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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 May 2017 (18.05.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/082969 A1

(51) International Patent Classification:
G06F 7/04 (2006.01) *G06F 17/30* (2006.01)
G06F 15/16 (2006.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/US2016/038592

(22) International Filing Date:
22 June 2016 (22.06.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/254,229 12 November 2015 (12.11.2015) US
15/084,969 30 March 2016 (30.03.2016) US

(71) Applicant: **FINJAN MOBILE, INC.** [US/US]; 2000 University Avenue, East Palo Alto, California 94303 (US).

(72) Inventors: **KREMER, Alexander Lin**; 2810 Alvarado Avenue, San Mateo, California 94403 (US). **HOUSE, Geoffrey**; 413 Capp Street, San Francisco, California 94110 (US). **MCDOLE, Lee**; 528 66th Street, Apartment #3, Oakland, California 94609 (US). **GODLEWSKI, Michael**; 413 Capp Street, San Francisco, California 94110 (US). **MUTTER, Rudolph**; 349 El Camino Real, Apartment #1, Millbrae, California 94030 (US). **SHIPMAN, Timothy**; 1112 Larkin Street, Apartment #205, San Francisco, California 94109 (US). **PANOPOULOS, Jules**; 400 El Camino Real, Apartment #519, Mountain View, California 94040 (US).

(74) Agent: **BERGER, Marc**; SOQUEL GROUP I.P Ltd, 43A Gordon Street, 7628707 Rehovot (IL).

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

[Continued on next page]

(54) Title: AUTHORIZED AREAS OF AUTHENTICATION

(57) Abstract: A secure access system, including a stationary computing device that controls access to secure data over a secure network, including an authorized area of authentication (AAA) generator, generating an AAA for administering the secure data, an AAA validator, validating a mobile computing device that a request to access the secure data over the secure network, by verifying that a current location of the mobile device is within the AAA, and an access controller, enabling the mobile device to access the secure data, only in response to the validator affirmatively validating the mobile device, and a mobile computing device including a location identifier, dynamically identifying a current location of the mobile device, a connection controller for logging into the secure network, and an access requestor, submitting to the access controller via the secure network (i) an access request for the secure data, and (ii) the current location of the mobile device.

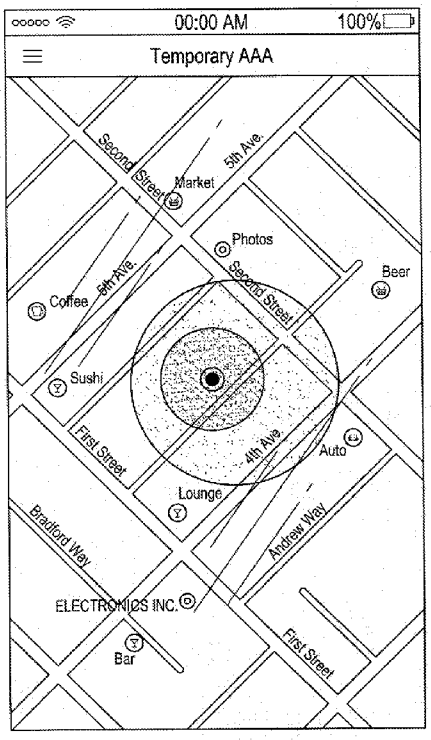


FIG. 9

WO 2017/082969 A1

SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

AUTHORIZED AREAS OF AUTHENTICATION

PRIORITY REFERENCES

[0001] This application claims benefit of and hereby incorporates by reference US Provisional Application No. 62/254,229, entitled METHOD AND SYSTEM USING GEO-LOCATION DATA AND INFORMATION FOR ADDED LAYER OF SECURITY, and filed on November 12, 2015 by inventors Alex Lin, Geoff House, Lee McDole, Michael Godlewski, Rudolph Mutter, Timothy Shipman and Jules Panopoulos.

[0002] This application also claims benefit of and hereby incorporates by reference US Patent Application No. 15/084,969, entitled AUTHORIZED AREAS OF AUTHENTICATION, and filed on March 30, 2016 by inventors Alexander Lin Kremer, Geoffrey House, Lee McDole, Michael Godlewski, Rudolph Mutter, Timothy Shipman and Jules Panopoulos.

FIELD OF THE INVENTION

[0004] The present invention relates to computer data security.

BACKGROUND OF THE INVENTION

[0005] Enterprises store sensitive and private company and customer data on secure file servers. As users become more mobile, it is becoming common for users to remotely access files on these file servers via their mobile computing devices. Typically, a user can login to an enterprise file server using a basic user ID and password, over a secure network such as a virtual private network. This is a relatively weak form of security, and data breaches often occur where sensitive data is accessed and used by unauthorized people.

[0006] As such, it would be of great advantage to provide an additional layer of security for remote access to file servers via mobile devices.

SUMMARY

[0007] Embodiments of the present invention provide modules, systems and methods for an additional layer of security for remote access to file servers via mobile devices of authorized users. Access to a file server is granted only if a mobile device is verified to be located within an authorized area of authentication (AAA). If the mobile device is not within the AAA, a temporary AAA, including the current location of the mobile device, may be authorized.

[0008] There is thus provided in accordance with an embodiment of the present invention a system for secure access, including a stationary computing device that controls access to secure data over a secure network, including an AAA generator, generating an AAA for administering the secure data, an AAA validator, validating a mobile computing device that submits an access request for the secure data via a connection over the secure network, by verifying that a current location of the mobile device is within the AAA, and an access controller, enabling the mobile device to access the secure data, only in response to the validator affirmatively validating the mobile device, and a mobile computing device in communication with the stationary device, including a location identifier, dynamically identifying a current location of the mobile device, a connection controller for logging in to and out of the secure network, and an access requestor, submitting to the access controller via the secure network (i) an access request for the secure data, and (ii) the current location of the mobile device.

[0009] There is additionally provided in accordance with an embodiment of the present invention a secure access server computer, including an authorized area of authentication (AAA) generator, generating an AAA for

administering secure data, access to which is controlled by the server over a secure network, an AAA validator, validating a mobile device that submits an access request for the secure data via a connection over the secure network, by verifying that a current location of the mobile device is within the AAA; and an access controller, enabling the mobile device to access the secure data over the secure network only in response to the AAA validator affirmatively validating the mobile device.

[0010] There is further provided in accordance with an embodiment of the present invention a mobile device for accessing secure data, including a location identifier, dynamically identifying a current location of the mobile device, a connection controller logging in to and out of a secure network, and an access requestor, submitting to a server computer via a connection over the secure network, both (i) an access request for secure data, access to which is controlled by the server, and (ii) the current location of the mobile device, wherein the server enables access to the secure data only when the current location of the mobile device is within an authorized area of authentication.

[0011] There is yet further provided in accordance with an embodiment of the present invention a method for secure access, including generating, by a stationary computing device, an authorized area of authentication (AAA) for administering secure data, access to which is controlled by the stationary device over a secure network, submitting, by a mobile computing device to the stationary device via a connection over a secure network, a request to access the secure data, further submitting, by the mobile device to the stationary device, a current location of the mobile device, validating, by the stationary device, the mobile device, including verifying that the current location of the mobile device is within the AAA,

and granting the mobile device access to the secure data, only in response to the validating being affirmative.

[0012] There is moreover provided in accordance with an embodiment of the present invention a method for a secure access server, including generating an authorized area of authentication (AAA), for administering secure data, access to which is controlled by a server computer over a secure network, receiving, from a mobile computing device via a connection over the secure network, a request to access the secure data, further receiving, from the mobile device over the secure network, a current location of the mobile device, validating the mobile device, comprising verifying that the current location of the mobile device is within the AAA, and enabling the mobile device to access to the secure data, only in response to the validating being affirmative.

[0013] There is additionally provided in accordance with an embodiment of the present invention a method for secure access by a mobile computer device, including identifying a current location of a mobile computing device, submitting, to a server computer via a connection over a secure network, a request to access secure data, access to which is controlled by the server, further submitting to the server over the secure network, the current location, and only when the current location is within an authorized area of authentication (AAA) for the server, receiving, from the server, an enablement to access the secure data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] The present invention will be more fully understood and appreciated from the following detailed description, taken in conjunction with the drawings in which:

[0016] **FIG. 1** is a simplified block diagram of a system for secure access, in accordance with an embodiment of the present invention;

[0017] **FIG. 2** is a simplified flowchart of a method for secure access, in accordance with an embodiment of the present invention;

[0018] **FIG. 3** is a screen shot of a mobile device prompting a user for his username and password for logging in to a secure network, and acquiring the user's current location, in accordance with an embodiment of the present invention;

[0019] **FIG. 4** is a screen shot showing the user's current location on a map, in accordance with an embodiment of the present invention;

[0020] **FIG. 5** is a screen shot showing the mobile device logging in to the secure network with the username and password, and with the user's current location, in accordance with an embodiment of the present invention;

[0021] **FIG. 6** is a screen shot showing the mobile device informing that user that he is located in an unauthorized area, and prompting the user to request a temporary authorized area of authentication (AAA), in accordance with an embodiment of the present invention; and

[0022] **FIG. 7** is a screenshot showing an area centered about the user's current location, in accordance with an embodiment of the present invention;

[0023] **FIG. 8** is a screen shot showing fingerprint identification prior to setting a temporary AAA, in accordance with an embodiment of the present invention;

[0024] **FIG. 9** is a screen shot showing that a temporary AAA has been set for the user, in accordance with an embodiment of the present invention;

[0025] **FIG. 10** is a screen shot of the user logging out of the secure network, in accordance with an embodiment of the present invention;

[0026] **FIG. 11** is a screen shot showing an exemplary log report for an administrator, generated by an access log recorder, in accordance with an embodiment of the present invention;

[0027] **FIG. 12** is a screen shot of a temporary AAA being reported to an the administrator, in accordance with an embodiment of the present invention; and

[0028] **FIG. 13** is a screen shot showing an exemplary log report generated for an administrator, by an access log recorder, in accordance with an embodiment of the present invention.

