



(51) International Patent Classification:

G06F 21/32 (2013.01) H04W 12/08 (2009.01)
H04W 12/06 (2009.01) H04W 4/80 (2018.01)

(21) International Application Number:

PCT/US2018/019705

(22) International Filing Date:

26 February 2018 (26.02.2018)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/492,610 01 May 2017 (01.05.2017) US

(71) Applicant: **CARRIER CORPORATION** [US/US];
17900 Beeline Highway, Jupiter, Florida 33478 (US).

(72) Inventors: **MANIKANTAN SHILA, Devu**; 411 Silver
Lane, East Hartford, Connecticut 06108 (US). **SRIVAS-
TAVA, Kunal**; 411 Silver Lane, East Hartford, Connecti-

cut 06108 (US). **O'NEILL, Paul C.**; 411 Silver Lane, East
Hartford, Connecticut 06108 (US).

(74) Agent: **RODRIGUEZ, Paul A.**; Cantor Colburn LLP,
20 Church Street, 22nd Floor, Hartford, Connecticut
06103-3207 (US).

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

(84) Designated States (*unless otherwise indicated, for every
kind of regional protection available*): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,

(54) Title: SYSTEM AND METHOD OF MOBILE BASED USER AUTHENTICATION FOR AN ACCESS CONTROLLED ENVIRONMENT

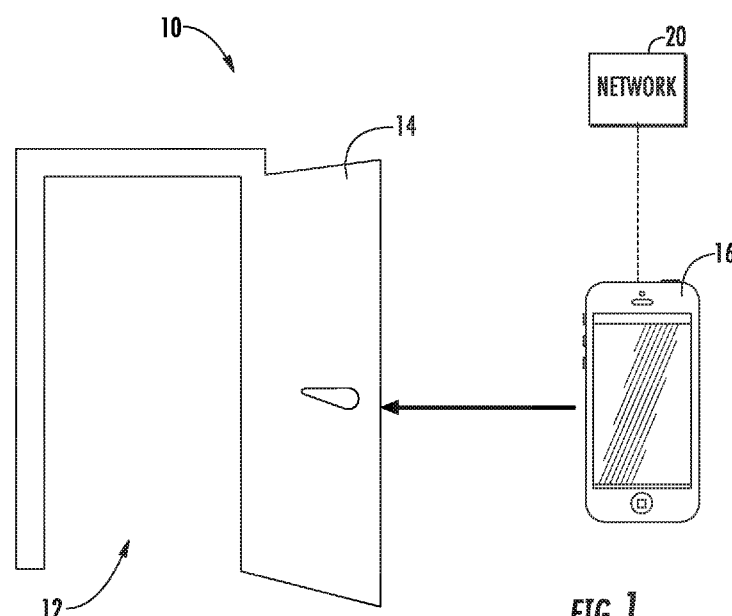


FIG. 1

(57) Abstract: A method of mobile based user authentication includes storing a plurality of categories of data associated with user activity with a mobile device carried or worn by a user. The method also includes analyzing the plurality of categories of data over a recent period of time to determine a user trust score based on a historical period of time, the historical period of time greater than the recent period of time. The method further includes granting access to an access controlled environment if the user trust score is within a predetermined score range.



UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*
- *of inventorship (Rule 4.17(iv))*

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

SYSTEM AND METHOD OF MOBILE BASED USER AUTHENTICATION FOR AN ACCESS CONTROLLED ENVIRONMENT

FEDERAL RESEARCH STATEMENT

[0001] This invention was made with Government support under contract number D15PC00155 awarded by the Science and Technology Directorate of the United States Department of Homeland Security. The Government has certain rights in the invention.

BACKGROUND

[0002] Mobile devices may be used to manage and access many devices and environments (e.g., thermostats, door locks, garage, etc.). In the case of access control solutions, while accessing door locks, a user must perform several time consuming and thereby inconvenient steps. This may include entering a mobile device passcode or PIN to access available applications, opening the mobile device application, and entering lock specific passcodes, for example.

[0003] Wireless communication between a lock and a mobile device also may involve very strong cryptographic operations which cause communication latencies. Currently, it would take approximately five or more seconds to open the lock via the wireless communication after the access verification steps have been performed by the user. More importantly, the passcodes are vulnerable to classic cybersecurity threats.

