(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 January 2016 (28.01.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/014346 A1

(51) International Patent Classification:
G06Q 20/00 (2012.01)

(21) International Application Number:
PCT/US2015/040819

(22) International Filing Date:
16 July 2015 (16.07.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/027,855 23 July 2014 (23.07.2014) US
14/752,698 26 June 2015 (26.06.2015) US

(71) Applicant: **SQUARE, INC.** [US/US]; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US).

(72) Inventors: **REZAYEE, Afshin**; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US). **SMITH, Malcolm, R.**; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US). **VADERA, Kshitiz**; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US). **WAI NG, Kevin, Ka**; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US). **YAN, Haipeng**; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US).

(74) Agents: **VAN HOVEN, Joshua** et al.; Maynard Cooper & Gale, P.C., 655 Gallatin Street, SW, Huntsville, AL 35801 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report (Art. 21(3))*

(54) Title: POINT OF SALE SYSTEM WITH SECURE AND UNSECURE MODES

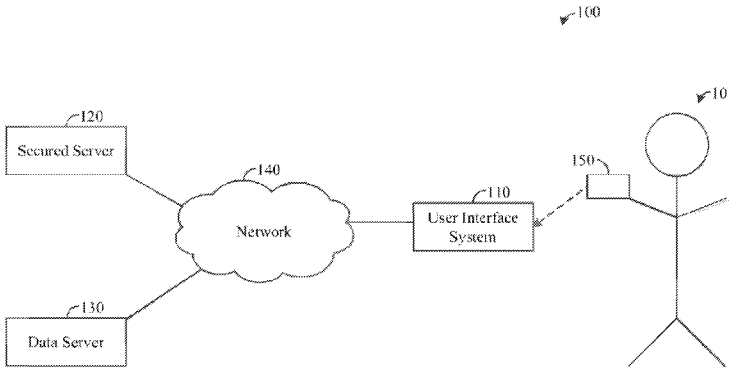

FIG. 1

(57) Abstract: A point of sale system has a display for receiving touch inputs, a controller to receive the touch inputs from the display, and a secure controller to receive touch input data from the controller. The system also has a card interface module and a contactless interface module to provide encrypted data to the secure controller. The secure controller can operate in either a secure mode or a non-secure mode. When a non¬ secure mode is engaged, the secure controller provides the touch input data to a processor. When a secure mode is engaged, the secure controller blocks at least a portion of the touch input data from the processor.

WO 2016/014346 A1

POINT OF SALE SYSTEM WITH SECURE AND UNSECURE MODES

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 62/027,855, filed July 23, 2014, and U.S. Non-Provisional Application No. 14/752,698, filed June 26, 2015, which applications are hereby incorporated by reference in entirety.

BACKGROUND

[0002] Many computing systems and devices now typically include some form of display. Displays are becoming more common for various reasons, such as decreasing manufacturing costs due to advancing technologies and increasing functionalities. For example, displays can act as input and output devices (*e.g.*, touch sensitive displays) and can also show varying types of media with ease (*e.g.*, high-definition videos and images).

[0003] Touch sensitive displays are increasingly used in computing systems and devices that involve some user interaction. Unlike typical input devices, such as keypads or pointing devices, touch sensitive displays can accommodate a wider range of inputs, such as keyboard entries and gestures. Touch sensitive displays can, therefore, facilitate greater user interactions between the users and the computing systems since there is less restriction on the types of user inputs that can be received by the system.

[0004] Certain displays can operate to show and/or receive data of varying degrees of security. For example, a point of sale system can receive authentication information from a user, via a touch sensitive device, to complete a payment transaction while also engaging the user for other purposes, such as marketing campaigns. However, data involved in payment transactions needs to comply with industry security protocols and can require increased data processing by the point of sale system that can cause delays in the operation of the point of sale system as a whole.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] FIG. 1 is a block diagram of an embodiment of components interacting with a user interface system.

[0006] FIGS. 2A-2C are block diagrams of embodiments of the user interface system of FIG. 1.

[0007] FIGS. 3A and 3B illustrate an embodiment of a touch sensitive computing device in operation.

[0008] FIGS. 4A and 4B illustrate an embodiment of the touch sensitive computing device of FIGS. 3A and 3B in another operation.

[0009] FIG. 5 is a block diagram of a further embodiment of the user interface system of FIG. 1.

[0010] FIG. 6A illustrates an embodiment of a computing device in operation.

[0011] FIG. 6B illustrates an embodiment of the computing device of FIG. 6A in another operation.

[0012] The drawings, described below, are provided for purposes of illustration, and not of limitation, of the aspects and features of various examples of embodiments described herein. For simplicity and clarity of illustration, elements shown in the drawings have not necessarily been drawn to scale. The dimensions of some of the elements may be exaggerated relative to other elements for clarity. It will be appreciated that for simplicity and clarity of illustration, where considered appropriate, reference numerals may be repeated among the drawings to indicate corresponding or analogous elements or steps.

DETAILED DESCRIPTION

[0013] The various embodiments described herein generally relate to a user interface system operable to provide secured and unsecured modes for handling data. Some of the described embodiments can be directed to receiving secured and unsecured touch input. The user interface system can include a touch sensitive computing device in one embodiment. In some described embodiments, the user interface system can be for providing secured and unsecured outputs. Some other embodiments of the user interface system may involve receiving secured and unsecured touch input as well as providing secured and unsecured outputs.

[0014] Data being provided or received at a computing system such as a user interface system typically cannot be easily distinguished based on security levels and/or requirements. Secured data generally needs to comply with certain industry security protocols and thus, the processing of such secured data can consume a substantial portion of the processing resources available at the computing system. However, unsecured data does not need to comply with any industry security protocols and processing the unsecured data in the same manner as the secured data can impair the operation of the computing system as a whole.

[0015] For example, touch sensitive computing devices with touch sensitive displays can generally facilitate greater user interactions between the users and the respective computing system than most typical input devices, such as keypads or pointing devices. Touch sensitive displays can accommodate a wider range of inputs, such as keyboard entries and gestures and so, the design of the user interfaces for the touch sensitive computing device are less restricted by the types of inputs that can be used.

[0016] Points of sale systems, for example, that incorporate a user interface system can receive authentication information from a user to complete a payment transaction and can also engage the user for other purposes, such as marketing campaigns offered by the merchant. The data involved in payment transactions, however, needs to comply with industry security protocols, which can consume a substantial portion of the processing resources at the point of sale system. Processing of both the transaction data and unsecured data in the same manner is likely to impair the operation of the point of sale system.

[0017] It will be appreciated that numerous specific details are set forth in order to provide a thorough understanding of the example embodiments described herein. However, it will be understood by those of ordinary skill in the art that the embodiments described herein may be practiced without these specific details. In other instances, well-known methods, procedures and components have not been described in detail so as not to obscure the embodiments described herein. Furthermore, this description and the drawings are not to be considered as limiting the scope of the embodiments described herein in any way, but rather as merely describing the implementation of the various embodiments described herein.

[0018] Reference is first made to FIG. 1, which illustrates a block diagram 100 of a user 10 and components interacting with a user interface system 110.

[0019] The user interface system 110 can be in electronic communication with a secured server 120 and a data server 130 via a network 140. The user interface system 110 can also receive input, directly or indirectly, from the user 10. For example, the user interface system 110 can receive input indirectly from the user 10 via a payment card 150 or a computing device.

[0020] The secured server 120 can operate generally with secured data while the data server 130 can operate generally with other data. Each of the secured server 120 and the data server 130 may include one or more processors with computing processing abilities and memory such as a database(s) or file system(s).

