IJARIIT

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume3, Issue5)

Available online at www.ijariit.com

A Method and a System for Secure Access to a Network Resource

Uma Shankar Gupta
GNIMT, Ludhiana
usgupta955@gmail.com

Ram Chander Rohilla
PCTE, Punjab
ramchander.pcte@gmail.com

Abstract. Bank, casino and ATM Safe is not just a vault. Every individual have believe that their money is completely secure in ATMs and strong rooms. All the banks and casinos protect their safe with their man power and latest technologies. However some masterminds have ability to deceive these systems for stealing money, important data and reputation of that organization get ruin too. The entire organization those related to money wants completely secure their money and data hence no one can Robb their safe. The present invention relates to security of resources such as monetary funds, data stores and document stores etc. and more specifically, to a method and system for secure access to a network resource.

***Keywords:** New Era of Securing Bank, Casino, Homes, Defense, Security Agencies, ATM Machine, ATM Card Transaction.*

1. INTRODUCTION

Humans are becoming very dependent on the machines and it is correct to do so as the machines are much more reliable from the security point of concern. The advancement of technology has led to increment the use of reliable safety devices. For example, ATMs, banks or any high security zone are somehow or other are managed and controlled by the use of electronically controlled high level security apparatuses. But as technology is evolving, traditional security systems are lagging to provide the required security. So advancement of technology is required so that confidential data or monetary funds can be kept into safer zones. There has been number of varied type of security systems and method developed and some of them have been discussed below:

CN205428063U discloses an ATM security machine that is provided with a controller, fingerprint identification device, face recognition devices, control password keyboard region of opening and closing gates means.

WO2016160816A1 talks about a smart card such that connects, wirelessly or by contact, to a reader or other device, and permits the flow of information/data to/from the card when connected thereto, after fingerprint scanning authorization/user verification system, or image scanning authorization/user verification, or PIN number entry from an on-card pad, or both, including a display screen for displaying changing/static user identification data stored thereon/therein after such authorization/verification.

WO2016013999A1 discloses a secure sales and payment terminal where payment is carried out using methods such as biometric definition and fingerprint definition. Definition of the biometric face data and/or fingerprints of the user, carrying out secure payment via a bank, printing the payment details on a slip, submitting an electronic slip to the e-mail address of the customer, forming accounting records and storing all procedures carried out on the terminal is performed by means of the invention.
The above mentioned documents talks about system and method of securing information, transactions and means related thereto. However, the solutions discussed above disclose little about the protection of the network resource when a wrong password or a biometric is provided by any miscreant or about ways of nabbing the miscreant, once the miscreant has been identified. Accordingly, there remains a need in the prior art to have a method and a system for secure access to a network resource, which does not suffer from above mentioned deficiencies.

2. SUMMARY

The methods and systems provides solution including setting a duplicate password by an authorized person which will be predefined, and that skips the machine from original interface and provides it with a duplicate network resource that seems original to a miscreant.

According to a first aspect of the present invention, there is provided a method for secure access to a network resource the method comprising steps of receiving an identification number, one or more biometrics and a password at a front end machine, transmitting the identification number, the one or more biometrics and the password from the front end machine to an authentication server, comparing the received identification number, the one or more biometrics and the password with stored predefined user credentials at the authentication server for verification of the received identification number, the one or more biometrics and the password, also transmitting a verification confirmation from the authentication server to the front end machine on verification of the received identification number, the one or more biometrics and the password.

In accordance with an embodiment of the present invention, the network resource is selected from a group consisting of a monetary fund, a document store and a data store.

In accordance with an embodiment of the present invention, the identification number is selected from a group consisting of an account number, a customer relationship number and a personal identification number.

In accordance with an embodiment of the present invention, the identification number has been provided in form of a membership card. Further, the membership card further comprises a biometric recognition device configured to read the one or more biometrics. Further, the biometrics recognition device has been provided at one or more location of the membership card.

In accordance with an embodiment of the present invention, the one or more biometrics is one or more of a finger print scan and a facial scan or eyes.

In accordance with an embodiment of the present invention, the password is anyone of an original password and a duplicate password. Further, the method for secure access to a network resource further comprises of transmitting a verification failure message from the authentication server to the front end machine on receiving the duplicate password at the authentication server. Also, execution of one or more security protocols at the front end machine on receipt of the verification failure message at the front end machine.

The front end machine is one of electronic safe, further comprises steps of reading and authentication of one or more finger prints, if authentication fails a safety alarm rings otherwise moved to next step, reading and authentication of a password, if authentication fails access to a duplicate material is provided otherwise, moved to next step and face recognition and authentication, if authentication fails access to the duplicate material is provided otherwise access to original network resource is provided.

The front end machine is one of electronic safe further comprising steps of reading and authentication of one or more finger prints, if authentication fails a safety alarm is rings otherwise, moved to next step, face recognition and authentication is done, if authentication fails a safety alarm rings otherwise moved to next step and reading and authentication of a password, If authentication fails access to duplicate network resource is provided otherwise access to original network resource is provided.

In accordance with an embodiment of the present invention, the front end machine further comprises a rotatable mechanism for providing a hiding the original material and/or providing access to a duplicate network resource.

In accordance with an embodiment of the present invention, a rotatable mechanism further comprises a cylindrical vault having an inner rotatable cylindrical chamber inscribed inside the cylindrical vault, the inner rotatable chamber further having an original phase and a duplicate phase bisecting the rotatable cylindrical chamber into two equal halves and a motor means to rotate the inner rotatable cylindrical chamber, wherein the motor means is fixed at the bottom of the inner rotatable cylindrical chamber that provides rotation to the inner rotatable cylindrical chamber.

In accordance with an embodiment of the present invention, the motor means further comprising a plurality of motors and a means for rotating the inner rotatable cylindrical chamber of front end machine.

In accordance with an embodiment of the present invention, the rotatable mechanism is having an elevator mechanism configured to hide the front end machine.

In accordance with an embodiment of the present invention, elevator mechanism further includes a plurality of motors connected to a plurality of pulleys, via a rope means and a lift platform having a stopper a means. Further, the plurality of motors is configured to rotate the pulley with the rope means and the lift platform is configured to move the front end machine up and down.

In accordance with an embodiment of the present invention, the elevator mechanism includes a hydraulic means configured to move the lift platform up and down.

