

COMPUTER-IMPLEMENTED SYSTEM FOR MANAGING A PLURALITY OF REPOSITORIES

FIELD OF INVENTION

5

The invention relates to a computer-implemented system. More particularly, the invention relates to a computer-implemented system for managing a plurality of repositories.

10 BACKGROUND OF THE INVENTION

Storage management is essential for any industries. Managing storage can be particularly difficult in areas such as repositories or a container where materials or containers are deposited and stored over a large area. Security level of such repositories
15 or containers are often a concern of the users when comes to storing privacy documents or valuable contents. Therefore, the prevention of unauthorized access to such repositories or containers by a third party from being able to freely access is important. Conventionally, mechanical locks are the most common method that is applied in order to secure the repositories or containers. Although multiple locks can be applied to one
20 repository, however there are still chances for unwanted breakthrough of the repository to be happened.

Over the years, there are a few patented technologies in providing teachings for securing a closure. Of interest to a US patent document US20050044906A1, which
25 discloses a security system for controlling access to a moveable enclosure. The system comprises a lock on the moveable enclosure, a control circuit couple to the lock and configured to receive an entry code and open the lock in response to receipt of the entry code, a Global Positioning System device couple to the control circuit and configured to generate latitude and longitude data relating to the moveable enclosure; and a

personal computing device wirelessly coupleable to the control circuit and configured to generate the entry code using GPS latitude and longitude data. However, the system does not perform any authentication on user's identity before providing the entry code.

- 5 Another patent document US20180061149A1 also discloses a portable electronic wireless lock for efficiently managing and assuring the safety, quality and security of goods stored within a truck. The system comprises a portable electronic wireless lock for ensuring the safety of goods and is controlled by a smartphone, which also acts as a communications hub between the lock and a truckload owner or supervisor. The
- 10 electronic lock permit only a limited number of locking cycles initiated by a truck driver until a loading supervisor intercedes in compliance with FSMA. However, the drawbacks of the system is that the system allows a single device to unlock a multiple locks of the trucks.
- 15 On the other hand, another patent document JP2006336255A also discloses an electronic lock to prevent the opening and closing of the delivery container. The lock comprises a first communication means and second communication means for receiving the unlocking information for unlock the electronic lock, and an electronic lock controller for locking and unlocking the electronic lock according to the unlocking
- 20 information received by the first communication means and the second communication means. However, the unlocking process of the electronic lock is not monitored by an admin server for ensuring the authorization of the user.

- To summarize, it is desirable to develop and provide a system which is able to overcome
- 25 the aforementioned drawbacks. This invention provides such a system.

SUMMARY OF INVENTION

The main objective of the invention is to provide users with a computer-implemented

system for managing a plurality of repositories, the system comprising a server; a plurality of mobile devices in communication with the server via a communication network; and a plurality of storage unit stored within the repositories, wherein the storage unit and the repositories are individually secured by at least one locking
5 mechanism.

Preferably, the server may be configured to generate at least one access code for unlocking a designated storage unit with a designated repository upon receiving a request and to transmit the generated codes to the designated mobile device
10 respectively.

Preferably, the mobile device may be further configured to establish a communication link to the locking mechanisms of said storage unit and/or said repository via a short range radio frequency protocol, to transmit at least one instruction for unlocking the
15 linked locking mechanisms upon successful authentication.

Preferably, the access key may further includes a time stamp for allowing the unlocking of the linked locking mechanisms within a predetermined time frame.

20 Preferably, the server may further includes a storage subsystems for storing various databases information.

Preferably, the short range radio frequency communication technique operates at frequencies range of substantially 2402 MHz and 2480 MHz.
25

Preferably, the locking mechanism may in the form of a robust lock for securing an entrance of the repository.

Preferably, the robust lock may includes a portable battery to provide power supply for

actuating the robust lock.

Preferably, the locking mechanism may in the form of portable lock for securing the storage unit.

5

Preferably, the mobile device may be pre-installed with an application configured to perform authentication and instructs the unlocking of the locking mechanisms.

One skilled in the art will readily appreciate that the invention is well adapted to carry
10 out the objects and obtain the ends and advantages mentioned, as well as those inherent therein. The embodiments described herein are not intended as limitations on the scope of the invention.

15 BRIEF DESCRIPTION OF THE DRAWINGS

For the purpose of facilitating an understanding of the invention, there is illustrated in the accompanying drawing the preferred embodiments from an inspection of which
when considered in connection with the following description, the invention, its
20 construction and operation and many of its advantages would be readily understood and appreciated.