[0021] For example, when the user interface system 110 operates to receive data, the secured server 120 can operate based generally on secured data provided from the user interface system 110, and the data server 130 can operate based on other data provided from the user interface system 110. When the user interface system 110 operates to provide data, the secured server 120 can operate to provide secured data while the data server 130 can operate to provide the other data to the user interface system 110.

[0022] It will be understood that, although only one secured server 120 and one data server 130 are shown in FIG. 1, each of the secured server 120 and the data server 130 may include one or more servers that may be distributed over a wide geographic area and connected via the network 140. It is also possible for the secured server 120 and the data server 130 to be provided as one server, and for the secured server 120 to be separated by data encryption or security.

[0023] The network 140 can generally be any network capable of carrying data, including the Internet, Ethernet, plain old telephone service (POTS) line, public switch telephone network (PSTN), integrated services digital network (ISDN), digital subscriber line (DSL), coaxial cable, fiber optics, satellite, mobile, wireless (*e.g.*, Wi-Fi, WiMAX), SS7 signaling network, fixed line, local area network, wide area network, and others, including any combination of these, capable of interfacing with, and enabling communication between, the user interface system 110, the secured server 120 and the data server 130.

[0024] In some embodiments, different networks can be provided for each of the secured server 120 and the data server 130. A secured network may be provided to facilitate electronic communication between the user interface system 110 and the secured server 120. For example, when the user interface system 110 operates as a

point-of-sale system, the secured server 120 can be a payment processing gateway for authorizing payment transactions initiated at the point-of-sale system and the data server 130 can be a merchant server for facilitating other operations available via the point-of-sale system, such as marketing campaigns or loyalty programs offered by the merchant. The secured network between the payment processing gateway (secured server) 120 and the point-of-sale system (user interface system) 110 can therefore be provided to enable secured and encrypted data transfer, whereas another network can be used to provide data transfer between the merchant server (data server) 130 and the point-of-sale system (user interface system) 110.

[0025] The user interface system 110 can include any computing device with a display or operable with a display. The display may be a touch sensitive display in some embodiments. The computing device can also be operable to connect to the network 140. The computing device may couple to the network 140 through a wired or wireless connection. Example computing devices may include at least a processor and memory. In one embodiment, the computing device may be an electronic tablet device, a personal computer, workstation, server, portable computer, mobile device, personal digital assistant, laptop, smart phone, WAP phone, an interactive television, video display terminals, gaming consoles, and portable electronic devices or any combination of these.

[0026] Reference will be made to FIG. 2A, which is a block diagram 200A of an embodiment of the user interface system 110. The user interface system 110 in this embodiment can operate as a touch sensitive system and as shown in FIG. 2A, the touch sensitive system 200A can include a touch sensitive display 212, a processing module 210, and an interface module 230.

[0027] The interface module 230 can include a secure input controller 232 and an input controller 234. As shown in FIG. 2A, the input controller 234 can be operatively coupled to the touch sensitive display 212, and the secure input controller 232 can be operatively coupled to the touch sensitive display 212 and the input controller 234. Input controllers 232, 234 may receive the input data from the touch sensitive display 212 via touch electrodes.

[0028] Each of the input controller 234 and the secure input controller 232 can receive input data provided via the touch sensitive display 212, and interpret the touch input accordingly.

[0029] The secure input controller 232 can be dedicated to receiving and interpreting touch input that requires compliance with certain security protocols. The secure input controller 232 can receive secured input directly from the touch sensitive display 212, or indirectly via the input controller 234. Compliance with security protocols can involve various control measures that require substantial processing power, such as maintenance of a firewall, regular updates of anti-virus software applications, restriction to access, application of various encryption protocols, etc. The secure input controller 232, therefore, is likely to operate slower than the input controller 234, which is not limited by the security protocols.

[0030] In some embodiments, the touch sensitive display 212 can include a secured display portion for receiving only secured touch input. Any data received at the secured display portion will be processed by the secure input controller 232.

[0031] The secure input controller 232 can, in some embodiments, operate in conjunction with the input controller 234. The input controller 234 can receive touch input from all regions of the touch sensitive display 212 or, if there is a secured display portion, the input controller 234 can receive touch input from regions of the touch sensitive display 212 apart from the secured display portion. The secure input controller 232 can then receive data based on the touch input provided from the input controller 234. Based on the data provided by the input controller 234, the secure input controller 232 can identify the secured touch input and prevent the secured touch input from being provided to the processing module 210.

[0032] With the input controller 234 and the secure input controller 232, the touch sensitive system 200A may, therefore, engage in different modes of operations, such as a non-secure input mode and a secure input mode. In some embodiments, the touch sensitive system 200A can be engaged in the secure input mode in response to a signal received from a software application stored at the touch sensitive system 200A or a signal received from the secured server 120.

[0033] During the non-secure input mode, the touch sensitive system 200A can receive input at the touch sensitive display 212 that is not limited by security protocols and can be provided directly to the processing module 210. The touch sensitive system 200A can couple the input controller 234 to the processing module 210 for communicating the received touch input to the processing module 210. In some embodiments, the input controller 234 can be coupled to the processing module 210 via the secure input controller 232. The input controller 234 may be coupled to the secure input controller

232 via an Inter-Integrated Circuit (I2C) connection. Similarly, the secure input controller 232 may be coupled to the processing module 210 via an I2C connection.

[0034] During the secure input mode, the touch sensitive system 200A can receive input at the touch sensitive display 212 that needs to comply with security protocols. As described, the secure input controller 232 can receive the secured touch input directly from the touch sensitive display 212 (e.g., via a secured display portion) and/or indirectly via the input controller 234.

[0035] After receiving the touch data from the touch sensitive display 212 and/or the input controller 234, the secure input controller 232 can block at least some of the touch inputs received at the touch sensitive display 212 from being provided to the processing module 210. By blocking at least some of the touch inputs from being communicated to the processing module 210, the secure input controller 232 can control the type of data that is provided to the processing module 210. For example, data such as authentication information are not provided to the processing module 210.

[0036] In some embodiments, the touch sensitive system 200A can activate an indicator 250 to visually show that the secure input mode is engaged. The indicator 250 can be operatively coupled to the secure input controller 232 so that when the secure input controller 232 is engaged in the secure input mode, the secure input controller 232 can also activate the indicator 250. The indicator 250 may be a LED or other visual indicator provided at the touch sensitive system 200A.

[0037] Reference will now be made to FIG. 2B. FIG. 2B is a block diagram 200B of another embodiment of the user interface system 110. In the block diagram 200B, the user interface system 110 is provided as a point-of-sale system.

[0038] Similar to the touch sensitive system 200A shown in FIG. 2A, the point-of-sale system 200B includes the processing module 210, the touch sensitive display 212 and an interface module 230'.

[0039] The interface module 230' of the point-of-sale system 200B, like the interface module 230 of FIG. 2A, includes a secure input controller 232 and an input controller 234. During the secure input mode, the secure input controller 232 in this example needs to comply with industry security requirements, such as the Payment Card Industry Data Security Standards (PCI DSS).

[0040] The interface module 230' also includes a card interface module 236, a contactless interface module 238 and a tamper-resistance measure module 240.

