September 2023

EQUALAUTH: FAIR AND SECURE BIOMETRICS FOR ALL ABILITIES

SAHIL ARORA
VISA

EQUALAUTH: FAIR AND SECURE BIOMETRICS FOR ALL ABILITIES

VISA

INVENTOR:

SAHIL ARORA

TECHNICAL FIELD

[0001] The present subject matter relates to biometric authentication systems and, more particularly, to a multi model behavioral biometric authentication system.

BACKGROUND

[0002] Authentication is a process of verifying user identity. Some examples of current authentication methods may include password-based authentication, physical biometrics-based authentication, multi-factor-based authentication, certificate-based authentication, token-based authentication, and the like. Biometrics is an automated recognition of individuals by means of unique physical characteristics, typically for the purposes of security. These authentication methods, however, fall short in both security and accessibility as they are susceptible to breaches, hacking and the like. Further, these methods also pose significant usability issues for people with disabilities. In an example, for a visually impaired user, visual passwords are a barrier in performing authentication to verify their identity. In another example, physical biometrics may be a barrier for users with certain physical disabilities. Therefore, there is a need for a system that is not only secure but can also accommodate users with different disabilities.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, serve to explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same numbers are used throughout the figures to reference features and components. Some embodiments of device or system and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[0004] **FIG. 1** illustrates a simplified representation of an environment related to behavioral biometric authentication for implementing embodiments consistent with the present disclosure.

[0005] **FIG. 2** illustrates a system for behavioral biometric authentication, in accordance with an embodiment of the present disclosure.

[0006] **FIG. 3** is a sequence flow diagram illustrating registration of a user for behavioral biometric authentication, in accordance with an embodiment of the present disclosure.

[0007] **FIG. 4** depicts a flowchart illustrating a method for performing behavioral biometric authentication, in accordance with an embodiment of the present disclosure.

DESCRIPTION OF THE DISCLOSURE

[0008] In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0009] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

[0010] The terms “comprises”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0011] The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment" mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

[0012] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0013] In the following detailed description of the embodiments of the disclosure, reference is made to the accompanying drawings that form a part hereof, and in which are shown by way of illustration specific embodiments in which the disclosure may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the disclosure, and it is to be understood that other embodiments may be utilized and that changes may be made without departing from the scope of the present disclosure. The following description is, therefore, not to be taken in a limiting sense.

[0014] Various embodiments of the present disclosure disclose a method and system for secure behavioural biometric authentication of the user. The term ‘behavioural biometrics’ as used herein refers to study related to the measure of uniquely identifying and measurable patterns in human activities. These activities may include but are not limited to keystroke dynamics, mouse movements, touchscreen interactions, voice patterns, device handling and the like. For example, keystroke dynamics may include measuring the rhythm, speed, pressure and the like. Further, measurable patterns related to mouse movement may include measuring the speed, acceleration, patterns of movement and the like. Measurable patterns related to touchscreen interactions may include but are not limited to the speed, pressure, patterns of touchscreen gestures, such as swipes, taps, pinches and the like. Measurable patterns related to voice patterns may include but are not limited to a user's unique voice characteristics, including pitch, rhythm, inflection and the like. Measurable patterns related to device handling may include but are not limited to how a user physically handles their device, such as the angle at which they hold their smartphone and the like.

[0015] **FIG.1** illustrates a simplified representation of an environment 100, in which at least some example embodiments of the disclosure can be implemented. The environment 100 exemplarily depicts a user 102 accessing an user device 104. It is noted that the user 102 may use one or more user devices, such as a smartphone, a laptop, a desktop, a personal computer, or any spatial computing device to perform secure digital transactions. For example, the user device 104 may work on multiple platforms and/or Operating Systems to perform digital transactions with different entities. As such, the user device 104 may obtain a password and/or physical biometric from the user 102 associated with the user device 104 to authenticate the user 102 for processing any digital transaction. Furthermore, the user device 104 may also collate user data related to behavior biometrics of the user 102 such as keystroke dynamics, mouse movements, touchscreen interactions, voice patterns, device handling and the like for a predefined time. The user data may be stored in a database 110. Further, the database 110 may also store behavioural biometric data of a plurality of users collected over a period of time. This behavioural biometric data stored in the database 110 may be provided as a training dataset to a system 108 to train the system 108 for authenticating users such as, the user 102.