In accordance with an embodiment of the present invention, the front end machine is one of electronic safe further comprising steps of reading and authentication of one or more finger prints, if authentication fails a safety alarm is rings otherwise, moved to next step and face recognition and authentication is done, if authentication fails a safety alarm rings otherwise access to the front end machine is provided.

In accordance with an embodiment of the present invention, the front end machine is an ATM and hit by the miscreant, further comprising steps of reading of the magnitude of hit, if the magnitude of hit is low, image is captured. Otherwise, if magnitude of hit is high, the front end machine is configured to execute group of operations.

In accordance with an embodiment of the present invention, the front end machine is an ATM and miscreant try to uproot the front end machine. The method comprises step of checking if front end machine is uprooted, if the front end machine is not uprooted, the method ends otherwise, the front end machine is configured to execute group of operations.

In accordance with an embodiment of the present invention the group of operations is selected from moving and/or hiding the monetary fund tray, ringing alarm and sending an alert message to police station and bank.

In accordance with an embodiment of the present invention, a hiding mechanism is used for moving and hiding the monetary fund tray. The mechanism further includes a motor means connected to the monetary fund tray and a belt and pulley drive connecting the motor means and the monetary fund tray. Further, the motor means is configured to rotate the belt and a consequence the monetary fund tray is moved to the one or more safe place.
In accordance with an embodiment of the present invention the hiding mechanism is having a hydraulic means is configured to move or hide the monetary fund tray.

In accordance with an embodiment of the present invention the monetary fund tray further comprises a door lock to access the network resource when moved to the one or more safe place.

In accordance with an embodiment of the present invention wherein the door lock further comprises a specifically designed lock and key. The lock is having a female locking part and the key is having a male locking part designed to completely mesh up with each other. Further, lock further includes a magnetic strip and key includes a magnetic strip reader. Further, lock and key is configured to unlock the one or more safe place when meshed and swiped with each other.

In accordance with an embodiment of the present invention, the front end machine further includes an ultrasonic finger print sensor that allows access of front end machine without the membership card.

In accordance with an embodiment of the present invention, system for secure access to a network resource comprises of an interface module and an authentication module. Further, the interface module is configured to receive an identification number, one or more biometrics and a password at a front end machine. Also, transmit the identification number, the one or more biometrics and the password from the front end machine to an authentication server. Further, the authentication module is configured to compare the received identification number, the one or more biometrics and the password with stored predefined user credentials at the authentication server for verification of the received identification number, the one or more biometrics and the password. Also transmit a verification confirmation from the authentication server to the front end machine on verification of the received identification number, the one or more biometrics and the password.

In accordance with an embodiment of the present invention, the network resource is selected from a group consisting of a monetary fund, a document store and a data store.

In accordance with an embodiment of the present invention, the identification number is selected from a group consisting of an account number, a customer relationship number and a personal identification number.

In accordance with an embodiment of the present invention, the identification number has been provided in form of a membership card. Further, the membership card further comprises a biometric recognition device configured to read the one or more biometrics. Further, the biometrics recognition device has been provided at one or more location of the membership card.

In accordance with an embodiment of the present invention, the one or more biometrics is one or more of a finger print scan and a facial scan.

In accordance with an embodiment of the present invention, the password is anyone of an original password and a duplicate password. Further, the authentication module is further configured to transmit a verification failure message from the authentication server to the front end machine on receiving the duplicate password at the authentication server. Also the interface module is further configured to execute of one or more security protocols at the front end machine on receipt of the verification failure message at the front end machine.

3. BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS

So that the manner in which the above recited features of the present invention can be understood in detail, a more particular description of the invention, briefly summarized above, may have been referred by embodiments, some of which are illustrated in the appended drawings. It is to be noted, however, that the appended drawings illustrate only typical embodiments of this invention and are therefore not to be considered limiting of its scope, for the invention may admit to other equally effective embodiments.

These and other features, benefits, and advantages of the present invention will become apparent by reference to the following text figure, with like reference numbers referring to like structures across the views, wherein:

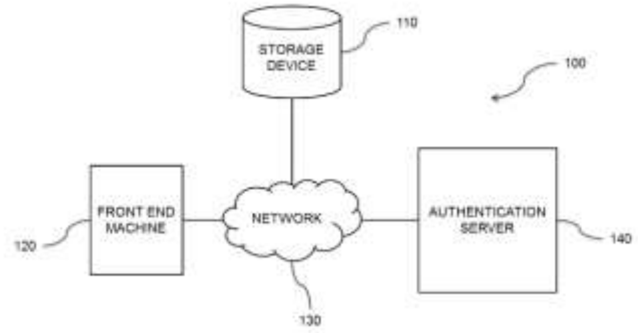

Fig. 1

Fig. 1 illustrates an exemplary environment to which various embodiment of the present invention may be implemented;

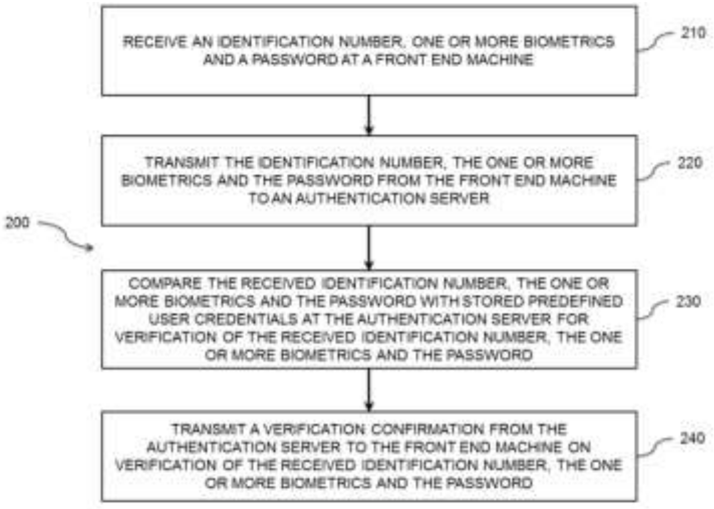
RECEIVE AN IDENTIFICATION NUMBER, ONE OR MORE BIOMETRICS AND A PASSWORD AT A FRONT END MACHINE
210
TRANSMIT THE IDENTIFICATION NUMBER, THE ONE OR MORE BIOMETRICS AND THE PASSWORD FROM THE FRONT END MACHINE TO AN AUTHENTICATION SERVER
220
200
COMPARE THE RECEIVED IDENTIFICATION NUMBER, THE ONE OR MORE BIOMETRICS AND THE PASSWORD WITH STORED PREDEFINED USER CREDENTIALS AT THE AUTHENTICATION SERVER FOR VERIFICATION OF THE RECEIVED IDENTIFICATION NUMBER, THE ONE OR MORE BIOMETRICS AND THE PASSWORD
230
TRANSMIT A VERIFICATION CONFIRMATION FROM THE AUTHENTICATION SERVER TO THE FRONT END MACHINE ON VERIFICATION OF THE RECEIVED IDENTIFICATION NUMBER, THE ONE OR MORE BIOMETRICS AND THE PASSWORD
240