[0041] The card interface module 236 and the contactless interface module 238 operate to receive and process data from the payment card 150 or other compatible computing devices. Each of the card interface module 236 and the contactless interface module 238 can be operatively coupled to the secure input controller 232, as shown in FIG. 2B, to encrypt data received from the payment card 150 or other compatible computing devices. Briefly, as shown in FIG. 3B, an example point-of-sale system 200B can include various card interfaces, such as a chip reader 336a and a magnetic strip reader 336b, for receiving card data that is to be processed by the card interface module 236. A contactless reader 338 is also illustrated in FIG. 3B for receiving data to be processed by the contactless interface module 238.

[0042] Referring still to FIG. 2B, the tamper-resistance measure module 240 can be operatively coupled to the secure input controller 232. The tamper-resistance measure module 240 can operate with the secure input controller 232 to engage one or more different tamper resistance components provided in the physical tamper-resistance measures 214 at the point-of-sale system 200B, or to receive tamper signals from the physical tamper-resistance measures 214 indicating there was an attempt at modifying the point-of-sale system 200B. The physical tamper-resistance measures 214 generally prevent counterfeiters from modifying the point-of-sale system 200B or otherwise accessing the interface module 230' for obtaining the secured data. The physical tamper-resistance measures 214 can include components, such as a mesh or switches, that can detect any attempt at physical disassembly or modification of the point-of-sale system 200B.

[0043] Another embodiment of the user interface system 110 will now be described with reference to FIG. 2C. FIG. 2C is yet another block diagram 200C of the user interface system 110 in accordance with yet another example embodiment. In the block diagram 200C, the user interface system 110 may be provided as a display system.

[0044] Similar to the touch sensitive system 200A of FIG. 2A and the point-of-sale system 200B of FIG. 2B, the display system 200C includes a processing module 210', the touch sensitive display 212 and an interface module 230. It will be understood that the interface module 230' may similarly be provided as part of the display system 200C in some other embodiments.

[0045] The processing module 210' of the display system 200C includes a secure processing module 252 and a device processing module 254. The secure processing module 252, like the secure input controller 232, can include processing components

that are configured to comply with security protocols. As a result, the secure processing module 252 may operate slower than the device processing module 254. The device processing module 254 can be native to the computing device(s) providing the display system 200C.

[0046] Similar to the touch sensitive system 200A and the point-of-sale system 200B, when operating in the secure input mode, the display system 200C can receive input at the touch sensitive display 212 that needs to comply with security protocols. The secure input controller 232 can receive the secured touch input and initiate operation by the secure processing module 252.

[0047] During the non-secure input mode, the display system 200C can receive input at the touch sensitive display 212 that is not limited by security protocols and can be provided directly to the device processing module 254.

[0048] An example operation of the point-of-sale system 200B will now be described with reference to FIGS. 3A to 4B. FIGS. 3A to 4B illustrate an example point-of-sale system 300.

[0049] The point-of-sale system 300 includes a touch sensitive display 312, a chip reader 336a, a magnetic strip reader 336b, and a contactless reader 338. It will be understood that the point-of-sale system 300 illustrated in FIGS. 3A to 4B is merely an example and other configurations and designs are possible.

[0050] FIGS. 3A and 3B illustrate user interfaces 302A and 302B, respectively, for facilitating a payment transaction at the point-of-sale system 300. In FIG. 3A, the user interface 302A includes control buttons 314a to 314c for receiving a touch input for selecting a form of payment. The point-of-sale system 300 can continue to operate in the non-secured mode since the touch input being received is not secured data information.

[0051] In response to a selection of the form of payment or detection of an insertion of the payment card 150 at the chip reader 336a, the point-of-sale system 300 can be engaged in the secured mode since the touch input being received is authentication information that needs to comply with the payment security protocols. The point-of-sale system 300 may similarly be engaged in the secured mode in response to a signal received from the payment processing gateway 120. As shown in FIG. 3B, the user interface 302B provides a keypad for receiving a personal identification number (PIN) from the user. The PIN is then provided to the secure input controller 232 to complete the payment transaction. While the keypad is shown on the touch sensitive display 312,

an indicator (not shown in FIG. 3B) at the point-of-sale system 300 may be activated to indicate that the secured mode has been engaged.

[0052] Continuing with reference to FIGS. 4A and 4B, which illustrate user interfaces 402A and 402B, respectively, for facilitating other user interactions at the point-of-sale system 300. In FIG. 4A, the user interface 402A includes control buttons 414a and 414b for receiving a touch input for selecting a type of interaction, such as to join a loyalty program or to enter a contest. In the example of FIGS. 4A and 4B, the control button 414a was selected and the loyalty membership interface 402B of FIG. 4B is then shown. The point-of-sale system 300 can operate in the non-secured mode for both FIGS. 4A and 4B since the touch input received at user interfaces 402A and 402B does not need to comply with any industry security protocol. Inputs received via the loyalty membership interface 402B can be provided to the input controller 234 and eventually provided to the data server 130.

[0053] In the example of FIGS. 4A and 4B, the input controller 234 can continue to facilitate the user interactions at the point-of-sale system 300. Unlike operations involving the secure input controller 232, the user interactions shown in FIGS. 4A and 4B do not need to comply with any industry security protocols and therefore, unaffected by any compliance requirements.

[0054] Referring now to FIG. 5, which is a block diagram 500 of another embodiment of the user interface system 110 of FIG. 1.

[0055] The embodiment shown in the block diagram 500 can operate as a display system. The display system 500 includes a display 512, a processing module 510 and an interface module 530. The processing module 510 includes a secure processing module 552 and a device processing module 554. The interface module 530 includes a secure output controller 532 and an output controller 534.

[0056] Unlike the systems 200A to 200C, the display system 500 does not include a touch sensitive display 212. Instead, the display 512 can operate to show various data information.

[0057] As shown in FIG. 5, the processing module 510 is operatively coupled to the display 512 via the interface module 530. Depending on the operational mode, one of the secure processing module 552 and the device processing module 554 can be coupled to the display 512 via the interface module 530. As noted, the secure processing module 552, like the secure output controller 532, can include processing components that are configured to comply with security protocols. As a result, the

secure processing module 552 may operate slower than the device processing module 554. The secure processing module 552, therefore, should operate only to facilitate compliance with security protocols in order to avoid impairing the display system 500 unnecessarily.

[0058] During a secure output mode, for example, the secure output controller 532 can detect that the data to be provided to the display 512 requires compliance with certain security protocols. Accordingly, the secure output controller 532 can couple the secure processing module 552 with the display 512 to facilitate control of the display 512 by the secure processing module 552. On the other hand, during a non-secure output mode, the secure output controller 532 can couple the device processing module 554 with the display 512 so that the device processing module 554 controls the display 512. An example will now be described with reference to FIGS. 6A and 6B.

[0059] FIGS. 6A and 6B illustrate a computing device 600 having a display 612. The computing device 600 in this example is used at a bank to display data to a customer. For instance, the computing device 600 may be provided at a teller counter to provide various data to a customer being serviced by the teller. The data provided to the computing device 600 can range in varying levels of security, such as personal banking information and marketing campaigns developed by the bank.

[0060] FIG. 6A illustrates the computing device 600 operating in a secure mode. As shown on the display 612, a user interface 602A provides bank account balances. To control operation of the display 612 for providing the bank account data, the secure output controller 532 can couple the secure processing module 552 to the display 612.

[0061] FIG. 6B illustrates the computing device 600 operating in a non-secured mode. A user interface 602B provides information regarding mortgages and home insurance that are part of a marketing campaign offered by the bank.

[0062] Various embodiments have been described herein by way of example only. Various modification and variations may be made to these example embodiments without departing from the spirit and scope of the invention, which is limited only by the appended claims. Also, in the various user interfaces illustrated in the figures, it will be understood that the illustrated user interface text and controls are provided as examples only and are not meant to be limiting. Other suitable user interface elements may be possible.