[0016] Various embodiments of the present disclosure disclose a method and system 108 which use behavioral biometrics for authenticating users. More specifically, the system 108 uses measurable patterns in human activities unique to the user 102 for identifying the user 102. These activities may include keystroke dynamics, mouse movements, touchscreen interactions, voice patterns, device handling and the like. Therefore, using behavioral biometric data to authenticate user increases the security during authentication process and reduces unauthorized access to services. Thus, the system 108 not only ensures security, but also improves the accessibility for a disabled user.

[0017] The user device 104 sends the collated user data to the system 108 via a communication network 110. It is understood that the electronic device 104 may be in operative communication with the communication network 110, such as the Internet, enabled by a network provider, also known as an Internet Service Provider (ISP). The user device 104 may connect to the communication network 110 using a wired network, a wireless network, or a combination of wired and wireless networks. Some non-limiting examples of wired networks may include the Ethernet, the Local Area Network (LAN), a fiber-optic network, and the like. Some non-limiting examples of wireless networks may include the Wireless LAN (WLAN), cellular networks, Bluetooth or

ZigBee networks, and the like. An example of the system 108 is shown and explained next with reference to **FIG. 2**.

[0018] **FIG. 2** illustrates a block diagram of the system 108 implementing embodiments consistent with the present disclosure. In an embodiment, the system 108 may be embodied within the user device 104 and the authentication happens locally within the user device 104. In another embodiment, the system 108 may be a distributed or a centralized server performing one or more of the operations described herein.

[0019] The system 108 comprises a processor 202, a memory 204, an input/output module 208 and a communication interface 206. It shall be noted that, in some embodiments, the system 108 may include more or fewer components than those depicted herein. The various components of the system 108 may be implemented using hardware, software, firmware or any combinations thereof. Further, the various components of the system 108 may be operably coupled with each other. More specifically, various components of the system 108 may be capable of communicating with each other using communication channel media (such as buses, interconnects, etc.). It is also noted that one or more components of the system 108 may be implemented in a single server or a plurality of servers, which are remotely placed from each other.

[0020] In one embodiment, the processor 202 may be embodied as a multi-core processor, a single core processor, or a combination of one or more multi-core processors and one or more single core processors. For example, the processor 202 may be embodied as one or more of various processing devices, such as a coprocessor, a microprocessor, a controller, a digital signal processor (DSP), a processing circuitry with or without an accompanying DSP, or various other processing devices including, a microcontroller unit (MCU), a hardware accelerator, a special-purpose computer chip, or the like. The processor 202 includes a training module 210, a validation module 212 and an anomaly detection module 214.

[0021] In one embodiment, the memory 204 is capable of storing user profiles, referred to herein as user profile 214 and a plurality of models. Some examples of the models include, but not limited to, Machine Learning (ML) models, deep learning models, neural network models (e.g., Convolutional Neural Network (CNN) model, Deep Convolutional Neural Network (DCNN) model, etc.) and the like in a model repository 218. In an embodiment, the processor 202 is configured to train the plurality of models in the model repository 218 using the training dataset. The memory 204 can be any type of storage accessible to the processor 202 to perform respective functionalities. For example, the memory 204 may include one or more volatile or non-volatile memories, or a combination thereof. For example, the memory 204 may be embodied as semiconductor memories, such as flash memory, mask ROM, PROM (programmable ROM), EPROM (erasable PROM), RAM (random access memory), etc. and the like.

[0022] In an embodiment, the processor 202 is configured to execute operations for: (1) receiving user data, (2) identifying a type of disability based on the user data, (3) extracting appropriate model based on the identified disability, (4) training the model based on the user data, (5) generating a user profile based on the user data, (6) storing the user profile in the database 110, (7) receiving new user data at a pre-defined time period, (8) generating an updated user profile based on the new user data, and (9) storing the updated user profile in the database 110.

[0023] In an embodiment, the I/O module 208 may include mechanisms configured to receive inputs from and provide outputs to peripheral devices such as, an operator of the system 108. To enable reception of inputs and provide outputs to the system 108, the I/O module 208 may include at least one input interface and/or at least one output interface. Examples of the input interface may include, but are not limited to, a keyboard, a mouse, a joystick, a keypad, a touch screen, soft keys, a microphone, and the like. Examples of the output interface may include, but are not limited to, a display such as a light emitting diode display, a thin-film transistor (TFT) display, a liquid crystal display, an active-matrix organic light-emitting diode (AMOLED) display, a microphone, a speaker, a ringer, and the like.

