(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 163 546 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
03.05.2017 Bulletin 2017/18

(51) Int Cl.:
G08B 21/04 *(2006.01)*

(21) Application number: **15306726.9**

(22) Date of filing: **29.10.2015**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
MA

(71) Applicant: **Thomson Licensing**
92130 Issy-les-Moulineaux (FR)

(72) Inventors:
- **GUEGAN, Marie**
  35576 Cesson-Sévigné (FR)
- **LAMBERT, Anne**
  35576 Cesson-Sévigné (FR)
- **GAUTIER, Eric**
  35576 Cesson-Sévigné (FR)

(74) Representative: **Huchet, Anne**
TECHNICOLOR
1-5, rue Jeanne d'Arc
92130 Issy-les-Moulineaux (FR)

(54) METHOD AND DEVICE FOR DETECTING ANOMALOUS BEHAVIOR OF A USER

(57) A method for detecting anomalous behavior of a user is described including logging first time-stamped event data of initial behavior of the user from sensors in an environment of the user for a period of time, mining the logged time-stamped event data to identify patterns of life routines of the user, determining which of the identified patterns are frequent patterns of life routines of the user, determining a duration of each of the identified frequent patterns, logging second time-stamped event data of subsequent behavior of the user from the sensors in the environment of the user and identifying a new occurrence of a known pattern of the life routines of the user, detecting anomalous behavior and creating an alert based on the detected anomalous behavior.

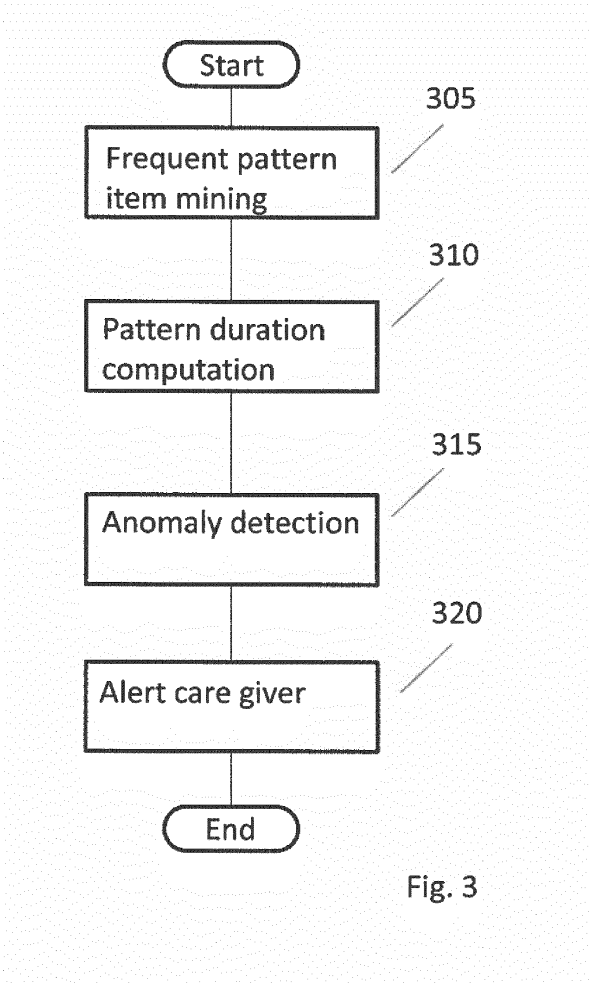

Fig. 3

EP 3 163 546 A1

Description

FIELD

[0001] The proposed method and apparatus relates to detection of anomalies in the duration of activities of daily living of elderly or handicapped users in their homes or non-medical residences.

BACKGROUND

[0002] This section is intended to introduce the reader to various aspects of art, which may be related to the present embodiments that are described below. This discussion is believed to be helpful in providing the reader with background information to facilitate a better understanding of the various aspects of the present disclosure. Accordingly, it should be understood that these statements are to be read in this light.

[0003] In the domain of the care of elderly and handicapped people staying in their own homes or in non-medical residences (such as senior apartment complexes or assisted living facilities), one key area of interest is the life habits of the individual. Care workers (givers) monitoring the elderly or handicapped individuals may effectively use a report on the life patterns of the person as a tool for diagnosis of behavioral or health problems. Anomalies may be detected for further investigation and alerts may be raised for immediate action in the case of an emergency.

[0004] To monitor the health of a smart home resident and detect anomalous behavior, some solutions rely on automatic recognition of daily living activities like standing, sitting, sleeping, etc... This approach requires a data collection infrastructure in the home implementing generally a large number of sensors (bed and chair occupancy sensors, etc...), which can be complex and expensive to implement. In addition sensors may sometimes be considered to be intrusive by the individual (camera, wearable sensors, etc...), consequently not widely accepted by elderly or handicapped individuals. Finally these solutions are frequently based on supervised machine learning techniques and require labeling a large amount of data to learn a model for activities. This is not always feasible.

[0005] Other nonintrusive anomaly detection approaches rely on sensors located in the living environment such as motion detectors or door contactors, enabling the individual not to be disturbed with the technology. These solutions, which are generally accepted by elderly and handicapped people are frequently based on unsupervised machine learning techniques and use sensory data directly to find outliers. However, such a model of a user's behavior does not have any information or knowledge as to whether the individual is sitting, standing, walking, etc.

SUMMARY

[0006] The proposed method and apparatus uses non-intrusive sensors in the home or non-medical residences to detect deviations in the time spent on activities of daily living. While principally directed to detecting anomalous behavior of elderly or handicapped individuals, the proposed method and apparatus are not so limited and may be employed to monitor prisoners, children or other individuals that find themselves in restricted environments. The description of the proposed method and apparatus uses elderly or handicapped individuals as examples. Using time-stamped sensor events, the proposed method and apparatus identifies and mines patterns in the sequence of sensor activation signals and records the patterns in a data base. The duration of patterns is then computed. The computed pattern durations are assigned to each pattern in the data base. A new behavior pattern occurs and is assigned an anomaly score based on the similarity of the new pattern's duration to known pattern durations. A care giver is alerted if the anomaly score of the new pattern is above a threshold. The detection of anomalous behavior is used to alert a care giver of the anomalous behavior. The care giver may be a nurse, a doctor, an aide, a family member etc. In a prison or other environment, a care giver may be a person who monitors the activities of the individual being monitored. The alert may be by phone, by email, by text message or any other reasonable means.

