January 2023

CONTINUOUS AUTHENTICATION USING ACCESSIBILITY SETTINGS AND USAGE ANALYSIS

Rakesh Ramamurthy
Visa

Amrendra Narayan Jha
Visa

Avi Bomb
Visa

Santosh Kumar KVS
Visa

Madhusmita Mohapatra
Visa

TITLE: "CONTINUOUS AUTHENTICATION USING ACCESSIBILITY SETTINGS AND USAGE ANALYSIS"

VISA

Inventors:

Rakesh Ramamurthy

AMRENDRA NARAYAN JHA

Avi Bomb

Santosh Kumar KVS

Madhusmita Mohapatra

TECHNICAL FIELD

[0001] This disclosure relates generally to the field of software application security. More particularly, the present disclosure relates to a system and method for authentication of a user using accessibility settings and usage analysis the device.

BACKGROUND

[0002] Multi-factor authentication (MFA; encompassing two-factor authentication, or 2FA) is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. These factors can be one or more of three things: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). MFA protects user data—which may include personal identification or financial assets—from being accessed by an unauthorized third party that may have been able to discover, for example, a single password.

[0003] Enforcing MFA every time a user tries to login to a device for example a mobile application, will hamper its useability and would result in a bad user experience. At the same time by-passing MFA also poses security risks in the form of an account being taken over or being hacked as the user's username/password would be compromised.

[0004] Many of the existing behavioural analysis solution where some of the user's behaviour like, typing speed, Wi-Fi settings, touch details etc, may not be suitable for specially abled users, as their behaviour is different when compared with regular users. Thus, a system is needed to gather data and make an informed decision about whether a user is a fraudster and should be blocked from using a mobile application.

[0005] Therefore, there is a need for an efficient way of solving one or more of the above mentioned problems.

SUMMARY:

[0006] The proposed solution is an Artificial Intelligence (AI) based system, which continuously captures and analyses a specially abled user's behaviour and accessibility settings in order to come up with the risk based score. This risk score will then be used to decide whether or not to skip MFA.

BRIEF DESCRIPTION OF THE DRAWINGS AND APPENDICES

[0007] The features and characteristics of the present invention, as well as the methods of operation and functions of the related elements of structures and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification, wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of the invention. As used in the specification, the singular form of "a," "an," and "the" include plural referents unless the context clearly dictates otherwise.

[0008] Additional advantages and details of non-limiting embodiments are explained in greater detail below with reference to the exemplary embodiments that are illustrated in the accompanying schematic figures, in which:

[0009] Fig. 1 discloses a flowchart diagram for collecting accessibility settings and training the machine learning model.

[0010] Fig. 2 discloses a flowchart diagram of authentication flow.

[0011] FIG. 3 is a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

DESCRIPTION OF THE DISCLOSURE

[0012] 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.

[0013] 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.

[0014] 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.

[0015] 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.

[0016] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0017] As used herein, the terms “communication”, “communicate”, “post”, “sent”, “return” and “returned” may refer to the reception, receipt, transmission, transfer, provision, and/or the like of information (e.g., data, signals, messages, instructions, commands, and/or the like). For one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication with another unit means that the one unit is able to directly or indirectly receive information from and/or transmit information to the other unit. This may refer to a direct or indirect connection (e.g., a direct communication connection, an indirect communication connection, and/or the like) that is wired and/or wireless in nature.

Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives information and does not actively transmit information to the second unit. As another example, a first unit may be in communication with a second unit if at least one intermediary unit (e.g., a third unit located between the first unit and the second unit) processes information received from the first unit and communicates the processed information to the second unit. In some non-limiting embodiments, a message may refer to a network packet (e.g., a data packet and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

[0018] As used herein, the term "computing system" may refer to one or more electronic devices that are configured to directly or indirectly communicate with or over one or more networks. A computing system may be a mobile or portable computing device, a desktop computer, a server, mobile phones (e.g., cellular phones), PDAs, tablet computers, net books, laptop computers, personal music players, hand-held specialized readers, wearable devices (e.g., watches), vehicles (e.g., cars) and/or the like. Furthermore, the term "computer" may refer to any computing device that includes the necessary components to receive, process, and output data, and normally includes a display, a processor, a memory, an input device, and a network interface. A "computing system" may include one or more computing devices or computers. An "application" or "Application Program Interface" (API) refers to computer code or other data sorted on a computer-readable medium that may be executed by a processor to facilitate the interaction between software components, such as a client-side front-end and/or server-side back-end for receiving data from the client. An "interface" refers to a generated display, such as one or more graphical user interfaces (GUIs) with which a user may interact, either directly or indirectly (e.g., through a keyboard, mouse, touchscreen, etc.). Further, multiple computers, e.g., servers, or other computerized devices, such as an autonomous vehicle including a vehicle computing system, directly or indirectly communicating in the network environment may constitute a "system" or a "computing system".

