

A COMPUTER-IMPLEMENTED METHOD FOR ACCESS CONTROL IDENTIFICATION AND ITS SYSTEM THEREOF

FIELD OF INVENTION

5

The invention relates to a method for access control identification system. More particularly, the invention relates to a method for providing access control identification system to user accurately and its system thereof.

10 BACKGROUND OF THE INVENTION

A conventional access control identification system provides a guard house at an entrance to manually grant access to a person to enter a designated location through the entrance. Generally, a security personnel is stationed at the guard house for
15 checking if the person is allowed entry into the designated location by having relevant documents such as a ticket or entry pass. As time goes on, the conventional access control identification system is gradually replaced by new technologies which eliminate the needs of having a security personnel and a guard house. Places such as theme parks and cinemas have started to implement QR code identification system
20 that typically use static QR code to gain access to those places. The static QR codes may be printed on the entry pass or tickets, or displayed over a mobile phone, which are to be scanned by a code reader at the entrance. Upon validation of the static QR codes, the code reader signals an actuator of a door such that the door is opened for the person to pass through. Such system also depends on cloud services to function,
25 such as information retrieval for generation of the static QR code. The existing access control identification systems also rely on cloud services in order for the identification system to work, especially for storage and processing of information.

However, there are several drawbacks arise from the above-mentioned system. Such

system does not provide security protection against cloning of the static QR code. A third party may easily snap a picture of the static QR code or possess a screenshot of the static QR code, and is granted access by scanning the static QR code at the code reader. Furthermore, some access control systems do not subscribe to cloud services as the subscription fees are expensive. The cloud services are also prone to cybersecurity attacks such as risks of hacking, as the cloud services contain sensitive user credentials. The cloud services also burden the access control systems as the cloud services and the access control system have to exchange information regularly to achieve real-time access authentication.

10

There are a few patented technologies over the prior art relating to the access control method. US20120280783A1 discloses a system and method for operating a remotely operable lock. In an example embodiment, a method comprises providing a first web service for receiving credentials or a command from a portable electronic device having a software application installed thereon, issuing a command for receipt by the lock from the web service, and providing an application programming interface at the first web service for integrating a second web service or the software application with the first web service to allow the portable electronic device to communicate with the lock or web service.

20

Another method and apparatus for access control is disclosed in US9378470B2. The present invention is directed towards systems and methods for improved access to an attraction via a computing device of a user. A first computing device of a user records an identification code associated with an attraction. The first computing device transmits, to a second computing device, a request for access to the attraction, the request comprising the identification code. The first computing device receives, from the second computing device, an access authorization comprising an access code. The first computing device presents the access code to an attraction operator for access to the attraction.

25

Accordingly, it would be desirable to provide an access control identification system that provides better security and does not rely on Internet connectivity. This invention provides such a system and method thereof.

5

SUMMARY OF INVENTION

One object of the present invention is to provide an access control identification system that provides better security by reducing risk of hacking. Another object of the invention is to incorporate various recognition methods to prevent an unauthorized user from bypassing an access point. The present invention also seeks to provide an access control identification system that does not rely on cloud services during information processing to grant access to the user.

15 The present invention provides a computer-implemented method for access control identification, the method comprising the steps of selecting, by a selection module of the mobile device, an identifier prestored in the memory device; retrieving, by a scanning module of the mobile device, a biometric data from a user; determining, by a matching module of the mobile device, a match between the retrieved biometric data and a biometric data of an authorized user that is prestored in a memory device of the mobile device; securing, by an integrity module of the mobile device, the integrity of the selected identifier; encrypting, by an encryption module of the mobile device, the secured identifier using an encryption key and the mobile device's time stamp information; converting, by a conversion module of the mobile device, the encrypted identifier into a displayable access code carrying a time stamp to indicate its expiry time; generating, by the conversion module of the mobile device, a new access code by re-encrypting the selected identifier using the existing encryption key and an updated time stamp to replace the expired access code; displaying, by a display of the mobile device, the updated access code to an access point; and scanning, by the access

point, the updated access code to provide access to the user upon validation of the updated access code; wherein the access point is in communication with a computing device which connects to a same server with the mobile device, such that the access point synchronises its clock with the mobile device through communication with the
5 computing device at a predetermined time.

