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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 June 2022 (30.06.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/136103 A1

(51) International Patent Classification:
G07C 9/00 (2020.01) *G08B 21/18* (2006.01)
G08B 21/04 (2006.01)

(21) International Application Number:
PCT/EP2021/086178

(22) International Filing Date:
16 December 2021 (16.12.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2051514-4 21 December 2020 (21.12.2020) SE

(71) Applicant: **ASSA ABLOY AB** [SE/SE]; P.O. Box 70340, 107 23 Stockholm (SE).

(72) Inventors: **NORDBECK, Per**; Trumgatan 12, 239 36 Skanör (SE). **RYD, Gustav**; Sankt Eriksgatan 23, 112 39 Stockholm (SE). **PERNYER, Kenneth**; Kungsholms Hamnplan 7, 112 20 Stockholm (SE).

(74) Agent: **KRANSELL & WENNBORG KB**; P.O. Box 2096, 403 12 GÖTEBORG (SE).

(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, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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,

(54) Title: IDENTIFYING HEALTH EMERGENCY

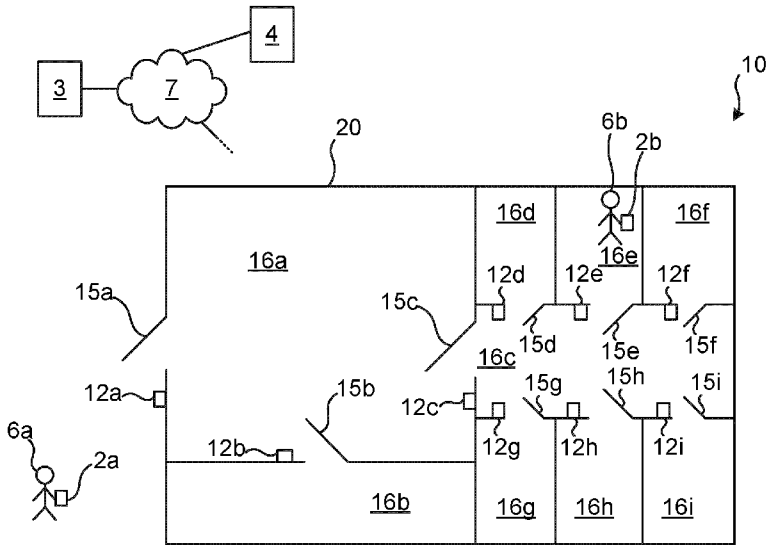

Fig. 1

(57) Abstract: It is provided a method a method for identifying a health emergency of a user. The method is performed in a behaviour determiner. The method comprises: obtaining, from an access control system, access data of the user, the access data indicating when the user has accessed an electronic lock in the access control system to gain access to a physical space secured by the electronic lock; determining that the access data indicates a health emergency; and transmitting an alert message, indicating the health emergency for the user.

WO 2022/136103 A1

[Continued on next page]

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))*

IDENTIFYING HEALTH EMERGENCY

TECHNICAL FIELD

[0001] The present disclosure relates to the field of identifying a health emergency and in particular to identifying a health emergency based on access data from an access control system.

BACKGROUND

[0002] Abnormal behaviour is a constant problem in modern societies. For instance, it is beneficial to be able to identify certain types of abnormal behaviour such as psychological problems, health emergencies. Traditionally, such behaviour is identified when reported by the affected person, or when observed by someone, either a professional in the field or by a third-party witness that reports the situation.

[0003] Certain types of health emergencies can create great personal suffering. Hence, it would be of great benefit if there were to be a way to automatically flag up a potential a health emergency. Such instances could then be manually evaluated.

SUMMARY

[0004] One object is to improve identification of a health emergency.

According to a first aspect, it is provided a method for identifying a health emergency of a user. The method is performed in a behaviour determiner. The method comprises: obtaining, from an access control system, access data of the user, the access data indicating when the user has accessed an electronic lock in the access control system to gain access to a physical space secured by the electronic lock; determining that the access data indicates a health emergency; and transmitting an alert message, indicating the health emergency for the user.

The determining may comprise determining that the access data indicates a health emergency when the access data indicates that the user accesses an electronic lock less than a threshold amount.

The determining may comprise determining that the access data indicates a health emergency when the access data indicates that the user accesses an electronic lock more than a threshold amount.

The determining may comprise determining that the access data indicates a health emergency when the access data indicates that the user deviates more than a threshold from average behaviour of other users of the access control system.

The determining may comprise determining that the access data indicates a health emergency based on a machine learning, ML, model.

The ML model may comprise both a local ML model and a central ML model.

The determining may be based also on a current time.

The method may be repeated, in which case the determining comprises determining an increased level of confidence of health emergency, when a health emergency is repeatedly determined in successive iterations of the method.

The method may further comprise: obtaining auxiliary data, in which case the step of determining is based also on the auxiliary data.

The auxiliary data may comprise energy consumption of a dwelling of the user, secured by the electronic lock.

The auxiliary data may comprise wireless-traffic data of the user.

