USER IDENTIFICATION WITH BLENDED RESPONSE FROM DUAL-LAYER IDENTIFICATION SERVICE

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of U.S. Provisional Application No. 63/085,591, filed on September 30, 2020 and U.S. Provisional Application No. 63/085,598, filed on September 30, 2020, the entire contents of which are hereby incorporated by reference.

FIELD

[0002] The present disclosure relates generally to user identification. More specifically, the present disclosure relates to user identification with a blended response from a dual-layer identification service.

BAGROUND

[0003] User identification may occur in a variety of different ways. For example, a user may be identified with individual or combinations of distinctive biometrics that are associated with the user. However, a problem with user identification using passive biometrics is that the number of iterations of user identification that are required before a user may be accurately identified is unwarrantably high. For example, user identification using passive biometrics requires ten or more iterations before a user may be accurately identified using passive biometrics. Passive biometrics are biometrics that are derived from the user's interaction with a webpage via a computing device.

SUMMARY

[0004] The present disclosure improves user identification using passive biometrics and solves the aforementioned problem by performing user identification with a blended response from a dual-layer identification service. Even if a first identification of a user is unsuccessful with a passive biometrics model, a second identification of the user may be successful using a specified set of device identification rules to modify, or in place of, the first identification.

[0005] The first and second identifications of the user may be blended to form a blended response that successfully identifies a user without requiring ten or more iterations to

accurately identify the user. For example, the user identification of the present disclosure using passive biometrics may require just two iterations before a user is accurately identified with the dual-layer identification service.

[0006] For example, the first identification may be a passive biometric score and two biometric score thresholds (i.e., an upper threshold and a lower threshold). The second identification may be an indication that the user is the same user or a different user (e.g., an IP address of the user's cell phone). The blended response may be the passive biometric score with two modified biometric score thresholds that indicate whether the user is the same user or a different user even when the first identification, by itself, was inconclusive or unsuccessful.

[0007] The combination of the first identification and the second identification in the blended response achieves more than the expected sum because the blended response reduces the number of iterations down to just two iterations necessary to accurately identify the user using passive biometrics. While the second identification may be individually used in place of the first identification, the first identification using passive biometrics may take, for example, ten or more iterations to accurately identify the user. In other examples, the passive biometrics may take less than ten iterations to accurately identify the user.

[0008] Additionally, the second identification may be used until the first identification is successful. The second identification is an identification with non-behavioral rules (e.g., device-based rules) to assess a likelihood the same user while the first identification uses biometric features (e.g., biometric features derived from typing and device interaction). Therefore, a true identification of a user is achieved faster with the blended response of the present disclosure.

[0009] One example of the present disclosure is a server including a communication interface, a memory, and an electronic processor. The communication interface is configured to communicate with a second server via a network. The memory includes an input profile record (IPR) program, an IPR repository, and a dual-layer identification service. The electronic processor, when executing the IPR program, is configured to detect an access request by a user of a user interface device, and retrieve a plurality of input profile records associated with the user from an input profile record repository in the memory in response to detecting the access request of the user, each of the plurality of input profile records including

a plurality of user inputs from the user interacting with a webpage or a mobile application. Additionally, when executing the dual-layer identification service, the electronic processor configured to perform an identification of the user with one or more passive biometrics models and the plurality of input profile records that are retrieved, generate an identification response and an additional identification request based on an outcome of the identification of the user with the one or more passive biometrics models and the plurality of input profile records that are retrieved, control the communication interface to transmit the additional identification request to the second server via the network, receive a second identification response from the second server via the communication interface and the network, and generate a blended response by modifying one or more characteristics of the identification response with the second identification response, the blended response indicating the identification of the user.

[0010] Another example of the present disclosure includes a method for user identification. The method includes detecting, with an electronic processor, an access request by the user of a user interface device. The method includes retrieving, with the electronic processor, a plurality of input profile records associated with the user from an input profile record repository in a memory in response to detecting the access request of the user, each of the plurality of input profile records including a plurality of user inputs from the user interacting with a webpage or a mobile application. The method includes performing, with the electronic processor, an identification of the user with one or more passive biometrics models and the plurality of input profile records that are retrieved. The method includes generating, with the electronic processor, an identification response and an additional identification request based on an outcome of the identification of the user with the one or more passive biometrics models and the plurality of input profile records that are retrieved. The method includes controlling, with the electronic processor, a communication interface to transmit the additional identification request to a second server via a network. The method includes receiving, with the electronic processor, a second identification response from the second server via the communication interface and the network. The method also includes generating, with the electronic processor, a blended response by modifying one or more characteristics of the identification response with the second identification response, the blended response indicating the identification of the user.

[0011] Yet another example of the present disclosure is a system. The system includes a first server and a second server. The first server includes a communication interface, a memory, and an electronic processor. The communication interface is configured to communicate with the second server via a network. The memory includes an input profile record (IPR) program, an IPR repository, and a dual-layer identification service. The electronic processor, when executing the IPR program, configured to detect an access request by a user of a user interface device, and retrieve a plurality of input profile records associated with the user from an input profile record repository in the memory in response to detecting the access request of the user, the plurality of input profile records including a plurality of user inputs from the user interacting with a webpage or a mobile application. Additionally, when executing the dual-layer identification server, the electronic processor configured to perform an identification of the user with one or more passive biometrics models and the plurality of input profile records that are retrieved, generate an identification response and an additional identification request based on an outcome of the identification of the user with the one or more passive biometrics models and the plurality of input profile records that are retrieved, control the communication interface to transmit the additional identification request to the second server via the network, receive a second identification response from the second server via the communication interface and the network, and generate a blended response by modifying one or more characteristics of the identification response with the second identification response, the blended response indicating the identification of the user.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 is a block diagram illustrating a system with user identification using a blended response from a dual-layer identification service, in accordance with various aspects of the present disclosure.