CLAIMS

WHAT IS CLAIMED IS:

1. A point of sale system to facilitate a payment transaction by a user, the point of sale system comprising:

a touch sensitive display including touch electrodes configured to receive a touch input from a user, the touch sensitive display configured to display a user interface to facilitate a user interaction with the point of sale system, the user interface includes at least one selectable control button to receive a touch input by the user during the payment transaction; and

an interface module comprising:

an input controller configured to receive the touch input by the user from the touch sensitive display and to interpret the received touch input;

a card interface module configured to receive data from one of a chip reader or a magnetic strip reader in response to the one of a chip reader or a magnetic strip reader receiving data from a payment card, the card interface module configured to encrypt the data received from the one of a chip reader or a magnetic strip reader;

a contactless interface module configured to receive data from a contactless reader in response to the contactless reader receiving data from a device, the contactless interface module configured to encrypt the data received from the contactless reader; and

a secure input controller configured to receive touch input data from the input controller, the encrypted data from the card interface module, and the encrypted data from the contactless interface module, the secure input controller further configured to process the encrypted data received from the card interface module and the encrypted data received from the contactless interface module, the secure input controller configured to operate in a secure input mode and a non-secure input mode, the secure input controller configured to provide the touch input data received from the input controller to a device processing module when operating in the non-secure input mode and to provide the touch input data received from the input controller to a secure processing module when operating in the secure input mode.

2. The point of sale system of claim 1, wherein the secure input mode is engaged in response to one of a selection of a control button in the user interface indicating a form of payment or an insertion of the payment card into the one of a chip reader or a magnetic strip reader.

3. The point of sale system of claim 1, wherein the interface module further comprises a tamper-resistance measure module configured to receive a tamper signal from a tamper resistance component in response to an attempt to modify the point of sale system, the tamper resistance component comprising at least one of a mesh or switches, the secure input controller configured to receive the tamper signal from the tamper-resistance measure module.

4. The point of sale system of claim 1, wherein the user interface is configured to display a keypad configured to receive a touch input corresponding to a personal identification number (PIN), and the PIN is provided to the secure input controller to complete the payment transaction when the secure input controller is operating in a secure input mode.

5. A user interface system comprising:

a display including a user interface configured to receive touch input data from a user; and

an interface module comprising:

a secure controller configured to receive the touch input data, the secure controller further configured to operate in a secure mode and a non-secure mode; and

the secure controller configured to prevent a non-secure processing module from receiving the touch input data when the secure controller is operating in the secure mode and to provide the non-secure processing module with the touch input data when the secure controller is operating in the non-secure mode.

6. The user interface system of claim 5, wherein the secure mode is engaged in response to one of a selection of a control button in the user interface indicating a form of payment or an insertion of a payment card into the one of a chip reader or a magnetic strip reader.

7. The user interface system of claim 5, further comprising a secure processing module, the secure processing module configured to receive the touch input data from the secure controller when the secure controller is operating in the secure mode.

8. The user interface system of claim 7, wherein the secure controller is configured to couple the secure processing module to the display for output of data to the display when the secure controller is operating in the secure mode and couple the non-secure processing module to the display for output of data to the display when the secure controller is operating in the non-secure mode.

9. The user interface system of claim 5, further comprising a controller configured to receive and process the touch input data from the display and the secure input controller configured to receive the processed touch input data from the controller.

10. The user interface system of claim 9, wherein the secure controller is configured to identify secure touch input in the touch input data from the controller and to prevent the secure touch input from being provided to the non-secure processing module.

11. The user interface system of claim 5, wherein the display comprises a secure display portion, the secure display portion configured to receive a secured touch input, and wherein the secure controller is configured to receive the secured touch input directly from the secure display portion.

12. The user interface system of claim 5, further comprising an indicator, the secure controller configured to activate the indicator when operating in the secure mode.

13. The user interface system of claim 5, wherein the interface module comprises:

a card interface module configured to receive data from one of a chip reader or a magnetic strip reader, the card interface module configured to encrypt the data received from the one of a chip reader or a magnetic strip reader;

a contactless interface module configured to receive data from a contactless reader, the contactless interface module configured to encrypt the data received from the contactless reader; and

the secure controller configured to receive and process the encrypted data from the card interface module and the encrypted data from the contactless interface module.

14. A method of operating a point of sale system comprising:

displaying on a point of sale system a user interface to facilitate a user interaction with the point of sale system;

receiving touch input data from a user via a touch sensitive display of the point of sale system;

receiving, by a secure input controller, the touch input data from the touch sensitive display;

preventing, by the secure input controller, the touch input data from being provided to a processing module when operating the secure input controller in the secure input mode; and

providing, by the secure input controller, the touch input data to the processing module when operating the secure input controller in the non-secure input mode.

15. The method of claim 14, further comprising:

receiving, by the secure input controller, a signal to initiate operation in a secure input mode;

operating the secure input controller in the secure input mode in response to receiving the signal;

the processing module comprising a secure processing module and a non-secure processing module;

providing, by the secure input controller, the touch input data to the secure processing module when operating the secure input controller in the secure input mode; and

providing, by the secure input controller, the touch input data to the non-secure processing module when operating the secure input controller in the non-secure input mode.

16. The method of claim 14, further comprising:

receiving user data from one of a chip reader, a magnetic strip reader or a contactless reader;

encrypting, by a module, the received user data;

providing, by the module, the encrypted user data to the secure input controller; and

processing, by the secure input controller, the encrypted data received from the module.

17. A point of sale system comprising:

a user interface system configured to receive an input from a user, the user interface system comprising:

a touch sensitive display including a user interface configured to receive touch input data provided by the user;

an input controller configured to receive and process the touch input data provided by the user from the touch sensitive display;

a module configured to receive and encrypt payment data provided by a user via the user interface system; and

a secure input controller configured to receive the processed touch input data from the input controller and receive the encrypted payment data from the module, the secure input controller configured to provide the processed touch input data received from the input controller to a processing module when operating in a non-secure input mode and to prevent at least some of the processed touch input data received from the input controller from being provided to the processing module when operating in a secure input mode; and

the user interface system configured to provide secure data over a network to a secure server and to provide non-secure data over the network to a data server.

18. The point of sale system of claim 17, wherein the secure input mode is engaged in response to a signal from the secure server.

19. The point of sale system of claim 17, wherein:

the user interface system further comprises at least one of a chip reader, a magnetic strip reader or a contactless reader to receive data from a user; and

the module further comprises at least one of:

a card interface module configured to receive and encrypt user data provided via one of the chip reader or the magnetic strip reader; and

a contactless interface module configured to receive and encrypt user data provided via the contactless reader.

20. The point of sale system of claim 17, wherein:

the secure server is configured to operate as a payment processing gateway to authorize payment transactions initiated at the user interface system;

the data server is configured to operate as a merchant server to facilitate marketing campaigns or loyalty programs; and

the user interface system is configured to provide the secure data over a secured network to the secure server, the secured network is configured to enable secure and encrypted data transfer between the user interface system and the secure server.

