March 2023

SYSTEM AND METHOD FOR SENSITIVE DATA PROTECTION FOR ACCESSIBILITY USERS

SHREEHARSHA RANGARAJAN
Visa

SHASHANKA ARNADY
Visa

NITHIN SHAKTHIDHAR BG
Visa

SYSTEM AND METHOD FOR SENSITIVE DATA PROTECTION FOR ACCESSIBILITY USERS

VISA

INVENTORS:

- **SHREEHARSHA RANGARAJAN**
- **SHASHANKA ARNADY**
- **NITHIN SHAKTHIDHAR BG**

TECHNICAL FIELD

[0001] The present subject matter is, in general, relates to obfuscation and data protection techniques, and particularly, system and method for sensitive data protection for accessibility users.

BACKGROUND

[0002] Recently, due to increase in use of electronic transactions via electronic devices for online shopping, payments, and the like, there are many ways introduced for securing and authenticating such electronic transactions. One of the ways of securing and authenticating such electronic transactions is using sensitive data such as One Time Password (OTP). However, such passwords should be private and not shared with any third party who is not related to the electronic transaction. Further, user details such as Permanent Account Number (PAN), bank details, card numbers and the like may be required for completing some electronic transactions, which also need to be maintained private and not shared with any third party who is not related to the transaction. However, when the accessibility users are performing such electronic transactions, conventional techniques provide a screen reader that reads out the sensitive data such as OTP, card number etc., from the electronics device for the accessibility users to complete the e-transactions. However, in such scenarios, reading of the sensitive data may lead to privacy breach, as people in the vicinity of the accessibility users would be able to hear the sensitive data when the screen reader reads out the sensitive data. Due to this reason, the accessibility users may refrain from performing electronic transactions or may delay the transaction until they are in a safe location where there is no possibility of potential fraud by eavesdropping on the sensitive information.

[0003] Therefore, there is a need to provide an improvised system and method for sensitive data protection for accessibility users.

[0004] The information disclosed in the background section of the disclosure is only for enhancement of understanding of the general background of the invention and should not be taken as an acknowledgement or any form of suggestion that this information forms the prior art already known to a person skilled in the art.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same numbers are used throughout the figures to reference like features and components. Some embodiments of device or system and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[0006] FIG. 1 shows a block diagram of an exemplary environment for sensitive data protection for accessibility users, in accordance with some embodiments of the present disclosure;

[0007] FIG. 2 shows a flowchart illustrating a method for sensitive data protection for accessibility users using a data protection system, in accordance with some embodiments of the present disclosure; and

[0008] FIG. 3 illustrates a block diagram of an exemplary computer system for implementing some embodiments of the present disclosure.

[0009] The figures depict embodiments of the disclosure for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the disclosure described herein.

DESCRIPTION OF THE DISCLOSURE

[0010] 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.

[0011] 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.

[0012] 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.

[0013] 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.

[0014] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise. The terms “user” and “customer” have been used interchangeably throughout the disclosure. In the present disclosure, the term “offers” “promotions” and “promotional offers” have been used interchangeably throughout the disclosure. The offers/promotions may include discounts, incentives, rewards, rebates, gifts, cashbacks, coupons, reward points, or any such benefit which can be availed/redeemed upon satisfaction of certain conditions.

[0015] The present disclosure provides a system and a method for sensitive data protection for accessibility users. The method includes receiving a message via one or more user devices from user, and identifying if the message includes the sensitive data by using a predefined technique. In case, the message includes sensitive data, the method comprises detecting if an audio device is plugged in or not plugged in to the one or more user devices. If the audio device is not plugged in to the one or more user devices, the method includes performing obfuscation of the sensitive data and reads out the obfuscated sensitive data on the one or more user devices. However, if the audio device is plugged in to the user device, the method includes reading out the sensitive data without obfuscation. Thus, the present disclosure provides a way to obfuscate

the sensitive data intended for a visually impaired user such that, only the visually impaired user may decipher the obfuscated sensitive data.

[0016] FIG. 1 shows a block diagram (100) of an exemplary environment for sensitive data protection for accessibility users, in accordance with some embodiments of the present disclosure.