[0005] According to a second aspect, it is provided a behaviour determiner for identifying a health emergency of a user. The behaviour determiner comprises: a processor; and a memory storing instructions that, when executed by the processor, cause the behaviour determiner to: obtain, from an access control system, access data of the user, the access data indicating when the user has accessed an electronic lock in the access control system to gain access to a physical space secured by the electronic lock; determine that the access data indicates a health emergency; and transmit an alert message, indicating the health emergency for the user.

[0006] The instructions to determine may comprise instructions that, when executed by the processor, cause the behaviour determiner to determine that the access data

indicates a health emergency when the access data indicates that the user accesses an electronic lock less than a threshold amount.

[0007] The instructions to determine may comprise instructions that, when executed by the processor, cause the behaviour determiner to determine that the access data indicates a health emergency when the access data indicates that the user accesses an electronic lock more than a threshold amount.

[0008] The instructions to determine may comprise instructions that, when executed by the processor, cause the behaviour determiner to determine that the access data indicates a health emergency when the access data indicates that the user deviates more than a threshold from average behaviour of other users of the access control system.

[0009] The instructions to determine may comprise instructions that, when executed by the processor, cause the behaviour determiner to determine that the access data indicates a health emergency based on a machine learning, ML, model.

[0010] The ML model may comprise both a local ML model and a central ML model.

[0011] The instructions to determine may comprise instructions that, when executed by the processor, cause the behaviour determiner to determine that the access data indicates a health emergency based also on a current time.

[0012] The behaviour determiner may further comprise instructions that, when executed by the processor, cause the behaviour determiner to repeat the instructions to obtain and determine, in which case the instructions to determine comprise instructions that, when executed by the processor, cause the behaviour determiner to determine an increased level of confidence of health emergency, when a health emergency is repeatedly determined in successive iterations of the method.

[0013] The behaviour determiner may further comprise instructions that, when executed by the processor, cause the behaviour determiner to: obtain auxiliary data; in which case the instructions to determine comprise instructions that, when executed by the processor, cause the behaviour determiner to determine a health emergency also based on the auxiliary data.

[0014] The auxiliary data may comprise energy consumption of a dwelling of the user, secured by the electronic lock.

[0015] The auxiliary data may comprise wireless-traffic data of the user.

[0016] According to a third aspect, it is provided a computer program for identifying a health emergency of a user. The computer program may comprise computer program code which, when executed on a behaviour determiner causes the behaviour determiner to: obtain, from an access control system, access data of the user, the access data indicating when the user has accessed an electronic lock in the access control system to gain access to a physical space secured by the electronic lock; determine that the access data indicates a health emergency; and transmit an alert message, indicating the health emergency for the user.

[0017] According to a fourth aspect, it is provided a computer program product comprising a computer program according to the third aspect and a computer readable means on which the computer program is stored.

[0018] Generally, all terms used in the claims are to be interpreted according to their ordinary meaning in the technical field, unless explicitly defined otherwise herein. All references to "a/an/the element, apparatus, component, means, step, etc." are to be interpreted openly as referring to at least one instance of the element, apparatus, component, means, step, etc., unless explicitly stated otherwise. The steps of any method disclosed herein do not have to be performed in the exact order disclosed, unless explicitly stated.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] Aspects and embodiments are now described, by way of example, with reference to the accompanying drawings, in which:

[0020] Fig 1 is a schematic diagram illustrating an environment in which embodiments presented herein can be applied;

[0021] Figs 2A-D are schematic diagrams illustrating embodiments of where the behaviour determiner can be implemented;

[0022] Fig 3 is a flow chart illustrating embodiments of methods for identifying a health emergency of a user;

[0023] Fig 4 is a schematic diagram illustrating components of the behaviour determiner of Figs 2A-D according to one embodiment; and

[0024] Fig 5 shows one example of a computer program product comprising computer readable means.

DETAILED DESCRIPTION

[0025] The aspects of the present disclosure will now be described more fully hereinafter with reference to the accompanying drawings, in which certain embodiments of the invention are shown. These aspects may, however, be embodied in many different forms and should not be construed as limiting; rather, these embodiments are provided by way of example so that this disclosure will be thorough and complete, and to fully convey the scope of all aspects of invention to those skilled in the art. Like numbers refer to like elements throughout the description.

[0026] According to embodiments presented herein, a behaviour determiner uses access data from an access control system to determine a health emergency. This can be used e.g. to detect when someone has fallen ill or certain criminal activity. The access data from access control systems, e.g. for a residential property for multiple residents, is often collected in any case. Hence, this data is often readily available and can be used to efficiently determine a health emergency. Since this process can, to a large extent, be automated, this allows cases to be flagged up earlier than with traditional methods, whereby more of these cases do not go unnoticed.

[0027] Fig 1 is a schematic diagram illustrating an environment in which embodiments presented herein can be applied. An (electronic) access control system 10 contains a plurality of electronic locks 12a-i and optionally one or more online components, such as a server 3.

[0028] A set of electronic locks 12a-i are provided in a building 20, for securing access to respective physical spaces (i.e. rooms or set of rooms) 16a-i, by selectively

locking or unlocking respective doors 15a-i. It is to be noted that more buildings with respective electronic locks can be provided, forming part of the same access control system 10. The building 20 can e.g. be a residential property for multiple residents.