[0019] As used herein, the term "credential" may refer to any suitable information that serves as reliable evidence of worth, ownership, identity, or authority. An "access credential" may be a credential that may be used to gain access to a particular resource (e.g., a good, service, location, etc.). A credential may be a string of numbers, letters, or any other suitable characters, or any object or document that can serve as confirmation. Examples of credentials include identification cards, certified documents, access cards, passcodes and other login information, payment account numbers, access badge numbers, payment tokens, etc.

[0020] As used herein, the term "user" may include an individual. In some embodiments, a user may be associated with one or more personal accounts and/or mobile devices.

.

[0021] As used herein, the term "processor" may refer to any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to accomplish a desired function. The processor may include CPU comprises at least one high-speed data processor adequate to execute program components for executing user and/or system-generated requests. The CPU may be a microprocessor such as AMD's Athlon, Duron and/or Opteron; IBM and/or Motorola's PowerPC; IBM's and Sony's Cell processor; Intel's Celeron, Itanium, Pentium, Xeon, and/or XScale; and/or the like processor(s).

[0022] As used herein, the term "memory" may be any suitable device or devices that can store electronic data. A suitable memory may comprise a non-transitory computer readable medium that stores instructions that can be executed by a processor to implement a desired method. Examples of memories may comprise one or more memory chips, disk drives, etc. Such memories may operate using any suitable electrical, optical, and/or magnetic mode of operation.

[0023] It will be apparent that systems and/or methods, described herein, can be implemented in different forms of hardware, software, or a combination of hardware and software. The actual specialized control hardware or software code used to implement these systems and/or methods is not limiting of the implementations. Thus, the operation and behavior of the systems and/or methods are described herein without reference to specific software code, it being understood that software and hardware can be designed to implement the systems and/or methods based on the description herein.

[0024] In an embodiment, AI based system, which continuously captures and analyses a specially abled user’s behaviour and accessibility settings in order to come up with the risk based score. This risk score will then be used to decide whether or not to skip MFA. A combination of multiple accessibility settings parameters is used to identify users uniquely. This includes, but is not limited to:

1. **Visibility enhancements**: Normal, High Contrast or Large Display
    i. High Contrast with different color modes like (Yellow, Blue or any custom color).
    ii. High Contrast Fonts: Used to adjust color and outline of fonts to make them stand out.
    iii. High Contrast keyboard: Used to adjust color of the keyboard.
    iv. Highlight buttons: Highlights the buttons in app.
    v. Color inversion: Reverse the colors on your screen so that light colous appear dark and vice versa. This also sets the screen mode to Vivid.
    vi. Color adjustment: If user has trouble seeing some colors, this setting may make things clearer.
    vii. Add color filter: User can add color filter over the entire screen. This may help make text easier to read.
    viii. Remove animations: Prevent screen effects. Useful if you are sensitive to animations or screen movement.
    ix. Reduce transparency: Reduce visual effects and menus to make them easier to see.
    x. Magnification: User can magnify the full screen or use the magnifier window. If user choose the magnifier window, he/she will see the zoomed-in window immediately after using the shortcut. If user choose full screen, one can choose to zoom in continuously or temporarily.
    We can use this information to evaluate user uniquely.
    xi. Large mouse/touchpad pointer: User can use this setting to increase size of mouse/touchpad pointer.
    xii. Font size and style: User can use their own font styles, bold font, and font sizes which can be used as one of the parameters to identify the unique user.
    xiii. Screen zoom: User can make the items on the screen smaller or larger.

2. **Hearing enhancements**: These settings will be used by users with hearing impairment.
    i. Live transcribe: Can be any 3rd party apps.

ii. Live Caption: Detects speech on users' device and automatically generates captions. Some of the fine-grained settings are as follows:
Languages: Language of caption
Profanity: Profanity will be replaced by asterisk symbol *
Show sound labels: Includes sounds like laughter, applause and music.
Live caption in volume control:

iii. Caption preference: Will be used to change caption settings.

iv. Sound detectors.

v. Doorbell: No doorbell sound recorded.

vi. Hearing aid support

   1. Hearing aid compatibility: Adjust the user (specially abled) phone's audio so it works better with hearing aids.
   2. Bluetooth hearing aids: External device.

vii. Amplify ambient sound: Amplify the world around you. Hear distant sounds clearly, and put the focus on conversations even when the user is somewhere noisy (recommended to use headphones for this settings)

viii. Adapt sound: user ears are unique. The user may be more sensitive or less sensitive to certain frequencies of sound compared to other people. The user hearing varies with age and may even differ from your left ear to your right ear.
Adapt sound gives user perfect sound that's tuned just for the user ears. It works whenever you are wearing headphones.
Choose a preset that matches their age, or try a hearing test to get fully personalized sound:

   1. Off (no boost)
   2. Under 30 years old (boost high frequencies)
   3. 30 to 60 years old (boost high/mid frequencies)
   4. Over 60 years old (boost all frequencies)

ix. Mute all sounds: Turn off all sounds on your phone, including calls, alerts and media.

x. Mono audio: Play the same sound out of both speakers.

xi. Left/right sound balance.