[0017] In some embodiments, the environment comprises a user device (102-1) to a user device (102-N) (also referred as one or more user devices 102), a data protection system (104), and an audio device (106) and an external data source (114-1) to an external data source (114-N) (also referred as one or more one or more external data sources 114). The one or more user devices (102) may include, but not limited to, a smartphone, a computer, a laptop, and a tablet and the like. For the ease of understanding, the present disclosure is explained from the perspective of a single user device of the accessibility user. However, it should not be construed as a limitation since the same invention is applicable for any number of user devices used by the accessibility users. In some embodiments, the accessibility users are users who may have the disability such as blindness because of which they may not be able to see or read any data on their own. To perform sensitive data protection for the accessibility user, the accessibility user may initially register with the data protection system (104). As part of registration, the accessibility user may provide registration details and user details as required by the data protection system (104) via the user device (102-1). As an example, the registration details and user details may include, but not limited to, name, email ID, obfuscation key set by the accessibility user, banks details associated to the accessibility users and the like. In some embodiments, the data protection system (104) may be associated with the user device (102-1) through a wireless or wired communication network. In some other embodiments, the data protection system (104) may be configured/installed in the user device (102-1).

[0018] The data protection system (104) includes a processor (108), an I/O interface (110) and a memory (112). The memory (112) is communicatively coupled to the processor (108). The I/O interface (110) may receive a message from the user device (102-1). In some embodiments, the user device (102-1) may receive the message from the one or more external data sources (114). The one or more external data sources (114) may include, but not limited to, bank associated websites, career websites, e-commerce websites and the like that provide One Time Passwords (OTPs), secret codes and the like for completing a transaction. Upon receiving the

message, the processor (108) may identify if the message includes sensitive data by using a predefined technique. In some embodiments, the predefined technique may include, utilizing custom attributes for the sensitive data using Hyper Text Markup Language 5 (HTML5) such that upon receiving the sensitive data because of utilizing the custom attributes, the processor (108) identifies the sensitive data. In some other embodiments, the predefined techniques may include, but not limited to, AI based techniques such as Natural Language Processing (NLP). The NLP may identify keywords associated with sensitive data from the message such as OTP, Permanent Account Number (PAN), telephone number, bank details and the like. The sensitive data is a type of data where if this type of data is revealed, it may lead to privacy breach of the accessibility user. In some cases, if a third party is present in the vicinity of the accessibility user when the sensitive data is being read out, then there is a potential possibility that the third party can hack the bank account or the transaction of the accessibility user leading to fraud. In some other embodiments, there may be data theft and threat to valuable entities involved in transactions such as money if the third party finds out about the sensitive data associated with the accessibility user. Upon identifying the presence of sensitive data in the message, the processor (108) detects if the audio device (106) is plugged in or not plugged in to the user device (102-1). The audio device (106) may include, but not limited to, earphones, headphones and the like. If the audio device (106) is not plugged in to the user device (102-1), the processor (108) performs obfuscation of the sensitive data and reads out the obfuscated sensitive data for the accessibility user for further action. Detailed explanation is illustrated in **FIG.2**. In some other embodiments, if the audio device (106) is plugged in to the user device (102-1), the processor (108) reads out the sensitive data without performing obfuscation of the sensitive data.

[0019] FIG. 2 shows a flowchart illustrating a method (200) for sensitive data protection for accessibility users using a data protection system (104), in accordance with some embodiments of the present disclosure.

[0020] The method (200) may be described in the general context of computer executable instructions. Generally, computer executable instructions can include routines, programs, objects, components, data structures, procedures, modules, and functions, which perform functions or implement abstract data types.

[0021] The order in which the method (200) is described is not intended to be construed as a limitation, and any number of the described method blocks can be combined in any order to implement the method (200). Additionally, individual blocks may be deleted from the methods without departing from the spirit and scope of the subject matter described herein. Furthermore, the method (200) can be implemented in any suitable hardware, software, firmware, or combination thereof.