[0029] For reference to the figures, the following index of elements and their numerals is provided. Similarly numbered elements represent elements of the same type, but they need not be identical elements.

Table of elements in the figures	
Element	**Description**
100	stationary computing device
110	processor
120	AAA generator
130	AAA validator
140	AAA access controller
150	organization file server
160	organization administrator computer
170	access log recorder
200	mobile computing device
210	processor
220	location identifier
230	connection controller
240	access requestor
250	biometric / passcode scanner
260	biometric / passcode validator

[0030] Elements numbered in the **1000**'s are operations of flow charts.

DETAILED DESCRIPTION

[0031] In accordance with embodiments of the present invention, modules, systems and methods are provided for an additional layer of security for remote access to file servers via mobile devices. These modules, systems and methods are implemented using computing systems including inter alia servers, clients, network devices, and combinations of such devices.

[0032] Reference is made to **FIG. 1**, which is a simplified block diagram of a system for secure access, in accordance with an embodiment of the present invention. **FIG. 1** shows a stationary computing device **100** and a mobile computing device **200**. Stationary device **100** controls access to an organization's file server **150** that stores secure data. More generally, file server **150** represents any type of server that allows one or more users of mobile devices to access content of the organization.

[0033] Access to file server **150** via stationary device **100** is managed by an administrator computer **160**. File server **150** is remotely accessible over a secure network, such as a virtual private network (VPN). An access log recorder **170** logs each access to file server **150** and each attempt to access file server **150**, and report the logs to administrator **160**.

[0034] Stationary device **100** may be inter alia a server, a network device, and a combination of such devices. Administrator **160** may be a desktop computer, a laptop computer, a network device, or such other computing device. Administrator **160** manages user accounts and their associated remote devices. In accordance with an embodiment of the present invention, each user and account must be authorized by stationary device **100** before a user may access files on file server **150**.

[0035] Stationary device **100** includes a processor **110**, an authorized area of authentication (AAA) generator **120**, an AAA validator **130**, and an AAA access controller **140**. An "*authorized area of authentication*" is one or more geographic areas that provide an additional layer of security to supplement conventional user authentication credentials such as username and password. In order to access file server **150**, a user must be authenticated by his current location, in additional to conventional authentication. If the user is not located in an AAA, then his access to file server **150** is denied. The user may request a temporary authentication, as explained in detail below, but otherwise he is not granted access.

[0036] In alternative embodiments of the present invention, one or more of AAA generator **120**, AAA validator **130**, and AAA access controller **140** reside in administrator **160** instead of stationary device **100**.

[0037] Use of AAA is of particular advantage when an organization has mobile users, with mobile computing devices **200** that include a processor **210** and a location identifier **220**, such as inter alia a GPS tracker or an agent that provides location data, that dynamically determines a device's current geographic location. By transmitting an identifier of the location to stationary device **100**, AAA validator **130** is able to determine whether or not a user of mobile device **200** is located in an AAA. Mobile device **200** also includes a connection controller **230**, for connection to stationary device **100** and to file server **150** over a secure network, and an access requestor **240** for requesting temporary authentication. Regarding the secure network, mobile device **200** may be inter alia on a VPN connection with stationary device **100** and file server **150**. Stationary device **100** and file server **150** may be on that same secure network as well.

[0038] Mobile device **200** also includes a biometric/passcode scanner **250**, which scans a biometric, such as a fingerprint or an iris, or scans a passcode, such as a PIN, of a user who is currently using mobile device **200**; and a biometric/passcode validator **260**, which validates the user's biometric/passcode that was scanned by scanner **250**.

[0039] Operation of the various components of stationary device **100** and mobile device **200** is described below with regards to **FIGS. 2 – 13**.

[0040] Mobile device **200** may be inter alia a smartphone, a tablet computer, a laptop computer and such other remote access device. Stationary device **100**, file server **150**, administrator **160** and mobile device **200** are not limited to any particular operating system. Administrator **160** and mobile device **200** may each be implemented inter alia using an application program interface (API) that communicates with stationary device **100**.

[0041] Reference is made to **FIG. 2**, which is a simplified flowchart of a method **1000** for secure access, in accordance with an embodiment of the present invention. The flowchart of **FIG. 2** is divided into two columns. The left column includes operations performed by stationary device **100**, and the right column includes operations performed by mobile device **200**. At operation **1005** AAA generator **120** generates an AAA for accessing an organization's secure data stored on file server **150**. The AAA is set by an organization administrator **160**, and includes one or more geographical areas. E.g., the AAA may include various office locations of the organization, and various home locations of employees who work for the organization from their homes. Individual AAAs may be set up by AAA generator **120** for different users on a per-user basis, for different groups of users on a per-group basis, or for an entire enterprise.

In an alternative embodiment of the present invention, AAA **120**, which performs operation **1005**, is a component of administrator **160** instead of stationary device **100**.

[0042] At operation **1010** connection controller **230** attempts to log in to a secure network of the organization, such as a virtual private network (VPN), to access file server **150**. At operation **1015** the user presents his credentials, such as username and password, for authentication. At operation **1020** the user's current location is identified by location identifier **220**, and submitted to AAA validator **130**. Reference is made to **FIG. 3**, which is a screen shot of mobile device **200** prompting a user for his username and password for logging in to the secure network, and acquiring the user's current location, in accordance with an embodiment of the present invention. Reference is made to **FIG. 4**, which is a screen shot showing the user's current location on a map, in accordance with an embodiment of the present invention. **FIG. 4** shows the user being located within a circular area between First and Second Street and between 4th and 5th Avenue. Reference is made to **FIG. 5**, which is a screen shot showing mobile device **200** logging in to the secure network with the username and password, and with the user's current location, in accordance with an embodiment of the present invention.

[0043] At operation **1025**, AAA validator **130** authenticates mobile device **200** by checking credentials such as username and password. AAA validator **130** also verifies that the location submitted at operation **1020** is within an AAA that was generated at operation **1005**. At decision **1030**, AAA validator **130** decides whether or not the authentication at operation **1025** is verified. If so, then at operation **1035** mobile device **200** is granted access to file server **150**, and mobile

device **200** is then enabled to access file server **150** such as via SSH FTP. Otherwise, if authentication is not verified at decision **1030**, then at operation **1040** mobile device **200** is denied access to file server **150**. In either case, the grant of or denial of access is logged by access log recorder **170** at operation **1045**, for reporting to administrator **160**.

[0044] When access to file server **150** is denied at operation **1040** because mobile device **200** is not within an AAA, then at operation **1050** the user of mobile device **200** requests AAA access controller **140** to instantiate a temporary AAA that includes the current location of mobile device **200**, so that the user can temporarily access file server **150**. Reference is made to **FIG. 6**, which is a screen shot showing mobile device **200** informing the user that he is located in an unauthorized area, and prompting the user to request a temporary AAA, in accordance with an embodiment of the present invention. Reference is made to **FIG. 7**, which is a screenshot showing an area centered about the user's current location, in accordance with an embodiment of the present invention.

[0045] At operation **1055**, biometric/passcode scanner **250** scans a biometric, such as inter alia a fingerprint or iris, of a user who is currently using mobile device **200**, or a passcode, such as inter alia a PIN code, for the user. At operation **1060**, biometric/passcode validator **260** validates the identity of the user, based on the user's scanned biometric/passcode, to ensure that the user who is currently using mobile device **200** is indeed authorized to use mobile device 200 and request a temporary AAA. Reference is made to **FIG. 8**, which is a screen shot showing fingerprint identification prior to setting a temporary AAA, in accordance with an embodiment of the present invention.

[0046] At decision **1065**, mobile device **200** decides whether or not the validation at operation **1060** is affirmative. If not, then at operation **1070** the request for the temporary AAA is denied, and the user is denied access to file server **150**. Denial of access is then logged by access log recorder **170** at operation **1045**, for reporting to administrator **160**. Otherwise, if decision **1065** decides that the validation is affirmative, then at operation **1075** the request for the temporary AAA is submitted to stationary device **200**, and at operation **1080** AAA access controller **140** sets a temporary AAA for the user, at his current location. Reference is made to **FIG. 9**, which is a screen shot showing that a temporary AAA has been set for the user, in accordance with an embodiment of the present invention. At operation **1035** mobile device **200** is granted access to file server **150**, and mobile device **200** is then enabled to access file server **150** such as via SSH FTP. Access to file server **150** via the temporary AAA is logged by access log recorder **170** at operation **1045**, for reporting to administrator **160**.