3. **Interaction and dexterity**: If a user has mobility or coordination concerns, such user can improve his phone screen's functionality with interaction and dexterity controls, so that the user can enjoy all the apps on the device, text friends, and make calls. Connect devices for easy navigation if the user prefer using a mouse or keyboard and adjust the user screen's sensitivity to taps and touches. That way, the user will never select something accidentally

    i. Universal switch: Use external accessories to control the phone and select items on the screen.

    ii. Assistant menu: Show a menu of easy-to-reach buttons that let you replace hardkeys, gestures, and other common interactions.

    iii. Answering and ending calls:

        1. Read caller names aloud: User can use set over Bluetooth and headphones only or always as the option.
        2. Answer automatically: Automatically answer incoming calls after a set time (2, 5, 10 seconds or custom time) while a headset or a Bluetooth device is connected.
        3. Press volume up to answer calls.
        4. Press power key to end.

    iv. Interaction control: Keeps the focus on a single app by blocking the back, home, and recent buttons, as well as incoming calls and notifications. The user can also choose whether to block the side key, volume keys, and keyboard, or block touches from an area of the screen.

    v. Touch and hold delay: Set how long it takes for a continuous touch to be recognized as a touch and hold. This doesn't affect the keyboard. As an example, some of the values can be:

        1. Very short (0.3 seconds)
        2. Short (0.5 seconds)
        3. Medium (1 second)
        4. Long (1.5 seconds)
        5. Custom

    vi. Tap duration: Set how long an interaction needs to be held to be recognized as a tap.

vii. Ignore repeated touches: Set a time within which to ignore repeated touches. Only the user first tap will be recognized. Multiple touches will be ignored for time you set.

viii. Auto action after pointer stops: Choose an action to happen automatically after the mouse pointer stops moving.

    1. Auto action: none, click, click and hold, double-click.
    2. Corner actions: Choose actions to happen when you move the muse pointer to each corner. TOP LEFT, TOP RIGHT, BOTTOM LEFT, BOTTOM RIGHT.
    3. Delay time before action.

ix. Sticky keys: When you press a modifier key like SHIFT, CTLR or ALT, it will stay pressed so you can enter keyboard shortcuts one key at a time.

x. Show keys: Type by touching and holding for a set time to avoid accidental key presses.

xi. Bounce keys: Prevent accidental key presses by setting a delay before a second tap on the same key is accepted.

4. **Advanced settings:** Set the keys for accessing different accessibility features:

i. Accessibility button: Choose what to use (all accessibility options like Talkback, magnification, color inversion etc) with the accessibility button in combination with Location (Navigation bar, floating over other apps).

ii. Power and volume up keys.

iii. Volume up and down keys.

iv. Flash notification: Flash the camera light or the screen when you receive notifications or when alarms sound.

    1. Camera flash notification
    2. Screen flash notification

v. Time to take action: Choose how long to show messages that ask you to take action, but are visible only temporarily, such as temporary on-screen notifications or the volume controller. Values can be 10seconds, 30 seconds, 1 minute, 2 minutes.

vi. Speak keyboard input aloud:

1. What to read: Characters, Words, Characters and words.
2. Read deleted characters aloud.
3. Phonetic alphabet: When reading letters aloud, use the corresponding word from the phonetic alphabet instead of the letter name.

vii. Bixby vision for accessibility: Offers various features to make it easier to learn the world around you.

1. Screen describer: Capture a scene to hear a detailed description of it.
2. Object identifier: Point the camera at something to hear what it is.
3. Text reader: Point the camera at some text to hear it read out aloud.
4. Color detector: Point camera at an object to hear what color it is.

viii. Voice Label: Write voice recordings to NFC tags to provide the user with information when you are nearby. The tags are purchased separately and can be associated with objects or locations you use regularly.

ix. Notification remainders:

1. Vibrate when sound plays.
2. Remind every 3, 5, 10, 15 minutes.
3. Select apps to get remainders for messages and phone.

5. **Link to Windows:** This service is for those using the screen reading tool on the PC. When the service is enabled, it lets you control all your phone’s apps from the user PC using Android/iOS keyboard navigation while receiving spoken feedback from your PC speakers.

6. **Talk back**: It provides spoken feedback so that user can use the device without looking at the screen. Taklback is intended for situations or people who have difficulty seeing the screen.

   When Talkback is enabled, we can track the following gesture movements:

   - Swipe right or left while moving between items.
   - Double tap gesture while activating item.

