PERMITTING
PAYLOADS
AND
PERMITTING PAYLOAD EXCHANGES THEREBETWEEN

Title: SYSTEM AND METHOD OF RECOGNIZING ELECTRONIC DEVICES FOR EXCHANGING PAYLOADS AND PERMITTING PAYLOAD EXCHANGES THEREBETWEEN

Abstract: Systems and methods are provided for recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween. Payloads can include electronic payments, electronic business cards, and privacy-sensitive electronic data or information. A payload requester can request a payload from a payload transferor via a communication network without extensive setup procedures. The payload requester can connect to the communication network, such as a cloud network, and receive a list of available payload transferors located within a proximity to the payload requester. The payload requester can select one or more of the available payload transferors and request a payload therefrom. The selected payload transferor can send a confirmation to permit the payload exchange. In response, a payload exchange interface can be established, between the payload transferor's device and the payload requester's device, thereby permitting payload exchanges therebetween. The payload exchange interfaces can be established impromptu with minimal setup procedures.
SYSTEM AND METHOD OF RECOGNIZING ELECTRONIC DEVICES FOR EXCHANGING PAYLOADS AND PERMITTING PAYLOAD EXCHANGES THEREBETWEEN

CLAIM OF PRIORITY

[0001] This PCT application claims the benefit of U.S. Provisional Patent Application No. 61/441,167 entitled "Mobile Recognition and Payload Transfer Software," filed February 9, 2011, the entire contents of which are incorporated herein by reference.

FIELD OF THE INVENTION

[0002] One or more implementations relate generally to transferring files between devices, and more specifically, to recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween.

BACKGROUND

[0003] The subject matter discussed in the background section should not be assumed to be prior art merely as a result of its mention in the background section. Similarly, a problem mentioned in the background section or associated with the subject matter of the background section should not be assumed to have been previously recognized in the prior art. The subject matter in the background section merely represents different approaches, which in and of themselves may also be inventions.

[0004] Electronic transferring of information has grown extraordinarily with widespread Internet usage. The electronic transfers of information can include electronic fund transfers, electronic document transfers, and other transfers of digital or electronic information. Conventional electronic transferring systems typically use the World Wide Web although it may encompass a wider range of technologies such as e-mail, mobile devices and telephones as well.

[0005] In one example, electronic transferring of information has been utilized for electronic funds transfer (EFT) for exchanging or transferring money from one account to another, either within a single financial institution or across multiple institutions, using computer-based systems. However, typically, for such EFTs, the sender (the person transferring funds) and the
recipient (the person receiving funds) are members of the same financial institution. Also, the sender must know the financial account information of the recipient in order to transfer the funds electronically. In other instances, when the recipient desires an electronic fund transfer from the sender, the recipient must contact the sender and request financial account information from the sender in order to initiate the electronic fund transfer. After receiving such information, the sender and the recipient must wait for the financial institutions of the sender and the recipient to verify the accounts and allow the sender and recipient to electronically send funds to each other. Such electronic transfers can be burdensome, confusing and complicated to the sender and recipient as the information needed to setup the transfer, determine and verify to whom to send funds or from whom to receive funds, can be cumbersome and time-consuming.

**BRIEF DESCRIPTION OF THE DRAWINGS**

[0006] In order to describe the manner in which the features of the disclosure can be obtained, a more particular description of the principles briefly described herein will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only exemplary embodiments of the disclosure and are therefore not to be considered as limiting of its scope, the principles described and explained herein with additional specificity and detail through the use of the following accompanying drawings in which:

[0007] FIG. 1 illustrates a block diagram of a system for recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween in accordance with an example embodiment of the present disclosure;

[0008] FIG. 2 illustrates a flow chart of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween in accordance with an example embodiment of the present disclosure, taken from the perspective of the device establishing the payload exchange interface;

[0009] FIG. 3 illustrates a flow chart of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween in accordance with an example embodiment of the present disclosure, taken from the perspective of the device requesting the payload;
FIG. 4 illustrates a flow chart of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween in accordance with an example embodiment of the present disclosure, taken from the perspective of the device exchanging the payload;

FIGS. 5-7 illustrate one example embodiment of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween, illustrating the recognition of devices available for exchanging payloads;

FIG. 8 is an illustration of one example embodiment of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween, illustrating a payload exchange interface established between two devices;

FIGS. 9-12 illustrate an example embodiment of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween, where the device that exchanges the payload is in a privacy mode;

FIGS. 13-16 illustrate an example embodiment of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween, illustrating generating a code associated with securing the payload exchange;

FIGS. 17-18 illustrate an example embodiment of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween, illustrating establishing a payload exchange interface by a bump contact between two devices;

FIG. 19 illustrates a block diagram of an example of an environment wherein an on-demand payload exchange service might be used; and

FIG. 20 illustrates a block diagram of an embodiment of elements of FIG. 19 and various possible interconnections between these elements.

DETAILED DESCRIPTION

Various embodiments of the disclosure are discussed in detail below. While specific implementations are discussed, it should be understood that this is done for illustration purposes only. A person skilled in the relevant art will recognize that other components and configurations may be used without parting from the scope of the disclosure.
Several definitions that apply throughout this document will now be presented. The phrase "coupled" is defined as connected, whether directly or indirectly through intervening components and is not necessarily limited to physical connections. Coupled devices are devices which are in signal communication with one another.

The term "electronic device" is defined as any device that is capable of at least accepting data, transmitting data, and executing commands. For example, electronic devices can include, but are not limited to, portable communication devices, mobile communication devices, mobile computers, smartphones, computing pads, tablet computers, personal computers, desktop computers, laptop computers, netbooks, servers, routers, set-top phones, or other electronic devices capable of at least accepting data, transmitting data, and executing commands.

Systems and methods are provided for recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween. As discussed above, conventional electronic transfers can be burdensome, confusing and complicated to the sender and recipient as the information needed to setup the transfer, determine and verify whom to send funds to or receive funds from can be cumbersome and time-consuming. Accordingly, the present disclosure provides for systems and methods for devices for quickly, efficiently, and securely recognizing electronic devices for exchanging payloads and quickly, efficiently, and securely exchanging payloads therebetween.

In one non-limiting example, a payload requester device (for example, a first device) can request a payload (for example, an payment) from a payload transferor device (for example, a second device) via a communication network (for example, a cloud network) without the need to request account information, verify account information, or utilize a website or computer system of financial institutions associated with either one of the payload requester or the payload transferor device. Instead, with the system and method for recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween, the payload requester device can transmit a request for a secured payload exchange interface with a specific payload transferor device, and the secured payload exchange interface can be established impromptu, on-the-spur-of-moment, spontaneously, or otherwise without substantial preparation for the payload exchange.

For example, the payload requester device (for example, the first device) can connect
to a communication network, such as a cloud network, a wireless network, a social network, a geographical proximity network, a peer-to-peer device network (such as a vicinity in which Bluetooth devices can connect to one another), or any other communication network by which a payload exchange interface can be established. When the payload requester device connects to the communication network, the payload requester device can receive a list of other devices of available payload transferors located within a proximity to the payload requester device or located on the same communication network as the payload requester. The payload requester can then select one or more of the available payload transferor devices and request a payload (such as a payment) from one or more of the payload transferor device listed in the list. After selecting the payload transferor device, a notification can be sent to the selected payload transferor devices indicating that the payload requester device is requester payment from it. The selected payload transferor device can send a confirmation from its device indicating that the selected payload transferor agrees to exchanging or transferring a payment to the payload requester device. In response to the selected payload transferor device's confirmation, a payload exchange interface can be established between the payload transferor device and the payload requester device, thereby enabling the payload transferor device to exchange or transfer a payment to the payload requester device or account associated with the payload requester device. The established payload exchange interface can be a secured network connection, a portion of a cloud network temporarily dedicated or assigned to the payload requester device and the payload transferor device, a secured peer-to-peer connection, a near-field communication connection, or any other interface by which a payload can be exchanged between the payload requester device and the payload transferor device. As the payload requester device can easily identify available payload transferor devices and as the payload exchange interface can be established or set up "on the fly," impromptu, on-the-spur-of-moment, spontaneously, or otherwise without substantial preparation for the payload exchange, the exchange of payloads between devices is simplified and made more efficient, while also remaining secure, as the payload exchange interface is established for a specific exchange between specifically-identified devices and can also be established for the specific duration of the payload exchange.

Various mechanisms and methods for recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween will be described with reference to non-limiting example embodiments illustrated in FIGS. 1-18.
FIG. 1 illustrates a block diagram of a system for recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween in accordance with an example embodiment. In FIG. 1, the system 1000 can include a first device 100 (for example, a payload requester device), a second device 150 (for example, a payload transferor device), and a communication network 140 to which the first device 100 and the second device 150 can connect. The first device 100 can be an electronic device such as a portable communication device, a mobile communication device, a mobile computer, a smartphone, a computing pad, a tablet computer, a personal computer, a desktop computer, a laptop computer, a netbook, servers, a set-top phone, a portable digital assistant (PDA), a DVD player, a portable Blu-ray® player, a peer-to-peer cable television (for example, a network television), and audio-playback device, a portable music player, a peer-to-peer capable printer (for example, a network printer), or any other electronic device capable of at least accepting data, transmitting data, and executing commands. The second device 100 can be of the same type of electronic device as the first device 100 or can be a different type of electronic device.

The first device 100 can include a processor 105. The processor 105 can be directly or indirectly coupled to the first device 100. The processor 105 can be a processor assembly including one or more processors. The processor 105 can be a solid state processor, a core processor, or any other processor 105 configured to execute instructions for carrying out the method for recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween as will be described herein.

The first device 100 can include a display 115. The display 115 can be a touchscreen, a touch-sensitive display, a liquid crystal display (LCD), a light emitting diode display (LED), an active matrix organic light emitting diode display (AMOLED), or any other display which can display graphical information.

