August 2023

BRAILLE OTP TOKEN

ASHISH DHYANI Visa

CHRISTANTIA WIRAWAN Visa

SASHANKH CHENGAVALLI KUMAR Visa

BRAILLE OTP TOKEN

VISA

INVENTORS:

ASHISH DHYANI

CHRISTANTIA WIRAWAN

SASHANKH CHENGAVALLI KUMAR

TECHNICAL FIELD

[0001] The present subject matter is, in general, related to communicating sensitive information, and in particular to, a system and method for securely communicating sensitive information to specially abled (or visually impaired) users using a token device that comprises refreshable braille display.

BACKGROUND

[0002] Generally, while performing an online transaction (e.g., making an online payment or through a mobile application), user authentication is performed to verify that the online transaction is initiated by an authentic user or with the consent of the authentic user. Typically, performing the user authentication may involve transmitting (textual) sensitive information, for instance a one-time password (OTP), to a user device registered with the user and prompting the user to enter the sensitive information received on his/her registered device into a payments page associated with the online transaction. The authenticity of the transaction is confirmed (i.e., it is determined that the transaction is being initiated by the authorized user or with the consent of the authorized user) when the sensitive information entered by the user matches the sensitive information delivered to the user device. In certain aspects, performing the user authentication may additionally or alternatively involve prompting the user to enter a Card Verification Value (CVV) number associated with a payments card used for making the online payment.

[0003] However, problem arises when users with visual disabilities (also referred to as “specially abled users”) try to perform such online transactions. The visually impaired users may be unable to read the textual sensitive information like OTP delivered to their registered devices. To read the sensitive information received in textual form, the visually impaired users typically need to install screen-reader software or need to have “talkback feature” on their device, which can read the sensitive information received in the textual format i.e., OTP. The screen reader’s output may be sent to an audio output device (e.g., speakers) associated with the user device as a synthesized voice which reads out the sensitive information to enable the visually impaired users perform the online transaction. However, reading the sensitive information aloud may pose serious risk of exposing the sensitive information to attackers that might eavesdrop or overhear the sensitive information. Based on the heard sensitive information, the attackers may perform fraudulent transactions on behalf of the user.

[0004] Hence, to overcome these security vulnerabilities and other associated problems, there exists a need for secure techniques for communicating sensitive information for specially abled users to validate online payments and transactions.

[0005] 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

[0006] 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:

[0007] **Figure. 1A** shows an exemplary system **100** where the proposed technique of securely communicating sensitive information for specially abled users may be implemented, in accordance with some embodiments of the present disclosure.

[0008] **Figure 1B** shows a payment system implementing the proposed technique of securely communicating sensitive information for specially abled users, in accordance with some embodiments of the present disclosure.

[0009] **Figure 2** shows an exemplary block diagram **200** of the system **100** as illustrated in **Figure 1**, in accordance with some embodiments of the present disclosure.

[0010] **Figure 3** illustrates a flow diagram representing an exemplary method **300** of securely communicating sensitive information for specially abled users, in accordance with some embodiments of the present disclosure.

[0011] 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

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

[0016] The present disclosure relates to a system and a method of efficiently and securely communicating sensitive information for specially abled users. Typically security tokens are devices that are connected externally to a user device and may act like an electronic key to

access restricted content and sensitive or confidential data from the user device. Some examples of security tokens include wireless keycards that are used to open locked doors, banking tokens that are used as a digital authenticator for signing into online banking or signing a transaction such as a wire transfer. The security token is used in addition to or in place of a password. Security tokens may also store sensitive information such as passwords, cryptographic keys, biometric data, but not limited thereto. Some security tokens may include small keypads to allow entry of a PIN or a simple button to start a generating routine with some display capability to show a generated key number. Connected tokens utilize a variety of wires or wireless interfaces including Universal Serial Bus (USB), near-field communication (NFC), radio-frequency identification (RFID), or Bluetooth.