[0004] Accordingly, access control may be improved, both with respect to user convenience and from a security standpoint.

BRIEF SUMMARY

[0005] Disclosed is a method of mobile based user authentication. The method includes storing a plurality of categories of data associated with user activity with a mobile device carried or worn by a user. The method also includes analyzing the plurality of categories of data over a recent period of time to determine a user trust score based on a historical period of time, the historical period of time greater than the recent period of time. The method further includes granting access to an access controlled environment if the user trust score is within a predetermined score range.

[0006] In addition to one or more of the features described above, or as an alternative, further embodiments may include that analyzing the plurality of categories of data is initiated

once the mobile device is located within a predetermined distance of the access controlled environment.

[0007] In addition to one or more of the features described above, or as an alternative, further embodiments may include granting access to the access controlled environment subsequent to the user providing a user intent signal.

[0008] In addition to one or more of the features described above, or as an alternative, further embodiments may include that the user intent signal comprises tapping the mobile device.

[0009] In addition to one or more of the features described above, or as an alternative, further embodiments may include that the user intent signal comprises shaking the mobile device.

[0010] In addition to one or more of the features described above, or as an alternative, further embodiments may include that the user intent signal comprises providing a voice command.

[0011] In addition to one or more of the features described above, or as an alternative, further embodiments may include that granting access to the access controlled environment comprises unlocking a lock associated with an entry point of the access controlled environment.

[0012] In addition to one or more of the features described above, or as an alternative, further embodiments may include that the plurality of categories of data comprises at least one of location history, mobile device use, activity level, and biometrics.

[0013] In addition to one or more of the features described above, or as an alternative, further embodiments may include that the access controlled environment is a residential home.

[0014] In addition to one or more of the features described above, or as an alternative, further embodiments may include that the access controlled environment is a commercial office space.

[0015] Also disclosed is a method of mobile based user authentication. The method includes storing a plurality of categories of data associated with user activity with a mobile device carried or worn by a user to determine a user pattern over a historical period of time. The method also includes analyzing the plurality of categories of data over a recent period of time to determine a user trust score based on the user pattern, the recent period of time less than the historical period of time. The method further includes analyzing a risk value as a function of a plurality of variables, the user trust score one of the plurality of variables. The method yet further includes granting access to an access controlled environment if the risk value is within a predetermined value.

[0016] In addition to one or more of the features described above, or as an alternative, further embodiments may include that analyzing the plurality of categories of data is initiated once the mobile device is located within a predetermined distance of the access controlled environment.

[0017] In addition to one or more of the features described above, or as an alternative, further embodiments may include granting access to the access controlled environment subsequent to the user providing a user intent signal.

[0018] In addition to one or more of the features described above, or as an alternative, further embodiments may include that the user intent signal comprises tapping the mobile device.

[0019] In addition to one or more of the features described above, or as an alternative, further embodiments may include that the user intent signal comprises shaking the mobile device.

[0020] In addition to one or more of the features described above, or as an alternative, further embodiments may include that the user intent signal comprises providing a voice command.

[0021] In addition to one or more of the features described above, or as an alternative, further embodiments may include that granting access to the access controlled environment comprises unlocking a lock associated with an entry point of the access controlled environment.

[0022] In addition to one or more of the features described above, or as an alternative, further embodiments may include that the plurality of categories of data comprises at least one of location history, mobile device use, activity level, and biometrics.

[0023] In addition to one or more of the features described above, or as an alternative, further embodiments may include that the access controlled environment is a residential home.

[0024] In addition to one or more of the features described above, or as an alternative, further embodiments may include that the access controlled environment is a commercial office space.

BRIEF DESCRIPTION OF THE DRAWINGS

[0025] The present disclosure is illustrated by way of example and not limited in the accompanying figures in which like reference numerals indicate similar elements.

[0026] FIG. 1 is a simplified schematic illustration of an access control system; and

[0027] FIG. 2 illustrates a system and method associated with use of the access control system.

DETAILED DESCRIPTION

[0028] FIG. 1 depicts an environment 10 in an example embodiment. In some embodiments, the environment 10 is a building, residential or commercial, a part of a building, or a collection of buildings that are physically located near each other. The environment 10 includes an access controlled location 12. The access controlled location 12 may be a room or otherwise enclosed space that is secured with at least one entry point 14, such as the illustrated door. It is to be appreciated that the access controlled location 12 may be a door of a home or garage in the case of a residential structure.