[0024] In an embodiment, the communication interface 206 may include mechanisms configured to communicate with other entities in the environment 100. In other words, the communication interface 206 is configured to access the training dataset corresponding to a plurality of users. In an example, the training dataset may be stored in the database 110 and the communication interface 206 may access the training dataset to train the plurality of models. In yet another example, the user data may be obtained via the communication interface. More specifically, user data related to behavioural pattern of the user 102 may be captured as keystroke dynamics, mouse movements, touchscreen interactions, voice patterns, device handling and the like and sent to the system 108. The system 108 receives the training dataset and the user data to perform one or more operations described herein.

[0025] The database 110 may include multiple storage units such as hard disks and/or solid-state disks in a redundant array of inexpensive disks (RAID) configuration. In some embodiments, the database 110 may include a storage area network (SAN) and/or a network attached storage (NAS) system. In one embodiment, the database 110 may correspond to a distributed storage system, wherein individual databases are configured to store custom information, such as, behavioural biometric data of the plurality of users collected over a period of time, pre-trained models, user profiles, and the like.

[0026] In some embodiments, the database 110 is integrated within the system 108. For example, the system 108 may include one or more hard disk drives as the database 110. In other embodiments, the database 110 is external to the system 108 and may be accessed by the system 108 using a storage interface (not shown in FIG. 2). The storage interface is any component capable of providing the processor 202 with access to the database 110. The storage interface may include, for example, an Advanced Technology Attachment (ATA) adapter, a Serial ATA (SATA) adapter, a Small Computer System Interface (SCSI) adapter, a RAID controller, a SAN adapter, a network adapter, and/or any component providing the processor 202 with access to the database 110.

[0027] As already explained, the communication interface 206 is configured to receive the user data from the user 102. More specifically, the user device 108 may provide the user data as part of an authentication request. The user data may include various attributes associated with behavioural biometrics, type of disability of the user 102, type of service, registration request and the like. More specifically, the behavioural biometrics of the user 102 such as keystroke dynamics, mouse movements, touchscreen interactions, voice patterns, device handling and the like may be received by the system 108 for authenticating the user 102. For example, data related to keystroke dynamics may include data about the rhythm, speed and pressure exerted on the keyboard. Further, data related to mouse movement may include measuring the speed, acceleration, patterns of movement and the like. Measurable data related to touchscreen interactions may include but are not limited to the speed, pressure, patterns of touchscreen gestures, such as swipes, taps, pinches and the like. Measurable data related to voice patterns may include but are not limited to a user's unique voice characteristics, including pitch, rhythm, inflection and the like. Measurable data related to device handling may include but are not limited to how a user physically handles their device, such as the angle at which they hold their smartphone and the like. The communication interface 206 forwards the user data to the processor 202. The modules of the processor 202 in conjunction with the user profiles 216 and model repository 218 in the memory 204 are configured to authenticate the user 102 based on the user data and process the user request.

[0028] In an embodiment, the processor 202 may be configured to pre-train the models in the model repository 218. The processor 202 obtains the training dataset from the database 110 wherein the training dataset comprises user data from a plurality of users with different disabilities. As already explained, the user data is collected over a period of time and stored in the database 110. The processor 202 trains the plurality of models based on the specific disability by prioritizing at least one attribute associated with the behavioural biometrics over others. For example, if the user 102 among the plurality of users is visually impaired, then attributes such as keystroke dynamics and voice patterns may be prioritized over the rest. This is done to achieve an accurate pre-trained models for each specific disability.

[0029] The pre-trained model may be stored in the model repository 218 and/or can be stored in the database 110. The operations of the processor 202 for processing the user request to generate user profile is explained as a sequence flow with reference to **FIG. 3**.

[0030] **FIG. 3** illustrates a sequence flow diagram illustrating registration of the user 102 for behavioral biometric authentication, in accordance with an embodiment of the present disclosure.

[0031] At step 302, a user data from the user device 104 is sent to the system 108. In an embodiment, the user data may be continuously captured for a predefined time period and forwarded to the system 108. This user data is a behavioural biometric data which may include, but not limited to, keystroke dynamics, mouse movements, touchscreen interactions, voice patterns, device handling and the like. Further, the user data related to keystroke dynamics may include measuring the rhythm, speed, pressure and the like. Further, data related to mouse movement may include measuring the speed, acceleration, patterns of movement and the like. Data related to touchscreen interactions may include but are not limited to the speed, pressure, patterns of touchscreen gestures, such as swipes, taps, pinches and the like. Data related to voice patterns may include, but are not limited to, a user's unique voice characteristics, including pitch, rhythm, inflection and the like. Data related to device handling may include, but not limited to, how the user 102 physically handles their user device 104, such as the angle at which they hold their smartphone and the like.