[0017] In an exemplary embodiment or aspect, the desired objective of communicating the sensitive information is achieved by connecting or pairing a braille token device (which may be similar to a security token) with a user device via a suitable network (e.g., Bluetooth), as shown in **Figure 1**A. Referring now to **Figure 1A**, which illustrates an exemplary communication system **100** where the proposed techniques of securely communicating sensitive information for specially abled users may be implemented, in accordance with some embodiments of the present disclosure. The system **100** may include a user device **110** and a braille token device **120** communicatively connected over a network. The user device **110** may be any mobile or non-mobile device such as a mobile phone, a tablet, a laptop, or any other computing device that may be communicatively connected with the braille token device **120**. In an exemplary embodiment, the network may be Bluetooth network. However, the present disclosure is not limited thereto and in general, the network may include any wired or wireless network such as USB, NFC, RFID, etc. In various embodiments, when the user device **110** and the braille token device **120** are paired for the first time, the user device **110** may grant permission to the braille token device **120** to access permitted contents from the user mobile device **110**. For example, the permitted contents may include SMS, email, notification, or the like**.**

[0018] In various embodiments, the braille token device **120** may include a refreshable braille display **122** that may comprise round-tipped pins raised through holes in a flat surface and a button **124** that when pressed by the user may indicate the braille token device **120** that the user is ready to read the sensitive information conveyed to or fetched by the braille token device **120**. In one embodiment, the braille token device **120** may include a biometric sensor as an

alternative or in addition to the button to authenticate the user for reading the conveyed sensitive information. The user's biometric data may be obtained and stored in the braille token device **120** when the user starts using the braille token device **120** for the first time**.**

[0019] Further, the braille token device **120** may store one or more regular expression formats matching with possible formats of the sensitive information and may include a driver program that may access the permitted contents from the user mobile device **110**. After accessing the permitted contents from the user mobile device **110**, the braille token device **120** may try to correlate the accessed content with the stored regular expression formats and if any format matches, the braille token device **120** may read the sensitive information comprised in the accessed content. For example, if the permitted content to the braille token device **120** is SMS and the sensitive information is OTP, the braille token device **120** reads SMSs received by the user mobile device **110** and try to match stored regular expression formats of a common OTP format i.e., 4-6 digits of contiguous numbers with SMSs received by the user mobile device **110**. If any common OTP format is found in the SMS, the braille token device **120** understands the OTP as the sensitive information and separates out the sensitive information (i.e., the OTP) from the accessed content (i.e., SMS).

[0020] In a non-limiting embodiment, upon reading the sensitive information (e.g., OTP), the braille token device **120** may show up a first digit of the sensitive information on the braille display **122** (e.g., by electronically raising and lowering different combinations of pins on the braille display **122**). The visually impaired user may read the first digit (e.g., by placing/moving their finger on the braille display **122** to sense tactile representation of the first digit) and may press the button **124** in the braille token device **120** to indicate that the user is ready to read the sensitive information. After the button is pressed, the braille token device **120** shows up the rest of the sensitive information (e.g., by electronically raising and lowering different combinations of pins on the braille display **122**). For example, when the sensitive information is an OTP, the braille token device **120** may read the OTP from an SMS and show up a first digit of the OTP on the braille display **122.** The user senses the display of the first digit of the OTP and may press the button **124.** When the button **124** is pressed, the braille token device **120** shows up the rest of the digits of the OTP. Alternatively, after pressing the button **124**, the braille token device **120** shows up the all digits of the OTP (including the first digit). In this manner, the visually impaired user may read the OTP from the braille display **122** to authenticate the online transaction**.**

[0021] In another embodiment, the braille token device **120** comprises a biometric sensor, when the braille token device **120** shows up the first digit of the OTP on the braille display **122,** the user may place their thumb/finger over the biometric sensor in the braille token device **120** for biometric authentication**.** The braille token device **120** may capture the user's biometric data and may compare the captured biometric data with the biometric data stored in the braille token device **120.** If the captured biometric data matches the biometric data stored in the braille token device **120,** then the braille token device **120** shows up the rest of the sensitive information on the braille display **122** and the user reads the OTP from the braille display **122.**