Preferably, the access point communicates with a code reader that decrypts the access code using the same encryption key from software application and the code reader's time stamp to obtain the selected identifier for comparison with the reference
10 identifier stored in the code reader respectively. The decryption process fails if the time stamp of the mobile device and the code reader do not fall within the allowable access code expiry threshold, and the code reader will deny access to the user.

Preferably, the biometric data comprises fingerprints, hand characteristics, eye
15 characteristics, facial characteristics, voice characteristics or in any combination thereof.

Preferably, the identifier comprises user credentials and a unique identifier retrieved from the mobile device.
20

Preferably, the encryption method comprises of a shared session key, which comprises an encryption key generated by the software application in the computing device and a time stamp data from the mobile device.

25 Preferably, the method further comprises the steps of scanning, by the scanning module of the mobile device, the biometric data of the user for registration of the authorised user; and storing the registered biometric data of an authorised user in the memory device.

Preferably, the server is connected to Network Time Protocol (NTP) for clock synchronization.

Preferably, the method further comprises the step of converting, by the conversion
5 module, the encrypted identifier from raw string data into two-dimensional barcode.

Preferably, the decryption method also comprises of a shared session key, which comprises an encryption key generated by the software application in the computing device and a time stamp data from the code reader.

10 Preferably, the method further comprises the steps of transmitting, by the code reader, the decrypted access code to a controller; determining, by the controller, validity of the access code and transmitting a signal to an actuator upon validation of the access code; and determining, by the controller, an operative mode of the actuator in response to the transmitted signal.

15 Preferably, the method further comprises the step of transmitting entry records from the controller to the computing device.

According to a further feature of the invention, an access control identification system
20 comprising a mobile device comprising a selection module for selecting an identifier prestored in a memory device, a scanning module for retrieving a biometric data from a user; a matching module for determining a match between the retrieved biometric data and a biometric data of an authorized user that is prestored in a memory device of the mobile device; an integrity module for securing the integrity of selected identifier;
25 an encryption module for encrypting the secured identifier using an encryption key and the mobile device's time stamp information; a conversion module for converting the encrypted identifier into a displayable access code carrying a time stamp to indicate its expiry time and generating a new access code by re-encrypting the selected identifier using the existing encryption key and an updated time stamp to

generate a new access code to replace the expired access code; and a display for displaying the updated access code; an access point for scanning the updated access code to provide access to the user upon validation of the updated access code; a computing device in communication with the access point; and a server for
5 connecting to the computing device and to the mobile device such that the access point synchronises its clock with the mobile device through communication with the computing device at a predetermined time.

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.

BRIEF DESCRIPTION OF THE DRAWINGS

15 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 construction and operation and many of its advantages would be readily understood
20 and appreciated.

Fig. 1 is a diagram illustrating an exemplary embodiment of an access control identification system.

25 **Fig. 2** is a flow chart for enrolment of the user's mobile device to the software application in the computing device.

Fig. 3 is a flow chart for enrolment of an authorized user to the software application in the computing device.

Fig. 4 is a flow chart for enrolment of the user's mobile device to the software application in the computing device via the use of internet connectivity and email services.

5

Fig. 5 is a flow chart for access control identification according to the present invention.

Fig. 6 is a flow chart of a detailed embodiment for access code generation.

10

Fig. 7 is a flow chart of a detailed embodiment for access code scanning;

Fig. 8 is a flow chart for enrolment of an authorized user by utilising the mobile device upon expiration of the identifier.

15

Fig. 9 is a flow chart for enrolment of an authorized user by utilising the email upon expiration of the identifier.

Fig. 10 is a flow chart for denying access of an unauthorized user.

20

DETAILED DESCRIPTION OF THE INVENTION

The present invention relates to a method and system for providing access control identification with dynamic quick response code. In a general configuration, the method comprises a mobile device, a computing device, a code reader, an access point and a server. Prior to discussing various embodiments of the invention, descriptions of some of the terms used herein are provided below for a better understanding of the invention.