- Drag 2 finger gesture while scrolling.
- Volume level settings.

[0025] In an embodiment, each user (specially abled) sets and uses the accessibility uniquely. Accessibility behavioural analysis relies on a user's unique behaviour patterns and accessibility settings to build a profile of behaviour of the user that is normal. A user who acts vastly different from the behaviour profile is considered to be a suspicious/malicious/fraudulent user. Usage pattern of Apps reveals the user' unique behaviour. For example, specially abled user may normally use talkback settings, some visibility enhancements settings like contrast, for keyboard, buttons, color filter, animations etc. A specially abled user can also have unique hearing enhancements settings like hearing aide, adaptable sound (based on age, left/ right ear hearing) etc.

[0026] In an embodiment, the system collects several parameters such as the ones listed above as data and forms a template of the user's accessibility settings and usage behaviour and trains the AI system. A behavioural pattern is determined and a threshold is set to identify when behaviour translates from normal to fraudulent. This threshold can be a trust score (for e.g., 90). When a user is encountered, a trust score is calculated. If the trust score is lesser than the threshold then it can be considered that the user encountered is a fraudulent user. When the trust score is above the threshold value, the user can be considered to be the normal returning user and can be granted access to the application.

[0027] In an embodiment, when the user encountered is considered to be a fraudulent user then the user is either blocked from accessing the App or MFA can be prompted.

[0028] In an embodiment, the threshold can be adjusted. Having too high of a threshold would mean potentially blocking out authentic users, while having too low of a threshold result in fraudsters going undetected.

[0029] Fig. 1 discloses a discloses a flowchart diagram for collecting accessibility settings and training the machine learning model.

[0030] In FIG. 1, a method 100 for collecting accessibility settings and training the machine learning model is disclosed.

[0031] At step 101, the method may include a user opening an app on a device for example a mobile application (App).

[0032] At step 102, the method may include collecting accessibility settings data such as talkback, visual enhancements, interaction and dexterity settings, etc. as detailed above, along with common user behavioral data, to accurately associate accessibility settings with the user.

[0033] At step 103, the method may include, analysing and cleaning the accessibility settings data collected.

[0034] In an embodiment, data cleaning is the process of either removing or using imputer function for null values or unrelated values to create a perfect dataset.

[0035] In an embodiment, analyzing the data entails selecting the best data (for e.g. data suitable for linear regression, logistics regression, clustering etc) for a machine leaning (ML) model. Relation between features for the chosen data set is found out.

[0036] At step 104, the method may include, splitting the data for training and testing. Almost 80% of data is used for training and 20% is used for testing.

[0037] At step 105, the method may include, data training of the ML model. At this step training data is also validated to avoid overfitting or under-fitting.

[0038] At step 106, the method may include, testing the ML model using cross-validation. In an embodiment, confusion matrix is used for checking the ML model’s performance

[0039] At step 107, the method may include, deploying the ML model to identify fraudulent users.

[0040] Fig. 2 discloses a flowchart diagram of authentication flow.

[0041] In FIG. 2, a method 200 of the authentication flow based on a user’s accessibility settings is disclosed.

[0042] At step 201, the method may include, the user opening a mobile application (App).

[0043] At step 202, the method may include, the user trying to login to the app using standard login mechanism.

[0044] At step 203, if the user has to pass additional authentication using Multi-Factor or Two-Factor Authentication (MFA or 2FA), a trust score in the form of user profile data which is created and trained using accessibility settings in fig. 1 is fetched. If the user does not have to pass additional authentication normal flow of events would continue.

[0045] At step 204, based on the trust score received in step 203 it is decided whether or not MFA/2FA can be skipped. For example, if a trust score value of 90 is set as a threshold, then a trust value score greater than 90 is considered as GOOD and MFA/2FA can be skipped as the user is not a fraudster. If trust score value is less than 90, it would mean that the user encountered could be a fraudster and a further mode of authentication can be suggested. This way for a genuine returning user of the app, additional overhead of MFA/2FA can be avoided and the usability of the app can also be improved, at the same time fraudulent activity can also be reduced.

[0046] At steps 204a and 205a, feedback is provided to the system to improve or train the model for better accuracy.