[0022] Prior to performing sensitive data protection for the accessibility user, at block 202, the method (200) includes receiving, by a processor (108) of the data protection system (104), registration details and user associated details from a user device (102-1) for registering for sensitive data protection as disclosed in the present disclosure. The registration details and user information may include, but not limited to, bank related information such as account number, Permanent Account Number (PAN) and the like, name, age and the like. Further, at block 202, the method (200) includes receiving, by the processor (108), a preset obfuscation key for performing the sensitive data protection via the user device (102-1) from the accessibility user. In some embodiments, for setting the preset obfuscation key, the accessibility user may hover over a character and set the preset obfuscation key using the vibration based touch screen. In some embodiments, the processor (108) may callout a voice output which includes a character and the accessibility user may double click for confirmation of the character using the vibration based touch screen. In some other embodiments, in a secure environment, the accessibility user may callout a character based on a voice guided menu via a microphone present in an audio device (106) of the user device (102-1) for setting the preset obfuscation key. Upon receiving voice prompt for setting the preset obfuscation key, in some embodiments, a screen with Braille keyboard is presented for the accessibility user, using which the accessibility user sets the preset obfuscation key at the time of registration.

[0023] At block 204, the method (200) includes receiving, by the processor (108) a message comprising an information. In some embodiments, the information may include sensitive data associated with the accessibility user. The user device (102-1) may receive the message from one or more external data sources (114). The external data sources (114) may include, but not limited to, bank associated websites, career websites, and the like. The sensitive data may include, but not limited to, One Time Password (OTP), PAN, telephone number, bank details and the like.

[0024] At block 206, the method (200) includes identifying, by the processor (108), if the message comprising the information includes the sensitive data using a predefined technique. In some embodiments, the predefined technique may include, utilizing custom attributes for the sensitive data using Hyper Text Markup Language 5 (HTML5) such that upon receiving the sensitive data because of utilizing the custom attributes, the processor (108) identifies the sensitive data. In some other embodiments, the predefined technique may include but not limited to, AI based techniques such as Natural Language Processing (NLP). The NLP may identify keywords associated with sensitive data from the message such as OTP, PAN, telephone number, bank details and the like.

[0025] Upon identifying the presence of sensitive data, at block 208, the method (200) includes detecting, by the processor (108), if the audio device (106) is plugged in to the user device (102-1). For instance, in order to detect if the audio device (106) is plugged in or not, the processor (108) may play a test sound to activate a mike associated with the user device (102-1) to hear the played sound for detection. If the test sound of the user device (102-1) is audible via the mike of the audio device (106) then the processor (108) detects that the audio device (106) is not plugged in to the user device (102-1). In some other embodiments, if the test sound is not audible via the mike of the audio device (106), then the processor (108) detects that the audio device (106) is plugged in to the user device (102-1).

[0026] If the audio device (106) is detected to be plugged in to the user device (102-1), the method (200) proceeds to block 210, via yes and if the audio device (106) is detected to be not plugged in to the user device (102-1), the method (200) proceeds to block 212, via no. At the block 210, the method (200) includes reading out the sensitive data without obfuscation on the user device (102-1) such that when the sensitive data is read out to the accessibility user, nobody can determine the sensitive data around the vicinity of the accessibility user since the sensitive data is heard by the accessibility user through the audio device (106) and not through the mike of the user device (102-1). Further, at the block 212 the method (200) includes performing, by the processor (108), obfuscation of the sensitive data. For instance, obfuscated sensitive data may be generated by obfuscating the sensitive data using a preset obfuscation key set by the accessibility user as illustrated in the block 202. Such obfuscation of the sensitive data may be performed using a carry over digit technique. For instance, if any digit in the sensitive data such as the OTP is less than the preset obfuscation key set by the accessibility user, then a predefined carry over digit is added to the digit to obtain a sum and then the preset