25

As used herein, a “mobile device” is a portable device capable of sending and receiving electronic communication through a mobile network. The electronic device can be configured to receive information from a server and display the information on a display on the electronic device. For example, but not limited to, the mobile device
5 can be a mobile phone, tablet or any suitable means which capable of receiving and displaying the received information. In addition, the electronic device may be capable of communicating with the communication network to be connected to the server. Preferably, the mobile device is capable of generating an access code such as barcodes and quick response codes.

10

As used herein, a “computing device” is an electronic device which is accessible over a communication network such as local area network, metropolitan area network, wide area network, wireless network and inter network. The computing device includes desktop computers and laptops.

15

As used herein, an “access point” is an entrance for a specific location the user intends to pass through, such as at a door of a building or a turnstile of a theme park.

As used herein, a “code reader” is a device that captures visual information and
20 translates the captured image into digital information which a computer is capable of understanding and displaying. For example, the code reader can be a barcode scanner which is capable of scanning and decrypting information contained in a quick response code.

25 As used herein, an “access code” is code that is encrypted with various information which is only decryptable with a code reader. The access code can be in the form of one-dimensional barcode, two-dimensional barcode or any suitable means for data encryption. For example, the two-dimensional barcode such as quick response code may contain encrypted information such as user credentials that only can be decrypted

when the two-dimensional barcode is scanned by the code reader within a predetermined area and within a predetermined time interval.

As used herein, a “server” is a networking protocol for clock synchronization between computing devices and mobile devices over packet-switched, variable-latency data networks. The server is intended to synchronize all participating computing devices and mobile devices to within a few milliseconds of Coordinated Universal Time.

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

Fig. 1 shows an exemplary embodiment of the present invention. The access control identification system comprises a mobile device **101** for registration of biometric data and executing a mobile application for access control identification, an access point **107** for having a code reader **111** to scan and decrypt an encrypted code, a computing device **108** for activating the software application and registration of an authorised user, and a server **109** for synchronizing the timing of the mobile device **101** and computing device **108**.

In one preferred embodiment, the code reader **111** is located at an access point **107** of a specific location, such as at a door of a building or a turnstile of a theme park. Preferably, the code reader is in communication with a controller **112** that links to an actuator **113** of the door or turnstile. The code reader **111** is configured to read an access code and decrypts the access code for retrieval of encrypted information within the access code. The code reader then transmits the decrypted access code to the controller for identification. Upon identification of an authorized user from the access code, the controller **112** signals the actuator **113** to provide access to the authorized user, such as by unlocking a latch of the door or actuating the turnstile.

In this particular embodiment, the mobile device **101** is installed with a mobile application which provides at least one scanning module **102**, matching module **103**, selection module **104**, memory device **110**, encryption module **116**, integrity module **117** and conversion module **105** for access control identification measures. The
5 memory device **110** of the mobile device **101** is used to store information such as identifier and biometric data during registration of an authorized user to the software application. The identifier may be user credentials such as username, site access name, email, contact number and password associated with the site access name, encryption key from the software application, and a unique identifier of the mobile
10 device **101** such as hashed IMEI number. In one particular embodiment, one user may register one identifier for accessing multiple access points **107** or more than one identifier for accessing different access points **107**. The encryption module **116** may construct time information such as a time interval for refreshing the access code regularly, and a time stamp data.

15 The scanning module **102** is configured to retrieve a biometric data from a user. By ways of example but not by limitation, the biometric data comprises fingerprints, hand characteristics, eye characteristics, facial characteristics, voice characteristics or in any combination thereof. Preferably, the scanning module **102** is co-operating with an
20 existing feature of the mobile device **101**, such as an audio recorder, a camera or a recognition sensor of fingerprint of the mobile device **101**. In one example, the user may scan his thumb with the recognition sensor for capturing its fingerprint data, and the scanning module **102** retrieves the fingerprint data from the recognition sensor. In another example, the user may capture an image of his face and the scanning module
25 **102** retrieves the facial image for recognising unique feature of the facial image.

Further, the matching module **103** is configured to determine a match between the retrieved biometric data and a biometric data of an authorized user that is stored in a memory device **110** of the mobile device **101**. In one particular embodiment, the

matching module **103** may run an algorithm which determines similarity between the retrieved biometric data with the biometric data of the authorized user. By way of example, a similarity value may be computed and compared to a predetermined similarity threshold.