[0029] In addition to the building environment described above, the embodiments described herein may be applicable to an outdoor setting with access controlled areas or to a building with an elevator system. In the case of the elevator system, certain elevator cars or floor destinations of the building may be access controlled, such that an access request must be granted by the access control system described herein.

[0030] Regardless of the particular environment that is access controlled, the entry point 14 is in a locked condition and access must be granted to a user in response to an access request. As illustrated and described herein, a mobile device 16 is employed to communicate with a lock of the entry point 14 and to send an access request. The mobile device 16 may be a device that is carried by a person, such as a smart phone, PDA, tablet, etc. Furthermore, the mobile device 16 may be wearable items, such as a smart watch, eyewear, etc. The mobile device 16 may include a processor, memory and a communication module. The processor can be any type or combination of computer processors, such as a microprocessor, microcontroller, digital signal processor, application specific integrated circuit, programmable logic device, and/or field programmable gate array. The memory is an example of a non-transitory computer readable storage medium tangibly embodied in the mobile device 16 including executable instructions stored therein, for instance, as firmware.

[0031] The mobile device 16 is in wireless and operative communication with a lock 18 (FIG. 2) of the access point 14. The communication between the mobile device 16 and the lock 18 may be facilitated through one or more network components 20 associated with a wireless network, such as a cloud network or telecommunication network. Examples of wireless networks that may be utilized include Bluetooth, Near Field Communication (NFC) and Wi-Fi.

[0032] Referring now to FIG. 2, an access control system and method is illustrated and generally referenced with numeral 30. The illustrated embodiment pertains to a home with a security system installed for controlling one or more lockable entry points. However, as

discussed above, any locked environment that requires the granting of access may benefit from the embodiments described herein, such that the illustrated embodiment is not limiting of the environments that may incorporate the embodiments described herein.

[0033] The mobile device 16 that is carried or worn by a user is configured to detect various activities of the user. In other words, at least one, but typically a plurality of categories of data 32 related to user activity is detected and stored on the mobile device 16 or with a remote medium, such as a wireless telecommunication network or a cloud network. The categories of data 32 may be any data associated with activities of a user that are detected and stored over a historical period of time. The historical period of time may vary in duration depending upon the particular application. Regardless of how long the historical period is defined as, the period provides a large enough sample size to confidently ascertain the habits and patterns of the user based on the detected and stored categories of data tracked by the mobile device 16.

[0034] In some embodiments, the historical period of time may correspond to a training phase that is triggered once the user installs the access control application on the mobile device 16. The training phase allows the mobile device 16 to learn various user activities, such as his walking patterns, his location transition patterns (e.g., user coming home from work), his skin temperature, his heart rate, whether the device is carried on his pocket (or phone placements). The training phase may be the first week, for example, but many alternative suitable time periods are contemplated. After the training phase, the mobile device 16 switches to a deployment phase where it uses the learned behavior models of the user (e.g., activity pattern, location pattern, skin temperature, heart rate) to predict if he is the real (i.e., authorized) user. The preceding examples are merely illustrative and some are discussed in more detail below in connection with the categories of data.

[0035] The device will also include modules to retrain the learning algorithm when needed. The behavior of the user can change over time. For instance his location transition patterns when he moves to a new residence or workplace, etc. In order to account for such behavioral changes over time, a retraining module that retrains the learned user behavior model when new samples are seen is provided in some embodiments. In order to prevent learning of unseen but malicious samples, the user will be requested to enter an active factor (e.g., biometric or a PIN number). If the user is authenticated, a new sample will be sent to the Cloud where it will learn the new model based on his old and new samples.

[0036] Various examples of the categories of data 32 are discussed herein, but the examples are not limiting of the categories that may be employed. One or more physical

activity levels 34 may be monitored. For example, the unique walking pattern of the user may be studied by the mobile device 16. The walking pattern may include length of stride and speed of stride. Additionally, the number of steps taken by the user over a given time period (e.g., hours, days, etc.), when such activity is performed (e.g., certain times of day), and the time of exercising may be monitored. Furthermore, one or more biometrics 36, such as average heart rate, may be monitored. A user's GPS location history 38 may be monitored to determine a travel pattern of the user. The usage 40 of the mobile device, such as game playing, social media usage, etc., may be monitored to determine usage patterns. As noted above, the examples discussed are not exhaustive of factors that may be monitored.