Fig. 2

Fig. 2 illustrates a method for secure access to a network resource, in accordance with an embodiment of the present invention;

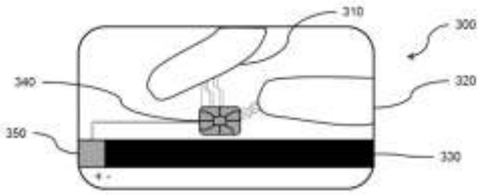

Fig. 3A

Fig. 3A illustrates a membership card, in accordance with an embodiment of the present invention;

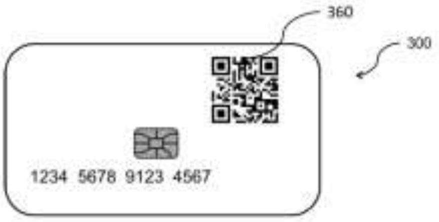

Fig. 3B

Fig. 3B illustrates a front view of the membership card, in accordance with an embodiment of the present invention;

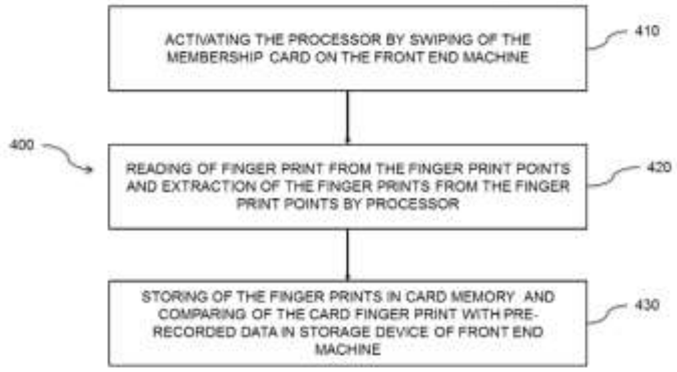
ACTIVATING THE PROCESSOR BY SWIPING OF THE MEMBERSHIP CARD ON THE FRONT END MACHINE
410
400
READING OF FINGER PRINT FROM THE FINGER PRINT POINTS AND EXTRACTION OF THE FINGER PRINTS FROM THE FINGER PRINT POINTS BY PROCESSOR
420
STORING OF THE FINGER PRINTS IN CARD MEMORY AND COMPARING OF THE CARD FINGER PRINT WITH PRE-RECORDED DATA IN STORAGE DEVICE OF FRONT END MACHINE
430

Fig. 4

Fig. 4 illustrates a method of reading one or more biometrics from the membership card, in accordance with an embodiment of the present invention;

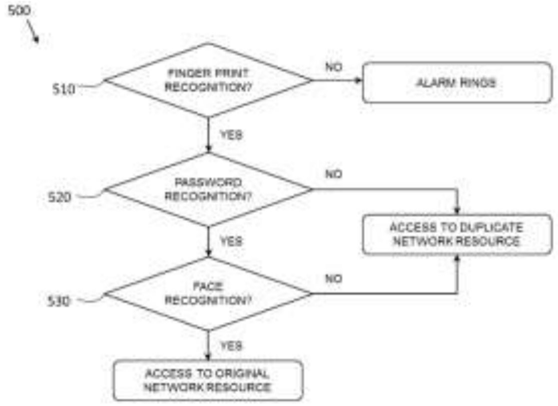
500
510
FINGER PRINT RECOGNITION?
NO
ALARM RINGS
YES
520
PASSWORD RECOGNITION?
NO
ACCESS TO DUPLICATE NETWORK RESOURCE
YES
530
FACE RECOGNITION?
NO
YES
ACCESS TO ORIGINAL NETWORK RESOURCE

Fig. 5

Fig. 5 illustrates a method of providing secure access to the front end machine, in accordance with first embodiment of the invention;

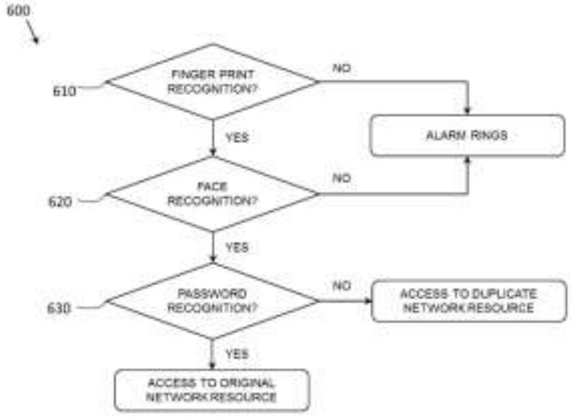
600
610
FINGER PRINT RECOGNITION?
NO
ALARM RINGS
YES
620
FACE RECOGNITION?
NO
YES
630
PASSWORD RECOGNITION?
NO
ACCESS TO DUPLICATE NETWORK RESOURCE
YES
ACCESS TO ORIGINAL NETWORK RESOURCE

Fig. 6

Fig. 6 illustrates a method of providing secure access to the front end machine, in accordance with second embodiment of the invention;

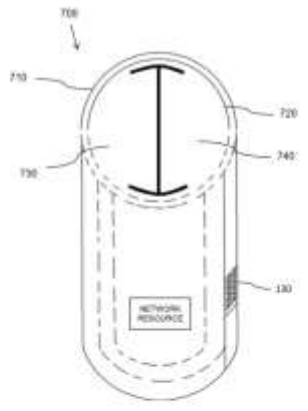

Fig. 7

Fig. 7 illustrates a rotatable mechanism, in accordance with first and second embodiment of the present invention;

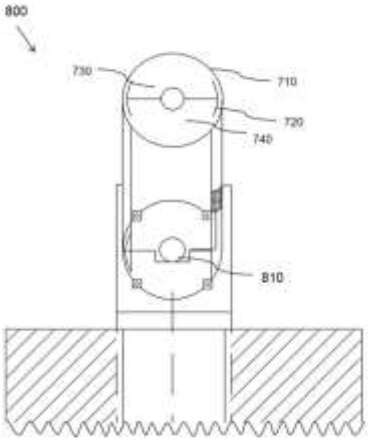

Fig. 8

Fig. 8 illustrates the motor means attached to the inner cylindrical chamber;