5

The selection module **104** is configured to select an identifier among a plurality of identifiers prestored in the memory device **110**. By way of example but not by limitation, the selection module **104** selects the identifier based on a GPS location data. In another example, the selection module **104** allows the user to manually select
10 an identifier among a plurality of identifiers. Such application is applicable in an event where GPS signals are not available. Upon selection of the identifier, the user may have to confirm the selected identifier via biometric authentication. The conversion module **105** converts the selected identifier into a format suitable to be converted into the access code. By way of example, the selected identifier is
15 converted into a raw string data which is in compliance with EMVCo standards.

The conversion module **105** is configured to convert the selected identifier in the format of raw string data into the access code. The access code is generated regularly by re-encrypting the selected identifier using the existing encryption key and the
20 mobile device's updated time stamp based on the time interval and expiry time provided by the time information recorded in the memory device without altering the user credentials. In one preferred embodiment, the conversion module **105** generates a new access code by re-encrypting the selected identifier using the existing encryption key and the mobile device's updated time stamp to replace the expired access code to
25 be displayed over a display **106** such that a dynamic access code is generated.

In one preferred embodiment, the computing device **108** is installed with a software application that assists during registration of an authorized user. The computing device **108** is provided with at least a generation module **114** for generating an

activation code for activating the mobile application in the mobile device **101** and a database **115** for storing log records of the user at the access point.

In one particular embodiment, the code reader **111** is in communication with the computing device **108** via the controller **112**. The code reader **111** comprises a memory device **110** for storing the encryption key obtained from the software application in the computing device. The code reader **111** decrypts the access code using the encryption key and the code reader's time stamp, and transmits the decrypted information to the controller **112** so that the controller **112** can instruct an operation for an actuator **113** of a door once the user credentials are validated. Preferably, the code reader **111** is located at an access point **107** of a specific location such as at an entrance of a building or theme park. Preferably, the code reader **111** is in communication with the controller **112** which communicates with the computing device **108**, and the computing device **108** connects to the same server **109** with the mobile device **101**, such that the code reader **111** synchronises its clock with the mobile device **101** through communication with the computing device **108** via the controller **112** at a predetermined time. By way of example, the mobile device **101** and the computing device **108** connect to the server **109** during enrolment of an authorized user. In another example, the mobile device **101** and computing device **108** are configured to connect to the server **109** at a regular time interval, such as weekly, monthly, quarterly or yearly basis. The time synchronization between the mobile device **101** and the code reader **111** enables the code reader **111** to accurately determine if the access code scanned is within the allowable access code expiry threshold, forming the basis of the dynamic access code identification system.

25

Fig. 2 illustrates a flow chart for enrolment of the user's mobile device to the software application in the computing device. At step **201**, the user executes the installed mobile application on the mobile device and pre-registers suitable information such as user credentials and biometric data into the memory device. At step **202**, the

conversion module of the mobile device converts the pre-registered information into a registration code. In this particular embodiment, the registration code is in the form of two-dimensional barcode containing the unique identifier of the mobile device such as IMEI as part of the cross-verification. Preferably, the computing device is connected

5 with a code reader for enrolment purpose. For the sake of clarity, the code reader as used herein is denoted as enrolment code reader. At step **203**, the enrolment code reader scans the registration code to receive the encrypted data embedded within the registration code. At step **204**, the generation module of the computing device generates an activation code embedded with the encryption key for scanning of the

10 mobile device. Preferably, the activation code is in the form of a two-dimensional barcode. The mobile device and computing device of this embodiment are connected to a same server such that the mobile device and computing device synchronize their respective time clock with the server. At step **205**, the generation module compiles the encrypted data from the registration code to generate a reference identifier containing

15 the hashed IMEI of the mobile device which is to be sent to the controller of the code reader. At step **206**, the mobile device scans the activation code as cross-verification. Preferably, the activation code is in the form of alphabetical, numerical or alphanumeric characters. In this particular embodiment, the software application in the computing device transfers the encryption key information to the mobile

20 application in the mobile device. As an alternative for step **206**, at step **207**, the user may manually input the activation code generated by the software application in the computing device into a template prompted on a display of the mobile device.