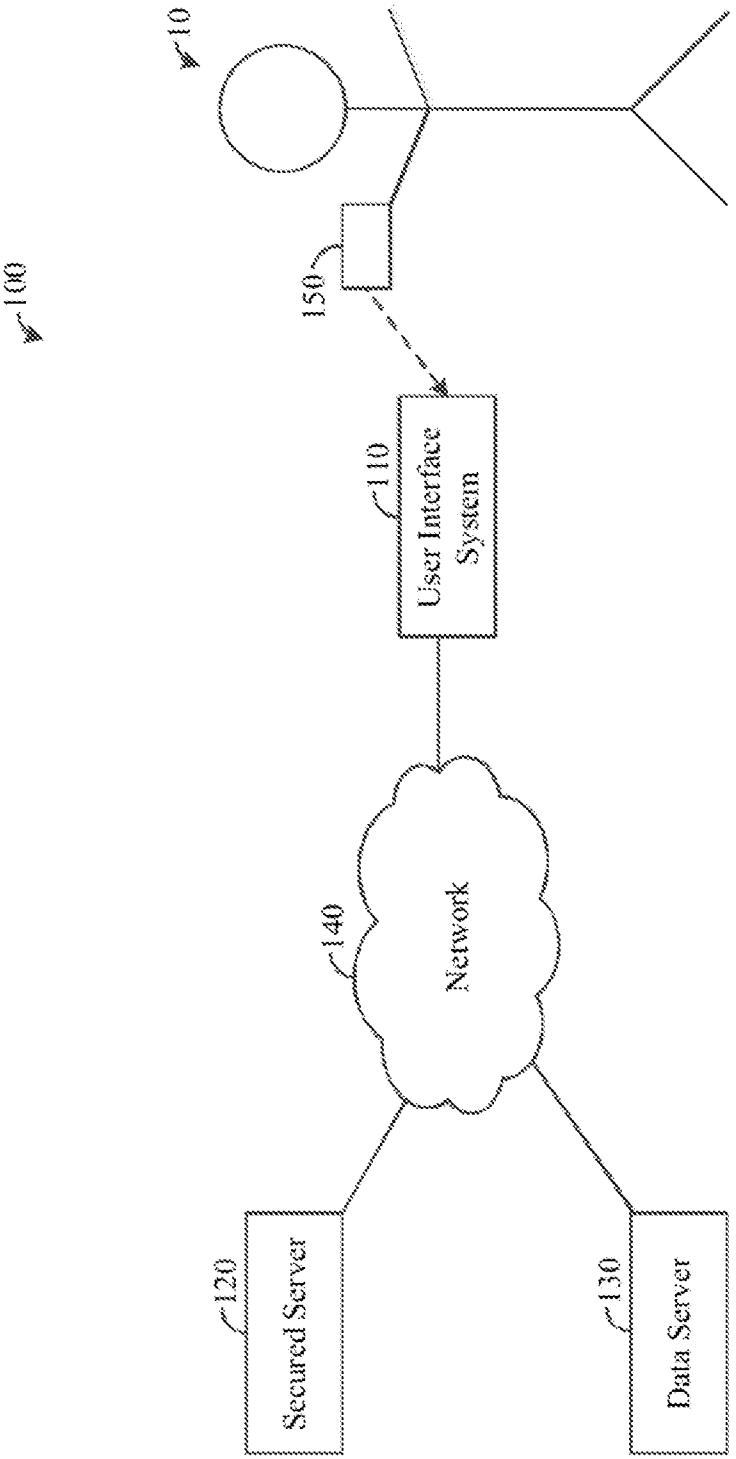
100
10
150
110
User Interface System
140
Network
120
Secured Server
130
Data Server

FIG. 1

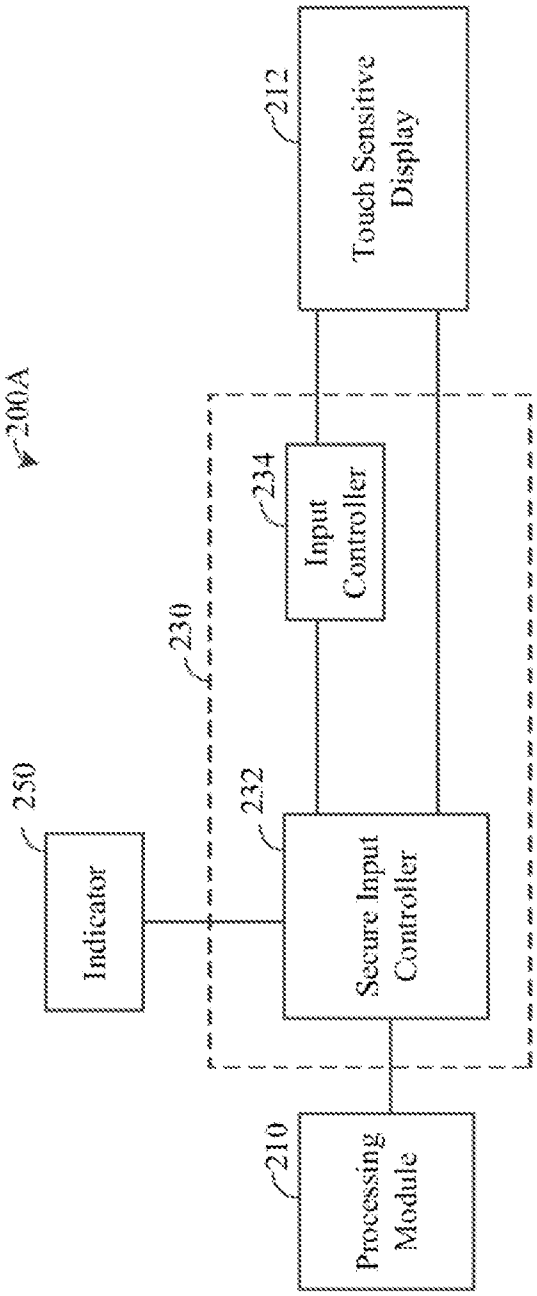
200A
250
Indicator
230
232
Secure Input Controller
234
Input Controller
212
Touch Sensitive Display
210
Processing Module