[0013] FIG. 2 is a flow diagram illustrating the dual-layer service of FIG. 1, in accordance with various aspects of the present disclosure.

[0014] FIG. 3 is a flowchart illustrating a method for identifying a user, in accordance with various aspects of the present disclosure.

DETAILED DESCRIPTION

[0015] Before any embodiments of the present disclosure are explained in detail, it is to be understood that the present disclosure is not limited in its application to the details of construction and the arrangement of components set forth in the following description or illustrated in the following drawings. The present disclosure is capable of other embodiments and of being practiced or of being carried out in various ways.

[0016] FIG. 1 is a block diagram illustrating a system 10 with user identification using a blended response from a dual-layer identification service. It should be understood that, in some embodiments, there are different configurations from the configuration illustrated in FIG. 1. The functionality described herein may be extended to any number of servers providing distributed processing.

[0017] In the example of FIG. 1, the system 10 includes a first server 100, a user interface device 120, a second server 160, and a network 180. The first server 100 includes an electronic processor 102 (for example, a microprocessor or another suitable processing device), a memory 104 (for example, a non-transitory computer-readable storage medium), and a communication interface 112. It should be understood that, in some embodiments, the first server 100 may include fewer or additional components in configurations different from that illustrated in FIG. 1. Also, the first server 100 may perform additional functionality than the functionality described herein. In addition, the functionality of the first server 100 may be incorporated into other servers, e.g., the second server 160. As illustrated in FIG. 1, the electronic processor 102, the memory 104, and the communication interface 112 are electrically coupled by one or more control or data buses enabling communication between the components.

[0018] The electronic processor 102 executes machine-readable instructions stored in the memory 104. For example, the electronic processor 102 may execute instructions stored in the memory 104 to perform the functionality described herein.

[0019] The memory 104 may include a program storage area (for example, read only memory (ROM)) and a data storage area (for example, random access memory (RAM), and other non-transitory, machine-readable medium). In some examples, the program storage area may store machine-executable instructions regarding an input profile record (IPR)

program 106 and a dual-layer identification service 110. In some examples, the data storage area may store data regarding an input profile record repository 108.

[0020] The IPR program 106 causes the electronic processor 102 to collect and store input profile records in the input profile record repository 108. Specifically, the IPR program 106 causes the electronic processor 102 to parse the IPR content received from a user interface device, determine biometric features based on the current IPR and historical/older IPRs associated with the user, and perform user identification using a biometric identification algorithm that compares current biometrics features based on a current IPR to the historical biometric features based on a set of historical IPRs. In some examples, a successful user identification may require ten historical IPRs associated with the user to establish a "user profile."

[0021] In some examples, the IPR program 106 also causes the electronic processor 102 to update a "user profile" stored in the input profile record repository 108. The "user profile" may be an account/device pair that stores the last x number of IPRs that are updated as a rolling window. In these examples, a single updated user profile may be functionally equivalent to a plurality of input profile records as described herein. Additionally, the user identification with the IPRs is a "passive" identification that does not need to query a user for additional information.

[0022] In some examples, the input profile record repository 108 is a central repository including a plurality of input profile records. Each input profile record is associated with a specific user. In some examples, an input profile record stored in the input profile record repository 108 may be updated periodically with the IPR program 106 as described above. The input profile record associated with the user is indicative of an identity of a user over a specific period of time. In other words, the input profile record as described herein solves the aforementioned problems with user identification because the input profile record is a dynamic identification of a user over a specific period of time rather than occurring at certain points in time and fixed to an initial biometric used to set up the user identification.

[0023] The dual-layer identification service 110 includes one or more passive biometrics models that may identify a user of the user interface device 120 based on a plurality of input profile records that are stored in the input profile record repository (referred to herein as a "first identification"). In some examples, the dual-layer identification service 110 generates

an identification response and an additional identification request from an attempt to identify the user of the user interface device 120 with the one or more passive biometrics models. In these examples, the identification response may indicate a verification of the user's identity or may indicate an inability to verify the user's identity.

[0024] Additionally, the dual-layer identification service 110 causes the electronic processor 102 to transmit the additional identification request and device characteristics of the user interface device 120 to the second server 160 via the network 180. The additional identification request requests additional verification of the user of the user interface device 120 that may be combined with the identification response to generate a blended response.

[0025] In some examples, a first model of the one or more passive biometrics models may identify the user of the user interface device 120 with a plurality of input profile records, each IPR based on a plurality of user inputs (e.g., user inputs with respect to a username and password) at a login page. Additionally or alternatively, in some examples, a second model of the one or more passive biometrics models may identify the user associated with a plurality of IPRs, each based on a plurality of user inputs (e.g., user inputs with respect to a behavioral one-time-passcode (OTP)) at a multifactor authentication page.

[0026] The communication interface 112 receives data from and provides data to devices external to the first server 100, such as the user interface device 120 via the network 180. For example, the communication interface 112 may include a port or connection for receiving a wired connection (for example, an Ethernet cable, fiber optic cable, a telephone cable, or the like), a wireless transceiver, or a combination thereof. In some examples, the network 180 is the Internet.

[0027] In the example of FIG. 1, the user interface device 120 includes an electronic processor 122 (for example, a microprocessor or another suitable processing device), a memory 124 (for example, a non-transitory computer-readable storage medium), a communication interface 132, a camera 134, a presence-sensitive display 136, and a device motion/orientation sensor(s) 138. In some examples, the user interface device may be a smartphone, tablet, laptop, or other suitable user interface device with a presence-sensitive display and an orientation sensor. As illustrated in FIG. 1, the electronic processor 122, the memory 124, the communication interface 132, the camera 134, the presence-sensitive

display 136, and the device motion/orientation sensor(s) 138 are electrically coupled by one or more control or data buses enabling communication between the components.

[0028] The electronic processor 122 executes machine-readable instructions stored in the memory 124. For example, the electronic processor 122 may execute instructions stored in the memory 124 to perform the functionality described herein.

