004] FIG. 1 illustrates a schematic view of a computing environment that facilitates granting a client device with an access privilege to a computing resource based on selectively authenticating biometric data received from the client device.

[0005] FIG. 2 illustrates a block diagram of a biometric authentication system that facilitates authenticating a client identity by selectively processing biometric samples received from a client device.

[0006] FIG. 3 illustrates a block diagram of a client device that facilitates authenticating a client identity by selectively collecting and transmitting client biometric samples to the biometric authentication system.

[0007] FIG. 4 illustrates a biometric authentication system process that authenticates a client identity via one or more biometric authentication protocols configured to comply with a security policy of a computing resource.

[0008] FIG. 5 illustrates a biometric authentication system process that generates an authentication policy based on a context of operation and environmental conditions of the client device.

[0009] FIG. 6 illustrates a biometric authentication system process for obtrusively and unobtrusively generating a registered biometric template for a biometric authentication protocol.

DETAILED DESCRIPTION

[0010] This disclosure describes techniques that facilitate granting a client device with an access privilege to a computing resource based on selectively authenticating biometric data received from the client device. Particularly, a biometric authentication system may generate an authentication policy that authenticates a client identity via one or more biometric authentication protocols. The authentication policy may be based at least in part on a security policy associated with the computing resource to which the client device has requested an access privilege. The biometric authentication system may be configured to automate and streamline access to computing resource, based on obtrusively and unobtrusively gathering

biometric samples of a client requesting access to a computing resource. By automating and streamlining access to such computing resources, the biometric authentication system may reduce an overall volume of communications between a client device and the underlying computing resource, which in turn may translate into a network bandwidth efficiency for the underlying computing resource.

[0011] In various examples, a biometric authentication system may authenticate a client identity via one or more biometric authentication protocols configured to comply with a security policy of a computing resource. The biometric authentication protocols may be based on a kinematic behavior of the client, body chemistry of the client, or physical features of the client. Kinematic behavior may correspond to a gait profile of the client, a finger-smear pattern on a user interface of the client device, or a grip configuration of a client device that corresponds to a relative position of fingers of the client while holding the client device. Similarly, biometric authentication protocols based on a body chemistry of the client may include a scent, smell, odor, heart rate, blood pressure, and skin conductance. Further, physical features of a client may include a facial image profile, a finger-print profile, an iris image profile, or a voice recognition profile.

[0012] Further, each biometric authentication protocol may be assigned an authentication score that reflects a likelihood that a biometric sample used to gain an access privilege to the computing resource, does in fact correspond to a feature of the client. In other words, the authentication score may a reflect a level of confidence that a person other than the client cannot use their own biometric sample to fraudulently gain access to a computing resource via a biometric authentication protocol.

[0013] In some examples, the biometric authentication system may generate an authentication policy by randomly selecting one or more biometric authentication protocols that comply with a security policy of the computing resource. However, at times it may prove difficult to execute

a particular biometric authentication protocol based on a disposition of the client or environmental conditions associated with the client device. In these instances, the biometric authentication system may determine a context of operation and environmental conditions to help select biometric authentication protocols to include in the authentication policy.

[0014] The context of operation may describe a disposition of the client at a time of a request for access to a computing resource. The context of operation may describe whether the client is running, walking, in conversation with one or more individuals, or in a moving vehicle. Additionally, environmental conditions may determine an intensity of light, sound, smell, moisture, and temperature within the environment proximate to the client device. Thus, the environmental conditions may determine whether that the client is in a noise-filled environment, or is located within a bright or dimly lit space.

[0015] In a non-limiting example, the biometric authentication system may determine that a voice-recognition authentication protocol may not be appropriate for a noise-filled environment, or that an image-based authentication protocol may not be appropriate in a brightly lit or dimly lit space. Similarly, a scent-based authentication protocol may not be appropriate in a highly scented environment.

[0016] Additionally, the biometric authentication system may facilitate generating a registered biometric template for a biometric authentication protocol. The biometric authentication system may monitor sensor data associated with the client device during a real-time session of authenticated access to a computing resource. In doing so, the sensor data may be used to refine existing biometric authentication protocols, or generate new biometric authentication protocols. In some examples, one or more sensors associated with the client device may unobtrusively monitor a gait profile of the client, a voice of the client, a scent profile of the client, a heart rate, blood pressure, or skin capacitance.

[0017] The biometric authentication system may also monitor and detect a location and time that a request for an access privilege is received. For example, a client may typically request an access privilege at a particular geographic location, or at particular times of the day, or day of the week. In doing so, the biometric authentication system may selectively modify a security policy of the computing resource to require more stringent biometrical authentication protocols at times when an access privilege is requested at an atypical geographic location, time of day, or day of the week.

[0018] The techniques described herein may be implemented in a number of contexts. Several example implementations and context are provided with reference to the following figures. Further, the term "techniques," as used herein, may refer to system(s), method(s), computer-readable instruction(s), module(s), algorithms, hardware logic, and/or operation(s) as permitted by the context described above and throughout the document.

[0019] FIG. 1 illustrates a schematic view of a computing environment 100 that facilitates granting a client device 102 with an access privilege to a computing resource 104 based on selectively authenticating biometric data received from the client device 102. Particularly, a biometric authentication system 106 may generate an authentication policy that authenticates a client identity via one or more biometric authentication protocols. The authentication policy may be based at least in part on a security policy associated with the computing resource 104 to which the client device 102 has requested access.

[0020] In the illustrated example, the client device 102 may transmit access request data 108 to the biometric authentication system 106, that includes at least a request for access to a computing resource 104. In some examples, the access request data 108 may also include sensor data associated with the client device 102. The sensor data may be used determine a context of operation and environmental conditions associated with the client device 102. Further, the biometric authentication system 106 may generate an authentication policy that

includes one or more biometric authentication protocols, based at least in part on the security policy of the computing resource. In some examples, the authentication policy may be further based at least in part on the context of operation and environmental conditions associated with the client device 102.

[0021] Moreover, the biometric authentication system 106 may communicate authentication data 110 to the client device 102 that includes the authentication policy and computer executable instructions that automatically executes the authentication policy on the client device. In response, the client device 102 may communicate authentication data 110 to the biometric authentication system 106 that includes biometric samples that correspond to the one or more biometric authentication protocols of the authentication policy. In response to authenticating an identity of the client 112, the biometric authentication system 106 may provide the client device 102 with an access privilege 114 for the computing resource 104.

[0022] In the illustrated example, the biometric authentication system 106 may operate on one or more distributed computing resource(s) 116. The one or more distributed computing resource(s) 116 may include one or more computing device(s) 118(1)-118(N) that operate in a cluster or other configuration to share resources, balance load, increase performance, provide fail-over support or redundancy, or for other purposes. The one or more computing device(s) 118(1)-118(N) may include one or more interfaces to enable communications with other networked devices, such as the client device 102, via one or more network(s) 120. Further, the one or more network(s) 120 may include public networks such as the Internet, private networks such as an institutional and/or personal intranet, or some combination of private and public networks. The one or more network(s) 120 can also include any type of wired and/or wireless network, including but not limited to local area network (LANs), wide area networks (WANs), satellite networks, cable networks, Wi-Fi networks, Wi-Max networks, mobile communications networks (e.g. 3G, 4G, and so forth), or any combination thereof.

[0023] Furthermore, the client device 102 may include any sort of electronic device, such as a cellular phone, a smart phone, a tablet computer, an electronic reader, a media player, a gaming device, a personal computer (PC), a laptop computer, etc. The client device 102 may have a subscriber identity module (SIM), such as an eSIM, to identify the client device 102 to a telecommunication service provider network (also preferred to herein as "telecommunication network"). Similarly, the computing resource 104 may correspond to any sort of electronic device, such as one of the one or more computing device(s) 118(1)-118(N) or the client device 102.

[0024] FIG. 2 illustrates a block diagram of a biometric authentication system 202 that facilitates authenticating a client identity by selectively processing biometric samples received from a client device. The biometric authentication system 202 may generate an authentication policy that authenticates a client identity via one or more biometric authentication protocols. In various examples, the biometric authentication protocols may be based on a kinematic behavior of the client, body chemistry of the client, or physical features of the client. The biometric authentication system 202 may select a biometric authentication protocol based on an authentication score of the biometric authentication protocol and a security policy associated with the computing resource. Further, a selection may be further based at least in part on a context of operation of the client device, environment conditions of client device, or a combination of both.

[0025] In the illustrated example, the biometric authentication system 202 may correspond to the biometric authentication system 106. Further the biometric authentication system 202 may include input/output interface(s) 204. The input/output interface(s) 204 may include any type of output interface known in the art, such as a display (e.g. a liquid crystal display), speakers, a vibrating mechanism, or a tactile feedback mechanism. Input/output interface(s) 204 also include ports for one or more peripheral devices, such as headphones, peripheral speakers, or

a peripheral display. Further, the input/output interface(s) 204 may further include a camera, a microphone, a keyboard/keypad, or a touch-sensitive display. A keyboard/keypad may be a push button numerical dialing pad (such as on a typical telecommunication device), a multi-key keyboard (such as a conventional QWERTY keyboard), or one or more other types of keys or buttons, and may also include a joystick-like controller and/or designated navigation buttons, or the like.