Fig. 3 illustrates a flow chart for enrolment of an authorized user to the software application in the computing device. At step **301**, the user executes the installed software application on the computing device and registers suitable information such as user credentials and biometric data into the software application in the computing device. At step **302**, the generation module of the computing device generates an activation code based on the registered information. In this particular embodiment, the

25

activation code is in the form of two-dimensional barcode containing the user credentials. The mobile device and computing device of this embodiment are connected to a same server such that the mobile device and computing synchronize their respective time clock with the server. At step **303**, the generation module
 5 compiles the user credentials to generate a reference identifier containing the user's credentials, which the reference identifier is transmitted to the controller of the code reader. At step **304**, the mobile device scans the activation code to obtain the user credentials. Alternatively at step **305**, the user may manually input the activation code into a template prompted on a display of the mobile device to generate the access
 10 code. In this alternate embodiment, the activation code is in the form of alphabetical, numerical or alphanumeric characters. An identifier having the user's credential is generated and stored within the memory device in the mobile device. Advantageously, such steps allow the user to register at the computing device and then transfer the necessary user credentials to the mobile device without the need to subscribe to any
 15 cloud services.

Fig. 4 illustrates a flow chart for enrolment of the user's mobile device to the software application in the computing device via the use of internet connectivity and email services. The enrolment method in **Fig. 4** is an alternate embodiment of the enrolment
 20 method described in **Fig. 2**. At step **401**, the user executes the installed mobile application on the mobile device and pre-registers suitable information such as user credentials and biometric data into the software application. At step **402**, the conversion module of the mobile device converts the pre-registered information into a registration code. In this particular embodiment, the registration code is in the form of
 25 two-dimensional barcode containing the unique identifier of the mobile device such as IMEI as part of the cross-verification. In one preferred embodiment, the pre-registered information comprises user credentials such as username, site access name, email, contact number and password associated with the site access name, and a unique identifier of the mobile device such as hashed IMEI number. Preferably, the

computing device is connected with a code reader for enrolment purpose. For the sake of clarity, the code reader herein is denoted as enrolment code reader. At step **403**, the enrolment code reader scans the registration code to receive the encrypted data embedded within the registration code. At step **404**, the generation module of the

5 computing device generates an activation code embedded with an encryption key for scanning of the mobile device. Preferably, the activation code is in the form of a two-dimensional barcode. The mobile device and computing device of this embodiment are connected to a same server such that the mobile device and computing synchronize their respective time clock with the server. At step **405**, the generation

10 module compiles the encrypted data from the registration code to generate a reference identifier containing the hashed IMEI which is to be sent to the controller of the code reader. At step **406** the mobile device scans the activation code to receive the activation code as cross-verification. In this embodiment, user need not go through steps **407** and **408**. This application is useful when cloud subscriptions are not

15 available. In an alternate embodiment for step **406**, at step **407**, the computing device may deliver the activation code to the mobile device. In one particular embodiment, the activation code can be delivered via an email or the like. The activation code delivered by the computing device preferably is in the form of alphabetical, numerical or alphanumeric characters. Such application requires the computing device to have

20 access to internet. At step **408**, the user inputs the received activation code into a template prompted on a display of the mobile device as part of the cross-verification exercise. In this particular embodiment, the software application in the computing device transfers the encryption key information to the mobile application in the mobile device.

25

Fig. 5 illustrates a flow chart for access control identification according to the present invention. At step **501**, the selection module selects the identifier based on a GPS location data. In another example, the selection module allows the user to manually select an identifier among a plurality of identifiers. Such application is applicable in

an event where GPS signals are not available. At step **502**, the scanning module of the mobile device retrieves a biometric data from the user. At step **503**, the matching module determines a match between the retrieved biometric data and a biometric data of an authorized user that is prestored in a memory device of the mobile device. At

5 step **504**, the securing module secures the selected identifier using the integrity module. At step **505**, an encryption module of the mobile device encrypts the secured identifier using an encryption key and mobile device's time stamp information. In this particular embodiment, the encryption module retrieves the encryption keys from the activation code that is generated by the generation module of the computing device.