obfuscation key is subtracted from the sum. In some other instances, if any number of the sensitive data is greater than the preset obfuscation key, then the carry over digit is not added to the number. The preset obfuscated key is directly subtracted from the number. For example, if the OTP is 3456 and the preset obfuscation key set by the accessibility user is 4, then the generated obfuscated OTP is 9012. Since, the digit 3 is less than the preset obfuscation key, a predefined carry over of 10 is provided and the first digit in the OTP is given as **10+3-4=9**. Further, in the case of the digit 4, since the digit 4 is same as the preset obfuscation key, the predefined carry over of 10 is provided and the second digit in the OTP is given as **4-4=0.** Further, in the case of the digit 5, since the digit 5 is greater than the preset obfuscation key, the predefined carry over of 10 is not provided and directly subtracted from the preset obfuscation key and is given as **5-4=1**. Similarly, in the case of the digit 6, since the digit 6 is greater than the preset obfuscation key, the predefined carry over of 10 is not provided and directly subtracted from the preset obfuscation key and is given as **6-4=2**. Therefore, in this example, the final code for 3456 post obfuscation is 9012.

[0027] Upon obfuscating the sensitive data, at block 214 the method (200) includes reading out, by the processor (108), the generated obfuscated sensitive data on the user device (102-1). Therefore, even when the accessibility user listens to the sensitive data in the crowded region, people in the vicinity may not know the original sensitive data due to the obfuscation.

General computer system:

[0028] FIG. 3 illustrates a block diagram of an exemplary computer system (300) for implementing embodiments consistent with the present disclosure.

[0029] In an embodiment, the computer system (300) may be used to implement the system. In the present disclosure, the computer system (300) may be a data protection system (104). The computer system (300) may include a central processing unit (“CPU” or “processor”) (302). The processor(302) may receive a message via a network interface (303) and communication network (309) from one or more user devices (102) for performing obfuscation of sensitive data. 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.

[0030] The processor (302) may be disposed in communication with one or more Input/Output (I/O) devices (310 and 311) via I/O interface (301). The I/O interface (301) employ communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, Radio Corporation of America (RCA) connector, stereo, IEEE-1394 high speed serial bus, serial bus, Universal Serial Bus (USB), infrared, Personal System/2 (PS/2) port, Bbayonet Neill-Concelman (BNC) connector, coaxial, component, composite, Digital Visual Interface (DVI), High-Definition Multimedia Interface (HDMI), Radio Frequency (RF) antennas, S-Video, Video Graphics Array (VGA), IEEE 802.11b/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), Worldwide Interoperability for Microwave access (WiMax), or the like, etc.

[0031] Using the I/O interface (301), the computer system (300) may communicate with one or more I/O devices such as input devices (310) and output devices (311). For example, the input devices (310) may be an antenna, keyboard, mouse, joystick, (infrared) remote control, camera, card reader, fax machine, dongle, biometric reader, microphone, touch screen, touchpad, trackball, stylus, scanner, storage device, transceiver, video device/source, etc. The output devices (311) may be a printer, fax machine, video display (e.g., Cathode Ray Tube (CRT), Liquid Crystal Display (LCD), Light-Emitting Diode (LED), plasma, Plasma Display Panel (PDP), Organic Light-Emitting Diode display (OLED) or the like), audio speaker, etc.

[0032] In some embodiments, the processor (302) may be disposed in communication with the 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) may include, without limitation, a direct interconnection, Local Area Network (LAN), Wide Area Network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, etc. Using the network interface (303) and the communication network (309), the computer system (300) may communicate with inputs and provides output. The network interface (303) may employ connection protocols include, but not limited to, 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. In some embodiments, the computer system (300) may be

communicatively connected with the one or more user devices (102) and an audio device (106). As an example, the one or more user devices (102) may include, but not limited to, a smartphone, a computer, a laptop, and a tablet and the like. As an example, the audio device (106) may include, but not limited to, earphones, headphones and the like.

[0033] The communication network (309) includes, but is not limited to, a direct interconnection, a Peer-to-Peer (P2P) network, Local Area Network (LAN), Wide Area Network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, Wi-Fi 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), 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.

[0034] 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 (304). The storage interface (304) 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-1394, Universal Serial Bus (USB), fiber 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.

[0035] The memory (305) may store a collection of program or database components, including, without limitation, user interface (306), an operating system (307), etc. In some embodiments, 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.