[0026] Additionally, the biometric authentication system 202 may include network interface(s) 206. The network interface(s) 206 may include any sort of transceiver known in the art. For example, the network interface(s) 206 may include a radio transceiver that performs the function of transmitting and receiving radio frequency communications via an antenna. In addition, the network interface(s) 206 may also include a wireless communication transceiver and a near field antenna for communicating over unlicensed wireless Internet Protocol (IP) networks, such as local wireless data networks and personal area networks (e.g. Bluetooth or near field communication (NFC) networks). Further, the network interface(s) 206 may include wired communication components, such as an Ethernet port or a Universal Serial Bus (USB).

[0027] Further, the biometric authentication system 202 may include one or more processor(s) 208 that are operably connected to memory 210. In at least one example, the one or more processor(s) 208 may be a central processing unit(s) (CPU), graphics processing unit(s) (GPU), a both a CPU and GPU, or any other sort of processing unit(s). Each of the one or more processor(s) 208 may have numerous arithmetic logic units (ALUs) that perform arithmetic and logical operations as well as one or more control units (CUs) that extract instructions and stored content from processor cache memory, and then executes these instructions by calling on the ALUs, as necessary during program execution. The one or more processor(s) 208 may also be responsible for executing all computer applications stored in the memory, which can be associated with common types of volatile (RAM) and/or nonvolatile (ROM) memory.

[0028] In some examples, memory 210 may include system memory, which may be volatile (such as RAM), non-volatile (such as ROM, flash memory, etc.) or some combination of the two. The memory may also include additional data storage devices (removable ad/or non-removable) such as, for example, magnetic disks, optical disks, or tape.

[0029] The memory 210 may further include non-transitory computer-readable media, such as volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules, or other data. System memory, removable storage and non-removable storage are all examples of non-transitory computer-readable media. Examples of non-transitory computer-readable media include, but are not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other non-transitory medium which can be used to store the desired information.

[0030] In the illustrated example, the memory 210 may include an operating system 212, a biometric authentication application 214, a computing resource security policy data store 216, and a client profile data store 218. The operating system 212 may be used to implement the biometric authentication application 214. The operating system 212 may be any operating system capable of managing computer hardware and software resources. The biometric authentication application 214 may include routines, program instructions, objects, and/or data structures that perform particular tasks or implement particular abstract data types.

[0031] The biometric authentication application 214 may include a sensor data processing module 220, a pattern matching module 222, a registered template module 224, an authentication protocol module 226, a location module 228, and a user interface 230. The sensor data processing module 220 may receive and process sensor data associated with one or

more sensors of the client device. Further, the sensor data processing module 220 may determine a context of operation of the client device and environmental conditions that are within a predetermined proximity of the client device. The context of operation of a client device may be associated with the disposition of the client at a time of the request for access to a computing resource. The context of operation may describe whether the client is running, walking, in conversation with one or more individuals, or in a moving vehicle. In some examples, a combination of sensor data may be used to describe a context of operation. For example, the sensor data processing module 220 may use sensor data from a GPS sensor, one or more accelerometers, and a proximity sensor to determine that short-wave pendulum oscillations suggest that the client device is being carried by the client while running. Additionally, environmental conditions that may affect the selection and execution of a biometric authentication protocol. For example, the biometric authentication system may determine that the client is in a noise-filled environment, or is located within a bright or dimly lit space. In a non-limiting example, the sensor data processing module 220 may determine an ambient light intensity, ambient noise-level, and an ambient temperature, based on sensor data from an ambient light sensor, a microphone sensor, or thermal sensor.

[0032] In other examples, the sensor data processing module 220 may also interpret biometric samples received from a client via the client device. In one example, a biometric sample may include a grip configuration may include the relative position of fingers when holding and touching the mobile device. In other examples, the biometric sample may include a scent or odor of a client, facial image of a client, or a hand thermogram. Further, a facial biometric sample may include a facial thermogram that measures a heat signature of a client' facial region. A heat signature may be limited to features associated with a client's earlobe or lips, which is commensurate with regions of a client's face that the client device is likely to overlap.

Other biometric samples, particularly body chemistry samples, may include vascular biometrics such as blood pressure and heart rate.

[0033] Further, some biometric samples may be obtained from a client using an unobtrusive process, and thus captured without distracting the client. For example, detecting an image of the user's face, heat beat patterns (or rhythms in heart rate), odor or pheromone may be captured without first drawing the client's attention.

[0034] Moreover, the pattern matching module 222 may compare a biometric sample from a client device with a registered biometric template. The pattern matching module 222 may use statistically reliable pattern matching techniques to ensure that biometric samples received from a client device, reliably match a registered biometric template. For example, the pattern matching module 222 may determine a similarity between a biometric sample and a registered biometric template. Authentication of a client identity may be based at least in part on the similarity being greater than a predetermined similarity threshold. The predetermined similarity threshold may be specified within the security policy of the computing resource or within the authentication policy that is transmitted to the client device.

[0035] Additionally, the registered template module 224 may generate statistical pattern-matching templates that can be used as registered biometric templates for the purpose biometric authentication. In some examples, a client may proactively generate a registered biometric template based on a selected biometric authentication protocol. In other examples, a registered biometric template may be generated unobtrusively by monitoring client features and posture during real-time sessions of authenticated access to a computing resource. A registered biometric template may model physical features of the client, such as a facial image profile, a finger-print profile, an iris image profile, or a voice recognition profile of client. Further, a registered biometric template may also model a kinematic behavior of a client, such as a gait profile of the client, a finger-smear pattern on a user interface of the client device, or a grip

configuration of a client device that corresponds to a relative position of fingers of the client while holding the client device. Additionally, or alternatively, the registered biometric templates may model body chemistry of the client such as, a scent, a smell, an odor, a heart rate, a blood pressure, and a skin conductance of the client.

[0036] The registered template module 224 may generate a registered biometric template by receiving a repeated number of a same type of biometric sample. The repetition allows for a construction of a statistically reliable template.

[0037] Further, the authentication protocol module 226 may generate an authentication policy for access to a computing resource. In various examples, the authentication policy may include one or more biometric authentication protocols, based at least in part on the security policy of the computing resource. It is noteworthy that a biometric authentication protocol comprises of a request for a particular biometric sample, using a particular sensor of the client device, that may be compared with a particular a registered biometric template. For example, a biometric authentication protocol for a scent profile of client may request sensor data from an olfactory sensor of a client device for the purpose of determining a similarity of the biometric sample with a registered scent-based biometric template of the client.

[0038] Moreover, the authentication protocol module 226 may selectively incorporate one or more biometric authentication protocols into the authentication policy based at least in part on the authentication scores of the biometric authentication protocols and a requisite authentication score of the security policy. In a non-limiting example, the authentication protocol module 226 may select a biometric authentication protocol with an authentication score that is greater than the requisite authentication score of the security policy. Alternatively, the authentication protocol module 226 may select a plurality of biometric authentication protocols that in combination generate a total authentication score that is greater than the requisite authentication score of the security policy. In another example, consider a first and

second biometric authentication protocol, each of which retain an authentication score that is less than the requisite authentication score of the security policy. In this example, the authentication protocol module 226 may select the first and second biometric authentication protocols, in combination, on the basis that a sum of the respective authentication scores may be greater than the requisite authentication score of the security policy. Additionally, the authentication protocol module 226 may select a plurality of biometric authentication protocols, whereby each biometric authentication protocol has an authentication score that is greater than the requisite authentication score of the security policy.

[0039] Additionally, authentication protocol module 226 may configure an authentication policy such that each biometric authentication protocol of a plurality of biometric authentication protocols may be executed in sequential order. Alternatively, or additionally, one or more biometric authentication protocols may periodically authenticate a client identity during a session of authenticated access to the computing resource. In this example, a client may be required to selectively authenticate their identity via the one or more biometric authentication protocols in order to maintain access to the computing resource.

[0040] Further, the location module 228 may obtain location data associated with a client device. The location data may be obtained using a Global Positioning System (GPS) sensor, cell tower triangulation, or any other manner that may identify a physical location of a client device.

[0041] Moreover, the user interface 230 may facilitate generating a security policy associated with a computing resource. In one example, a service provider or a client may generate a security policy that is associated with a computing resource. The user interface 230 may also facilitate generating a registered biometric template that may be used to generate an authentication policy. In some examples, the user interface 230 may interact with one or more

sensors of the client device for the purpose of capturing a predetermined number biometric samples from the client device.

[0042] Additionally, the computing resource security policy data store 216 may store the security policies associated with each computing resource. Each security policy may include an indication of a requisite authentication score for biometric authentications protocols that control access to the computing resource. The requisite authentication score may be assigned by one of a service provider or client, whomever retains ownership or control over the computing resource. For example, the requisite authentication score for a security policy that authenticates access to a service provider computing platform may be determined by the service provider. Alternatively, a requisite authentication score of a security policy that protects client personal data on a client device may be determined by the client.

[0043] Further, the client profile data store 218 may store the registered biometric templates associated with the client, along with assigned authentication scores. Additionally, the client profile data store 218 may include metadata that describes a geographic location, time of day, or day of the week for particular registered biometric template. For example, a client scent profile may be associated with a client for conditions when the client is running in an environment having a particular ambient temperature.