[0047] FIG. 3 is a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0048] In some embodiments, FIG. 3 illustrates a block diagram of an exemplary computer system 300 for implementing embodiments consistent with the present disclosure. The processor 302 may include at least one data processor for executing program components for executing user or system-generated business processes. A user may include a person, a person using a device such as those included in this disclosure, or such a device itself. The processor 302 may include specialized processing units such as integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[0049] The processor 302 may be disposed in communication with input devices 311 and output devices 312 via I/O interface 301. The input devices 311 may be devices such as, without limitation to, keyboard, mouse, touch screen, sensors, microphones, scanners, camera, finger print scanner etc. The output devices 312 may be devices such as, without limitation to, speaker, electronic screen, etc. The I/O interface 301 may employ communication protocols/methods such as, without limitation, audio, analog, digital, stereo, IEEE-1393, serial bus, Universal Serial Bus (USB), infrared, PS/2, BNC, coaxial, component, composite, Digital Visual Interface (DVI), high-definition multimedia interface (HDMI), Radio Frequency (RF) antennas, S-Video, Video Graphics Array (VGA), IEEE 802.n /b/g/n/x, Bluetooth, cellular (e.g., Code-Division Multiple Access (CDMA), High-Speed Packet Access (HSPA+), Global System For Mobile Communications (GSM), Long-Term Evolution (LTE), WiMax, or the like), etc.

[0050] Using the I/O interface 301, the computer system 300 may communicate with the input devices 311 and the output devices 312.

[0051] In some embodiments, the processor 302 may be disposed in communication with a communication network 309 via a network interface 303. The network interface 303 may communicate with the communication network 309. The network interface 303 may employ connection protocols including, without limitation, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), Transmission Control Protocol/Internet Protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. The communication network 309 can be implemented as one of the different types of networks, such as intranet or Local Area Network (LAN), Closed Area Network (CAN) and such. The communication network 309 may either be a dedicated network or a shared network, which represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), CAN Protocol, Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), etc., to communicate with each other. Further, the communication network 309 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc. In some embodiments, the processor 302 may be disposed in communication with a memory 305 (e.g., RAM, ROM, etc. not shown in FIG.3) via a storage interface 303. The storage interface 303 may connect to memory 305 including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as Serial Advanced Technology Attachment (SATA), Integrated Drive Electronics (IDE), IEEE-1393, Universal Serial Bus (USB), fibre channel, Small Computer Systems Interface (SCSI), etc. The memory drives may further include a drum, magnetic disc drive, magneto-optical drive, optical drive, Redundant Array of Independent Discs (RAID), solid-state memory devices, solid-state drives, etc.

[0052] The memory 305 may store a collection of program or database components, including, without limitation, a user interface 306, an operating system 307, a web browser 308 etc. In some embodiments, the computer system 300 may store user/application data, such as the data, variables, records, etc. as described in this disclosure. Such databases may be implemented as fault-tolerant, relational, scalable, secure databases such as Oracle or Sybase.

[0053] The operating system 307 may facilitate resource management and operation of the computer system 200. Examples of operating systems include, without limitation, APPLE® MACINTOSH® OS X®, UNIX®, UNIX-like system distributions (E.G., BERKELEY SOFTWARE DISTRIBUTION® (BSD), FREEBSD®, NETBSD®, OPENBSD, etc.), LINUX® DISTRIBUTIONS (E.G., RED HAT®, UBUNTU®, KUBUNTU®, etc.), IBM®OS/2®, MICROSOFT® WINDOWS® (XP®, VISTA®/7/8, 10 etc.), APPLE® IOS®, GOOGLE™ ANDROID™, BLACKBERRY® OS, or the like. The User interface 206 may facilitate display, execution, interaction, manipulation, or operation of program components through textual or graphical facilities. For example, user interfaces may provide computer interaction interface elements on a display system operatively connected to the computer system 300, such as cursors, icons, checkboxes, menus, scrollers, windows, widgets, etc. Graphical User Interfaces (GUIs) may be employed, including, without limitation, Apple® Macintosh® operating systems' Aqua®, IBM® OS/2®, Microsoft® Windows® (e.g., Aero, Metro, etc.), web interface libraries (e.g., ActiveX®, Java®, Javascript®, AJAX, HTML, Adobe® Flash®, etc.), or the like.

[0054] In some embodiments, the computer system 300 may implement the web browser 308 stored program components. The web browser 308 may be a hypertext viewing application, such as MICROSOFT® INTERNET EXPLORER®, GOOGLE™ CHROME™, MOZILLA® FIREFOX®, APPLE® SAFARI®, etc. Secure web browsing may be provided using Secure Hypertext Transport Protocol (HTTPS), Secure Sockets Layer (SSL), Transport Layer Security

(TLS), etc. Web browsers 308 may utilize facilities such as AJAX, DHTML, ADOBE® FLASH®, JAVASCRIPT®, JAVA®, Application Programming Interfaces (APIs), etc. In some embodiments, the computer system 300 may implement a mail server stored program component. The mail server may be an Internet mail server such as Microsoft Exchange, or the like. The mail server may utilize facilities such as Active Server Pages (ASP), ACTIVEX®, ANSI® C++/C#, MICROSOFT®, .NET, CGI SCRIPTS, JAVA®, JAVASCRIPT®, PERL®, PHP, PYTHON®, WEBOBJECTS®, etc. The mail server may utilize communication protocols such as Internet Message Access Protocol (IMAP), Messaging Application Programming Interface (MAPI), MICROSOFT® exchange, Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), or the like. In some embodiments, the computer system 300 may implement a mail client stored program component. The mail client may be a mail viewing application, such as APPLE® MAIL, MICROSOFT® ENTOURAGE®, MICROSOFT® OUTLOOK®, MOZILLA® THUNDERBIRD®, etc.