[0036] The operating system (307) may facilitate resource management and operation of the computer system (300). Examples of operating systems include, without limitation, Apple™ Macintosh ™ OS X™, UNIX™, Unix-like system distributions (e.g., Berkeley Software

Distribution (BSD), FreeBSD™, Net BSD™, Open BSD™, etc.), Linux distributions (e.g., Red Hat™, Ubuntu™, K-Ubuntu™, etc.), International Business Machines (IBM™) OS/2™, Microsoft Windows™ (XP™, Vista/7/8, etc.), Apple iOS™, Google Android™, Blackberry™ operating system (OS), or the like.

[0037] In some embodiments, the computer system (300) may implement web browser (308) stored program components. 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, 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 ASP, ActiveX, ANSI C++/C#, Microsoft .NET, Common Gateway Interface (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.

[0038] 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.

[0039] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer-readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., be non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc (CD) ROMs, DVDs, flash drives, disks, and any other known physical storage media.

Advantages of the present disclosure

[0040] The present disclosure is configured to provide a secure environment with personalized obfuscation mechanism for protection of sensitive data for accessibility users by utilizing the method steps as described in the **FIG.2**. Therefore, even when the accessibility users are in public when it is crowded, the accessibility users can listen to sensitive data and use the same for transactions in banks, websites and the like.

[0041] The described operations may be implemented as a method, system or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof. The described operations may be implemented as code maintained in a "non-transitory computer readable medium", where a processor may read and execute the code from the computer readable medium. The processor is at least one of a microprocessor and a processor capable of processing and executing the queries. A non-transitory computer readable medium may include media such as magnetic storage medium (e.g., hard disk drives, floppy disks, tape, etc.), optical storage (CD-ROMs, DVDs, optical disks, etc.), volatile and non-volatile memory devices (e.g., EEPROMs, ROMs, PROMs, RAMs, DRAMs, SRAMs, Flash Memory, firmware, programmable logic, etc.), etc. Further, non-transitory computer-readable media may include all computer-readable media except for a transitory. The code implementing the described operations may further be implemented in hardware logic (e.g., an integrated circuit chip, Programmable Gate Array (PGA), Application Specific Integrated Circuit (ASIC), etc.).

[0042] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed

embodiments. It must also be noted that as used herein, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise.

[0043] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., are non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0044] 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.

[0045] 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.

“SYSTEM AND METHOD FOR SENSITIVE DATA PROTECTION FOR ACCESSIBILITY USERS”

ABSTRACT

Present disclosure discloses a method and a system for sensitive data protection for accessibility users. In some embodiments, the method includes receiving a message from user device (102-1) from the accessibility user, and identifying if the message includes sensitive data by using a predefined technique. Thereafter, the method discloses detecting if an audio device (106) is plugged in or not plugged in to the user device (102-1). If the audio device (106) is not plugged in to the user device (102-1) , the method includes performing obfuscation of the sensitive data and reads out the sensitive data with obfuscation. However, if the audio device (106) is plugged in to the user device (102-1), the method includes reading out the sensitive data without obfuscation. The present disclosure provides a secure environment with personalized obfuscation mechanism for protection of sensitive data for the accessibility users.