The first device 100 can include a location sensor 110 configured to detect the current location of the first device 100. The location sensor 110 can be configured to transmit location data indicative of the current location of the first device 100. The location sensor 110 can be a global positioning system sensor, a gravimeter, a magnetometer, a radio frequency identification (RFID) reader or tag, a Bluetooth™ transmitter or receiver, or any other sensor configured to detect, determine, or both detect and determine the location of the first device 100.
The first device 100 can comprise a computer readable storage medium 120. For example, the computer readable storage medium 120 can be transitory or non-transitory. The computer readable storage medium 102 can be any available media that can be accessed by a general purpose or special purpose computer, including the functional design of any special purpose processor as discussed above. By way of example, and not limitation, such non-transitory computer-readable media can include RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code means in the form of computer-executable instructions, data structures, or processor chip design. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or combination thereof) to a computer, the computer properly views the connection as a computer-readable medium. Thus, any such connection is properly termed a computer-readable medium. Combinations of the above should also be included within the scope of the computer-readable media. The computer-readable storage medium 120 can store instructions which can be executed by one or more processors to perform the steps or commands associated with the presently disclosed method for recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween.

The first device 100 can include an input input/output device 125, as illustrated in FIG. 1. The input/output device 125 can be one or more of a keyboard, a keypad, a virtual keyboard, a plurality of keys, a single key, a mouse, a trackball, a trackpad, a touchpad, a touchscreen, a touch-sensitive display, a camera, a proximity sensor, a gesture sensor, an input device, an auxiliary input device, or any other input interface by which data can be input by a user. The input/output device 125 can be integrated with the display 115. For example, the input/output device 125 can be a touchscreen which is configured to display graphical information (such as a shared user interface) and also receive user inputs. The input/output device 125 can be configured to output or transmit data from the first device 100 to one or more of an electronic device (for example the second device 150), a communication network 140, a server (not shown), or any other device which can receive data. For example, the input/output device 125 can include a transmitter, a transceiver, or any other device that can transmit or output data.
In FIG. 1, the second device 150 can include components similar to those illustrated with the first device 100, for example, a processor 155, a location sensor 160, a display 165, a computer-readable storage medium 170, and an input/output device 175 substantially similar to those of the first device 100. Additionally, while the first device 100 and the second device 150 are illustrated with particular components, those of ordinary skill in the art will appreciate that the first device 100 and second device 150 can include other components than those illustrated in FIG. 1. Additionally, those of ordinary skill in the art will appreciate that the system 1000 can include more electronic devices than as illustrated in FIG. 1.

Also illustrated in FIG. 1, the first device 150 and the second device 155 can be communicatively couple to one another via a peer-to-peer connection 135. For example, the peer-to-peer connection 135 can be a Bluetooth™ pairing, a near-field-communication (NFC) pairing, a peer-to-peer near-field-communication (P2P NFC) pairing, a Wi-Fi pairing, a telecommunication connection, or any other peer-to-peer connection 135 that permits the first device 150 and the second device 155 to be communicatively coupled to one another.

In FIG. 1, the system 1000 can also include a communication network 140 to which the first device 100 and the second device 150 can connect or communicatively couple. The first device 100 and the second device 150 illustrated in FIG. 1 can connect or communicatively couple to the communication network 140 via wireless links, hardwire links, airspace links, or any other link that permits an electronic device to communicatively couple to the communication network. In FIG. 1, each of the first device 100 and second device 150 is communicatively couple to the communication network 140 via a wireless link 130, such as a Wi-Fi connection, a Bluetooth™ connection, a peer-to-peer connection, or any other similar connection. The communication network 140 can be a cloud network, a wireless network, a social network, a geographical proximity network (such as a near-field-communication network established between electronic devices located within a predetermined proximity or predetermined distance from one another), a peer-to-peer device network (such as a vicinity in which Bluetooth devices can connect to one another), or any other communication network by which a payload exchange interface can be established.

FIG. 2 illustrates a flow chart of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween in accordance with an example embodiment. The method 200 is provided by way of example, as there are a variety of...
ways to carry out the method. Additionally, while the exemplary method 200 is illustrated with a
particular order of steps, those of ordinary skill in the art will appreciate that FIG. 2 and the steps
illustrated therein can be executed in any order that accomplishes the technical advantages of the
present disclosure and can include fewer or more steps than illustrated.

[0035] Each block shown in FIG. 2 represents one or more processes, methods or
subroutines, carried out in the example method 200. The steps illustrated in FIG. 2 can be
implemented in a system including a first device 100 (for example, a payload requester device)
and a second device 150 (for example, a payload transferor device) which can be
communicatively coupled to a communication network 140. For example, where the first device
100 and the second device 150 are both smartphones and the communication network 140 is a
cloud network, the method 200 of recognizing electronic devices for exchanging payloads and
permitting payload exchanges can be accomplished via computing components of the cloud
network 140. Each block shown in FIG. 2 can be carried out by one or more processors or
computing systems, for example, a server-based processor, a web-based processor, a cloud-based
computing system, a network-based server, or any other processor or computing system of the
communication network 140. In other embodiments, the blocks shown in FIG. 2 can be carried
out by one or more processors 105 of the first device 100, one or more processors 155 of the
second device 150, or one or more processors 105, 150, of the first device 100, second device
150, and the communication network 140, or any combination thereof. The flow chart illustrated
in FIG. 2 will be described from the perspective of the communication network 140 and will
make reference to the first device 100 (such as a payload requester device) and the second device
150 (such as an available payload transferor device) as illustrated in FIG. 1. The following
discussion of the method illustrated in FIG. 2 will also make reference to the illustrations
provided in FIGS. 5-18.

[0036] In FIG. 2, the method 200 comprises steps for carrying out the method of
recognizing electronic devices for exchanging payloads and permitting payload exchanges is
described from the perspective of the communication network 140 that is configured to establish
a payload exchange interface by which electronic devices 100, 150 can exchange payloads
between one another. In FIG. 2, the method 200 can begin at block 205. At block 205, a request
to exchange a payload 180 (shown in FIG. 8) with an available device 150 (for example, an
available payload transferor device) can be received from a first device 100 (for example, a
payload requester device), such as a smartphone, that is communicatively coupled to the communication network 140. For example, the request can be a request to receive a payload 180 such as an electronic payment 182, an electronic transfer fund, a digital photo 196, a business card 184, an electronic legal document 185, an electronic bill, electronic medical records, a privacy-sensitive electronic document, private electronic information, or any other document, information, or data that can be transferred electronically, from an available device 150. The request can be received and processed by one or more processors or computing systems of the communication network 140 (such as a cloud network 140 or a cloud computer). The request to exchange a payload with the available device can be a request to exchange a payload with an available device that is located with a predetermined proximity of the first device 100. The available device can be located within a predetermined proximity of the first device 100 when the available device is located within at least one of a cloud network, a peer-to-peer pairing proximity, a near-field-communication pairing proximity, a wireless network, a social network, and a predetermined geographic proximity of with the first device 150. For example, the available device can be the second device 150 communicatively coupled the communication network 140 to which the first device 150 is communicatively coupled. In at least one embodiment, the request can be a request to exchange a payload with a plurality, more than one, or at least one available device.

[0037] Although not illustrated in FIG. 2, the method 200 can include a determination of the available devices from which the first device 100 can request a payload 180, can be made by one or more processors or computing systems of the communication network 140 and can be transmitted to the first device 100 as a list of selectable available devices. For example, the communication network 140 can detect a plurality of available devices. For example, the communication network 140 can detect a plurality of available devices communicatively coupled to or connected to the communication network 140. In one embodiment, the communication network 140 can detect the plurality of available devices by receiving a plurality of location data transmitted by corresponding available devices. The communication network 140 can also receive location data transmitted by the first device 100 indicating the current location of the first device 100. The communication network 140, via one or more processors or computing systems, can compare the location data transmitted by the available devices and the location data transmitted by the first device 100 to determine which of the available devices are located within
a predetermined proximity of the first device 100. For example, the predetermined proximity can be a predetermined distance (such as within a 500 foot radius, a one mile radius, a 10 mile radius, a 25 foot radius, within a same venue, within a same address, a distance sufficient to establish a peer-to-peer device connection, a Bluetooth connection, a near-field communication connected, or any other predetermined distance). In other embodiments, the available devices can be determined as being located within a predetermined proximity of the first device 100 when the first device and one or more of the available devices are located on the same cloud network, the same Wi-Fi network, the same peer-to-peer pairing proximity, a near-field-communication pairing proximity, a wireless network, a social network, or any other network.

[0038] In response to determining, detecting, or both determining and detecting the available devices located within a predetermined proximity of the first device 100, the communication network 140 can transmit, to the first device 100, a list 102 (shown in FIG. 6) listing the available devices located within a predetermined proximity of the first device 100. For example, the communication network 140 can transmit a request to the first device 100 to display the list 106 on the display 115 of the first device 100. The list 102 can include at least one of an email address associated with one of the plurality of available devices, a telephone number associated with one of the plurality of available devices, an unique identifier associated with one of the plurality of available devices, an identification number associated with one of the plurality of available devices, and at least a portion of an account number associated with one of the plurality of available devices. The first device 100 can designate one or more available devices 104 as a selected available device 152 (shown in FIG. 7) from which to request a payload 180.

[0039] In such an embodiment, the request to exchange a payload received by the communication network 140 can include an identification of the one or more available devices selected, by the first device 100, from which the first device 100 desires to receive the payload. In response to receiving the request, the communication network 140 can process the request and proceed to block 210.

[0040] At block 210, the communication interface 140, via one or more processors of computing systems, can transmit a confirmation request 1605 (shown in FIG. 16) to the available device 150. The confirmation request 1605 can be a request to confirm that the available device 150 accepts the request to exchange the payload with the first device 100. For example, the confirmation request 1605 can include instructions or a request to display a notification, a pop-up
window, a graphical user interface, a text message, an email, an SMS message, an MSM, message, or any other notification which notifies the available device 150 that the first device 100 requests a payload (for example, a payment) from the available device 150. In response to transmitting the confirmation request 1605, the method can proceed to block 215.