[0022] **Figure 1B** illustrates a payment transaction system for securely communicating sensitive information for specially abled users. As illustrated in Figure 1B, a visually impaired user's mobile device is paired with a braille token device through Bluetooth and is placed close to the user's mobile device. The visually impaired user may try to perform an online transaction e.g., making an online payment or through a mobile application. The user may first open/run the mobile application installed in the user's mobile device and may fill up necessary transaction details. To complete the payment transaction, the user may send an authorization request to the transaction provider such as a bank. In response, the transaction provider may send an OTP to the user's mobile device through SMS. Since the braille token device is paired with the user's mobile device, the braille token device may read the OTP from the SMS received in the user's mobile device and may show up the first digit of the OTP on the braille display of the braille token device. The user may sense the displayed first digit of the OTP on the braille display and may either press a button on the braille token device or may perform authentication through the biometric sensor integrated in the braille token device to indicate that the user is ready to read the OTP. Upon detecting the pressing of the button or the authentication through the biometric sensor, the braille token device displays the rest of the digits of the OTP on the braille display**.** The user may read the OTP from the braille display to authenticate the online transaction**.**

[0023] The mobile device may communicate with the transaction provider through a data network such as, but not restricted to, the Internet, Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), etc. In certain embodiments, the network may include a wireless network, such as, but not restricted to, a cellular network and may employ various technologies including Enhanced Data rates for Global Evolution

(EDGE), General Packet Radio Service (GPRS), Global System for Mobile Communications (GSM), Internet protocol Multimedia Subsystem (IMS), Universal Mobile Telecommunications System (UMTS) etc. In one embodiment, the network may include or otherwise cover networks or subnetworks, each of which may include, for example, a wired or wireless data pathway.

[0024] Referring now to **Figure 2** that shows an exemplary block diagram **200** of the system **100** as illustrated in **Figure 1**. As shown in **Figure 2**, the user mobile device **110** may include a memory **212**, a transceiver **216**, and a processor **214**. The transceiver **216** is configured to facilitate exchange of data between the user mobile device **110** and a braille token device **120**. The transceiver **216** is also configured to facilitate exchange of data between the user mobile device **110** and a payment system. The memory **212** is configured to store necessary commands needed for pairing with the braille token device 120 and to provide access to read permitted contents to the braille token device **120**. Further, the memory **212** is configured to store necessary commands needed for initiating a payment transaction and for performing subsequent steps required for completing a payment transaction. The processor **214** is communicatively coupled to the memory **212** and to the transceiver **216**. The processor **214** may perform various operations of the mobile device **110**. In an exemplary embodiment, the processor **214** may execute the instructions to run mobile applications and initiate a payment transaction request. The processor **214**, may also respond to the requests received from the digital payment system **120**.

[0025] Likewise, the braille token device **120** may include a memory **232**, the display **122** (though not shown again in Figure 2), a transceiver **236**, and a processor **234**. The transceiver **236** is configured to facilitate exchange of data between the braille token device **120** and the user mobile device **110**. The memory **232** is configured to store necessary commands needed for a driver program that may read permitted contents in the user mobile device 110 and may recognize sensitive information. Further, the memory **232** may store commands to display a part of the read data initially on the braille display and to respond to a click of a button by displaying the remining sensitive data in the braille display. Further, the memory **232** may also contain biometric data of the user stored in it. The processor **234** is communicatively coupled to the memory **232** and to the transceiver **236**. The processor **234** processes or performs various operations of the system **100**. In an exemplary embodiment, the processor **214** may execute the instructions for a driver program to read permitted contents in the user mobile device **110** and

to recognize sensitive information. Further, the processor **234** may store commands to display a part of the sensitive information initially on the braille display **122** and to respond to a click of a button by displaying the remining sensitive information on the braille display **122**.

[0026] The memory **212**, **232** may include a Random-Access Memory (RAM) unit and/or a non-volatile memory unit such as a Read Only Memory (ROM), optical disc drive, magnetic disc drive, flash memory, Electrically Erasable Read Only Memory (EEPROM), a memory space on a server or cloud and so forth. For the sake of illustration, it is assumed here that the memory is a non-volatile memory. Examples of the processor may include, but not restricted to, a general-purpose processor, a Field Programmable Gate Array (FPGA), an Application Specific Integrated Circuit (ASIC), a Digital Signal Processor (DSP), microprocessors, microcomputers, micro-controllers, digital signal processors, central processing units, state machines, logic circuitries, and/or any devices that manipulate signals based on operational instructions.