[0055] 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., non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc (CD) ROMs, Digital Video Disc (DVDs), flash drives, disks, and any other known physical storage media.

[0056] 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.

[0057] 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.

[0058] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0059] The above disclosed methods and system have several advantageous effects including, but not limited to:

1. catering to the needs of all kinds of users including specially abled users.

2.behavioral analysis is a high security, low friction method of fraud prevention. Businesses can integrate it with traditional security measures like passwords to build a system resistant to old and new fraud methods.

3.improving usability of the mobile apps for returning users by removing additional MFA overhead.

[0060] The above description is illustrative and is not restrictive. Many variations of the invention may become apparent to those skilled in the art upon review of the disclosure. The scope of the invention can, therefore, be determined not with reference to the above description, but instead can be determined with reference to the pending claims along with their full scope or equivalents.

[0061] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0062] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0063] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

[0064] Although the invention has been described in detail for the purpose of illustration based on what is currently considered to be the most practical and preferred embodiments, it is to be understood that such detail is solely for that purpose and that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the spirit and scope of the appended claims. For example, it is to be understood that the present invention contemplates that, to the extent possible, one or more features of any embodiment can be combined with one or more features of any other embodiment.

CONTINUOUS AUTHENTICATION USING ACCESSIBILITY SETTINGS AND USAGE ANALYSIS

ABSTRACT

The present invention discloses a method and system for continuous authentication using accessibility settings and usage analysis which can be used during mobile application login. An Artificial Intelligence (AI) based system, continuously captures and analyses a specially abled user's behaviour and accessibility settings. The AI would then come up with a risk based score. This risk score will then be used to decide whether or not to skip Multi Factor Authentication (MFA).

FIG. 1

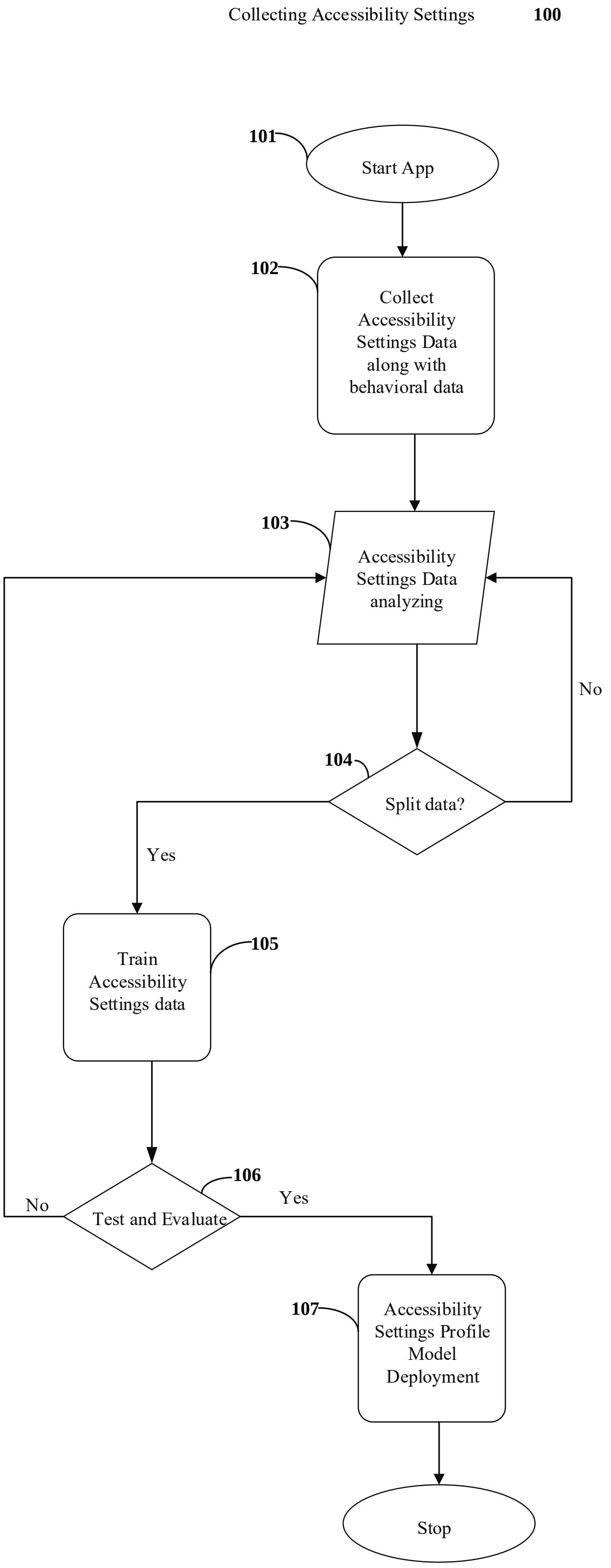
Collecting Accessibility Settings
100
101
Start App
102
Collect Accessibility Settings Data along with behavioral data
103
Accessibility Settings Data analyzing
No
104
Split data?
Yes
Train Accessibility Settings data
105
106
No
Test and Evaluate
Yes
107
Accessibility Settings Profile Model Deployment
Stop