10 At step **506** and **507**, the conversion module converts the selected identifier into a displayable access code carrying a time stamp to indicate its expiry time. Upon its expiry, the conversion module generates a new access code by re-encrypting the selected identifier using the existing encryption key and an updated time stamp to replace the expired access code. At step **508** and **509**, the updated access code is

15 displayed by a display of the mobile device to an access point so that the access point provides access to the user upon validation of the user credential in the access code. In one preferred embodiment, the access point provides a code reader to scan and decrypt the access code using the same encryption key and the code reader's time stamp to obtain its selected identifier for validation by the controller. Upon decryption

20 of the access code, the decrypted identifier is sent to the controller. At step **510**, the controller sends an entry record to the computing device if the decryption is successful and the decrypted identifier matches with the reference identifier. At step **511** and **512**, the controller signals the code reader to display an "open door" notification to the user. The controller then transmits a signal to an actuator and

25 determines an operative mode of the actuator in response to the transmitted signal. If the user is granted access, the actuator is actuated to provide access at the access point.

In one preferred embodiment, the code reader of the access point is in communication

with the computing device via the controller, where the computing device connects to the same server with the mobile device, such that the access point synchronises its clock with the mobile device through communication with the computing device at a predetermined time. Such arrangement allows the code reader to synchronize its time
 5 with mobile device through the computing device whenever the mobile device and the computing device connect to the server. Advantageously, the mobile device and the computing device do not need to be connected to the server at the same time. The mobile device and the computer device can connect to the server at different times, but the synchronized time will still be the same as long as the locale of the devices
 10 remains the same. As the computing device is in communication with the code reader, this ensures the code reader to synchronize its time with the mobile device. Advantageously, with precise and synchronised timing between the code reader and the mobile device, the code reader is able to compare the time stamp from the access code and the synchronized clock of the code reader and successfully decrypt the
 15 access code to grant access to the user if the time stamp falls within the allowable access code expiry threshold. Such embodiment is suitable for location without stable internet connectivity. The server is also connected to Network Time Protocol (NTP) for clock synchronization such that the server synchronizes its time with the world clock.

20

Fig. 6 and **Fig. 7** each illustrates a detailed embodiment for access code generation and access code scanning respectively.

Referring to **Fig. 6**, the mobile application of the mobile device is launched to recall
 25 the selected identifier and prompt biometric authentication at step **601**. At step **602**, an integrity module of the mobile device runs the integrity checking function on the identifier and embed the integrity checksum in the identifier. At step **603**, an encryption module of the mobile device encrypts the identifier using an encryption key and mobile device's time stamp information. In this particular embodiment, the

encryption module retrieves the encryption keys from the activation code that is generated by the generation module of the computing device. At step **604**, the conversion module of the mobile device converts the encrypted identifier into a format suitable to be converted to two-dimensional barcode. By way of example, the encrypted identifier is converted to raw string data. At step **605**, the conversion module of the mobile device converts the raw string data into an access code in the form of a two-dimensional barcode. By way of example, the two-dimensional barcode is a quick response code. At step **606**, the conversion module re-encrypts the selected identifier using the existing encryption key and an updated time stamp to generate a new access code to replace the expired access code. By way of example, the conversion module generates a new access code every 3 seconds with reference to the time stamp.

Referring to **Fig. 7**, the user presents the access code to the code reader at step **701**. At step **702**, the code reader reads the access code and the code reader decrypts the access code using the encryption key and the code reader's time stamp for retrieval of encrypted information, such as the user credentials, within the access code. The access code is denied access if the access code is found to have expired. At step **703**, an integrity module of the controller runs the integrity checking function on the decrypted identifier to determine if the access code has been tampered with. In this particular embodiment, if the checksum obtained by the controller does not match the checksum embedded by the mobile device, the integrity of the access code has been tampered with. At step **704**, the controller determines the validity of the decrypted identifier and if the user credentials contain access rights through comparison with the user credentials stored in the controller. If the access code is valid and possesses the right user credentials, the user is granted access and can go beyond the access point. If the access code is invalid, the user is not granted access and the door is not actuated to open for the user to go beyond the access point.