[0027] Referring now to **Figure 3** that depicts a flowchart illustrating a method **300** of securely communicating sensitive information for specially abled users, in accordance with some embodiments of the present disclosure. The method comprises, at block **302,** pairing a braille token device **120** with a user mobile device **110** for a first time and providing permission to the braille token device **120** to access permitted contents of the user mobile device **110**. At block **304,** when the user tries to make a transaction the braille token device **120** is paired with the user mobile device **110** and a transaction is initiated through an application installed in the user mobile device **110.** At block **306,** upon initiating the transaction, an authorization request is sent from the user mobile device **110** to a transaction provider to authenticate the transaction. In response to the authorization request sent to the transaction provider, the user mobile device **110** receives a SMS having sensitive information from the transaction provider. Further, at block **308**, the braille token device **120** accesses permitted contents from the user mobile device **110** and correlates the accessed content with stored regular expression formats and if there is any match, the braille token device **120** may read sensitive information from the accessed content.

[0028] Further, at block **310**, after the braille token device has read the sensitive information, the braille token device **120** shows up a first digit of the sensitive information on a braille display **122** of the braille token device **120**. The user may sense the displayed first digit of the

sensitive information on the braille display **122** and may press a button **124** on the braille token device **120** to indicate that the user is ready to read the sensitive information from the braille token device **120**. Upon pressing the button **124** in the braille token device **120**, the braille token device **120** displays the rest of the digits in the sensitive information (with or without the first digit) on the braille display **122.** In another embodiment, upon sensing the displayed first digit of the sensitive information on the braille display **122,** the user may perform biometric authentication through a biometric sensor integrated with the braille display device **122.** Upon successful authentication of the user, the braille token device **120** may display the rest of the digits on the sensitive information on the braille display **122.** The user may read the sensitive information from the braille display **122** and accordingly authenticate the online transaction.

Advantages of the proposed disclosure

[0029] The proposed techniques may help visually impaired users to authenticate payment transactions in a secure way without the fear of intruders listening or gaining access to the sensitive information read aloud while performing the online transaction. Using the device, sensitive information like OTP is conveyed to the visually impaired users through a media i.e., “Braille” that is already familiar to them. Hence, there is no need for the users to learn something completely new again, e.g., morse code, just to do everyday tasks like making use of OTP. Additionally, braille token device can be attached to the user device. For example, it can be affixed/attached at the front side of the user device or at the back of the user device with the use of device cases/covers.

[0030] 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.

[0031] 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.

[0032] 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.

.

BRAILLE OTP TOKEN

ABSTRACT

The present disclosure relates to a system and a method of providing secured authentication to visually impaired users. The secured authentication is provided by connecting a braille token device (120) with a user mobile device (110) and receiving sensitive information in the braille token device read from Short Mailing Service (SMS) received in the user mobile device. To receive the sensitive information, the braille token device includes a driver program that may match a format of sensitive information stored in the braille token device with the format of the sensitive information received in the SMS of the user mobile device. If the format matches, the braille token device reads the sensitive information from the SMS. The proposed techniques may help the users to authenticate payment transactions in a secured way.

