



(22) Date de dépôt/Filing Date: 2012/10/30

(41) Mise à la disp. pub./Open to Public Insp.: 2013/05/01

(45) Date de délivrance/Issue Date: 2016/04/12

(30) Priorité/Priority: 2011/11/01 (EP11187362.6)

(51) Cl.Int./Int.Cl. *G06F 21/31* (2013.01),
G06F 21/36 (2013.01), *G06F 9/445* (2006.01),
H04L 9/32 (2006.01), *H04W 12/06* (2009.01)

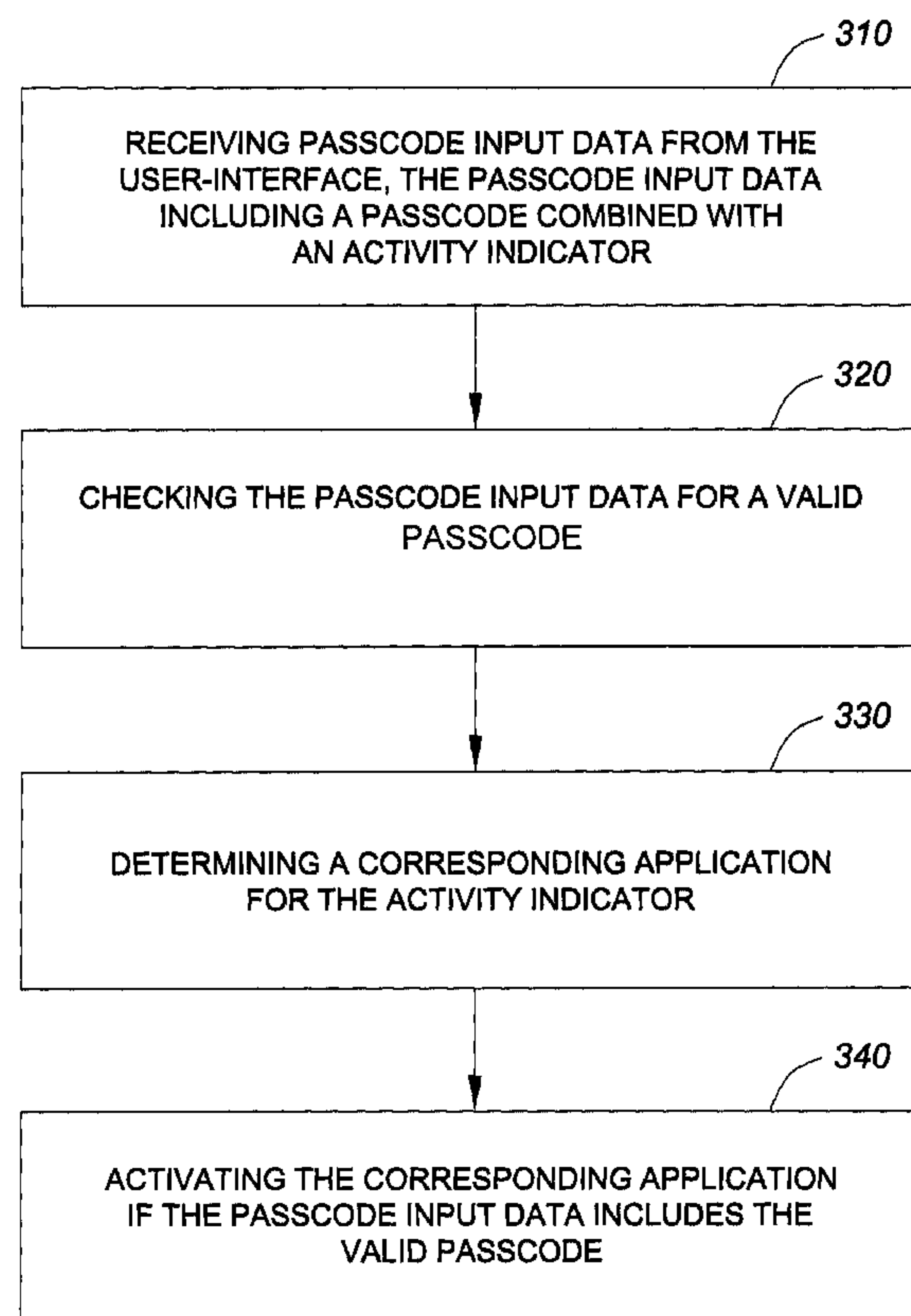
(72) Inventeurs/Inventors:
GRIFFIN, JASON TYLER, CA;
HAMILTON, ALISTAIR ROBERT, CA

(73) Propriétaire/Owner:
BLACKBERRY LIMITED, CA

(74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : COMBINAISON DE MOT DE PASSE ET DE MODIFICATEUR DE LANCEMENT D'ACTIVITE

(54) Title: COMBINED PASSCODE AND ACTIVITY LAUNCH MODIFIER



(57) Abrégé/Abstract:

A method and system are disclosed whereby an activity launch modifier is combined with a passcode. The activity launch modifier is used to determine a portion of an application to activate upon valid authentication.

ABSTRACT

A method and system are disclosed whereby an activity launch modifier is combined with a passcode. The activity launch modifier is used to determine a portion of an application to activate upon valid authentication.

COMBINED PASSCODE AND ACTIVITY LAUNCH MODIFIER**TECHNICAL FIELD**

5 The present disclosure relates generally to methods and systems for unlocking electronic devices.

BACKGROUND

10 Passwords may be used in many situations to authenticate a user before using a portion of an electronic device. Situations requiring authentication may include the ability to access or use a computer, mobile phone, tablet device, PDA (Personal Digital Assistant), or any other device. Authentication may also enable access to a physical location, or allow use of a credit/debit card or similar instrument. Passwords are typically alpha-numeric strings or sequences entered on a keyboard. However, with the advent of touch sensitive input
15 devices, graphical authentication systems are also available. For example, a user may have to align icons on a display or touch certain images in a particular order in order to authenticate.

There are many actions that users repeat frequently on their devices, such as macros within an application. Likewise, there are other actions that are not
20 used commonly due to the amount of time or effort to access the actions. Examples of actions repeated frequently include entering a BBM (Blackberry Messenger™) conversation with a particular person, checking a particular website, making a phone call and sending an email. Examples of actions that may not be used as frequently as desired due to the time or effort involved
25 might include taking a picture, recording a voice note and opening a document stored on the electronic device. Today these actions can be tedious because of the traditional access steps of unlock/wakeup, enter password, open application, and activate the action within the application.

Providing shortcuts for specific actions outside of a password is known. However shortcuts can create security holes. By giving access to an application outside a security screen there is a risk that the devices data can be accessed or unlocked through the application. In some situations,

5 shortcuts can create a very limited set of actions where the user is not able to access any data on the device. For example, a shortcut might allow the user to take a picture but not for communicate with someone over BBM.

There are examples of devices that provide access to a limited set of functions outside of a password. For example, on some smart phones, you

10 can answer a phone call without entering a password.