[0047] After completion of the user's access to file server **1050**, the user logs out and the temporary AAA is canceled. Reference is made to **FIG. 10**, which is a screen shot of the user logging out of the secure network by use of a side-bar menu, in accordance with an embodiment of the present invention. Alternatively, the temporary AAA may expire after a designated time period.

[0048] There are many variations for division of processing labor between stationary device **100**, administrator **160** and mobile device **200**, all of which are contemplated by the present invention. Thus inter alia, referring to **FIG. 2**, operations **1060** – **1075**, relating to validating the identity of the user via fingerprint or such other biometric, or via

passcode or via another PIN-based mechanism, may be performed by stationary device **100** or alternatively by administrator **160**, instead of mobile device **200**. In such case, mobile device **200** transmits the scanned biometric/passcode to stationary device **100** or administrator **160** after performing operation **1055**, and stationary device **100** or administrator **160** performs the validation, and the denial or grant of access.

[0049] Reference is made to **FIG. 11**, which is a screen shot showing an exemplary log report generated by access log recorder **170** for administrator **160**, in accordance with an embodiment of the present invention. The log report lists authorized logins to file server **160** and unauthorized logins that were blocked, with dates and times, according to username.

[0050] Reference is made to **FIG. 12**, which is a screen shot of a temporary AAA being reported to administrator **160**, in accordance with an embodiment of the present invention.

[0051] Reference is made to **FIG. 13**, which is a screen shot showing an exemplary log report generated by access log recorder **170** for administrator **160**, in accordance with an embodiment of the present invention. Valid user logins are indicated with a check mark, and invalid login attempts are indicated with a dash. The log report identifies locations, including latitude and longitude and addresses of users who logged into file server **150** and attempted to login to file server **150**, according to dates and times.

[0052] It will thus be appreciated that embodiments of the present invention provide modules, systems and methods for data security

whereby a remote device is granted access to a file server only when it is currently located in an authorized area of authentication.

Implementation Details

[0053] In an embodiment of the subject invention in accordance with the Django Python web framework, an AAA is modeled by the following class definition and table.

```
# AAA
class Location(CoreModel):
       name = models.CharField(max_length=125, blank=True,
null=True)
       status =
models.PositiveSmallIntegerField(choices=LOCATION_STATUS,
default=LOCATION_STATUS.temporary)
       latitude = models.FloatField()
       longitude = models.FloatField()
       radius = models.FloatField(help_text="(meters)")
       address = models.CharField(max_length=500,blank=True,
null=True)
       enabled = models.BooleanField(default=True)
       # required for temporary AAA
       user = models.ForeignKey(User, related_name="temporary
locations", blank=True, null=True)
       temp_start_time = models.DateTimeField(blank=True,
null=True)
       temp_end_time = models.DateTimeField(blank=True,
null=True)
```

Table "public.users_location"		
Column	Type	Modifiers
id	integer	not null default nextval('users_location_id_seq'::regclass)
created	timestamp with time zone	
name	character varying(125)	not null
latitude	double precision	not null
longitude	double precision	not null
radius	double precision	not null
address	character varying(500)	
status	smallint	not null
user_id	integer	
temp_end_time	timestamp with time zone	
temp_start_time	timestamp with time zone	
enabled	boolean	not null

[0054] In an embodiment of the subject invention in accordance with the Django Python web framework, an access attempt is modeled by the following class definition and table.

```
class Access (CoreModel):
        user = models.CharField(max_length=125, blank=True,
null-True)
        latitude = models.FloatField()
        longitude = models.FloatField()
        trust_level =
models.PositiveSmallIntegerField(choices=TRUST_LEVELS)
        allowed = models.BooleanField(default=False)
        authorized_location = models.ForeignKey(Location,
related_name="authorized_logins"), blank=True, null=True)
        unauthorized_location =
models.CharField(max_length=500, blank=True, null=True)
```

Table "public.users_access"		
Column	Type	Modifiers
id	integer	not null default nextval('users_access_id_seq'::regclass)
created	timestamp with time zone	
latitude	double precision	not null
longitude	double precision	not null
trust_level	smallint	not null
allowed	boolean	not null
authorized_location_id	integer	
unauthorized location	character varying(500)	
user_id	integer	not null

[0055] In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made to the specific exemplary embodiments without departing from the broader spirit and scope of the invention. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A secure access server computer, comprising:

an authorized area of authentication (AAA) generator, generating an AAA for administering secure data, access to which is controlled by the server over a secure network;

an AAA validator, validating a mobile device that submits an access request for the secure data via a connection over the secure network, by verifying that a current location of the mobile device is within the AAA; and

an access controller, enabling the mobile device to access the secure data over the secure network only in response to said AAA validator affirmatively validating the mobile device.

2. The server of claim **1** further comprising an AAA approver approving a request from the mobile device to generate a temporary AAA that includes a current location of the mobile device.

3. The server of claim **2** wherein said AAA generator generates the temporary AAA and monitors the temporary AAA so as to expire after a specified time.

4 The server of claim **2** wherein said AAA generator generates the temporary AAA and monitors the temporary AAA so as to expire after the mobile device closes its connection with the secure network.

5. A mobile device for accessing secure data, comprising:

a location identifier, dynamically identifying a current location of the mobile device;

a connection controller logging in to and out of a secure network; and

an access requestor, submitting to a server computer via a connection over the secure network, both (i) an access request for secure data, access to which is controlled by the server, and (ii) the current location of the mobile device,

wherein the server enables access to the secure data only when the current location of the mobile device is within an authorized area of authentication (AAA).

6. The mobile device of claim **5** wherein said access requestor submits to the server over the secure network a request that the server generate a temporary AAA that includes the current location of the mobile device, when the current location of the mobile device is not within an existing AAA.

7. The mobile device of claim **6**, further comprising:

a biometric or passcode scanner, scanning a biometric or passcode of a user who is currently using the mobile device; and

a biometric or passcode validator, validating the biometric data or passcode scanned by said biometric or passcode scanner,

and wherein said access requestor submits to the server the request that the server generate a temporary AAA only in response to said biometric

or passcode validator affirmatively validating the user's biometric or passcode.

8. A method for a secure access server, comprising:

generating an authorized area of authentication (AAA), for administering secure data, access to which is controlled by a server computer over a secure network;

receiving, from a mobile computing device via a connection over the secure network, a request to access the secure data;

further receiving, from the mobile device over the secure network, a current location of the mobile device;

validating the mobile device, comprising verifying that the current location of the mobile device is within the AAA; and

enabling the mobile device to access to the secure data, only in response to said validating being affirmative.

9. The method of claim **8**, further comprising:

receiving, from the mobile device over the secure network, a request for a temporary AAA that includes the current location of the mobile device;

determining whether or not to approve the request for the temporary AAA; and

generating a temporary AAA that includes the current location of the mobile device, only in response to said determining being affirmative.

10. The method of claim **9** further comprising monitoring the temporary AAA so as to expire after a specified time.

11. The method of claim **9** further comprising monitoring the temporary AAA so as to expire after the mobile device logs out of the secure network.

12. A method for secure access by a mobile computer device, comprising:

identifying a current location of a mobile computing device;

submitting, to a server computer via a connection over a secure network, a request to access secure data, access to which is controlled by the server;

further submitting to the server over the secure network, the current location; and

only when the current location is within an authorized area of authentication (AAA) for the server, receiving, from the server, an enablement to access the secure data.

13. The method of claim **12**, further comprising submitting, to the server over the secure network, a request for a temporary AAA that includes the current location, when the current location is not within an existing AAA.

14. The method of claim **13** further comprising:

scanning a biometric or passcode of a user who is currently using said mobile device; and

validating the biometric data or passcode scanned by said scanning,

wherein said submitting the request for a temporary AAA is contingent upon said validating being affirmative.

