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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 January 2019 (24.01.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/014775 A1

(51) International Patent Classification:
G07C 9/00 (2006.01) *G06F 21/43* (2013.01)
G06F 21/32 (2013.01) *H04Q 1/04* (2006.01)

(21) International Application Number:
PCT/CA2018/050884

(22) International Filing Date:
20 July 2018 (20.07.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/535,413 21 July 2017 (21.07.2017) US

(71) Applicant: **BIOCONNECT INC.** [CA/CA]; 202-109 Atlantic Avenue, Toronto, Ontario M6K 1X4 (CA).

(72) Inventors: **PATEL, Pritesh Yogesh**; 5080 Fairview Street, Unit 33, Burlington, Ontario L7L 7E9 (CA). **SOLOMON, Josh**; 38 Joe Shuster Way, Unit 528, Toronto, Ontario M6K 0A5 (CA). **ALEXANDER, Chris**; 215 Fort York Blvd., Toronto, Ontario M5V 4A2 (CA). **SNELL, Anthony**; 198 St. Clarens Ave., Toronto, Ontario M6H 3W3 (CA). **DOUGLAS, Jordan**; c/o BioConnect Inc., 202-109 Atlantic Avenue, Toronto, Ontario M6K 1X4 (CA). **DOUGLAS, Robert Murray**; 183 Wellington St. West, Toronto, Ontario M5V 0A1 (CA). **CREWS, Jeff**; c/o BioConnect Inc., 202-109 Atlantic Avenue, Toronto, Ontario M6K 1X4 (CA).

(74) Agent: **NORTON ROSE FULBRIGHT CANADA LLP**; 1 Place Ville Marie, Suite 2500, Montreal, Québec H3B 1R1 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM,

(54) Title: BIOMETRIC ACCESS SECURITY PLATFORM

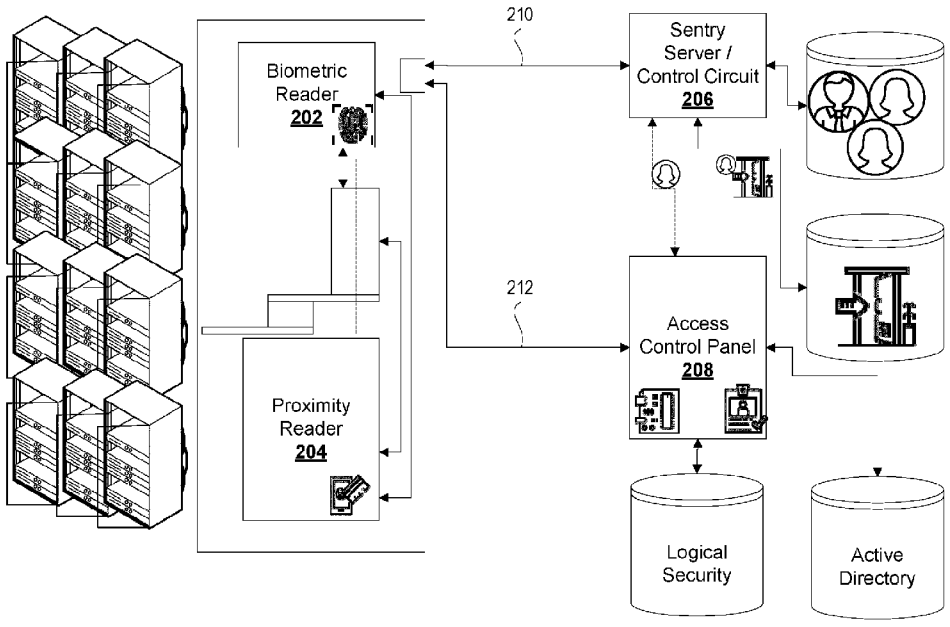

FIG. 2

(57) Abstract: An electronic, securement system for controlling physical access to a controlled space by one or more users, the system including a controller configured to actuate a physical locking mechanism in response to one or more control signals; a biometric receiver configured for receiving a biometric data set obtained from a user of the one or more users; a network interface component configured for transmitting a data representation derived from at least the biometric data set to a sentry component; and a sentry component configured for (i) performing a matching challenge to determine whether the data representation matches a corresponding authorized user, and (ii) responsive to a positive determination of a match, communicating the one or more control signals to the physical locking mechanism to actuate an unlocking by the physical locking mechanism, provisioning physical access to the controlled space.

WO 2019/014775 A1

[Continued on next page]

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

BIOMETRIC ACCESS SECURITY PLATFORM

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is a non-provisional of, and claims all benefit, including priority to, United States Patent Application No. 62/535413, entitled "BIOMETRIC ACCESS SECURITY PLATFORM", dated 21-Jul-2017. The above application is incorporated herein by reference in its entirety.

FIELD

[0002] The present disclosure generally relates to the field of physical access security, and more particularly, improved physical access security for computing component enclosures utilizing biometric matching challenges.

INTRODUCTION

[0003] Improving physical access security to computing components is a desirable objective. Conventional approaches include the use of locked cabinets (e.g., requiring a specific physical key or keypad combination. In the course of Applicants' development of improved security products for data center facilities, Applicants found that simple physical mechanisms alone were not sufficient to provide a satisfactory level of access security and traceability.

[0004] Physical access security is important. Computing components, for example, in some cases are held off-network or without internet access deliberately to further shield the computing components from cyberattacks. These computing components often store extremely valuable information, such as cold storage for cryptocurrency wallets.

[0005] These computing components can be 'air-gapped' such that a closed or limited access system is provided. The computing components can store other critical information or perform critical functions, such as for use in life-support systems (medical equipment), power plant control, industrial control systems, among others. Some computing components store access keys or provide high-security certificate management systems.

[0006] Computing components may have varying levels of security depending on the criticality of the functions performed and/or value of data stored thereon. For example, production servers and disaster recovery servers may have a higher level of access control, while test servers may have a lower level of access control.

[0007] Data centers can be very large. Facilities under consideration include large shared data centers that house hundreds of thousands of computing devices, and require significant cooling and electricity resources.

SUMMARY

[0008] A securement device is described in various embodiments that is adapted for providing technical security improvements that specifically segregate communications for determination of the identity of a user and the determination of whether the user should be provisioned access. The securement device is configured for network communications across one or more communication links. The networked securement device is a tangible device adapted for improving physical security to prevent direct physical access to computing devices.

[0009] Physical security for data centers is a point of vulnerability. The devices described herein are provided as a portion of the security that is a component of an overall security strategy (e.g., protected buildings and facilities).

[0010] The system improves on simple cabinet / rack server mechanisms whose securement mechanisms can potentially be overcome by a malicious user or penetration tester with adequate access to lockpicking or door latch bypassing tools. Furthermore, these malicious users or penetration testers may also attack vulnerabilities of an electronic credential (e.g., token) / biometric reader (e.g., fingerprint, voiceprint, eyeprint) itself, for example, attempting to overwhelm the reader with spoofed information (e.g., a brute force attack), among others.

[0011] The devices, in some embodiments, interoperate with access control management systems, active directory systems, among others. Identities are first verified and determined based on physical access credentials provided (e.g., NFC card, biometric scanner).

[0012] If the identity matches an identity stored on a separate device and that identity, based on logic circuitry stored thereon the separate device, should be provisioned access, access is granted. Separation of identity determination and identity management by utilizing independent networks and independent computing devices decreases system vulnerability to attack, at the cost of increased infrastructure and complexity.

[0013] Access is granted through the physical actuation of a physical security mechanism, which, for example, can include a magnetic lock, a physical lock (e.g., a latch, a lever, a bolt). Actuation may include the transmission of an electrical signal that controls an actuation device (e.g., a solenoid).

[0014] The networked securement device controls physical access to a controlled space by one or more users. The controlled space, in a preferred embodiment, is a server cabinet that can hold data center server racks. These racks house computing infrastructure devices, such as computer servers, rack mounted computer appliances, networking cables, among others. The computing devices of the racks may be connected to various input interfaces, including displays, such as a keyboard, video, and mouse (KVM) switch that allows control of multiple devices within the rack. The KVM allows an administrator to access a server and login and perform various functions. In some embodiments, the ability to login may be coupled to the verified identity and/or the open/close status of the cabinet lock (e.g., continuous detection of operating state or event detection indicative of toggled states).

[0015] Users that require access are varied. The users can include system administrators, cleaning personnel, programmers, among others. In the context of this description, data centers having highly secure access controls are contemplated. This is especially challenging in view of shared, non-exclusive computing environments, such as data centers that allow for colocation or managed hosting. In shared, non-exclusive computing environments, the set of users who have access credentials may be dynamically modified as users purchase or release allocations.

[0016] Malicious users may attempt to gain entry through various approaches, including spoofing identities, flooding the device with a large number of entry attempts, disabling electrical power, disabling networked communications, tapping into electrical circuits to

modify signals, etc. Avoiding direct connections between the physical access credential scanner and the mechanism that acts as an arbiter to determine access control provisioning decisions is important.

[0017] The networked securement device includes a controller circuit configured to actuate a physical locking mechanism in response to one or more control signals, the physical locking mechanism coupled to a biometric receiver configured for receiving a biometric data set obtained from a user of the one or more users and transmitting a representation of the biometric data set to a communications splitter circuit. The communications splitter circuit, in some embodiments, is a physical communications mechanism that bifurcates communications paths. A benefit of using the communications splitter circuit includes a reduced need for retrofits or modifications. In other embodiments, two separate communication links (e.g., wires) are used rather than the communications splitter circuit. In these embodiments, the networked securement device includes separate network interfaces.

[0018] The communications splitter circuit is configured to receive the biometric data set and the communications splitter circuit including a first electronic communication interface and a second electronic communication interface.