SUMMARY

In one aspect, there is provided a method of activating an application on an electronic device comprising: receiving passcode input data from a user-interface, the passcode input data including a passcode combined with an

15 activity launch modifier; checking the passcode input data for a valid passcode; determining a corresponding application for the activity launch modifier; and activating the corresponding application if the passcode input data includes the valid passcode.

In an embodiment, activating the corresponding application comprises

20 activating a portion of the application corresponding to the activity launch modifier.

In an embodiment, activating the corresponding application comprises implementing an action within the application corresponding to the activity launch modifier.

25 In an embodiment, checking for the valid passcode comprises determining if the valid passcode appears anywhere in the passcode input data.

In an embodiment, the passcode input data comprises a character string and checking for the valid passcode comprises determining if the valid passcode appears starting at the beginning of the character string.

In an embodiment, checking for the activity launch modifier comprises determining if an additional character appears in the character string after the valid passcode.

- 5 In an embodiment, the passcode input data comprises a character string and checking for the valid passcode comprises determining if the valid passcode appears at the end of the character string.

In an embodiment, checking for the activity launch modifier comprises determining if an additional character appears in the character string before the valid passcode.

- 10 In an embodiment, the valid passcode is a graphical authentication passcode and the activity launch modifier is a gesture.

In an embodiment, the valid passcode requires alignment on a display of a first reference point on an overlay image with a second reference point on a base image and the activity launch modifier is a gesture.

- 15 In an embodiment, the valid passcode requires alignment on a display of a first reference point on an overlay image with a second reference point on a base image and the activity launch modifier is a manner of aligning the first reference point and the second reference point.

- 20 In an embodiment, the activity launch modifier is a selectable modifier displayed on a display.

In an embodiment, the activity launch modifier is a colour of at least a portion of a display.

- 25 In a second aspect, there is provide a computer readable medium having computer readable instructions stored thereon that when implemented cause a processor to implement a method of activating an application on an electronic device, the comprising: receiving passcode input data from a user-interface, the passcode input data including a passcode combined with an activity launch modifier; checking the passcode input data for a valid passcode; determining a corresponding application for the activity launch

modifier; and activating the corresponding application if the passcode input data includes the valid passcode.

In an embodiment, the valid passcode is a graphical authentication passcode and the activity launch modifier is a gesture.

- 5 In an embodiment, the valid passcode requires alignment on a display of a first reference point on an overlay image with a second reference point on a base image and the activity launch modifier is a gesture.

- In an embodiment, the valid passcode requires alignment on a display of a first reference point on an overlay image with a second reference point on a
10 base image and the activity launch modifier is a manner of aligning the first reference point and the second reference point.

- In a third aspect, there is provide an electronic system comprising: a processor; an input interface; a memory having computer readable instruction stored thereon that when executed cause the processor to
15 implement a method of activating an application comprising: receiving passcode input data from the user-interface, the passcode input data including a passcode combined with an activity launch modifier; checking the passcode input data for a valid passcode; determining a corresponding application for the activity launch modifier; and activating the corresponding
20 application if the passcode input data includes the valid passcode.

In an embodiment, the input interface is a touch screen display.

In an embodiment, the at least a portion of the electronic system is a mobile electronic device.

BRIEF DESCRIPTION OF THE DRAWINGS

- 25 Figure 1 is a block diagram illustrating a communication system including a mobile communication device in which example embodiments of the present disclosure can be applied;

Figure 2 is a block diagram illustrating a mobile communication device in accordance with one example embodiment of the present disclosure;

Figure 3 is a flowchart of a method in accordance with one example embodiment of the present disclosure; and

Figure 4 is a block diagram of a system in accordance with one example embodiment of the present disclosure.

- 5 Like reference numerals are used in the drawings to denote like elements and features.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS

Typically, authentication systems restrict access by requiring a user to authenticate before permitting access to a system or application. Some
 10 systems require a user to re-authenticate after a period of time. The present application combines a password/unlock action with a shortcut command to a specific action/macro. Examples of password/unlock are Clixel™, entering a code on a number pad (virtual or real), entering a password on a qwerty keyboard (virtual or real), and gesture passwords.
 15 Clixel™ is a graphical authentication system in which a point from an overlay image must be aligned with a point on a base image in order to authenticate. In embodiments described herein, a modifier or activity launch modifier is combined with the password/unlock process to trigger a macro/shortcut that is defined for an action the user wants to take. For
 20 example, if the user's password is "qwerty" he or she can access the device in a traditional way by typing "qwerty" then enter. If the user wants to take a voice note immediately, the authentication process might be set up so that the user can type "qwertyv" then enter and the voice note application will automatically open. If the user wants to be placed in a BBM conversation
 25 with his wife, for example, the system might be set up so that "qwertyw" can be input followed by enter and the BBM conversation will automatically be started. For a Clixel™ example where you are moving an element (number or symbol) to a target, the modifier might be in how you get it there, for example, the modifier could be moving the element in clearly
 30 clockwise or counter clockwise directions, or possibly using multi-touch to move the element. For example, the relative location of two fingers on a touch screen might be the modifier to allow for different commands. In a

numerical pass code, the first or last number can be used as a modifier to provide different commands. In this case the security level is decreased because one digit is used as the activity launch modifier. However, in some cases this decrease in security might be an acceptable trade-off for the convenience. In a pass code or password a gesture on the final letter/number might provide the modifier. In other embodiments, a fingerprint scanner might be set up so the direction in which a finger is scanned is the modifier.

In some embodiments, the modifier is indicative of an activity for which a shortcut is created. One or more activity launch modifiers or modifiers can be factory preset in some embodiments. Alternatively or in addition to factory preset activity launch modifiers, some embodiments allow for users to set user-defined activity launch modifiers. In other words, users can create customize activity launch modifiers to combine with a passcode to create shortcuts to applications, portions of applications or actions within applications.

Non-limiting examples of a passcode include a password, an unlock code and a graphical authentication process. The passcode can be for operating or accessing at least a portion of the electronic device.

Reference is first made to FIG. 1 which shows in block diagram of a communication system 100 in which example embodiments of the present disclosure can be applied. The communication system 100 comprises a number of mobile electronic devices 201 which may be connected to the remainder of system 100 in any of several different ways. Accordingly, several instances of mobile electronic devices 201 are depicted in FIG. 1 employing different example ways of connecting to system 100. Mobile electronic devices 201 are connected to a wireless communication network 101 which may comprise one or more of a Wireless Wide Area Network (WWAN) 102 and a Wireless Local Area Network (WLAN) 104 or other suitable network arrangements. In some embodiments, the mobile electronic devices 201 are configured to communicate over both the WWAN 102 and WLAN 104, and to roam between these networks. In some embodiments, the wireless network 101 may comprise multiple WWANs 102

and WLANs 104.