[0029] The memory 124 may include a program storage area (for example, read only memory (ROM)) and a data storage area (for example, random access memory (RAM), and other non-transitory, machine-readable medium). The program storage area includes a user input collection and input profile record (IPR) application 126. In some examples, the user input collection and IPR application 126 may be a standalone application. In other examples, the user input collection and IPR application 126 is a feature that is part of a separate application (e.g., the user input collection and IPR application 126 may be included as part of a camera application, a banking application, or other suitable application).

[0030] The user input collection and IPR application 126 causes the electronic processor 122 to collect user inputs, i.e., user interactions, from a user relative to a mobile application (e.g., time to fill data field entries, use of specific autofill, or other suitable user inputs) of the user interface device 120 and generate an input profile record (IPR) based on the user inputs (also referred to as a "mobile platform"). The user input collection and IPR program 106 may also cause the electronic processor 122 to collect user inputs at a particular website (e.g., time to fill data field entries, use of specific autofill, or other suitable user inputs) and generate (or update) the input profile record based on these user inputs (also referred to as a "web platform").

[0031] In some examples, the user input collection and IPR application 126 causes the electronic processor 122 to collect user inputs with respect to the presence-sensitive display 136 (e.g., type of keyboard, typing speed, use of patterns, or other suitable user inputs (see Tables 1–3)). In these examples, the user input collection and IPR application 126 may also cause the electronic processor 122 to output the generated IPR to the server 100 via the communication interface 132 and the network 180. Additionally, in some examples, the user input collection and IPR application 126 may cause electronic processor 122 to control the memory 124 to store the user inputs that are collected and/or the IPR that is generated for a period of time or until the generated IPR is output to the server 100.

[0032] In other examples, the user input collection and IPR application 126 causes the electronic processor 122 to collect user inputs with respect to the camera 134 (e.g., facial recognition, user gestures, or other suitable user inputs), which may be part of the mobile platform. In these examples, the user input collection and IPR application 126 may also cause the electronic processor 122 to generate (or update) an IPR based on the aforementioned user inputs and output the IPR to the server 100 via the communication interface 132 and the network 180. Additionally, in some examples, the user input collection and IPR application 126 may cause electronic processor 122 to control the memory 124 to store the user inputs that are collected and/or the IPR that is generated for a period of time or until the generated IPR is output to the server 100.

[0033] The communication interface 132 receives data from and provides data to (e.g., generated IPR(s)) devices external to the user interface device 120, i.e., the server 100. For example, the communication interface 132 may include a port or connection for receiving a wired connection (for example, an Ethernet cable, fiber optic cable, a telephone cable, or the like), a wireless transceiver, or a combination thereof.

[0034] The camera 134 includes an image sensor that generates and outputs image data of a subject. In some examples, the camera 134 includes a semiconductor charge-coupled device (CCD) image sensor, a complementary metal-oxide-semiconductor (CMOS) image sensor, or other suitable image sensor. The electronic processor 122 receives the image data of the subject that is output by the camera 134.

[0035] The presence-sensitive display 136 includes a display screen with an array of pixels that generate and output images. In some examples, the display screen is one of a liquid crystal display (LCD) screen, a light-emitting diode (LED) and liquid crystal display (LCD) screen, a quantum dot light-emitting diode (QLED) display screen, an interferometric modulator display (IMOD) screen, a micro light-emitting diode display screen (mLED), a virtual retinal display screen, or other suitable display screen. The presence-sensitive display 136 also includes circuitry that is configured to detect the presence of the user. In some examples, the circuitry is a resistive or capacitive panel that detects the presence of an object (e.g., a user's finger).

[0036] The device motion/orientation sensor(s) 138 is a sensor that detects a movement and/or an orientation of the user interface device 120. In some examples, the device

motion/orientation sensor(s) 138 is an accelerometer, gyroscope, magnetometer, or other suitable device motion/orientation sensor that detects the motion and/or orientation of the user interface device 120.

[0037] It should be understood that, in some embodiments, the server 100 may include fewer or additional components in configurations different from that illustrated in FIG. 1. Also, the server 100 may perform additional functionality than the functionality described herein. In addition, some of the functionality of the user interface device 120 (for example, the IPR generation) may be incorporated into other servers (e.g., incorporated into the server 100). Likewise, some of the functionality of the server 100 may be incorporated into the user interface device 120 (for example, the user identification).

[0038] The second server 160 is similar to the first server 100. For example, the second server 160 includes an electronic processor (for example, a microprocessor or another suitable processing device), a memory (for example, a non-transitory computer-readable storage medium), and a communication interface. It should be understood that, in some embodiments, the second server 160 may include fewer or additional components in configurations different from the first server 100 that is illustrated in FIG. 1. Also, the second server 160 may perform additional or different functionality than the functionality described herein with respect to the first server 100. In other embodiments, the functionality described herein with respect to the second server 160 may be performed by the first server 100 and the second server 160 may be omitted.

[0039] The second server 160 may receive the additional identification request from the first server 100 via the network 180. The additional identification request from the first server 100 causes the second server 160 to perform a second identification of the user based on a set of device identification rules. The second identification of the user is not based on a biometric model (e.g., the one or more passive biometrics models as described above). Instead, the second identification is based on a set of device identification rules as set forth in Table 1 below.