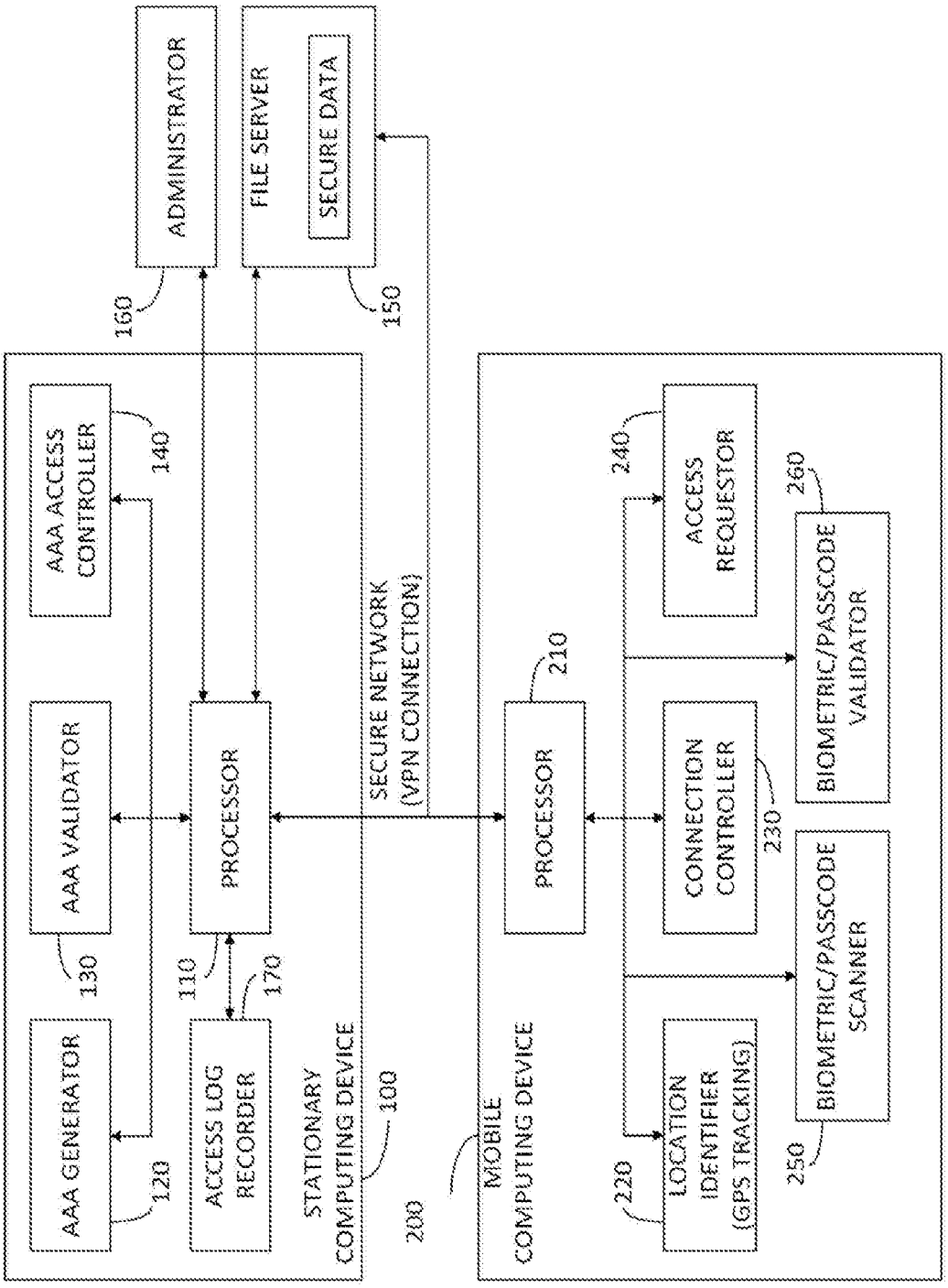

ADMINISTRATOR
160
FILE SERVER
SECURE DATA
150
AAA ACCESS CONTROLLER
140
AAA VALIDATOR
130
PROCESSOR
110
ACCESS LOG RECORDER
170
AAA GENERATOR
120
STATIONARY COMPUTING DEVICE
100
SECURE NETWORK (VPN CONNECTION)
200
PROCESSOR
210
ACCESS REQUESTOR
240
CONNECTION CONTROLLER
230
LOCATION IDENTIFIER (GPS TRACKING)
220
BIOMETRIC/PASSCODE VALIDATOR
260
BIOMETRIC/PASSCODE SCANNER
250
MOBILE COMPUTING DEVICE

FIG. 1

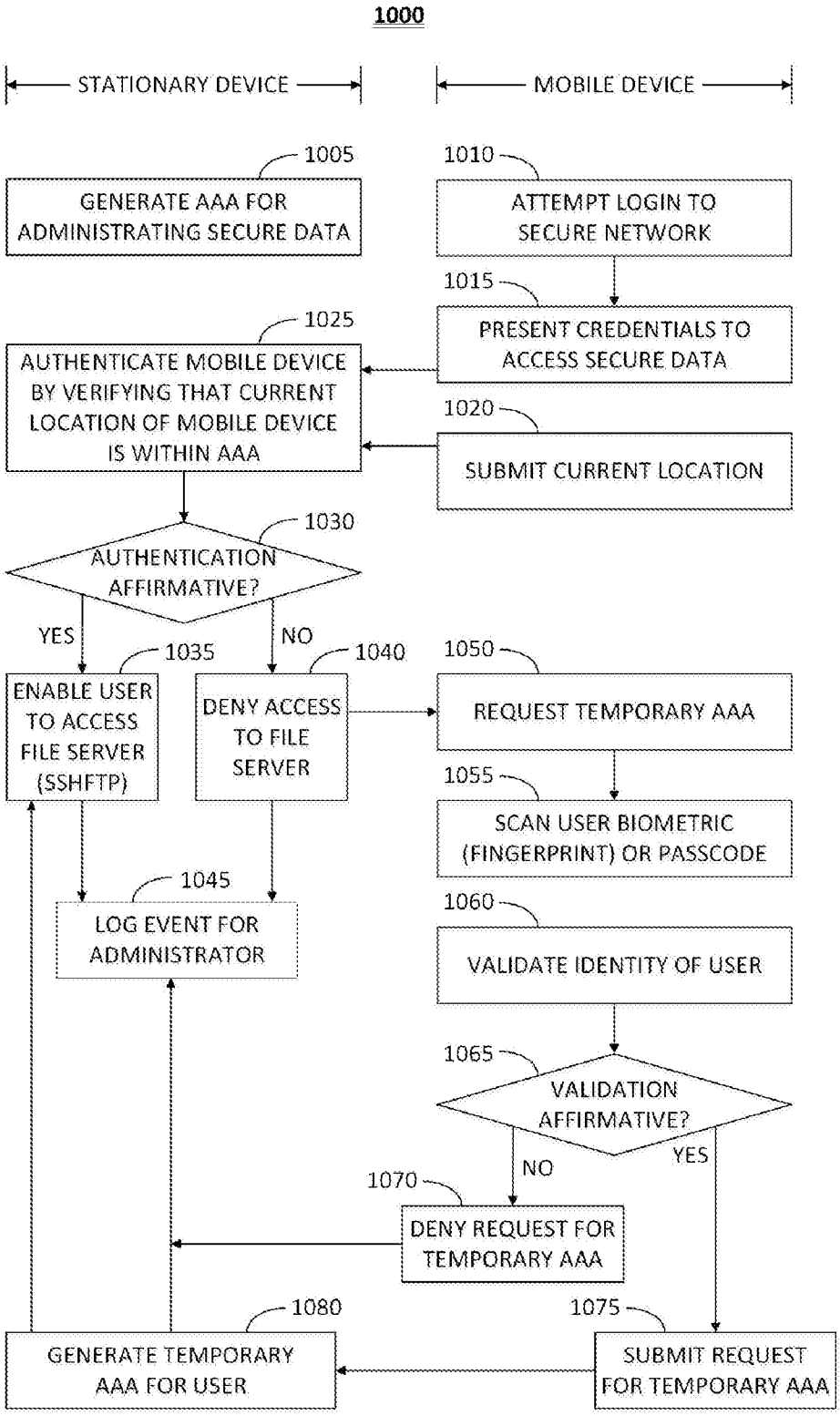

1000
STATIONARY DEVICE
MOBILE DEVICE
1005
GENERATE AAA FOR ADMINISTRATING SECURE DATA
1010
ATTEMPT LOGIN TO SECURE NETWORK
1015
PRESENT CREDENTIALS TO ACCESS SECURE DATA
1025
AUTHENTICATE MOBILE DEVICE BY VERIFYING THAT CURRENT LOCATION OF MOBILE DEVICE IS WITHIN AAA
1020
SUBMIT CURRENT LOCATION
1030
AUTHENTICATION AFFIRMATIVE?
YES
NO
1035
ENABLE USER TO ACCESS FILE SERVER (SSHFTP)
1040
DENY ACCESS TO FILE SERVER
1050
REQUEST TEMPORARY AAA
1055
SCAN USER BIOMETRIC (FINGERPRINT) OR PASSCODE
1045
LOG EVENT FOR ADMINISTRATOR
1060
VALIDATE IDENTITY OF USER
1065
VALIDATION AFFIRMATIVE?
NO
YES
1070
DENY REQUEST FOR TEMPORARY AAA
1080
GENERATE TEMPORARY AAA FOR USER
1075
SUBMIT REQUEST FOR TEMPORARY AAA