In one particular embodiment, the identifier on the mobile device is configured to expire after a predetermined time. For example, the information contained in the identifier is no longer valid for the authorized user to use for getting access through an access point upon its expiry. Such configuration is to ensure the authorized user to
 5 update the information in the identifier in order for the software application in the computing device to receive latest data on the active user count. By way of example, the identifier expires one month after enrolment of the authorized user.

Fig. 8 illustrates a flow chart for enrolment of an authorized user by utilising the
 10 mobile device upon expiration of the identifier. At step **801**, the mobile application of the mobile device generates a notification and displays the notification at the display. By way of example, the notification contains a reminder message of the expiry and renewal option. At step **802**, the user requests for new activation code through the mobile application of the mobile device. At step **803** and **804**, the conversion module
 15 generates a request code for scanning at the code reader connected to the computing device. In this particular embodiment, the request code is in the form of two-dimensional barcode. At step **805**, the generation module of the computing device generates an activation code embedded with the previously registered information by the user and the identifier's new expiration date. Preferably, the activation code is in
 20 the form of a two-dimensional barcode. At step **806**, the generation module compiles the previously registered information to generate a reference identifier which is to be sent to the controller along with the new identifier expiration date. At step **807** the mobile device scans the activation code to receive the activation code. This application is useful when internet connectivity is not available. As an alternate
 25 embodiment for step **807**, as illustrated in step **808**, the user can manually enter the activation code into the mobile application in the mobile device.. An identifier having the updated user's credential is generated and stored within the memory device of the mobile device.

Fig. 9 illustrates a flow chart for enrolment of an authorized user by utilising the email upon expiration of the identifier. The enrolment method in **Fig. 9** is an alternate embodiment of the enrolment method described in **Fig. 8**. At step **901**, the mobile application of the mobile device generates a notification and displays the notification at the display. By way of example, the notification contains a reminder message of the expiry and renewal option. At step **902**, the user requests for new activation code through the mobile application of the mobile device. At step **903** and **904**, the conversion module generates a request code for scanning at the code reader connected to the controller. In this particular embodiment, the request code is in the form of two-dimensional barcode. At step **905**, the code reader sends the information embedded in the request code to the controller. At step **906**, the controller transmits a request for activation to the software application of the computing device. At step **907**, the computing device delivers the activation code to the mobile device using internet connectivity. In one particular embodiment, the activation code can be delivered via an email or the like. Preferably, the activation code is in the form of alphabetical, numerical or alphanumeric characters. At step **908**, the user inputs the activation code into a template prompted on a display of the mobile device for permitting the mobile application to generate the new access code.

Fig. 10 illustrates a flow chart for denying access for an unauthorized user. At step **1001**, the selection module selects the identifier based on a GPS location data. In another example, the selection module allows the user to manually select an identifier among a plurality of identifiers. Such application is applicable in an event where GPS signals are not available. At step **1002**, the scanning module of the mobile device retrieves a biometric data from the user. The matching module determines a match between the retrieved biometric data and a biometric data of an authorized user that is prestored in a memory device of the mobile device. Upon matching of the biometric data obtained at step **1002**, the mobile application in the mobile device generates the access code encrypted with the updated time stamp following the process as outlined

- in Fig. 6. At step **1003**, the access code carrying the updated time stamp is displayed by a display of the mobile device to an access point so that the access point provides access to the user upon validation of the user's credentials in the access code. At step **1004**, the controller receives the decrypted identifier from the access code. At step **1005**, the controller generates an error message to the code reader and the unauthorized user is denied access through the access point. The invalid entry record is also delivered to the computing device at step **1006** if the decryption using the time stamp failed or the selected identifier does not match with the reference identifier.
- 10 The present disclosure includes as contained in the appended claims, as well as that of 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
- 15 resorted to without departing from the scope of the invention.