[0037] The categories of data 32 are analyzed to determine a user trust score 50 that provides a level of confidence that the mobile device 16 is in the presence of the trusted user (e.g., being carried or worn by user) that is authorized to access the access controlled environment. The user trust score 50 is determined by analysis of the categories of data 32 over a recent period of time that is less than the historical period of time. It is to be appreciated that the recent period of time may vary in duration based on the application of use. In some embodiments, the recent period of time is a number of hours or a number of days. Analysis of the categories of data over the recent time period allows the user trust score 50 to determine if recent activity detected by the mobile device 16 corresponds to the known patterns and habits of the authorized user based on the collection of data over the historical time period. In other words, each category analyzed over the recent period of time that does not correspond to the category data analyzed over the historical period of time alters the user trust score. An algorithm is programmed on the mobile device 16, on a wireless telecommunication network or cloud network, with the algorithm determining the user trust score 50.

[0038] In some embodiments, the user trust score 50 is the sole determining factor regarding whether access to the access controlled environment is granted. Therefore, if the user trust score 50 is within a predetermined range then access granted. It is to be appreciated that the algorithm may be structured such that a higher score is indicative of a higher degree of confidence that the user of the mobile device 16 is the authorized user. In such embodiments, the user trust score 50 must exceed a threshold score to provide access. Conversely, the algorithm may be structured such that a lower score is indicative of a higher degree of confidence that the user of the mobile device 16 is the authorized user. In such embodiments, the user trust score 50 must be lower than a threshold score to provide access. In an embodiment where the user trust score 50 is the sole determining factor, if the score is within the predetermined range then access is granted, such as by unlocking the entry point 14.

[0039] In some embodiments, the user trust score 50 is merely one factor that is part of an algorithm that determines an overall risk factor associated with granting access. Such an algorithm and process is illustrated and generally referenced with numeral 60 in FIG. 2. Other factors that may be employed include policies and the sensitivity of the mobile device application that controls access. As illustrated, if the risk is deemed too high based on the algorithm, access is denied. If the risk is deemed low and within a predetermined value based on the algorithm, access is granted. In some embodiments, an intermediate value that indicates a medium risk results in a requirement for further feedback to be provided by the user. For example, a biometric test may be required, such as fingerprint analysis, eye scan, voice recognition, etc. There are merely examples of the additional feedback that may be required.

[0040] Analysis of the data employed to determine whether access is to be granted is initiated once the mobile device 16, and therefore the user, is located within certain proximity of a component of the security system that is responsible for the access controlled environment. The component may be the lock 18 itself or a central unit that is in operative communication with the lock 18. Therefore, the mobile device 16 application senses when the mobile device 16 is located within a predetermined distance of the security system component and triggers initiation of the analysis that is described in detail above. This alleviates the need for the user to take action.

[0041] In some embodiments, access is still not granted even after the user trust score 50 and/or the overall risk algorithm indicate authentication of the user. This avoids unintentional granting of access, such as unlocking doors when the user is in close proximity. In such embodiments, a user intent signal is required to signify user intent to access the environment and complete the access request. The user intent signal may be a physical signal that requires contact between the user and the mobile device 16. Examples of physical signals include tapping the mobile device, shaking the mobile device. The user intent signal may be a voice command provided by the user. Regardless of what user intent signal is required, inadvertent opening of locks is avoided.

[0042] In operation, the system and method described herein provide users in the operating environment with a nearly seamless and interactive access request experience. Advantageously, the user may step into the environment and receive the granting of access without interacting with anything other than their mobile device 16 and even then only doing so in a minimalistic fashion.

[0043] Embodiments may be implemented using one or more technologies. In some embodiments, an apparatus or system may include one or more processors, and memory storing

instructions that, when executed by the one or more processors, cause the apparatus or system to perform one or more methodological acts as described herein. Various mechanical components known to those of skill in the art may be used in some embodiments.

[0044] Embodiments may be implemented as one or more apparatuses, systems, and/or methods. In some embodiments, instructions may be stored on one or more computer program products or computer-readable media, such as a transitory and/or non-transitory computer-readable medium. The instructions, when executed, may cause an entity (e.g., a processor, apparatus or system) to perform one or more methodological acts as described herein.