The WWAN 102 may be implemented as any suitable wireless access network technology. By way of example, but not limitation, the WWAN 102 may be implemented as a wireless network that includes a number of
5 transceiver base stations 108 (one of which is shown in FIG. 1) where each of the base stations 108 provides wireless Radio Frequency (RF) coverage to a corresponding area or cell. The WWAN 102 is typically operated by a mobile network service provider that provides subscription packages to users of the mobile electronic devices 201. In some embodiments, the
10 WWAN 102 conforms to one or more of the following wireless network types: Mobitex Radio Network, DataTAC, GSM (Global System for Mobile Communication), GPRS (General Packet Radio System), TDMA (Time Division Multiple Access), CDMA (Code Division Multiple Access), CDPD (Cellular Digital Packet Data), iDEN (Integrated Digital Enhanced Network),
15 EvDO (Evolution-Data Optimized) CDMA2000, EDGE (Enhanced Data rates for GSM Evolution), UMTS (Universal Mobile Telecommunication Systems), HSDPA (High-Speed Downlink Packet Access), IEEE 802.16e (also referred to as Worldwide Interoperability for Microwave Access or "WiMAX), or various other networks. Although WWAN 102 is described as a "Wide-Area"
20 network, that term is intended herein also to incorporate wireless Metropolitan Area Networks (WMAN) and other similar technologies for providing coordinated service wirelessly over an area larger than that covered by typical WLANs.

The WWAN 102 may further comprise a wireless network gateway 110
25 which connects the mobile electronic devices 201 to transport facilities 112, and through the transport facilities 112 to a wireless connector system 120. Transport facilities may include one or more private networks or lines, the public internet, a virtual private network, or any other suitable network. The wireless connector system 120 may be operated, for example, by an
30 organization or enterprise such as a corporation, university, or governmental department, which allows access to a network 124 such as an internal or enterprise network and its resources, or the wireless connector system 120, may be operated by a mobile network provider. In some

embodiments, the network 124 may be realised using the internet rather than an internal or enterprise network.

The wireless network gateway 110 provides an interface between the wireless connector system 120 and the WWAN 102, which facilitates communication between the mobile electronic devices 201 and other devices (not shown) connected, directly or indirectly, to the WWAN 102.

Accordingly, communications sent via the mobile electronic devices 201 are transported via the WWAN 102 and the wireless network gateway 110 through transport facilities 112 to the wireless connector system 120.

Communications sent from the wireless connector system 120 are received by the wireless network gateway 110 and transported via the WWAN 102 to the mobile electronic devices 201.

The WLAN 104 comprises a wireless network which, in some embodiments, conforms to IEEE 802.11x standards (sometimes referred to as Wi-Fi) such as, for example, the IEEE 802.11a, 802.11b and/or 802.11g standard. Other communication protocols may be used for the WLAN 104 in other embodiments such as, for example, IEEE 802.11n, IEEE 802.16e (also referred to as Worldwide Interoperability for Microwave Access or "WiMAX"), or IEEE 802.20 (also referred to as Mobile Wireless Broadband Access). The WLAN 104 includes one or more wireless RF Access Points (AP) 114 (one of which is shown in FIG. 1) that collectively provide a WLAN coverage area.

The WLAN 104 may be a personal network of the user, an enterprise network, or a hotspot offered by an internet service provider (ISP), a mobile network provider, or a property owner in a public or semi-public area, for example. The access points 114 are connected to an access point (AP) interface 116 which may connect to the wireless connector system 120 directly (for example, if the access point 114 is part of an enterprise WLAN 104 in which the wireless connector system 120 resides), or indirectly via the transport facilities 112 if the access point 14 is a personal Wi-Fi network or Wi-Fi hotspot (in which case a mechanism for securely connecting to the wireless connector system 120, such as a virtual private network (VPN), may be appropriate). The AP interface 116 provides translation and routing services between the access points 114 and the wireless connector system

120 to facilitate communication, directly or indirectly, with the wireless connector system 120.

The wireless connector system 120 may be implemented as one or more servers, and is typically located behind a firewall 113. The wireless
5 connector system 120 manages communications, including email messages, to and from a set of managed mobile electronic devices 201. The wireless connector system 120 also provides administrative control and management capabilities over users and mobile electronic devices 201 which may connect to the wireless connector system 120.

10 The wireless connector system 120 allows the mobile electronic devices 201 to access the network 124 and connected resources and services such as a messaging server 132 (for example, a Microsoft Exchange™, IBM Lotus Domino™, or Novell GroupWise™ email messaging server) having a global address book 134, and optionally other servers 142. The other servers 142
15 may comprise a content server for providing content such as internet content or content from an organization's internal servers to the mobile electronic devices 201 in the wireless network 101, an authentication server and an application server for implementing server-based applications.

The global address book 134 comprises electronic contact records generated
20 and maintained by an IT (information technology) administrator of the network 124. Typically, the global address book is maintained exclusively by the messaging server 132 and there is no local copy on the mobile electronic device 201. In addition, the global address book typically comprises contact records for all users of the respective network 124 (e.g.,
25 enterprise). The contact records in the global address book 134 may be one or more of individual contact records (or user records) or a group address or distribution list which lists multiple individual (users).

The wireless connector system 120 typically provides a secure exchange of data (e.g., email messages, personal information manager (PIM) data, and
30 IM data) with the mobile electronic devices 201. In some embodiments, communications between the wireless connector system 120 and the mobile electronic devices 201 are encrypted. In some embodiments,

communications are encrypted using a symmetric encryption key implemented using Advanced Encryption Standard (AES) or Triple Data Encryption Standard (Triple DES) encryption. Private encryption keys are generated in a secure, two-way authenticated environment and are used for
5 both encryption and decryption of data.

The wireless network gateway 110 is adapted to send data packets received from the mobile electronic device 201 over the WWAN 102 to the wireless connector system 120. The wireless connector system 120 then sends the data packets to the appropriate connection point such as the messaging
10 server 132, other servers 142 or application servers 136. Conversely, the wireless connector system 120 sends data packets received, for example, from the messaging server 132 or other servers 142 to the wireless network gateway 110 which then transmit the data packets to the destination mobile electronic device 201. The AP interfaces 116 of the WLAN 104 provide
15 similar sending functions between the mobile electronic device 201, the wireless connector system 120 and network connection point such as the messaging server 132, other servers 142 and application server 136.

The network 124 may comprise a private local area network, metropolitan area network, wide area network, the public internet or combinations
20 thereof and may include virtual networks constructed using any of these, alone, or in combination. Computers 117 may be connected to the network 124 directly or indirectly via an intermediate communication network such as the Internet 112. When computers 117 connect to the network indirectly, e.g. via the Internet 112, a VPN or other mechanism for securely
25 connecting to the network 124 may be appropriate. Computers 117 may be of any suitable construction and include at least a processor, and a display screen, one or more user input devices, and a memory each connected to the processor as is known in the art. The computers 117 could be desktop computers, laptop/notebook/netbook computers, or combinations thereof,
30 and may have wired or wireless communication subsystems for connecting to the network 124.

A mobile electronic device 201 may alternatively connect to the wireless connector system 120 using a computer 117 via the network 124. In at

least some embodiments, for security purposes the computers 117 with which the mobile electronic devices 201 can connect to the wireless connector system 120 are limited to computers 117 which are directly connected to the network 124. A link 106 may be provided for exchanging
5 information between the mobile electronic device 201 and computer 117 connected to the wireless connector system 120. The link 106 may comprise one or both of a physical interface and short-range wireless communication interface. The physical interface may comprise one or combinations of an Ethernet connection, Universal Serial Bus (USB)
10 connection, Firewire™ (also known as an IEEE 1394 interface) connection, or other serial data connection, via respective ports or interfaces of the mobile electronic device 201 and computer 117. The short-range wireless communication interface may be a personal area network (PAN) interface. A personal area network is a wireless point-to-point connection meaning no
15 physical cables are required to connect the two end points.