[0044] FIG. 3 illustrates a block diagram of a client device 302 that facilitates authenticating a client identity by selectively collecting and transmitting client biometric samples to the biometric authentication system 202. The client device 302 may correspond to the client device 102. Further, the client device 302 may include network interface(s) 304 and input/output interface(s) 306 that correspond to network interface(s) 206 and input/output interface(s) 204.

[0045] Additionally, the client device 302 may include one or more processor(s) 308 operably connected to memory 310. The one or more processor(s) 308 may correspond to the one or more processor(s) 208, and the memory 310 may correspond to the memory 210.

[0046] In the illustrated example, the memory 310 may include an operating system 312 and a biometric authentication application 314. The operating system 312 may be used to implement the biometric authentication application 314. The operating system 312 may be any operating system capable of managing computer hardware and software resources. The biometric authentication application 314 may include routines, program instructions, objects, and/or data structures that perform particular tasks or implement particular abstract data types.

[0047] Moreover, the biometric authentication application 314 may be configured to communicate biometric data with the biometric authentication system 202. In some examples, the biometric authentication application 314 may be configured to perform the computational processing that is associated with the one or more modules of the biometric authentication system 202, such as the biometric authentication application 214. In some examples, the memory 310 may include a data store that corresponds to the client profile data store 218, the computing resource security policy data store 216, or both.

[0048] Further, the client device may include sensor(s) 316, such as accelerometer(s) 318, proximity sensor(s) 320, digital camera(s) 322, GPS sensor(s) 324, biometric sensor(s) 326, and environmental sensor(s) 328. The one or more accelerometer(s) 318 may be offset from one another in each of the three translational planes. Doing so allows for a calculation of a change in angular orientation of the client device 302. Further, the one or more accelerometer(s) 318 may also measure a vibration or oscillation of the client device 302. In some examples, a measured vibration or oscillation may be used to identify a particular template of movement, such as running, walking, or movement within a vehicle. For example, short-wave pendulum oscillations may suggest that the client device 302 is being held while

running, while long-wave pendulum oscillations may suggest that the client device 302 is being held while walking.

[0049] Further, proximity sensor(s) 320 and/or digital camera(s) 322 may be used to measure a movement of the client device along a particular axis. In some examples, the proximity sensor(s) 320 may be used to detect stationary, open, or enclosed areas. For example, detecting a stationary area may correspond to a lack of movement of the client device 302. Additionally, the digital camera(s) 322 may record low resolution imagery at a high frame rate that is greater than typical video production. In doing so, imagery may be analyzed to quantify a movement of the client device 302 along a particular axis, or axes.

[0050] The GPS sensor(s) 324 may be used to determine a geolocation of the client device 302. In some examples, the geographic location of the client device 302 may be used to enable or disable particular biometric authentication protocols. In a non-limiting example, the GPS sensor(s) 324 may determine that the client device 302 is located at or near a work location or a home location of the client. In doing so, the biometric authentication system 202 may elect to enable particular biometric authentication protocols that rely registered biometric templates created at the work location or the home location of the client, such as odor-based biometric templates.

[0051] Environmental sensor(s) 328, such as an ambient light sensor, noise-level sensor, temperature-sensor, and a moisture sensor. In various examples, the environmental sensor(s) 328 may be used to detect environmental conditions associated with the client device 302 at a time that biometrical authentication protocols are to be executed. The environmental sensor(s) 328 may detect an ambient light intensity, an ambient noise-level, an ambient temperature, and an ambient humidity that surrounds the client device 302. Sensor data from the environmental sensor(s) 328 may be transmitted to the biometric authentication system 202 to enable a selection of one or more biometric authentication protocols. For

example, sensor data from noise-level sensors that detect a noise-filled environment may suggest that a voice-recognition biometric authentication profile may not be appropriate.

[0052] Further, the biometric sensor(s) 326 that may capture a biometric sample of a client may include digital camera(s), a microphone sensor, a capacitance sensor, an odor sensor, a heart-rate sensor, and a thermal sensor. For example, the digital camera(s) 322 may detect physical features of a client, such as physical features of the client, such as a facial image profile, a finger-print profile, an iris image profile. The microphone sensor may detect a voice recognition associated with the client. The voice print may include an accent, tonality, refraction of sound, frequency and pitch of the client voice. The capacitance sensor may detect a grip configuration of a client holding the client device 302. In this example, a biometric sample may comprise of the relative position of fingers when holding and touching the client device 302. The odor sensor may detect a smell, scent, or odor associated with the client. In some examples, the odor sensor may detect a smell, scent, or odor within a particular region of the client body, such as a side of the head, or adjacent to an eye lobe. In other examples, the odor sensor may detect a general smell, scent, or odor that is within a predetermined distance of the client body. Further, the heart-rate sensor may detect a heart rate of the client, and the thermal sensor may generate a thermogram of a client hand, face, or other body part.

[0053] FIGS. 4, 5, and 6 present processes 400, 500, and 600 that relate to operations of the biometric authentication system, and more specifically generating and executing an authentication policy. Each of processes 400, 500, and 600 illustrate a collection of blocks in a logical flow chart, which represents a sequence of operations that can be implemented in hardware, software, or a combination thereof. In the context of software, the blocks represent computer-executable instructions that, when executed by one or more processors, perform the recited operations. Generally, computer-executable instructions may include routines, programs, objects, components, data structures, and the like that perform particular functions

or implement particular abstract data types. The order in which the operations are described is not intended to be construed as a limitation, and any number of the described blocks can be combined in any order and/or in parallel to implement the process. For discussion purposes, the processes 400, 500, and 600 are described with reference to the computing environment 100 of FIG. 1.

[0054] FIG. 4 illustrates a biometric authentication system process that authenticates a client identity via one or more biometric authentication protocols configured to comply with a security policy of a computing resource. The biometric authentication protocols may be based on a kinematic behavior of the client, body chemistry of the client, or physical features of the client. For example, a kinematic behavior may correspond to a gait profile of the client, a finger-smear pattern on a user interface of the client device, or a grip configuration of a client device that corresponds to a relative position of fingers of the client while holding the client device. In some examples, biometric authentication protocols based on a body chemistry of the client may include, but are not limited to, scent, smell, odor, heart rate, blood pressure, and skin conductance. A client device may be equipped with one or more body chemistry sensors that capture body biometric samples of the client. In some instances, biometric samples may be captured unobtrusively, while in other instances, a client may engage with a user interface of the client device. Further, physical features of a client may include, but are not limited to, a facial image profile, a finger-print profile, an iris image profile, or a voice recognition profile.

[0055] Further, each biometric authentication protocol may be assigned an authentication score that reflects a likelihood that a biometric sample used to gain an access privilege to the computing resource, does in fact correspond to a feature of the client. In other words, the authentication score may a reflect a level of confidence that a person other than the client cannot use their own biometric sample to fraudulently gain access to a computing resource via a biometric authentication protocol.

[0056] In a non-limiting example, the authentication score may comprise of a numerical value that reflects the likelihood that the biometric sample used to gain an access privilege to the computing resource does in fact correspond to a feature of the client. The authentication score may vary from a value that reflects a least secure biometric authentication protocol condition to a most secure biometric authentication protocol. A least secure biometric authentication protocol may reflect a condition whereby a counterfeit biometric sample may provide access privilege to a computing resource. Further, the most secure authentication protocol may reflect a condition whereby a counterfeit biometric sample is unlikely to provide an access privilege to the computing resource.

[0057] At 402, the biometric authentication system may receive from a client device, a request to access a computing resource. In various examples, the computing resource may correspond to a software application that is installed on the client device. In other examples, the computing resource may be stored on a remote server that is accessed via one or more communications networks.

[0058] At 404, the biometric authentication system may identify a security policy that is associated with the computing resource. In some examples, the security policy may be stored within a data store of the biometric authentication system. Further, the security policy may include a requisite authentication score for biometric authentication protocols that control access to the computing resource. The requisite authentication score may be assigned by one of a service provider or client, whomever retains ownership or control over the computing resource. For example, the requisite authentication score for a security policy that authenticates access to a service provider computing platform may be determined by the service provider. Alternatively, a requisite authentication score of a security policy that protects client personal data on a client device may be determined by the client.

[0059] At 406, the biometric authentication system may generate an authentication policy that includes one or more biometric authentication protocols, based at least in part on the security policy of the computing resource. In a non-limiting example, the biometric authentication system may select a biometric authentication protocol with an authentication score that is greater than a requisite authentication score associated with the security policy. Alternatively, the biometric authentication system may select a plurality of biometric authentication protocols that in combination generate a total authentication score that is greater than the requisite authentication score associated with the security policy. For example, consider a first and second biometric authentication protocol, each of which retain an authentication score that is less than the requisite authentication score of the security policy. In this example, the biometric authentication system may select the first and second biometric authentication protocols, in combination, on the basis that a sum of the respective authentication scores may be greater than the requisite authentication score of the security policy.

[0060] Further, the biometric authentication system may select a plurality of biometric authentication protocols, whereby each biometric authentication protocol has an authentication score that is greater than the requisite authentication score of the security policy. In one example, each biometric authentication protocol may be executed in sequential order. Alternatively, or additionally, one or more biometric authentication protocols may periodically authenticate a client identity during a session of authenticated access to the computing resource. In this example, a client may be required to selectively authenticate their identity via the one or more biometric authentication protocols in order to maintain access to the computing resource.