[0032] At 304, the system 108 identifies a disability based on the user data. The system 108 identifies a disability based on the user data, wherein the disabilities may include visual impairment, motor disability, and the like. More specifically, the system 108 compares one or more behavioural attributes from the user data with a predefined threshold to identify the disability. For example, visual disability is characterized by keystroke dynamics which may be slower i.e., rate at which user data is provided may be slower. This attribute may be used to identify visual disabilities. As such, each disability may be defined by one or more behavioural attributes which may be identifies based on different thresholds.

[0033] At 306, the system 108 sends a request for a model among a plurality of models from the database 110 based on the identified disability. The plurality of models may include a plurality of ML models, deep learning models, neural network models such as CNN model, DCNN model and the like. These models are pre-trained models which have been trained based on the training dataset from the plurality of users with similar disability. In an example, the models can be pre-trained and stored in the database 110. In another example, the models can be trained by the processor 202 using the training dataset from the database 110 and stored in the model repository 218.

[0034] At 308, the model is sent to the system 108 based on the disability. The model sent to the system 108 is trained using data from plurality of users having similar disability by prioritizing some attributes of behavioural biometrics over the other based on the type of disability.

[0035] At 310, the model is trained using the user data. Based on the user data obtained during registration process, the model is trained over a period of time to obtain an accurate user profile. This data is also obtained over a period of time by monitoring various attributes of behavioural biometrics.

[0036] At step 312, the trained model generates a user profile. The user profile is unique to the user, some attributes of the user 102 is prioritized over other based on the type of disability. For example, if the user 102 is visually impaired, the system 108 may prioritize keystroke dynamics and voice patterns over other attributes.

[0037] At 314, the user profile generated by the system 108 is stored in the database 110 this user profile is later used to authenticate the user during processing of a user request.

[0038] At step 318, the user profile is retrieved during authentication process. When the user 102 requests for authentication during the processing of user request, the user profile is retrieved from the database 110 and used to authenticate the user.

[0039] At step 320, new user data is obtained every pre-defined time period to enable continuous learning of the model. The model continues training and learning process throughout the duration of usage, the user data that is collected of the period of usage of the system 108, is used to train the model to update the user profile. This also makes it more accurate than the initial user profile and avoids any false positives.

[0040] At step 322, the user profile is updated based on the new user data. Based on the data obtained every pre-defined time period, the user profile is updated. At step 324, the updated user profile is stored in the database 110 which is retrieved during next authentication process.

[0041] **FIG. 4** depicts a flowchart illustrating a method 400 for performing authentication, in accordance with an embodiment of the present disclosure. At 402, the user 102 sends an authentication request which also comprises the user data. This authentication request is to verify the user 102 and to process an user request. The user request may correspond to accessing a service, for example, authenticating the user 102 for facilitating a payment transaction.

[0042] At 404, the system 108 retrieves the user profile associated with the user 102 from the database 110 and/or from memory 204 and compares the user profile with the user data. At 406, the system 108 validates if the user data matches with the user profile.

[0043] At 408, if the validation of the user data is unsuccessful, then the processing of the user request is terminated. Alternatively, if the processing of the user data is successful, then operation 412 is performed. Further, at 410, a notification regarding the status of the processing is sent to the user 102.

[0044] At 412, during processing of the user request, the system 108 monitors for any anomalies. At 414, the system 108 checks if any anomalies are detected. At 416a, if no anomalies are detected, the user request is completed and at 418, a notification is sent to the user 102 upon completion of the user request.

[0045] At 416b, if any anomaly is detected, the system 108 sends an alert to the user device 104 and/or temporarily locks the account associated with the user 102. At 420, the system 108 sends a notification to the user device 104 on the status of the user request.

[0046] In an exemplary embodiment, when the user 102 wants to open a bank account online, as part of the account setup process, the user sets up a username and a password as authentication steps to use that bank account. The bank, however, continuously collects the behavioural biometric data of the user 102 for a pre-defined period of time in order to set up behavioural biometric based authentication feature. Once the bank collects the user data for the pre-defined time period, a user profile is created for the user 102. Further, the user 102 needs to enable this behavioural biometric feature in order to use this feature the next time the user 102 is authenticating their identity. This ensures that the process of authentication to access the account associated with the user 102 is faster as the system 108 automatically obtained the behavioural biometric data and grants access to the user 102 on successful authentication.