Fig. 1

2/3

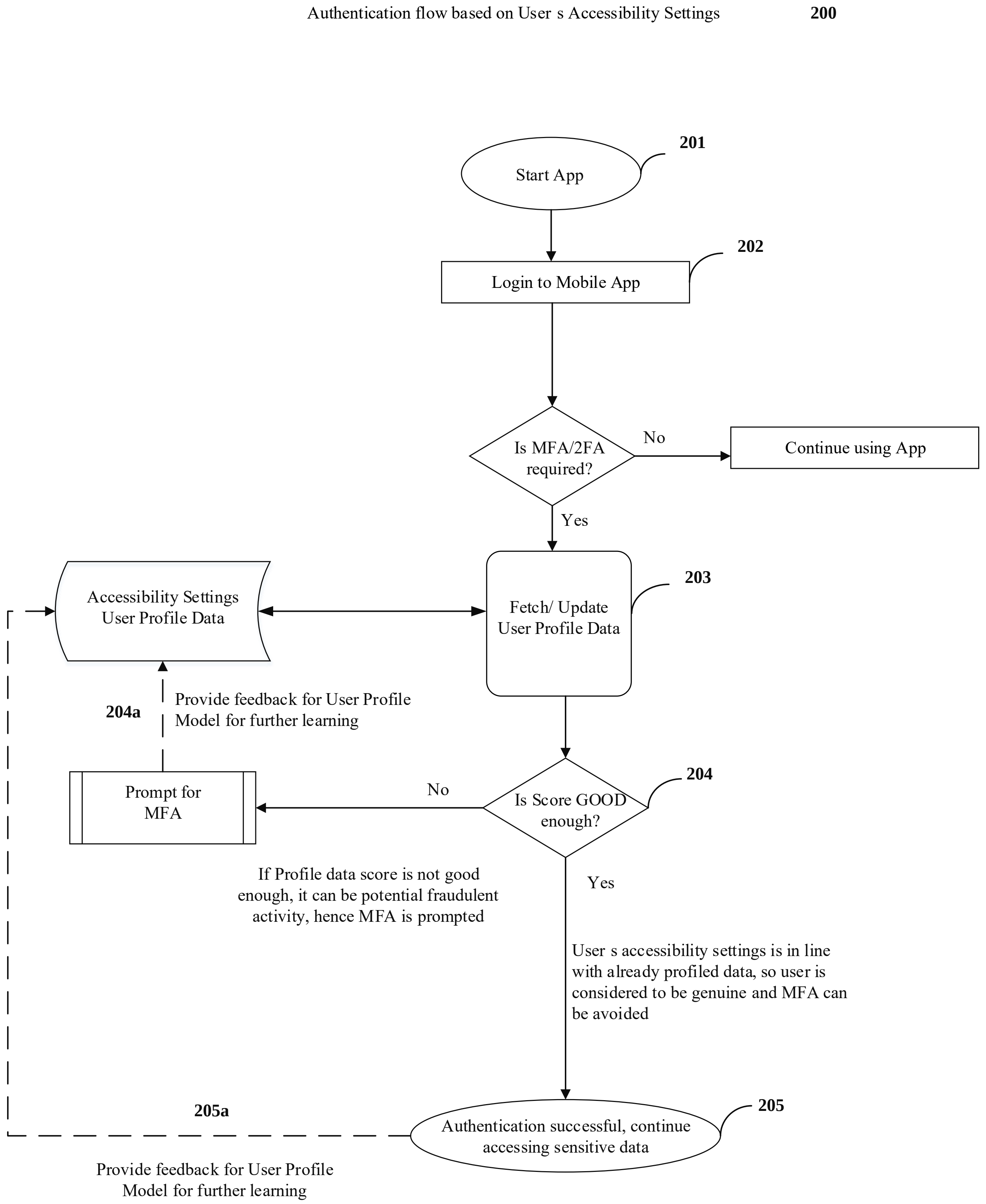
Authentication flow based on User s Accessibility Settings
200
201
Start App
202
Login to Mobile App
Is MFA/2FA required?
No
Continue using App
Yes
Accessibility Settings User Profile Data
203
Fetch/ Update User Profile Data
204a
Provide feedback for User Profile Model for further learning
Prompt for MFA
No
204
Is Score GOOD enough?
If Profile data score is not good enough, it can be potential fraudulent activity, hence MFA is prompted
Yes
User s accessibility settings is in line with already profiled data, so user is considered to be genuine and MFA can be avoided
205a
205
Authentication successful, continue accessing sensitive data
Provide feedback for User Profile Model for further learning