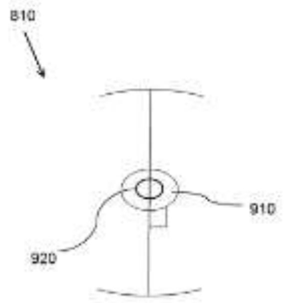

Fig. 9

Fig. 9 illustrates the motor means for rotating the inner cylindrical chamber;

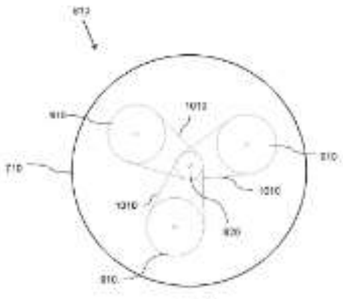

Fig. 10

Fig. 10 illustrates the motor means for rotating the inner cylindrical chamber;

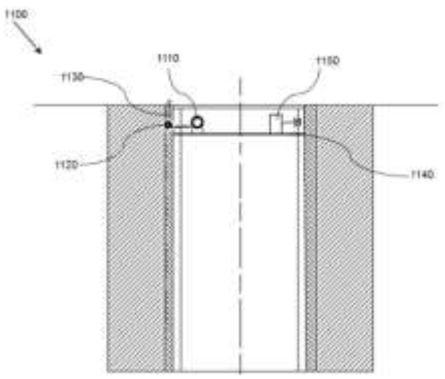

Fig. 11

Fig. 11 illustrated an elevator mechanism, in accordance with first and second embodiment of the present invention;

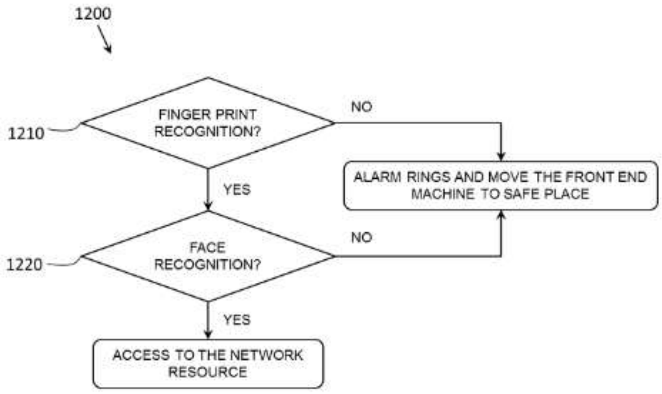
1200
1210
FINGER PRINT RECOGNITION?
NO
ALARM RINGS AND MOVE THE FRONT END MACHINE TO SAFE PLACE
YES
1220
FACE RECOGNITION?
NO
YES
ACCESS TO THE NETWORK RESOURCE

Fig. 12

Fig. 12 illustrates a method of providing secure access to the front end machine, in accordance with third embodiment of the invention;

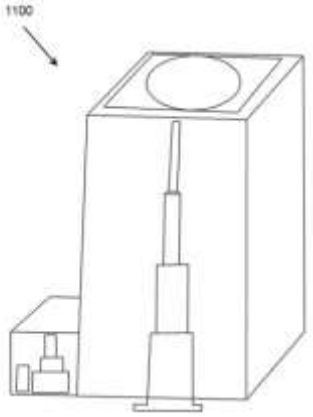

Fig. 13

Fig. 13 illustrates the hydraulic mechanism, in accordance with third embodiment of the present invention;

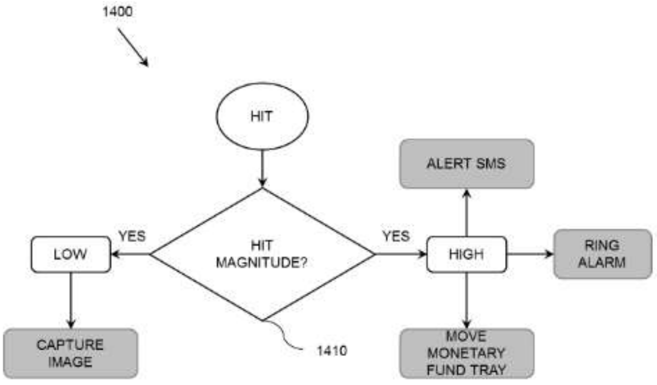

Fig. 14

Fig. 14 illustrates a method of providing secure access to the front end machine, in accordance with fourth embodiment of the invention;

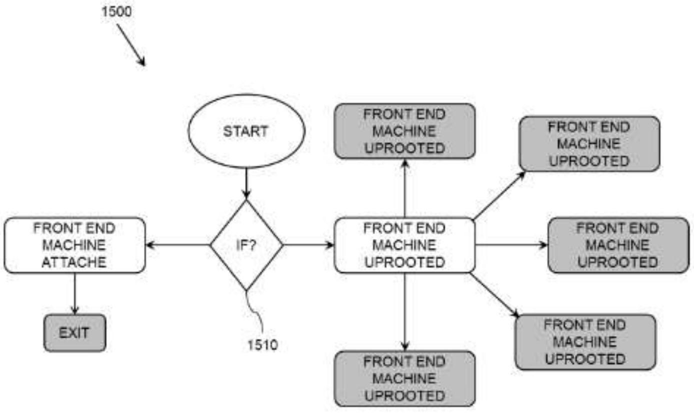
1500
START
IF?
FRONT END MACHINE ATTACHE
EXIT
1510
FRONT END MACHINE UPROOTED
FRONT END MACHINE UPROOTED
FRONT END MACHINE UPROOTED
FRONT END MACHINE UPROOTED
FRONT END MACHINE UPROOTED
FRONT END MACHINE UPROOTED

Fig. 15

Fig. 15 illustrates a method of providing secure access to the front end machine, in accordance with fifth embodiment of the invention;