[0019] The first electronic communication interface is adapted to provide a first communication channel between the communications splitter circuit and a sentry computer server, and the second electronic communication interface is adapted to provide a second communication channel between the communications splitter circuit and an access control device.

[0020] The communications splitter circuit transmits the representation of the biometric data set to the sentry computer server across the first communication channel, the sentry computer server configured for (i) performing a matching challenge to determine whether the representation of the biometric data set matches a corresponding authorized user, and (ii) responsive to a positive determination of a match, generating and transmitting a data set representative of an identity profile corresponding to the user to the communications splitter

circuit across the first communication channel. The sentry computer server thus aids in determination of "who" the user should be.

[0021] The sentry computer server is an intermediary mechanism that, while requiring increased complexity of computing infrastructure, allows for a more systematic and specialized approach in validating credentials. For example, the sentry computer server in some embodiments includes additional logic and connections to external systems that can be used to determine whether a user profile is actually associated with a set of credentials (e.g., a verification can be checked against a front door sensor, such as a revolving door mantrap, to ensure that the user actually entered the premises before the sentry computer server outputs an identity to the access control device). Accordingly, against falsified credentials (e.g., by stealing or cloning prints), the sentry computer server is a first line of defense.

[0022] Furthermore, the sentry computer server of some embodiments is configured to track patterns of entry and flag aberrations in patterns that may be indicative of falsified entry (e.g., fingerprints that have been cloned using powder and cello tape over the reader, or identity information stolen or cloned by hacking into on-board storage of a biometric reader).

[0023] Responsive to the receipt of the data set representative of the identity profile across the first communication channel, the communications splitter circuit or the controller circuit is further configured to transmit the data set representative of the identity profile to an access control device across the second communication channel, and the access control device, upon determining that the identity profile matches an authorized user of a set of authorized users, is configured to transmit the one or more control signals to the controller circuit across the second communication channel and the communications splitter circuit to cause the actuating of the physical locking mechanism. The access control device, based on "who" the user is, utilizes computer logic to determine whether access should be granted to that user.

[0024] The embodiments described herein increase security of the access control device by segregating the access control device and communications thereof from direct queries or signals from the coupled biometric receiver. Accordingly, a denial of service type attack or a

brute force attack cannot be used to overwhelm the access control device, which is effectively the adjudication mechanism for ultimately determining whether access should be granted. Rather, such an attack would result in an overwhelmingly large number of queries to be transmitted to the sentry computer server, which may then result in processing issues at the sentry computer server, but unauthorized access will not be granted from the access control device. Furthermore, an attacker physically splicing wires to inject packets may find it difficult to intercept and modify signals from the biometric receiver due to the presence of the splitter circuit, as the biometric sets are not used directly for access control decisions by the access control device, but rather, it is a specially formed signal indicative of a specific user's profile or identity that is received at the sentry computer server.

[0025] In an embodiment, the access control device, rather than receiving a signal from the splitter circuit, includes a connection directly to the sentry computer server.

[0026] In another aspect, the biometric receiver is configured to generate one or more periodic electronic heartbeat signals periodically transmitted to the sentry computer server across the first communication channel.

[0027] In another aspect, the biometric receiver is configured to stagger the one or more periodic electronic heartbeat signals periodically transmitted to the sentry computer server across the first communication channel relative to one or more periodic electronic heartbeat signals from other biometric receivers.

[0028] In another aspect, the matching challenge performed by the sentry computer server includes a verification of whether the user has successfully verified at one or more preceding verification mechanisms.

[0029] In another aspect, the one or more preceding verification mechanisms includes an interlocking door controller configured to enable only a single user to validate and pass through at each operation of the interlocking door controller.

[0030] In another aspect, the controlled space includes one or more access-controlled computing devices having one or more user accounts residing on memory stored thereon; the one or more access-controlled computing devices are electronically coupled to the

communications splitter circuit or the controller circuit; and the one or more access-controlled computing devices are configured only to allow access to one or more user accounts corresponding to the identity profile.

[0031] In another aspect, the controller circuit is configured to track an open or close status of the physical locking mechanism; and wherein the one or more access-controlled computing devices are configured only to allow access to the one or more user accounts during a duration that the physical locking mechanism is in the open status.

[0032] In another aspect, the controller circuit is configured to track an open or closed status of the physical locking mechanism; and wherein the one or more access-controlled computing devices are configured to revoke access to the one or more user accounts during a duration that the physical locking mechanism is in the closed status.

[0033] In another aspect, the controller circuit is configured to track an open or closed status of the physical locking mechanism; and wherein the one or more access-controlled computing devices are configured to revoke access to all user accounts responsive to a determination that the physical locking mechanism is in the closed status.

[0034] In another aspect, the one or more access-controlled computing devices is configured to automatically authenticate the user on a backend electronic directory service, enabling access the to one or more user accounts during a duration that the physical locking mechanism is in an open status.

[0035] In another aspect, the communications splitter circuit is configured to monitor network connection statuses corresponding to each of the first communication channel and the second communication channel; the controller circuit includes on-board non-transitory computer memory storing one or more biometric profiles; and the controller circuit is configured to, responsive to a determination by the communications splitter circuit that the first communication channel is inactive, perform the matching challenge against the stored one or more biometric profiles, and transmit the data set representative of the identity profile across the first communication channel to the access control device.

[0036] In another aspect, the first communication channel and the second communication channel are physically independent of one another.

[0037] In another aspect, the first communication channel and the second communication channel are electrically separated relative to one another.

[0038] In another aspect, the first communication channel and the second communication channel utilize different encryption protocols.

[0039] In another aspect, the first communication channel and the second communication channel utilize different communication protocols.

[0040] In accordance with one aspect, there is provided an electronic, networked securement device for controlling physical access to a controlled space by one or more users, the device comprising: a controller configured to actuate a physical locking mechanism in response to one or more control signals; a biometric receiver configured for receiving a biometric data set obtained from a user of the one or more users; a network interface component configured for transmitting a data representation derived from at least the biometric data set to a sentry component; and a sentry component configured for (i) performing a matching challenge to determine whether the data representation matches a corresponding authorized user, and (ii) responsive to a positive determination of a match, communicating the one or more control signals to the physical locking mechanism to actuate an unlocking by the physical locking mechanism, provisioning physical access to the controlled space.

[0041] In accordance with another aspect, the sentry component is configured to manage a first and a second electronic, networked securement device, the first electronic, networked securement device securing a front access panel of a computing component rack, and the second electronic, networked securement device securing a rear access panel of a computing component rack.

[0042] In accordance with another aspect, the physical locking mechanism and the biometric receiver reside in a housing, the housing connected to a network cable, the

network cable connected to a splitter that enables parallel communication with the sentry and with a centralized access control panel.

[0043] In accordance with another aspect, the sentry component is electronically coupled to a backend template matching engine, the backend template matching engine configured to receive the data representation and to determine whether the data representation matches any corresponding authorized user, and to provide the positive determination of the match where a match is successfully identified.

[0044] In accordance with another aspect, the sentry component is electronically coupled to one or more other sentry components.

[0045] In accordance with another aspect, the sentry component is electronically coupled to an access control system, the access control system configured for provisioning access to a secured facility.

[0046] In accordance with another aspect, the biometric receiver includes on-board computer-readable memory for local storage of data representations for the one or more authorized users.

[0047] In accordance with another aspect, the device further includes a near-field communications receiver configured to wirelessly receive user identification inputs stored on a proximity card.

[0048] In accordance with another aspect, the proximity card locally stores a copy of the data representation, and wherein the matching challenge is performed first against the local copy of the data representation.

[0049] In accordance with another aspect, upon a failed challenge, the matching challenge is performed second against a networked copy of the data representation.

[0050] In accordance with another aspect, there is provided a method for controlling physical access to a controlled space by one or more users, the method including: actuating, by a controller a physical locking mechanism in response to one or more control signals; receiving, by a biometric receiver, a biometric data set obtained from a user of the one or

more users; transmitting, by the biometric receiver a data representation derived from at least the biometric data set to a sentry component; and performing, by the sentry component, a matching challenge to determine whether the data representation matches a corresponding authorized user; and responsive to a positive determination of a match, communicating, by the sentry component, the one or more control signals to the physical locking mechanism to actuate an unlocking by the physical locking mechanism, thereby provisioning physical access to the controlled space.

[0051] In accordance with another aspect, there is provided a computer-readable medium storing machine-readable instructions, which when executed by a processor, cause the processor to perform method for controlling physical access to a controlled space by one or more users, the method comprising: actuating, by a controller a physical locking mechanism in response to one or more control signals; receiving, by a biometric receiver, a biometric data set obtained from a user of the one or more users; transmitting, by the biometric receiver a data representation derived from at least the biometric data set to a sentry component; and performing, by the sentry component, a matching challenge to determine whether the data representation matches a corresponding authorized user; and responsive to a positive determination of a match, communicating, by the sentry component, the one or more control signals to the physical locking mechanism to actuate an unlocking by the physical locking mechanism, thereby provisioning physical access to the controlled space.

[0052] In accordance with another aspect, a process to generate authorized users for the matching challenge includes at least generation of one or more user profiles corresponding to each of the authorized users in an access control system, which are then synchronized to the sentry computer server which is configured to associate one or more biometric profiles to each of the user profiles that are utilized for conducting the matching challenges.

[0053] In various further aspects, the disclosure provides corresponding systems and devices, and logic structures such as machine-executable coded instruction sets for implementing such systems, devices, and methods.

[0054] In this respect, before explaining at least one embodiment in detail, it is to be understood that the embodiments are not limited in application to the details of construction

and to the arrangements of the components set forth in the following description or illustrated in the drawings. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

[0055] Many further features and combinations thereof concerning embodiments described herein will appear to those skilled in the art following a reading of the instant disclosure.