[0045] While the disclosure has been described in detail in connection with only a limited number of embodiments, it should be readily understood that the disclosure is not limited to such disclosed embodiments. Rather, the disclosure can be modified to incorporate any number of variations, alterations, substitutions or equivalent arrangements not heretofore described, but which are commensurate with the scope of the disclosure. Additionally, while various embodiments have been described, it is to be understood that aspects of the disclosure may include only some of the described embodiments. Accordingly, the disclosure is not to be seen as limited by the foregoing description, but is only limited by the scope of the appended claims.

What is claimed is:

1. A method of mobile based user authentication comprising:
storing a plurality of categories of data associated with user activity with a mobile device carried or worn by a user;
analyzing the plurality of categories of data over a recent period of time to determine a user trust score based on a historical period of time, the historical period of time greater than the recent period of time; and
granting access to an access controlled environment if the user trust score is within a predetermined score range.
2. The method of claim 1, wherein analyzing the plurality of categories of data is initiated once the mobile device is located within a predetermined distance of the access controlled environment.
3. The method of any of the preceding claims, further comprising granting access to the access controlled environment subsequent to the user providing a user intent signal.
4. The method of claim 3, wherein the user intent signal comprises tapping the mobile device.
5. The method of claim 3, wherein the user intent signal comprises shaking the mobile device.
6. The method of claim 3, wherein the user intent signal comprises providing a voice command.
7. The method of any of the preceding claims, wherein granting access to the access controlled environment comprises unlocking a lock associated with an entry point of the access controlled environment.
8. The method of any of the preceding claims, wherein the plurality of categories of data comprises at least one of location history, mobile device use, activity level, and biometrics.
9. The method of any of the preceding claims, wherein the access controlled environment is a residential home.
10. The method of any of the preceding claims, wherein the access controlled environment is a commercial office space.
11. A method of mobile based user authentication comprising:
storing a plurality of categories of data associated with user activity with a mobile device carried or worn by a user to determine a user pattern over a historical period of time;

analyzing the plurality of categories of data over a recent period of time to determine a user trust score based on the user pattern, the recent period of time less than the historical period of time;

analyzing a risk value as a function of a plurality of variables, the user trust score one of the plurality of variables; and

granting access to an access controlled environment if the risk value is within a predetermined value.

12. The method of claim 11, wherein analyzing the plurality of categories of data is initiated once the mobile device is located within a predetermined distance of the access controlled environment.

13. The method of claim 11 or 12, further comprising granting access to the access controlled environment subsequent to the user providing a user intent signal.

14. The method of claim 13, wherein the user intent signal comprises tapping the mobile device.

15. The method of claim 13, wherein the user intent signal comprises shaking the mobile device.

16. The method of claim 13, wherein the user intent signal comprises providing a voice command.

17. The method of any of claims 11-16, wherein granting access to the access controlled environment comprises unlocking a lock associated with an entry point of the access controlled environment.

18. The method of any of claims 11-17, wherein the plurality of categories of data comprises at least one of location history, mobile device use, activity level, and biometrics.