Figure 1 is a diagram illustrating the repositories management system.

25 Figure 2 is a diagram illustrating an embodiment of the robust lock.

Figure 3 is a diagram illustrating an embodiment of the portable lock.

DETAILED DESCRIPTION OF THE INVENTION

The invention will now be described in greater detail, by way of example, with reference to the drawings.

5

Conditional language used herein, such as, among others, “can,” “could,” “might,” “may,” “e.g.,” and the like, unless specifically stated otherwise understood within the context as used, is generally intended to convey that certain embodiments include, while other embodiments do not include, certain features, elements and/or steps. Thus, such conditional language is not generally intended to imply that features, elements and/or steps are in any way required for one or more embodiments or that one or more embodiments necessarily include logic for deciding, with or without author input or prompting, whether these features, elements and/or steps are included or are to be performed in any particular embodiment. The terms “comprising”, “including”, “having”, and the like are synonymous and are used inclusively, in an opened fashion, and do not exclude additional elements, features, acts, operations and so forth. Also the term “or” is used in its exclusive sense (and not in its inclusive sense) so that when used, for example, to connect a list of elements, the term “or” means one, some or all of the elements in the list.

20

The system disclosed herein may be applied within a number of different devices and computer systems, including, for example, general-purpose computing systems, telephone computing systems, laptop computers, cellular phones, personal digital assistants (PDAs), tablet computers, video capturing devices, video game consoles, speech processing systems, distributed computing environments, etc. thus the components, components and/or processes described may be combined or rearranged without departing from the scope of the present disclosure. The functionality of any component described may be allocated among multiple components, or combined with a different component. As discussed in the present disclosure, any or all of the

components may be embodied in software implemented by a processing unit. Further, one or more of the components may be omitted from the processes entirely.

The present invention provides a system for managing a plurality of repositories over
5 any form of communication network, such as Internet or a private local or wide area network, for the purpose of regulating access to the repositories.

As used herein, the term “Application” and/or “Software” refer to all, or a portion of a computer program or software code that carries out a specific function and may be used
10 alone or combined with other programs. It comprises computer program instructions adapted for execution by a hardware element, such as a processor, wherein the instruction comprise commands that when executed to cause the processor to perform a corresponding set of command. The software may be written or coded using a programming language, and stored using any type of non-transitory computer-readable
15 media or machine-readable media well known in the art. Examples of software in the present disclosure comprise any software components, programs, applications, computer programs, application programs, system programs, machine programs and operating system software.

20 As used herein, the term “repositories” refers to a place, a room or a container where an article and/or an item is deposited or stored. Examples of repositories shall include but not limit to a room, a vault, shipping containers to a warehouse and/or a building or any enclosure that is spacious for allowing the storage of a quantity of items therewithin.

25

Referring to **Fig. 1**, a computer-implemented system for managing a plurality of repositories is illustrated. The system comprises a server **100**, a plurality of mobile devices **200** in communication with the server **100**, and a plurality of storage unit stored within the repositories, wherein the storage unit and the repositories are individually

secured by at least one locking mechanism. Preferably, the server **100** is configured to generate at least one access code for unlocking a designated storage unit with a designated repository upon receiving a request and to transmit the generated codes to the designated mobile device **200** respectively. The mobile device **200** then further
 5 configured to establish a communication link to the locking mechanisms of said storage unit and/or said repository via a short range radio frequency protocol, for receiving at least one instruction to unlock the linked locking mechanism upon successful authentication.

10 Preferably, the short range radio frequency communication technique operates at frequencies range of substantially 2402 MHz and 2480 MHz. However, it should be understood that the short range radio frequency communication technique any other techniques, technologies, and/or methods that is able to achieve the objective of establishing communication link within a short range.

15 Preferably, the access code may include a variety of data. The data can be biometric codes of any kind such as fingerprints and/or retinal scans, barcodes, radio frequency codes, infrared, proximity based, sound codes, numbers, letters, digital signatures, public and private key generated codes, implant sensors of any kind, wearable sensors
 20 and/or activators such as Bluetooth device or card devices such as smart cards, key fobs, electronic keys, or any combination of the above. Entry codes may also be embodied as any combination of the above items, such as a biosensor and/or a Bluetooth device.