FIG. 2A

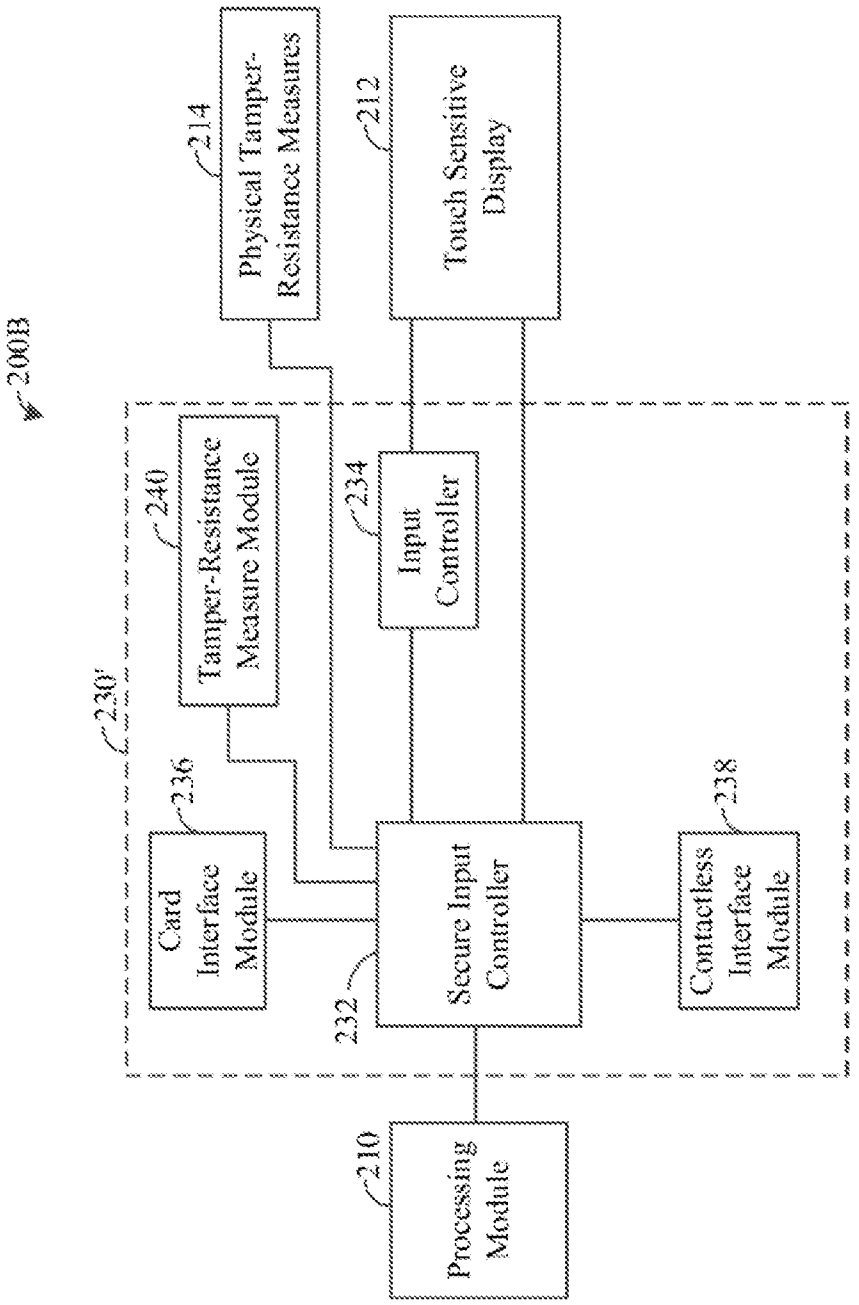
200B
230'
Processing Module
210
Secure Input Controller
232
Card Interface Module
236
Tamper-Resistance Measure Module
240
Input Controller
234
Contactless Interface Module
238
Physical Tamper-Resistance Measures
214
Touch Sensitive Display
212

FIG. 2B

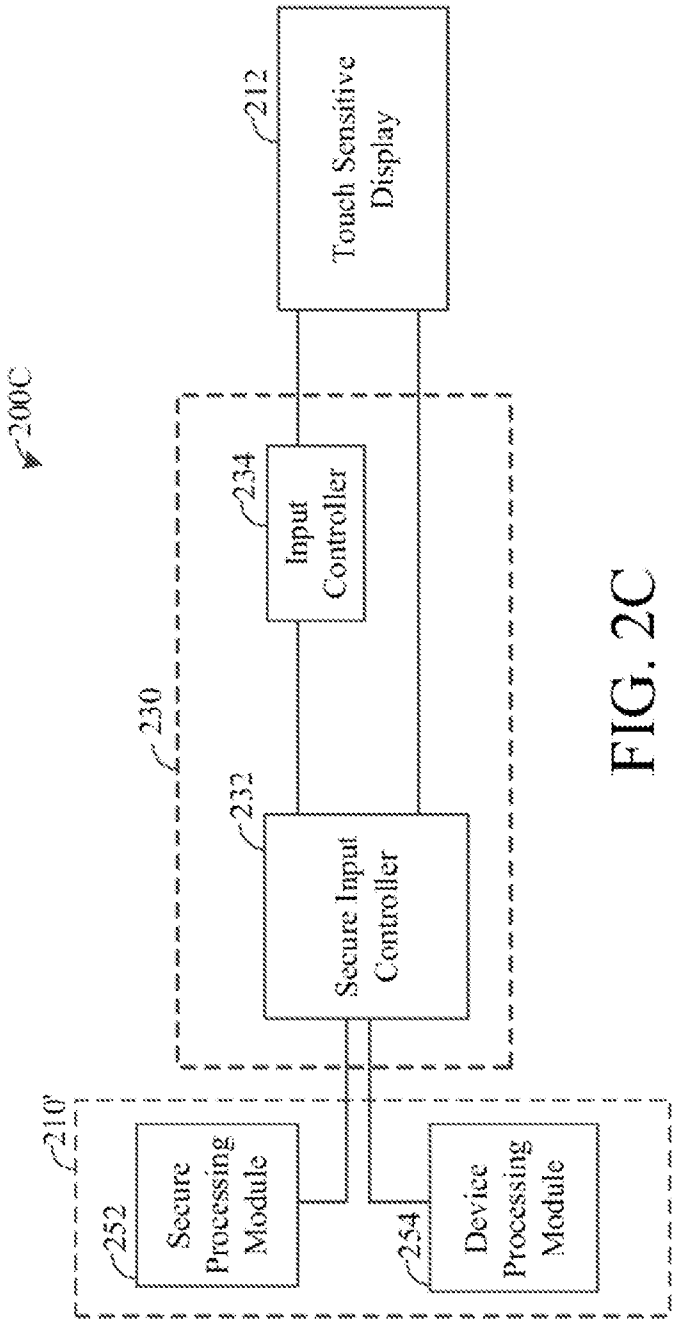
200C
212
Touch Sensitive Display
234
Input Controller
230
232
Secure Input Controller
210'
252
Secure Processing Module
254
Device Processing Module

FIG. 2C

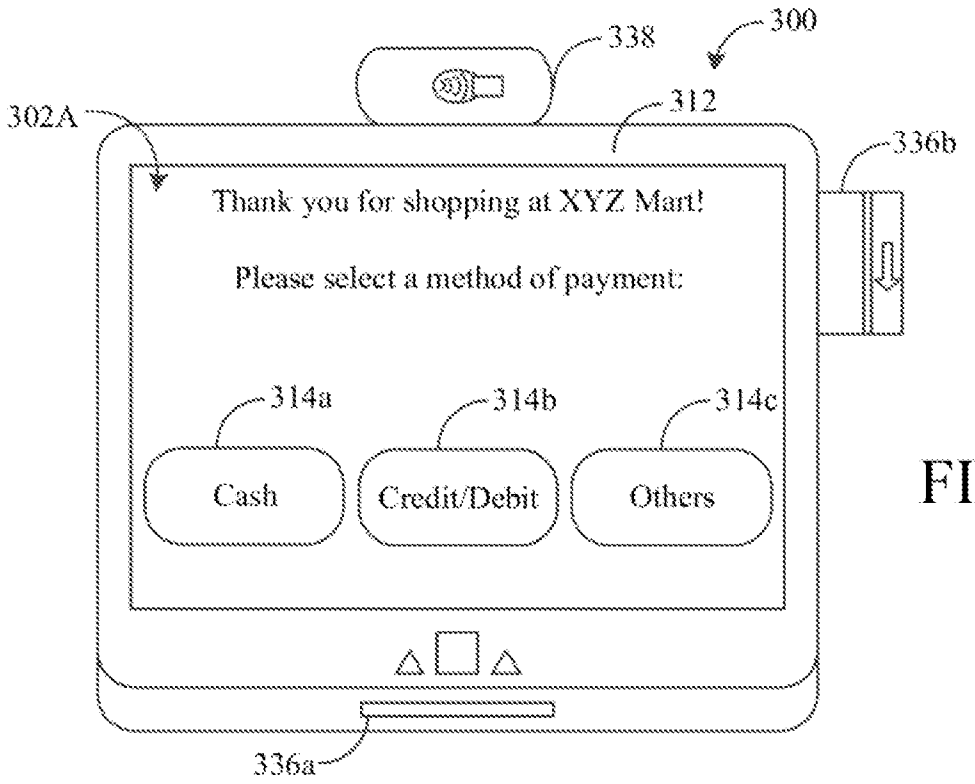
338
300
312
302A
336b
Thank you for shopping at XYZ Mart!
Please select a method of payment:
314a
314b
314c
Cash
Credit/Debit
Others
336a