DESCRIPTION OF THE FIGURES

[0056] In the figures, embodiments are illustrated by way of example. It is to be expressly understood that the description and figures are only for the purpose of illustration and as an aid to understanding.

[0057] Embodiments will now be described, by way of example only, with reference to the attached figures, wherein in the figures:

[0058] **FIG. 1** is a drawing of a locking mechanism that can be actuated to secure a cabinet, according to some embodiments.

[0059] **FIG. 2** is an exploded side perspective view of a locking mechanism, showing a rotation limiter, and a pawl, according to some embodiments.

[0060] **FIG. 3** is an illustration of an enclosure having a locking mechanism of **FIG. 2** coupled to it to provide secure access control to a front panel, according to some embodiments.

[0061] **FIG. 4** is an illustration of an embodiment wherein a communication cable connects the locking mechanism to an intermediary sentry component, which may be used to coordinate and/or record access attempts, successes, among others, to a centralized backend management device or processors.

[0062] **FIG. 5** is an illustration of an example panel, relay, and power supply, according to some embodiments.

[0063] **FIG. 6** is a circuit diagram showing an example embodiment where the interface panel is connected to a reader / door contact, and coordinated access control is provisioned through the panel such that the lock can only be released on the server rack where not only the user has to successfully pass a biometric challenge, but also ensure that the user checked in the user's identity at a door, according to some embodiments.

[0064] **FIG. 7** is a perspective view illustrating an example housing and example proximity token, according to some embodiments.

[0065] **FIG. 8** is an example drawing of a general replication workflow, that may be utilized for large scale deployments, according to some embodiments.

[0066] **FIG. 9** is an example drawing of the communication architecture for our platform to provide device-agnostic access control mechanisms, according to some embodiments.

[0067] **FIG. 10** is a schematic diagram of computing device, exemplary of an embodiment.

[0068] **FIG. 11** and **FIG. 12** are example screenshots of a centralized access control interface, according to some embodiments.

DETAILED DESCRIPTION

[0069] Embodiments of methods, systems, and apparatus are described through reference to the drawings.

[0070] The following discussion provides many example embodiments of the inventive subject matter. Although each embodiment represents a single combination of inventive elements, the inventive subject matter is considered to include all possible combinations of the disclosed elements. Thus if one embodiment comprises elements A, B, and C, and a second embodiment comprises elements B and D, then the inventive subject matter is also considered to include other remaining combinations of A, B, C, or D, even if not explicitly disclosed.

[0071] Physical and cybersecurity are increasingly prevalent issues as organizations become more dependent on computing systems for both data storage and data processing.

Data center facilities are utilized to store and house computing equipment, which may include, for example, processors, monitors, servers, network attached storage, routers, etc., which may be essential for the operation of an organization. Other equipment may be stored, such as audio and scientific lab equipment. Computing devices may be stored on various rails, etc., and may be interconnected with one another or external devices via wires, wireless communication, etc.

[0072] These may be grouped or stored in physical containment, storage, or housing mechanisms, such as server cabinets, server cages, rack enclosures, enclosures, safes, etc. For the purposes of this description, physical containment mechanisms will be referred to as computing system racks, and it should be understood that this term should not be limited to physical cabinets, but is a broad term encompassing various types of enclosures, containers, shelves, etc., where physical securement is possible. The computing system cabinets may have various panels, such as a front access panel, and a back access panel. One or more computing systems may be centrally managed or in communication with a physical input / output interface, such as a KVM (keyboard, video, mouse) switch or other control mechanisms.

[0073] The securement system may be deployed into new or existing installations. A data center facility may have one or more of computing system racks, and they may be, for example, provided in various standardized sizes, mounted or otherwise secured / fastened to locations within the data center. For example, a type of rack may be a 19 inch rack enclosure, and may be stored in a rack cabinet. Locking mechanisms of some embodiments described can be retrofit onto existing installations or housings, and communication wiring or wireless protocols may be utilized to provide secure communication pathways of identity challenge information / data sets.

[0074] Data center facilities may include server rooms, testing environments, production server environments, data storage facilities (e.g., disaster recovery, failover, redundant sites), among others. Organizations using or having data center facilities may include, among others, internet service providers, networking services providers, computing companies, military / emergency service organizations, financial institutions.

[0075] Accordingly, data center facilities are often considered highly sensitive, and various deterrent and protective measures are provided to prevent unauthorized access. A breach of physical access security could lead to significant losses of functionality and/or economic losses. A data center facility may have different tiers and levels of security (e.g., some areas may have a higher level of security than others, or may require membership in a particular access group). A data center may also have facilities that are disparately located from one another, or has servers / server racks located in different rooms or locations, and in some embodiments, there may be more than one data center in a geographical area.

[0076] The data center may also have shared use between different clients / customers (e.g., a shared computing service facility), and different computing device may service or otherwise store the data of different organizations. Accordingly, access may need to be provisioned based on access credentials pertaining to an organization that is being serviced by the computing devices secured behind a physical access prevention mechanism. Access may require monitoring and tracking such that access provisioning can be audited, monitored, reviewed, etc., and unauthorized attempts may cause alerts or alarms to be generated. In some embodiments, access to computing system cabinets may be provisioned to different individuals, such as system administrators, janitorial staff, equipment installers / manufacturers / repairpersons, among others. An example of a shared use where granular access control is useful is a co-location data center, where customers are beginning to demand additional security protecting their data both physically and digitally. As described below, various embodiments include technical solutions that allow co-location data centers to meet the stringent compliance requirements of their customers. Many colocation facilities provide data center space for customers of various industries. Depending on the data that is stored in the physical location, various governing bodies (PCI, HIPAA, AICPA SOC, or other) enforce that any entity handling or storing data must adhere to specific asset documentation, configuration and change management, as well as transparent documentation and physical access security policies.

[0077] Granular control may include time-based control, user identity based control, coordinated access control (e.g., if the user did not check in at the door, they should not be allowed to unlock the server cabinet), etc. For example, in a co-location environment the

securement devices add an extra layer of assurance to the customers who can guarantee and monitor when authorized personnel are accessing their designated cabinets at the desired times. The securement device can also be used as a value-added tool for co-location data centers to increase revenue from their customers.

[0078] **FIG. 1** is a drawing of a locking mechanism **100** that can be actuated to secure a cabinet, according to some embodiments. The locking mechanism **100** of **FIG. 1** may include a latch, pawl or other flange **106**, which operates to secure the cabinet / door / panel such that it cannot be opened without actuating the lock (e.g., by allowing for the rotation along an axis). The flange **106** can be coupled to a rotating barrel **102** by way of an engaging mechanism **104**. Other types of locking mechanisms are possible, including, for example, magnetic locks (e.g., where an electromagnetic force is electrically activated or deactivated in a solenoid), electronic locks, other types of mechanical locks, bolts, pin-tumblers, among others. In some embodiments, the locking mechanism receives an authentication tool, such as a physical key, which allows for the turning of the lock.

[0079] The locking mechanism is coupled to an actuation mechanism which is electronically controlled through received electrical signals. The signals represent commands that cause the activation, toggling, locking, unlocking, of the physical access control mechanism. The signals can, in some embodiments, specially formed signal packets having a specific format or protocol prior to the actual activation of the access control mechanism.

[0080] In some embodiments, the locking mechanism is a specific pawl or magnetic connector whose status is toggled by way of activation of a solenoid. The locking status of the locking mechanism is tracked (or sensed) in some embodiments, which is then utilized for modifying one or more downstream device statuses, or to log in / log out automatically various user accounts and/or profiles on accounts on devices residing within the enclosure housing.

[0081] **FIG. 2** is a view of a locking mechanism and securing mechanism, showing a rotation limiter, and a pawl, according to some embodiments. In this example, a proximity card **204** or biometric reader **202** is combined with the locking mechanism of **FIG. 1**, to

provide an additional level of security. In this example, the device provides dual-factor authentication for data center cabinets through biometric reader **202** and proximity reader **204**. Other authentication combinations and approaches are contemplated (e.g., just one of a biometric reader **202** or a proximity reader **204**).

[0082] The locking mechanism and securing mechanism is part of a networked securement device that includes a controller circuit configured to actuate a physical locking mechanism in response control signals from an access control panel **208**. The physical locking mechanism is coupled to a biometric receiver **202** configured for receiving a biometric data set obtained from a user of the one or more users and transmitting a representation of the biometric data set and/or other authentication information to an interface, such as a communications splitter circuit, which manages separated communication channels **210** and **212**, which in some preferred embodiments, are electrically separated communication links (e.g., having hardware components that reduce the presence of cross-talk effects). The communication links are wired linkages in a preferred embodiment, but wireless linkages are also contemplated in other embodiments. Communication channel **210** connects to sentry server / control circuit **206**.

[0083] The communication channels **210** and **212** in some embodiments utilize differing encryption protocols and have different reliability and throughput characteristics. The communication channel **212**, in some embodiments, has a higher level of security relative to the communication channel **210**, and is a purely dedicated channel utilized specifically utilized for the transmission of access control signals. On the other hand, communication channel **210** may also be utilized for heartbeat signals, conducting software / firmware updates, among others. In a specific example, communication channel **210** utilizes 128 bit encryption designed for improved speed of encryption, and communication channel **212** utilizes 4096 bit RSA encryption. Communication channel **210** is comingled with other wiring (e.g., Ethernet cables and other twisted pair wiring from the rack server) and communication channel **212** is a fully separated wire that is specially insulated to reduce crosstalk leakage using improved shielding mechanisms, including conductive films, shielding gaskets, and ferrite blockers. Communication channel **212** is specifically physically separated and utilizes a different wiring pathway from communication channel **210**.