It will be appreciated that the above-described communication system is provided for the purpose of illustration only, and that the above-described communication system comprises one possible communication network configuration of a multitude of possible configurations for use with the
20 mobile electronic devices 201. The teachings of the present disclosure may be employed in connection with any other type of network and associated devices that are effective in implementing or facilitating wireless communication. Suitable variations of the communication system will be understood to a person of skill in the art and are intended to fall within the
25 scope of the present disclosure.

Reference is now made to FIG. 2 which illustrates an exemplary embodiment of the mobile electronic device 201 in which example embodiments described in the present disclosure can be applied. The mobile electronic device 201 is a two-way communication device having
30 data and voice communication capabilities, and the capability to communicate with other computer systems, for example, via the Internet. Depending on the functionality provided by the mobile electronic device 201, in various embodiments the mobile electronic device 201 may be a multiple-

mode communication device configured for both data and voice communication, a smartphone, a mobile telephone or a PDA (personal digital assistant) enabled for wireless communication, a tablet device or a computer system with a wireless modem.

5 The mobile electronic device 201 includes a rigid case (not shown) housing the components of the mobile electronic device 201. The internal components of the mobile electronic device 201 are constructed on a printed circuit board (PCB). The mobile electronic device 201 includes a controller comprising at least one processor 240 (such as a microprocessor) which
10 controls the overall operation of the mobile electronic device 201. The processor 240 interacts with device subsystems such as a wireless communication subsystem 211 (sometimes referred to as a radio layer) for exchanging radio frequency signals with the wireless network 101 to perform communication functions. The processor 240 interacts with
15 additional device subsystems including a display screen 204 such as a liquid crystal display (LCD) screen and a touchscreen, input devices 206 such as a keyboard, a touchpad, a fingerprint sensor and control buttons, flash memory 244, random access memory (RAM) 246, read only memory (ROM) 248, auxiliary input/output (I/O) subsystems 250, data port 252 such as
20 serial data port, such as a Universal Serial Bus (USB) data port, speaker 256, microphone 258, short-range communication subsystem 262, and other device subsystems generally designated as 264. Some of the subsystems shown in FIG. 2 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions.

25 The mobile electronic device 201 may comprise a touch screen display in some embodiments. The touch screen display may be constructed using a touch-sensitive input surface connected to an electronic controller and which overlays the display screen 204. The touch-sensitive overlay and the electronic controller provide a touch-sensitive input device and the processor
30 240 interacts with the touch-sensitive overlay via the electronic controller. In some embodiments, a touch screen is integrated directly with the display. In still other embodiments, a touch screen is placed behind the display.

The communication subsystem 211 includes a receiver 214, a transmitter 216, and associated components, such as one or more antenna elements 218 and 220, local oscillators (LOs) 222, and a processing module such as a digital signal processor (DSP) 224. The antenna elements 218 and 220 may
5 be embedded or internal to the mobile electronic device 201 and a single antenna may be shared by both receiver and transmitter, as is known in the art. As will be apparent to those skilled in the field of communication, the particular design of the wireless communication subsystem 211 depends on the wireless network 101 in which mobile electronic device 201 is intended
10 to operate.

The mobile electronic device 201 may communicate with any one of a plurality of fixed transceiver base stations 108 of the wireless network 101 within its geographic coverage area. The mobile electronic device 201 may send and receive communication signals over the wireless network 101 after
15 the required network registration or activation procedures have been completed. Signals received by the antenna 218 through the wireless network 101 are input to the receiver 214, which may perform such common receiver functions as signal amplification, frequency down conversion, filtering, channel selection, etc., as well as analog-to-digital
20 (A/D) conversion. A/D conversion of a received signal allows more complex communication functions such as demodulation and decoding to be performed in the DSP 224. In a similar manner, signals to be transmitted are processed, including modulation and encoding, for example, by the DSP 224. These DSP-processed signals are output to the transmitter 216 for
25 digital-to-analog (D/A) conversion, frequency up conversion, filtering, amplification, and transmission to the wireless network 101 via the antenna 220. The DSP 224 not only processes communication signals, but may also provide for receiver and transmitter control. For example, the gains applied to communication signals in the receiver 214 and the transmitter 216 may
30 be adaptively controlled through automatic gain control algorithms implemented in the DSP 224.

The processor 240 operates under stored program control and executes software modules 221 stored in memory such as persistent memory, for

example, in the flash memory 244. As illustrated in FIG. 2, the software modules 221 comprise operating system software 223, software applications 225 comprising an email messaging application 272 (also referred to as an email client 272), a personal address book 274, a calendar application 276, a phone application 278, and an authentication module 280. The authentication module 280 includes instructions for implementing any of the methods described herein. It is recognized that the authentication module 280 and its various components as described herein can form a discrete module running on the mobile electronic device 201, or the functions of the authentication module 280 can be distributed on the mobile electronic device 201 as separate modules or integrated within other existing modules as desired. Such discrete or distributed implementations all fall within the embodiments of the authentication module 280 as described herein.

The software applications 225 also may include a range of applications, including, for example, a notepad application, Internet browser application, voice communication (i.e. telephony) application, mapping application, or a media player application, or any combination thereof. Each of the software applications 225 may include layout information defining the placement of particular fields and graphic elements (e.g. text fields, input fields, icons, etc.) in the user interface (i.e. the display screen 204) according to the application.

Those skilled in the art will appreciate that the software modules 221 or parts thereof may be temporarily loaded into volatile memory such as the RAM 246. The RAM 246 is used for storing runtime data variables and other types of data or information, as will be apparent to those skilled in the art. Although specific functions are described for various types of memory, this is merely one example, and those skilled in the art will appreciate that a different assignment of functions to types of memory could also be used.

In some embodiments, the auxiliary I/O subsystems 250 may comprise an external communication link or interface, for example, an Ethernet connection. The mobile electronic device 201 may comprise other wireless communication interfaces for communicating with other types of wireless networks, for example, a wireless network such as an orthogonal frequency

division multiplexed (OFDM) network or a GPS (Global Positioning System) subsystem comprising a GPS receiver or transceiver for communicating with a GPS satellite network (not shown). The auxiliary I/O subsystems 250 may comprise a pointing or navigational input device such as a touchpad, a
5 clickable trackball or scroll wheel or thumbwheel, or a vibrator for providing vibratory notifications in response to various events on the mobile electronic device 201 such as receipt of an electronic message or incoming phone call, or for other purposes such as haptic feedback (touch feedback).

In some embodiments, the mobile electronic device 201 also includes a
10 removable memory card or module 230 (typically comprising flash memory) and a memory card interface 232. Network access is typically associated with a subscriber or user of the mobile electronic device 201 via the memory card 230, which may be a Subscriber Identity Module (SIM) card for use in a GSM network or other type of memory card for use in the relevant wireless
15 network type. The memory card 230 is inserted in or connected to the memory card interface 232 of the mobile electronic device 201 in order to operate in conjunction with the wireless network 101.