[0007] Because it is preferable to rely on non-intrusive sensors, the proposed method and apparatus use the non-intrusive approach to detect anomalies in the behavior of elderly or handicapped individuals in their homes or non-medical residences. The home or non-medical residences are equipped with sensors such as motion sensors and door contacts (non-intrusive sensors). It would be advantageous to detect anomalous behavior of users using the duration of activities of daily living. Detection of anomalous behavior is crucial to an ability to alert and dispatch help or a caregiver in response to the anomalous behavior. If an elderly or handicapped individual takes significantly more time for a given activity (bathroom, moving from room to room), this is often due to a physical problem (issue) or injury that has slowed the individual down. If the anomalous behavior is detected early enough then a care worker (giver) may be alerted and dispatched to help or provide intervention before the problem worsens and become critical requiring hospitalization or other more intense and costly intervention.

[0008] A method for detecting anomalous behavior of a user is described including logging first time-stamped event data of initial behavior of the user from sensors in an environment of the user for a period of time, mining the logged

time-stamped event data to identify patterns of life routines of the user, determining which of the identified patterns are frequent patterns of life routines of the user, determining a duration of each of the identified frequent patterns, logging second time-stamped event data of subsequent behavior of the user from the sensors in the environment of the user and identifying a new occurrence of a known pattern of the life routines of the user, detecting anomalous behavior and creating an alert based on the detected anomalous behavior. A server for detecting anomalous behavior of a user is also described including a receive data module, the receive data module logging first time-stamped event data of initial behavior of the user from sensors in an environment of the user for a period of time, an identify patterns module, the identify patterns module mining the time-stamped event data to identify patterns of life routines of the user, the identify patterns module in communication with the receive data module, a determine frequent patterns module, the determine frequent patterns module determining a duration of each of the identified frequent patterns, the determine frequent patterns module in communication with the identify patterns module, the receive data module logging second time-stamped event data of subsequent behavior of the user from the sensors in the environment of the user and identifying a new occurrence of a known pattern of the life routines of the user and an anomaly detection module, the anomaly detection module detecting anomalous behavior and creating an alert based on the detected anomalous behavior.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The proposed method and apparatus is best understood from the following detailed description when read in conjunction with the accompanying drawings. The drawings include the following figures briefly described below:

Fig. 1 shows an exemplary case, where one individual is living in a residence equipped with a non-intrusive data collection infrastructure and where each main room is covered by one omni-directional motion detector installed on the ceiling.
Fig. 2 is a schematic diagram of the proposed method and apparatus.
Fig. 3 is a flowchart of an exemplary embodiment of the proposed method.
Fig. 4 is a flowchart of an exemplary implementation of step 305 of Fig. 3.
Fig. 5 is a flowchart of an exemplary implementation of step 310 of Fig. 3.
Fig. 6 is a flowchart of an exemplary implementation of step 315 of Fig. 3.
Fig. 7 is a block diagram of an exemplary server that performs the proposed method.

[0010] It should be understood that the drawing(s) are for purposes of illustrating the concepts of the disclosure and is not necessarily the only possible configuration for illustrating the disclosure.

DETAILED DESCRIPTION

[0011] The present description illustrates the principles of the present disclosure. It will thus be appreciated that those skilled in the art will be able to devise various arrangements that, although not explicitly described or shown herein, embody the principles of the disclosure and are included within its scope.

[0012] All examples and conditional language recited herein are intended for educational purposes to aid the reader in understanding the principles of the disclosure and the concepts contributed by the inventor to furthering the art, and are to be construed as being without limitation to such specifically recited examples and conditions.

[0013] Moreover, all statements herein reciting principles, aspects, and embodiments of the disclosure, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future, i.e., any elements developed that perform the same function, regardless of structure.

[0014] Thus, for example, it will be appreciated by those skilled in the art that the block diagrams presented herein represent conceptual views of illustrative circuitry embodying the principles of the disclosure. Similarly, it will be appreciated that any flow charts, flow diagrams, state transition diagrams, pseudocode, and the like represent various processes which may be substantially represented in computer readable media and so executed by a computer or processor, whether or not such computer or processor is explicitly shown.

[0015] The functions of the various elements shown in the figures may be provided through the use of dedicated hardware as well as hardware capable of executing software in association with appropriate software. When provided by a processor, the functions may be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which may be shared. Moreover, explicit use of the term "processor" or "controller" should not be construed to refer exclusively to hardware capable of executing software, and may implicitly include, without limitation, digital signal processor (DSP) hardware, read only memory (ROM) for storing software, random access memory (RAM), and nonvolatile storage.

[0016] Other hardware, conventional and/or custom, may also be included. Similarly, any switches shown in the figures

are conceptual only. Their function may be carried out through the operation of program logic, through dedicated logic, through the interaction of program control and dedicated logic, or even manually, the particular technique being selectable by the implementer as more specifically understood from the context.

[0017] In the claims hereof, any element expressed as a means for performing a specified function is intended to encompass any way of performing that function including, for example, a) a combination of circuit elements that performs that function or b) software in any form, including, therefore, firmware, microcode or the like, combined with appropriate circuitry for executing that software to perform the function. The disclosure as defined by such claims resides in the fact that the functionalities provided by the various recited means are combined and brought together in the manner which the claims call for. It is thus regarded that any means that can provide those functionalities are equivalent to those shown herein.

[0018] Fig. 1 shows an exemplary case, where one individual is living in a residence equipped with a non-intrusive data collection infrastructure and where each main room is covered by one omni-directional motion detector installed on the ceiling. These main rooms are labeled the "bedroom", the "living", the "kitchen", the "bedroom2", the "office" and the corresponding motion sensors are respectively indicated as "mB", "mL", "mK", "mB2", "mO". Furthermore, one external "door" is equipped with a door contactor indicated as "cD". It should also be noted that should there be any corridors (halls), these could also be covered with one or more sensors. The sensors emit ON/OFF signals whether they are activated by something moving in front of the sensors (ON) or the sensors become silent (OFF). Door contacts may also be installed on the bedroom door, the office door, the bathroom door and perhaps even the refrigerator door. The door contacts emit OPEN/CLOSE signals whenever the door is opened or closed. All signals are collected in a single time-stamped file, one signal per line. The format includes the date, the time, the sensor identification and the event type (ON/OFF/OPEN/CLOSE).