[0029] A first user 6a carries a first electronic key device 2a. The first electronic key device 2a can be in any suitable format that allows an electronic lock to communicate (wirelessly or conductively) with the electronic key device to evaluate whether to grant access. For instance, the first electronic key device 2a can be in the form of a key fob, a key card, a hybrid mechanical/electronic key or a smartphone. Depending on the access rights for the first electronic key device 2a, it can be used to unlock one or more of the electronic locks 12a-i. Analogously, a second user 6b is shown carrying a second electronic key device 2b, which can be of the same type or a different type compared to the first electronic key device. 2a.

[0030] The physical spaces 16a-i have different purposes. In this example, the building 20 is a college dormitory with a common area 16a, a kitchen 16b and a corridor 16c. Additionally, there are six dormitory rooms 16d-i. The first user 6a is here located outside the building 20, while the second user 6b is in her dormitory room 16e.

[0031] It is to be noted that, while two electronic key devices 2a-b and two users 6a-b are shown in Fig 1, there can be any suitable number of users with respective electronic key devices.

[0032] The server 3 can be used to control access rights for electronic key devices in the access control system 10 and can be provided in what is sometimes known as 'the cloud'. The server 3 can be connected to a communication network 7, which can be an Internet protocol (IP) based network. The communication network 7 can e.g. comprise any one or more of a wired local area network, a local wireless network, a cellular network, a wide area network (such as the Internet), etc. The communication network 7 can be used for communication between the server 3 and any online components of the access control system 10, e.g. all or a subset of the electronic locks 12a-i and/or the electronic key devices 2a-b.

[0033] When one of the electronic key device 2a-b is brought up to one of the electronic locks 12a-i, the electronic lock in question checks the access rights for the electronic key device to determine whether to grant or deny access, according to any suitable method. For instance, the access rights can be supplied by the electronic key devices 2a-b to the electronic lock, in which case the access rights can be cryptographically signed and/or encrypted by a party trusted by the electronic lock, such as the server 3. Alternatively, the electronic lock is online and, after obtaining the identity of the electronic key devices 2a-b, the electronic lock checks with the server 3 to determine whether the electronic key device is to be allowed access. Alternatively or additionally, the electronic lock has access (locally or remotely) to white lists (indicating identities of electronic key devices to be granted access) and/or blacklists (indicating identities of electronic key devices to be denied access).

[0034] Figs 2A-D are schematic diagrams illustrating embodiments of where the behaviour determiner 1 can be implemented.

[0035] In Fig 2A, the behaviour determiner 1 is shown implemented in the server 3. The server 3 is thus the host device for the behaviour determiner 1 in this implementation. The behaviour determiner 1 can be based on a central ML model in the server 3 and/or based on rule-based logic. When implemented in the server 3, the behaviour determiner has access to significant resources, e.g. in terms of processing power, memory, power, etc.

[0036] In Fig 2B, the behaviour determiner 1 is shown implemented in the electronic key device 2, e.g. one of the electronic key devices 2a-b of Fig 1. The electronic key device 2 is thus the host device for the behaviour determiner 1 in this implementation. In this case, the electronic key device 2 can e.g. be a smartphone, capable of running a local ML model and/or rule-based logic.

[0037] In Fig 2C, the behaviour determiner 1 is shown implemented in one or more electronic lock 12 (corresponding to the electronic locks 12a-i of Fig 1). The electronic lock 12 is thus the host device for the behaviour determiner 1 in this implementation. The lock 12 is then capable of running a local ML model and/or rule-based logic.

[0038] In Fig 2D, the behaviour determiner 1 is shown implemented as a stand-alone device. The behaviour determiner 1 thus does not have a host device in this implementation. The behaviour determiner 1 is capable of running a local ML model, a central ML model and/or rule-based logic.

[0039] Fig 3 is a flow chart illustrating embodiments of methods for identifying a health emergency of a user 6a, 6b. The method is performed in a behaviour determiner 1. The method is performed for a single user, but multiple instances of the method can run in parallel for respective users.

[0040] In an *obtain access data* step 40, the behaviour determiner 1 obtains, from an access control system 10, access data of the user 6a, 6b. The access data indicates when the user has accessed an electronic lock 12a-i in the access control system to gain access to a physical space secured by the electronic lock 12a-i. Hence, the access data can be in the form of access logs. This access data is relatively easy to obtain from the access control system 10, since this data is readily available. It is to be noted that access data indicating no access for the user is also valuable access data, as long as the access data covers a meaningful time period.

[0041] In an optional *obtain auxiliary data* step 42, the behaviour determiner 1 obtains auxiliary data. The auxiliary data can e.g. comprise energy consumption of a dwelling 16d-i of the user, secured by the electronic lock 12a-i. Alternatively or additionally, the auxiliary data may comprise wireless-traffic data of the user, e.g. in the form of Wi-Fi-traffic data and/or cellular-traffic data.