The mobile electronic device 201 also stores other data 227 in an erasable persistent memory, which in one example embodiment is the flash memory
20 244. In various embodiments, the data 227 includes service data comprising information required by the mobile electronic device 201 to establish and maintain communication with the wireless network 101. The data 227 may also include user application data such as email messages, address book and contact information, calendar and schedule information,
25 notepad documents, image files, and other commonly stored user information stored on the mobile electronic device 201 by its user, and other data. The data 227 stored in the persistent memory (e.g. flash memory 244) of the mobile electronic device 201 may be organized, at least
30 partially, into a number of databases each containing data items of the same data type or associated with the same application. For example, email messages, contact records, and task items may be stored in individual databases within the device memory.

The mobile electronic device 201 also includes a battery 238 as a power source, which is typically one or more rechargeable batteries that may be charged, for example, through charging circuitry coupled to a battery interface such as the serial data port 252. The battery 238 provides
5 electrical power to at least some of the electrical circuitry in the mobile electronic device 201, and the battery interface 236 provides a mechanical and electrical connection for the battery 238. The battery interface 236 is coupled to a regulator (not shown) which provides power V+ to the circuitry of the mobile electronic device 201.

10 The short-range communication subsystem 262 is an additional optional component which provides for communication between the mobile electronic device 201 and different systems or devices, which need not necessarily be similar devices. For example, the subsystem 262 may include an infrared
15 compliant communication mechanism such as a Bluetooth® communication module to provide for communication with similarly-enabled systems and devices.

A predetermined set of applications that control basic device operations, including data and voice communication applications will normally be
20 installed on the mobile electronic device 201 during or after manufacture. Additional applications and/or upgrades to the operating system 221 or software applications 225 may also be loaded onto the mobile electronic device 201 through the wireless network 101, the auxiliary I/O subsystem 250, the serial port 252, the short-range communication subsystem 262, or
25 other suitable subsystem 264. The downloaded programs or code modules may be permanently installed, for example, written into the program memory (i.e. the flash memory 244), or written into and executed from the RAM 246 for execution by the processor 240 at runtime. Such flexibility in application installation increases the functionality of the mobile electronic
30 device 201 and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the mobile electronic device 201.

The mobile electronic device 201 may provide two principal modes of communication: a data communication mode and a voice communication mode. In the data communication mode, a received data signal such as a text message, an email message, or Web page download will be processed
5 by the communication subsystem 211 and input to the processor 240 for further processing. For example, a downloaded Web page may be further processed by a browser application or an email message may be processed by the email messaging application and output to the display 204. A user of the mobile electronic device 201 may also compose data items, such as
10 email messages, for example, using the input devices in conjunction with the display screen 204. These composed items may be transmitted through the communication subsystem 211 over the wireless network 101.

In the voice communication mode, the mobile electronic device 201 provides telephony functions and operates as a typical cellular phone. The overall
15 operation is similar, except that the received signals are output to the speaker 256 and signals for transmission are generated by a transducer such as the microphone 258. The telephony functions are provided by a combination of software/firmware (i.e., the phone application 278) and hardware (i.e., the microphone 258, the speaker 256 and input devices).
20 Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the mobile electronic device 201. Although voice or audio signal output is typically accomplished primarily through the speaker 256, the display screen 204 may also be used to provide an indication of the identity of a calling party, duration of a voice
25 call, or other voice call related information.

The phone application 278 can be split into multiple applications or sub-modules, for example one or more user phone modules and a call control module. The user phone modules provide a variety of telephony features through a user interface, while the call control module provides access to
30 common telephony functions desired by the user phone modules, such that telephony requests from phone modules can be coordinated and so that the user phone modules do not need to each provide instructions understood by the wireless communications subsystem 211. The call control function

typically makes telephony features available to user phone modules through an application programming interface (API). It is to be recognized that all or part of the phone application 278 features or functions could be provided through the operating system or otherwise distributed in the mobile
5 electronic device 201, while continuing to fall within the term phone application 278.

Referring now to Figure 3, a method of activating an application on an electronic device will be described. At action 310 the method starts with receiving passcode input data from a user-interface, the passcode input data
10 including a passcode combined with an activity launch modifier. Then at action 320, the method continues with checking the passcode input data for a valid passcode. The next action 330 is determining a corresponding application for the activity launch modifier. The method ends with action 340 which is activating the corresponding application if the passcode input
15 data includes the valid passcode.

In an embodiment, activating the corresponding application comprises activating a portion of the application corresponding to the activity launch modifier. Thus, activating the application in some cases is opening the application such that the user can navigate from a default start point in the
20 application. In other cases, a particular the application is opened to a particular subroutine or menu item. For example, if the corresponding application is an email application, a new compose email window can be opened. In an embodiment, activating the corresponding application comprises implementing an action within the application corresponding to
25 the activity launch modifier. Thus, in some embodiments, the corresponding application is instructed to perform a particular action. For example, if the application is a phone application, the action could be to dial a particular phone number. For the email application example previously given, the compose email window can have the addressee information filled out.
30 Another non-limiting example is for a map application whereby the action could be to find a current location.

In some embodiments, checking for the valid passcode comprises determining if the valid passcode appears anywhere in the passcode input data. Thus, in the case of an alphanumeric code, the valid passcode could appear anywhere in the character string: at the beginning, in the middle or
5 at the end. The passcode could feasibly comprise the entire passcode. In other words, there may be situations where no activity launch modifier is entered. Thus, where no activity launch modifier is found when checking for the activity launch modifier, entering a valid passcode can result in positive authentication with a default action, such as unlocking the electronic device.

10 In some embodiments, the passcode input data comprises a character string and checking for the valid passcode comprises determining if the valid passcode appears starting at the beginning of the character string. In some embodiments, checking for the activity launch modifier comprises determining if an additional character appears in the character string after
15 the valid passcode.

In some embodiments, the passcode input data comprises a character string and checking for the valid passcode comprises determining if the valid passcode appears at the end of the character string. In some embodiments, checking for the activity launch modifier comprises determining if an
20 additional character appears in the character string before the valid passcode.

In some embodiments, the valid passcode is a graphical authentication passcode and the activity launch modifier is a gesture. In some embodiments, such as the Clixel™ example given above, the valid passcode
25 requires alignment on a display of a first reference point on an overlay image with a second reference point on a base image. A gesture can be used as the activity launch modifier. In cases where a touch screen or a touch pad is used as an input interface, gestures are convenient activity launch modifiers.

30 In some embodiments where the valid passcode requires alignment on a display of a first reference point on an overlay image with a second

reference point on a base image, the activity launch modifier is a manner of aligning the first reference point and the second reference point.

In some embodiments, the activity launch modifier is a selectable modifier displayed on a display. For example, in some embodiments, instead of
5 hitting enter after entering a passcode, a user can select the modifier to go directly to an activity within an application.