[0047] Some advantages achieved by the present disclosure are increasing the security of accessing services such as, payment services, by secure authentication, reducing the time taken to authenticate a user and increased accessibility for users with disability. The present disclosure provides the system 108 that is inclusive of users with different disabilities wherein the system 108 will automatically adapt based on the identified disability. Further, user data consists of a plurality of features that are considered to generate a user profile which will be unique to an individual. Moreover, the system 108 also monitors anomalies which adds another layer of protection and makes the system 108 more reliable. Furthermore, the system 108 also sends alerts to the user 102 if any anomaly is detected and, in some cases, can temporarily lock the account associated with the user 102 until the user 102 can verify their identity. The system 108 is also robust when compared with existing authentication systems.

[0048] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer-readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., be non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc (CD) ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0049] The described operations may be implemented as a method, system or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof. The described operations may be implemented as code maintained in a “non-transitory computer readable medium”, where a processor may read and execute the code from the computer readable medium. The processor is at least one of a microprocessor and a processor capable of processing and executing the queries. A non-transitory computer readable medium may include media such as magnetic storage medium (e.g., hard disk drives, floppy disks, tape, etc.), optical storage (CD-ROMs, DVDs, optical disks, etc.), volatile and non-volatile memory devices (e.g., EEPROMs, ROMs, PROMs, RAMs, DRAMs, SRAMs, Flash Memory, firmware, programmable logic, etc.), etc. Further, non-transitory computer-readable media may include all computer-readable media except for a transitory. The code implementing the described operations may further be implemented in hardware logic (e.g., an integrated circuit chip, Programmable Gate Array (PGA), Application Specific Integrated Circuit (ASIC), etc.).

[0050] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items or meant to be limited to only the listed item or items. It must also be noted that as used herein, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise.

[0051] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer readable medium" should be understood to include tangible items and exclude carrier waves and transient signals, i.e., are non-transitory. Examples include random access memory (RAM), read-only memory (ROM), volatile memory, non-volatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0052] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

[0053] With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

EQUALAUTH: FAIR AND SECURE BIOMETRICS FOR ALL ABILITIES

ABSTRACT

The present disclosure relates to a behavioral biometric based authentication system. User device sends user data associated with a user to a system. The user data includes behavioral biometric data such as keystroke dynamics, mouse movements, touchscreen interactions, voice patterns, device handling and the like. The system identifies a disability based on the user data and extracts a pre-trained model associated with that specific disability from any one of: database and model repository. The model is further trained using the user data to generate and store a user profile. The user sends an authentication request during processing of a user request, the processor extracts the user profile to verify the identity of the user. Further, the anomaly detector checks for any anomalies during the processing of user request. The system sends alerts to the user device and/or temporarily locks an account and terminates the processing of the user request upon detection of an anomaly.

DRAWINGS:

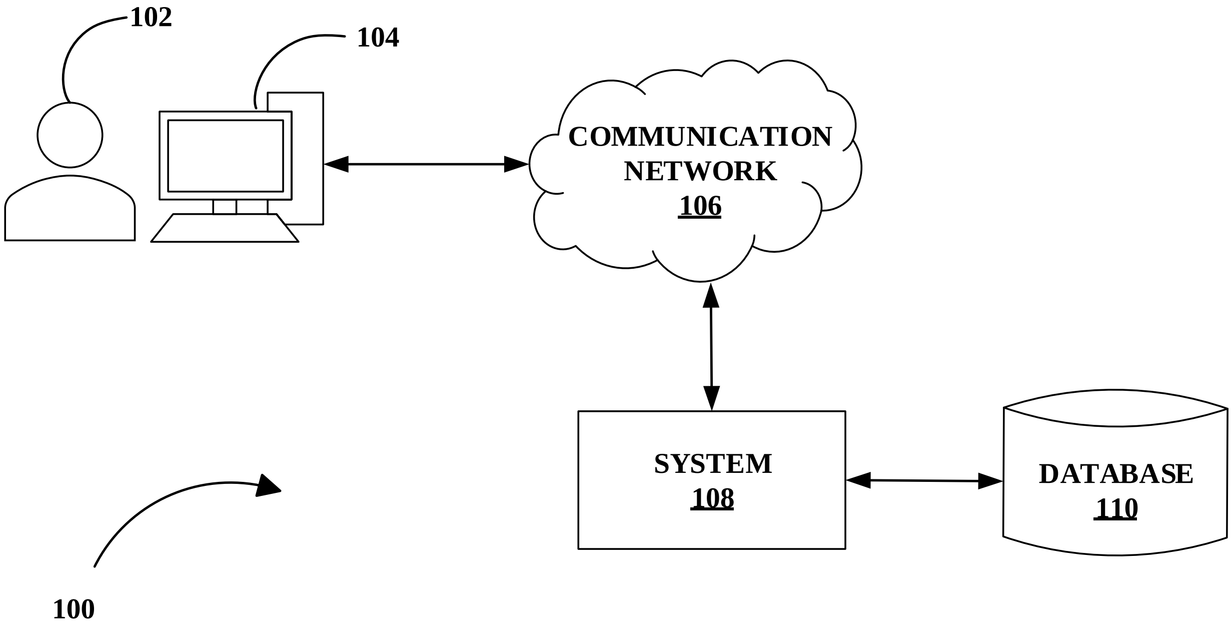

FIG. 1

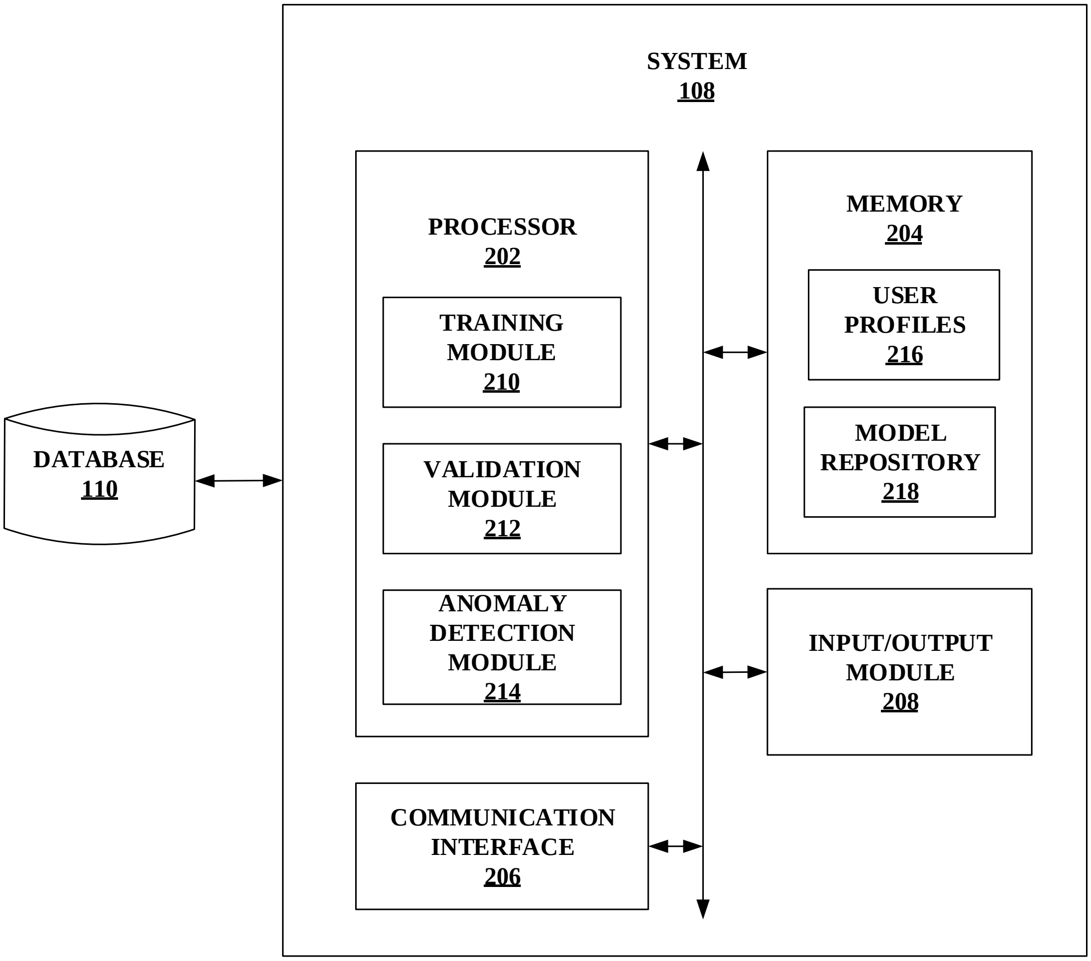
SYSTEM
108
PROCESSOR
202
TRAINING MODULE
210
VALIDATION MODULE
212
ANOMALY DETECTION MODULE
214
MEMORY
204
USER PROFILES
216
MODEL REPOSITORY
218
INPUT/OUTPUT MODULE
208
COMMUNICATION INTERFACE
206
DATABASE
110