Table 1 – Device Identification Rules

Rule Category	**Rules in Category**	**Inequality**	**Threshold at which**

			to trigger category
Frequent Rules	frequent device frequent city frequent state	>=	3
Known Rules	known device known geolocation normal user input	>=	2
Last 7 Days Location Rules	last 7 days city last 7 days country last 7 days state last 7 days zip code	>=	4
Last 7 Days Lat Long Rules	last 7 days latitude longitude 1000km last 7 days latitude longitude 100km last 7 days latitude longitude 10km	>=	3
Last 7 Days Device Rules	last 7 days DFP2 last 7 days DID last 7 days useragent last 7 days IP last 7 days IP org last 7 days endpoint last 7 days UDID last 7 days browser name	>=	4
Unfamiliar Rules	unfamiliar device unfamiliar state	<=	0
Login Familiarity Rules	login frequency familiarity login daytime familiarity	>=	1
Usual WPM Rules	account usual WPM endpoint usual WPM device usual WPM	>=	2
Anomalous Input Rules	no user interaction input anomaly	<=	0

Fraud Associated Rules	fraud associated account id fraud associated email domain fraud associated endpoint fraud associated IP negative cloud account id reputation negative cloud email domain reputation negative cloud endpoint reputation negative cloud IP reputation	<=	0
Frequent Anomalous Rules	frequent anomalous device frequent anomalous city frequent anomalous state	<=	0
Known Anomalous Rules	known anomalous device known anomalous geolocation	<=	0
Last 7 Days Anomalous Device Rules	last 7 days anomalous DFP2 last 7 days anomalous DID last 7 days anomalous useragent last 7 days anomalous IP last 7 days anomalous IP org last 7 days anomalous endpoint last 7 days anomalous UDID last 7 days anomalous browser name	<=	0
Last 7 Days Anomalous Lat Long Rules	last 7 days anomalous latitude longitude 1000km last 7 days anomalous latitude longitude 100km last 7 days anomalous latitude longitude 10km	<=	0
Last 7 Days Anomalous Location Rules	last 7 days anomalous city last 7 days anomalous country last 7 days anomalous state last 7 days anomalous zip code	<=	0

Anomalous Login Familiarity Rules	anomalous login frequency familiarity anomalous login daytime familiarity	<=	0

[0040] In Table 1, the frequent rules category includes a frequent device rule, a frequent city rule, and a frequent state rule. The frequent device rule looks for successful logins using same device in last 4 weeks associated with the account. The device includes device identifier (DID) and device fingerprint (DFP). The frequent city rule looks for successful logins using same IP city in last 4 weeks associated with the account. The frequent state rule looks for successful logins using same IP state in last 4 weeks associated with the account. The frequent rules category triggers with a threshold equal to three.

[0041] However, while the threshold may be interpreted as "equal to three," the thresholds in Table 1 are defined according to inequality. The use of inequality makes an optimization process for each client easier than the use of equality. All the thresholds described herein may be interpreted from the perspective of equality for ease of understanding, however, the thresholds are defined from the perspective of inequality.

[0042] In Table 1, the known rules category includes a known device rule, a known geolocation rule, and a normal user input rule. The known device rule uses several device anchors and several time periods to calculate a percentage of successful logins associated with the account (e.g., 30% or more successful logins). The known geolocation rule uses several geo anchors and several time periods to calculate a percentage of successful logins associated with the account (e.g., 30% or more successful logins). The normal user input rule looks into widget cycle data to see if the user input is "normal" and is not account based. The known rules category triggers with a threshold greater than or equal to two.

[0043] In Table 1, the last 7 days location rules category includes a last 7 days city rule, a last 7 days country rule, a last 7 days state rule, and a last 7 days zip code rule. These rules check whether there are successful logins in last 7 days by the same anchor (i.e., city, country, state, or zip code) associated with the account. The last 7 days location rules category triggers with a threshold greater than or equal to four.

[0044] In Table 1, the last 7 days latitude longitude rules category includes a last 7 days latitude longitude 1000km rule, a last 7 days latitude longitude 100km rule, and a last 7 days latitude longitude 10km rule. These rules check whether there are successful logins in last 7

days by the same anchor (i.e., a latitude and longitude within a distance of 1000km, 100km, or 10km) associated with the account. The last 7 days latitude longitude rules category triggers with a threshold greater than or equal to three.

[0045] In Table 1, the last 7 days device rules category includes a last 7 days DFP2 rule, a last 7 days DID rule, a last 7 days useragent rule, a last 7 days IP rule, a last 7 days IP org rule, a last 7 days endpoint rule, a last 7 days UDID rule, and a last 7 days browser name rule. These rules check whether there are successful logins in last 7 days by the same anchor (i.e., a second device fingerprint (DFP2), a device identifier (DID), a device's user agent, a device's IP, an organization of the device's IP, a device's endpoint, a device's universal device identifier (UDID), a name of the device's web browser) associated with the account. The last 7 days device rules category triggers with a threshold greater than or equal to four.

[0046] In Table 1, the unfamiliar rules category includes an unfamiliar device rule and an unfamiliar state rule. The unfamiliar device rule looks for zero successful logins of the device anchor defined and associated with the account. The unfamiliar state rule looks for zero successful logins of the state anchor defined and associated with the account. The unfamiliar rules category triggers with a threshold equal to zero.

[0047] In Table 1, the login familiarity rules category includes a login frequency familiarity rule and a login daytime familiarity rule. The login frequency familiarity rule checks whether current login is occurring within a time window based on their successful login frequency. The login daytime familiarity rule checks whether current login is during a time of week that the user most frequently successfully logs in. The login familiarity rules category triggers with a threshold greater than or equal to one.

[0048] In Table 1, the usual words-per-minute (WPM) rules category includes an account usual WPM rule, an endpoint usual WPM rule, and a device usual WPM rule. The account usual WPM rule looks at whether the observed WPM is within a certain bound associated to the account, and the bound is set pretty wide +/- 40 WPM currently (i.e. "outliers"). The endpoint usual WPM rule looks at whether observed WPM is within a certain bound associated to the endpoint, and the bound is set pretty wide +/- 40 WPM currently (i.e. "outliers"). The device usual WPM rule looks at whether observed WPM is within a certain bound associated to the device, and the bound is set pretty wide +/- 40 WPM currently (i.e.

"outliers"). The usual WPM rules category triggers with a threshold greater than or equal to two.