[0061] At 408, the biometric authentication system may transmit to the client device, a data packet that includes the authentication policy for access to the computing resource. In some examples, the data packet may include computer executable instructions that automatically

execute the one or more biometric authentication protocols of the authentication policy, on the client device.

[0062] At 410, the biometric authentication system may receive one or more biometric samples associated with the one or more biometric authentication protocols. In various examples, the one or more biometric samples may correspond to a kinematic behavior of the client, a body chemistry of the client, or physical features of the client.

[0063] At 412, the biometric authentication system may authenticate a client identity associated with the client device, based at least in part on the one or more biometric samples. The biometric authentication system may selectively compare each biometric sample with a registered biometric template that corresponds to the biometric authentication protocol. For example, the biometric authentication system may receive a biometric sample that corresponds to a finger-print or a voice recognition of a client. In doing so, the biometric authentication system may access registered biometric templates that corresponds to the finger-print or the voice recognition of the client.

[0064] At 414, the biometric authentication system may provide the client device with access to the computing resource based at least in part on authenticating the identity of the client. In some examples, an authentication of a client identity may be based at least in part on a similarity of the biometric sample and the registered biometric template being greater than a predetermined similarity threshold. The predetermined similarity threshold may be specified within the security policy of the computing resource or within the authentication policy that is transmitted to the client device.

[0065] FIG. 5 illustrates a biometric authentication system process that generates an authentication policy based on a context of operation and environmental conditions of the client device. In some examples, the biometric authentication system may generate an authentication policy by randomly select one or more biometric authentication protocols that comply with a

security policy of the computing resource. However, at times it may prove difficult to execute a particular biometric authentication protocol based on a disposition of the client or environmental conditions associated with the client device. In these instances, the biometric authentication system may determine a context of operation and environmental conditions to help select biometric authentication protocols to include in the authentication policy.

[0066] The context of operation may describe a disposition of the client at a time of a request for access to a computing resource. The context of operation may describe whether the client is running, walking, in conversation with one or more individuals, or in a moving vehicle. Additionally, environmental conditions may determine an intensity of light, sound, smell, moisture, and temperature within the environment proximate to the client device. Thus, the environmental conditions may determine whether that the client is in a noise-filled environment, or is located within a bright or dimly lit space.

[0067] In a non-limiting example, the biometric authentication system may determine that a voice-recognition authentication protocol may not be appropriate for a noise-filled environment, or that an image-based authentication protocol may not be appropriate in a brightly lit or dimly lit space. Similarly, a scent-based authentication protocol may not be appropriate in a highly scented environment.

[0068] At 502, the biometric authentication system may receive from a client device, a data packet that includes a request to access a computing resource and sensor data associated with the client device. The computing resource may correspond to a software application that is installed on the client device. In other examples, the computing resource may be stored on a remote server that is accessed via one or more communications networks.

[0069] Further, the sensor data may indicate a particular type of motion of a client associated with the client device, such walking or running, or a particular geographic location, such as a home location or a work location. In some examples, the one or more sensors that detect a

movement of the client device may include accelerometer(s), proximity sensor(s), gyroscope(s), digital camera(s), or global positioning system (GPS) sensor(s).

[0070] Similarly, sensor data may indicate environmental conditions within a predetermined proximity of the client device, such as an ambient light intensity, ambient noise-level, and an ambient temperature. In some examples, the one or more sensors that detect environmental conditions may include an ambient light sensor, a microphone sensor, or thermal sensor.

[0071] At 504, the biometric authentication system may identify a security policy that is associated with the computing resource. In some examples, the security policy may be stored within a data store of the biometric authentication system. In other examples, the security policy may be stored within a remote server of the service provider and selectively accessed at each instance of authentication.

[0072] At 506, the biometric authentication system determine a context of operation and environmental conditions associated with the client device, based at least in part on the sensor data. For example, the sensor data may determine various environmental conditions associated with the client device. For example, sensor data from a global position system (GPS) sensor and one or more accelerometer(s) may approximate a movement of the client device, and further determine whether the client is stationary, walking, running, or in a moving vehicle. Further, sensor data from a proximity sensor may determine whether the client device is likely stored in an enclosed area, such as a client's bag or a client's waist pocket. Moreover, a combination of sensor data from a GPS sensor, one or more accelerometers, and proximity sensor may determine that short-wave pendulum oscillations suggest that the client device is being carried by the client while walking.

[0073] Similarly, sensor data may also determine environmental conditions within a predetermined proximity of the client device. For example, a microphone sensor may determine whether the client device is in a noise-filled space or a quiet space, an ambient light

sensor may determine whether the client is in a brightly lit or dimly lit space, and an ambient temperature sensor may determine an ambient environmental temperature that proximate to the client device.

[0074] At 508, the biometric authentication system may generate an authentication policy that includes one or more biometric authentication protocols, based at least in part on the security policy of the computing resource, and the context of operation and environmental conditions associated with the client device. For example, the biometric authentication system may identify a set of biometric authentication protocols that comply with the security policy of the computing resource. Further, the biometric authentication system may determine a movement of a client and environmental conditions surrounding the client to select an appropriate biometric authentication protocol from the set of biometric authentication protocols.

[0075] For example, sensor data that indicates that the client device is located in a noise-filled space may cause the biometric authentication system select a biometric authentication protocol other than one associated with a voice recognition profile. Similarly, sensor data that indicates that the client device is being accessed while walking or running may cause the biometric authentication system to avoid image-based biometric authentication protocols that may capture stuttering images. Additionally, sensor data that indicates that the client device is located in a highly-scented space, or that the client is wearing an overpowering perfume or fragrance may cause the biometric authentication protocol to selectively avoid including a scent-based biometric authentication protocol within the authentication policy.

[0076] At 510, the biometric authentication system may transmit to the client device, a second data packet that automatically executes the one or more biometric authentication protocols on the client device. In some examples, each biometric authentication protocol may be executed in sequential order. Alternatively, or additionally, one or more biometric authentication protocols may periodically authenticate a client identity during a session of authenticated

access to the computing resource. In this example, a client may be required to selectively authenticate their identity via the one or more biometric authentication protocols in order to maintain access to the computing resource.

[0077] FIG. 6 illustrates a biometric authentication system process for obtrusively or unobtrusively generating a registered biometric template for a biometric authentication protocol. The biometric authentication system may monitor sensor data associated with the client device during a real-time session of authenticated access to a computing resource. In doing so, the sensor data may be used to refine existing biometric authentication protocols, or generate new biometric authentication protocols. In some examples, one or more sensors associated with the client device may unobtrusively monitor a gait profile of the client, a voice of the client, a scent profile of the client, a heart rate, blood pressure, or skin capacitance of the client.

[0078] In some examples, the biometric authentication system may generate a plurality of client profiles for a particular biometric authentication protocol. Each client profile may be based on biometric samples captured at different geographic locations, times of the day, days of the week, or detected movements of the client device. For example, the biometric authentication system may generate a first scent profile for a client for occasions that the client is inactive, a second scent profile for occasions that the client is walking, and a third scent profile for occasions that the client is running.

[0079] The biometric authentication system may also monitor and detect a location and time that a request for an access privilege is received. For example, a client may typically request an access privilege at a particular geographic location, or at particular times of the day, or day of the week. In doing so, the biometric authentication system may selectively modify a security policy of the computing resource to require more stringent biometrical authentication protocols

at times when a request for an access privilege is received at an atypical geographic location, time of day, or day of the week.

[0080] At 602, the biometric authentication system may receive sensor data associated with a client device, during a real-time session of authenticated access to a computing resource. In a non-limiting examples, one or more sensors associated with the client device may unobtrusively monitor a gait profile of the client, a voice profile of the client, a scent profile of the client, along with other body chemistry characteristics, such as heart rate, blood pressure, and skin capacitance. Further, sensor data may include metadata that describes a geographic location, time of day, and day of the week that is associated with each instance of monitored sensor data.

[0081] At 604, the biometric authentication system may generate one or more biometric authentication protocols based at least in part on the sensor data and associated metadata. For example, a scent profile for a client may be generated for conditions when a client is running in an environment having a particular ambient temperature.

[0082] At 606, the biometric authentication system may assign an authentication score to each of the one or more biometric authentication protocols based at least in part on the underlying type of biometric data. For example, the authentication score may reflect a level of confidence that an individual other than the client may cannot use their own biometric sample, in place of a biometric sample belonging to the client, to gain access to a computing resource via a biometric authentication protocol. Thus, a voice-recognition authentication protocol may have a lower authentication score relative to a scent recognition authentication protocol on the basis that a client voice may be easier to imitate relative to a scent.

[0083] At 608, the biometric authentication system may update a client profile associated with the client to include the one or more biometric authentication protocols along with corresponding authentication scores. In some instances, the biometric authentication system

may update existing biometric authentication protocols with a client profile, or include new biometric authentication protocols within the client profile. In some instances, an accuracy of an existing biometric authentication protocol may be improved via updating of the client profile. In some instances, an authentication score of an updated biometric authentication protocol may correspondingly improve.