FIG. 2

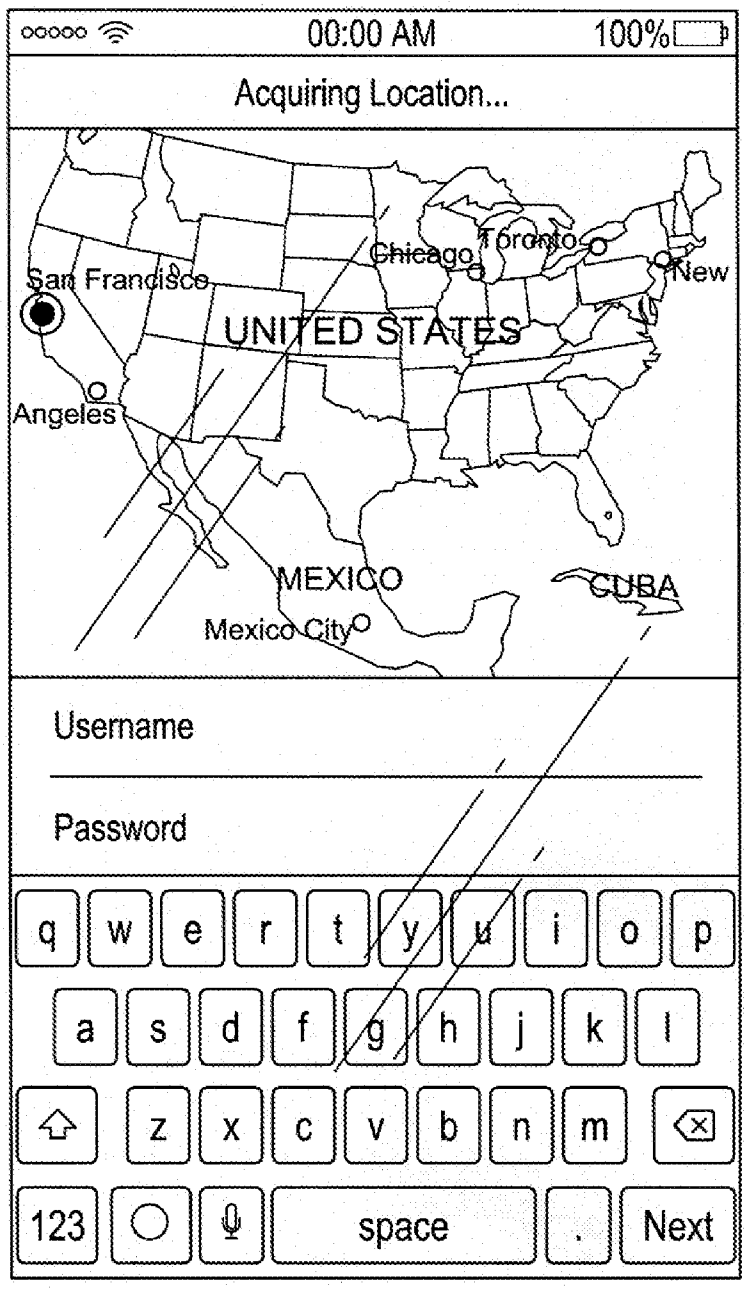

00:00 AM
100%
Acquiring Location...
Chicago
Toronto
New
San Francisco
UNITED STATES
Angeles
MEXICO
CUBA
Mexico City
Username
Password
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
.
Next

FIG. 3

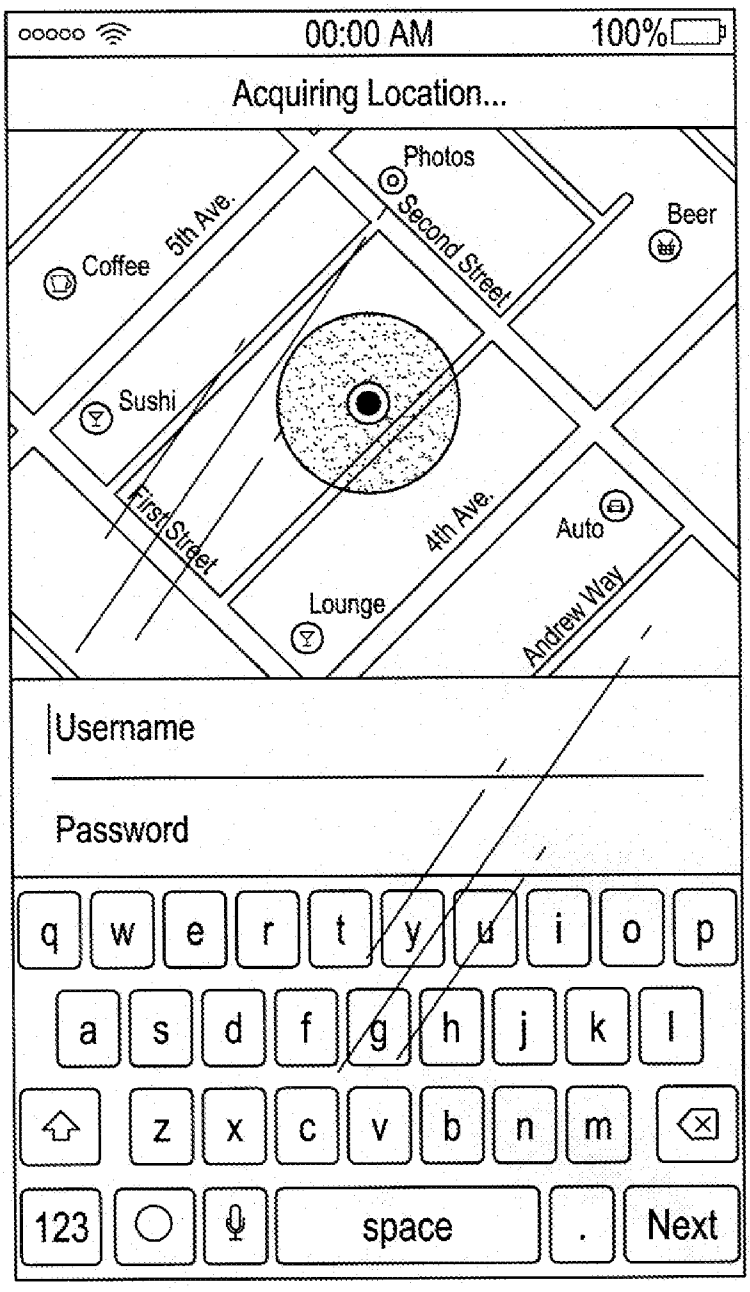

00:00 AM
100%
Acquiring Location...
Photos
Second Street
Beer
5th Ave.
Coffee
Sushi
First Street
4th Ave.
Auto
Lounge
Andrew Way
Username
Password
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
.
Next

FIG. 4

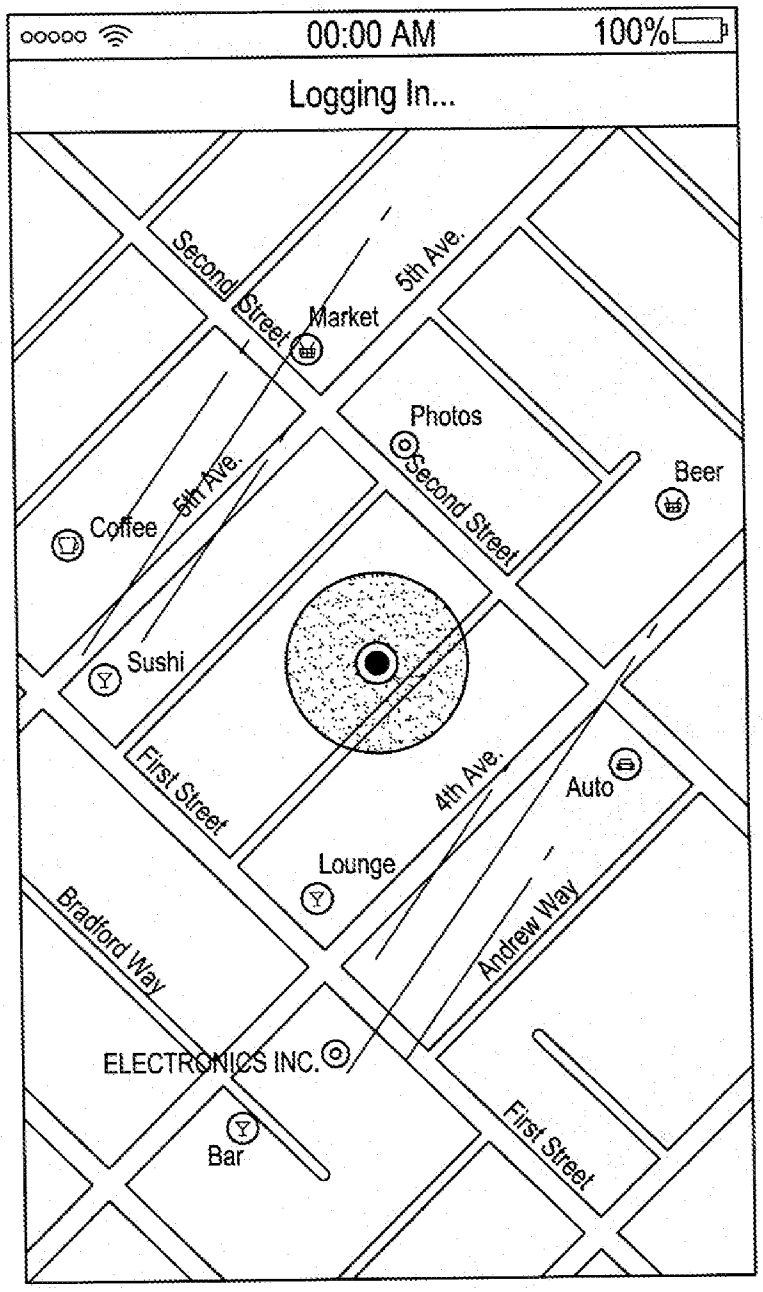

00:00 AM
100%
Logging In...
Second Street
5th Ave.
Market
Photos
Second Street
Beer
5th Ave.
Coffee
Sushi
First Street
4th Ave.
Auto
Lounge
Bradford Way
Andrew Way
ELECTRONICS INC.
Bar
First Street