In an embodiment that is especially useful when a high level of security is desired,
 25 access codes may be generated in a way that to be unique to the entry event, unique to the shipment, unique to the lock, unique to the lock, unique to the computer software, unique to the mobile application, unique to a person, and/or unique to the repositories and/or portable storage units. The setting of the access codes generated by the server may be manually generated, automatically generated, or based on a selection by the

lock user. Thus, the access code may be created in several ways.

The communication network is preferably a wireless network which may include but is not limited to a Code Division Multiple Access (CDMA) network, a General Packet
5 Radio Service (GPRS) network for use in conjunction with Global System for Mobile Communication (GSM) network, future third-generation (3G) network like Enhanced Data rates for GSM Evolution (EDGE) and Universal Mobile Telecommunications System (UMTS), fourth-generation (4G) network and/or fifth-generation (5G) network. It should be understood that although particular IP-based wireless networks have been
10 described, the system could be utilized in any suitable type of wireless network.

Preferably, the mobile devices **200** include smart phones, tablets, phablets, personal digital assistants (PDA), phoblets, iPad or any suitable means which is capable of communicating with the server **100** and the locking mechanism for unlocking the
15 repositories. The mobile device **200** is pre-installed with an application configured to perform authentication and instructs the unlocking of the locking mechanisms.

In a preferred embodiment, the server **100** may include a computing device **102** for regulating and processing the authentication process. The computing device **102** may
20 be any one of various devices including, for example, a desktop computer, a laptop computer, a personal digital assistant, a workstation, and the like. In some embodiments, the server **100** also further includes a storage subsystem **101** which stores the basic programming and data constructs that provide the functionality of the system. For example, the various modules and applications implementing the functionality of
25 the present invention may be stored in the storage subsystem **101** of the server **100**. Preferably, these software modules are generally executed by processor(s) within the computing device **102**.

Further, the storage subsystem **101** also provides a repository for storing the various

databases information according to the present invention. The storage subsystem **101** typically comprises memory component and file storage component. Preferably, the memory component includes but not limit to a number of memories including a main random access memory (RAM) for storage of instructions and data during program execution and a read only memory (ROM) in which fixed instructions are stored. Whereas, the file storage component provides persistent (non-volatile) storage for program and data files, and may include a hard disk drive, a floppy disk drive along with associated removable media, a Compact Digital Read Only Memory (CD-ROM) drive, an optical drive, removable media cartridges, and other like storage media.

10

In a preferred embodiment, the repositories may be of any size that is preferably remain stationary at a predefined location. Preferably, the repositories may be range from a room, a vault, shipping containers to a warehouse and/or a building or any enclosure that is spacious for allowing the storage of a quantity of items therewithin. Whereas, the storage unit may be of an enclosure of any size that is moveable, either under its own power or moved by any other means. Examples of portable storage unit may include but not limit to toolboxes, briefcases, luggage, backpacks, or any other objects that are able to be carried.

15

Fig. 2 illustrates an exemplary embodiment of the locking mechanism. Preferably, the locking mechanism is in the form of a robust lock **300** for securing at least an entrance of the repositories. Preferably, the repositories include at least a door panel **301** and a door frame **302**. The robust lock **300** comprises a linear actuator **303** for actuating a shaft **305** such that the shaft **305** is extended from a housing **304** to reach the door frame **302** of the repository. However, it should be understood that the shaft **305** may also be replaced by any other means such as knob, lever and the like, which is able to restrict the movement of the door panel **301** and locking the door panel **301** in position. Preferably, the shaft **305** is made of corrosive resistant material such as stainless steel or any other metal alloy, for ensuring the smooth locking and unlocking of the robust

20
25

lock **300**. Preferably, the robust lock **300** is disposed at an upper portion of the door panel **301** of the repository.

In a preferred embodiment, the robust lock **300** is operated by a microprocessor having
 5 a short range radio frequency module for communicating with the mobile devices **200** to receive an unlock instruction. Preferably, the robust lock **300** is a mechanical lock that will release or lock whenever power is supplied to the robust lock **300**. Preferably, a portable battery is provided as power supply when actuating the robust lock **300** and is taken out of the robust lock **300** when it is not actuated.

10

Preferably, when the robust lock **300** is in a locking position, a gap for opening **306** is provided between the shaft **305** and the door frame for allowing a smooth retraction of the shaft **305** into the housing **304**. Advantageously, the configuration of having the opening gap **306** prevents the bending of the shaft and thus prolong the life span of the
 15 robust lock **300**. Further, the robust lock **300** also able to withhold the strength of the door panel **301** from an inner side of the repositories.