CONCLUSION

[0084] Although the subject matter has been described in language specific to features and methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described herein. Rather, the specific features and acts are disclosed as exemplary forms of implementing the claims.

WHAT IS CLAIMED:

1. A computer-implemented method, comprising:

under control of one or more processors:

receiving, from a client device, a request for access to a computing resource;

identifying a security policy associated with the computing resource, the security policy indicating a degree of data sensitivity of data associated with the computing resource;

selecting a biometric authentication protocol from a plurality of biometric authentication protocols, based at least in part on the security policy of the computing resource;

generating an authentication policy for access to the computing resource, the authentication policy including at least the biometric authentication protocol;

transmitting a first data packet to the client device that includes the authentication policy and computer executable instructions that automatically execute the authentication policy on the client device;

receiving, from the client device, a second data packet that includes a biometric sample that corresponds to the biometric authentication protocol;

authenticating a client identity associated with the client device, based at least in part on the biometric sample; and

providing the client device with access to the computing resource based at least in part on authenticating the client identity.

2. The computer-implemented method of claim 1, further comprising:

comparing the biometric sample with a registered biometric template, the registered biometric template being associated with a client of the client device; and

determining a similarity of the biometric sample and the registered biometric template,

wherein, authenticating the client identity is based at least in part on the similarity being greater than a predetermined threshold.

3. The computer-implemented method of claim 1, further comprising:

causing a user interface of the client device to display one or more selectable options to create a registered biometric template;

receiving, via the user interface, a selection to create the registered biometric template;

prompting, via the user interface, a client to submit a biometric sample that is to be associated with the registered biometric template; and

generating the registered biometric template based at least in part on receipt of the biometric sample.

4. The computer-implemented method of claim 1, further comprising:

identifying a set of biometric authentication protocols from the plurality of biometric authentication protocols, based at least in part on the security policy of the computing resource, and

wherein selecting the biometric authentication protocol occurs randomly from the set of biometric authentication protocols.

5. The computer-implemented method of claim 1, wherein the biometric authentication protocol is a first biometric authentication protocol, and further comprising:

determining a first authentication score that is associated with the first biometric authentication protocol, and a second authentication score that is associated with a second biometric authentication protocol of the plurality of biometric authentication protocols;

determining that the first authentication score and the second authentication score are less than a predetermined score threshold of the security policy of the computing resource; and

determining that a summation of the first authentication score and the second authentication score is greater than the predetermined score threshold of the security policy of the computing resource,

wherein the authentication policy further includes the second biometric authentication protocol.

6. A system, comprising:

one or more processors;

memory coupled to the one or more processors, the memory including one or more modules that are executable by the one or more processors to:

receive a first data packet from a client device, the first data packet including a request for access to a computing resource and environmental sensor data associated with the client device, the environmental sensor data including at least one of a geographic location of the client device, an ambient light intensity and an ambient noise level;

identify a security policy associated with the computing resource;

determine a context of operation of the client device, based at least in part on the environmental sensor data;

generate an authentication policy to authenticate an identity of a client associated with the client device, based at least in part on the security policy and the context of operation, the authentication policy including at least one biometric authentication protocol of a plurality of biometric authentication protocols;

generate a second data packet for transmission to the client device, the second data packet including computer executable instructions that automatically execute the authentication policy on the client device;

receive a third data packet from the client device, the third data packet including at least one biometric sample of a client associated with the client device that corresponds to the at least one biometric authentication protocol; and

authenticate an identity of the client based at least in part on the at least one biometric sample.

7. The system of claim 6, wherein the one or more modules are further executable by the one or more processors to:

access, via a data store, a client profile associated with the client, the client profile including data entries that indicate one or more previous contexts of operations that correspond with previously authenticated requests for access to the computing resource; and

determine a similarity between the context of operation of the client device and the one or more previous contexts of operation,

wherein to generate the authentication policy is further based at least in part on similarity.

8. The system of claim 6, wherein the at least one biometric authentication protocol include a scent recognition protocol, wherein the one or more modules are further executable by the one or more processors to:

determine an ambient scent associated with the client device, based at least in part on an olfactory sensor of the client device,

wherein the at least one biometric authentication protocol corresponds to the scent recognition protocol based at least in part on the ambient scent being less than a predetermined scent threshold.

9. The system of claim 6, wherein the one or more modules are further executable by the one or more processors to:

access a client profile associated with the client that includes at least one registered biometric template that correspond to the at least one biometric authentication protocol; and

determine a similarity between the at least one biometric sample and the at least one registered biometric template,

wherein to authenticate the identity of the client is based at least in part on the similarity being greater than a predetermined threshold.

10. The system of claim 6, wherein the one or more modules are further executable by the one or more processors to:

monitor, one or more body chemistry patterns of a client during one or more sessions of authenticated access to the computing resource, the one or more body chemistry patterns including at least a scent profile of the client;

generate at least one registered biometric template based at least in part on the one or more body chemistry patterns; and

store the at least one registered biometric template within a client profile associated with the client.

11. The system of claim 6, wherein the one or more modules are further executable by the one or more processors to:

monitor, a kinematic behavior of the client during one or more sessions of authenticated access to the computing resource, the kinematic behavior of the client including at least a gait profile of the client, or a grip configuration of the client device, the grip configuration corresponding to a relative position of fingers of the client while holding the client device;

generate at least one registered biometric template based at least in part on the kinematic behavior of the client; and

store the at least one registered biometric template within a client profile associated with the client.

12. One or more non-transitory computer-readable media storing computer-executable instructions, that when executed on one or more processors, causes the one or more processors to perform acts comprising:

receiving, from a client device, a request for access to a computing resource, the request further including sensor data associated with environmental conditions that surround the client device;

identifying a security policy associated with the computing resource, the security policy indicating a degree of data sensitivity of data associated with the computing resource;

generating an authentication policy for access to the computing resource, based at least in part on the security policy and the environmental conditions, the authentication policy including at least one biometric authentication protocol of a plurality of biometric authentication protocols;

transmitting a data packet to the client device that automatically execute the authentication policy on the client device;

receiving, from the client device, at least one biometric sample that corresponds to the at least one biometric authentication protocol; and

authenticating a client identity based at least in part on the biometric sample and the at least one biometric authentication protocol.

13. The one or more non-transitory computer-readable media of claim 12, wherein the plurality of biometric authentication protocols includes at least a voice-recognition authentication protocol and a scent-recognition authentication protocol,

wherein, the sensor data associated with the environmental conditions includes an ambient noise level that surrounds the client device, and further comprising:

determining that the ambient noise level is greater than a predetermined noise threshold; and

selecting the scent-recognition authentication protocol as the at least one biometric authentication protocol, based at least in part on the ambient noise level.

14. The one or more non-transitory computer-readable media of claim 12, wherein the request further includes sensor data associated with a context of operation of the client device, the context of operation corresponds to a walking motion or a running motion of the client device,

wherein the plurality of biometric authentication protocols includes at least a scent-recognition authentication protocol and a facial image-recognition authentication protocol, and further comprising:

selecting the scent-recognition authentication protocol as the at least one biometric authentication protocol, based at least in part on the context of operation.

15. The one or more non-transitory computer-readable media of claim 12, wherein prior to receiving the request for access to the computing resource, further comprising:

generating a first registered template and a second registered template that correspond to the at least one biometric authentication protocol, the first registered template being based at least in part on a first set of biometric samples received a first time of day, and the second registered template being based at least in part on a second set of biometric samples received at a second time of day, the first time of day being different from the second time of day,

wherein, the request further includes an indication of a particular time of day, the particular time of day corresponding to the first time of day associated with the first registered template,

wherein, authenticating the client identity is further based at least in part on the first registered template.