[0041] At block 215, the communication network 140 can receive confirmation data 1610 (shown in FIG. 16) associated with the available device 150. For example, the available device 150 can transmit the confirmation data 1610 in response to the transmitted confirmation request 1605. The confirmation data 1610 can indicate an acceptance by the available device 150 to exchange the payload with the first device 100. For example, in the embodiment where the payload 180 is a payment, the confirmation data 1610 can indicate that the available device 150 accepts or confirms that the request for the available device 150 to transfer, deliver, or otherwise exchange a payment to the first device 100. After receiving the confirmation data 1610, the method can proceed to block 240.

[0042] At block 220, the communication network 240 can establish a payload exchange interface 190 (shown in FIG. 8) in response to the received request to exchange the payload and the received confirmation data. The payload exchange interface 190 can be an encrypted network, a portion of the communication network 140 dedicated to the first device 100 and the available device(s) 150 for the payload exchange, a temporary peer-to-peer connection between the first device 100 and the available device(s) 150, a portion of a cloud network dedicated or assigned (for example, temporarily) to the payload requester and the payload transferor, a secured peer-to-peer connection, a near-field communication connection, or any other interface by which a payload can be exchanged between first device 100 (for example, the payload requester device) and the available device 150 (for example, the payload transferor device).

[0043] Although not illustrated in FIG. 2, the method 200 can include generating a verification code 1005 (shown in FIG. 10) in response to the request to exchange a payload. The verification code 1005 can be at least one of an alphanumeric code, a pin code, a facial recognition code, a photo recognition code (for example, the first device 100 and second device 150 can capture the same image), an audio recognition code (for example, the first device 100 and the second device 150 can capture or record audio playing in the same location as the first device 100 and the second device 150). The communication network 140 can transmit the verification code 140 to one or both of the first device 100 and the second device 150 from...
which the first device desires a payload 180. The communication network 140 can receive validation data in response to the transmitted code 1005. The validation data can be received from one or both of the first device 100 and the second device 150. The validation data can correspond to an input 1010 (shown in FIG. 12) entered at the second device 150, and the input 1010 can be an input of the verification code 1005 at the second device 150. The validation data corresponding to the input 1010 can be compared to the generated code 1005. In the event the validation data matches the generated code 1005, the communication network 140 can establish the payload exchange interface 190 to permit payload exchanges between the first device 100 and the second device 150. In other words, the validation data can indicate that the second device 150 is the intended device from which the first device 100 desires a payload. That is, the validation data and the verification code can be security measures ensuring that the communication network 140 will be established for the proper or appropriate devices 100, 150 associated with the received request to exchange a payload.

[0044] In yet another embodiment, the communication network 140 can transmit, to at least one of the first device 100 and the second device 150, a bump request 1705 (shown in FIG. 17). The bump request 1705 can be a request for an input indicative of a physical contact between the first device 100 and the second device 150. For example, the bump request 1705 can be a notification, pop-up window, text message, email, SMS message, MSM, message, or any other notification which can notify the first device 100 and/or second device 150 that an input 1805 (shown in FIG. 18) indicative of a physical contact between the first device 100 and the available device 150 is needed to establish the payload exchange interface 190. The communication network 140 can receive bump data from one or both of the first device 100 and the available device 150. The bump data can be associated with an input (1805) corresponding to the physical contact between the first device 100 and the available device 150. In response to receiving the bump data, the communication network 140 can establish the payload exchange interface 190 to permit payload exchanges between the first device 100 and the second device 150 or plurality of available devices.

[0045] FIG. 3 illustrates a flow chart of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween in accordance with an example embodiment, taken from the perspective of the device requesting the payload. While the exemplary method 300 is illustrated with a particular order of steps, those of ordinary skill in
the art will appreciate that FIG. 3 and the steps illustrated therein can be executed in any order that accomplishes the technical advantages of the present disclosure and can include fewer or more steps than illustrated. Each block shown in FIG. 3 can be carried out by one or more processors communicatively coupled to the first device 100, one or more processors 155 of the second device, or a combination of one or more processors 105, 150, of the first device 100, second device 150, and the communication network 140, or any combination thereof.

[0046] In FIG. 3, the method 300 can begin at block 305. At block 305, one or more processors 105 communicatively coupled to the first device 100 can transmit a request to exchange a payload 180. For example, the first device 100 can transmit the request to the communication network 140 to establish a payload exchange interface 190 by which the first device 100 can exchange, transfer, deliver, or receive a payload 180. The first device 100 can be associated with a predetermined proximity. For example, the first device 100 can transmit, to the communication network 140, location data indicative of the current location of the first device 100, and the predetermined proximity can be based at least in part on the current location of the first device 100, a current network to which the first device 100 is connected, or a combination of both. Predetermined criteria can be utilized to determine whether an available device 150 is within a proximity of the first device 100. For example, the predetermined criteria can include: a predetermined distance (such as within a 500 foot radius, a one mile radius, a 10 mile radius, a 25 foot radius, within a same venue, within a same address, a distance sufficient to establish a peer-to-peer device connection, a Bluetooth connection, a near-field communication connected, or any other predetermined distance), a determination that an available device is located on the same cloud network, the same Wi-Fi network, the same peer-to-peer pairing proximity, a near-field-communication pairing proximity, a wireless network, a social network, or any other network, or any combination of predetermined criteria that can indicate whether an available device 150 is within a proximity of the first device 100.

[0047] Although not illustrated in FIG. 3, the first device 100 can receive a list 102 of available devices (for example, second devices that can be payload transferors) located within a proximity of the first device 100. For example, the first device 100 can receive the list 102 from the communication network 140. The list 102 can include an email address associated with one of the available devices, a telephone number associated with one of the available devices, an unique identifier associated with one of the available devices, an identification number
associated with one of the available devices, an identification number associated with one of the available devices and an account number associated with one of the available devices. In response to receiving the list 102 and/or a determination of the available devices 150 located within a predetermined proximity of the first device 100, the method can proceed to block 310.

[0048] At block 310, one or more processors 105 communicatively coupled to the first device 100 can identify a second device 150 to exchange the payload 180. For example, a detection of an input entered, via the input/output device 125 of the first device 100, can indicate a selection or designation of one or more of the available devices located within a predetermined proximity of the first device 100. That is, an input corresponding to the selection 152 of one or more available devices 150 from which the first device 100 desires to receive a payload 180 (for example, a payment) can be transmitted to the communication network 140. After transmitting the identification of the second device 150, the method 300 can proceed to block 315.

[0049] At block 315, the first device 100 can receive confirmation data corresponding to an establishment of a payload exchange interface 190 and corresponding to an acceptance 1610 by the second device 150 to exchange the payload 180. The confirmation data can be transmitted by the confirmation network 140. After the first device 100 receives the confirmation data, the method can proceed to block 320.

[0050] At block 320, the first device 100 can exchange the payload 180 via the payload exchange interface 190. For example, the first device 100 can receive, exchange, transfer, or receive information or data via the payload exchange interface 190. As described above, the first device 100 can receive one or more of an electronic payment 182, an electronic transfer fund, a digital photo 196, a business card 184, an electronic legal document 185, an electronic bill, electronic medical records, a privacy-sensitive electronic document, private electronic information, or any other document, information, or data that can be transferred electronically.

[0051] In another embodiment, although not illustrated in FIG. 3, the first device 100 can identify a second device 150 that is not listed in the list 102 transmitted by the communication network 140. For example, the first device 100 can identify a second device 150 that the operator of the first device 100 knows is within a predetermined proximity of the first device 100 but does not appear in the list 102. For example, the second device 150 can be in a private mode where the identity of the second device 150 can be hidden even though the second device 150 may be connected to the communication network 140 or within a predetermined proximity of the
first device 100. In another embodiment, the second device 150 can be a device the operator of the first device 100 knows is within a predetermined proximity of the first device 100 but is not connected or communicatively coupled to the communication network 140.

[0052] In the event the first device 100 identifies a second device 150 that is not listed in the list 102, the first device 100 can request a verification code 1005 from the communication network 140 to associate with the payload 190. The communication network 140 can generate the verification code 1005. In another embodiment, the first device 100 can generate the code 1305 itself. The code 1005, 1305 can include at least one of an alphanumeric code, a pin code, a facial recognition code, a photo recognition code (for example, the first device 100 and second device 150 can capture the same image), an audio recognition code (for example, the first device 100 and the second device 150 can capture or record audio playing in the same location as the first device 100 and the second device), a gesture code, and a voice command.

[0053] In either embodiment, the first device 100 can receive the generated verification code 1005, 1305 and can then transmit the code to the second device 150 from which the first device 100 desires the payload 180. For example, the first device 100 can transmit a message, an email, a text message, a multimedia message, an SMS message, a MSM message, a video message, a video conference, a telephone call, or any other communication or transmission of the code to the second device 150. In at least one embodiment, where the operators of the first device 100 and the second device 150 are located within the same physical venue as the other, the operator of the first device 100 can speak the code 1005, 1305 or demonstrate the code 1005, 1305 to the operator of the second device 150. The operator of the second device 150 can then enter an input 1010, 1310 corresponding to the code 1005, 1305 transmitted by the first device 100. For example, the second device 150 can enter or input the code 1005, 1305 transmitted by the first device 100, and the input 1010, 1310 can be transmitted to the communication network 140 as a corresponding code to verify, validate, or otherwise confirm that the second device 150 is the device from which the first device 100 desires a payload 180.

[0054] In another embodiment, the transmitted code 1005, 1305 can represent an invitation by the first device 100 to the second device 150 to connect to the communication network 140 in order to exchange, transmit, or otherwise transfer a payload 180 to the first device 100. In response to transmitting the code 1005, 1305 to the second device 150 and the second device 150 transmitting a corresponding code 1010, 1310 to the communication network 140, the
confirmation data received by the first device 100 can further correspond to a confirmation of a match between the transmitted code 1005, 1305 and the corresponding code 1010, 1305 associated with the second device 150 to establish a payload exchange interface 190 through which the first device 100 can receive a payload 180 from the second device 150.