[0084] **FIG. 3** is an illustration of an enclosure **300** having a locking mechanism of **FIG. 2** coupled to provide secure access control to a front panel, according to some embodiments. The biometric reader, for example, may be configured to receive as inputs data sets of fingerprints, retinal scans, olfactory cues, among others. These data sets may then be transformed into representative data values (e.g., to prevent the transmission of the actual fingerprint data, increasing security / reducing the likelihood of identity theft, and allowing for compressed values of data to be provided). In some embodiments, the representative data values include vectors or other data structures storing a subset or a transformed subset of values in accordance with one or more protocols, and may be standardized or otherwise transformed for compliance or interoperability.

[0085] In an example for fingerprint data, patterns may include identifications of locations of bifurcations, arches, loops, whorls, minutiae features, and/or transforms or reflections of the same. These are stored in the form of biometric templates (e.g., collections of extracted features), and these values may be further compressed or transformed using, for example, hash functions, etc.

[0086] A challenge with simple locking mechanisms that do not authenticate or otherwise verify identity of a user is that it becomes difficult to troubleshoot, identify patterns of unauthorized access, or generate audit records. Accordingly, an example improved system **400** is illustrated in **FIG. 4**, wherein a communication cable connects the locking mechanism to an intermediary sentry component **206**, which may be used to coordinate and/or record access attempts, successes, among others, to a centralized backend management device or processors.

[0087] The intermediary sentry component **206** is configured to configured for performing (e.g., transmitting control signals indicative of a request and passing parameters) a matching challenge (e.g., comparison, validation) to determine whether the data representation matches a corresponding authorized user. In some embodiments, the intermediary sentry component **206** includes cache memory storage of most likely used or recent biometric templates for verification, and in other embodiments, the intermediary sentry component **206** includes networking interface components for networked communication with a backend mechanism for conducting identity challenges.

[0088] Verification can either be against a specific, known user (e.g., a proximity card is also utilized that has a user identity, and the verification is conducted by transmitting the representation data set to be matched against the specific, known user), or in some cases, a matching process may be utilized whereby the representation data set is performed as a challenge against all known authorized users (e.g., so that the sentry component would not need the identity of the user).

[0089] Where there is a positive determination of a match (e.g., by way of a raised interrupt signal, corresponding cryptographic response code), the sentry component **206** is configured to communicate data sets representing identity back to the access control panel **208**, in some embodiments. In other embodiments, the sentry component **206** provides the data sets to a three way splitter **502** which then re-routes the signal from the sentry component **206** to the access control panel **208**. It is only the access control panel **208** which can send control signals to the physical locking mechanism that are adapted to actuate an unlocking of the physical locking mechanism, thereby provisioning physical access to the controlled space (e.g., the user is now able to open the panel and access the server).

[0090] The intermediary sentry component **206** may coordinate the activity of a single physical locking mechanism, or multiple physical locking mechanisms. For example, there may be first electronic, networked securement device securing a front access panel of a computing component rack, and the second electronic, networked securement device securing a rear access panel of a computing component rack, both controlled by the same intermediary sentry component. Similarly, there may be a single access control panel **208** that controls access to various secured spaces and is coupled to a plurality of physical locking mechanisms. In a preferred embodiment, each server cabinet has a dedicated access control panel **208**, but connects to a shared sentry component **206**. Heartbeat signals are routed through communication channel **210** to reserve the high security communication channel **212** for dedicated communications with access control panel **208**.

[0091] An example panel, relay, and power supply are shown in **FIG. 5**, according to some embodiments. The intermediary sentry component may also be configured for

connecting to an access interface (e.g., an interface panel), where other challenges may occur, or access control can be centrally provisioned.

[0092] For example, there may be a central interface panel in the center of a data center that provides access to specific data center rack panels based on a centralized challenge mechanism (e.g., a retinal scanner panel where a user indicates which server rack panel the user would like to have access to).

[0093] A communications splitter circuit **502** is electronically coupled to the locking mechanism housing to split communication pathways. The communications splitter circuit **502**, in some embodiments, is a physical communications mechanism that bifurcates communications paths. In some embodiments, communications splitter circuit **502** is a RJ45 splitter. In other embodiments, communications splitter circuit **502** is a router or network switch configured to mediate communication traffic.

[0094] In other embodiments, two separate communication links (e.g., wires) are used rather than the communications splitter circuit **502**. In some embodiments, the communications splitter circuit **502** includes communications routing circuitry that enables the locking mechanism housing to communicate across different, independent pathways (e.g., channels) to a profile identification subsystem device **206** and to an access control panel device **208**.

[0095] The segregated, independent pathways are useful in reducing vulnerability of the overall system, as the access control panel device is only communicated with after a successful identification of the identity of the profile of the user attempting to provide credentials at the locking mechanism's biometric or token reader. The access control panel **208** includes logic circuits that provide a final determination as to whether access should be provisioned by activating and/or toggling the locking mechanism.

[0096] The communications splitter circuit **502** is configured to receive the biometric data set from the locking mechanism or the reader, and the communications splitter circuit **502** includes both the first electronic communication interface and the second electronic communication interface. These can be provided, for example, by a suitably configured

network card or circuit, among others. For example, the first electronic communication interface can be an output wire or connection.

[0097] The first electronic communication interface is adapted to provide a first communication channel between the communications splitter circuit **502** and a sentry computer server **206**. The sentry computer server may include devices provided by BioConnect™, including profile tracking and identification systems that utilize one or more biometrics to establish the identity through, for example, either a match (1:n, if the identity is not known *a priori*) or a verification (1:1, if the identity is provided alongside the credentials). 1:n is slower than 1:1, and is less secure. The sentry computer may also be configured to only provide a positive identification where the user has satisfied other access conditions, such as checking in at the front door of the building, etc.

[0098] The second electronic communication interface is adapted to provide a second communication channel **212** between the communications splitter circuit and an access control device. The second communication channel **212**, in some embodiments, utilizes a different security protocol than the first communication channel so that the ability to maliciously access the channel may be reduced. Similarly, in preferred embodiments, the second communication channel **212** utilizes a higher level of security than the first communication channel **210**, and may be configured to detect tampering through a continuously changing protocol (e.g., time-based). The first communication channel **210** and the second communication channel **212** are physically independent of one another, and in some embodiments, are electrically separated relative to one another (e.g., insulated from one another to avoid cross-talk effects).

[0099] The communications splitter circuit **502** transmits the representation of the biometric data set to the sentry computer server **206** across the first communication channel **210**, the sentry computer server **206** configured for (i) performing a matching challenge to determine whether the representation of the biometric data set matches a corresponding authorized user, and (ii) responsive to a positive determination of a match, generating and transmitting a data set representative of an identity profile corresponding to the user to the communications splitter circuit across the first communication channel **210**.

[00100] A process to generate authorized users for the matching challenge includes at least generation of one or more user profiles corresponding to each of the authorized users in an access control system, which are then synchronized to the sentry computer server **206**, the sentry computer server **206** configured to associate one or more biometric profiles to each of the user profiles that are utilized for conducting the matching challenges.

[00101] The data set representative of the identity profile being provided by the sentry computer server **206**, in a preferred embodiment, the data set representative of the identity profile is encrypted using rolling or time-based encryption mechanisms such that a malicious user cloning or otherwise using an older intercepted identity profile data set is unable to falsify an identity. For example, the data set representing Alice may utilize one or more shared encryption mechanisms using a shared secret key that is known between the sentry computer server **206** and the access control panel **208** (e.g., stored in data repositories at both and shared earlier, but unknown to the panel reader at the biometric or other authentication data set receiver).

[00102] The shared key can, for example, include seed aspects based on timestamps (e.g., Unixtime + salt + seed) that can be utilized to modify a specific encryption mechanism such that earlier encryptions that are out of sync cannot be utilized for future authentications without knowledge of the shared key. The shared key can be utilized to validate (e.g., check signatures) and/or otherwise decrypt the data set. The data storage repositories storing the shared keys, in some embodiments, are secure processors with enhanced levels of security. In some embodiments, clocks are synchronized between the sentry computer server **206** and the access control panel **208** for generation and usage of the shared secret key. For example, a shared cryptographic hash function can be used to generate one-time passwords that are used for generating the data sets.

[00103] Responsive to the receipt of the data set representative of the identity profile across the first communication channel **210**, the communications splitter circuit **502** or the controller circuit is further configured to transmit the data set representative of the identity profile to an access control device across the second communication channel.

[00104] The access control device, upon determining that the identity profile matches an authorized user of a set of authorized users, is configured to transmit the one or more control signals to the controller circuit across the second communication channel **212** and the communications splitter circuit **502** to cause the actuating of the physical locking mechanism.

[00105] The biometric receiver can be configured to generate one or more periodic electronic heartbeat signals periodically transmitted to the sentry computer server across the first communication channel.

[00106] For example, these heartbeat signals are utilized to indicate the operational status of the biometric receiver. The biometric receiver can be configured to stagger the one or more periodic electronic heartbeat signals periodically transmitted to the sentry computer server across the first communication channel relative to one or more periodic electronic heartbeat signals from other biometric receivers.

[00107] Optionally, the one or more preceding verification mechanisms includes an interlocking door controller configured to enable only a single user to validate and pass through at each operation of the interlocking door controller, for example, at a mantrap or other type of revolving entry / airlock mechanism.

[00108] For example, some data centers include additional data center access control mechanisms, including laser trip beams not visible to the human eye, among others. Accordingly, from a data structure perspective, the sentry computer server can track a chain of activity (e.g., a set of flags) that all must be satisfied prior to generating a response indicating the profile of the user.