FIG. 5

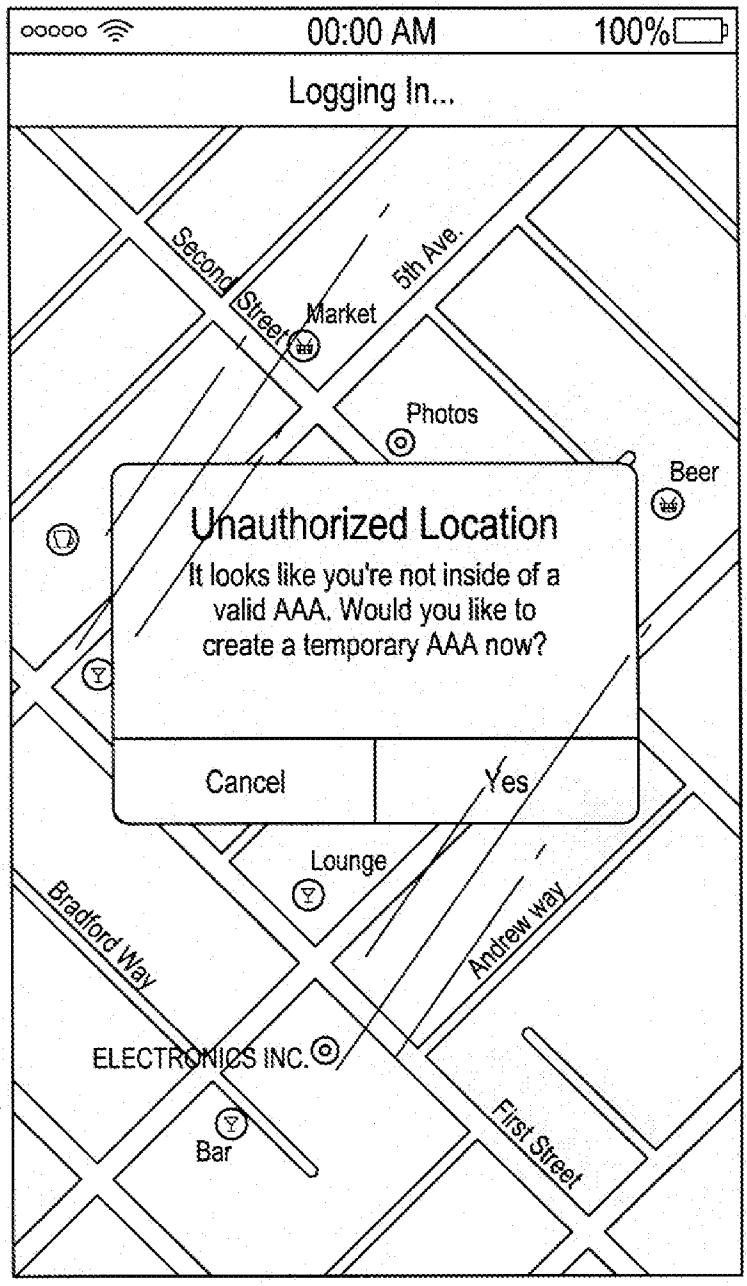

00:00 AM
100%
Logging In...
Second Street
5th Ave.
Market
Photos
Beer
Unauthorized Location
It looks like you're not inside of a valid AAA. Would you like to create a temporary AAA now?
Cancel
Yes
Lounge
Bradford Way
Andrew Way
ELECTRONICS INC.
Bar
First Street

FIG. 6

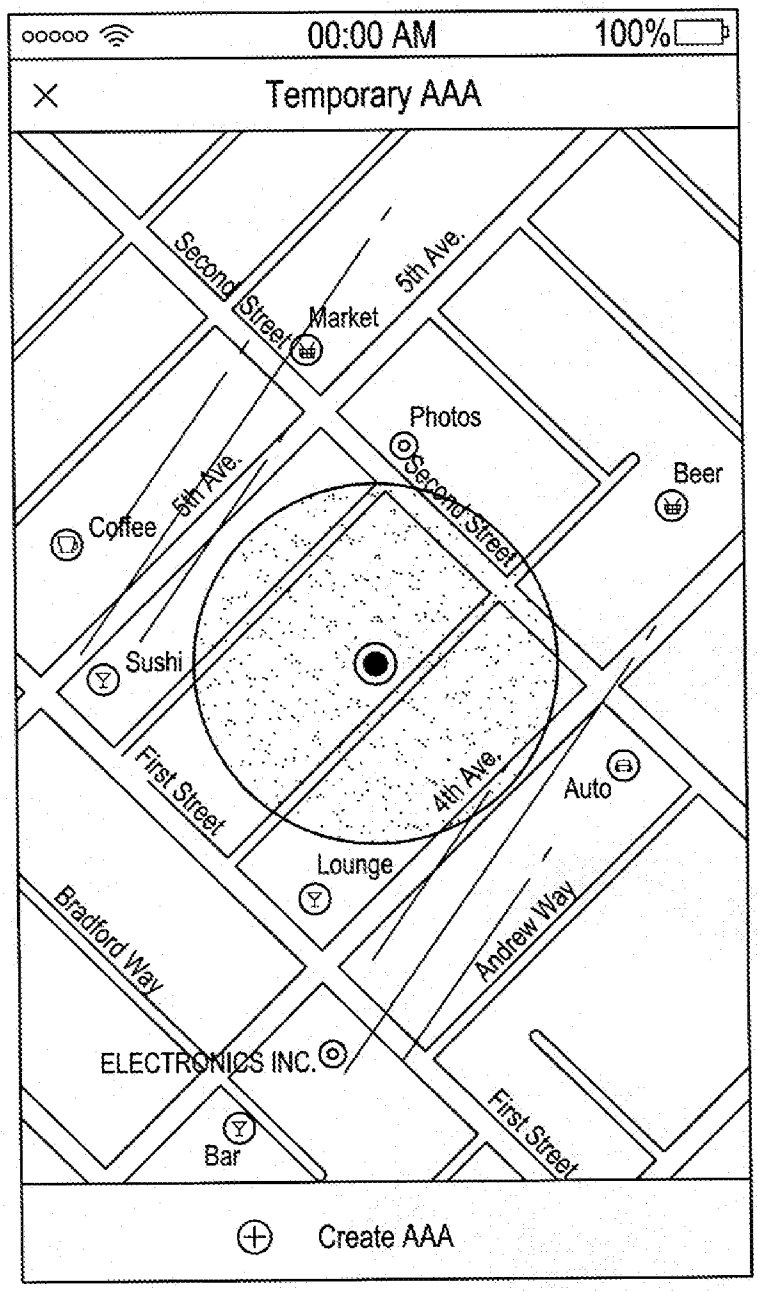

00:00 AM
100%
Temporary AAA
Second Street
5th Ave.
Market
Photos
Second Street
Beer
5th Ave.
Coffee
Sushi
First Street
4th Ave.
Auto
Lounge
Bradford Way
Andrew Way
ELECTRONICS INC.
Bar
First Street
Create AAA