In yet another embodiment, the first device 100 can receive a bump request 1705 (shown in FIG. 17), from the communication network 140, for an input 1805 (shown in FIG. 18) indicative of a physical contact with the second device 150. The first device 100 can receive a bump input 1805 from the second device 150. For example, the bump input 1805 can be a physical contact between a corner 101 or other portion of the first device 100 with a corner 151 or other portion of the second device 150. The physical contact can be a direct contact or a substantially direct contact, such as input 1805 that is indicative of at least a portion the first device 100 and at least a portion of the second device 150 being within a predetermined proximity to one another to constitute a physical contact. For example, within an inch, within 1.5 inches, 0.5 inches, 10 millimeters, one centimeter, or any other distance which can constitute a physical contact. The physical contact can further be determined by magnetometers of the first device 100 and the second device 150, RFID tags and readers, or any other proximity sensors which can indicate that the first device 100 and the second device 150 are sufficiently close in proximity to one another to constitute a physical contact therebetween. In response to transmitting bump data corresponding to the input 1805, the communication network can establish a payload exchange interface 190 between the first device 100 and the second device 150 and transmit confirmation data to the first device 100 from the communication network 140.

FIG. 4 illustrates a flow chart of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween in accordance with an example embodiment, taken from the perspective of the device exchanging the payload. While the exemplary method 400 is illustrated with a particular order of steps, those of ordinary skill in the art will appreciate that FIG. 4 and the steps illustrated therein can be executed in any order that accomplishes the technical advantages of the present disclosure and can include fewer or more steps than illustrated. Each block shown in FIG. 4 can be carried out by one or more processors communicatively coupled to the second device 155, one or more processors of the first device 150, or a combination of one or more processors 105, 150, of the first device 100, second device 150, and the communication network 140, or any combination thereof.
In FIG. 4, the method 400 can begin at block 405. At block 405, the available device (that is, the payload transferor device 150) can receive a request to exchange a payload 180 with a payload requester device 100 located within a predetermined proximity to the payload transferor device 150. The predetermined proximity between the payload transferor device 150 and the payload requester device 100 can be any one of the predetermined proximities as discussed in relation to FIGS. 2-3. The request can be transmitted by the communication network 140 or the payload requester device 100. The request can include a code 1005, 1305 associated with the payload 1805, as described above. In response to receiving the request, the method can proceed to block 410.

At block 410, a detection of an input corresponding to the received code can be made. For example, the processor 155 of the payload transferor device 150 can detect an input 1010, 1310 corresponding to the received code 1005, 1305 entered at the input/output device 175 of the payload transferor device 150. For example, the input 1010, 1310 can correspond to the entry of the code 1005, 1305 at the second device 150. In response to inputting the received code or detecting an input 1010, 1310 corresponding to the received code 1005, 1305, the method can proceed to block 415.

At block 415, the payload transferor device 150 can transmit data corresponding to the detected input 1010, 1310. For example, the payload transferor device 150 can transmit the data to the communication network 140. The communication network 140 can verify the data transmitted by the payload transferor device 150 to confirm that the payload transferor device 150 is the device from which the payload requester device 100 desires a payload 180. In response to transmitting data corresponding to the detected input 1010, 1310, the method can proceed to block 420.

At block 420, the payload transferor device 150 can receive confirmation data corresponding to the establishment of a payload exchange interface 190 by which the payload transferor device 150 can transmit, transfer, or otherwise exchange a payload (such as a payment) to the payload requester device 100. The payload exchange interface 190 can include those discussed in relation to FIGS. 2-3. In response to receiving the confirmation data, the method can proceed to block 425.

At block 425, the payload transferor device 150 can transmit the payload 180 via the payload 180 exchange interface 190. The payload 180 can be at least one of a monetary...
exchange, a picture exchange, a business card exchange, a medical records exchange, and a privacy-sensitive document exchange.

[0062] Although not illustrated in FIG. 4, the method 400 can include receiving a bump request 1705 from the communication network 140 as discussed in relation to FIGS. 2-3.

[0063] The disclosure now turns to FIGS. 5-18 which illustrate example implementations of systems and methods of recognizing electronic devices for exchanging payloads and permitting payload exchanges. In FIGS. 5-18, the method is implemented as a mobile phone application, but those of ordinary skill in the art will appreciate that the method can be implemented as a web-based application, a physically-purchased software application, an electronic tablet application, or any other implementation that can permit payload exchanges between electronic devices located within a predetermined proximity to one another.

[0064] FIGS. 5-7 illustrate one example embodiment of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween, illustrating the recognition of devices available for exchanging payloads. In FIG. 5, a first device 100 and a second device 150, both of which are smartphones, are communicatively coupled to a communication network 140 that is a cloud network. As illustrated in FIG. 5, the first device 100 includes a touch-sensitive display 115 configured to receive inputs and display graphical information. The second device 150 includes a similar touch-sensitive display 165. The first device 100 and the second device 150 can each include location sensors 110, 160. The first device 100 can transmit location data, detected by the location sensor 110 (shown in FIG. 1) indicative of the first device's 100 current location. Similarly, the second device 150 can transmit location data, detected by the location sensor 160 (shown in FIG. 1) indicative of the second device's 150 current location. Although, FIG. 5 illustrates two devices 100, 150, those of ordinary skill in the art will appreciate that more devices can be communicatively coupled to the communication network 140. In FIG. 5, the first device 100 is the payload requester, and the second device 150 is the payload transferor. In FIG. 5 both the first device 100 and the second device 150 have connected or communicatively coupled to the communication network 140, but a request for a payload exchange has not yet been transmitted from either the first device 100 or the second device 150.

[0065] In FIG. 6, the first device 100 (for example, the payload requester device) can transmit a request to the communication network 140 to exchange a payload 180 with a second
device 150 (for example, an available payload transferor device). In response to the request, the communication network 140 can transmit a list 102 which can be displayed on the display 115 of the first device 100. In FIG. 6, the list 102 includes a plurality of identifiers 104 associated with available devices or available payload transferor devices located within a predetermined proximity of the first device 100. In FIG. 6, the identifiers 104 are usernames associated with the available devices. However, in other embodiments, the list 102 can include email addresses of respective available devices, telephone numbers of respective available devices, unique identifiers (for example, user names, profile pictures, nicknames, full names) of respective available devices, identification numbers of respective available devices, at least a portion of an account number of respective available devices, or other identifiers by which the available devices can be distinguished from one another. In FIG. 6, the second device 150 can be associated with the username "Lisa" 152 presented on the list 102 displayed on the display 115 of the first device 100.

[0066] In FIG. 7, the operator of the first device 100 (for example, the payload requester device) can select one of the identifier 104 presented in the list 102 displayed on the display 115 of the first device 100. For example, in FIG. 7, the operator of the first device 100 has selected the username "Lisa" 152 from the displayed list 102. The username "Lisa" 152 associated with the second device 150. The operator of the first device 100 can select the username "Lisa" 152 by tapping the portion of the touch-sensitive display 115 proximate to the location of the username "Lisa" 152, controlling a cursor using an input/output device (for example, a mouse, cursor keys, arrow keys, etc.) to select the username "Lisa" 152, speaking the username "Lisa" 152, or using any other mechanism for selecting, choosing, identifying, or otherwise designating at least one username 104 presented in the list 102. The selection of the username "Lisa" 152 can be transmitted to the communication network 140 to identify the available device from which the first device 100 desires to receive a payload 180. As illustrated in FIG. 7, the username "Lisa" 152 has been selected, and therefore, the first device 100 has indicated to the communication network 140 that the first device 100 desires a payload from the second device 150, associated with the username "Lisa" 152. As illustrated in FIG. 7, the first device 100 need not enter any financial information associated with the second device 150 in order to request a payload or payment from the second device 150. Instead, the first device 100 can view the devices within a predetermined proximity from the first device 100 and/or devices located on a
same network as the first device 100, and simply select the identifier 104 associated with the
available device from which the first device 100 desires a payload exchange, thereby making
electronic transfers and exchanges simpler, more efficient, and user-friendly.

[0067] In response to the selection of the username 152, the communication network 140 can
transmit a request to the selected available device (e.g., the second device 150 that is the selected
payload transferor device) to connect the second device 150 with the first device 100. For
example, a pop-up window (not shown) can be displayed on the display 165 of the second device
150 requesting permission to connect the first device 100 to the second device 100 or otherwise
notifying the second device 150 that the first device 100 desires to request a payload 180 from
the second device 150. In other embodiments, the notification can indicate that the first device
100 desires to transmit, transfer, or exchange a payload to the second device 150. The second
device 150 can transmit a signal back to the communication network 140 indicating the
acceptance or denial of permission to connect with the first device 100 and/or the acceptance or
denial of the payload exchange. If the second device 150 denies the request, a notification can
be transmitted by the communication network to the first device 100 indicating so, the username
152 associated with the second device 150 can be removed from the list 102, or any other
notification or indication that the second device 150 does not desire to exchange payloads with
the first device 110 can be transmitted.

[0068] If, however, the second device 150 transmits data to the communication network 140
indicating that the second device 150 accepts the first device's 100 request to exchange payloads
and/or grants permission to the communication network 140 to connect the first device 100 to the
second device 150 for a payload exchange, the communication network 140 can establish a
payload exchange interface 190 (such as a temporary portion of the cloud network, a gateway, a
secured network connection, an encrypted network connection, or any other interface by which a
payload can be exchanged) between the first device 100 and the second device 150, for example,
as illustrated in FIG. 8. In at least one embodiment, the communication network 140 can
transmit a notification to one or both of the first device 100 and the second device 150 indicating
that the payload exchange interface 190 has been established and is available for exchanging
payloads. As the payload exchange interface 190 has been established by the communication
network 140 and has been designated specifically for the first device 100 and second device 150
without requiring excessive setup procedures from either one of the first device 100, second
device 150, or the associated financial institutions associated with the financial accounts of the first device 100 and the second device 150, the payload exchange interface 190 can be established in a quick and efficient manner. That is, the payload exchange interface 190 can be established impromptu or "on the fly."