[00109] The controlled space within the housing includes one or more access-controlled computing devices having one or more user accounts residing on memory stored thereon; the one or more access-controlled computing devices are electronically coupled to the communications splitter circuit or the controller circuit; and the one or more access-controlled computing devices are configured only to allow access to one or more user accounts corresponding to the identity profile.

[00110] Optionally, the controller circuit is configured to track an open or close status of the physical locking mechanism; and wherein the one or more access-controlled computing devices are configured only to allow access to the one or more user accounts during a duration that the physical locking mechanism is in the open status.

[00111] The controller circuit is configured to track an open or closed status of the physical locking mechanism; and wherein the one or more access-controlled computing devices are configured to revoke access to the one or more user accounts during a duration that the physical locking mechanism is in the closed status. The one or more access-controlled computing devices, in some embodiments, is configured to revoke access to all user accounts responsive to a determination that the physical locking mechanism is in the closed status.

[00112] In an alternate embodiment, the one or more access-controlled computing devices is configured to automatically authenticate the user on a backend electronic directory service, enabling access the to one or more user accounts during a duration that the physical locking mechanism is in an open status.

[00113] In another aspect, the communications splitter circuit is configured to monitor network connection statuses corresponding to each of the first communication channel and the second communication channel; the controller circuit includes on-board non-transitory computer memory storing one or more biometric profiles; and the controller circuit is configured to, responsive to a determination by the communications splitter circuit that the first communication channel is inactive, perform the matching challenge against the stored one or more biometric profiles, and transmit the data set representative of the identity profile across the first communication channel to the access control device.

[00114] In a non-limiting example, a penetration tester, George, provides credentials through the use of a combined proximity card and a fingerprint reading. George is posing as a system administrator who is attempting to enter so that he can perform a routine upgrade of an image of a virtual machine hosted on a rack server housed within the cabinet.

[00115] George provides data sets using his proximity card and the fingerprint reading. The proximity card is a 13.56 MHz contactless smart card having inductive elements for resonant signal transfer and a read range of approximately 5 inches. The proximity card uses the Weigand protocol to send the signal. A rolling cryptographic algorithm is used in relation to the proximity card. George's fingerprints are provided as a data structure representing a set of fingerprint features, including location and distances between whorls, loops, arches, ridges, valleys, among others (or a hashed representation thereof).

[00116] In an alternate approach where there is simply a reader and an authentication mechanism comparing against on-board memory, the device would be susceptible to various types of attacks, including brute-force dictionary-type attacks, malicious access of onboard memory (e.g., a hacker attaching a cable to the pins of the on-board circuitry), and the access control panel backend could be vulnerable to attack as signals may be directly sent from the reader to the access control panel. Accordingly, the access control panel itself could be damaged through the sending of a deluge of data to overcome its circuitry and interfaces. The access control panel, upon being damaged, may revert to a default setting where on-board memory or cached information utilized. At that point, George is able to make his proximity card or biometric results match one of the cached results and access the server cabinet and steal the hard drives.

[00117] However, in the system of **FIG. 5**, George's data sets would be first received by the splitter **502**, which acts as a routing mechanism that is configured to mediate electronic communication traffic between communication channels **210** and **212**. The lower security communication channel **210** is utilized to transmit the signals, which are only routed to sentry server / control circuit **206**. At this point, there are no signals sent across **212** to access control panel **208**. The sentry server / control circuit **206** performs the first adjudication of the authentication signals, and in some embodiments, the sentry server / control circuit **206** connects to an enterprise level cybersecurity backend that continually updates user profiles and their associated match scores (e.g., how confident the system is that a user is who the user purports to be given the access credentials provided and the trustworthiness of the network linkage, in view of patterns and trends of authentication, or global trends of breached technologies).

[00118] The sentry server / control circuit **206** is configured to generate a first determination that is utilized to establish the identity that George is purporting to be only if George's data sets are able to achieve a sufficiently high match score on the sentry server / control circuit **206**. In this example, as George is a penetration tester, the sentry server / control circuit **206** may have detected a level of tampering or unusual access aspects in relation to George's access request (e.g., atypical hour of access that does not match a sysadmin maintenance schedule, the person who George is impersonating has a GPS location on a mobile device that is not located within the building). Accordingly, the sentry server / control circuit **206** does not transmit a signal indicative of the authenticated user profile, and George cannot gain entry into the server rack cabinet. It is important to note that in this instance, there is no signal sent to the access control panel **208** and accordingly, the access control panel **208** is segregated from tampering and malicious use.

[00119] In another instance, if Bob, the actual system administrator, seeks to gain access, the data sets are first adjudicated at splitter mechanism **502** which routes the signal across first communication channel **210**. The sentry server / control circuit **206** receives the data sets, generates a match score for Bob, and if Bob's data sets yield a sufficiently high match score, an authentication signal is sent from sentry server / control circuit **206** to splitter mechanism **502** over communication channel **210**. The profile data structure is then sent to the access control panel **208** across high security communication channel **212**, which includes improved shielding and insulation components that reduce the potential for cross-talk leakage snooping. The profile data structure can include additional security encoding, such as time-based rolling encryption salting, among others.

[00120] The access control panel **208**, upon conducting a comparison against profiles which should be given access at a particular set of times, then sends a control signal back across high security communication channel **212** that actuates the physical lock (e.g., mechanical or magnetic lock) on the cabinet. In various other embodiments described herein, the locking status or toggling thereof can also be utilized as a signal to provision or revoke access to user accounts of the devices (e.g., in conjunction with a backend active directory system). For example, when Bob locks the cabinet after usage, all accounts on the devices in the cabinet can be automatically logged out.

[00121] In another embodiment, the sentry server / control circuit **206** instead directly connects to the access control panel **208** over a high security communication channel bypassing communication channel **210** entirely.

[00122] A further improvement of the system as described in some embodiments is an ability to interoperate with readers and devices of different vendors, as long as they are able send the data sets to the sentry server / control circuit **206** as opposed to using the data sets for local authentication directly. A heterogeneous set of devices can thus be utilized, reducing operational friction. A sufficient audit trail is generated through the profiles identified on sentry server / control circuit **206**, and recorded entry / exit logs, which can be used to assess overall security metrics.

[00123] **FIG. 6** is a circuit diagram showing an example embodiment where the interface panel is connected to a reader / door contact, and coordinated access control is provisioned through the panel such that the lock can only be released on the server rack where not only the user has to successfully pass a biometric challenge, but also ensure that the user checked in the user's identity at a door.

[00124] In some embodiments, a single networking cable from the locking mechanism housing is provided that is split into two signal carriers, one signal carrier for connecting to an interface panel, and another signal carrier for connecting to the sentry component. An example wiring standard for communications may be a Wiegand interface™.

[00125] Different lighting mechanisms can be used to indicate access, such as if access is permitted, a LED is controlled to switch to illuminate a green colour, and the user can unlock the cabinet lock. If access is not granted, a LED may be controlled to emit red and user cannot open the cabinet door. Devices may be configured for operation using Standard ISO 19794-2 templates, for example.

[00126] Physical access control mechanisms may utilize physical security devices, or a combination of physical security devices (e.g., locks, mechanical or electronic fastening devices, magnetic devices) that may be released, activated, deactivated, etc., upon triggering. Physical access control mechanisms, in some embodiments, are triggered in

relation to received control signals, which, for example, on receiving an affirmative response to a challenge, such as a biometric challenge (e.g., facial, fingerprint, olfactory, gait, retinal). In some embodiments, combinations of different types of physical access control mechanisms are utilized (e.g., requiring both a key / proximity card, and an authorized biometric identity that is able to pass a biometric challenge). Access may be tracked via timestamped or otherwise encoded response messages, allowing for post-access review of access attempts, refusals, and grants.

[00127] These physical access control mechanisms may be operated in communication or in concert with one or more backend control systems, which may include facility access control systems (e.g., door lock tracking, scheduling, and/or other related computing systems). These facility access control systems may include communication or coupling to one or more user identification management systems, which may, for example, provide a directory service that maintains one or more data sets on users for authentication, verification, and authorization of users in relation to specific resources (e.g., access to a specific computer or rack) or facility access points (e.g., doors, turnstiles, panels, windows). The facility access control systems may include the provisioning, maintenance, and setup of electronic access credentials, such as proximity cards, time-encoded tokens, etc.

[00128] **FIG. 7** is a perspective view illustrating an example housing and example proximity token, according to some embodiments. A biometric reader may be provided, along with a proximity reader and latch mechanism, and these may all be stored together in a electronically coupled, networked, housing. As shown in **FIG. 7**, the housing may be attached or otherwise securely fastened to a rack, and wiring connections / wireless connections may be used for communications.

[00129] In a further embodiment, a proximity token (e.g., a proximity card, a smartphone) may include one or more data stored thereon, which may include local storage for biometric templates and/or representations thereof. The locally stored token may be associated with a user of associated with identity credentials that may also be stored on the locally stored token (or otherwise provided using another verification mechanism). The local storage for biometric templates and/or representations thereof may, in some embodiments, be provided to reduce an overall computing burden on a system.

[00130] Local storage and comparison provides speed and verification advantages. For example, data centers may need to have scalable high-security systems for large number of users, and a first local storage matching challenge may help ease the networking burden of transmitting biometric and/or other challenge data across networks, especially where the network infrastructure is required to handle large volumes of traffic (e.g., other information is being transmitted, system "heartbeats" may utilize a significant amount of bandwidth), etc. A challenge mechanism may be configured, for example, to first validate against the locally stored representation, and then validate against a backend matching engine if no match is found. In some embodiments, the locally stored templates or representations may be associated with an enrollment quality value. When the user uses a biometric identity aspect to perform matching / a challenge, in some embodiments, a new template may be received from the biometric sensor and compared against the existing locally stored templates or representations.