[0042] In a conditional *abnormal behaviour* step 44, the behaviour determiner 1 determines that the access data indicates a health emergency, which is a type of abnormal behaviour. This can be determined by first determining a percentage, indicating a level of confidence of a health emergency. This level of confidence can then be converted to a threshold level to conclude whether a health emergency is determined or not. This threshold level can be configured and reconfigured to adjust the sensitivity of the determining of health emergency determination. When a health emergency is determined, this is used for other processing, or the method proceeds to an optional

transmit alert message step 46. When a health emergency is not determined, the method returns to the *obtain access data* 40, optionally after a wait period (not shown).

[0043] The determining can comprise determining that the access data indicates a health emergency when the access data indicates that the user accesses an electronic lock less than a threshold amount. For instance, if the access data indicates that user has not accessed any of the electronic locks for a period longer than a threshold time, this can be an indicator of a health emergency, e.g. due to the user being incapacitated.

[0044] Alternatively, the determining can comprise determining that the access data indicates abnormal behaviour when the access data indicates that the user accesses an electronic lock more than a threshold amount. For instance, if there are openings on a regular basis throughout the night, particularly if the electronic lock is then unlocked from the inside, this can be an indication of drug sales or prostitution.

[0045] The degree of health emergency can also be determined from how much the user deviates from the average behaviour of other users of the access control system. This can prevent e.g. inactivity from being considered a health emergency in a college dormitory in the summertime, when nobody or very few people are living there.

[0046] The determination of whether a health emergency exists can be based on a machine learning (ML) model. An ML model can be trained to detect the types of a health emergency that are desired to be detected, and thus can be tailored accordingly.

[0047] The ML model can be locally based, on a local model e.g. in the electronic key device or the electronic lock. Alternatively, the ML model can be centrally based, on a central model in the server 3 or in a stand-alone behaviour determiner 1.

[0048] In one embodiment, the ML model comprises both a local ML model and a central ML model, in a distributed ML architecture. In a distributed ML architecture, the local ML can be of a simpler type and the central model can then be used to obtain a second opinion on determinations by the local ML model. Alternatively, the determinations of the local ML model and the central ML model determine their own levels of confidence and these are combined with different weights, to gain a composite level of confidence. The level of confidence is then compared to the level threshold to

determine if a health emergency exists or not. When ML is first used, an initial model can be based on a base model for a certain demographic group (age, sex, etc.). This initial model can then be tailored using continuous learning to learn what is normal and what is a health emergency for the particular user.

[0049] The determining can also be based also on a current time. For instance, certain behaviour can be normal when it occurs in the afternoon, but abnormal when it occurs in the middle of the night.

[0050] When step 42 is performed, the health emergency determination is based also on the auxiliary data. For instance, if energy consumption is reduced without explanation (e.g. when compared to other users), this can indicate a health emergency. Similarly, longer-than-expected absence of data wireless data traffic can indicate a health emergency.

[0051] In optional *transmit alert message* step 46, the behaviour determiner 1 transmits an alert message, indicating that the user exhibits a health emergency. This can e.g. be transmitted to a security company employing security agents that can go and check on the user to see if she/he is ok.

[0052] The method can be repeated. In this case, the conditional *abnormal behaviour* step 44 step can comprise determining an increased level of confidence of a health emergency when a health emergency is repeatedly determined in successive iterations of the method.

[0053] It is to be noted that the determination of a health emergency is not decisive; the determination of a health emergency results is an indication that should be verified by other means, e.g. by manual confirmation.

[0054] Fig 4 is a schematic diagram illustrating components of the behaviour determiner 1 of Figs 2A-D. It is to be noted that, when implemented in a host device, one or more of the mentioned components can be shared with the host device. A processor 60 is provided using any combination of one or more of a suitable central processing unit (CPU), graphics processing unit (GPU), multiprocessor, microcontroller, digital signal processor (DSP), etc., capable of executing software instructions 67 stored

in a memory 64, which can thus be a computer program product. The processor 60 could alternatively be implemented using an application specific integrated circuit (ASIC), field programmable gate array (FPGA), etc. The processor 60 can be configured to execute the method described with reference to Fig 3 above.

[0055] The memory 64 can be any combination of random-access memory (RAM) and/or read-only memory (ROM). The memory 64 also comprises persistent storage, which, for example, can be any single one or combination of magnetic memory, optical memory, solid-state memory or even remotely mounted memory.

[0056] A data memory 66 is also provided for reading and/or storing data during execution of software instructions in the processor 60. The data memory 66 can be any combination of RAM and/or ROM.

[0057] The behaviour determiner 1 further comprises an I/O interface 62 for communicating with external and/or internal entities. Optionally, the I/O interface 62 also includes a user interface.

[0058] Other components of the behaviour determiner 1 are omitted in order not to obscure the concepts presented herein.

[0059] Fig 5 shows one example of a computer program product 90 comprising computer readable means. On this computer readable means, a computer program 91 can be stored, which computer program can cause a processor to execute a method according to embodiments described herein. In this example, the computer program product is in the form of a removable solid-state memory, e.g. a Universal Serial Bus (USB) drive. As explained above, the computer program product could also be embodied in a memory of a device, such as the computer program product 64 of Fig ###. While the computer program 91 is here schematically shown as a section of the removable solid-state memory, the computer program can be stored in any way which is suitable for the computer program product, such as another type of removable solid-state memory, or an optical disc, such as a CD (compact disc), a DVD (digital versatile disc) or a Blu-Ray disc.