Figure 1B

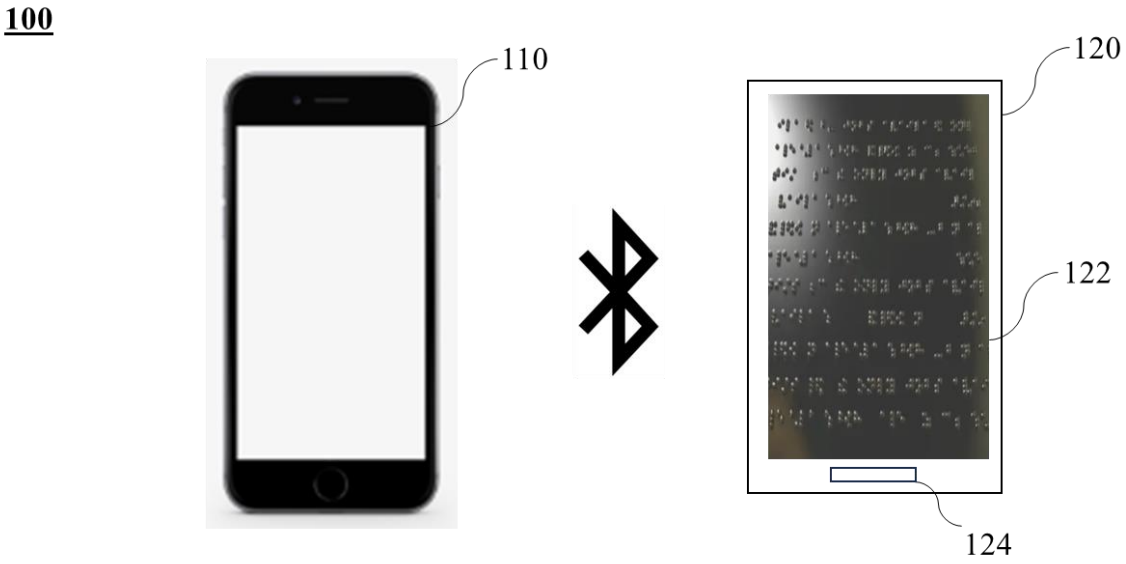

Figure 1A

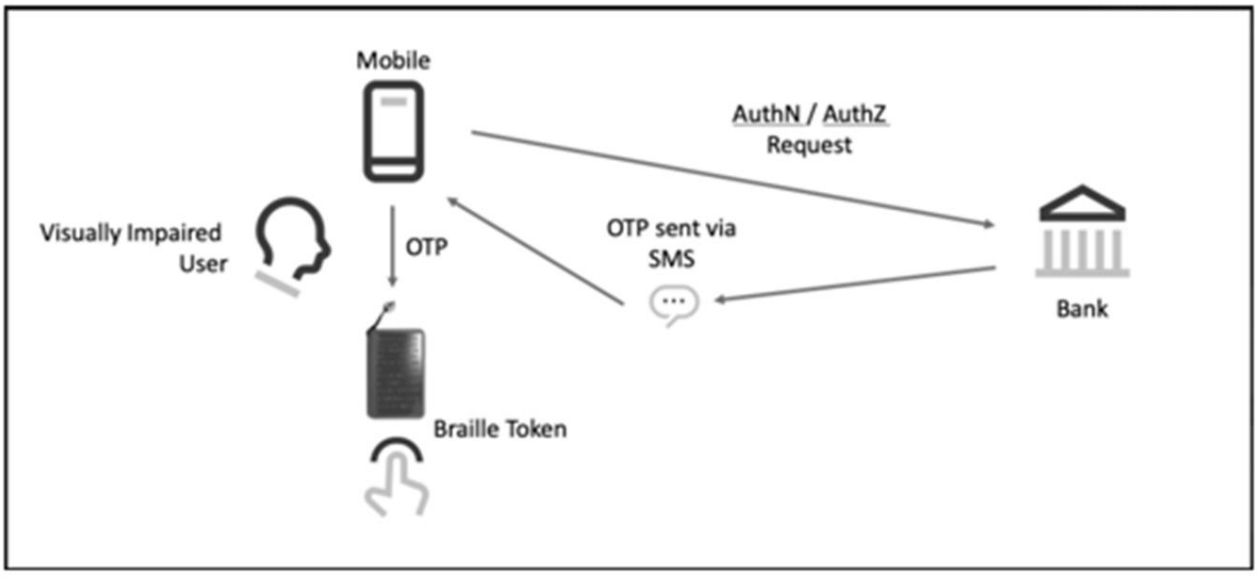