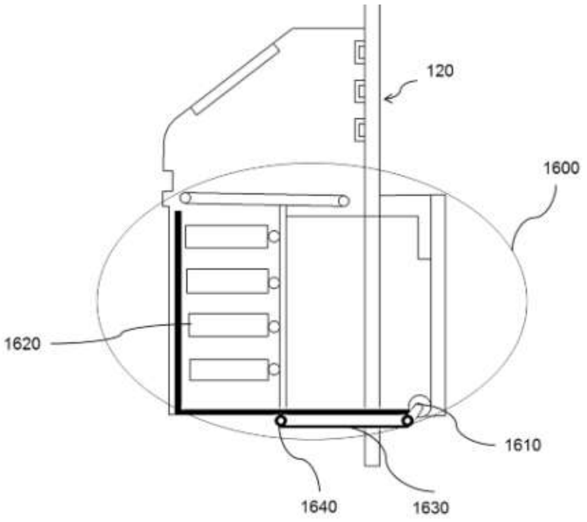

Fig. 16

Fig. 16 illustrates hiding mechanism in accordance with fourth and fifth embodiment of the present invention;

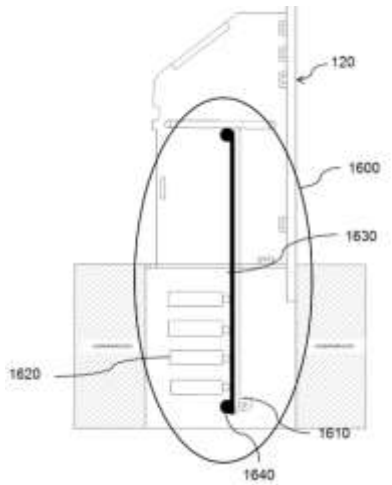

Fig. 17 illustrates hiding mechanism in accordance with fourth and fifth embodiment of the present invention;

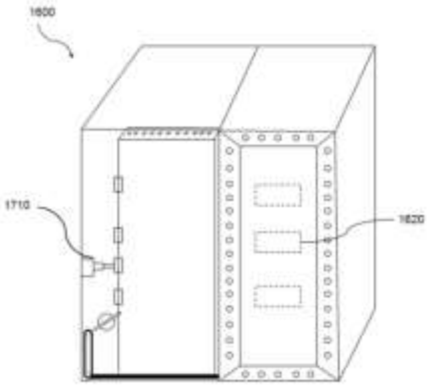

Fig. 18

Fig. 18 illustrates a hiding mechanism, in accordance with fourth and fifth embodiment of the present invention;

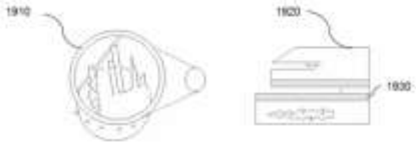

Fig. 19

Fig. 19 illustrates a lock and key, in accordance with fourth and fifth embodiment of the present invention;

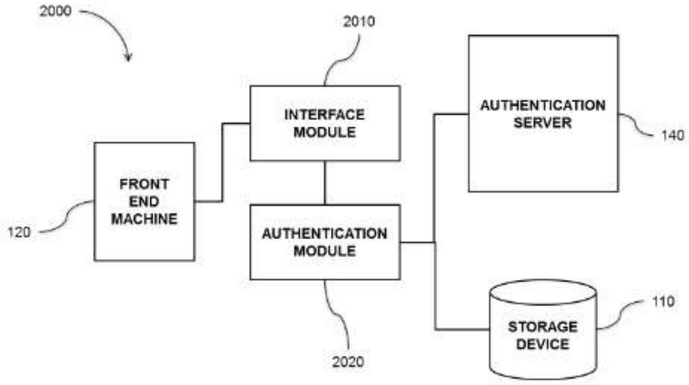

Fig. 20

Fig. 20 illustrates a system for secure access to a network resource, in accordance with an embodiment of the present invention.

4. DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

While the present invention is described herein by way of example using embodiments and illustrative drawings, those skilled in the art will recognize that the invention is not limited to the embodiments of drawing or drawings described, and are not intended to represent the scale of the various components. Further, some components that may form a part of the invention may not be illustrated in certain figures, for ease of illustration, and such omissions do not limit the embodiments outlined in any way. It should be understood that the drawings and detailed description thereto are not intended to limit the invention to the particular form disclosed, but on the contrary, the invention is to cover all modifications, equivalents, and alternatives falling within the scope of the present invention as defined by the appended claim. As used throughout this description, the word "may" is used in a permissive sense (i.e. meaning having the potential to), rather than the mandatory sense, (i.e. meaning must). Further, the words "a" or "an" mean "at least one" and the word "plurality" means "one or more" unless otherwise mentioned. Furthermore, the terminology and phraseology used herein is solely used for descriptive purposes and should not be construed as limiting in scope. Language such as "including," "comprising," "having," "containing," or "involving," and variations thereof, is intended to be broad and encompass the subject matter listed thereafter, equivalents, and additional subject matter not recited, and is not intended to exclude other additives, components, integers or steps. Likewise, the term "comprising" is considered synonymous with the terms "including" or "containing" for applicable legal purposes. Any discussion of documents, acts, materials, devices, articles and the like is included in the specification solely for the purpose of providing a context for the present invention. It is not suggested or represented that any or all of these matters form part of the prior art base or were common general knowledge in the field relevant to the present invention. In this disclosure, whenever a composition or an element or a group of elements is preceded with the transitional phrase "comprising", it is understood that we also contemplate the same composition, element or group of elements with transitional phrases "consisting of", "consisting", "selected from the group of consisting of, "including", or "is" preceding the recitation of the composition, element or group of elements and vice versa.

The present invention is described hereinafter by various embodiments with reference to the accompanying drawing, wherein reference numerals used in the accompanying drawing correspond to the like elements throughout the description. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiment set forth herein. Rather, the embodiment is provided so that this disclosure will be thorough and complete and will fully convey the scope of the invention to those skilled in the art. In the following detailed description, numeric values and ranges are provided for various aspects of the implementations described. These values and ranges are to be treated as examples only, and are not intended to limit the scope of the claims. In addition, a number of materials are identified as suitable for various facets of the implementations. These materials are to be treated as exemplary, and are not intended to limit the scope of the invention.

Referring to the drawings, the invention will now be described in more detail. As shown in Figure 1, an exemplary environment (100) to which various embodiments of the present invention may be implemented. The environment (100) comprises a front end machine (120) connected to an authentication server (140) via a network (130). Then network (100) is further connected to a storage device (110). The front end machine (120) is selected from a group consisting of, but not limited to, ATM, electronic data capture (EDC) machine, electronic access documents safe etc. Further, the EDC machine is configured to swipe debit/credit card for payment transactions. Further, in accordance with various embodiments, the network (140) is a Local Area Network (LAN) or a Wide Area Network (WAN). Preferably, the network (130) is internet. Further, the authentication server (140) is configured to compare the data stored in storage device (110). The storage device (110) contains predefined set of data. A method for secure access to a network resource can now be understood taking the exemplary environment (100) as a reference.