[0060] Here now follows a list of embodiments, enumerated with roman numerals.

[0061] i. A method for identifying abnormal behaviour of a user, the method being performed in a behaviour determiner, the method comprising:

obtaining, from an access control system, access data of the user, the access data indicating when the user has accessed an electronic lock in the access control system to gain access to a physical space secured by the electronic lock; and

determining that the access data indicates abnormal behaviour.

[0062] ii. The method according to embodiment i, wherein the determining comprises determining that the access data indicates abnormal behaviour when the access data indicates that the user accesses an electronic lock less than a threshold amount.

[0063] iii. The method according to embodiment i or ii, wherein the determining comprises determining that the access data indicates abnormal behaviour when the access data indicates that the user accesses an electronic lock more than a threshold amount.

[0064] iv. The method according to any one of the preceding embodiments, wherein the determining comprises determining that the access data indicates abnormal behaviour when the access data indicates that the user deviates more than a threshold from average behaviour of other users of the access control system.

[0065] v. The method according to any one of the preceding embodiments, wherein the determining comprises determining that the access data indicates abnormal behaviour based on a machine learning, ML, model.

[0066] vi. The method according to embodiment v, wherein the ML model comprises both a local ML model and a central ML model.

[0067] vii. The method according to any one of the preceding embodiments, wherein the determining is based also on a current time.

[0068] viii. The method according to any one of the preceding embodiments, further comprising:

transmitting an alert message, indicating that the user exhibits abnormal behaviour.

[0069] ix. The method according to any one of the preceding embodiments, wherein the method is repeated and wherein the determining comprises determining an increased level of confidence of abnormal behaviour, when abnormal behaviour is repeatedly determined in successive iterations of the method.

[0070] x. The method according to any one of the preceding embodiments, further comprising:

obtaining auxiliary data;

and wherein the step of determining is based also on the auxiliary data.

[0071] xi. The method according to embodiment x, wherein the auxiliary data comprises energy consumption of a dwelling of the user, secured by the electronic lock.

[0072] xii. The method according to embodiment x or xi, wherein the auxiliary data comprises wireless-traffic data of the user.

[0073] xiii. A behaviour determiner for identifying abnormal behaviour of a user, the behaviour determiner comprising:

a processor; and

a memory storing instructions that, when executed by the processor, cause the behaviour determiner to:

obtain, from an access control system, access data of the user, the access data indicating when the user has accessed an electronic lock in the access control system to gain access to a physical space secured by the electronic lock; and

determine that the access data indicates abnormal behaviour.

[0074] xiv. The behaviour determiner according to embodiment xiii, wherein the instructions to determine comprise instructions that, when executed by the processor, cause the behaviour determiner to determine that the access data indicates abnormal behaviour when the access data indicates that the user accesses an electronic lock less than a threshold amount.

[0075] xv. The behaviour determiner according to embodiment xiii or xiv, wherein the instructions to determine comprise instructions that, when executed by the processor, cause the behaviour determiner to determine that the access data indicates abnormal behaviour when the access data indicates that the user accesses an electronic lock more than a threshold amount.

[0076] xvi. The behaviour determiner according to any one of embodiments xiii to xv, wherein the instructions to determine comprise instructions that, when executed by the processor, cause the behaviour determiner to determine that the access data indicates abnormal behaviour when the access data indicates that the user deviates more than a threshold from average behaviour of other users of the access control system.

[0077] xvii. The behaviour determiner according to any one of embodiments xiii to xvi, wherein the instructions to determine comprise instructions that, when executed by the processor, cause the behaviour determiner to determine that the access data indicates abnormal behaviour based on a machine learning, ML, model.

[0078] xviii. The behaviour determiner according to embodiment xvii, wherein the ML model comprises both a local ML model and a central ML model.

[0079] xix. The behaviour determiner according to embodiment xviii, wherein the instructions to determine comprise instructions that, when executed by the processor, cause the behaviour determiner to determine that the access data indicates abnormal behaviour based also on a current time.

[0080] xx. The behaviour determiner according to any one of embodiments xiii to xix, further comprising instructions that, when executed by the processor, cause the behaviour determiner to:

transmit an alert message, indicating that the user exhibits abnormal behaviour.

[0081] xxi. The behaviour determiner according to any one of embodiments xiii to xx, further comprising instructions that, when executed by the processor, cause the behaviour determiner to repeat the instructions to obtain and determine, and wherein the instructions to determine comprise instructions that, when executed by the

processor, cause the behaviour determiner to determine an increased level of confidence of abnormal behaviour, when abnormal behaviour is repeatedly determined in successive iterations of the method.

[0082] xxii. The behaviour determiner according to any one of embodiments xiii to xxi, further comprising instructions that, when executed by the processor, cause the behaviour determiner to:

obtain auxiliary data;

and wherein the instructions to determine comprise instructions that, when executed by the processor, cause the behaviour determiner to determine abnormal behaviour also based on the auxiliary data.