[00131] During Applicants' development of testing models, Applicants' encountered problems due to non-standardization of biometric templates, where several different template types could be utilized. While there are some standardization approaches to specific types of templates, a significant hurdle is the requirement to obtain new re-enrollments. The process of enrolling user templates during the implementation of a biometric system can be burdensome. For organizations with hundreds of thousands of users, the enrollment process alone can take weeks, if not months to complete. Time consuming re-enrollments have therefore caused a large number of consumers to remain on legacy technology in order to avoid the burden of a re-enrollment process. Accordingly, some embodiments of the system provide for improved re-enrollment processes that are invisible to users as new, high quality enrollments can be obtained over time through the use of the existing readers installed in the securement housings. Re-enrollments, for example, may be directed to different types of templates, including proprietary technologies, standard templates, etc.

[00132] **FIG. 8** is an example drawing of a general replication workflow, that may be utilized for large scale deployments, according to some embodiments. The facility access control systems may be configured for combining door-to-cabinet solutions that manage identity

across a full enterprise deployment. A single-system solution provides an improvement that coordinates multiple software solutions managing the access to the perimeter as well as to all of the cabinets.

[00133] The devices, through networked sentry components, may be configured to interoperate with a wider network of devices that can control other cabinets and physical access points across an enterprise architecture. A datacenter may thus be secured across a unified system from door down to the cabinet.

[00134] **FIG. 9** is an example drawing of the communication architecture for our platform to provide device-agnostic access control mechanisms, according to some embodiments.

[00135] The embodiments of the devices, systems and methods described herein may be implemented in a combination of both hardware and software. These embodiments may be implemented on programmable computers, each computer including at least one processor, a data storage system (including volatile memory or non-volatile memory or other data storage elements or a combination thereof), and at least one communication interface.

[00136] **FIG. 10** is a schematic diagram of computing device **1000**, exemplary of an embodiment. As depicted, computing device includes at least one processor **1002**, memory **1004**, at least one I/O interface **1006**, and at least one network interface **1008**.

[00137] Each processor **1002** may be, for example, microprocessors or microcontrollers, a digital signal processing (DSP) processor, an integrated circuit, a field programmable gate array (FPGA), a reconfigurable processor, a programmable read-only memory (PROM), or combinations thereof. Processors are be used to implement the various logical and computing units of the system, as shown in **FIG. 1**, for example, and different units may have different processors, or may be implemented using the same set of processors or the same processor.

[00138] Memory **1004** may include a suitable combination of computer memory that is located either internally or externally such as, for example, random-access memory (RAM), read-only memory (ROM), compact disc read-only memory (CDROM), electro-optical memory, magneto-optical memory, erasable programmable read-only memory (EPROM),

and electrically-erasable programmable read-only memory (EEPROM), Ferroelectric RAM (FRAM). Memory **1004** may be used to store verification information, hashes thereof, among others.

[00139] Each I/O interface **1006** enables computing device **1000** to interconnect with one or more input devices, such as a keyboard, mouse, camera, touch screen and a microphone, or with one or more output devices such as a display screen and a speaker. I/O interfaces **1006** can include command line interfaces. These I/O interfaces **1006** can be utilized to interact with the system, for example, to provide inputs, conduct inquiries, respond to identity challenges, etc.

[00140] Each network interface **1008** enables computing device **1000** to communicate with other components, to exchange data with other components, to access and connect to network resources, to serve applications, and perform other computing applications by connecting to a network (or multiple networks) capable of carrying data including the Internet, Ethernet, plain old telephone service (POTS) line, public switch telephone network (PSTN), integrated services digital network (ISDN), digital subscriber line (DSL), coaxial cable, fiber optics, satellite, mobile, wireless (e.g. Wi-Fi, WiMAX), SS7 signaling network, fixed line, local area network, wide area network, and others, including combinations of these. Network interfaces **1008** are utilized, for example, to interact with various applications, receive inputs from biometric applications, external tracking systems, etc.

[00141] **FIG. 11** and **FIG. 12** are example screenshots of a centralized access control interface, according to some embodiments.

[00142] Program code is applied to input data to perform the functions described herein and to generate output information. The output information is applied to one or more output devices. In some embodiments, the communication interface may be a network communication interface. In embodiments in which elements may be combined, the communication interface may be a software communication interface, such as those for inter-process communication. In still other embodiments, there may be a combination of communication interfaces implemented as hardware, software, and combination thereof.

[00143] Throughout the foregoing discussion, numerous references will be made regarding servers, services, interfaces, portals, platforms, or other systems formed from computing devices. It should be appreciated that the use of such terms is deemed to represent one or more computing devices having at least one processor configured to execute software instructions stored on a computer readable tangible, non-transitory medium. For example, a server can include one or more computers operating as a web server, database server, or other type of computer server in a manner to fulfill described roles, responsibilities, or functions.

[00144] The term “connected” or "coupled to" may include both direct coupling (in which two elements that are coupled to each other contact each other) and indirect coupling (in which at least one additional element is located between the two elements).

[00145] The technical solution of embodiments may be in the form of a software product. The software product may be stored in a non-volatile or non-transitory storage medium, which can be a compact disk read-only memory (CD-ROM), a USB flash disk, or a removable hard disk. The software product includes a number of instructions that enable a computer device (personal computer, server, or network device) to execute the methods provided by the embodiments.

[00146] The embodiments described herein are implemented by physical computer hardware, including computing devices, servers, receivers, transmitters, processors, memory, displays, and networks. The embodiments described herein provide useful physical machines and particularly configured computer hardware arrangements. The embodiments described herein are directed to electronic machines and methods implemented by electronic machines adapted for processing and transforming electromagnetic signals which represent various types of information. The embodiments described herein pervasively and integrally relate to machines, and their uses; and the embodiments described herein have no meaning or practical applicability outside their use with computer hardware, machines, and various hardware components. Substituting the physical hardware particularly configured to implement various acts for non-physical hardware, using mental steps for example, may substantially affect the way the embodiments work. Such computer hardware limitations are clearly essential elements of the embodiments described herein, and they cannot be omitted

or substituted for mental means without having a material effect on the operation and structure of the embodiments described herein. The computer hardware is essential to implement the various embodiments described herein and is not merely used to perform steps expeditiously and in an efficient manner.

[00147] Although the embodiments have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein.

[00148] Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed, that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized.

[00149] As can be understood, the examples described above and illustrated are intended to be exemplary only.

WHAT IS CLAIMED IS:

1. A securement system for controlling physical access to a controlled space by one or more users, the system comprising:

a controller circuit configured to generate signals to control actuation of a physical locking mechanism, the physical locking mechanism coupled to a biometric receiver configured for receiving a biometric data set obtained from a user of the one or more users and transmitting a representation of the biometric data set to a communications splitter circuit;

the communications splitter circuit configured to receive the biometric data set, the communications splitter circuit including a first electronic communication interface and a second electronic communication interface, the first electronic communication interface adapted for communication over a first communication channel between the communications splitter circuit and a sentry computer server, the second electronic communication interface adapted for communication over a second communication channel between the communications splitter circuit and an access control device;

the communications splitter circuit configured to transmit the representation of the biometric data set to the sentry computer server across the first communication channel, the sentry computer server configured for (i) performing a matching challenge to determine whether the representation of the biometric data set matches a corresponding authorized user, and (ii) responsive to a positive determination of a match, generating and transmitting a data set representative of an identity profile corresponding to the user to the communications splitter circuit across the first communication channel;

wherein responsive to the receipt of the data set representative of the identity profile across the first communication channel, the communications splitter circuit or the controller circuit is further configured to transmit the data set representative of the identity profile to an access control device across the second communication channel,

wherein the access control device, upon determining that the identity profile matches an authorized user of a set of authorized users, is configured to transmit one or more control signals to the controller circuit across the second communication channel and the communications splitter circuit to cause the actuating of the physical locking mechanism.

2. The securement system of claim 1, wherein the biometric receiver is configured to generate one or more periodic electronic heartbeat signals periodically transmitted to the sentry computer server across the first communication channel.

3. The securement system of claim 2, wherein the biometric receiver is configured to stagger the one or more periodic electronic heartbeat signals periodically transmitted to the sentry computer server across the first communication channel relative to one or more periodic electronic heartbeat signals from other biometric receivers.

4. The securement system of claim 1, wherein the matching challenge performed by the sentry computer server includes a verification of whether the user has successfully verified at one or more preceding verification mechanisms.

5. The securement system of claim 4, wherein the one or more preceding verification mechanisms includes an interlocking door controller configured to enable only a single user to validate and pass through at each operation of the interlocking door controller.

6. The securement system of claim 1, wherein the controlled space includes one or more access-controlled computing devices having one or more user accounts residing on memory stored thereon;

wherein the one or more access-controlled computing devices are electronically coupled to the communications splitter circuit or the controller circuit; and

wherein the one or more access-controlled computing devices are configured only to allow access to one or more user accounts corresponding to the identity profile.

7. The securement system of claim 6, wherein the controller circuit is configured to track an open or close status of the physical locking mechanism; and wherein the one

or more access-controlled computing devices are configured only to allow access to the one or more user accounts during a duration that the physical locking mechanism is in the open status.

8. The securement system of claim 6, wherein the controller circuit is configured to track an open or closed status of the physical locking mechanism; and wherein the one or more access-controlled computing devices are configured to revoke access to the one or more user accounts during a duration that the physical locking mechanism is in the closed status.

9. The securement system of claim 6, wherein the controller circuit is configured to track an open or closed status of the physical locking mechanism; and wherein the one or more access-controlled computing devices are configured to revoke access to all user accounts responsive to a determination that the physical locking mechanism is in the closed status.

10. The securement system of claim 6, wherein the one or more access-controlled computing devices is configured to automatically authenticate the user on a backend electronic directory service, enabling access the to one or more user accounts during a duration that the physical locking mechanism is in an open status.