FIG. 3A

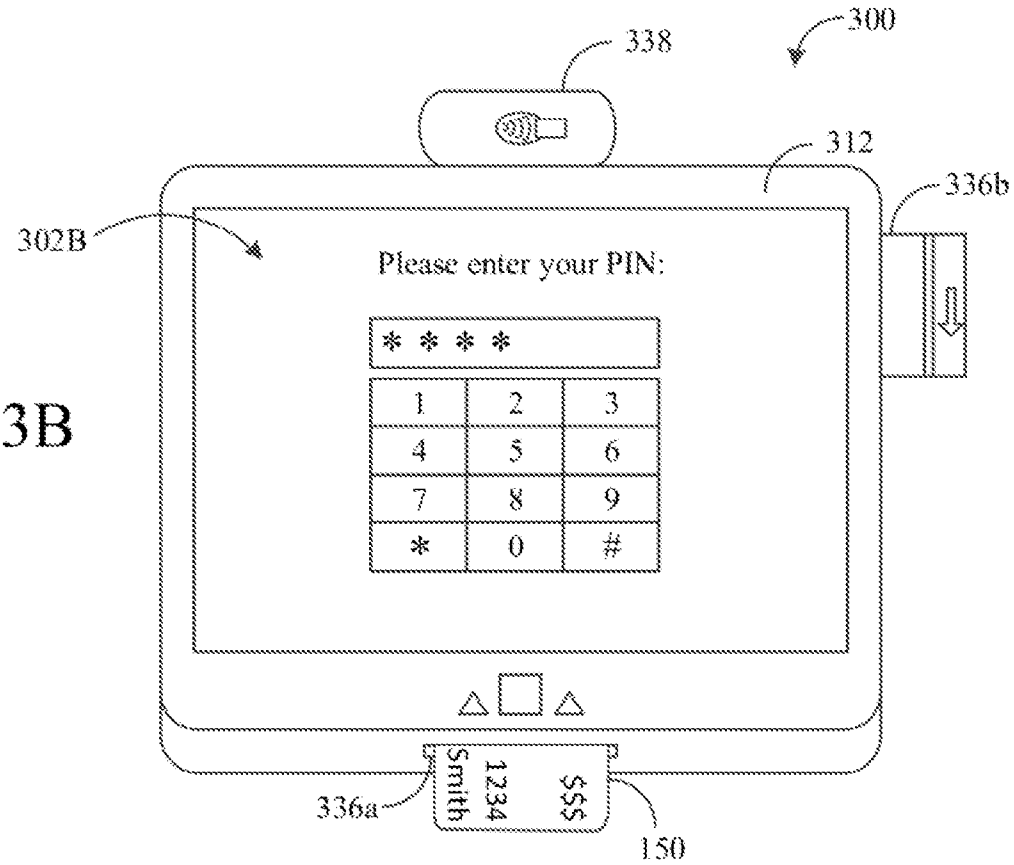
338
300
312
336b
302B
Please enter your PIN:
* * * *
1 2 3
4 5 6
7 8 9
* 0 #
336a
Smith 1234 $$$
150

FIG. 3B


338
300
312
402A
336b
Thank you for shopping at XYZ Mart!
Would you like to do the following:
414a
Join our loyalty program
414b
Enter a contest to WIN!
336a

FIG. 4A

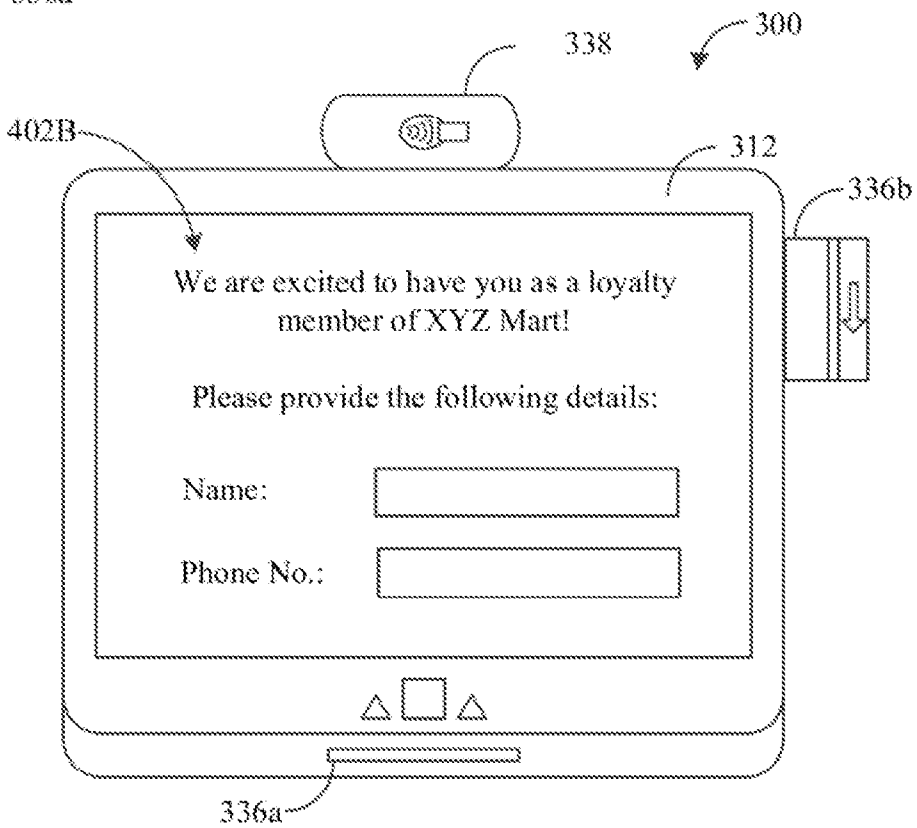
338
300
402B
312
336b
We are excited to have you as a loyalty member of XYZ Mart!
Please provide the following details:
Name:
Phone No.:
336a