[0019] Depending on the way data is collected and the way information is organized, in numerous cases data format can be reconstructed from data originally collected and provided by the collection infrastructure as a sequence of ordered time-stamped events. A representation of a time-stamped event (TSE) includes listing the events corresponding to the sensor activations together with the date and time at which the events occurred. The following is a short sample of such a data format for types of sensor including door activator and motion sensors:

Date	Time	Sensor	Event
2014-11-06	T16:59:10.966903	cD	OPEN
2014-11-06	T16:59:11.528494	mL	ON
2014-11-06	T16:59:12.773843	mL	OFF
2014-11-06	T16:59:13.768215	mL	ON
2014-11-06	T16:59:20.492125	mL	OFF
2014-11-06	T16:59:22.162185	cD	CLOSE
2014-11-06	T16:59:22.934276	mK	ON
2014-11-06	T16:59:24.467157	mL	ON
2014-11-06	T16:59:24.536898	mK	OFF
2014-11-06	T16:59:26.95258	mL	OFF
2014-11-06	T16:59:28.374536	mB	ON
2014-11-06	T16:59:30.897865	mB	OFF

[0020] In order to simplify the problem and without loss of generality, the special case where the person has been localized in the rooms using the sensor signals is considered. The sensor data is represented one time-stamped event per line below:

2014-11-06	T16:59:11.528494	LIVING
2014-11-06	T16:59:22.934276	KITCHEN
2014-11-06	T16:59:24.467157	LIVING
2014-11-06	T16:59:28.374536	BEDROOM

[0021] Here the person (individual, user) activated a sensor while he/she was in the living at 2014-11-06 T16:59:11.528494. The first step of the proposed method and apparatus (identification and mining patterns in the sequence of sensor activation signals and recording the patterns in a data base) includes detecting frequent patterns in the sequence of sensor activations or in the sequence of activities of the daily living (e.g. presence in room). If a pattern has occurred only once, for example, it is may not be useful, for among other reasons, that no typical duration distribution

can be calculated (computed) in a later step. The motion sensors and door contacts are not necessarily smart devices and they do not have sufficient processing power to perform the proposed method so the time-stamped event data is transmitted to a server for recordation (storage) and processing. The collected time-stamped event data is, thus, forwarded to a server where the collected time-stamped event data is used to identify the user's life patterns in their home or non-medical residence. For example, a pattern could be:

LIVING - KITCHEN - LIVING - BEDROOM

[0022] These patterns may be found using known methods of data base (data set) mining. During this step, it is unnecessary to use the time-stamp, although the time-stamp could also be used. A set (collection) of frequent patterns, each being characteristic of an activity of the daily living of the person is obtained by the server and recorded (stored) for further processing. Each pattern is represented by a set of its occurrences in the data set (data base).

[0023] In the second step (pattern duration computation), the frequently occurring pattern occurrences in the dataset and their duration are considered. For example, the duration of the occurrence of a pattern may be computed as the time difference between the time-stamp of the last item in the pattern and the timestamp of the first item in the pattern. Given its set of occurrences, a set of known typical durations of the data base (data set) of patterns of activities of daily living is obtained (determined, calculated).

[0024] In the third step (anomaly detection), given a new occurrence of an already known pattern, together with its duration, the probability of this duration is tested against known typical durations for this pattern. This may be done using statistical hypothesis testing or any other method that would compute a deviation score between the observed duration and the set of typical durations. For example, if a set of typical durations has a Gaussian distribution, then a duration that is greater than the mean plus (or minus) twice the standard deviation is an anomaly (it is outside of the confidence interval of 95% for this pattern). This step produces a confidence anomaly score for this new occurrence. The anomaly score may for instance be a Boolean (yes/no value) or the p-value obtained from the statistical hypothesis test.

[0025] If there is a pattern already stored for going to the bathroom from the bedroom in the middle of the night and there is a usual duration, then an anomaly may be detected if the monitored user goes to the bathroom from the bedroom and the usual duration is exceeded. The duration of each pattern is recomputed using the last (latest) occurrence of the pattern. Once the pattern duration exceeds usual durations for the pattern, an anomaly is detected and an alert is sent (transmitted). In practice, if the monitored person (user) usually spends half an hour and almost never spends a whole hour in the bathroom after leaving the bedroom, then it would take about an hour to detect the anomaly (incident). The sensitivity of anomaly detection may be adapted according to use cases (for example, it may be preferable to receive too many alerts as opposed to not enough alerts so the anomaly detection sensitivity may be set higher thus anomaly detection may occur earlier and vice versa).

[0026] It should be noted that a same pattern may be characteristic of several activities of the daily living. For example, going in the kitchen at night to drink water and going in the kitchen at noon to prepare lunch may exhibit similar patterns but very different durations. Thus, a pattern may exhibit several types of duration distributions. This may be detected by modeling the durations of the pattern as a mixture of distributions. These patterns may also be labeled differently based on the time of day at which the pattern occurred. In a last optional step (alert), a threshold may be used to determine which alerts should be raised for care givers. An alert may show the pattern occurrence, the duration observed and the confidence score for the anomaly.

[0027] Referring to Fig. 2, which is a schematic diagram of an exemplary embodiment of a proposed method and apparatus, the time-stamped event data is received and forwarded to a server for recordation (logging, storage) in a data base (data set). The data base (data set) is mined for frequently occurring patterns. The frequent patterns are stored at the server. The server then calculates (computes) the duration of the patterns. The typical pattern duration distributions are then calculated (computed). A new pattern occurrence is then received by the server and the new pattern is compared to the existing patterns and their durations to determine if there is anomalous behavior (an anomaly). An anomaly score is then calculated (computed). The anomaly score is a confidence anomaly score. If a set of typical durations has a Gaussian distribution, then a duration that is greater than the mean plus (or minus) twice the standard deviation is an anomaly (it is outside of the confidence interval of 95% for this pattern). The anomaly score may for instance be a Boolean (yes/no value) or the p-value obtained from the statistical hypothesis test.