19. The method of any of claims 11-18, wherein the access controlled environment is a residential home.

20. The method of any of claims 11-18, wherein the access controlled environment is a commercial office space.

1/2

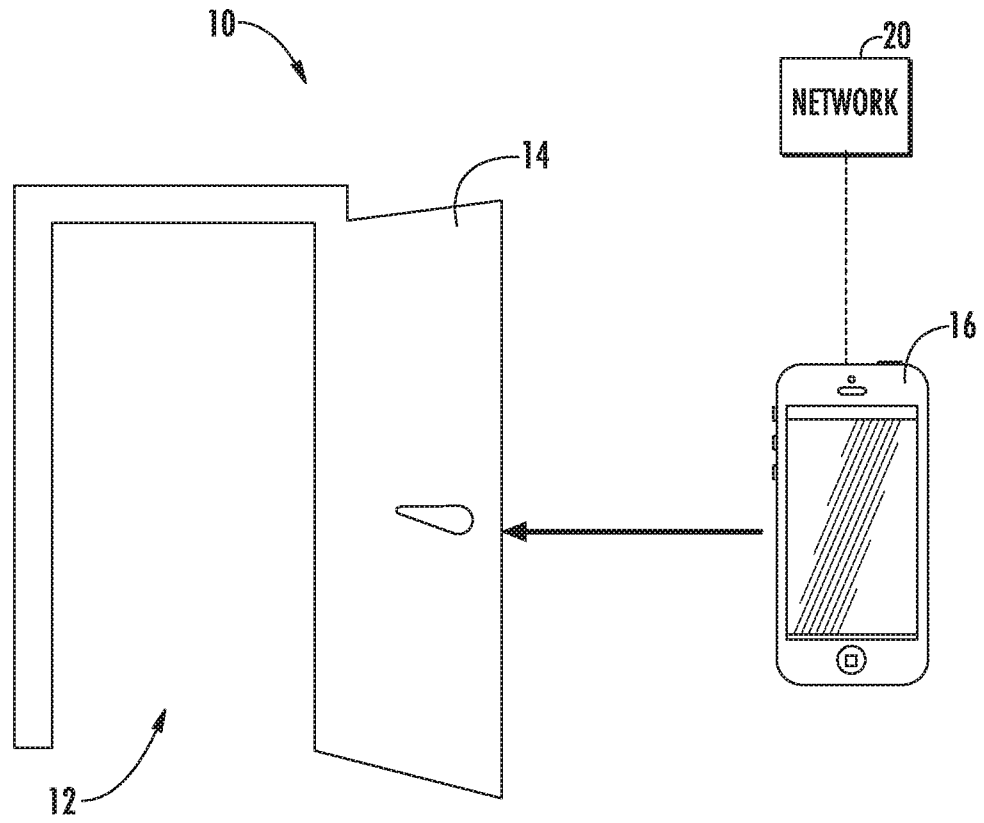


FIG. 1

2/2

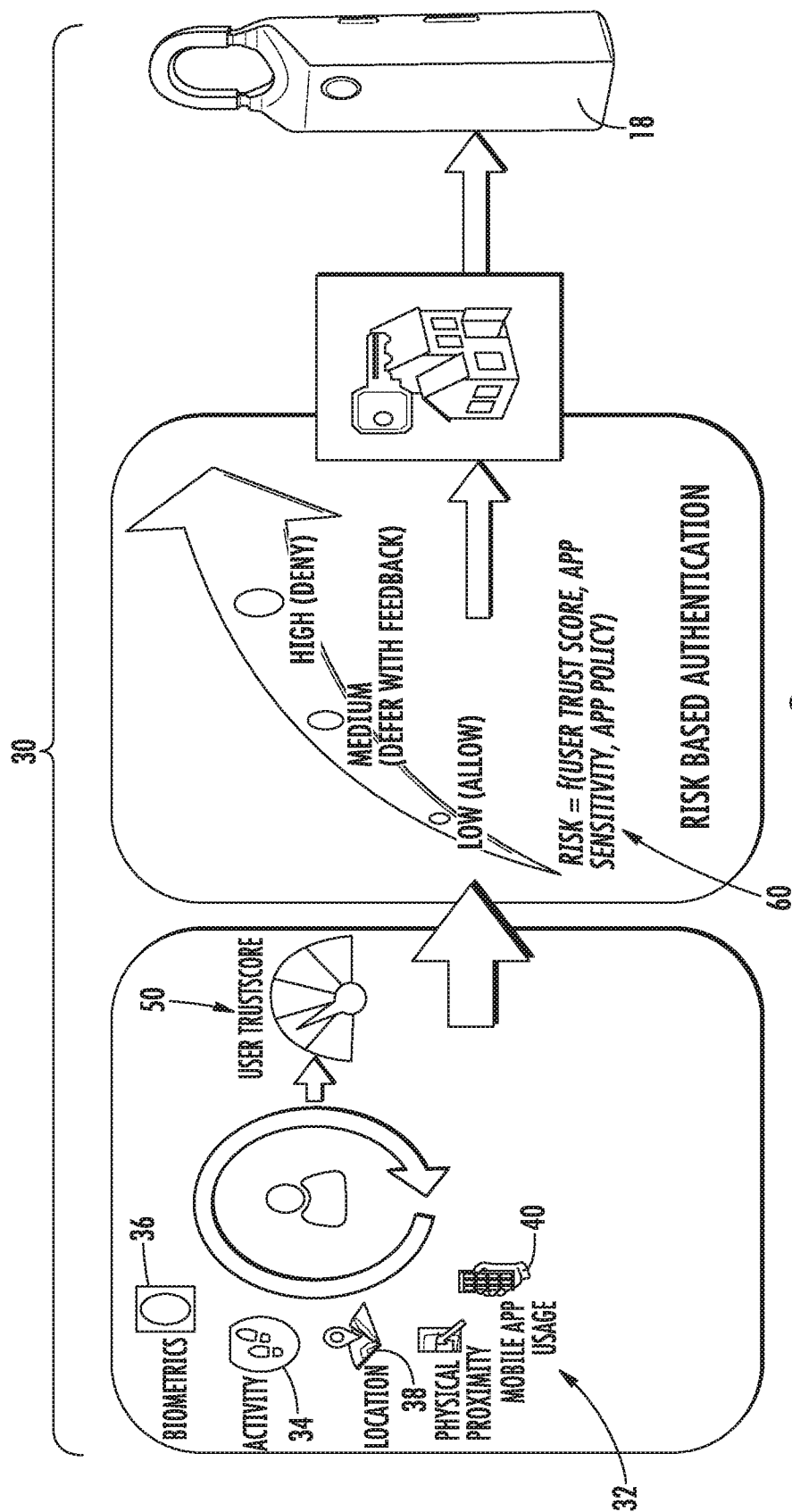


FIG. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/019705

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/32 H04W12/06 H04W12/08 H04W4/80
ADD.

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)

G06F H04W

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)

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2016/055487 A1 (VOTAW ELIZABETH S [US] ET AL) 25 February 2016 (2016-02-25) paragraphs [0003], [0025], [0027], [0032], [0043], [0045], [0052], [0071], [0087], [0089], [0090], [0091], [0092]; figures 1-4 -----	1-20
X A	US 2013/102283 A1 (LAU ALVIN [US] ET AL) 25 April 2013 (2013-04-25) paragraphs [0017] - [0019], [0026] - [0029], [0032], [0047] - [0049], [0058] - [0062], [0074] - [0076], [0103] - [0112]; figures 1,3,4,5,6,7 ----- -/-	1,2,11, 12 7-10, 17-20



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 but published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

26 September 2018

Date of mailing of the international search report

05/10/2018

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Herzog, Till-Henning

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2018/019705