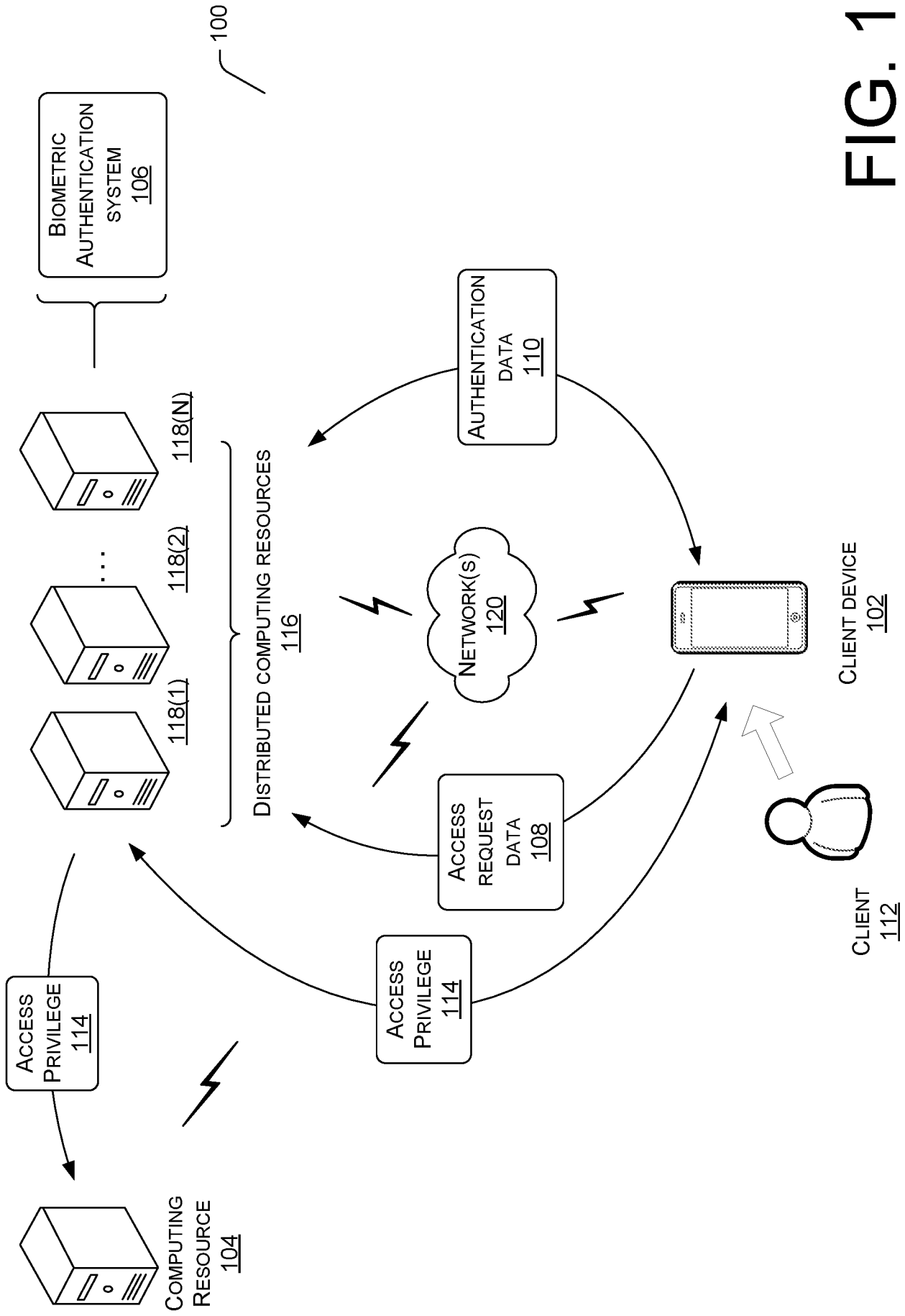
100
BIOMETRIC AUTHENTICATION SYSTEM 106
118(N)
118(2)
118(1)
DISTRIBUTED COMPUTING RESOURCES 116
AUTHENTICATION DATA 110
NETWORK(S) 120
CLIENT DEVICE 102
ACCESS REQUEST DATA 108
ACCESS PRIVILEGE 114
ACCESS PRIVILEGE 114
COMPUTING RESOURCE 104
CLIENT 112

FIG. 1

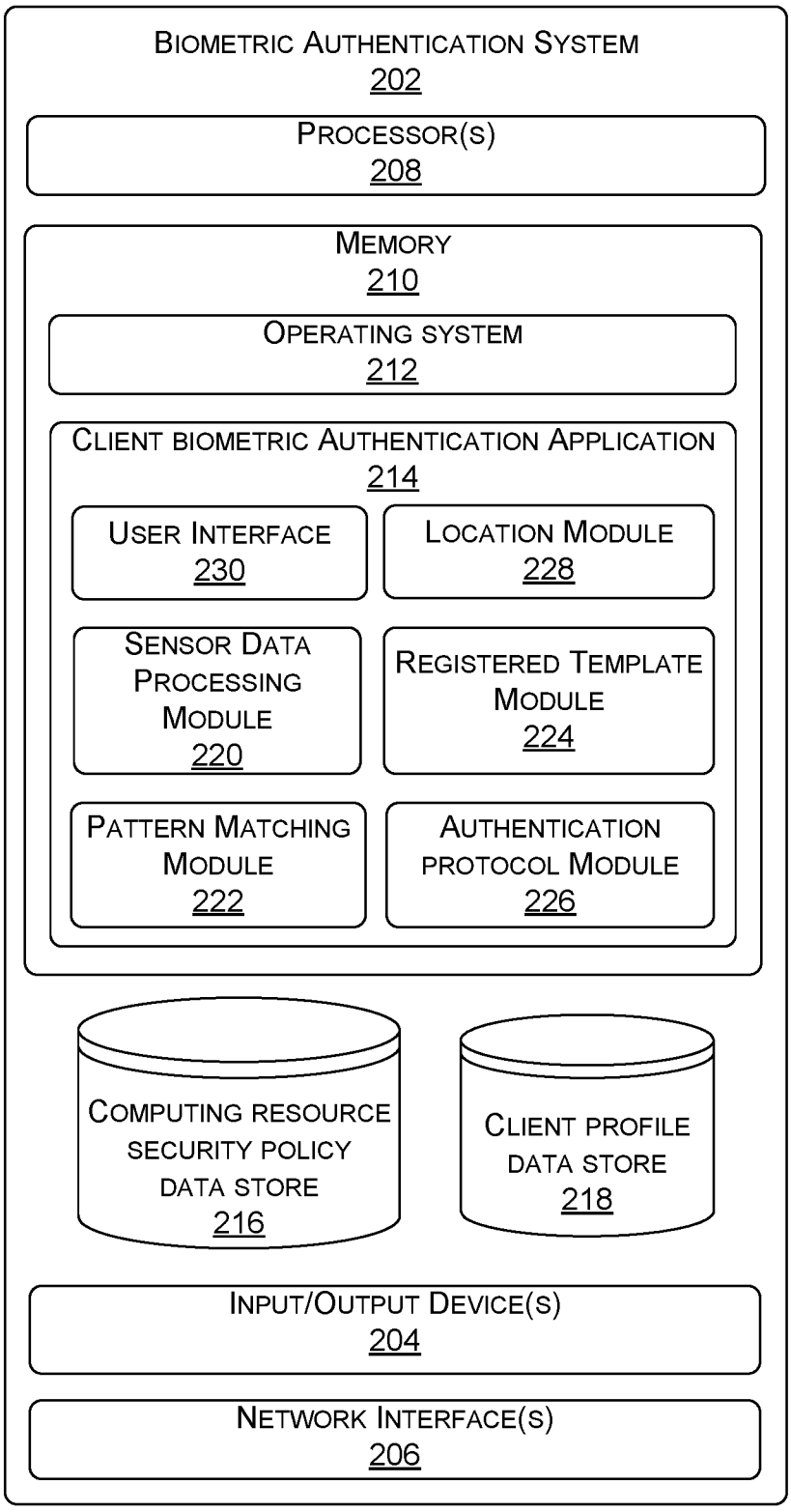
BIOMETRIC AUTHENTICATION SYSTEM
202
PROCESSOR(S)
208
MEMORY
210
OPERATING SYSTEM
212
CLIENT BIOMETRIC AUTHENTICATION APPLICATION
214
USER INTERFACE
230
LOCATION MODULE
228
SENSOR DATA PROCESSING MODULE
220
REGISTERED TEMPLATE MODULE
224
PATTERN MATCHING MODULE
222
AUTHENTICATION PROTOCOL MODULE
226
COMPUTING RESOURCE SECURITY POLICY DATA STORE
216
CLIENT PROFILE DATA STORE
218
INPUT/OUTPUT DEVICE(S)
204
NETWORK INTERFACE(S)
206

FIG. 2

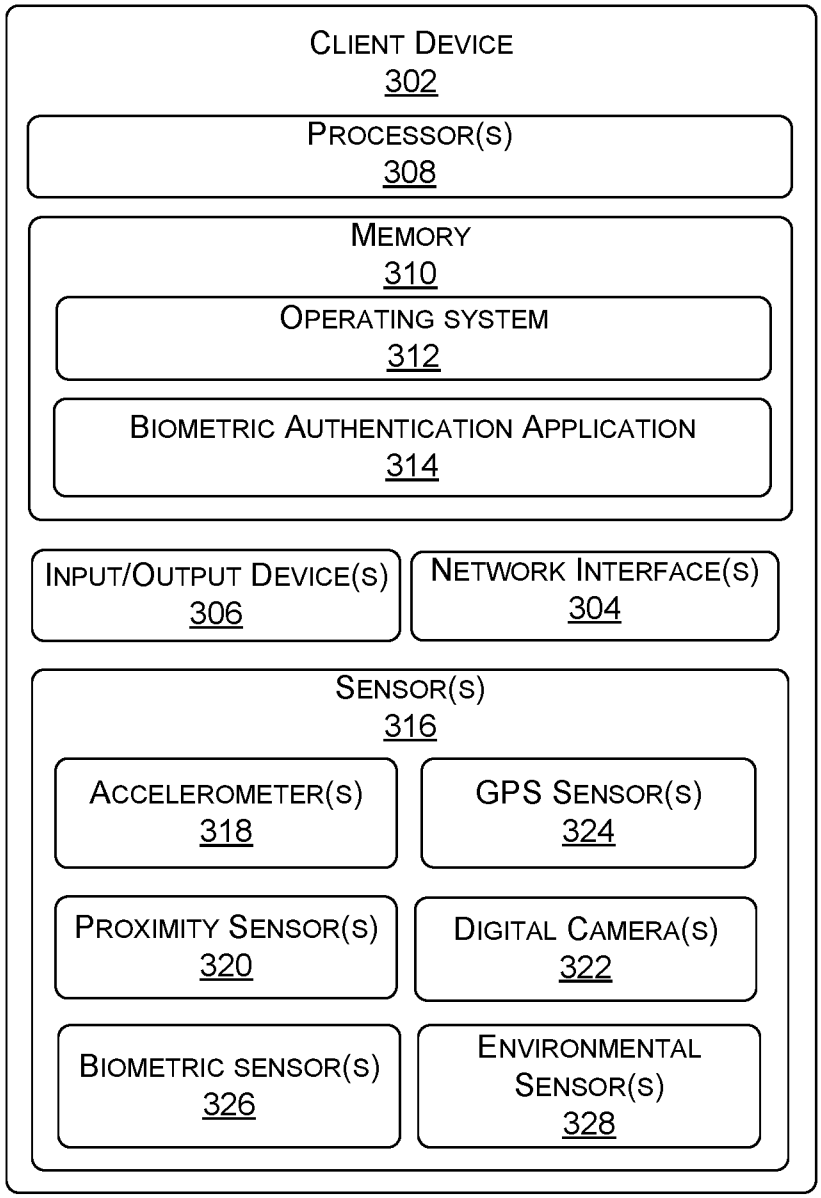
CLIENT DEVICE
302
PROCESSOR(S)
308
MEMORY
310
OPERATING SYSTEM
312
BIOMETRIC AUTHENTICATION APPLICATION
314
INPUT/OUTPUT DEVICE(S)
306
NETWORK INTERFACE(S)
304
SENSOR(S)
316
ACCELEROMETER(S)
318
GPS SENSOR(S)
324
PROXIMITY SENSOR(S)
320
DIGITAL CAMERA(S)
322
BIOMETRIC SENSOR(S)
326
ENVIRONMENTAL SENSOR(S)
328