[0028] Fig. 3 is a flowchart of an exemplary embodiment of a proposed method. At 305 the server mines the time-stamped event data to identify frequent patterns of user life routines. The number of occurrences of the patterns may be compared to a threshold to determine if they are occurring with sufficient frequency. If a pattern has occurred only once, for example, it is not going to be useful for among other reasons no typical duration distribution can be calculated (computed) in a later step. These patterns may be found using known methods of data base (data set) mining. During this step, it is unnecessary to use the time-stamp, although the time-stamp could also be used. A set of frequently occurring patterns, each being characteristic of an activity of the daily living of the person is obtained by the server and recorded (logged, stored) for further processing. Each pattern is represented by a set of its occurrences in the data set

(data base). At 310 the duration of the frequently occurring patterns is calculated (computed). The duration of the occurrence of a pattern may be computed as the time difference between the time-stamp of the last item in the pattern and the time-stamp of the first item in the pattern. Given its set of occurrences, a set of known typical durations of the data base (data set) of patterns of activities of daily living is obtained (determined, calculated). At 315 the server receives new time-stamped event data and identifies a new pattern occurrence from the newly received time-stamped event data. Given a new occurrence of an already known pattern, together with its duration, the probability of this duration is tested against known typical durations for this pattern. This may be done using statistical hypotheses testing or any other method that would compute a deviation score between the observed duration and the set of typical durations. For example, if a set of typical durations has a Gaussian distribution, then a duration that is greater than the mean plus (or minus) twice the standard deviation is an anomaly (it is outside of the confidence interval of 95% for this pattern). This step produces a confidence anomaly score for this new occurrence. The anomaly score may for instance be a Boolean (yes/no value) or the p-value obtained from the statistical hypothesis test. The server creates one or more alerts based on the anomalous behavior of the user and at 320 the server forwards the alerts to the care giver.

[0029] Fig. 4 is a flowchart of an exemplary implementation of step 305 of Fig. 3. At 405 the server receives time-stamped event data for a period of time and logs (records, stores) the received time-stamped data. The period of time for collection of the time-stamped event data is a period of time necessary to collect and identify enough patterns to be statistically meaningful. At 410 the server identifies patterns of user life routines. At 415 the server uses a threshold to isolate frequently occurring pattern of user life routines. If a pattern has occurred only once, for example, it is not going to be useful for among other reasons no typical duration distribution can be calculated (computed) in a later step. At 420 the frequent occurring patterns of user life routines are stored in a data base.

[0030] Fig. 5 is a flowchart of an exemplary implementation of step 310 of Fig. 3. At 505 the duration for each frequently occurring pattern is calculated (computed). This is accomplished by taking the difference of the time-stamp of the first item of each frequently occurring pattern of the user's life routine from the time-stamp of the last item of the respective frequently occurring pattern of user's life routine. At 510 the time duration of each frequently occurring pattern of user's life routine is stored back in the server's data base (data set) along with the corresponding frequently occurring pattern of the user's life routine.

[0031] Fig. 6 is a flowchart of an exemplary implementation of step 315 of Fig. 3. At 605 the server receives and logs (stores, records) new time-stamped event data and at 610 the server identifies a new pattern. Both 605 and 610 are or can be performed by 405 and 410 of the frequent pattern mining process described above and shown in Fig. 4. At 615 the server determines the duration of the new pattern. This is or can be performed by 505 of the pattern duration computation process described above and shown in Fig. 5. At 620 the server determines if the new pattern is known. Determination of if the new pattern is known can be performed before duration computation or during new pattern identification if a list of known patterns exists to which a new pattern can be compared. At 625 the server compares the new known pattern against the typical pattern duration distribution of the pattern. At 630 the server determines if there is an anomaly (anomalous behavior). That is, an anomaly score (confidence anomaly score) is calculated (computed, determined) for the new pattern. The server also creates one or more alerts based on the detected anomalous behavior at 630.

[0032] Fig. 7 is a block diagram of an exemplary server that performs the proposed method. The server has three main modules each of which has submodules. The three main modules are the Frequent Pattern Item Mining Module, the Pattern Duration Computation Module and the Anomaly Detection Module. There is also a module to report detected anomalies of the user's behavior to a care giver. The Frequent Pattern Item Mining Module logs time-stamped event data of initial behavior of the user for a period of time at the Receive Data Module. The period of time for collection of the time-stamped event data is a period of time necessary to collect and identify enough patterns to be statistically meaningful. The logged time-stamped event data of the initial behavior of the user is forwarded to the Identify Patterns Module which identifies (mines) patterns of user life routines. The Identify Patterns Module forwards the identified patterns of the user's life routine to the Determine Frequent Patterns Module, which uses a threshold to isolate frequently occurring pattern of user life routines. If a pattern has occurred only once, for example, it is not going to be useful for among other reasons no typical duration distribution can be calculated (computed) in a later step. The Determine Frequent Patterns Module forwards the frequent patterns to the Store Frequent Patterns Module which stores the frequent occurring patterns of user life routines in a data base (data set).

[0033] The Store Frequent Patterns Module is in communication with the Calculate Duration of Each Pattern Occurrence Module which calculates (computes) the duration for each frequently occurring pattern. This is accomplished by taking the difference of the time-stamp of the first item of each frequently occurring pattern of the user's life routine from the time-stamp of the last item of the respective frequently occurring pattern of user's life routine. The Calculate Duration of Each Pattern Occurrence Module forwards the durations of each frequently occurring pattern to the Store Durations Module which stores the time duration of each frequently occurring pattern of user's life routine in the server's data base (data set) along with the corresponding frequently occurring pattern of the user's life routine.

[0034] The Store Frequent Patterns Module and the Identify Patterns Module are in communication with the Determine

if New Pattern is Known Module which determines if the new logged pattern of subsequent behavior of the user is known. The Determine if New Pattern is Known Module forwards the new known pattern to the Compare New Pattern Against Typical Pattern Duration Distribution Module which compares the new known pattern against the typical pattern duration distribution of the pattern. The Store Durations Module and the Calculate Duration of Each Pattern Occurrence Module are in communication with the Compare New Pattern Against Typical Pattern Duration Distribution Module. The Compare New Pattern Against Typical Pattern Duration Distribution Module forwards the results of the comparison to the Detect Anomaly Module which determines if there is an anomaly (anomalous behavior). That is, an anomaly score (confidence anomaly score) is calculated (computed, determined) for the new pattern. The Detect Anomaly Module also creates an alert based on the detected anomalous behavior of the user. The Detect Anomaly Module forwards any detected anomalies and alerts to the Report Anomaly Module which reports detected anomalies to a care giver.