FIG.1

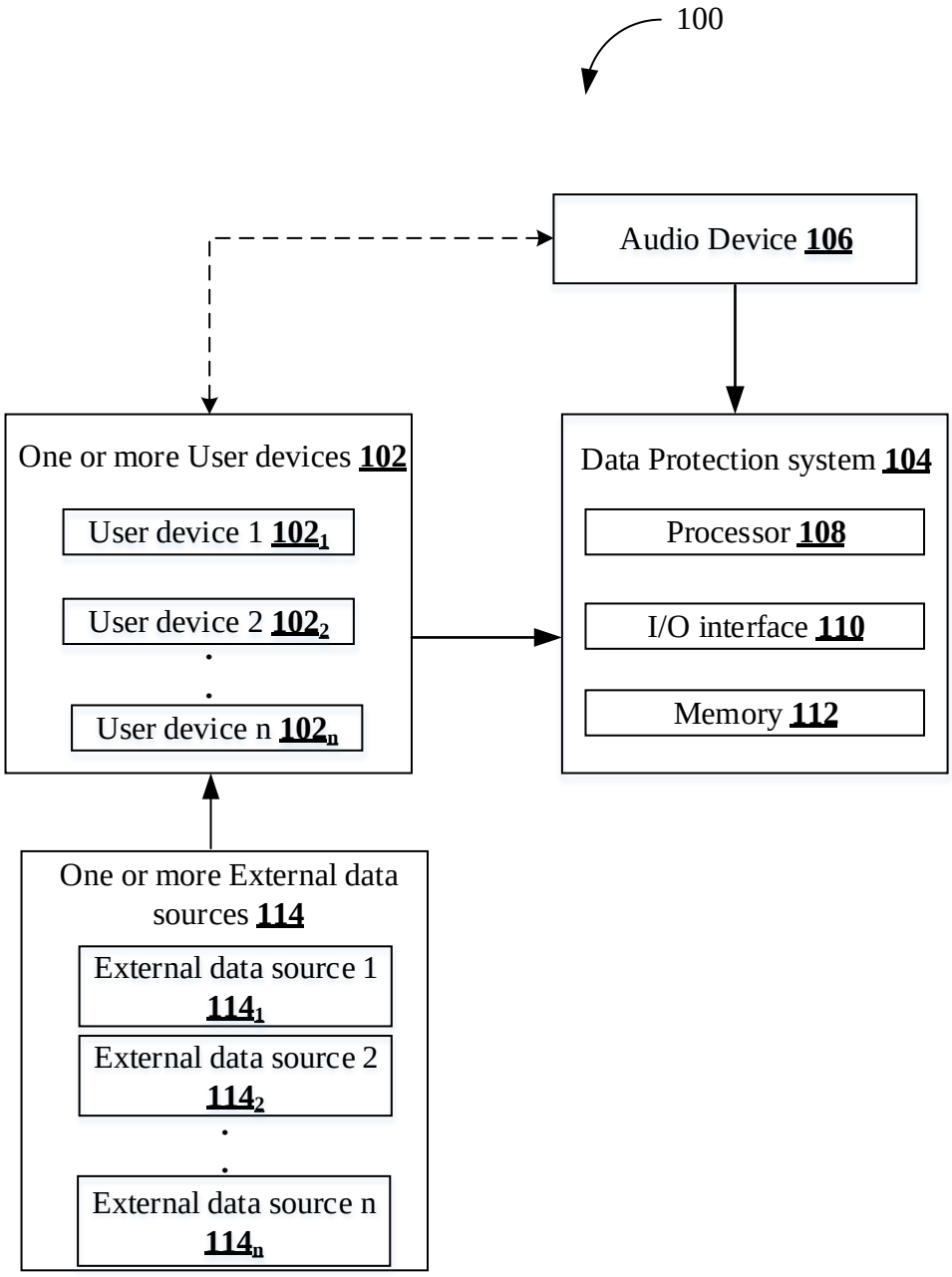
100
Audio Device 106
One or more User devices 102
User device 1 102₁
User device 2 102₂
User device n 102ₙ
Data Protection system 104
Processor 108
I/O interface 110
Memory 112
One or more External data sources 114
External data source 1 114₁
External data source 2 114₂
External data source n 114ₙ