FIG. 3

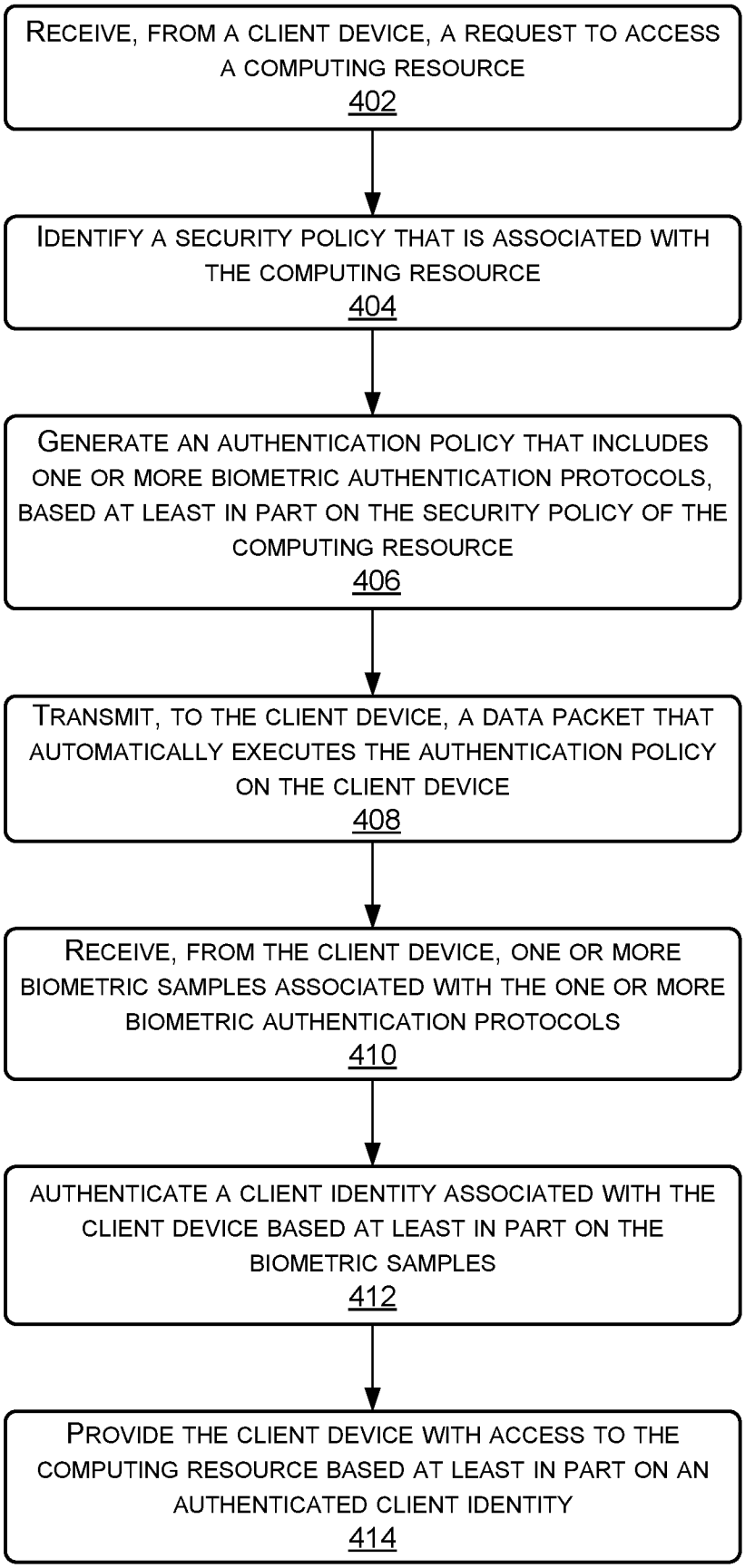
RECEIVE, FROM A CLIENT DEVICE, A REQUEST TO ACCESS A COMPUTING RESOURCE
402
IDENTIFY A SECURITY POLICY THAT IS ASSOCIATED WITH THE COMPUTING RESOURCE
404
GENERATE AN AUTHENTICATION POLICY THAT INCLUDES ONE OR MORE BIOMETRIC AUTHENTICATION PROTOCOLS, BASED AT LEAST IN PART ON THE SECURITY POLICY OF THE COMPUTING RESOURCE
406
TRANSMIT, TO THE CLIENT DEVICE, A DATA PACKET THAT AUTOMATICALLY EXECUTES THE AUTHENTICATION POLICY ON THE CLIENT DEVICE
408
RECEIVE, FROM THE CLIENT DEVICE, ONE OR MORE BIOMETRIC SAMPLES ASSOCIATED WITH THE ONE OR MORE BIOMETRIC AUTHENTICATION PROTOCOLS
410
AUTHENTICATE A CLIENT IDENTITY ASSOCIATED WITH THE CLIENT DEVICE BASED AT LEAST IN PART ON THE BIOMETRIC SAMPLES
412
PROVIDE THE CLIENT DEVICE WITH ACCESS TO THE COMPUTING RESOURCE BASED AT LEAST IN PART ON AN AUTHENTICATED CLIENT IDENTITY
414