[0069] FIG. 8 is an illustration of one example embodiment of a method recognizing electronic devices for exchanging payloads and permitting payload exchanges, illustrating a payload exchange interface established between two devices for exchanging payloads. In FIG. 8, the communication network 140 has established a payload exchange interface 190, such as a temporary encrypted gateway, between the first device 100 (e.g., the payload requester device) and the second device 150 (e.g., the payload transferor device). In FIG. 8, a plurality of payloads 180 can be exchanged between the first device 100 and the second device 150 over the payload exchange interface 190. For example, payloads 180 can include an electronic fund, currency 182, a business card 184, legal documents 185, medical records 183, digital photos 186, music, movies, media files (including audio, photo, and video files), text files, web files, presentations, virtual goods (such as downloadable software), information related to social games (for example, clues, hints, text messages, photographs), or any other information or data that can be electronically transferred, transmitted, received, or otherwise exchanged.

[0070] FIGS. 9-12 illustrate an example embodiment of a method of recognizing electronic devices for exchanging the payload 180 is in a privacy mode. In FIGS. 9-12, the payload requester device (e.g., the first device 100) has requested a payload from a payload transferor device (e.g., the second device 150) which is not listed in the list 102 of available devices transmitted by the communication network 140 and displayed on the display 115 of the payload requester device 100. For example, in FIG. 9, the payload requester device 100 desires a payload 180 from a payload transferor device 150 associated with the username "Lisa" 152 that is connected to the communication network 140 but is in a privacy mode. For example, in the privacy mode, the payload transferors 150 can be connected to the communication network 140 but may not visible to others connected to the communications network 140. The operator of the payload requester device 100 might physically see that the operator of the desired payload transferor device 150 associated with the username "Lisa" 152, as both operators can be in the same location within a visible vicinity of one another (for example, in the same room).
In FIG. 9, the payload requester device 100 can search the list 102 of identifiers 104 associated with available devices from which the payload requester device 100 can receive a payload. In FIG. 9, the payload requester device 100 does not see an identifier (e.g., username "Lisa" 152) associated with the payload transferor device 150 with whom the payload requester device 100 desires to receive a payload 180. For example, the payload requester device 100 desires to request a payment or receive a payment from the payload transferor device 150 associated with the username "Lisa" 152. As the username "Lisa" 152 is not present in the list 102, the payload requester device 100 can request a verification code 1005 from the communication network 140, as illustrated in FIG. 10, to invite the payload transferor device 150 to exchange, transmit, or transfer a payload 180 to the payload requester device 100 using a payload exchange interface 190 established by the communication network 140.

In FIG. 10, in response to the request for the verification code 1005, the communication network 140 can generate the verification code 1005 and transmit the verification code 1005 to the payload requester device 100. The verification code 1005 can be at least one of an alphanumeric code, a pin code, a facial recognition code, a photo recognition code, an audio recognition code, a gesture code, and a voice command uniquely associated with the payload to be exchanged with the payload requester device 100 and the payload transferor device 150. In FIG. 10, the verification code 1005 is a numeric code, such as a pin code.

In response to receiving the verification code 1005, the payload requester device 100 can transmit the verification code 1005 to the desired payload transferor device 150 (e.g., the device associated with the username "Lisa" 152), as illustrated in FIG. 11. For example, the payload requester device 100 can transmit the verification code 1005 verbally if the operator of the payload transferor device 150 associated with the user name "Lisa" 152 is in the same location, venue, room, etc. as the operator of the payload requester device 100. In other embodiments, the payload requester device 100 can transmit the verification code 1005 via a text message, an email, over a telephone call, over a videocall or videoconference, an SMS message, and MSM message, or any other transmission or communication to the payload transferor device 150. In FIG. 11, the operators of the payload requester device 100 and the payload transferor device 150 can be engaged in a videoconference, and the operator of the payload requestor 100 can verbally transmit the verification code 1005 to the payload transferor device 150.
Upon receiving the verification code 1005, the operator of the payload transferor device 150 can enter or input 1010 the verification code 1005 into the payload transferor device 150. Data corresponding to the inputted verification code 1010 at the payload transferor device 150 can be transmitted to the communication network 140, as illustrated in FIG. 12. The communication network 140 can compare the data corresponding to the inputted verification code 1010 at the payload transferor device 150 (for example, the corresponding code) with the verification code 1005 transmitted to the payload requester device 100, as illustrated in FIG. 12. In response to a determination that the inputted verification code 1010 substantially matches the verification code 1005, the communication network 140 can establish a payload exchange interface 190, such as the one illustrated in FIG. 8.

FIGS. 13-16 illustrate an example embodiment of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween, illustrating generating a code associated with securing the payload exchange. While FIGS. 9-12 illustrate a verification code 1005 generated by the communication network 140, the verification code can be generated by the payload requester device 100, as illustrated in FIG. 13. For example, in FIG. 13, the operator of the payload requester device 100 can generate the verification code 1305 using the touch-sensitive display 115 of the payload requester device 100. In FIG. 13, the verification code 1305 generated by the payload requester device 100 is a gesture code. Specifically, the operator of the payload requester device 100 has inputted a gesture code 1305 that is the letter "N" drawn beginning from the lower left corner of the letter to the upper right corner of the letter in one motion. After the payload requester device 100 completes the generation of the verification code 1305, the payload requester device 100 can connect to the communication network 140 and transmit the verification code 1305 to the communication network 140, as illustrated in FIG. 14.

Meanwhile, the operator of the payload requester device 100 can transmit the generated verification code 1305 to the operator of the payload transferor device 150 from which the payload requester device 100 desires to receive a payload, for example, as illustrated in FIG. 15. The verification code 1305 can be transmitted in a variety of ways, such as those discussed in relation to FIG. 11. In FIG. 15, the operator of the payload requester device 100 can transmit verbal instructions for the gesture code to the payload transferor device 100 via a phone call. As illustrated in FIG. 15, the payload transferor device 150 has not yet communicatively coupled
with or connected to the communication network 140. However, those of ordinary skill in the art will appreciate that the payload transferor device 150 can be communicatively coupled to the communication network 140 but can be in an invisible or privacy mode such as that discussed in relation to FIG. 9. In response to receiving the verification code 1305, the operator of the payload transferor device 150 can enter gestures corresponding to the verification code 1305 as inputted verification code 1310, as illustrated in FIG. 15.

[0077] After the inputted verification code 1310 is entered at the payload transferor device 150, the payload transferor device 150 can connect to or communicatively coupled with the communication network 140. The payload transferor device 150 can also transmit data corresponding to the inputted verification code 1310. The communication network 140 can compare the inputted verification code 1310 to the verification code 1305 generated and transmitted by the payload requester device 100. In the event the inputted verification code 1310 and the verification code 1305 match, the communication network 140 can transmit a confirmation request 1605 to the payload transferor device 150 (for example, via a pop-up message, an email, a text message, or other notification) requesting that the payload transferor device 150 confirm that the payload transferor device 150 grants permission to connect the payload requester device 100 thereto. The payload transferor device 150 can transmit a response 1610 back to the communication network 140 confirming that the payload transferor device 150 grants permission to connect with the payload requester device 100. In response, the communication network 140 can establish a payload exchange interface 190 between the payload requester device 100 and the payload transferor device 150 to permit payload exchanges therebetween, such as the payload exchange interface 190 illustrated and described in FIG. 8. While FIG. 16 illustrates the communication network 140 transmitting a confirmation request 1605 from the payload transferor device 150 that the payload transferor device 150 desires to exchange payloads with the payload requester device 100, those of ordinary skill in the art will appreciate that the payload exchange interface 190 can be established without such a confirmation request 1605 and can be established simply in response to receiving an inputted verification code 1310 that matches the verification code 1305 generated by the payload requester device 100. Those of ordinary skill in the art will appreciate that the confirmation request 1605 can be a security measure that can be included to further ensure that the payload exchange interface 190 is established for the proper devices. Similarly those of ordinary skill in
the art will appreciate that the verification codes 1305, 1005 illustrated in FIGS. 10-16 can serve as security measures to ensure that the payload exchange interface 190 is established for the proper devices.

[0078] While the verification codes 1005, 1305 are generated at the request of the payload requester device 100, those of ordinary skill in the art will appreciate that a verification code 1005, 1305 can be generated for each request for a payload exchange, whether or not a verification code 1005, 1305 is requested by the payload requester device 100.

[0079] FIGS. 17-18 illustrate an example embodiment of a method of recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween, illustrating establishing a payload exchange interface by a bump contact between two devices. FIGS. 17-18 illustrate another security measure to further ensure that the payload exchange interface 190 is established for the proper devices. In FIG. 17, the payload requester device 100 and the payload transferor device 150 can be connected to or communicatively coupled with the communication network 140. In FIG. 17, the payload requester device 100 has transmitted, to the communication network 140, a request for a payload exchange from the payload transferor device 150. In response to the request for the payload exchange, the communication network 140 can transmit a bump request 1705 to one or both of the payload requester device 100 and the payload transferor device 150. The bump request 1705 can be a request for an input indicative of a physical contact between the payload requester device 100 and the payload transferor device 150. For example, in FIG. 17, the communication network 140 can transmit the bump request 1705 to the payload requester device 100, and the bump request 1705 can be a request for an input indicative of a physical contact at the payload requester device 100 from the payload transferor device 150.

[0080] In response to the bump request 1705, the payload requester device 100 and the payload transferor device 150 can bump each other, as illustrated in FIG. 18. For example, a corner 101 or other portion of the payload requester device 100 can directly physically contact a corner 151 or other portion of the payload transferor device 150. In other embodiments, the payload requester device 100 and the payload transferor device 150 can approach one another, without directly contacting one another, such that predetermined bump criteria is met. For example, the predetermined bump criteria can be a predetermined distance between the payload requester device 100 and the payload transferor device 150, where the predetermined distance
can constitute a physical contact or bump contact. For example, the predetermined distance can be an inch, a centimeter, ten millimeters, two inches, five inches, one millimeter, or any other predetermined distance that can constitute a physical contact or bump contact, including those discussed above in relation to FIGS. 2-4. When the payload requester device 100 and the payload transferor device 150 physically contact one another, bump data corresponding to the input 1805 indicative of the physical contact between the payload requester device 100 and the payload transferor device 150 can be transmitted to the communication interface 140. Upon receiving the bump data corresponding to the input 1805, the communication interface 140 can establish a payload exchange interface 190, such as the payload exchange interface 190 illustrated in FIG. 8.