[0083] xxiii. The behaviour determiner according to embodiment xxii, wherein the auxiliary data comprises energy consumption of a dwelling of the user, secured by the electronic lock.

[0084] xxiv. The behaviour determiner according to embodiment xxii or xxiii, wherein the auxiliary data comprises wireless-traffic data of the user.

[0085] xv. A computer program for identifying abnormal behaviour of a user, the computer program comprising computer program code which, when executed on a behaviour determiner causes the behaviour determiner to:

obtain, from an access control system, access data of the user, the access data indicating when the user has accessed an electronic lock in the access control system to gain access to a physical space secured by the electronic lock; and

determine that the access data indicates abnormal behaviour.

[0086] xvi. A computer program product comprising a computer program according to embodiment xxv and a computer readable means on which the computer program is stored.

[0087] The aspects of the present disclosure have mainly been described above with reference to a few embodiments. However, as is readily appreciated by a person skilled in the art, other embodiments than the ones disclosed above are equally possible within the scope of the invention, as defined by the appended patent claims. Thus, while

various aspects and embodiments have been disclosed herein, other aspects and embodiments will be apparent to those skilled in the art. The various aspects and embodiments disclosed herein are for purposes of illustration and are not intended to be limiting, with the true scope and spirit being indicated by the following claims.

CLAIMS

1. A method for identifying a health emergency of a user (6a, 6b), the method being performed in a behaviour determiner (1), the method comprising:

obtaining (40), from an access control system (10), access data of the user (6a, 6b), the access data indicating when the user has accessed an electronic lock (12a-i) in the access control system to gain access to a physical space secured by the electronic lock (12a-i);

determining (44) that the access data indicates a health emergency; and

transmitting (46) an alert message, indicating the health emergency for the user.

2. The method according to claim 1, wherein the determining (44) comprises determining that the access data indicates a health emergency when the access data indicates that the user accesses an electronic lock less than a threshold amount.

3. The method according to claim 1 or 2, wherein the determining (44) comprises determining that the access data indicates a health emergency when the access data indicates that the user accesses an electronic lock more than a threshold amount.

4. The method according to any one of the preceding claims, wherein the determining (44) comprises determining that the access data indicates a health emergency when the access data indicates that the user deviates more than a threshold from average behaviour of other users of the access control system.

5. The method according to any one of the preceding claims, wherein the determining (44) comprises determining that the access data indicates a health emergency based on a machine learning, ML, model.

6. The method according to claim 5, wherein the ML model comprises both a local ML model and a central ML model.

7. The method according to any one of the preceding claims, wherein the determining (44) is based also on a current time.

8. The method according to any one of the preceding claims, wherein the method is repeated and wherein the determining (44) comprises determining an increased level of confidence of health emergency, when a health emergency is repeatedly determined in successive iterations of the method.

9. The method according to any one of the preceding claims, further comprising:

obtaining (42) auxiliary data;

and wherein the step of determining (44) is based also on the auxiliary data.

10. The method according to claim 9, wherein the auxiliary data comprises energy consumption of a dwelling (16d-i) of the user, secured by the electronic lock (12a-i).

11. The method according to claim 9 or 10, wherein the auxiliary data comprises wireless-traffic data of the user.

12. A behaviour determiner (1) for identifying a health emergency of a user (6a, 6b), the behaviour determiner (1) comprising:

a processor (60); and

a memory (64) storing instructions (67) that, when executed by the processor, cause the behaviour determiner (1) to:

obtain, from an access control system (10), access data of the user (6a, 6b), the access data indicating when the user has accessed an electronic lock (12a-i) in the access control system to gain access to a physical space secured by the electronic lock (12a-i);

determine that the access data indicates a health emergency; and

transmit an alert message, indicating the health emergency for the user.

13. The behaviour determiner (1) according to claim 12, wherein the instructions to determine comprise instructions (67) that, when executed by the processor, cause the behaviour determiner (1) to determine that the access data indicates a health emergency when the access data indicates that the user accesses an electronic lock less than a threshold amount.

14. The behaviour determiner (1) according to claim 12 or 13, wherein the instructions to determine comprise instructions (67) that, when executed by the processor, cause the behaviour determiner (1) to determine that the access data indicates a health emergency when the access data indicates that the user accesses an electronic lock more than a threshold amount.

15. The behaviour determiner (1) according to any one of claims 12 to 14, wherein the instructions to determine comprise instructions (67) that, when executed by the processor, cause the behaviour determiner (1) to determine that the access data

indicates a health emergency when the access data indicates that the user deviates more than a threshold from average behaviour of other users of the access control system.

16. The behaviour determiner (1) according to any one of claims 12 to 15, wherein the instructions to determine comprise instructions (67) that, when executed by the processor, cause the behaviour determiner (1) to determine that the access data indicates a health emergency based on a machine learning, ML, model.

17. The behaviour determiner (1) according to claim 16, wherein the ML model comprises both a local ML model and a central ML model.

18. The behaviour determiner (1) according to claim 17, wherein the instructions to determine comprise instructions (67) that, when executed by the processor, cause the behaviour determiner (1) to determine that the access data indicates a health emergency based also on a current time.