[0035] It is to be understood that the proposed method and apparatus may be implemented in various forms of hardware, software, firmware, special purpose processors, or a combination thereof. Special purpose processors may include application specific integrated circuits (ASICs), reduced instruction set computers (RISCs) and/or field programmable gate arrays (FPGAs). Preferably, the proposed method and apparatus is implemented as a combination of hardware and software. Moreover, the software is preferably implemented as an application program tangibly embodied on a program storage device. The application program may be uploaded to, and executed by, a machine comprising any suitable architecture. Preferably, the machine is implemented on a computer platform having hardware such as one or more central processing units (CPU), a random access memory (RAM), and input/output (I/O) interface(s). The computer platform also includes an operating system and microinstruction code. The various processes and functions described herein may either be part of the microinstruction code or part of the application program (or a combination thereof), which is executed via the operating system. In addition, various other peripheral devices may be connected to the computer platform such as an additional data storage device and a printing device.

[0036] It should be understood that the elements shown in the figures may be implemented in various forms of hardware, software or combinations thereof. Preferably, these elements are implemented in a combination of hardware and software on one or more appropriately programmed general-purpose devices, which may include a processor, memory and input/output interfaces. Herein, the phrase "coupled" is defined to mean directly connected to or indirectly connected with through one or more intermediate components. Such intermediate components may include both hardware and software based components.

[0037] It is to be further understood that, because some of the constituent system components and method steps depicted in the accompanying figures are preferably implemented in software, the actual connections between the system components (or the process steps) may differ depending upon the manner in which the proposed method and apparatus is programmed. Given the teachings herein, one of ordinary skill in the related art will be able to contemplate these and similar implementations or configurations of the proposed method and apparatus.

Claims

1. A method for detecting anomalous behavior of a user, said method comprising:

logging (305, 405) first time-stamped event data of initial behavior of said user from sensors in an environment of said user for a period of time;
mining (305, 410) said logged time-stamped event data to identify patterns of life routines of said user;
determining (305, 415) which of said identified patterns are frequent patterns of life routines of said user;
determining (310, 405) a duration of each of the identified frequent patterns;
logging (315, 605) second time-stamped event data of subsequent behavior of said user from said sensors in said environment of said user and identifying a new occurrence of a known pattern of said life routines of said user;
detecting (315, 630) anomalous behavior responsive to said determined duration of each of the identified frequent patterns compared to said identified new occurrence of said known pattern of said life routines of said user; and
creating (315, 630) an alert based on said detected anomalous behavior.

2. The method according to claim 1, wherein said mining further comprises:

determining frequent occurring patterns by comparing a number of occurrences of said pattern to a threshold;
storing said identified frequent occurring patterns; and
reporting said alert of detected anomalous behavior of said user to a care giver.

3. The method according to claim 2, wherein said threshold is selected based on a statistically meaningful number of occurrences of patterns.

4. The method according to claim 1, wherein said duration further comprises:

calculating said duration of each of the identified frequent patterns by subtracting a time-stamp of a first item of each of the identified frequent patterns from a time-stamp of a last item of each of the identified frequent patterns; and
storing said calculated durations of each of said identified frequent patterns.

5. The method according to claim 1, wherein said detecting further comprises:

determining if the new occurrence of an identified pattern is an anomaly;
comparing a duration of said new occurrence against typical durations for said known pattern of said user's life routine; and
calculating an anomaly score.

6. The method according to claim 5, wherein said anomaly score is a Boolean value.

7. The method according to claim 5, wherein said anomaly score is a p-value obtained from a statistical hypothesis test.

8. An apparatus for detecting anomalous behavior by a user, comprising:

means for logging time-stamped event data of initial behavior of said user from sensors in an environment of said user for a period of time (1, 11);
means for mining said logged time-stamped event data to identify patterns of life routines of said user(1, 12);
means for determining which of said identified patterns are frequent patterns of life routines of said user (1, 13);
means for determining a duration of each of the identified frequent patterns (3, 31);
means for logging new time-stamped event data of subsequent behavior of said user from said sensors in said environment of said user and identifying a new occurrence of a known pattern of said life routines of said user (1, 11);
means for detecting anomalous behavior responsive to said determined duration of each of the identified frequent patterns compared to said identified new occurrence of said known pattern of said life routines of said user (2, 22); and
means for creating an alert based on said detected anomalous behavior (2, 23).

9. The apparatus according to claim 8, wherein said means for mining further comprises:

means for determining frequent occurring patterns by comparing a number of occurrences of said pattern to a threshold;
means for storing said identified frequent occurring patterns; and
means for reporting said alert of said detected anomalous behavior of said user to a care giver.

10. The apparatus according to claim 9, wherein said threshold is selected based on a statistically meaningful number of occurrences of patterns.

11. The apparatus according to claim 8, wherein said duration further comprises:

means for calculating said duration of each of the identified frequent patterns by subtracting a time-stamp of a first item of each of the identified frequent patterns from a time-stamp of a last item of each of the identified frequent patterns; and
means for storing said calculated durations of each of said identified frequent patterns.

12. The apparatus according to claim 8, wherein said detecting further comprises:

means for determining if the new occurrence of the known pattern is an anomaly by comparing a duration of said new occurrence against typical durations for said known pattern of said user's life routine; and
means for calculating an anomaly score.

13. The apparatus according to claim 12, wherein said anomaly score is a Boolean value.

14. The apparatus according to claim 12, wherein said anomaly score is a p-value obtained from a statistical hypothesis test.

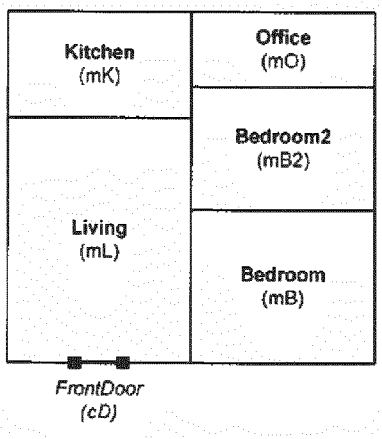
Kitchen
(mK)
Office
(mO)
Bedroom2
(mB2)
Living
(mL)
Bedroom
(mB)
FrontDoor
(cD)