[0081] The bump request 1805 and bump data corresponding to the input 1805 can further ensure that the payload exchange interface 190 is established for the proper or appropriate devices. For example, the bump request 1805 can require the payload requestor device 100 to be physically located within a same location or within a vicinity of the desired payload transferor device 150, thereby ensuring that the operators of the devices exchanging payloads are familiar with one another or are in each other's presence during the payload exchange. For example, if the payload requester device 100 is used by an operator different from the owner of the payload requester device 100, that operator can attempt to request funds, privacy-sensitive information, or other information from payload transferor device 150, but the operator of the payload transferor device 150 may not know that the payload requester device 100 is being operated by an operator different from the owner of the payload requester device 100, and can therefore create a situation where the non-owner operator can request an unauthorized payload exchange from the payload transferor device 150. In such an instance, the bump request 1805 transmitted by the communication network 140 can require the operators of the payload requester device 100 and the payload transferor device 150 to meet, thereby ensuring that the operator of the payload requester device 100 is authorized or permitted to receive funds, privacy-sensitive information, or other information from payload transferor device 150. Similarly, the confirmation request 1605 and the verification codes 1005, 1305 can prevent unauthorized exchanges of funds, privacy-sensitive information, or other information.

[0082] While the embodiments illustrated in FIGS. 1-18 illustrate one payload requester device 100 and one payload transferor device 150, those of ordinary skill will appreciate that
more than one payload requester device 100 and/or more than one payload transferor device 150 can be included. Additionally, those of ordinary skill in the art will appreciate that the steps, elements, and components described in relation to FIGS. 1-20 can be optionally included and/or combined with the various embodiments illustrated therein to achieve the technical advantages described above for the system and method for recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween.

[0083] The above described and illustrated embodiments provide for systems and methods for recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween, where the payload requester can request for a secured payload exchange interface with a specific payload transferor and the secured payload exchange interface can be established impromptu, on-the-spur-of-moment, spontaneously, or otherwise without substantial preparation for the payload exchange.

[0084] The following disclosure now turns to example embodiments in which the above disclosed system and method of the system and method for recognizing electronic devices for exchanging payloads and permitting payload exchanges therebetween can be implemented. FIG. 19 illustrates a block diagram of an environment 610 wherein an on-demand payload exchange service might be used. Environment 10 may include user systems 612, network 614, system 616, processor system 617, application platform 18, network interface 620, tenant data storage 622, system data storage 624, program code 626, and process space 628. In other embodiments, environment 10 may not have all of the components listed and/or may have other elements instead of, or in addition to, those listed above.

[0085] Environment 610 is an environment in which an on-demand database service exists. User system 612 may be any machine or system that is used by a user to access a database user system. For example, any of user systems 612 can be a handheld computing device, a mobile phone, a laptop computer, a work station, and/or a network of computing devices. As illustrated in FIG. 19 (and in more detail in FIG. 20) user systems 612 might interact via a network 614 with an on-demand database service, which is system 616.

[0086] An on-demand payload exchange interface, such as system 616, is a database system that is made available to outside users that do not need to necessarily be concerned with building and/or maintaining the database system, but instead may be available for their use when the users need the database system (e.g., on the demand of the users). Some on-demand payload exchange
service may store information from one or more tenants stored into tables of a common database image to form a multi-tenant database system (MTS). Accordingly, "on-demand database service 616" and "system 616" will be used interchangeably herein. A database image may include one or more database objects. A relational database management system (RDMS) or the equivalent may execute storage and retrieval of information against the database object(s).

Application platform 618 may be a framework that allows the applications of system 616 to run, such as the hardware and/or software, e.g., the operating system. In an embodiment, on-demand payload exchange service 16 may include an application platform 18 that enables creation, managing and executing one or more applications developed by the provider of the on-demand database service, users accessing the on-demand payload exchange interface via user systems 612, or third party application developers accessing the on-demand database service via user systems 612.

[0087] The users of user systems 612 may differ in their respective capacities, and the capacity of a particular user system 612 might be entirely determined by permissions (permission levels) for the current user. For example, where a salesperson is using a particular user system 612 to interact with system 616, that user system has the capacities allotted to that salesperson. However, while an administrator is using that user system to interact with system 616, that user system has the capacities allotted to that administrator. In systems with a hierarchical role model, users at one permission level may have access to applications, data, and database information accessible by a lower permission level user, but may not have access to certain applications, database information, and data accessible by a user at a higher permission level. Thus, different users will have different capabilities with regard to accessing and modifying application and database information, depending on a user's security or permission level.

[0088] Network 614 is any network or combination of networks of devices that communicate with one another. For example, network 614 can be any one or any combination of a LAN (local area network), WAN (wide area network), telephone network, wireless network, point-to-point network, star network, token ring network, hub network, or other appropriate configuration. As the most common type of computer network in current use is a TCP/IP (Transfer Control Protocol and Internet Protocol) network, such as the global internetwork of networks often referred to as the "Internet" with a capital "I," that network will be used in many of the examples herein. However, it should be understood that the networks that the one or more
implementations might use are not so limited, although TCP/IP is a frequently implemented protocol.

[0089] User systems 612 might communicate with system 616 using TCP/IP and, at a higher network level, use other common Internet protocols to communicate, such as HTTP, FTP, AFS, WAP, etc. In an example where HTTP is used, user system 612 might include an HTTP client commonly referred to as a "browser" for sending and receiving HTTP messages to and from an HTTP server at system 616. Such an HTTP server might be implemented as the sole network interface between system 616 and network 614, but other techniques might be used as well or instead. In some implementations, the interface between system 616 and network 614 includes load sharing functionality, such as round-robin HTTP request distributors to balance loads and distribute incoming HTTP requests evenly over a plurality of servers. At least as for the users that are accessing that server, each of the plurality of servers has access to the MTS' data; however, other alternative configurations may be used instead.

[0090] In one embodiment, system 616, shown in FIG. 19 implements a web-based customer relationship management (CRM) system. For example, in one embodiment, system 616 includes application servers configured to implement and execute CRM software applications as well as provide related data, code, forms, webpages and other information to and from user systems 612 and to store to, and retrieve from, a database system related data, objects, and Webpage content. With a multi-tenant system, data for multiple tenants may be stored in the same physical database object, however, tenant data typically is arranged so that data of one tenant is kept logically separate from that of other tenants so that one tenant does not have access to another tenant's data, unless such data is expressly shared. In certain embodiments, system 616 implements applications other than, or in addition to, a CRM application. For example, system 16 may provide tenant access to multiple hosted (standard and custom) applications, including a CRM application. User (or third party developer) applications, which may or may not include CRM, may be supported by the application platform 618, which manages creation, storage of the applications into one or more database objects and executing of the applications in a virtual machine in the process space of the system 616.

[0091] One arrangement for elements of system 616 is shown in FIG. 19, including a network interface 620, application platform 618, tenant data storage 622 for tenant data 623, system data storage 624 for system data 625 accessible to system 616 and possibly multiple
tenants, program code 626 for implementing various functions of system 616, and a process space 628 for executing MTS system processes and tenant-specific processes, such as running applications as part of an application hosting service. Additional processes that may execute on system 616 include database indexing processes.

[0092] Several elements in the system shown in FIG. 19 include conventional, well-known elements that are explained only briefly here. For example, each user system 612 could include a desktop personal computer, workstation, laptop, PDA, cell phone, or any wireless access protocol (WAP) enabled device or any other computing device capable of interfacing directly or indirectly to the Internet or other network connection. User system 612 typically runs an HTTP client, e.g., a browsing program, such as Microsoft's Internet Explorer browser, Netscape's Navigator browser, Opera's browser, or a WAP-enabled browser in the case of a cell phone, PDA or other wireless device, or the like, allowing a user (e.g., subscriber of the multi-tenant database system) of user system 612 to access, process and view information, pages and applications available to it from system 616 over network 614. Each user system 612 also typically includes one or more user interface devices, such as a keyboard, a mouse, trackball, touch pad, touch screen, pen or the like, for interacting with a graphical user interface (GUI) provided by the browser on a display (e.g., a monitor screen, LCD display, etc.) in conjunction with pages, forms, applications and other information provided by system 616 or other systems or servers. For example, the user interface device can be used to access data and applications hosted by system 616, and to perform searches on stored data, and otherwise allow a user to interact with various GUI pages that may be presented to a user. As discussed above, embodiments are suitable for use with the Internet, which refers to a specific global internetwork of networks. However, it should be understood that other networks can be used instead of the Internet, such as an intranet, an extranet, a virtual private network (VPN), a non-TCP/IP based network, any LAN or WAN or the like.

[0093] According to one embodiment, each user system 612 and all of its components are operator configurable using applications, such as a browser, including computer code run using a central processing unit such as an Intel Pentium® processor or the like. Similarly, system 616 (and additional instances of an MTS, where more than one is present) and all of their components might be operator configurable using application(s) including computer code to run using a central processing unit such as processor system 617, which may include an Intel
Pentium® processor or the like, and/or multiple processor units. A computer program product embodiment includes a machine-readable storage medium (media) having instructions stored thereon/in which can be used to program a computer to perform any of the processes of the embodiments described herein. Computer code for operating and configuring system 16 to intercommunicate and to process webpages, applications and other data and media content as described herein are preferably downloaded and stored on a hard disk, but the entire program code, or portions thereof, may also be stored in any other volatile or non-volatile memory medium or device as is well known, such as a ROM or RAM, or provided on any media capable of storing program code, such as any type of rotating media including floppy disks, optical discs, digital versatile disk (DVD), compact disk (CD), microdrive, and magneto-optical disks, and magnetic or optical cards, nanosystems (including molecular memory ICs), or any type of media or device suitable for storing instructions and/or data. Additionally, the entire program code, or portions thereof, may be transmitted and downloaded from a software source over a transmission medium, e.g., over the Internet, or from another server, as is well known, or transmitted over any other conventional network connection as is well known (e.g., extranet, VPN, LAN, etc.) using any communication medium and protocols (e.g., TCP/IP, HTTP, HTTPS, Ethernet, etc.) as are well known. It will also be appreciated that computer code for implementing embodiments can be implemented in any programming language that can be executed on a client system and/or server or server system such as, for example, C, C++, HTML, any other markup language, Java™, JavaScript, ActiveX, any other scripting language, such as VBScript, and many other programming languages as are well known may be used. (Java™ is a trademark of Sun Microsystems, Inc.).