19. The behaviour determiner (1) according to any one of claims 12 to 18, further comprising instructions (67) that, when executed by the processor, cause the behaviour determiner (1) to repeat the instructions to obtain and determine, and wherein the instructions to determine comprise instructions (67) that, when executed by the processor, cause the behaviour determiner (1) to determine an increased level of confidence of health emergency, when a health emergency is repeatedly determined in successive iterations of the method.

20. The behaviour determiner (1) according to any one of claims 12 to 19, further comprising instructions (67) that, when executed by the processor, cause the behaviour determiner (1) to:

obtain auxiliary data;

and wherein the instructions to determine comprise instructions (67) that, when executed by the processor, cause the behaviour determiner (1) to determine a health emergency also based on the auxiliary data.

21. The behaviour determiner (1) according to claim 20, wherein the auxiliary data comprises energy consumption of a dwelling (16d-i) of the user, secured by the electronic lock (12a-i).

22. The behaviour determiner (1) according to claim 20 or 21, wherein the auxiliary data comprises wireless-traffic data of the user.

23. A computer program (67, 91) for identifying a health emergency of a user (6a, 6b), the computer program comprising computer program code which, when executed on a behaviour determiner (1) causes the behaviour determiner (1) to:

obtain, from an access control system (10), access data of the user (6a, 6b), the access data indicating when the user has accessed an electronic lock (12a-i) in the access control system to gain access to a physical space secured by the electronic lock (12a-i);

determine that the access data indicates a health emergency; and

transmit an alert message, indicating the health emergency for the user.

24. A computer program product (64, 90) comprising a computer program according to claim 23 and a computer readable means on which the computer program is stored.