Fig. 2

3/3

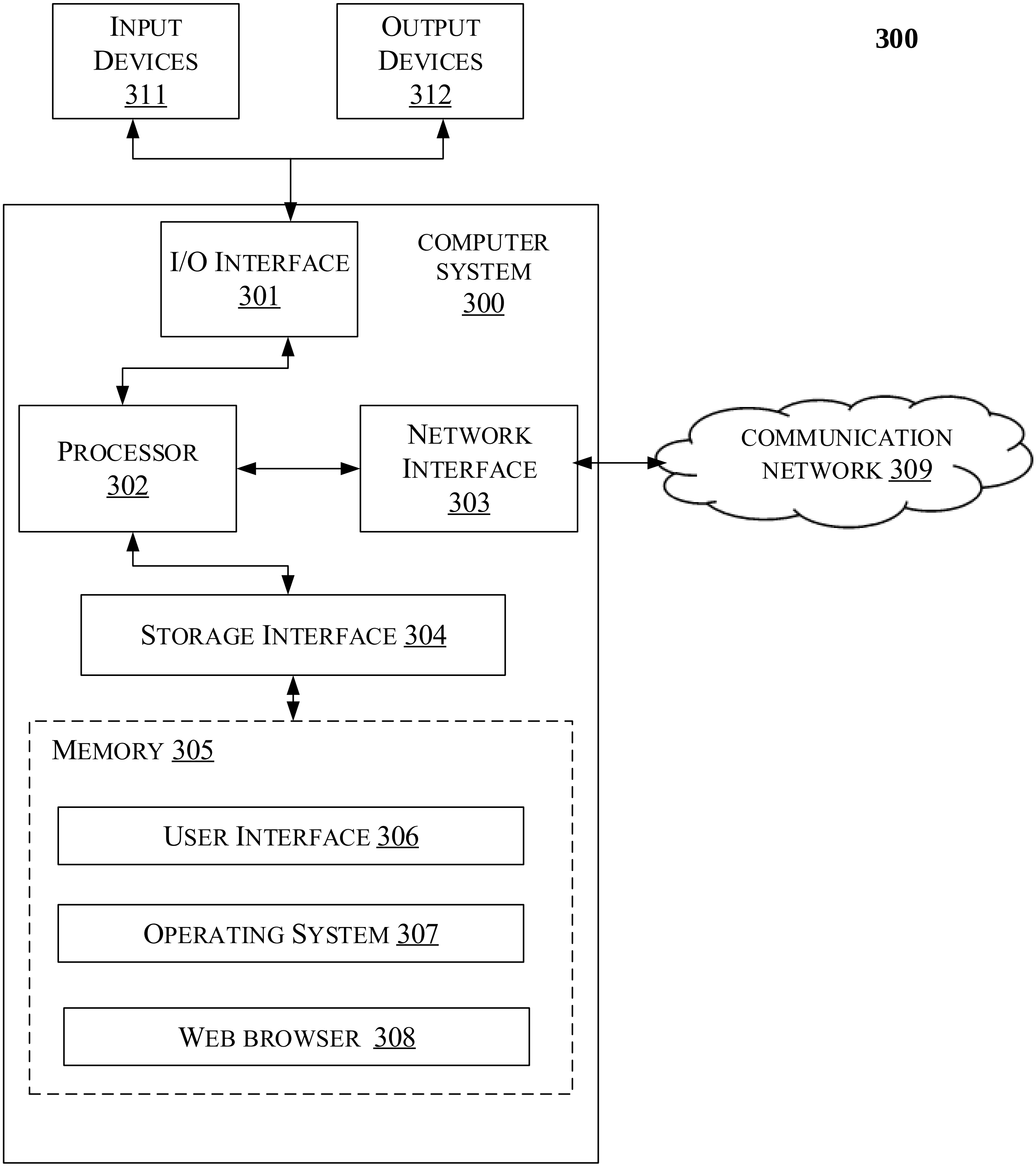
300
INPUT DEVICES 311
OUTPUT DEVICES 312
I/O INTERFACE 301
COMPUTER SYSTEM 300
PROCESSOR 302
NETWORK INTERFACE 303
COMMUNICATION NETWORK 309
STORAGE INTERFACE 304
MEMORY 305
USER INTERFACE 306
OPERATING SYSTEM 307
WEB BROWSER 308

Fig. 3