FIG. 4B

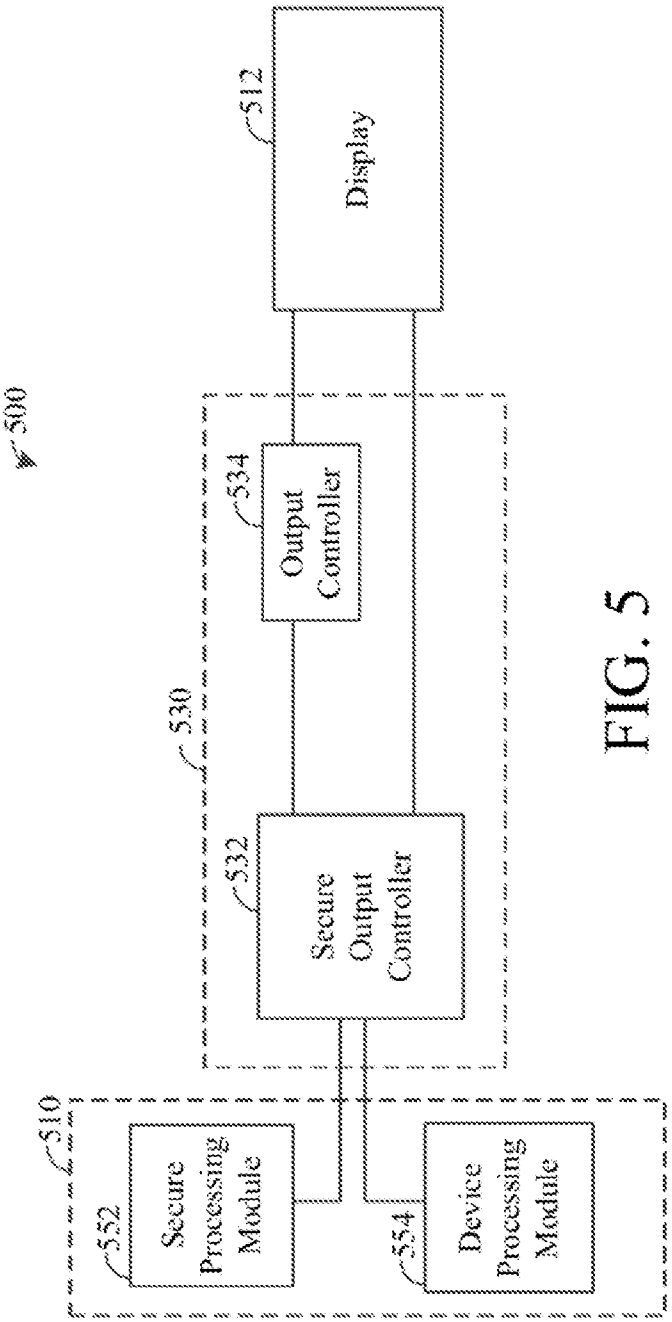
500
512
Display
534
Output Controller
530
532
Secure Output Controller
510
552
Secure Processing Module
554
Device Processing Module

FIG. 5

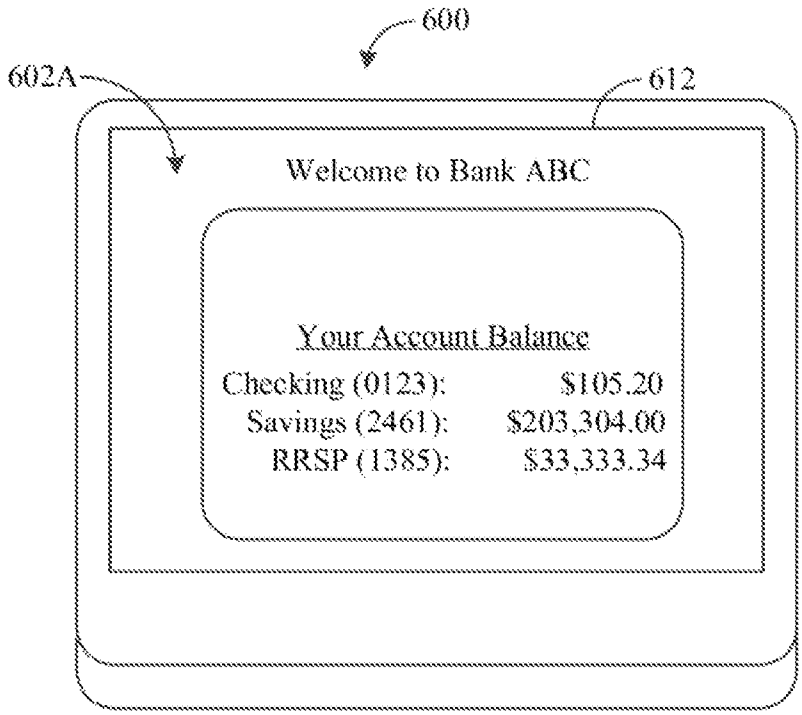
600
602A
612
Welcome to Bank ABC
Your Account Balance
Checking (0123): $105.20
Savings (2461): $203,304.00
RRSP (1385): $33,333.34

FIG. 6A

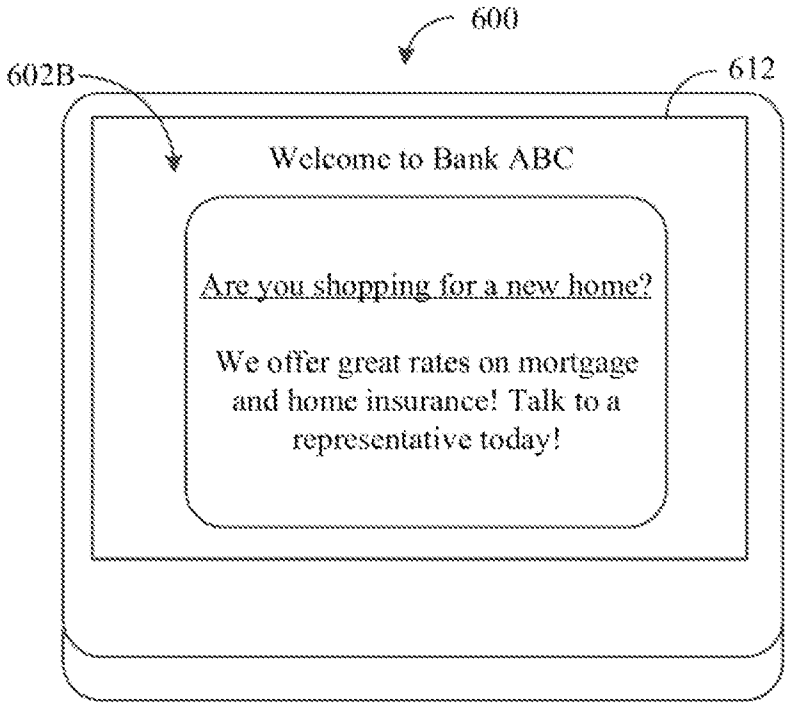
600
602B
612
Welcome to Bank ABC
Are you shopping for a new home?
We offer great rates on mortgage and home insurance! Talk to a representative today!

FIG. 6B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 15/40819

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 20/00 (2015.01)
CPC - G06Q20/20, G07G1/12, G06Q30/06, G06Q30/02, G06Q20/204
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8): G06Q 20/00 (2015.01); CPC: G06Q20/20, G07G1/12, G06Q30/06, G06Q30/02, G06Q20/204

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 705/16, 705/64, 713/150, 345/173

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, ProQuest Dialog, Google Web, Google Patents (Search terms: point of sale, POS, touch screen, contactless, wireless, reader, scanner, encrypt, cryptography, secure mode, unsecure, insecure, non-secure, select, choose, choice, tamper resistant, prevent, avoid, signal, mesh, switch, etc.)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/0097249 A1 (Gomez et al.) 10 April 2014 (10.04.2014), para. [0054], [0084]-[0092], [0099], [0102]-[0104], [0121]-[0124], [0136], [0148]-[0150], [0155]-[0159], [0177], [0199]-[0200], [0229], [0233]-[0234], [0239]-[0240], [0258]-[0260], [0266]-[0270], and [0272]-[0273], and Figs. 1a, 2a, 2e, 2h, 3a, 4a, 4L, 7d-7g, and 10c.	1-20
A	US 7,597,250 B2 (Finn) 06 October 2009 (06.10.2009) (entire document).	1-20
A	US 8,558,685 B2 (Long et al.) 15 October 2013 (15.10.2013) (entire document).	1-20
A	US 2013/0198086 A1 (Mardikar) 01 August 2013 (01.08.2013) (entire document).	1-20

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 September 2015 (14.09.2015)	13 OCT 2015
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)