FIG. 7

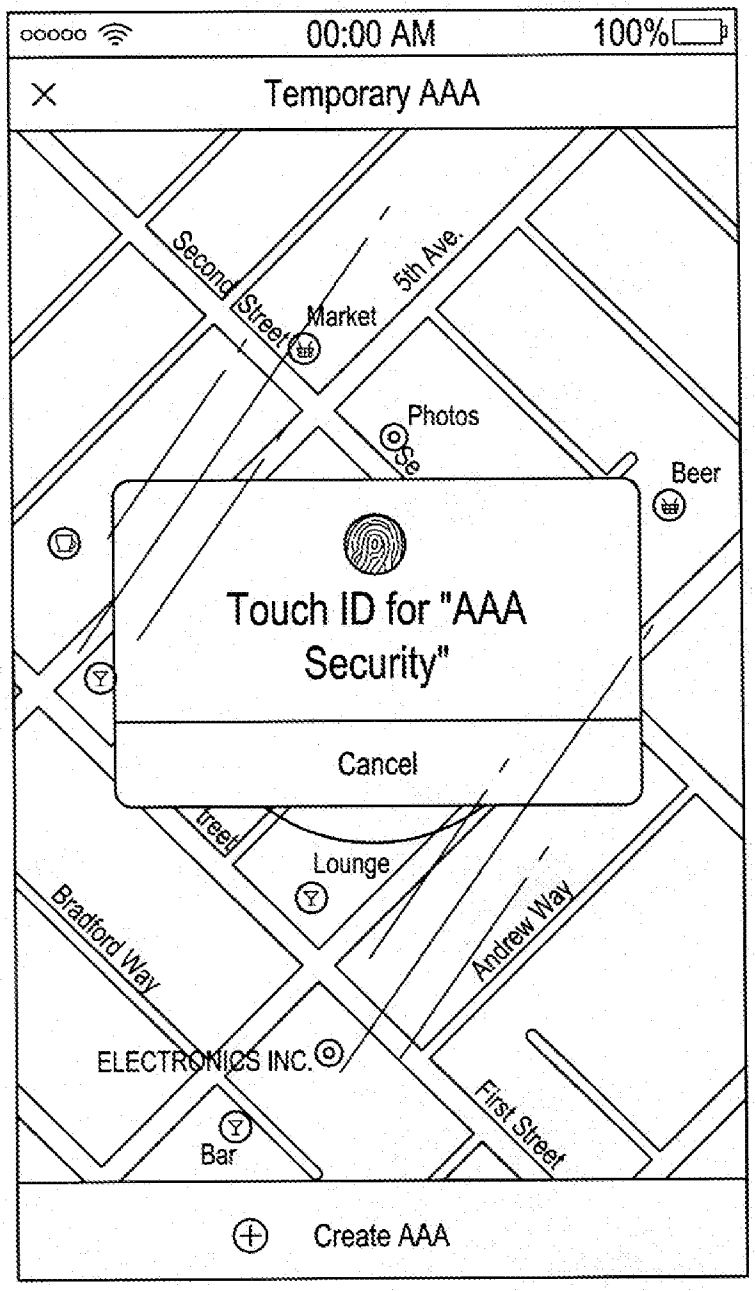

00:00 AM
100%
Temporary AAA
Second Street
5th Ave.
Market
Photos
Beer
Touch ID for "AAA Security"
Cancel
Lounge
Bradford Way
Andrew Way
ELECTRONICS INC.
First Street
Bar
Create AAA

FIG. 8

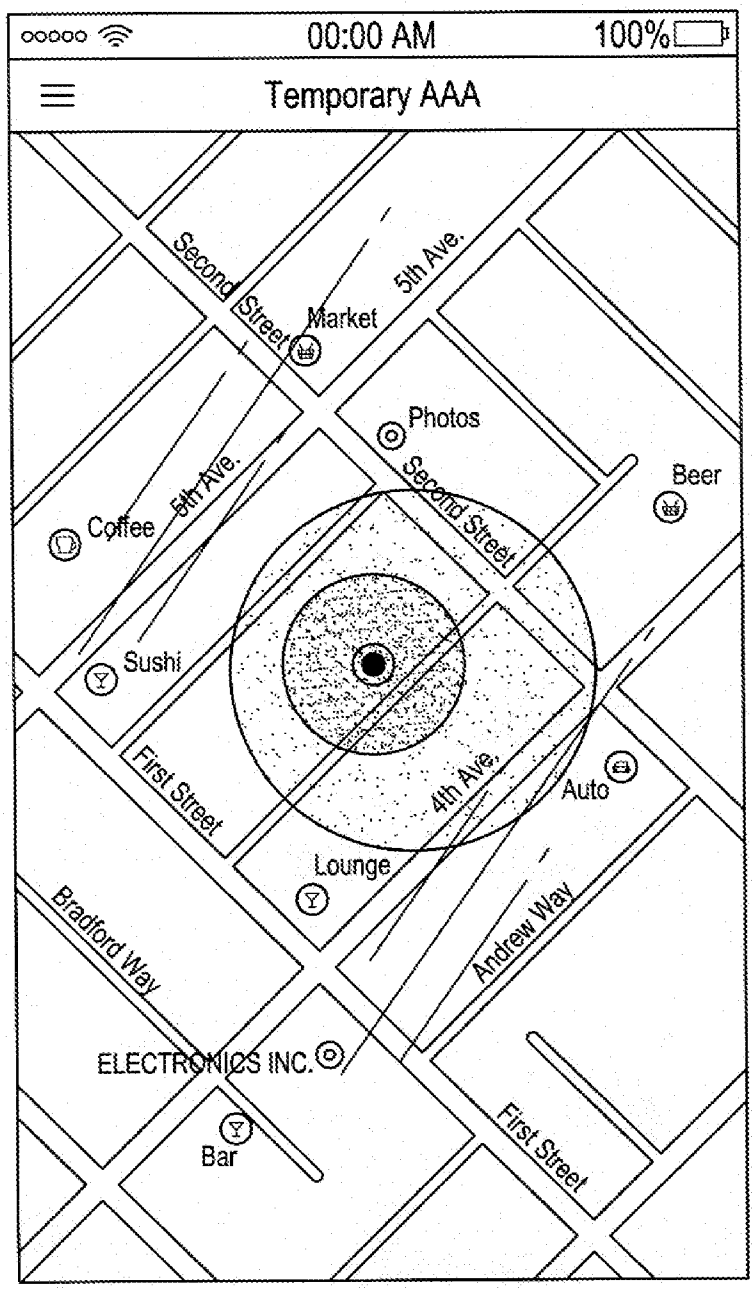

00:00 AM
100%
Temporary AAA
Second Street
5th Ave.
Market
Photos
Beer
5th Ave.
Second Street
Coffee
Sushi
First Street
4th Ave.
Auto
Lounge
Bradford Way
Andrew Way
ELECTRONICS INC.
Bar
First Street

FIG. 9

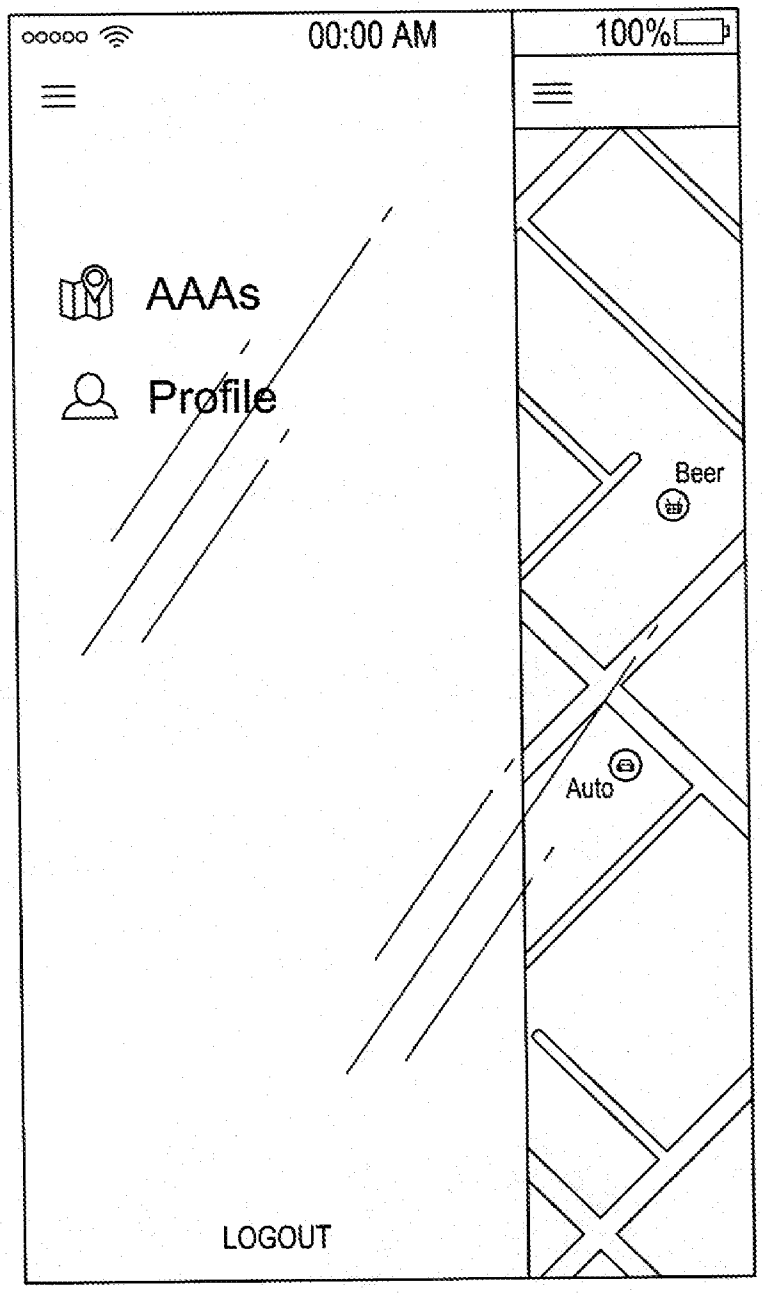


FIG. 10

Username	Most Recent Login Attempt
User1	Unauthorized Login - on Tuesday, August 25, 2015 at 12:15 AM
User2	Authorized Login - on Friday, September 4, 2015 at 6:36 PM
User3	(None)
User4	Unauthorized Login - 2121-2359 First Street, City, State Zip, USA on Thursday, September 10, 2015
User5	(None)
User6	(None)
User7	Unauthorized Login - 2345 Second Street, City, State Zip, USA on Thursday, December 17, 2015
User8	Authorized Login - Temporary AAA on Thursday, December 17, 2015 at 9:18 PM
User9	Authorized Login - London Marriott on Friday, September 4, 2015 at 10:02 PM