Referring to **Fig. 3**, a portable lock **400** for securing the storage unit is illustrated. In a preferred embodiment, the portable lock **400** is in generally a pad lock, having a
 20 generally U-shaped shackle **401** hold within a body **402**. The portable lock **400** further embedded with a controller **403** for controlling the operation of the portable lock **400**. Preferably, the controller **403** includes a short range radio frequency module for allowing the communication of the controller **403** and the mobile devices **200**.

25 In a preferred embodiment, each repository and storage unit is secured with a robust lock **300** and portable lock **400** respectively. However, the locking of the repositories may also include multiple locks combination such as one robust lock **300** paired with two portable locks **400**, two robust locks **300** paired with one portable lock **400**, and the like. Further, each of the repository may also managed by a plurality of users during

the retrieval of storage unit within the said repository. In an example, a first and second user is authorized to unlock a first and second robust lock **300** of the repository, while a third user is authorized to unlock a portable lock **400** of the storage unit stored therewithin.

5

In an example of operation, a user first send a request for a storage unit retrieval to the server **100** via the computing device **102** for authentication of access credentials. Preferably, the access credentials includes user login ID, passwords, repository's ID, portable storage's ID or any of the combination thereof. Upon successful authentication,
10 at least one access code is generated from the server **100** and the access code is further transmitted to the designated mobile device **200** respectively. The user with the mobile device **200**, further establish a communication link to the locking mechanisms of said storage unit and/or repository to transmit at least one instruction for unlocking the linking mechanisms.

15

In another example of operation, a user first approaches a repository and establishes communication link to the locking mechanisms of said repository with the mobile device **200**. The mobile device then retrieve an ID of the said repository and its locking mechanisms, and further sends the retrieved ID together with user's access credentials
20 to the server **100** for authentication. Upon successful authentication, the server **100** generates at least one access codes and forwards the generated codes to the mobile device **200** via communication network. Moving on, upon receiving the generated codes, the mobile device **200** transmits at least one instruction for unlocking the linked locking mechanisms of the repository.

25

The above embodiments of the present disclosure are meant to be illustrative. They were chosen to explain the principles and application of the disclosure and are not intended to be exhaustive or to limit the disclosure. Many modifications and variations of the disclosed embodiments may be apparent to those of skill in the art. Persons

having ordinary skill in the field of computers and/or digital imaging should recognize that components and process steps described herein may be interchangeable with other components or steps, or combinations of components or steps, and still achieve the benefits and advantages of the present disclosure. Moreover, it should be apparent to
5 one skilled in the art, that the disclosure may be practiced without some or all of the specific details and steps disclosed herein.

While the present invention has been described with respect to what is presently considered to be the preferred embodiment, it is to be understood that the invention is
10 not limited to the disclosed embodiments. To the contrary, the invention is intended over various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

The present disclosure includes as contained in the appended claims, as well as that of
15 the foregoing description. Although this invention has been described in its preferred form with a degree of particularity, it is understood that the present disclosure of the preferred form has been made only by way of example and that numerous changes in the details of construction and the combination and arrangements of parts may be resorted to without departing from the scope of the invention.

CLAIMS

1. A computer-implemented system for managing a plurality of repositories, the system comprising:
 - 5 a server (100);
 - a plurality of mobile devices (200) in communication with the server (100) via a communication network; and
 - a plurality of storage unit stored within the repositories, wherein the storage unit and the repositories are individually secured by at least one locking mechanism;
 - 10 characterised in that the server (100) is configured to generate access codes of a designated storage unit and a designated repository of which the designated storage unit is stored therewithin upon receiving a request and to transmit each generated codes to a designated mobile device (200) respectively;
 - wherein each designated mobile device (200) is further configured to establish a
 - 15 communication link to the locking mechanisms of said storage unit and/or said repository via a short range radio frequency protocol, and to transmit at least one instruction for unlocking the linked locking mechanisms upon successful authentication.
- 20 2. A system as claimed in claim 1, wherein the access key further includes a time stamp for allowing the unlocking of the linked locking mechanisms within a predetermined time frame.
3. A system as claimed in claim 1 or claim 2, wherein the server (100) further includes
 - 25 a storage subsystems (101) for storing various databases information.
4. A system as claimed in any of the preceding claims, wherein the short range radio frequency protocol operates at frequencies range of substantially 2402 MHz and 2480 MHz.
- 30 5. A system as claimed in any of the preceding claims, wherein the locking mechanism