Fig. 1

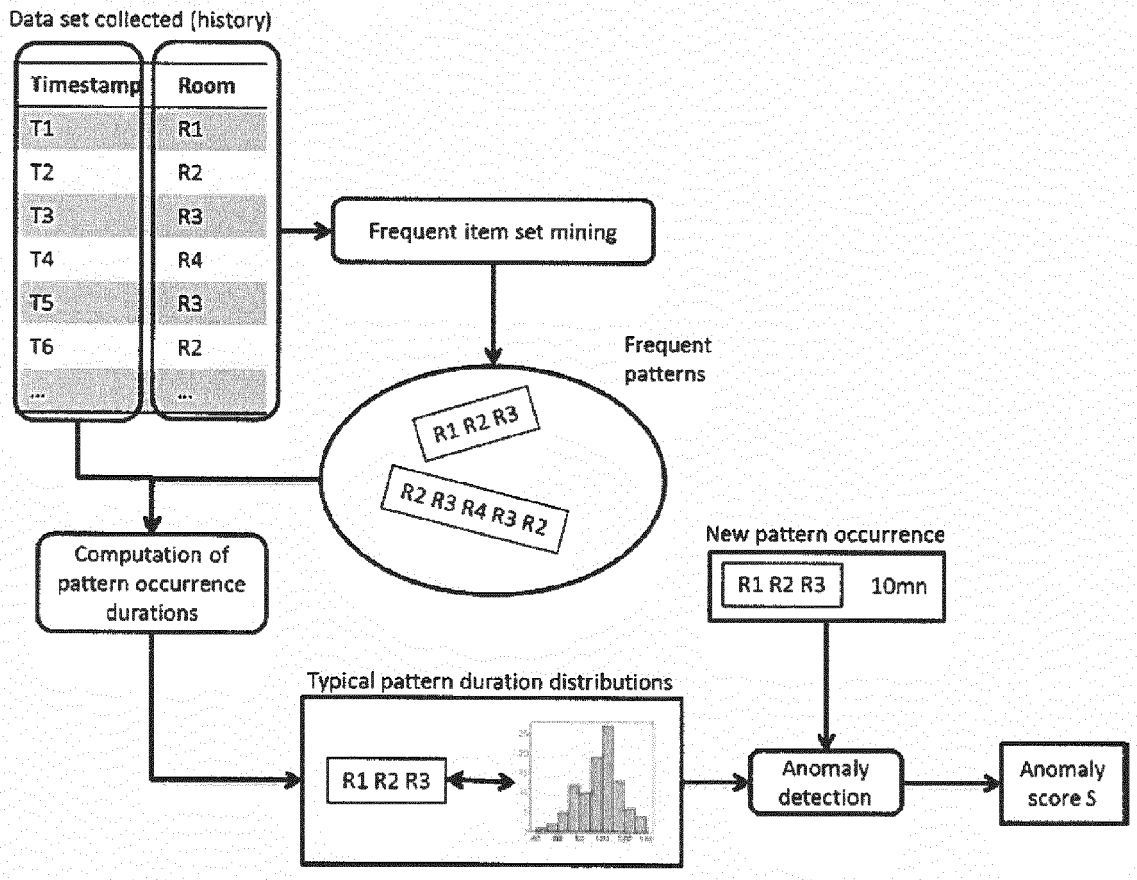
Data set collected (history)
Timestamp
Room
T1
R1
T2
R2
T3
R3
T4
R4
T5
R3
T6
R2
...
...
Frequent item set mining
Frequent patterns
R1 R2 R3
R2 R3 R4 R3 R2
Computation of pattern occurrence durations
New pattern occurrence
R1 R2 R3
10mn
Typical pattern duration distributions
R1 R2 R3
Anomaly detection
Anomaly score S

Fig. 2

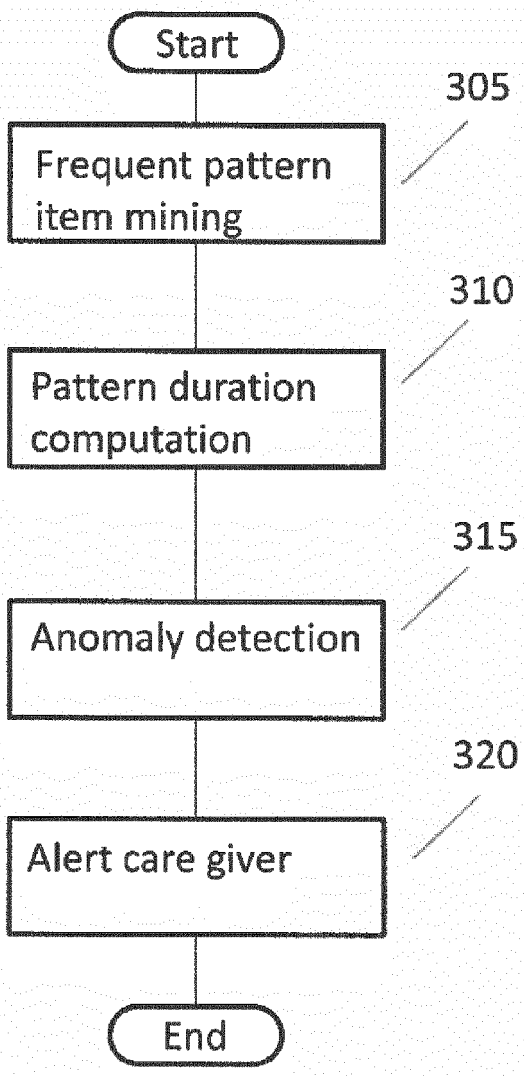
Start
305
Frequent pattern item mining
310
Pattern duration computation
315
Anomaly detection
320
Alert care giver
End

Fig. 3

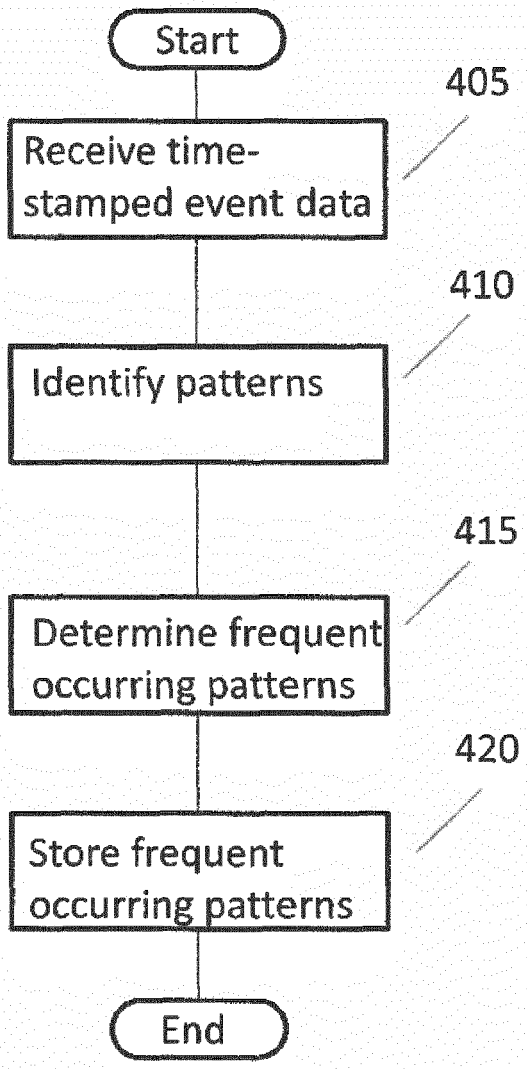
Start
405
Receive time-stamped event data
410
Identify patterns
415
Determine frequent occurring patterns
420
Store frequent occurring patterns
End