According to one embodiment, each system 616 is configured to provide webpages, forms, applications, data and media content to user (client) systems 612 to support the access by user systems 612 as tenants of system 616. As such, system 616 provides security mechanisms to keep each tenant's data separate unless the data is shared. If more than one MTS is used, they may be located in close proximity to one another (e.g., in a server farm located in a single building or campus), or they may be distributed at locations remote from one another (e.g., one or more servers located in city A and one or more servers located in city B). As used herein, each MTS could include one or more logically and/or physically connected servers distributed locally or across one or more geographic locations. Additionally, the term "server" is meant to
include a computer system, including processing hardware and process space(s), and an associated storage system and database application (e.g. OODBMS or RDBMS) as is well known in the art. It should also be understood that "server system" and "server" are often used interchangeably herein. Similarly, the database object described herein can be implemented as single databases, a distributed database, a collection of distributed databases, a database with redundant online or offline backups or other redundancies, etc., and might include a distributed database or storage network and associated processing intelligence.

[0095] FIG. 20 also illustrates environment 610. However, in FIG. 20 elements of system 616 and various interconnections in an embodiment are further illustrated. FIG. 20 shows that user system 612 may include processor system 612A, memory system 612B, input system 612C, and output system 612D. FIG. 20 shows network 614 and system 616. FIG. 20 also shows that system 616 may include tenant data storage 622, tenant data 623, system data storage 624, system data 625, User Interface (UI) 730, Application Program Interface (API) 732, PL/SQL 734, save routines 736, application setup mechanism 738, applications servers 10001-1000N, system process space 702, tenant process spaces 704, tenant management process space 710, tenant storage area 712, user storage 714, and application metadata 716. In other embodiments, environment 610 may not have the same elements as those listed above and/or may have other elements instead of, or in addition to, those listed above.

[0096] User system 612, network 614, system 616, tenant data storage 622, and system data storage 624 were discussed above in FIG. 19. Regarding user system 612, processor system 612A may be any combination of one or more processors. Memory system 612B may be any combination of one or more memory devices, short term, and/or long term memory. Input system 612C may be any combination of input devices, such as one or more keyboards, mice, trackballs, scanners, cameras, and/or interfaces to networks. Output system 612D may be any combination of output devices, such as one or more monitors, printers, and/or interfaces to networks. As shown by FIG. 20, system 616 may include a network interface 620 (of FIG. 19) implemented as a set of HTTP application servers 700, an application platform 618, tenant data storage 622, and system data storage 624. Also shown is system process space 702, including individual tenant process spaces 704 and a tenant management process space 710. Each application server 1000 may be configured to tenant data storage 622 and the tenant data 623 therein, and system data storage 624 and the system data 625 therein to serve requests of user systems 612. The tenant
data 623 might be divided into individual tenant storage areas 712, which can be either a physical arrangement and/or a logical arrangement of data. Within each tenant storage area 712, user storage 714 and application metadata 716 might be similarly allocated for each user. For example, a copy of a user's most recently used (MRU) items might be stored to user storage 714. Similarly, a copy of MRU items for an entire organization that is a tenant might be stored to tenant storage area 712. A UI 730 provides a user interface and an API 732 provides an application programmer interface to system 616 resident processes to users and/or developers at user systems 612. The tenant data and the system data may be stored in various databases, such as one or more Oracle™ databases.

[0097] Invocations to applications may be detected by one or more system processes, which manage retrieving application metadata 716 for the subscriber making the invocation and executing the metadata as an application in a virtual machine.

[0098] Each application server 700 may be communicably coupled to database systems, e.g., having access to system data 625 and tenant data 623, via a different network connection. For example, one application server 700i might be coupled via the network 614 (e.g., the Internet), another application server 700N.1 might be coupled via a direct network link, and another application server 700N might be coupled by yet a different network connection. Transfer Control Protocol and Internet Protocol (TCP/IP) are typical protocols for communicating between application servers 700 and the database system. However, it will be apparent to one skilled in the art that other transport protocols may be used to optimize the system depending on the network interconnect used.

[0099] In certain embodiments, each application server 700 is configured to handle requests for any user associated with any organization that is a tenant. Because it is desirable to be able to add and remove application servers from the server pool at any time for any reason, there is preferably no server affinity for a user and/or organization to a specific application server 700. In one embodiment, therefore, an interface system implementing a load balancing function (e.g., an F5 Big-IP load balancer) is communicably coupled between the application servers 700 and the user systems 612 to distribute requests to the application servers 700. In one embodiment, the load balancer uses a least connections algorithm to route user requests to the application servers 700. Other examples of load balancing algorithms, such as round robin and observed response time, also can be used. For example, in certain embodiments, three consecutive requests from the
same user could hit three different application servers 700, and three requests from different users could hit the same application server 700. In this manner, system 616 is multi-tenant, wherein system 616 handles storage of, and access to, different objects, data and applications across disparate users and organizations.

[00100] As an example of storage, one tenant might be a company that employs a sales force where each salesperson uses system 616 to manage their sales process. Thus, a user might maintain contact data, leads data, customer follow-up data, performance data, goals and progress data, etc., all applicable to that user's personal sales process (e.g., in tenant data storage 622). In an example of a MTS arrangement, since all of the data and the applications to access, view, modify, report, transmit, calculate, etc., can be maintained and accessed by a user system having nothing more than network access, the user can manage his or her sales efforts and cycles from any of many different user systems. For example, if a salesperson is visiting a customer and the customer has Internet access in their lobby, the salesperson can obtain critical updates as to that customer while waiting for the customer to arrive in the lobby.

[00101] While each user's data might be separate from other users' data regardless of the employers of each user, some data might be organization-wide data shared or accessible by a plurality of users or all of the users for a given organization that is a tenant. Thus, there might be some data structures managed by system 616 that are allocated at the tenant level while other data structures might be managed at the user level. Because an MTS might support multiple tenants including possible competitors, the MTS should have security protocols that keep data, applications, and application use separate. Also, because many tenants may opt for access to an MTS rather than maintain their own system, redundancy, up-time, and backup are additional functions that may be implemented in the MTS. In addition to user-specific data and tenant specific data, system 616 might also maintain system level data usable by multiple tenants or other data. Such system level data might include industry reports, news, postings, and the like that are sharable among tenants.

[00102] In certain embodiments, user systems 612 (which may be client systems) communicate with application servers 700 to request and update system-level and tenant-level data from system 616 that may require sending one or more queries to tenant data storage 622 and/or system data storage 624. System 616 (e.g., an application server 700 in system 616) automatically generates one or more SQL statements (e.g., one or more SQL queries) that are
designed to access the desired information. System data storage 624 may generate query plans to access the requested data from the database.

[00103] Examples within the scope of the present disclosure may also include tangible and/or non-transitory computer-readable storage media for carrying or having computer-executable instructions or data structures stored thereon. Such non-transitory computer-readable storage media can be any available media that can be accessed by a general purpose or special purpose computer, including the functional design of any special purpose processor as discussed above. By way of example, and not limitation, such non-transitory computer-readable media can include RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code means in the form of computer-executable instructions, data structures, or processor chip design. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or combination thereof) to a computer, the computer properly views the connection as a computer-readable medium. Thus, any such connection is properly termed a computer-readable medium. Combinations of the above should also be included within the scope of the computer-readable media.

[00104] Computer-executable instructions include, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. Computer-executable instructions also include program modules that are executed by computers in stand-alone or network environments. Generally, program modules include routines, programs, components, data structures, objects, and the functions inherent in the design of special-purpose processors, etc. that perform particular tasks or implement particular abstract data types. Computer-executable instructions, associated data structures, and program modules represent examples of the program code means for executing steps of the methods disclosed herein. The particular sequence of such executable instructions or associated data structures represents examples of corresponding acts for implementing the functions described in such steps.

[00105] Those of skill in the art will appreciate that other examples of the disclosure may be practiced in network computing environments with many types of computer system configurations, including personal computers, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers,
mainframe computers, and the like. Examples may also be practiced in distributed computing environments where tasks are performed by local and remote processing devices that are linked (either by hardwired links, wireless links, or by a combination thereof) through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

[00106] The various embodiments described above are provided by way of illustration only and should not be construed to limit the scope of the disclosure. For example, the principles herein apply not only to a smartphone device but to other devices capable of receiving communications such as a laptop computer. Those skilled in the art will readily recognize various modifications and changes that may be made to the principles described herein without following the example embodiments and applications illustrated and described herein, and without departing from the scope of the disclosure.
In the Claims:
What is claimed is:
1. A method comprising:
   receiving (205), from a first device (100), a request to exchange a payload (180) with an available device (150) being located within a predetermined proximity of the first device (100);
   transmit (210), to the available device (150), a confirmation request (1605) in response to receiving the request to exchange the payload (180);
   receiving (215) confirmation data (1610) associated with the available device (150), the confirmation data (1610) being indicative of an acceptance to exchange the payload (180); and
   establishing (220) a payload exchange interface (190) in response to the received request and the received confirmation data.

2. The method of claim 1,
   wherein the available device (150) comprises a plurality of available device; and
   further comprising receiving (310), from the first device (100), an identification (152) of a second device (150) from which to receive the payload (180), the second device (150) being selected from the plurality of available devices.

3. The method of claim 1, further comprising:
   determining the available device (150) is within a predetermined proximity (140) of the first device (100) when the available device is within at least one of a cloud network (140), a peer-to-peer pairing proximity, a near-field-communication pairing proximity, a wireless network, a social network, and a predetermined geographic proximity of the first device.

4. The method as recited in any one of claims 2 or 3, further comprising:
   detecting the plurality of available devices (104); and
   transmitting, to the first device, a list (102) comprising the plurality of available devices (104).