[0049] In Table 1, the anomalous rules category includes a no user interaction rule and an input anomaly rule. The no user interaction rule looks for any user interaction associated with the transaction by looking at various input methods such as keyboard typing, mouse clicks and form focus events, and triggers when all of the input methods indicate no activity detected. The input anomaly rule looks at whether an anomalous input was observed during the request. The anomalous rules category triggers with a threshold equal to zero.

[0050] In Table 1, the fraud associated rules category includes a fraud associated account id rule, a fraud associated email domain rule, a fraud associated endpoint rule, a fraud associated IP rule, a negative cloud account id reputation rule, a negative cloud email domain reputation rule, a negative cloud endpoint reputation rule, and a negative cloud IP reputation rule. The a fraud associated account id rule, the fraud associated email domain rule, the fraud associated endpoint rule, and the fraud associated IP rule looks at whether the anchor (i.e., the account id, the email domain, the endpoint (DFP2 and IP), or the IP) has been associated with recent fraud. The negative cloud account id reputation rule, the negative cloud email domain reputation rule, the negative cloud endpoint reputation rule, and the negative cloud IP reputation rule looks at whether the anchor (i.e., the account id, the email domain, the endpoint (DFP2 and IP), or the IP) has been associated with negative activity globally. The fraud associated rules category triggers with a threshold equal to zero.

[0051] In Table 1, the frequent anomalous rules category includes a frequent anomalous device rule, a frequent anomalous city rule, and a frequent anomalous state rule. The frequent anomalous rules category looks for three or more red scored logins from an anchor (i.e., device, city, and State) in the past four weeks. As described herein, a “red scored login” is a high risk or likely fraudulent login. The frequent anomalous rules category triggers with a threshold equal to zero.

[0052] In Table 1, the known anomalous rules category includes a known anomalous device rule and a known anomalous geolocation rule. The known anomalous rules category uses several anchors (i.e., device or geographical anchors) and several time periods to look for a percentage of red scored logins associated with the account in the past four weeks. The known anomalous rules category triggers with a threshold equal to zero.

[0053] In Table 1, the last 7 days anomalous location rules category includes a last 7 days city rule, a last 7 days country rule, a last 7 days state rule, and a last 7 days zip code rule. These rules check whether there are one or more red scored login in last 7 days by the same anchor (i.e., city, country, state, or zip code) associated with the account. The last 7 days anomalous location rules category triggers with a threshold equal to zero.

[0054] In Table 1, the last 7 days anomalous latitude longitude rules category includes a last 7 days latitude longitude 1000km rule, a last 7 days latitude longitude 100km rule, and a last 7 days latitude longitude 10km rule. These rules check whether there are one or more red scored logins in last 7 days by the same anchor (i.e., a latitude and longitude within a distance of 1000km, 100km, or 10km) associated with the account. The last 7 days anomalous latitude longitude rules category triggers with a threshold equal to zero.

[0055] In Table 1, the last 7 days anomalous device rules category includes a last 7 days DFP2 rule, a last 7 days DID rule, a last 7 days useragent rule, a last 7 days IP rule, a last 7 days IP org rule, a last 7 days endpoint rule, a last 7 days UDID rule, and a last 7 days browser name rule. These rules check whether there are one or more red scored logins in last 7 days by the same anchor (i.e., a second device fingerprint (DFP2), a device identifier (DID), a device's user agent, a device's IP, an organization of the device's IP, a device's endpoint, a device's universal device identifier (UDID), a name of the device's web browser) associated with the account. The last 7 days anomalous device rules category triggers with a threshold equal to zero.

[0056] In Table 1, the anomalous login familiarity rules category includes a login frequency familiarity rule and a login daytime familiarity rule. The login frequency familiarity looks for a red scored login frequency pattern of a device associated with the account. The login daytime familiarity rule looks for a red scored login time pattern of a device associated with the account. The anomalous login familiarity rules category triggers with a threshold equal to zero.

[0057] The second server 160 performs the second identification and confirms it is the same user when the combined categories triggered is greater than or equal to an upper "same user" threshold. For example, an upper threshold of fourteen categories.

[0058] Conversely, the second server 160 performs the second identification and confirms it is a different user when the combined categories triggered is less than or equal to

a lower “different user” threshold that is different from the upper threshold. For example, a lower threshold of eleven categories.

[0059] Lastly, the second server 160 designates a user as an “unknown user” when the combined categories triggered is between the upper threshold and the lower threshold. For example, twelve or thirteen categories when the upper threshold is fourteen categories and the lower threshold is eleven categories.

[0060] When the first server 100 cannot perform the first identification (i.e., identification with passive biometric models), then the first server 100 relies upon the second server 160 to perform the second identification on whether the user is the same or different users. For example, when the first server 100 cannot perform the first identification for some reason (e.g., the user uses auto-fill), then the first server 100 relies on the second identification performed by the second server 160 to determine whether the user is the same or different users.

[0061] When the first server 100 can perform the first identification (i.e., identification with passive biometric models), then the first server 100 relies upon the second server 160 to increase or decrease the biometric thresholds associated with the passive biometric model. For example, when the first identification is available and the “Unfamiliar Rules category” is triggered, then the first server 100 may increase an upper biometric threshold by 2% and increase a lower biometric threshold by 5%. In other words, an “unfamiliar” event changes the thresholds of the passive biometric model to reduce the chance of a same user match.

[0062] In a different example, when the first identification is available and the “Frequent Rules category” is triggered, then the first server 100 may lower the upper biometric threshold by 4% and decrease the lower biometric threshold by 8%. In other words, an “frequent” event changes the scoring thresholds of the passive biometric model to increase the chance of a same user match.

[0063] In some examples, the upper and lower biometric thresholds are numbers between 1 and 0, and the upper biometric threshold is a larger number than the lower biometric threshold. When a passive biometric score from one or more passive biometric models is greater than the upper biometric threshold, then the passive biometric score indicates it is a same user. When a passive biometric score from one or more passive biometric models is lower than the lower biometric threshold, then the passive biometric score indicates it is a

different user. When a passive biometric score from one or more passive biometric models is between the upper biometric threshold and the lower biometric threshold, then the passive biometric score is deemed undetermined.