Figure 2 illustrates a method (200) for secure access to a network resource in accordance with an embodiment of the present invention. In accordance with an embodiment of the invention, the network resource is selected from a group consisting of a monetary fund, a document store and a data store. The method (200) begins at step 210 by receiving an identification number, one or more biometrics and a password at the front end machine (120). In accordance with an embodiment of the invention, the identification number is selected from a group consisting of an account number, a customer relationship number and a personal identification number. At step 220, the identification number, the one or more biometrics and the password are transmitted from the front end machine (120) to the authentication server (140). At step 230, the received identification number, the one or more biometrics and the password are compared with stored predefined user credentials at the authentication server (140) for verification of the received identification number, the one or more 20 biometrics and the password. At step 240, a verification confirmation is transmitted from the authentication server (140) to the front end machine on verification of the received identification number, the one or more biometrics and the password. Figure 3 illustrates a membership card (300), in accordance with an embodiment of the present invention. As shown in figure 3, the membership card (300) comprises a biometric recognition device configured to read the one or more biometrics. In accordance with an embodiment of the invention, the one or more biometrics is one or more of a finger print scan and a facial scan. In accordance with an embodiment of the invention, the biometrics recognition device has been provided at one or more location of the membership card.

As can be seen from figure 3A, an exemplary biometric recognition device comprises a plurality of finger print points (310 and 320). Further, the membership card (300) comprises a processor (340), a card memory (350) and a magnetic strip (330). The finger print points (310 and 320) are configured to extract prints from the finger prints from the finger print points (310 and 320). Further, the processor (340) is configured to receive the extracted finger prints and store the extracted finger prints in the card memory (350). The magnetic strip (330) and processor (340) are configured to activate electronically when the magnetic strip (330) of the membership card (350) is swiped on the front end machine (120).

Figure 3B illustrates a membership card (300), in accordance with an embodiment of the present invention. As shown in figure 3B, the membership card contains a QR code (360). The QR code (360) is provided in form a sticker to the membership card owner. Further, the QR code (360) contains the one or more personal details of the membership card owner. The one or more personal detail is selected from group of, but not limited to, name, contact number, email ID etc. The reason of providing a QR code (360) sticker on the membership card is, if the membership is misplaced and found by someone, the person can be easily contacted through the personal details provided in the QR code (360).

In accordance with an embodiment of the present invention, the method for secure access to a network resource further comprises steps of, transmitting a verification failure message from the authentication server (140) to the front end machine (120) on receiving the duplicate password at the authentication server(140). Further, the storage device (110) contains two set of passwords, one is original password used by the authority to access original network resource whereas other is a duplicate password which is fed by the authority to mislead the miscreants. The two passwords are kept for a reason; if the authority is challenged or terrified by the miscreant then the authority can disclose the duplicate password.

In accordance with an embodiment of the present invention, the method for secure access to a network resource further comprises steps of execution of one or more security protocols at the front end machine (120) on receipt of the verification failure message at the front end machine.

In accordance with an embodiment of the invention, the front end machine (120) on receiving the verification failure message executes one or more security protocols.

Figure 4 illustrates a method (400) of reading one or more biometrics from the membership card, in accordance with an embodiment of the present invention. The method begins at step (410) by activating the processor (340) with swiping of the membership card (300) on the front end machine (120). At step (420), the finger prints are extracted from the finger print points (310 and 320) by the processor (340). At step 430, the finger prints are stored in card memory (350) and the finger prints are compared with stored predefined user credentials in storage device (110) of front end machine (120).

In accordance with embodiment of the invention, the finger prints can be taken from any part of the membership card (300). Further, the membership card (300) activates by swiping on front end machine (120) and no external source such as battery is required to activate the membership card (300).

In accordance with embodiment of the invention, the membership card (300) is slowly swiped and if required held for 1 to sec for activating the membership card (300). The front end machine (120) is further configured to send a message containing one time password at the handheld mobile device while accessing the network resource. Further, the message containing one-time password (OTP) is sent through the network (130) to a handheld mobile device which is further fed to front end machine (120) for authentication. The front end machine (120) is further configured to send a message containing one time password at the handheld mobile device while accessing the network resource. Further, the message containing one time password is send through the network (130) to the handheld mobile device which is further fed to front end machine for authentication. In accordance with embodiment of the present invention, the one or more security protocols includes hiding the original network resource and providing access to the duplicate network resource, hiding the front end machine (120) in one or more safe place, shifting or moving the network resource to one or more safe place. The one or more safe place is one of the, but not limited to beneath, left side or right side , above and/or inside and outside of the front end machine (120).

In accordance with first embodiment of the invention, an exemplary method (500) of providing secure access to the front end machine (120), wherein the front end machine (120) is one of electronic safe. The method (500) starts at step (510), by reading and authentication of the one or more finger prints, if authentication fails a safety alarm rings, otherwise the method (500) moves to step (520). The one or more finger prints are read at front end machine (120) and authentication is done at authentication server (140). Further, the one or more finger prints are read from at least three fingers. At step (520), reading and authentication of the password is done, if authentication fails access to a duplicate material is provided otherwise, the method moves to step (530). Further, the password is read by the front end machine (120) and authenticated by the authentication server (140). At step (530), face or eyes recognition and authentication is done, if authentication fails, access to the duplicate material is provided otherwise access to original network resource is provided. Further, face or eyes recognition is done by the front end machine (120) and compared with the store data at authentication server (140).

In accordance with second embodiment of the invention, an another exemplary method (600) of providing secure access to the front end machine (120), wherein the front end machine (120) is one of an electronic safe. The method (600) starts at step (610), reading and authentication of one or more finger prints, if authentication fails a safety alarm is rings otherwise, the method (600) moves to step (620). Further, reading of the one or more finger prints is done at the front end machine (120) and authentication is done at authentication server (140). The one or more finger prints are at least three fingers. At step (620), face or eyes recognition and authentication is done, if authentication fails a safety alarm rings, otherwise the method (600) moves to the step (630). Further, face or eyes recognition is done at the front end machine (120) and authentication is done at authentication server (140). The one or more finger prints are of at least three fingers.