11. The securement system of claim 1, wherein the communications splitter circuit is configured to monitor network connection statuses corresponding to each of the first communication channel and the second communication channel;

wherein the controller circuit includes on-board non-transitory computer memory storing one or more biometric profiles;

wherein the controller circuit is configured to, responsive to a determination by the communications splitter circuit that the first communication channel is inactive, perform the matching challenge against the stored one or more biometric profiles, and transmit the data set representative of the identity profile across the first communication channel to the access control device.

12. The securement system of claim 1, wherein the first communication channel and the second communication channel are physically independent of one another.

13. The securement system of claim 1, wherein the first communication channel and the second communication channel are electrically separated relative to one another.

14. The securement system of claim 1, wherein the first communication channel and the second communication channel utilize different encryption protocols.

15. The securement system of claim 1, wherein the first communication channel and the second communication channel utilize different communication protocols.

16. The securement system of claim 1, wherein a process to generate authorized users for the matching challenge includes at least generation of one or more user profiles corresponding to each of the authorized users in an access control system, which are then synchronized to the sentry computer server which is configured to associate one or more biometric profiles to each of the user profiles that are utilized for conducting the matching challenges.

17. The securement system of claim 1, wherein the controlled space is a rack mounted server cabinet.

18. The securement system of claim 1, wherein the sentry computer server is coupled to a plurality of networked securement systems.

19. The securement system of claim 1, wherein the controlled space includes a keyboard, video, and mouse (KVM) station that is coupled to a plurality of computing devices.

20. The securement system of claim 1, wherein the biometric data set is provided by a mobile device.

21. An securement method for controlling physical access to a controlled space by one or more users, the method comprising:

actuating a physical locking mechanism in response to one or more control signals, the physical locking mechanism coupled to a biometric receiver configured for receiving a biometric data set obtained from a user of the one or more users and transmitting a representation of the biometric data set to a communications splitter circuit;

receive, by a communications splitter circuit, the biometric data set, the communications splitter circuit including a first electronic communication interface and a second electronic communication interface, the first electronic communication interface adapted to provide a first communication channel between the communications splitter circuit and a sentry computer server, the second electronic communication interface providing a second communication channel between the communications splitter circuit and an access control device;

transmitting, by the communications splitter circuit, the representation of the biometric data set to the sentry computer server across the first communication channel, the sentry computer server configured for (i) performing a matching challenge to determine whether the representation of the biometric data set matches a corresponding authorized user, and (ii) responsive to a positive determination of a match, generating and transmitting a data set representative of an identity profile corresponding to the user to the communications splitter circuit across the first communication channel;

responsive to the receipt of the data set representative of the identity profile across the first communication channel, transmitting the data set representative of the identity profile to an access control device across the second communication channel,

wherein the access control device, upon determining that the identity profile matches an authorized user of a set of authorized users, transmits the one or more control signals to the controller circuit across the second communication channel and the communications splitter circuit to cause the actuating of the physical locking mechanism.

22. The securement method of claim 21, the method comprising generating one or more periodic electronic heartbeat signals periodically transmitted to the sentry computer server across the first communication channel.

23. The securement method of claim 22, wherein the biometric receiver is configured to stagger the one or more periodic electronic heartbeat signals periodically transmitted to the sentry computer server across the first communication channel relative to one or more periodic electronic heartbeat signals from other biometric receivers.

24. The securement method of claim 21, wherein the matching challenge performed by the sentry computer server includes a verification of whether the user has successfully verified at one or more preceding verification mechanisms.

25. The securement method of claim 24, wherein the one or more preceding verification mechanisms includes an interlocking door controller configured to enable only a single user to validate and pass through at each operation of the interlocking door controller.

26. The securement method of claim 21, wherein the controlled space includes one or more access-controlled computing devices having one or more user accounts residing on memory stored thereon;

wherein the one or more access-controlled computing devices are electronically coupled to the communications splitter circuit or the controller circuit; and

wherein the one or more access-controlled computing devices are configured only to allow access to one or more user accounts corresponding to the identity profile.

27. The securement method of claim 26, wherein the controller circuit is configured to track an open or close status of the physical locking mechanism; and wherein the one or more access-controlled computing devices are configured only to allow access to the one or more user accounts during a duration that the physical locking mechanism is in the open status.

28. The securement method of claim 26, comprising tracking an open or closed status of the physical locking mechanism; and wherein the one or more access-controlled computing devices are configured to revoke access to the one or more user accounts during a duration that the physical locking mechanism is in the closed status.

29. The securement method of claim 26, wherein the controller circuit is configured to track an open or closed status of the physical locking mechanism; and wherein the one or more access-controlled computing devices are configured to revoke access to all user accounts responsive to a determination that the physical locking mechanism is in the closed status.

30. The securement method of claim 26, wherein the one or more access-controlled computing devices is configured to automatically authenticate the user on a backend electronic directory service, enabling access the to one or more user accounts during a duration that the physical locking mechanism is in an open status.

31. The securement method of claim 21, wherein the communications splitter circuit is configured to monitor network connection statuses corresponding to each of the first communication channel and the second communication channel;

wherein the controller circuit includes on-board non-transitory computer memory storing one or more biometric profiles;

wherein the controller circuit is configured to, responsive to a determination by the communications splitter circuit that the first communication channel is inactive, perform the matching challenge against the stored one or more biometric profiles, and transmit the data set representative of the identity profile across the first communication channel to the access control device.

32. The securement method of claim 21, wherein the first communication channel and the second communication channel are physically independent of one another.

33. The securement method of claim 21, wherein the first communication channel and the second communication channel are electrically separated relative to one another.

34. The securement method of claim 21, wherein the first communication channel and the second communication channel utilize different encryption protocols.

35. The securement method of claim 21, wherein the first communication channel and the second communication channel utilize different communication protocols.

36. The securement method of claim 21, wherein a process to generate authorized users for the matching challenge includes at least generation of one or more user profiles corresponding to each of the authorized users in an access control system, which are then synchronized to the sentry computer server which is configured to associate one or more biometric profiles to each of the user profiles that are utilized for conducting the matching challenges.

37. The securement method of claim 21, wherein the controlled space is a rack mounted server cabinet.

38. The securement method of claim 21, wherein the sentry computer server is coupled to a plurality of networked securement devices.

39. The securement method of claim 21, wherein the controlled space includes a keyboard, video, and mouse (KVM) station that is coupled to a plurality of computing devices.

40. The securement method of claim 21, wherein the biometric data set is provided by a mobile device.

41. A computer readable media storing machine interpretable instructions, which when executed, cause a processor to perform steps of any method of claims 21-41.

42. A securement device for controlling physical access to a controlled space by one or more users, the device comprising:

a controller circuit configured to generate signals to control actuation of a physical locking mechanism, the physical locking mechanism coupled to a biometric receiver configured for receiving a biometric data set obtained from a user of the one or more users and transmitting a representation of the biometric data set to a communications splitter circuit;

the communications splitter circuit configured to receive the biometric data set, the communications splitter circuit including a first electronic communication interface and a second electronic communication interface, the first electronic communication

interface adapted for communication over a first communication channel between the communications splitter circuit and a sentry computer server, the second electronic communication interface adapted for communication over a second communication channel between the communications splitter circuit and an access control device;

the communications splitter circuit configured to transmit the representation of the biometric data set to the sentry computer server across the first communication channel, wherein the representation of the biometric data sets enables the sentry computer to (i) perform a matching challenge to determine whether the representation of the biometric data set matches a corresponding authorized user, and (ii) responsive to a positive determination of a match, generate and transmit a data set representative of an identity profile corresponding to the user to the communications splitter circuit across the first communication channel;

wherein responsive to the receipt of the data set representative of the identity profile across the first communication channel, the communications splitter circuit or the controller circuit is further configured to transmit the data set representative of the identity profile to an access control device across the second communication channel,

wherein the data set representative of the identity profile enables the access control device to determine that the identity profile matches an authorized user of a set of authorized users and to transmit one or more control signals to the controller circuit across the second communication channel and the communications splitter circuit to cause the actuating of the physical locking mechanism.