5. The method as recited in claim 4, wherein detecting plurality of available devices (104) comprises:
receiving location data (160) associated with each of the plurality of available devices (104);

comparing the received location data (160) to predetermined criteria associated with the predetermined proximity; and

determining at least one of the available devices (104) is within the predetermined proximity of the first device (100) based at least in part on the respective location data (160) matching at least the predetermined criteria.

6. The method of claim 4 or 5, wherein the list (102) comprises at least one of:

an email address associated with one of the plurality of available devices, a telephone number associated with one of the plurality of available devices, an unique identifier (104) associated with one of the plurality of available devices, an identification number associated with one of the plurality of available devices, and at least a portion of an account number associated with one of the plurality of available devices.

7. The method as recited in any one of claims 1-6 further comprising:

generating a verification code (1005) in response to the request;

transmitting, to the first device (100), the verification code (1005); and

receiving validation data (1010) in response to transmitting the verification code (1005), the validation data (1010) being associated with the second device (150) and corresponding to the verification code (1005) transmitted;

wherein, establishing the payload exchange interface (190) is further based on the verification code (1005) and the validation data (1010).

8. The method as recited in any one of claims 4-6, further comprising receiving a second request to exchange the payload (180) with a second device (150), wherein the second device (150) is not displayed in the list (102).

9. The method as recited in claim 8, further comprising:

in response to receiving the second request to exchange the payload (180) with the second device (150) that is not displayed in the list (102),
generating a verification code (1005) in response to the subsequent request; transmitting, to the first device (100), the verification code (1005); and receiving validation data (1010) in response to transmitting the verification code (1005), the validation data (1010) being associated with the second device (150) and corresponding to the verification code (1005) transmitted; wherein, establishing the payload exchange interface (190) is further based on the verification code (1005) and the validation data (1010).

10. The method as recited in any one of claims 7-9, wherein the verification code (1005) comprises at least one of an alphanumeric code, a pin code (1005), a facial recognition code, a photo recognition code, an audio recognition code, a gesture code (1305), and a voice command.

11. The method as recited in any one of claims 1-10, wherein establishing the payload exchange interface (190) comprises establishing an encrypted network connection.

12. The method as recited in any one of claims 1-11, further comprising:

   transmitting, to at least one of the first device (100) and the second device (150), a bump request for an input (1805) indicative of a physical contact from the second device (150); and receiving bump data, from at least one of the first device (100) and the second device (150), the bump data being indicative of the physical contact from the second device (150); and wherein establishing the payload exchange interface (190) is in response to receiving the bump data.

13. The method as recited in any one of claims 1-12, wherein the payload (180) comprises at least one of a monetary exchange (182), a picture exchange (186), a business card exchange (184), a medical records exchange (185), and a privacy-sensitive document exchange (185).

14. A non-transitory computer readable storage medium storing instructions for controlling a device to perform the steps of the method as recited in any one of claims 1-13.
15. A device comprising:
   a processor; and
   a non-transitory computer readable storage medium storing instructions for controlling
the processor to perform steps of the method recited in any one of claims 1-13.

16. A method comprising:
   transmitting (305), via a first device (100), a request to exchange a payload (180), the
first device (100) being associated with a predetermined proximity;
   identifying (310) a second device (150) to exchange the payload (180), the second device
(150) being located within the predetermined proximity of the first device (100);
   receiving (315) confirmation data corresponding to an establishment of a payload
exchange interface (190) and corresponding to an acceptance (1610) to exchange the payload
(190), the acceptance being associated with the second device (150); and
   exchanging the payload (180) via the payload exchange interface (190).

17. The method as recited in claim 16, further comprising:
   receiving a list (102) of available devices (104) from which the second device (150) can
be selected; and
   wherein, identifying (310) the second device (150) comprises selecting at least one of the
available devices (104) from the list (102) of available devices (104).

18. The method as recited in claim 17, wherein the list (102) of the at least one available devices
comprises at least one of: an email address associated with one of the available devices, a
telephone number associated with one of the available devices, an unique identifier (104)
associated with one of the available devices, an identification number associated with one of the
available devices, an identification number associated with one of the available devices and an
account number associated with one of the available devices.

19. The method as recited in any one of claims 16-18,
   further comprising transmitting location data (110) indicative of a current location of the
first device (100), the predetermined proximity being based at least in part on a predetermined
distance from the current location of the first device (100) associated with the location data (110);
wherein the second device (150) is located within the predetermined distance of the current location of the first device (100).

20. The method as recited in any one of claims 16-19, further comprising:
generating a code (1305) associated with payload (180); and
transmitting the code (1305) to the second device (150);
wherein, the confirmation data further corresponds to a match between the code (1305) transmitted and a received code (1310) associated with the second device (150).

21. The method as recited in any one of claims 16-21, further comprising:
transmitting a code request for a code (1005) to associate with the payload (180); receiving the code (1005) in response to the code request;
transmitting the code (1005) to the second device (150);
wherein, the confirmation data further corresponds to a match between the code (1005) transmitted and a corresponding code (1010) associated with the second device (150).

22. The method as recited in any one of claims 20 or 21, wherein the code (1005, 1305) comprises at least one of an alphanumeric code, a pin code (1005), a facial recognition code, a photo recognition code, an audio recognition code, a gesture code (1305), and a voice command.

23. The method as recited in any one of claims 16-22, wherein the payload exchange interface (190) comprises an encrypted network connection.

24. The method as recited in any one of claims 16-23 further comprising:
receiving a bump request (1705) for a bump input (1805) indicative of a physical contact with the second device (150);
receiving the bump input (1805); and
transmitting bump data associated with the bump input (1805);
wherein receiving the confirmation is in response to transmitting bump data associated
with the bump input indicative of a physical contact with the second device (150).

25. The method as recited in any one of claims 16-24, wherein the payload (180) comprises at
least one of a monetary exchange (182), a picture exchange (186), a business card exchange
(184), a medical records exchange (185), and a privacy-sensitive document exchange (185).

26. A non-transitory computer readable storage medium (115) storing instructions for
controlling a device (100) to perform the method as recited in any one of claims 16-25.

27. A device (100) comprising:
   a processor (105); and
   a non-transitory computer readable storage medium (120) storing instructions for
controlling the processor to perform the method as recited in any one of claims 16-25.

28. A method comprising:
   receiving (405), at a second device (150), a request to exchange a payload (180) with a
first device (150) located within a predetermined proximity to the second device (150), and a
code (1005) associated with the payload (180);
   detecting (410), at the second device (150), an input (1010) corresponding to the code
(1005) received;
   transmitting (415), from the second device (150), data corresponding to the input (1010);
   receiving (420), at the second device (150), confirmation data corresponding to a payload
exchange interface (190) established in response to a verification of the transmitted data
corresponding to the input (1010) detected; and
   transmitting (425), from the second device (150), the payload (180) via the payload
exchange interface (190).

29. The method as recited in any one claims 28, wherein the first device (100) is within a
predetermined proximity of the second device (150) when the first device (100) is within at least
one of a cloud network (140), a peer-to-peer pairing proximity, a near-field-communication pairing proximity, a wireless network, a social network, and a predetermined geographic proximity of the second device (150).

30. The method as recited in any one of claims 28-29, wherein the code (1005) comprises at least one of an alphanumeric code, a pin code (1005), a facial recognition code, a photo recognition code, an audio recognition code, a gesture code (1305), and a voice command.

31. The method as recited in any one of claims 28-30, wherein the payload exchange interface (190) comprises an encrypted network connection.

32. The method as recited in any one of claims 28-31 further comprising:
   receiving a bump request (1705) for a bump input (1805) indicative of a physical contact with the first device (100);
   receiving the bump input (1805); and
   transmitting bump data associated with the bump input (1805);
   wherein receiving the confirmation is in response to transmitting bump data associated with the bump input (1805) indicative of a physical contact with the first device (100).

33. The method as recited in any one of claims 28-32, wherein the payload (180) comprises at least one of a monetary exchange (182), a picture exchange (186), a business card exchange (184), a medical records exchange (185), and a privacy-sensitive document exchange (185).

34. A non-transitory computer readable storage medium (165) storing instructions for controlling a device (150) to perform the method as recited in any one of claims 28-33.

35. A device (150) comprising:
   a processor (155); and
   a non-transitory computer readable storage medium (165) storing instructions for controlling the processor to perform the method as recited in any one of claims 28-33.
receiving, from a first device, a request to exchange a payload with an available device being located within a predetermined proximity of the first device

transmitting, to the available device, a confirmation request in response to receiving the request to exchange the payload

receiving confirmation data associated with the available device, the confirmation data being indicative of an acceptance to exchange the payload

establishing a payload exchange interface in response to the received request and the received confirmation data

**FIG. 2**

transmitting, via a first device, a request to exchange a payload, the first device being associated with a predetermined proximity

Identifying a second device to exchange the payload, the second device being located within the predetermined proximity of the first device

receiving confirmation data corresponding to an establishment of a payload exchange interface and corresponding to an acceptance to exchange the payload, the acceptance being associated with the second device

exchanging the payload via the payload exchange interface

**FIG. 3**
receiving, at a second device, a request to exchange a payload with a first device located within a predetermined proximity to the second device, and a code associated with the payload

detecting, at the second device, an input corresponding to the code received

transmitting, from the second device, data corresponding to the input

receiving, at a second device, confirmation data corresponding to a payload exchange interface established in response to a verification of the transmitted data corresponding to the input detected

transmitting, from the second device, the payload via the payload exchange interface.

FIG. 4
FIG. 19
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

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) - H04L 27/00; H04W 4/00; 4/24 (2012.01)
USPC - 455/414.1, 426.1; 705/44

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

MicroPatent; Google Patents; Google Scholar

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category*</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
</table>

* 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
   "S" 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
   "Y" 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
   "r" 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: 14 May 2012
Date of mailing of the international search report: 23 May 2012

Name and mailing address of the ISA/US: Blaine R. Copenhaver
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Authorized officer: PCT Helpdesk: 571-272-4300
PCTOSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)
INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/024549

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1.☐ Claims Nos.:
   because they relate to subject matter not required to be searched by this Authority, namely:

2.☐ Claims Nos.:
   because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

   because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1.☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2.☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3.☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4.☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
☐ No protest accompanied the payment of additional search fees.