At step (630), reading and authentication of a password is done, if authentication fails access to duplicate network resource is provided otherwise access to original network resource is provided. Further, reading of the password is done at the front end machine (120) and authentication is done at authentication server (140).

In accordance with first and second embodiment of the present invention, an exemplary front end machine (120) further comprises a rotatable mechanism (700) for hiding the original material and providing access to a duplicate network resource or vice versa. The rotatable mechanism (700) is inside and controlled by the front end machine (120). As shown in figure 7, in accordance with first and second embodiment of the present invention, the rotatable mechanism (700) comprises a cylindrical vault (710) having an inner rotatable cylindrical chamber (720) inscribed inside the cylindrical vault (710), Further, the inner rotatable chamber (720) is further having an original face or eyes (730) and a duplicate face or eyes (740) bisecting the rotatable cylindrical chamber (720) into two equal halves and a motor means (not shown in figure 7) to rotate the inner rotatable cylindrical chamber. (720). Further, the motor means is fixed at the bottom of the inner rotatable cylindrical chamber (720) that provides rotation to the inner rotatable cylindrical chamber (720).

In accordance with first and second embodiment of the present invention, the original face or eyes (730) contains the original network resource and the duplicate face or eyes (740) contains the duplicate network resource. Each phase, duplicate phase (740) and original phase (730) has one separate door to provide access to their respective duplicate and original network resources.

In accordance with first and second embodiment of the present invention, the motor means further comprises a plurality of motors (910) and a means for rotating the inner rotatable cylindrical chamber (720) of front end machine (120).

Figure 8 illustrates the motor means (810) attached to the inner cylindrical chamber. As shown in figure 8, the motor means (810) is fixed at the bottom of the inner rotatable cylindrical chamber (720) that provides rotation to the inner rotatable cylindrical chamber (720). Figure 9 illustrates the motor means (810) for rotating the inner cylindrical chamber. As shown in figure 9, in accordance with first and second embodiment of the present invention. The motor means (810) is having a single motor (910), directly connected to a central hub (920). Further, the central hub (920) rotates the inner rotatable chamber. Figure 10 illustrates the motor means (810) for rotating the inner cylindrical chamber. As shown in figure 10, in accordance with first and second embodiment of the present invention the motor means (810) includes a plurality of motors (910) connected to the center hub (920) by belts (1010). The plurality of motors (910) rotates the central hub (920). The central hub (920) is directly connected with the inner rotatable chamber (620). Further, if one of the motor (910) becomes un-functional or fails the other two motors (910) rotate the central hub (920). The failure of one of the motor (910) is further read by the front end machine (120) and displayed at front end machine (120) to replace the faulty motor.

In accordance with first and second embodiment of the present invention, the rotatable mechanism (700) further comprises an elevator mechanism (not shown in figure 10). In the exemplary embodiment of the present invention, as shown in figure 11, the underground elevator mechanism (1100) is fixed beneath the rotatable mechanism (700) having an underground hole sufficient to accommodate the cylindrical vault (710) including the front end machine (120).

In accordance with first and second embodiment of the present invention, the elevator mechanism (1100) comprises a plurality of motors (1110) connected to a plurality of pulleys (1120), via a rope means (1130); and a lift platform (1140) having a stopper means (1150). Further, the plurality of motors (1110) is configured to rotate the pulley (1120) with the rope means (1130). The lift platform (1150) is configured to move the front end machine (120) up and down. Further, the stopper means (1150) holds the lift platform (1150) at up and/or down position.

Further, the elevator mechanism (1100) is provided as an added safety feature as and when miscreant tries to root up the cylindrical vault (710). The cylindrical vault (710) is moved to the underground hole by the elevator mechanism (1100) preventing the miscreants to uproot the front end machine (120).

In accordance with first and second embodiment of the present invention, the front end machine (120) further comprises a GPS module. Further, as and when cylindrical vault (710) with front end machine (120) is moved to the underground hole by the elevator mechanism. The front end machine (120) sends a location of the front end machine (120). Further, the front end machine (120) sends an alert message to nearest police station and authorized machine owner such as Casino, bank etc. The front end machine (120) sends the location after a fixed interval of time. A fixed interval of time is 10 sec, 30 sec and/or 1min.

In accordance with first and second embodiment of the invention, the front end machine (120) further comprises an audio and video recording means. The authentication server (140) records the audio and video, when the front end machine (120) is inside the underground hole of elevation system (1100).

In accordance with third embodiment of the invention, another exemplary method (1200) of providing secure access to the front end machine (120) is provided. Further, the front end machine (120) is one of an electronic safe. The method (1200) starts at step (1210), reading and authentication of one or more finger prints, if authentication fails a safety alarm is rung otherwise, the method (1200) moves to step (1220). At step (1220), face or eyes recognition and authentication is done, if authentication fails a safety alarm rings otherwise access to the front end machine (120) is provided.

In accordance with third embodiment of the present invention, reading of the one or more finger prints and face or eyes recognition is done at front end machine (120). Further, authentication is done at the authentication server (140)

In accordance with third embodiment of the present invention, the exemplary embodiment of the front end machine (120) further includes an elevator mechanism (1100) as explained above. The elevator mechanism (1100) is fixed beneath the front end machine

(120) and having an underground hole sufficient to accommodate the front end machine (120). The front end machine (120) is moved to a safe place such as an underground hole of the elevator mechanism (1100) preventing the miscreants to uproot the system. Figure 13 illustrates the hydraulic mechanism, in accordance with third embodiment of the present invention. As shown in figure 13, the elevator mechanism (1100) includes a hydraulic means configured to move the lift platform up and down.

In accordance with the third embodiment of the present invention, the front end machine (120) further comprises a GPS module. Further, as and when cylindrical vault (710) with front end machine (120) is moved to the underground hole by the elevator mechanism. The front end machine (120) sends location of the front end machine (120). Further, the front end machine (120) sends an alert message to nearest police station and authorized machine owner such as Casino, bank etc. The front end machine (120) sends the location after a fixed interval of time. A fixed interval of time is 10 sec, 30 sec and/or 1min.

In accordance with the first and second embodiment of the invention, the front end machine (120) further comprises an audio and video recording means. The front end machine (120) records the audio and video, when the front end machine (120) is inside the underground hole of elevator mechanism (1100).