[0064] The second identification performed by the second server 160 helps to reduce the instances that the passive biometric score is deemed undetermined by helping to adjust the passive biometric score. Additionally, the second identification performed by the second server 160 helps to identify the user in the event the passive biometric score is either unavailable or deemed undetermined.

[0065] FIG. 2 is a flow diagram illustrating the dual-layer service 110 of FIG. 1, in accordance with various aspects of the present disclosure. FIG. 2 is described with respect to FIG. 1. As illustrated in FIG. 2, the dual-layer service 110 includes login traffic database 202, a first layer 204, a second layer 206, and a user identity determination 208.

[0066] The first layer 204 includes qualified login traffic from the login traffic database 202 that is processed by the first server 100 with a biometrics model 210 (e.g., an active biometrics model or a passive biometrics model) to output a response for user identification in the second layer 206. In some examples, the passive biometrics model is at least one of a login information passive biometrics model or a one-time-passcode (OTP) passive biometrics model.

[0067] The second layer 206 includes the response from the first layer 205 that is processed by the second server 160 with device identification rules 212 (for example, the device identification rules set forth in Table 1). The device identification rules 212 may be used to enhance the biometrics score that is part of the identification response of the first server 100, where the first server 100 generates a blended identification response that classifies a user as “match,” “no-match,” or “undetermined” in the user identity determination 208. For example, if many “unfamiliar device” related rules are triggered in the device identification rules 212, the biometric thresholds are increased, whereas if many “familiar device” rules are triggered in the device identification rules 212, the biometric thresholds are decreased. The first server 100 re-analyzes both the biometrics score enhanced with the triggered rules to determine an overall match category for the blended identification response in the user identity determination 208.

[0068] Additionally, when the login traffic is disqualified, the disqualified login traffic from the login traffic database 202 is processed directly by the second server 160 with the device identification rules 212 to output an identification response for the user identity determination 208. The disqualified login traffic includes login attempts with auto-filled entries, invalid IPR data, or other login traffic that is disqualified or unsuitable for a biometrics model. In these examples, only triggered rules from the device identification rules 212 will be used to classify whether a user is "match," "no-match," or "undetermined" in the user identity determination 208.

[0069] FIG. 3 is a flowchart illustrating a method 300 for identifying a user, in accordance with various aspects of the present disclosure. FIG. 3 is described with respect to FIG. 1.

[0070] The method 300 includes detecting, with an electronic processor, an access request by a user of a user interface device (at block 302). For example, the electronic processor 102 detects an access request by a user of the user interface device 120 at a login page. Although the access request described herein is a login attempt, the method 300 is not limited to a login attempt. The method 300 is equally applicable to any form of access request, for example, an access request with respect to a remuneration vehicle.

[0071] The method 300 includes retrieving, with the electronic processor, a plurality of input profile record associated with the user from an input profile record repository in a memory in response to detecting the access request of the user, each of the plurality of input profile records including a plurality of user inputs from the user interacting with a webpage (at block 304). For example, the electronic processor 102 retrieves a plurality of input profile records associated with the user from the input profile record repository 108 in the memory 104 in response to the electronic processor 102 detecting the access request of the user. Each of the plurality of input profile records includes a plurality of user inputs from the user interacting with a webpage (e.g., one or more previous interactions with the login page or one or more previous interactions with a 3DS challenge page) or a mobile application.

[0072] The method 300 includes performing, with the electronic processor, an identification of the user with one or more passive biometrics models and the plurality of input profile records that are retrieved (at block 306). For example, the electronic processor 102 performs an identification of the user with one or more passive biometrics models that

are included in the dual-layer identification service 110 and the plurality of input profile records that are retrieved.

[0073] The method 300 includes generating, with the electronic processor, an identification response and an additional identification request based on an outcome of the identification of the user with the one or more passive biometrics models and the plurality of input profile records that are retrieved (at block 308). For example, the electronic processor 102 generates an identification response and an additional identification request based on an outcome of the identification of the user with the one or more passive biometrics models included in the dual-layer identification service 110 and the plurality of input profile records that are retrieved.

[0074] In some examples, the identification response includes a passive biometric score of the user, an upper biometric threshold, and a lower biometric threshold. The upper biometric threshold being a threshold that indicates the user is the same as a previous user. The lower biometric threshold being a threshold that indicates the user is a different user. Additionally, in some examples, the passive biometric score of the user is skipped entirely when the outcome of the identification of the user is a failed identification of the user using the one or more passive biometrics models.

[0075] The method 300 includes controlling, with the electronic processor, a communication interface to transmit the additional identification request to a second server via a network (at block 310). For example, the electronic processor 102 controls the communication interface 112 to transmit the additional identification request with device characteristics of the user interface device 120 to the second server 160 via the network 180.

[0076] The method 300 includes receiving, with the electronic processor, a second identification response from the second server via the communication interface and the network (at block 312). For example, the electronic processor 102 receives a second identification response from the second server 160 via the communication interface 112 and the network 180.

[0077] The method 300 includes generating, with the electronic processor, a blended response by modifying one or more characteristics of the identification response with the second identification response, the blended response indicating the identification of the user (at block 314). For example, the electronic processor 102 generates a blended response by

modifying one or more characteristics of the identification response with the second identification response, the blended response indicating the identification of the user.

[0078] In some examples, the blended response includes the passive biometric score of the user, a modified upper biometric threshold, and a modified lower biometric threshold. The modified upper biometric threshold being a threshold that indicates the user is the same as a previous user and is increased or decreased based on the second identification response. The modified lower biometric threshold being a threshold that indicates the user is a different user and is increased or decreased based on the second identification response.