FIG.2

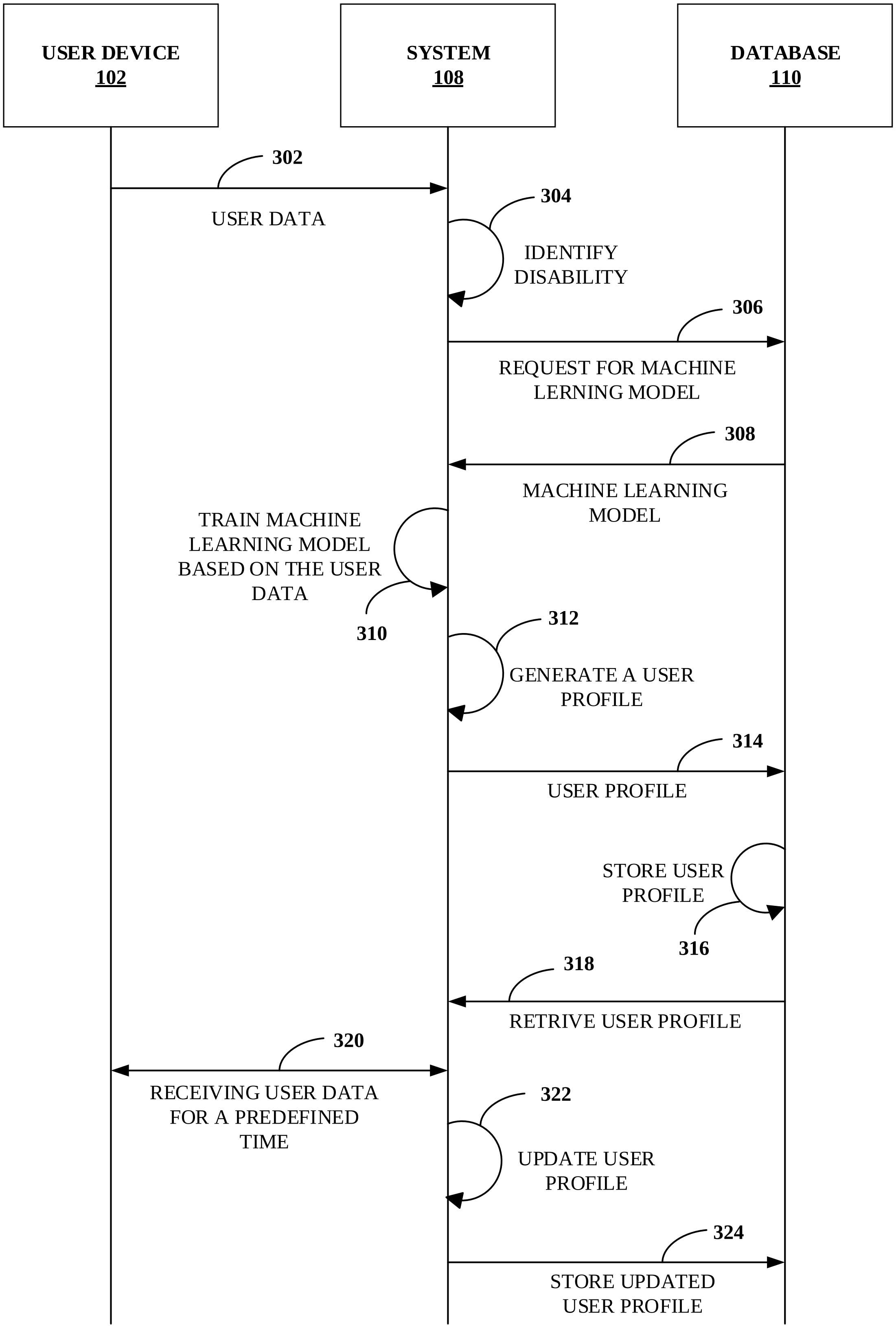
USER DEVICE
102
SYSTEM
108
DATABASE
110
302
USER DATA
304
IDENTIFY
DISABILITY
306
REQUEST FOR MACHINE
LERNING MODEL
308
MACHINE LEARNING
MODEL
TRAIN MACHINE
LEARNING MODEL
BASED ON THE USER
DATA
310
312
GENERATE A USER
PROFILE
314
USER PROFILE
STORE USER
PROFILE
316
318
RETRIVE USER PROFILE
320
RECEIVING USER DATA
FOR A PREDEFINED
TIME
322
UPDATE USER
PROFILE
324
STORE UPDATED
USER PROFILE