Fig:1

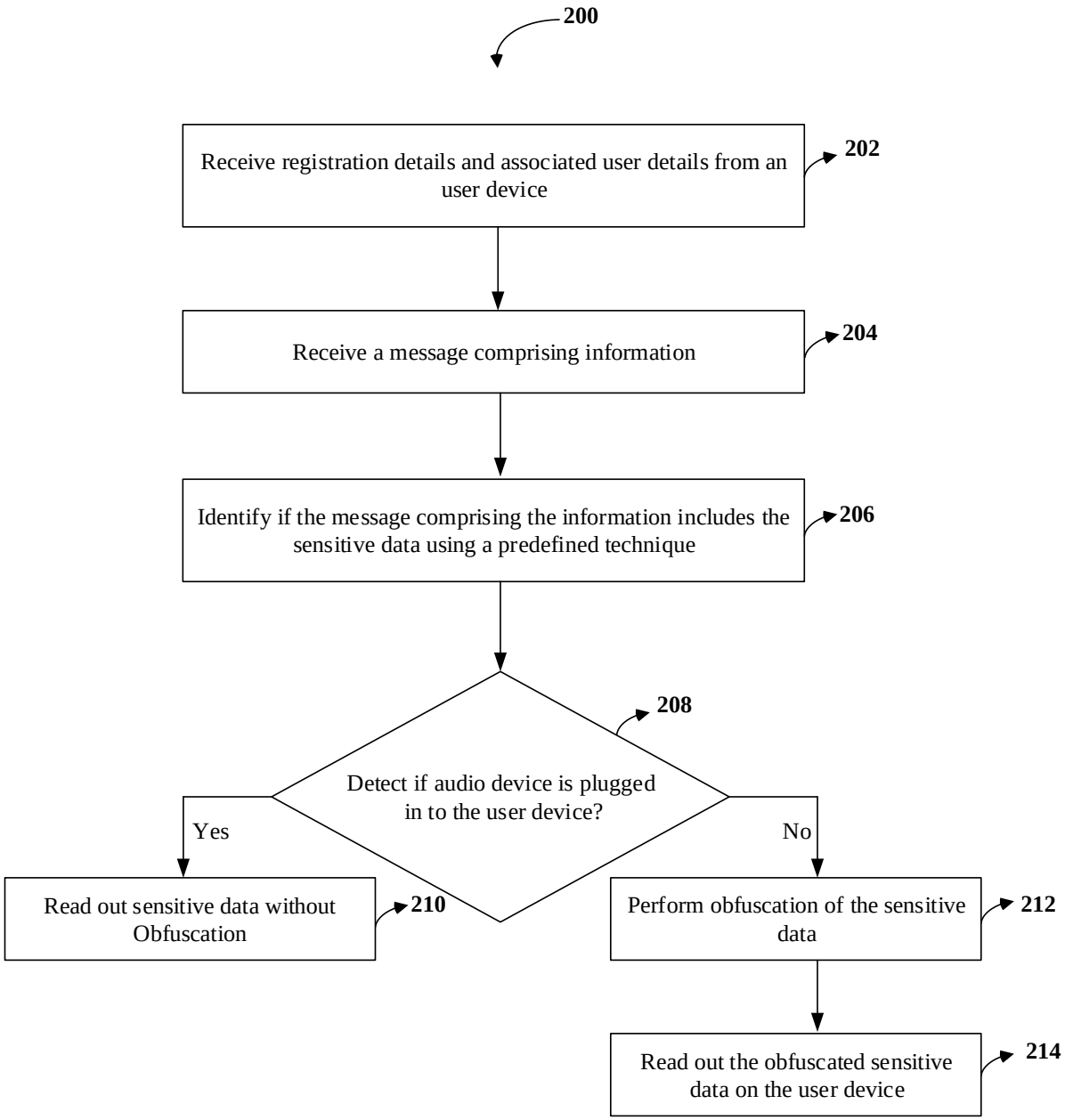
200
Receive registration details and associated user details from an user device
202
Receive a message comprising information
204
Identify if the message comprising the information includes the sensitive data using a predefined technique
206
Detect if audio device is plugged in to the user device?
208
Yes
No
Read out sensitive data without Obfuscation
210
Perform obfuscation of the sensitive data
212
Read out the obfuscated sensitive data on the user device
214