[0079] Additionally, in some examples, the passive biometric score of the user is skipped when the outcome of the identification of the user is a failed identification of the user using the one or more passive biometrics models. In other words, the second identification response replaces the null value of the passive biometric score to result in the blended response indicating the user is the same as a previous user.

[0080] In some examples, the method 300 may further include granting or denying access according to the access request based on the blended response. In other examples, the method 300 may further include outputting the blended response to control a third device to grant or deny access according to the access request based on the blended response.

[0081] In some examples, the additional identification request indicates to the second server 160 that the outcome of the identification of the user is a successful identification of the user. In these examples, the additional identification request is a request for an additional user identification based on device identification rules that enhances the successful identification of the user.

[0082] In some examples, the device identification rules are divided into a plurality of categories, the additional user identification is based on categories of the device identification rules that are triggered, and modifying the one or more characteristics of the identification response with the second identification response further includes adjusting biometric thresholds of the one or more passive biometrics models based on the categories of the device identification rules that are triggered.

[0083] In some examples, the additional identification request indicates to the second server 160 that the outcome of the identification of the user is a failed identification of the

user. In these examples, the additional identification request is a request for an additional user identification based on device identification rules.

[0084] In some examples, the device identification rules are divided into a plurality of categories. In these examples, the additional user identification is based on categories of the device identification rules that are triggered.

[0085] In some examples, the plurality of categories may include a frequent rules category, a known rules category, last 7 days location rules category, last 7 days latitude and longitude rules category, last 7 days device rules category, unfamiliar rules category, login familiarity rules category, usual words-per-minute (WPM) rules category, anomalous input rules category, fraud associated rules category, frequent anomalous rules category, known anomalous rules category, last 7 days anomalous device rules category, last 7 days anomalous latitude and longitude rules category, last 7 days anomalous location rules category, and an anomalous login familiarity rules category.

[0086] Additionally, in some examples, the frequent rules category has a trigger threshold of three or more rules, wherein the known rules category has a trigger threshold of two or more rules, wherein the last 7 days location rules category has a trigger threshold of four or more rules, wherein the last 7 days latitude and longitude rules category has a trigger threshold of three or more rules, wherein the last 7 days device rules category has a trigger threshold of four or more rules, unfamiliar rules category has a trigger threshold of zero rules, wherein the login familiarity rules category has a trigger threshold of one or more rules, wherein the usual words-per-minute (WPM) rules category has a trigger threshold of two or more rules, wherein the anomalous input rules category has a trigger threshold of zero rules, wherein the fraud associated rules category has a trigger threshold of zero rules, wherein the frequent anomalous rules category has a trigger threshold of zero rules, wherein the known anomalous rules category has a trigger threshold of zero rules, wherein the last 7 days anomalous device rules category has a trigger threshold of zero rules, wherein the last 7 days anomalous latitude and longitude rules category has a trigger threshold of zero rules, wherein the last 7 days anomalous location rules category has a trigger threshold of zero rules, and wherein the anomalous login familiarity rules category has a trigger threshold of zero rules.

[0087] Additionally, in some examples, the second identification response from the additional user identification indicates the user is a same user when the plurality of categories

has a first combined total of greater than or equal to a first number of categories triggered. Lastly, in some examples, the second identification response from the additional user identification indicates the user is a different user when the plurality of categories has a second combined total of less than or equal to a second number of categories triggered that is less than the first number.

[0088] Thus, the present disclosure provides, among other things, user identification with a blended response from a dual-layer identification service. Various features and advantages of the invention are set forth in the following claims.

CLAIMS

What is claimed is:

1. A server comprising:

a communication interface configured to communicate with a second server via a network;

a memory including an input profile record (IPR) program, an IPR repository, and a dual-layer identification service; and

an electronic processor, when executing the IPR program, configured to:

detect an access request by a user of a user interface device, and

retrieve a plurality of input profile records associated with the user from the input profile record repository in the memory in response to detecting the access request of the user, each of the plurality of input profile records including a plurality of user inputs from the user interacting with a webpage or mobile application,

wherein, when executing the dual-layer identification service, the electronic processor is configured to:

perform an identification of the user with one or more passive biometrics models and the plurality of input profile records that are retrieved,

generate an identification response and an additional identification request based on an outcome of the identification of the user with the one or more passive biometrics models and the plurality of input profile records that are retrieved,

control the communication interface to transmit the additional identification request to the second server via the network, wherein the additional identification request causes the second server to perform a second identification of the user, the second identification being based on a set of device identification rules associated with a device of the user,

receive a second identification response from the second server via the communication interface and the network, wherein the second identification response indicates whether the user is a same user or a different user, and

generate a blended response by modifying one or more characteristics of the identification response with the second identification response, the blended response indicating the identification of the user, wherein modifying one or more characteristics of the identification response comprises adjusting biometric thresholds

of the one or more passive biometric models based on one or more of the set of device identification rules.

2. The server of claim 1, wherein the additional identification request indicates to the second server that the outcome of the identification of the user is a successful identification of the user, and wherein the additional identification request is a request for an additional user identification based on device identification rules that enhances the successful identification of the user.

3. The server of claim 2, wherein the device identification rules are divided into a plurality of categories, wherein the additional user identification is based on all of the plurality of categories of the device identification rules that are triggered, and wherein modifying the one or more characteristics of the identification response with the second identification response further includes adjusting biometric thresholds of the one or more passive biometrics models based on the categories of the device identification rules that are triggered.