In some embodiments, the user holds down a key or touches a touchscreen while one or more images changes on a display or portions of the display change. The changing images or portions of the display represent activity
10 launch modifiers. Releasing the key when a particular activity launch modifier is displayed will start the activity if the passcode is entered correctly. For example, in some embodiments, the activity launch modifier is a colour of at least a portion of a display. For example, at some point in entering a passcode, graphic or alpha-numeric, the user may hold down a
15 key or touch a touchscreen until the portion of the display turns the color associated with the action desired.

In some embodiments, the methods described herein are implemented by a processor. In one aspect, there is provided a computer readable medium having computer readable instructions stored thereon that when
20 implemented cause a processor to implement any of the methods described herein.

Referring now to Figure 4, an electronic system 400 will be described. The electronic system comprises a processor 410, an input interface 420 and a memory 430. The memory 430 has computer readable instruction stored
25 thereon that when executed cause the processor to implement a method of activating an application according to any of the embodiments described herein. In some embodiments, the input interface 420 is a touch screen display. Other non-limiting examples of the input interface include a keyboard, a touch pad, and a joystick. In some embodiments, at least a
30 portion of the electronic system 400 is a mobile electronic device, such as but not limited to the mobile electronic device 201 described with reference

to Figure 1. In some embodiments, the electronic system is one device. In some embodiments, the electronic system is composed of separate devices. For example, the input interface 420 and the memory 430 can be peripheral devices that are connectable to another device housing the processor 410.

While the present disclosure is sometimes described in terms of methods, a person of ordinary skill in the art will understand that the present disclosure is also directed to various apparatus including components for performing at least some of the aspects and features of the described methods, be it by way of hardware components, software or any combination of the two, or in any other manner. Moreover, an article of manufacture for use with the apparatus, such as a pre-recorded storage device or other similar computer readable medium including program instructions recorded thereon may direct an apparatus to facilitate the practice of the described methods. It is understood that such apparatus and articles of manufacture, also come within the scope of the present disclosure.

The various embodiments presented above are merely examples and are in no way meant to limit the scope of this disclosure. Variations of the innovations described herein will be apparent to persons of ordinary skill in the art, such variations being within the intended scope of the present application. In particular, features from one or more of the above-described embodiments may be selected to generate alternative embodiments comprised of a sub-combination of features which may not be explicitly described above. In addition, features from one or more of the above-described embodiments may be selected and combined to generate alternative embodiments comprised of a combination of features which may not be explicitly described above. Features suitable for such combinations and sub-combinations would be readily apparent to persons skilled in the art upon review of the present application as a whole.

CLAIMS:

1. A method of activating an application on an electronic device, the electronic device having stored thereon a valid passcode and a plurality of activity launch modifiers, the method comprising:

receiving at the electronic device passcode input data from a user-interface, the passcode input data including a passcode combined with one of the plurality of activity launch modifiers, the passcode and the one of the plurality of activity launch modifiers being received at the electronic device contemporaneously;

after receiving the passcode input data,

checking the passcode input data for the valid passcode;

determining a corresponding application for the activity launch modifier; and

activating the corresponding application if the passcode input data includes the valid passcode.

2. The method of claim 1, wherein activating the corresponding application comprises activating a portion of the application corresponding to the activity launch modifier.

3. The method of claim 1 or 2, wherein activating the corresponding application comprises implementing an action within the application corresponding to the activity launch modifier.

4. The method of any one of claims 1 to 3, wherein checking for the valid passcode comprises determining if the valid passcode appears anywhere in the passcode input data.

5. The method of any one of claims 1 to 4, wherein the passcode input data comprises a character string and checking for the valid passcode comprises

determining if the valid passcode appears starting at the beginning of the character string.

6. The method of claim 5, wherein determining a corresponding application for the activity launch modifier comprises determining if an additional character appears in the character string after the valid passcode.

7. The method of any one of claims 1 to 4, wherein the passcode input data comprises a character string and checking for the valid passcode comprises determining if the valid passcode appears at the end of the character string.

8. The method of claim 7, wherein determining a corresponding application for the activity launch modifier comprises determining if an additional character appears in the character string before the valid passcode.

9. The method of any one of claims 1 to 4, wherein the valid passcode is a graphical authentication passcode and the activity launch modifier is a gesture.

10. The method of any one of claim 1 to 4, wherein the valid passcode requires alignment on a display of a first reference point on an overlay image with a second reference point on a base image and the activity launch modifier is a gesture.

11. The method of any one of claims 1 to 4, wherein the valid passcode requires alignment on a display of a first reference point on an overlay image with a second reference point on a base image and the activity launch modifier is a manner of aligning the first reference point and the second reference point.

12. The method of any one of claims 1 to 4, wherein the activity launch modifier is a selectable modifier displayed on a display.

13. The method of any one of claims 1 to 4, wherein the activity launch modifier is a colour of at least a portion of a display.

14. A non-transitory machine readable medium having tangibly stored thereon executable instructions that, when executed by a processor of a handheld electronic

device, cause the handheld electronic device to perform the method of any one of claims 1 to 13.

15. An electronic device, comprising:

a processor;

an input interface coupled to the processor;

a memory coupled to the processor, the memory storing executable instructions that, when executed by the processor, cause the handheld electronic device to perform the method of any one of claims 1 to 13.