In accordance with fourth embodiment of the invention, the exemplary method (1200) of providing secure access to a front end machine (120), wherein the front end machine (120) is an ATM and hit by the miscreant, further comprising steps of reading of the magnitude of hit, if the magnitude of hit is low, image is captured. Otherwise, if magnitude of hit is high, the front end machine is configured to execute a group of operation. In accordance with embodiment of the invention, the group of operations is selected from, but not limited to, move and/or hide the monetary fund tray, ring alarm and send an alert message to a police station and a bank.

In accordance with fifth embodiment of the invention, the method
(1200) of providing secure access to a front end machine (120), wherein the front end machine (120) is an ATM and miscreant try to uproot the front end machine (120). The method (1200) comprises step of checking if front end machine (120) is uprooted, if the front end machine (120) is not uprooted, the method ends otherwise, the front end machine (120) is configured to execute group of operations.

In accordance with fifth embodiment of the invention, the group of operations is selected from a group, but not limited to hiding and or moving the monetary fund tray, ringing alarm, send location of the front end machine, sending an alert message to police station and bank and record audio and video. Further, the location of the front end machine (120) is repeatedly sent after an interval of time. Further, the interval of time is one of, but not limited to 10 sec, 30sec and/or 1 min.

In accordance with fourth and fifth embodiment of the present invention, an exemplary embodiment of the hiding mechanism (1600) is provided. As shown in figure 16, the mechanism (1600) further includes a motor means (1610) connected to the monetary fund tray and a belt (1630) and pulley drive connecting the motor means and the monetary fund tray. Further, the motor means (1610) is configured to rotate the belt and a consequence the monetary fund tray is moved to the one or more safe place.

In accordance with fourth and fifth embodiment of the present invention the mechanism (1600) on receiving the signal of high magnitude of hit or uprooting of front end machine, it activates the hiding mechanism (1600) that further moves the monetary fund tray to the one or more safe place.

In accordance with fourth and fifth embodiment of the present invention, the one or more safe place is part of the front end machine and/or under the front end machine. Figure 17 illustrates the hiding mechanism (1600), in accordance with fourth and fifth embodiment of the present invention. As shown in figure 17, the monetary fund tray (1320) is moved under the front end machine by the hiding mechanism (1600). As shown in figure 18, in accordance with fourth and fifth embodiment of the present invention the hiding mechanism (1600) comprises hydraulic means (1810) that moves the monetary fund tray of the front end machine (120) and is shown in figure 18.

In accordance with fourth and fifth embodiment of the present invention, the one or more safe place is outside the front end machine (120) and is selected from, but not limited to a concrete wall, a steel wall.

In accordance with fourth and fifth embodiment of the present invention, one or more of the safe place is locked when monetary fund tray (1620) is moved to the one or more of the safe place. Further, monetary fund tray (1620) is locked inside the one or more safe place. Further, for accessing the monetary fund tray (1620), a door lock is provided on the door of the one or more safe place.

In accordance with fourth and fifth embodiment of the present invention, the lock (1910) and key (1920) of the one or more safe place is specially designed. As shown in figure 19, the lock (1910) is having a female locking part and the key (1920) is having a male locking part designed to completely mesh up with each other. The male and female pattern of the lock (1910) and key (1920) are critically designed so that key pattern cannot be replicated. Further, lock (1910) further includes a magnetic strip (1930) and key (1920) includes a magnetic strip reader.

Further, lock (1910) and key (1920) is configured to unlock the one or more safe place when meshed and swiped with each other. The magnetic strip (1930) on the key (1920) and the magnetic strip reader on the lock (1910) acts as an additional security feature for accessing the one or more safe place.

In accordance with fourth and fifth embodiment of the present invention, a method of providing secure access to the front end machine (120). The front end machine (120) further includes an ultrasonic finger print sensor that allows access of front end machine without the membership card (300). Further, once the front end machine (120) is accessed, the previous finger prints are brushed up by the front end machine (120). Figure 5 illustrates a system (2000) for secure access to a network resource, in accordance with an embodiment of the present invention. As shown in figure 5, the system (2000) comprises an interface or eyes module (2010) and an authentication module (2020). The interface module (2010) is configured to receive an identification number, one or more biometrics and a password at a front end machine (120) and transmit the identification number, the one or more biometrics and the password from the front end machine (120) to an authentication server (140). Further, the authentication module (2020) is configured to compare the received identification number, the one or more biometrics and the password with stored predefined user credentials at the authentication server (140) for verification of the received identification number, the one or more biometrics and the password. Also, transmit a verification confirmation from the authentication server (140) to the front end machine (120) on verification of the received identification number, the one or more biometrics and the password. The authentication module (2020) is further configured to verify the message containing one time password, when one time password is fed to the front end machine.

In accordance with an embodiment of the present invention, the authentication module (2020) is further configured to transmit a verification failure message from the authentication server (140) to the front end machine on receiving the duplicate password at the authentication server (140). Also, the interface module (2010) is further configured to execute one or more security protocols at the front end machine (120) on receipt of the verification failure message at the front end machine (120). The methods and systems discussed above provide solutions including setting a duplicate password by an authorized person which will be predefined, and that skips the front end machine (120) from original interface and provides it with a duplicate network resource that seems original to a miscreant. Further, the embodiments provide a very secure access to the front end machine (120). Further advantages include use of front end machine (120) without the membership card (300) only finger prints are required to access. The monetary funds, confidential and important documents are very safe as high tech security features are provided. Thus, the present invention provides the most secure access to the front end machine (120).

Various modifications to these embodiments are apparent to those skilled in the art from the description and the accompanying drawings. The principles associated with the various embodiments described herein may be applied to other embodiments. Therefore, the description is not intended to be limited to the embodiments shown along with the accompanying drawings but is to be providing broadest scope of consistent with the principles and the novel and inventive features disclosed or suggested herein.

Accordingly, the invention is anticipated to hold on to all other such alternatives, modifications, and variations that fall within the scope of the present invention and appended claim.

.

References

[1] Paul E. Sperry January 2011“The Great American Bank Robbery” The Unauthorized Report About What Really Caused the Great Recession.

[2] Yingzi (Eliza) Du 2013 “Biometrics: From Fiction to Practice”.

[3] Ronald Chase 2016 “The Great Mars Hill Bank Robbery”.

[4] Google, Robbery Movies, Robbery News.

Author Profile

	Uma Shankar Gupta received MCA. Degree in Computer Application from Punjab Technical University (Ludhiana), And also done Microsoft Certified IT Professional (Bangalore), Master in Network Administration (Bangalore), Ethical Computer Hacking (Ludhiana), Computer Hacking Forensic Investigation (Hyderabad), and CFX (Hyderabad).