4. A method for identifying a user, the method comprising:

detecting, with an electronic processor, an access request by the user of a user interface device;

retrieving, with the electronic processor, a plurality of input profile records associated with the user from an input profile record repository in a memory in response to detecting the access request of the user, each of the plurality of input profile records including a plurality of user inputs from the user interacting with a webpage or a mobile application;

performing, with the electronic processor, an identification of the user with one or more passive biometrics models and the plurality of input profile records that are retrieved;

generating, with the electronic processor, an identification response and an additional identification request based on an outcome of the identification of the user with the one or more passive biometrics models and the plurality of input profile records that are retrieved;

controlling, with the electronic processor, a communication interface to transmit the additional identification request to a second server via a network, wherein the additional identification request causes the second server to perform a second identification of the user, the second identification being based on a set of device identification rules associated with a device of the user;

receiving, with the electronic processor, a second identification response from the second server via the communication interface and the network, wherein the second identification response indicates whether the user is a same user or a different user; and

generating, with the electronic processor, a blended response by modifying one or more characteristics of the identification response with the second identification response, the blended response indicating the identification of the user, wherein modifying one or more characteristics of the identification response comprises adjusting biometric thresholds of the one or more passive biometric models based on one or more of the set of device identification rules.

5. The method of claim 4, wherein the additional identification request indicates to the second server that the outcome of the identification of the user is a successful identification of the user, and wherein the additional identification request is a request for an additional user identification based on device identification rules that enhances the successful identification of the user.

6. The method of claim 5, wherein the device identification rules are divided into a plurality of categories, wherein the additional user identification is based on all of the plurality of categories of the device identification rules that are triggered, and wherein modifying the one or more characteristics of the identification response with the second identification response further includes adjusting biometric thresholds of the one or more passive biometrics models based on the categories of the device identification rules that are triggered.

7. The server of claim 1 or method of claim 4, wherein the additional identification request indicates to the second server that the outcome of the identification of the user is a failed identification of the user, and wherein the additional identification request is a request for an additional user identification based on device identification rules.

8. The server of claim 1, or the method of claim 7, wherein the device identification rules are divided into a plurality of categories, and wherein the additional user identification is based on all of the plurality of categories of the device identification rules that are triggered.

9. The server of claim 1, or the method of claim 8, wherein the plurality of categories includes a frequent rules category, a known rules category, last 7 days location rules category, last 7 days latitude and longitude rules category, last 7 days device rules category, unfamiliar rules category, login familiarity rules category, usual words-per-minute (WPM) rules category, anomalous input rules category, fraud associated rules category, frequent anomalous rules category, known anomalous rules category, last 7 days anomalous device rules category, last 7 days anomalous latitude and longitude rules category, last 7 days anomalous location rules category, and an anomalous login familiarity rules category.

10. The server of claim 1, or the method of claim 9, wherein the frequent rules category has a trigger threshold of three or more rules, wherein the known rules category has a trigger threshold of two or more rules, wherein the last 7 days location rules category has a trigger threshold of four or more rules, wherein the last 7 days latitude and longitude rules category has a trigger threshold of three or more rules, wherein the last 7 days device rules category has a trigger threshold of four or more rules, unfamiliar rules category has a trigger threshold of zero rules, wherein the login familiarity rules category has a trigger threshold of one or more rules, wherein the usual words-per-minute (WPM) rules category has a trigger threshold of two or more rules, wherein the anomalous input rules category has a trigger threshold of zero rules, wherein the fraud associated rules category has a trigger threshold of zero rules, wherein the frequent anomalous rules category has a trigger threshold of zero rules, wherein the known anomalous rules category has a trigger threshold of zero rules, wherein the last 7 days anomalous device rules category has a trigger threshold of zero rules, wherein the last 7 days anomalous latitude and longitude rules category has a trigger threshold of zero rules, wherein the last 7 days anomalous location rules category has a trigger threshold of zero rules, and wherein the anomalous login familiarity rules category has a trigger threshold of zero rules.

11. The server of claim 1, or the method of claim 10, wherein the second identification response from the additional user identification indicates the user is the same user when the plurality of categories has a first combined total of greater than or equal to a first number of categories triggered, and wherein the second identification response from the additional user identification indicates the user is a different user when the plurality of categories has a second combined total of less than or equal to a second number of categories triggered that is less than the first number.

12. A system comprising:

a first server; and

a second server,

wherein the first server includes

a communication interface configured to communicate with the second server via a network;

a memory including an input profile record (IPR) program, an IPR repository, and a dual-layer identification service; and

an electronic processor, when executing the IPR program, configured to:

detect an access request by a user of a user interface device, and

retrieve a plurality of input profile records associated with the user from an input profile record repository in the memory in response to detecting the access request of the user, each of the plurality of input profile records including a plurality of user inputs from the user interacting with a webpage or a mobile application,

wherein, when executing the dual-layer identification server, the electronic processor is configured to:

perform an identification of the user with one or more passive biometrics models and the plurality of input profile records that are retrieved,

generate an identification response and an additional identification request based on an outcome of the identification of the user with the one or more passive biometrics models and the plurality of input profile records that are retrieved,

control the communication interface to transmit the additional identification request to the second server via the network, wherein the additional identification request causes the second server to perform a second identification of the user, the second identification being based on a set of device identification rules associated with a device of the user,

receive a second identification response from the second server via the communication interface and the network, wherein the second identification response indicates whether the user is a same user or a different user, and

generate a blended response by modifying one or more characteristics of the identification response with the second identification response, the

blended response indicating the identification of the user, wherein modifying one or more characteristics of the identification response comprises adjusting biometric thresholds of the one or more passive biometric models based on one or more of the set of device identification rules.

13. The server of claim 1, the method of claim 4 or the system of claim 12, wherein the additional identification request indicates to the second server that the outcome of the identification of the user is a successful identification of the user, and wherein the additional identification request is a request for an additional user identification based on device identification rules that enhances the successful identification of the user.

14. The system of claim 13, wherein the device identification rules are divided into a plurality of categories, wherein the additional user identification is based on all of the plurality of categories of the device identification rules that are triggered, and wherein modifying the one or more characteristics of the identification response with the second identification response further includes adjusting biometric thresholds of the one or more passive biometrics models based on the categories of the device identification rules that are triggered.

15. The system of claim 12, wherein the additional identification request indicates to the second server that the outcome of the identification of the user is a failed identification of the user, and wherein the additional identification request is a request for an additional user identification based on device identification rules.