Fig:2

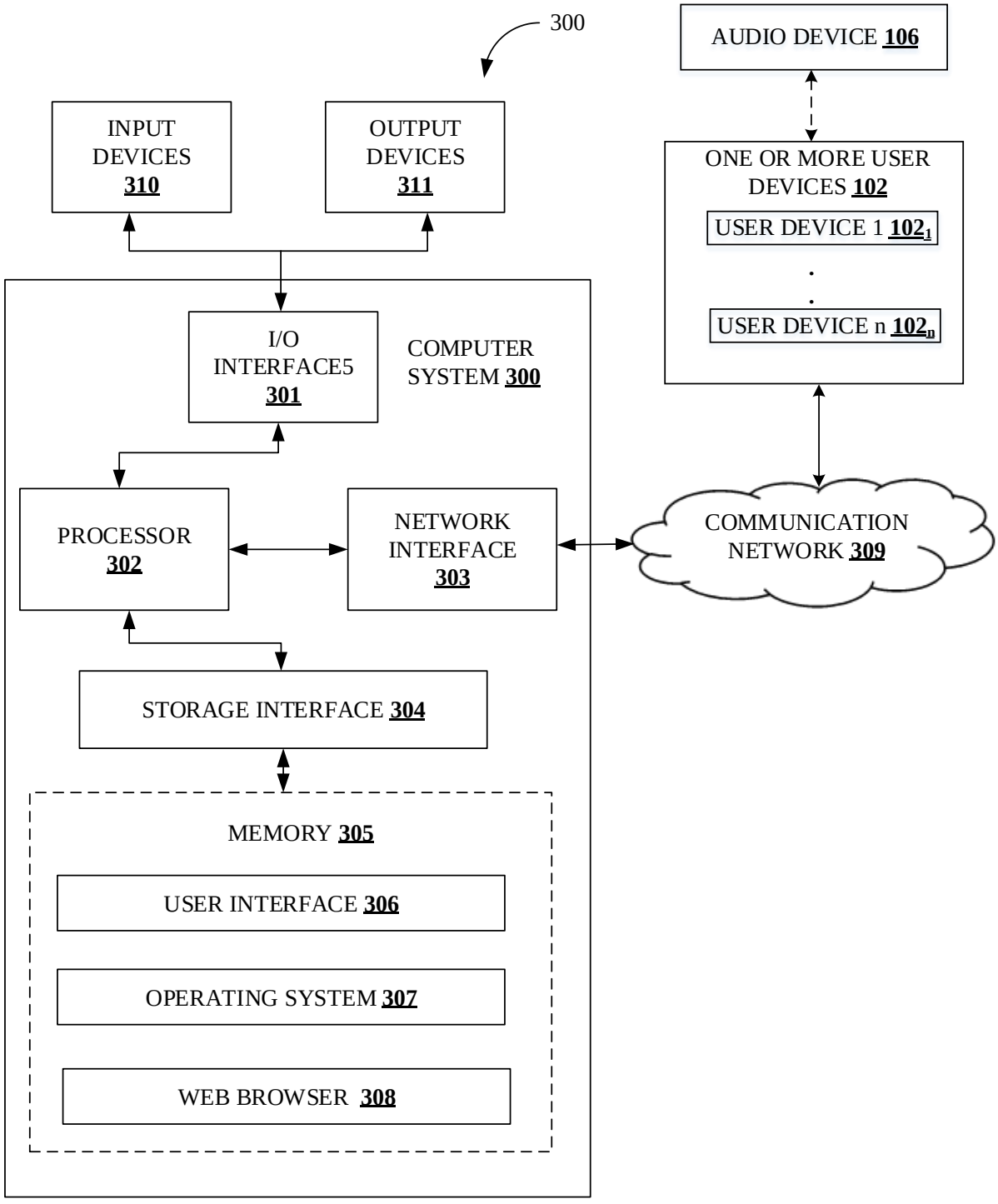
300
AUDIO DEVICE 106
INPUT DEVICES 310
OUTPUT DEVICES 311
ONE OR MORE USER DEVICES 102
USER DEVICE 1 102$_1$
USER DEVICE n 102$_n$
I/O INTERFACE5 301
COMPUTER SYSTEM 300
PROCESSOR 302
NETWORK INTERFACE 303
COMMUNICATION NETWORK 309
STORAGE INTERFACE 304
MEMORY 305
USER INTERFACE 306
OPERATING SYSTEM 307
WEB BROWSER 308

Fig:3