FIG. 11

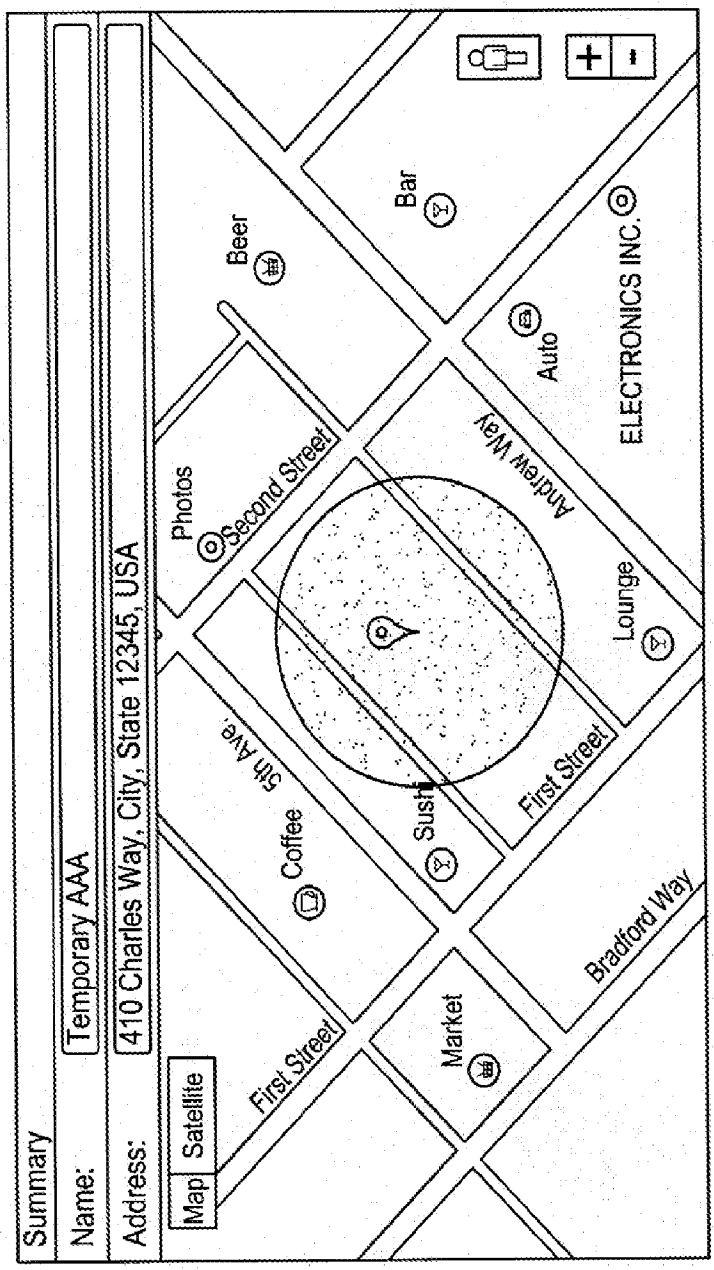
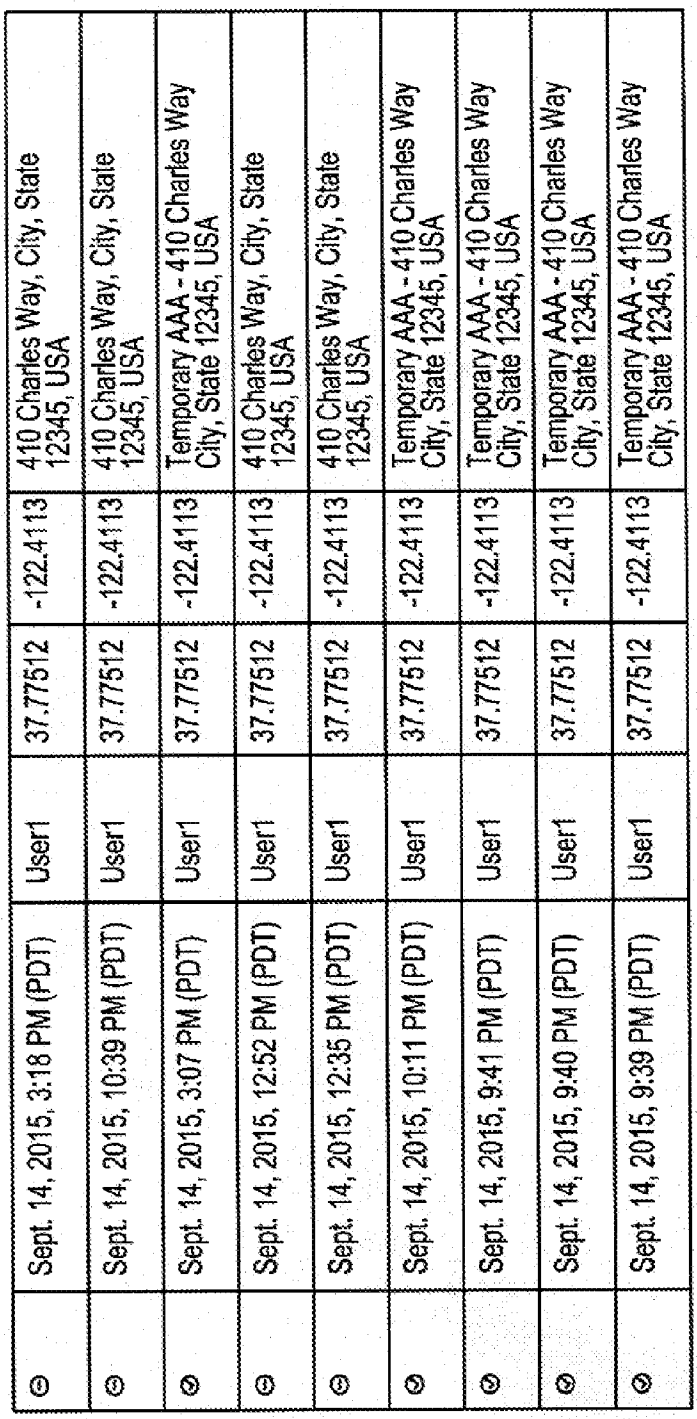

Summary
Name:
Temporary AAA
Address:
410 Charles Way, City, State 12345, USA
Map
Satellite
First Street
5th Ave
Coffee
Sushi
Market
Bradford Way
First Street
Andrew Way
Lounge
Photos
Second Street
Beer
Bar
Auto
ELECTRONICS INC.

FIG. 12



⊖	Sept. 14, 2015, 3:18 PM (PDT)	User1	37.77512	-122.4113	410 Charles Way, City, State 12345, USA
⊖	Sept. 14, 2015, 10:39 PM (PDT)	User1	37.77512	-122.4113	410 Charles Way, City, State 12345, USA
⊘	Sept. 14, 2015, 3:07 PM (PDT)	User1	37.77512	-122.4113	Temporary AAA - 410 Charles Way City, State 12345, USA
⊖	Sept. 14, 2015, 12:52 PM (PDT)	User1	37.77512	-122.4113	410 Charles Way, City, State 12345, USA
⊖	Sept. 14, 2015, 12:35 PM (PDT)	User1	37.77512	-122.4113	410 Charles Way, City, State 12345, USA
⊘	Sept. 14, 2015, 10:11 PM (PDT)	User1	37.77512	-122.4113	Temporary AAA - 410 Charles Way City, State 12345, USA
⊘	Sept. 14, 2015, 9:41 PM (PDT)	User1	37.77512	-122.4113	Temporary AAA - 410 Charles Way City, State 12345, USA
⊘	Sept. 14, 2015, 9:40 PM (PDT)	User1	37.77512	-122.4113	Temporary AAA - 410 Charles Way City, State 12345, USA
⊘	Sept. 14, 2015, 9:39 PM (PDT)	User1	37.77512	-122.4113	Temporary AAA - 410 Charles Way City, State 12345, USA

FIG. 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US16/38592

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **G06F 7/04**(2006.01),**15/16**(2006.01),**17/30**(2006.01);**H04L 29/06**(2006.01)

USPC: 726/006
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)
U.S. : 726/006

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 practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2015/0121464 A1 (HUGHES, JR et al) 30 April 2015 (30.04.2015), see entire documents.	1-14
Y	US 2014/0053250 A1 (WETHINGTON et al) 20 February 2014 (20.02.2014), see entire documents.	1-14
Y	US 2011/0028094 A1 (MASUDA) 03 February 2011 (03.02.2011), see entire documents.	4 and 11
Y	US 2015/0264573 A1 (GIORDANO et al) 17 September 2015 (17.09.2015), see entire documents.	7 and 14

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* 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 published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 July 2016 (28.07.2016)	05 AUG 2016
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-8300	Authorized officer Chris Grant Telephone No. 571-272-7294

INTERNATIONAL SEARCH REPORT	International application No. PCT/US16/38592

Continuation of B. FIELDS SEARCHED Item 3:
USPGPUB, USPAT, EPO, JPO, DERWENT, IBM_TDB: authorize, expire, remove, temporary, area, location, near, zone, same, mobile, geo-fence, delete, authenticate