FIG. 4

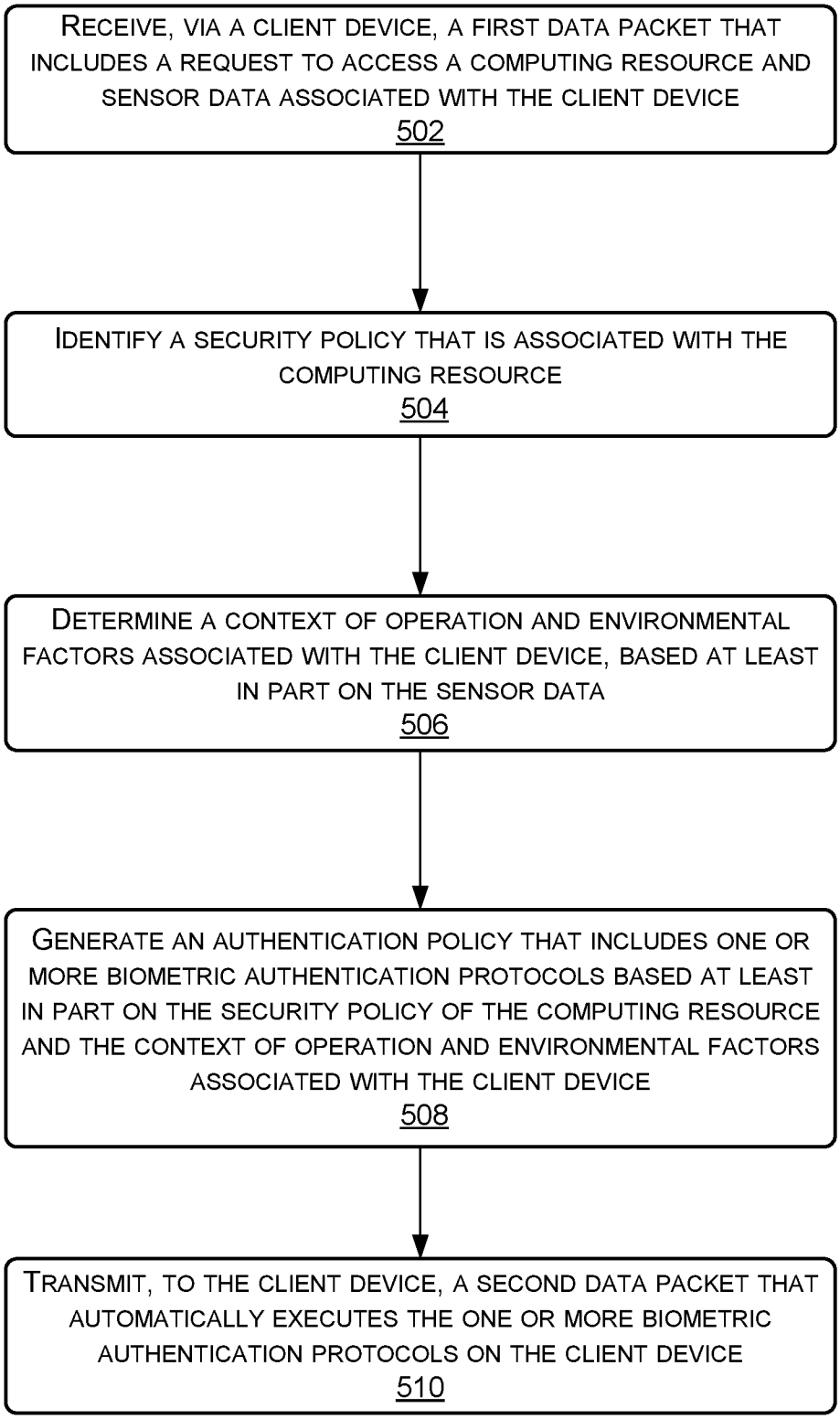
RECEIVE, VIA A CLIENT DEVICE, A FIRST DATA PACKET THAT INCLUDES A REQUEST TO ACCESS A COMPUTING RESOURCE AND SENSOR DATA ASSOCIATED WITH THE CLIENT DEVICE
502
IDENTIFY A SECURITY POLICY THAT IS ASSOCIATED WITH THE COMPUTING RESOURCE
504
DETERMINE A CONTEXT OF OPERATION AND ENVIRONMENTAL FACTORS ASSOCIATED WITH THE CLIENT DEVICE, BASED AT LEAST IN PART ON THE SENSOR DATA
506
GENERATE AN AUTHENTICATION POLICY THAT INCLUDES ONE OR MORE BIOMETRIC AUTHENTICATION PROTOCOLS BASED AT LEAST IN PART ON THE SECURITY POLICY OF THE COMPUTING RESOURCE AND THE CONTEXT OF OPERATION AND ENVIRONMENTAL FACTORS ASSOCIATED WITH THE CLIENT DEVICE
508
TRANSMIT, TO THE CLIENT DEVICE, A SECOND DATA PACKET THAT AUTOMATICALLY EXECUTES THE ONE OR MORE BIOMETRIC AUTHENTICATION PROTOCOLS ON THE CLIENT DEVICE
510

FIG. 5

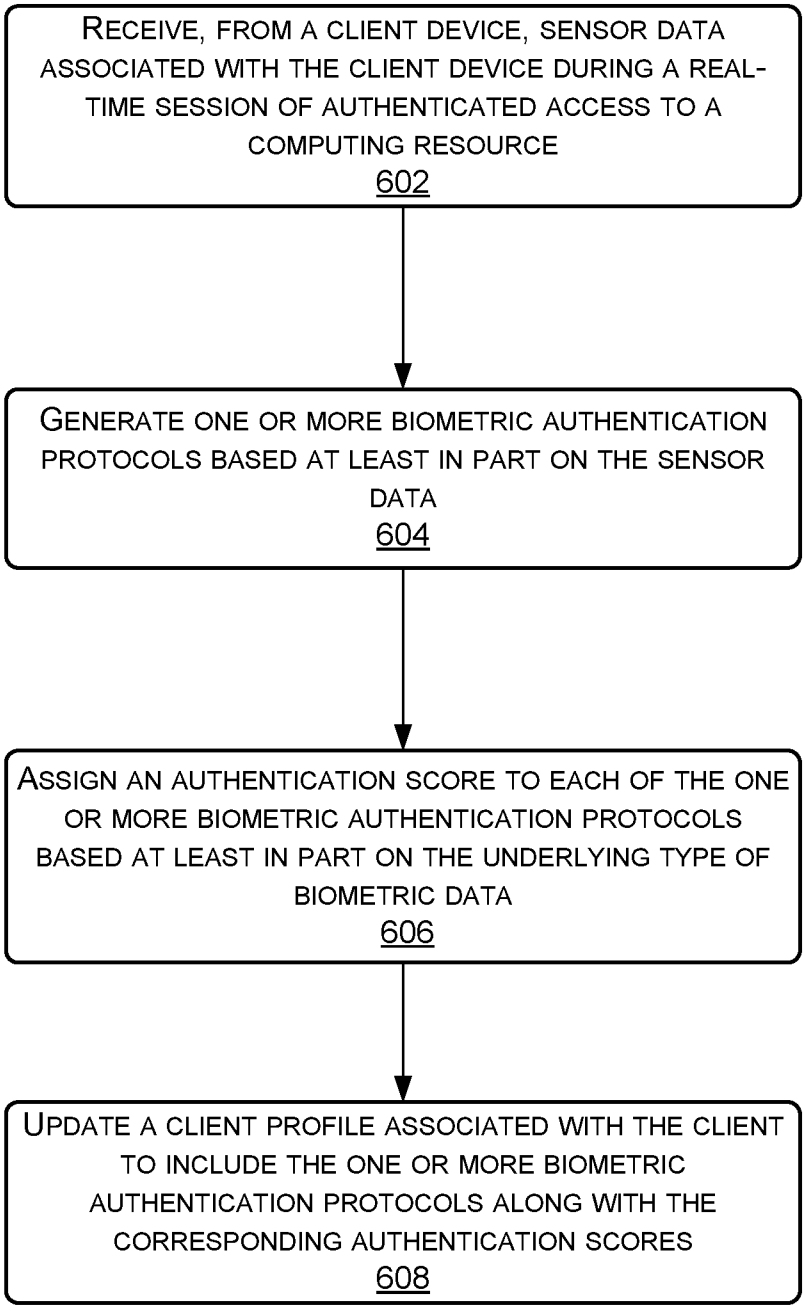
RECEIVE, FROM A CLIENT DEVICE, SENSOR DATA ASSOCIATED WITH THE CLIENT DEVICE DURING A REAL-TIME SESSION OF AUTHENTICATED ACCESS TO A COMPUTING RESOURCE
602
GENERATE ONE OR MORE BIOMETRIC AUTHENTICATION PROTOCOLS BASED AT LEAST IN PART ON THE SENSOR DATA
604
ASSIGN AN AUTHENTICATION SCORE TO EACH OF THE ONE OR MORE BIOMETRIC AUTHENTICATION PROTOCOLS BASED AT LEAST IN PART ON THE UNDERLYING TYPE OF BIOMETRIC DATA
606
UPDATE A CLIENT PROFILE ASSOCIATED WITH THE CLIENT TO INCLUDE THE ONE OR MORE BIOMETRIC AUTHENTICATION PROTOCOLS ALONG WITH THE CORRESPONDING AUTHENTICATION SCORES
608

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2018/025586

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i, G06F 21/32(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)
H04L 29/06; G06F 21/32; H04L 9/32; H04L 9/00; G06F 21/31; G06F 21/00

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: client, access, computing, resource, biometric, authentication, security, policy, multi-factor, context, sensitive, and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004-0148526 A1 (JUSTIN M. SANDS et al.) 29 July 2004 See paragraphs [0008], [0031]-[0032], [0090]-[0091]; claims 1, 13-15, 37; and figure 4.	1-2,4-5
Y		3,6-15
Y	US 2013-0227651 A1 (PAUL T. SCHULTZ et al.) 29 August 2013 See paragraphs [0015], [0028]-[0029], [0061], [0088]; and figures 1-2A.	3,6-15
A	US 2016-0055324 A1 (MOTOROLA MOBILITY LLC) 25 February 2016 See paragraphs [0015]-[0052]; and figures 1-6.	1-15
A	US 2007-0016777 A1 (JAMES D. HENDERSON et al.) 18 January 2007 See paragraphs [0012]-[0017]; and figures 1-4.	1-15
A	US 2014-0189809 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 03 July 2014 See paragraphs [0040]-[0054]; and figures 1-3.	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
24 July 2018 (24.07.2018)	**24 July 2018 (24.07.2018)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
LEE, Dal Kyong
Telephone No. +82-42-481-8440

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2018/025586

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004-0148526 A1	29/07/2004	US 7404086 B2	22/07/2008
		WO 2004-068283 A2	12/08/2004
		WO 2004-068283 A3	02/06/2005
US 2013-0227651 A1	29/08/2013	US 2013-0267204 A1	10/10/2013
		US 9100825 B2	04/08/2015
		US 9323912 B2	26/04/2016
US 2016-0055324 A1	25/02/2016	US 9589118 B2	07/03/2017
US 2007-0016777 A1	18/01/2007	WO 2007-008435 A2	18/01/2007
		WO 2007-008435 A3	16/04/2009
US 2014-0189809 A1	03/07/2014	US 9088555 B2	21/07/2015
		WO 2014-100902 A1	03/07/2014