CLAIMS

1. A computer-implemented method for access control identification, the method comprising the steps of:
 - 5 selecting, by a selection module of a mobile device, an identifier prestored in a memory device of the mobile device (501);
 - retrieving, by a scanning module of the mobile device, a biometric data from a user (502);
 - determining, by a matching module of the mobile device, a match between the
 - 10 retrieved biometric data and a biometric data of an authorized user that is prestored in a memory device of the mobile device (503);
 - encrypting, by an encryption module of the mobile device, a selected identifier using an encryption key and mobile device's time stamp information (505);
 - converting, by a conversion module of the mobile device, the selected
 - 15 identifier into a displayable access code carrying a time stamp to indicate its expiry time (506);
 - generating, by the conversion module of the mobile device, a new access code encrypted using an updated time stamp comprising the selected identifier to replace an expired access code (507);
 - 20 displaying, by a display of the mobile device, an updated access code to an access point (508); and
 - scanning, by the access point, the updated access code to provide access to the user upon validation of the updated access code (509);
 - wherein the access point is in communication with a computing device which
 - 25 connects to a same server with the mobile device, such that the access point synchronises its clock with the mobile device through communication with the computing device at a predetermined time;
 - wherein the access point communicates with a code reader, in which the code reader decrypts the access code using an encryption key obtained from the computing

device and a time stamp of the code reader, to obtain the selected identifier, for the selected identifier to be compared with a reference identifier stored in a controller that is in communication with the code reader; and

wherein the access point shall deny access to the user when the code reader
 5 fails to decrypt the access code using the time stamp of the code reader, when the selected identifier fails to match with the reference identifier, or when the code reader determines that the time stamps of the mobile device and the code reader fail to fall within an expiry threshold.

10 2. The method according to claim 1, wherein the biometric data comprises fingerprints, hand characteristics, eye characteristics, facial characteristics, voice characteristics or in any combination thereof.

3. The method according to claim 1, wherein the identifier comprises user
 15 credentials and a unique identifier retrieved from the mobile device.

4. The method according to claim 1 further comprising the steps of:
 scanning, by the scanning module of the mobile device, the biometric data of the user for registration of the authorised user (201); and
 20 storing the registered biometric data of the authorised user in the memory device.

5. The method according to claim 1, wherein the server is connected to Network Time Protocol (NTP) for clock synchronization.

25

6. The method according to claim 1 further comprising the step of converting, by the conversion module, the encrypted identifier from raw string data into two-dimensional barcode (603) that corresponds to the access code.

7. The method according to claim 1 further comprising the step of transmitting entry records from the controller to the computing device (507).
8. The method according to claim 1 further comprising the steps of:
 - 5 transmitting, by the code reader, the decrypted access code to a controller;
 - determining, by the controller, validity of the access code and transmit a signal to an actuator upon validation of the access code (509); and
 - determining, by the controller, an operative mode of the actuator in response to the transmitted signal (510).
- 10 9. An access control identification system comprising:
 - a mobile device (101) comprising:
 - a scanning module (102) for retrieving a biometric data from a user;
 - a matching module (103) for determining a match between the retrieved
 - 15 biometric data and a biometric data of an authorized user that is prestored in a memory device (110) of the mobile device (101);
 - a selection module (104) for selecting an identifier associated with the matched biometric data from a plurality of identifiers prestored in the memory device (101);
 - 20 an integrity module (117) for securing integrity of the selected identifier;
 - an encryption module (116) for encrypting the selected identifier using an encryption key and time stamp information;
 - a conversion module (105) for converting the selected identifier into a displayable access code carrying a time stamp to indicate its expiry time and
 - 25 generating a new access code carrying an updated time stamp using the selected identifier to replace an expired access code;
 - a display (106) for displaying an updated access code;
 - an access point (107) for scanning the updated access code to provide access to the user upon validation of the updated access code;

a computing device (108) in communication with the access point (107); and
a server (109) for connecting to the computing device (108) and to the mobile
device (101) such that the access point (107) synchronises its clock with the mobile
device (101) through communication with the computing device (108) at a
5 predetermined time;

wherein the access point (107) communicates with a code reader (111), in
which the code reader (111) decrypts the access code using an encryption key
obtained from the computing device (108) and a time stamp of the code reader (111),
to obtain the selected identifier, for the selected identifier to be compared with a
10 reference identifier stored in a controller (112) that is in communication with the code
reader (111); and

wherein the access point (107) shall deny access to the user when the code
reader (111) fails to decrypt the access code using the time stamp of the code reader
(111), when the selected identifier fails to match with the reference identifier, or when
15 the code reader (111) determines that the time stamps of the mobile device (101) and
the code reader (111) fail to fall within an expiry threshold.