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016/188848 A1 (SMITH NED M [US] ET AL) 30 June 2016 (2016-06-30) paragraphs [0031], [0032], [0035] - [0041] -----	1,2, 9-12,19, 20
A	N.A.: "Ultralog UL3 BT", 4 November 2016 (2016-11-04), pages 1-13, XP055510065, Retrieved from the Internet: URL:https://web.archive.org/web/2016110404 2950/http://www.u-tec.com:80/lock/u13/bt.h tml [retrieved on 2018-09-26] pages 1-4 -----	3,4,13, 14
A	Megan Wollerton: "Control a smart lock with your voice: Good idea or bad idea", www.cnet.com, 22 April 2017 (2017-04-22), pages 1-3, XP055510069, Retrieved from the Internet: URL:https://web.archive.org/web/2017042207 2421/https://www.cnet.com/news/controlling -locks-with-your-voice-good-idea-or-bad-id ea/ [retrieved on 2018-09-26] the whole document -----	3,6,13, 16
A	N.A.: "HID Mobile Access signals new era in security solutions", 28 March 2017 (2017-03-28), pages 1-3, XP055510075, www.assaabloy.com Retrieved from the Internet: URL:https://web.archive.org/web/2017032814 0055/https://www.assaabloy.com/en/com/pres s-news/news/2014/hid-mobile-access-signals -new-era-in-security-solutions-/ [retrieved on 2018-09-26] the whole document -----	3,5,13, 15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2018/019705

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016055487 A1	25-02-2016	NONE	
US 2013102283 A1	25-04-2013	NONE	
US 2016188848 A1	30-06-2016	CN 107004075 A	01-08-2017
		EP 3238115 A1	01-11-2017
		US 2016188848 A1	30-06-2016
		US 2016188853 A1	30-06-2016
		WO 2016105738 A1	30-06-2016