FIG.3

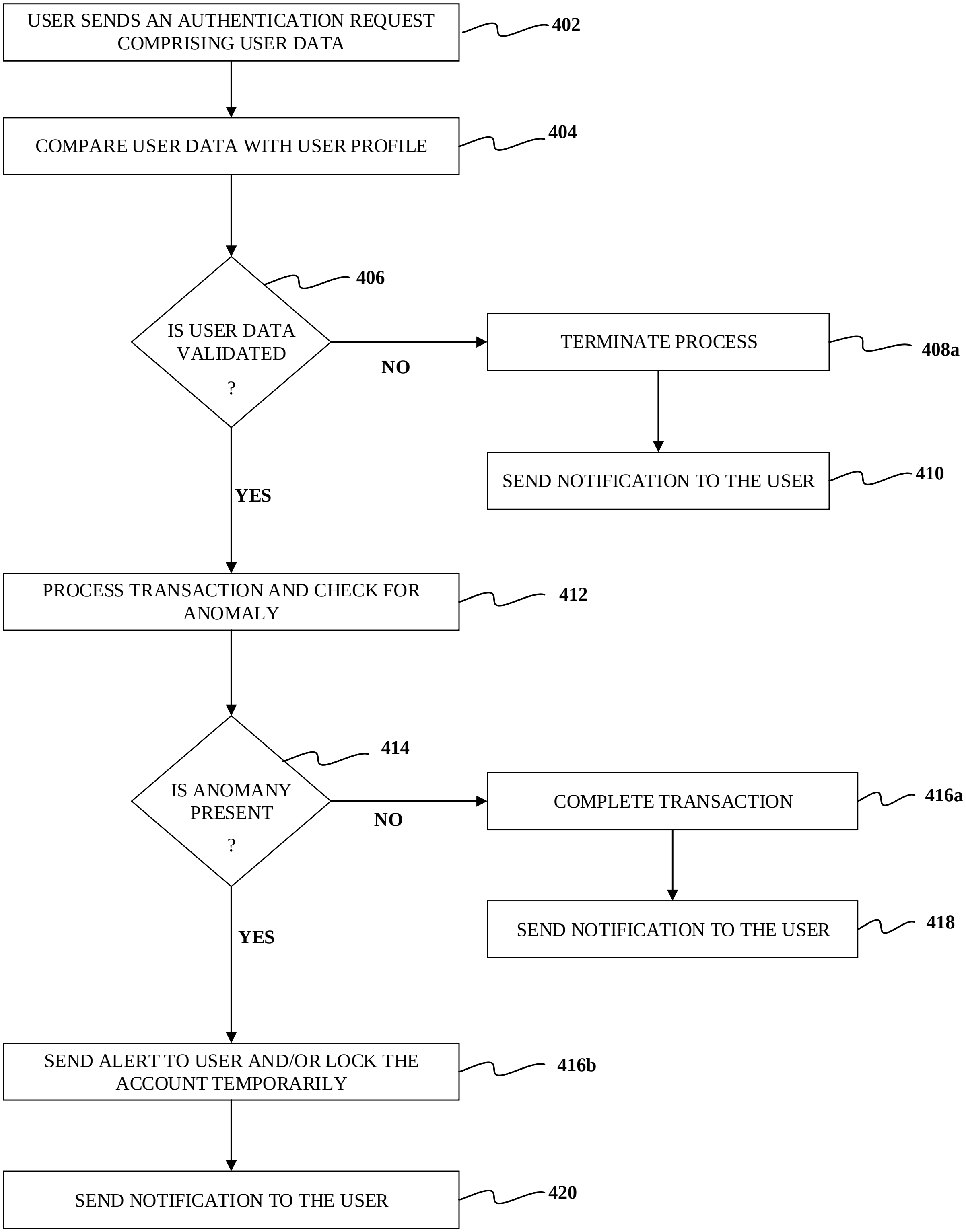
USER SENDS AN AUTHENTICATION REQUEST COMPRISING USER DATA
402
COMPARE USER DATA WITH USER PROFILE
404
IS USER DATA VALIDATED ?
406
NO
TERMINATE PROCESS
408a
SEND NOTIFICATION TO THE USER
410
YES
PROCESS TRANSACTION AND CHECK FOR ANOMALY
412
IS ANOMANY PRESENT ?
414
NO
COMPLETE TRANSACTION
416a
SEND NOTIFICATION TO THE USER
418
YES
SEND ALERT TO USER AND/OR LOCK THE ACCOUNT TEMPORARILY
416b
SEND NOTIFICATION TO THE USER
420

FIG.4