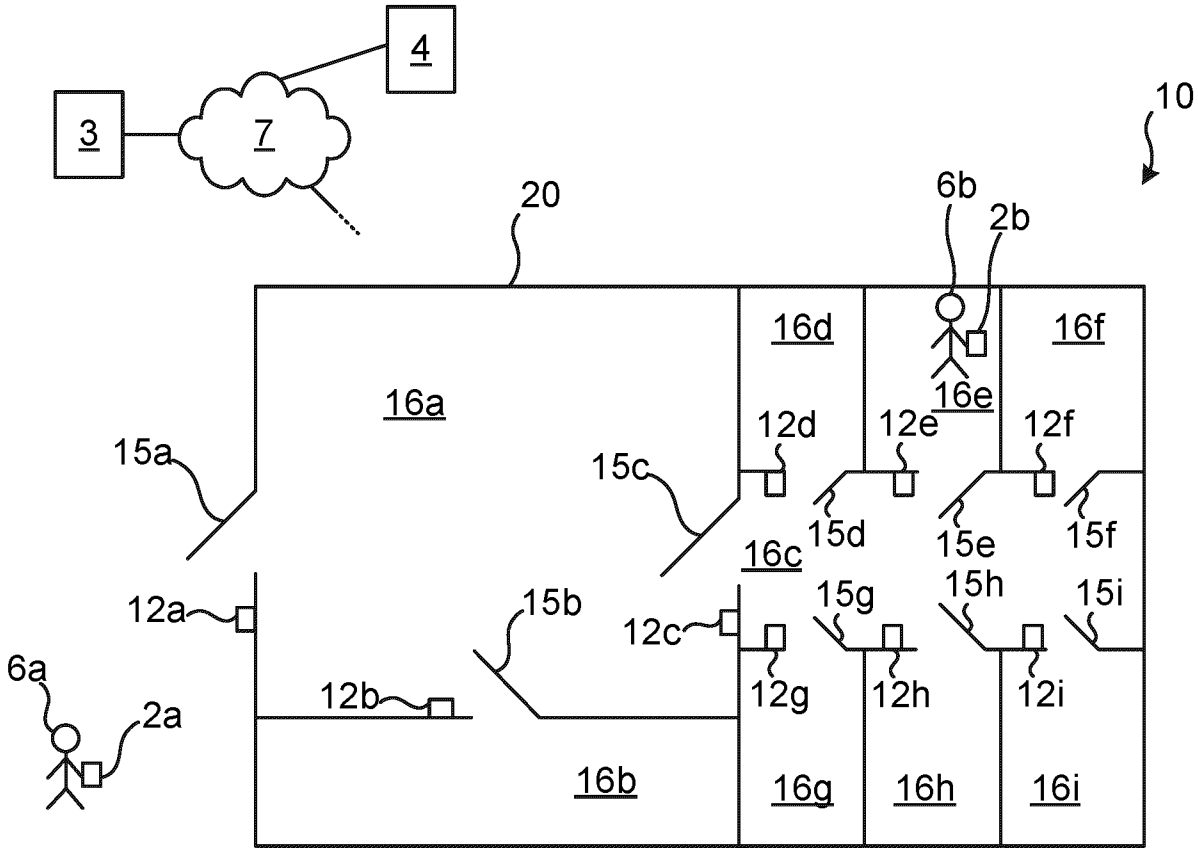

Fig. 1

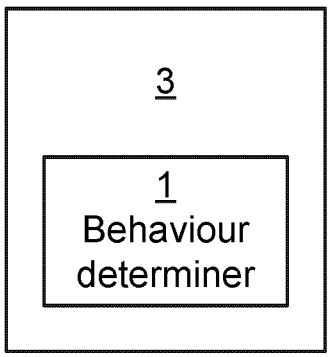

Fig. 2A

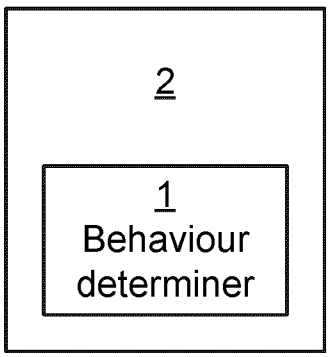

Fig. 2B

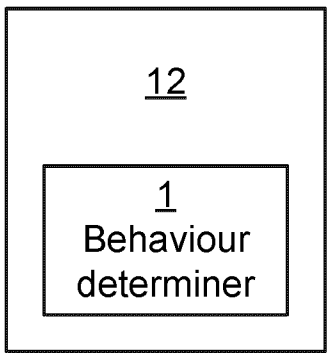

Fig. 2C

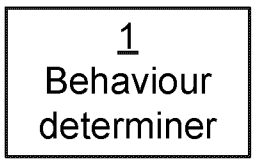

Fig. 2D

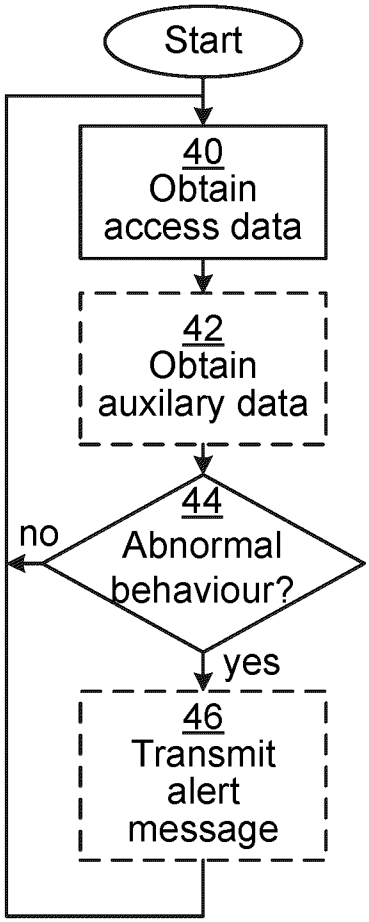

Fig. 3

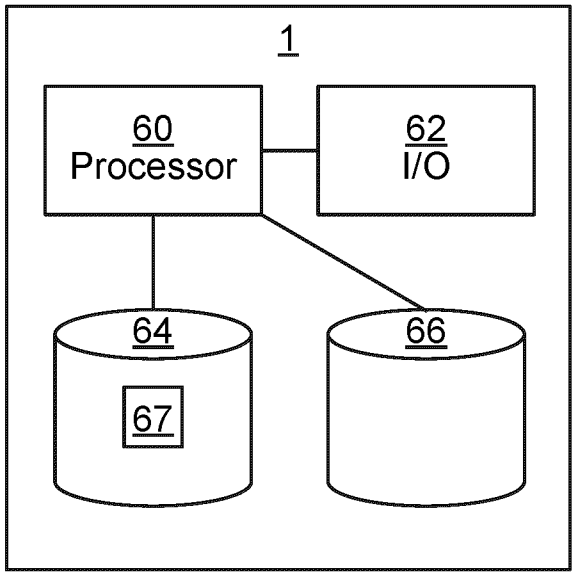

Fig. 4

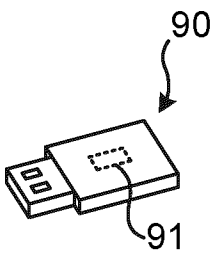

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/086178

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C9/00 G08B21/04
ADD. G08B21/18

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)
G07C G08B G06N

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, 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 2019/197866 A1 (MUKUNDALA SUMANTH KUMAR [IN] ET AL) 27 June 2019 (2019-06-27) claims 1-20 figures 1-3 paragraph [0003] - paragraph [0010] paragraph [0023] paragraph [0035] paragraph [0044] - paragraph [0048]	1-24
X	KR 2020 0091235 A (WINIADIMCHAE CO LTD [KR]) 30 July 2020 (2020-07-30) claims 1-6 paragraph [0010] - paragraph [0042]	1-24
X	CN 111 080 860 A (EVERSAFE ELECTRONIC LOCK CO LTD; YOUON TECH CO LTD) 28 April 2020 (2020-04-28) claims 1-9	1-24

☐ 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	Date of mailing of the international search report
4 April 2022	14/04/2022

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Hniene, Badr

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2021/086178

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2019197866 A1	27-06-2019	CN 110009867 A	12-07-2019
		EP 3503055 A1	26-06-2019
		ES 2847449 T3	03-08-2021
		US 2019197866 A1	27-06-2019
KR 20200091235 A	30-07-2020	NONE	
CN 111080860 A	28-04-2020	NONE	