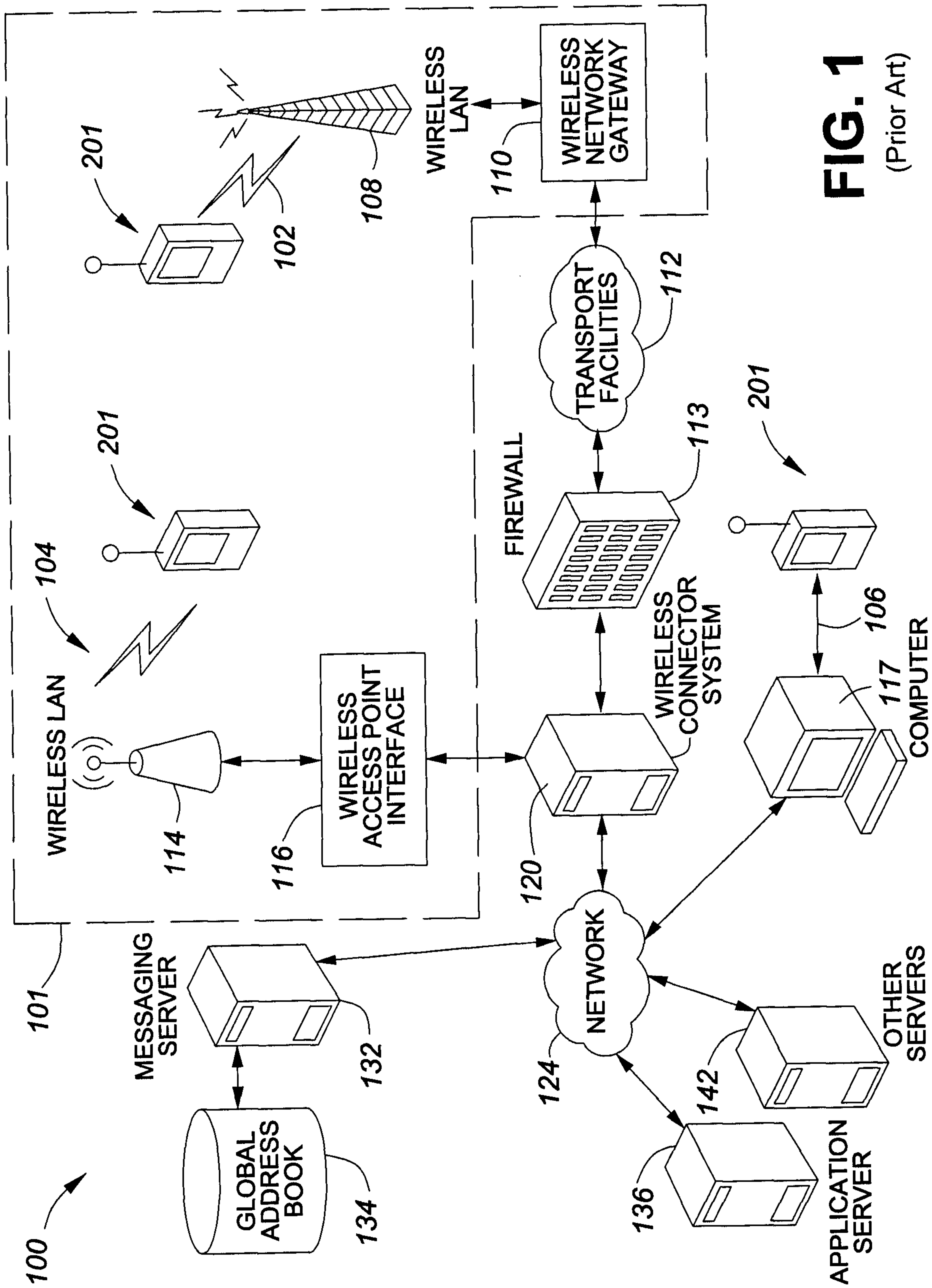


FIG. 1
(Prior Art)