Figure 1B

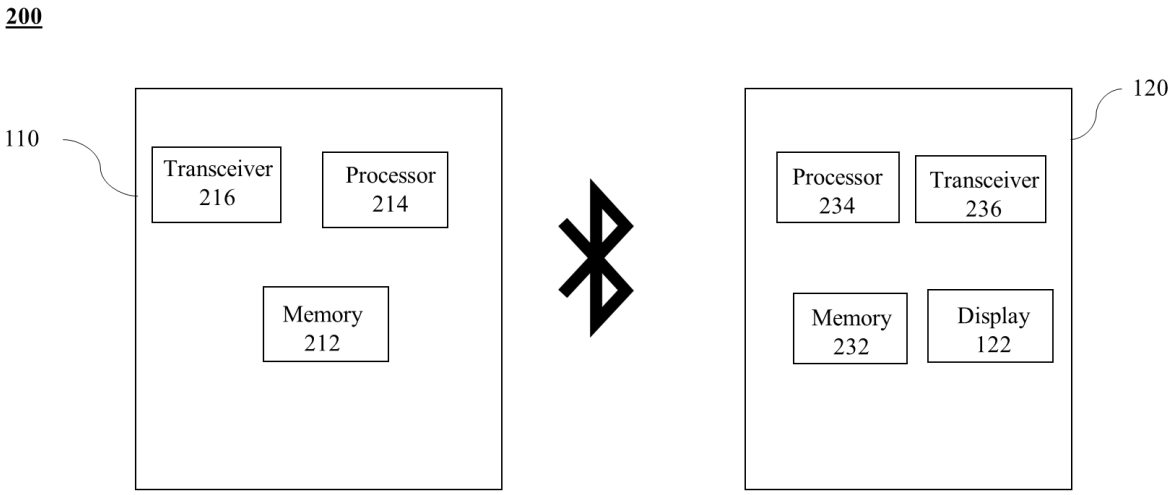

Figure 2

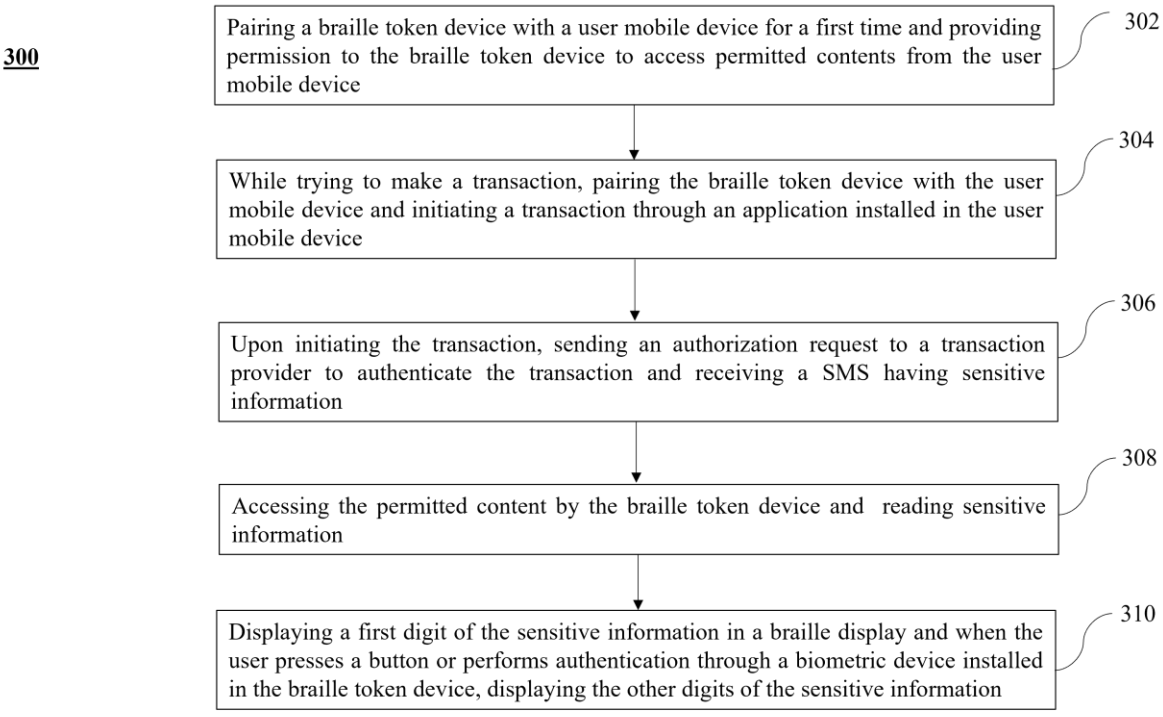

Figure 3