Fig. 4

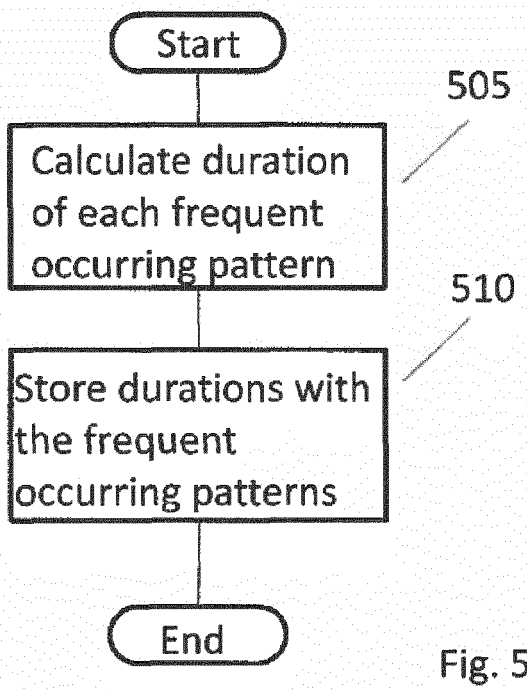
Start
505
Calculate duration of each frequent occurring pattern
510
Store durations with the frequent occurring patterns
End

Fig. 5

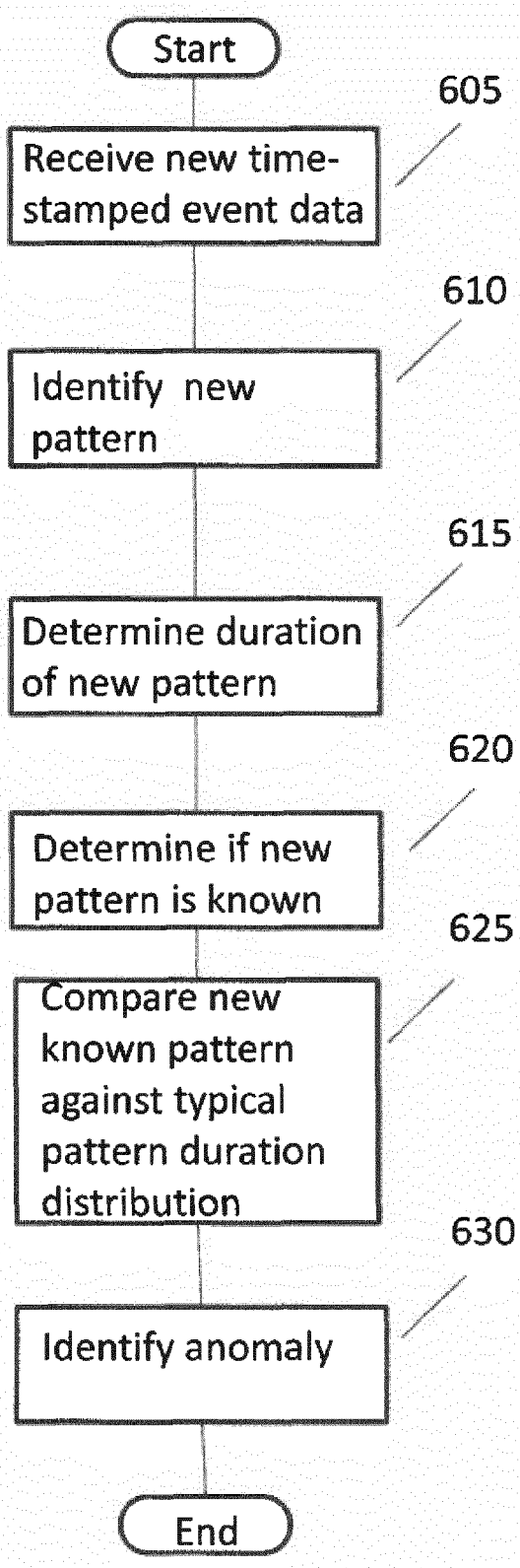
Start
605
Receive new time-stamped event data
610
Identify new pattern
615
Determine duration of new pattern
620
Determine if new pattern is known
625
Compare new known pattern against typical pattern duration distribution
630
Identify anomaly
End