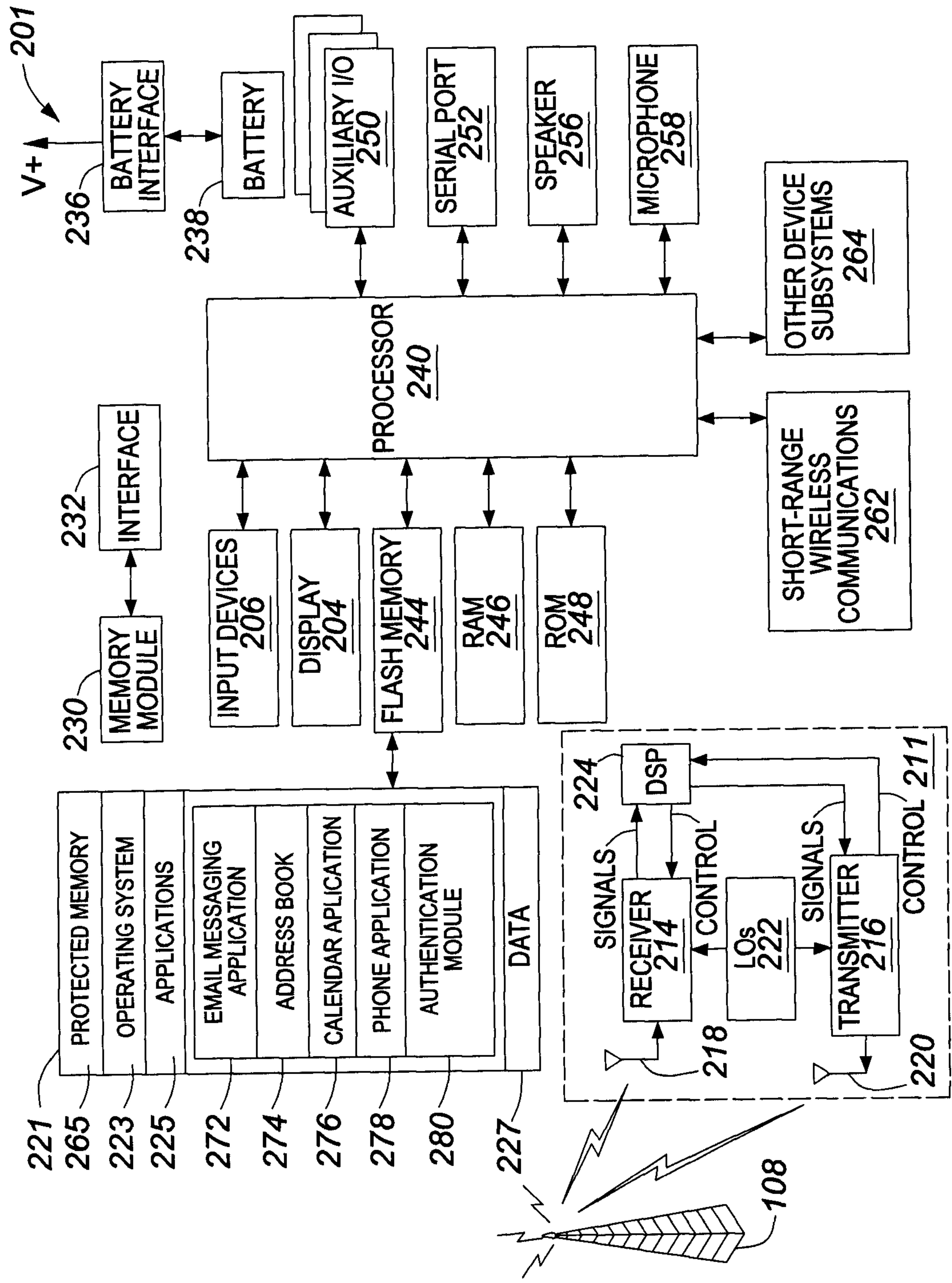
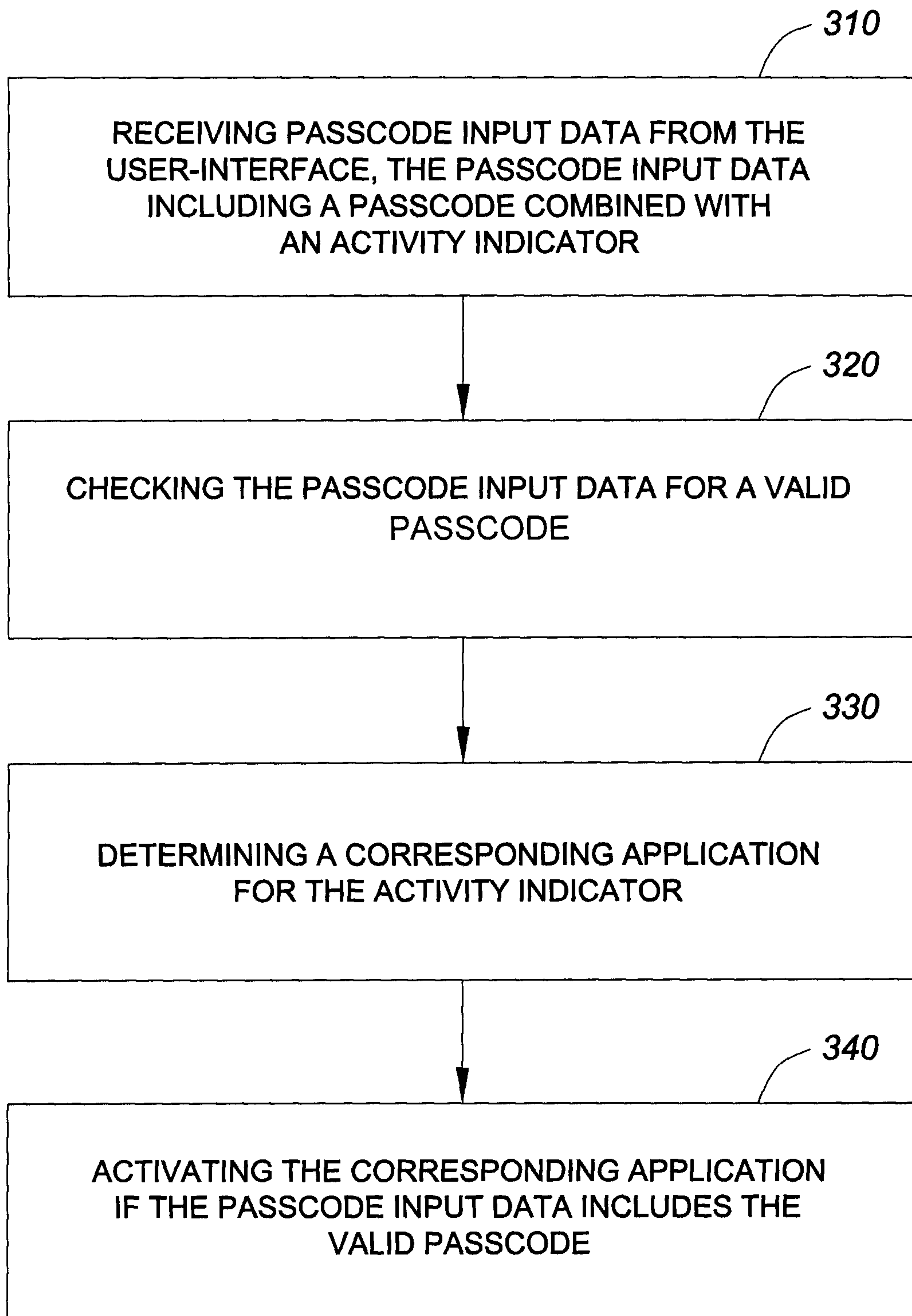
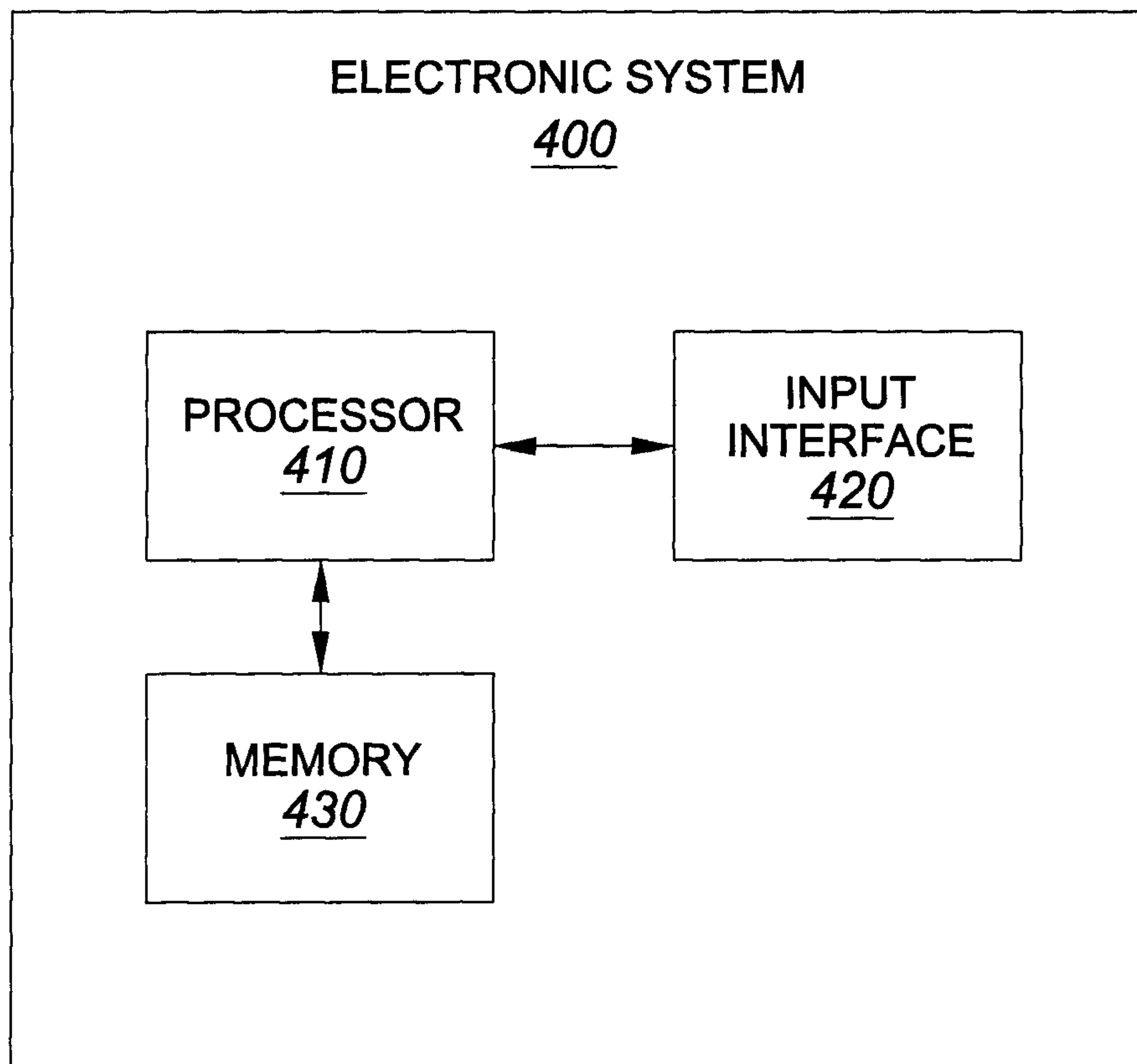


FIG. 2
(Prior Art)

3/4

**FIG. 3**

4/4

**FIG. 4**

310

RECEIVING PASSCODE INPUT DATA FROM THE
USER-INTERFACE, THE PASSCODE INPUT DATA
INCLUDING A PASSCODE COMBINED WITH
AN ACTIVITY INDICATOR

320

CHECKING THE PASSCODE INPUT DATA FOR A VALID
PASSCODE

330

DETERMINING A CORRESPONDING APPLICATION
FOR THE ACTIVITY INDICATOR

340

ACTIVATING THE CORRESPONDING APPLICATION
IF THE PASSCODE INPUT DATA INCLUDES THE
VALID PASSCODE