Fig. 6

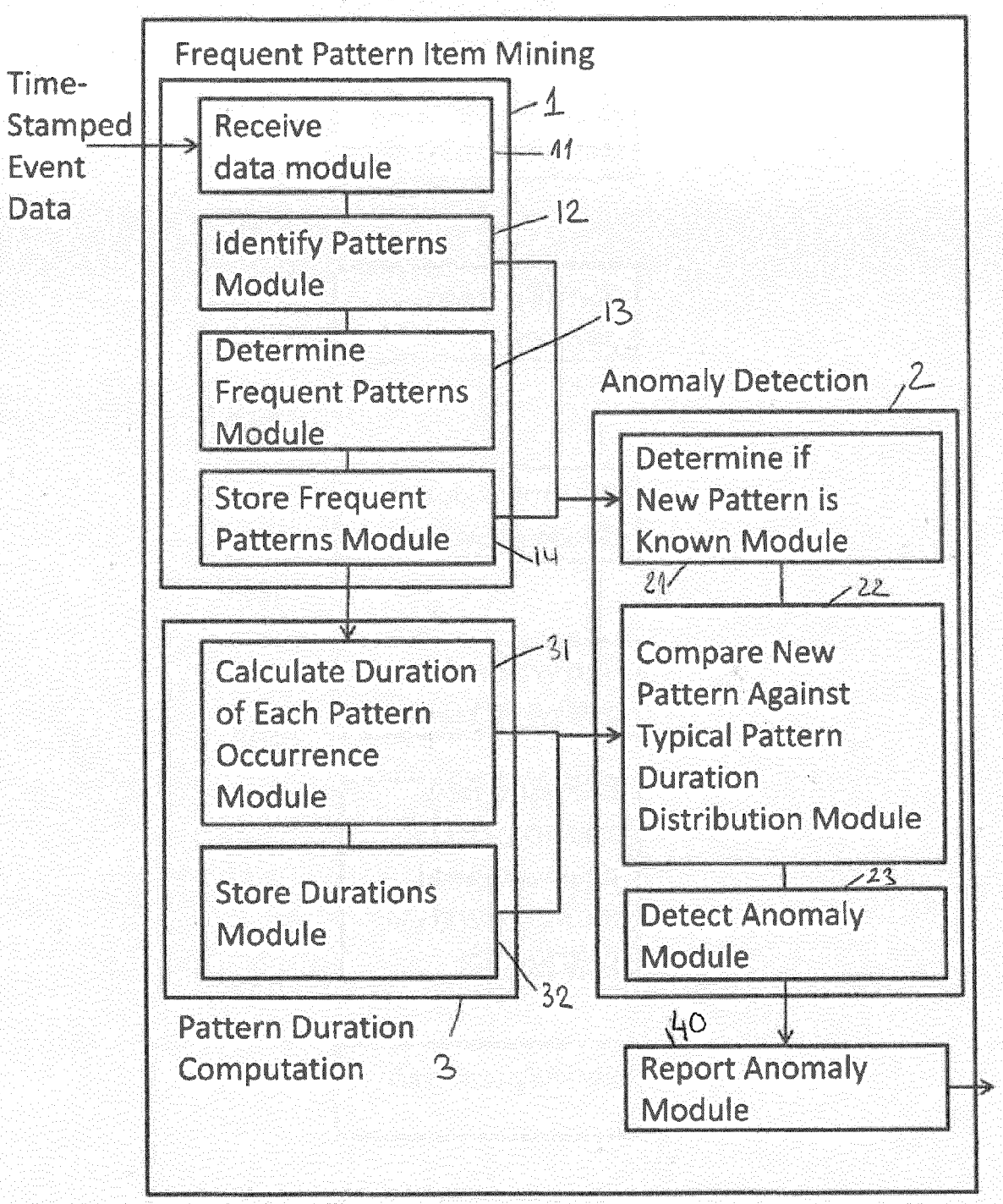
Time-Stamped Event Data
Frequent Pattern Item Mining
1
Receive data module
11
Identify Patterns Module
12
Determine Frequent Patterns Module
13
Store Frequent Patterns Module
14
Anomaly Detection
2
Determine if New Pattern is Known Module
21
22
Compare New Pattern Against Typical Pattern Duration Distribution Module
23
Detect Anomaly Module
Calculate Duration of Each Pattern Occurrence Module
31
Store Durations Module
32
Pattern Duration Computation
3
40
Report Anomaly Module

Fig. 7

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 15 30 6726

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2015/127491 A1 (UNIV MONASH [AU]) 3 September 2015 (2015-09-03) * paragraphs [0058] - [0077] * * paragraphs [0086] - [0104] *	1-4,8-11	INV. G08B21/04
X	JP 2001 216585 A (SEKISUI CHEMICAL CO LTD) 10 August 2001 (2001-08-10) * paragraphs [0002] - [0005] * * paragraphs [0010] - [0026] *	1-4,8-11	
X	US 2010/063774 A1 (COOK DIANE J [US] ET AL) 11 March 2010 (2010-03-11) * paragraphs [0019] - [0040] * * paragraphs [0054] - [0066] *	1-4,8, 10,11	
X	US 2011/295583 A1 (HOLLOCK STEPHEN [GB] ET AL) 1 December 2011 (2011-12-01) * paragraphs [0082] - [0108] *	1-4,8-11	
X	US 2003/059081 A1 (TRAJKOVIC MIROSLAV [US]) 27 March 2003 (2003-03-27) * paragraphs [0017] - [0022] * * paragraphs [0027] - [0036] *	1-4,8-11	TECHNICAL FIELDS SEARCHED (IPC) G08B

~~The present search report has been drawn up for all claims~~

Place of search	Date of completion of the search	Examiner
The Hague	5 April 2016	Tanguy Michotte

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Application Number
EP 15 30 6726

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing claims for which payment was due.

☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for those claims for which no payment was due and for those claims for which claims fees have been paid, namely claim(s):

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for those claims for which no payment was due.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

☐ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

☒ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

2-4, 9-11(completely); 1, 8(partially)

☐ The present supplementary European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims (Rule 164 (1) EPC).

Europäisches Patentamt
European Patent Office
Office européen des brevets

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 15 30 6726

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 2-4, 9-11(completely); 1, 8(partially)

A method for detecting anomalous behaviour of a user, wherein frequent patterns of life routines of said user are identified by comparing a number of occurrences of said pattern to a threshold. An apparatus for applying that method.

1.1. claims: 4, 11(completely); 1, 8(partially)

A method for detecting anomalous behaviour of a user, wherein a duration of frequent patterns of life routines is computed using time-stamps differences. An apparatus for applying that method.

---

2. claims: 5-7, 12-14(completely); 1, 8(partially)

A method for detecting anomalous behaviour of a user, wherein an anomaly score is calculated. An apparatus for applying that method.

Please note that all inventions mentioned under item 1, although not necessarily linked by a common inventive concept, could be searched without effort justifying an additional fee.

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 15 30 6726

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

05-04-2016

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2015127491 A1	03-09-2015	NONE	
JP 2001216585 A	10-08-2001	NONE	
US 2010063774 A1	11-03-2010	US 2010063774 A1	11-03-2010
		US 2013238538 A1	12-09-2013
US 2011295583 A1	01-12-2011	EP 2390820 A2	30-11-2011
		GB 2480805 A	07-12-2011
		US 2011295583 A1	01-12-2011
US 2003059081 A1	27-03-2003	AU 2003237024 A1	19-01-2004
		CN 1666232 A	07-09-2005
		EP 1520258 A2	06-04-2005
		JP 4936662 B2	23-05-2012
		JP 5143212 B2	13-02-2013
		JP 2005531845 A	20-10-2005
		JP 2011081823 A	21-04-2011
		US 2003059081 A1	27-03-2003
		WO 2004003848 A2	08-01-2004

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82