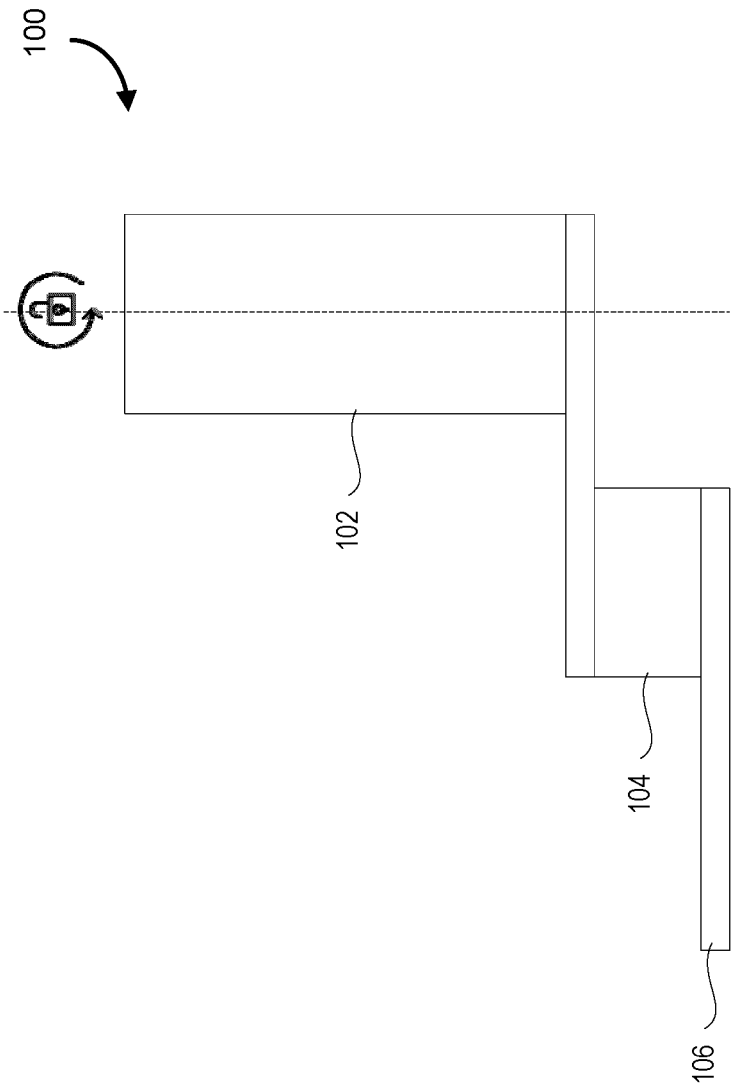

FIG. 1

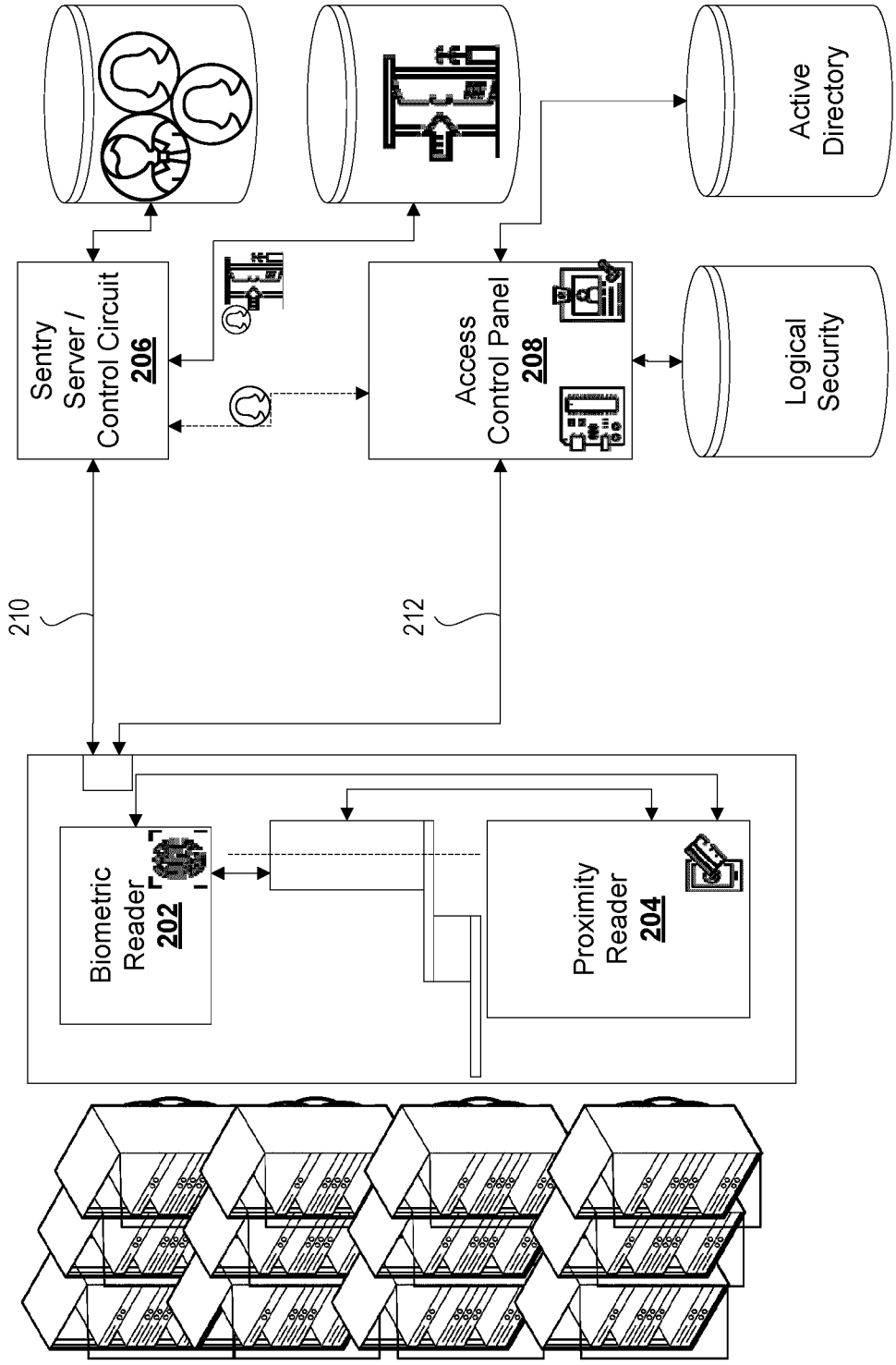
Active Directory
Sentry Server / Control Circuit 206
Access Control Panel 208
Logical Security
210
212
Biometric Reader 202
Proximity Reader 204

FIG. 2

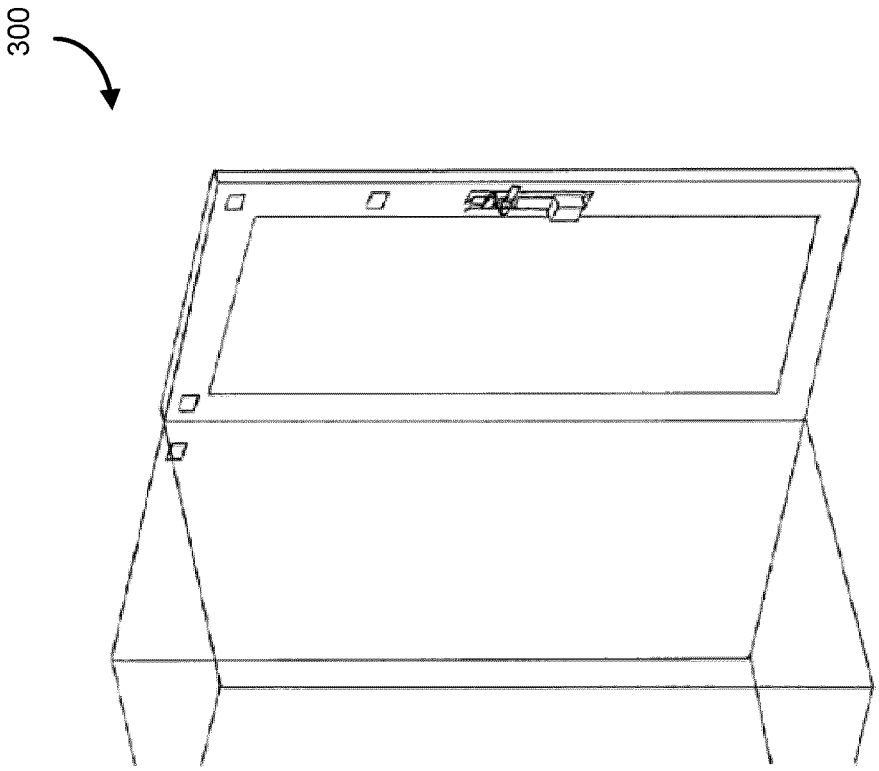

FIG. 3

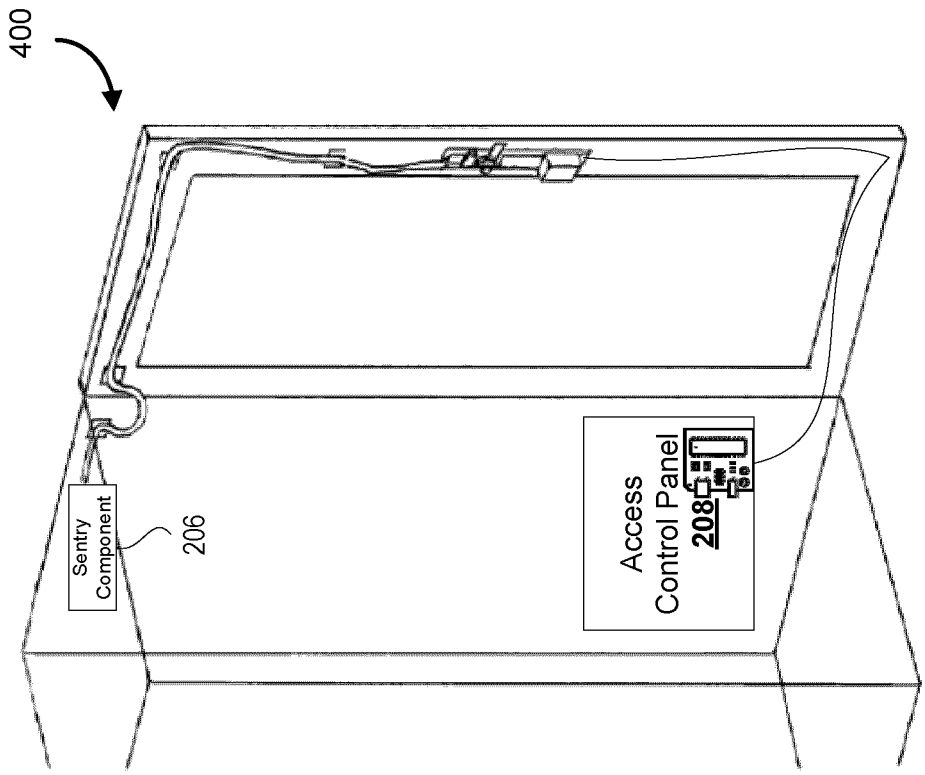

FIG. 4

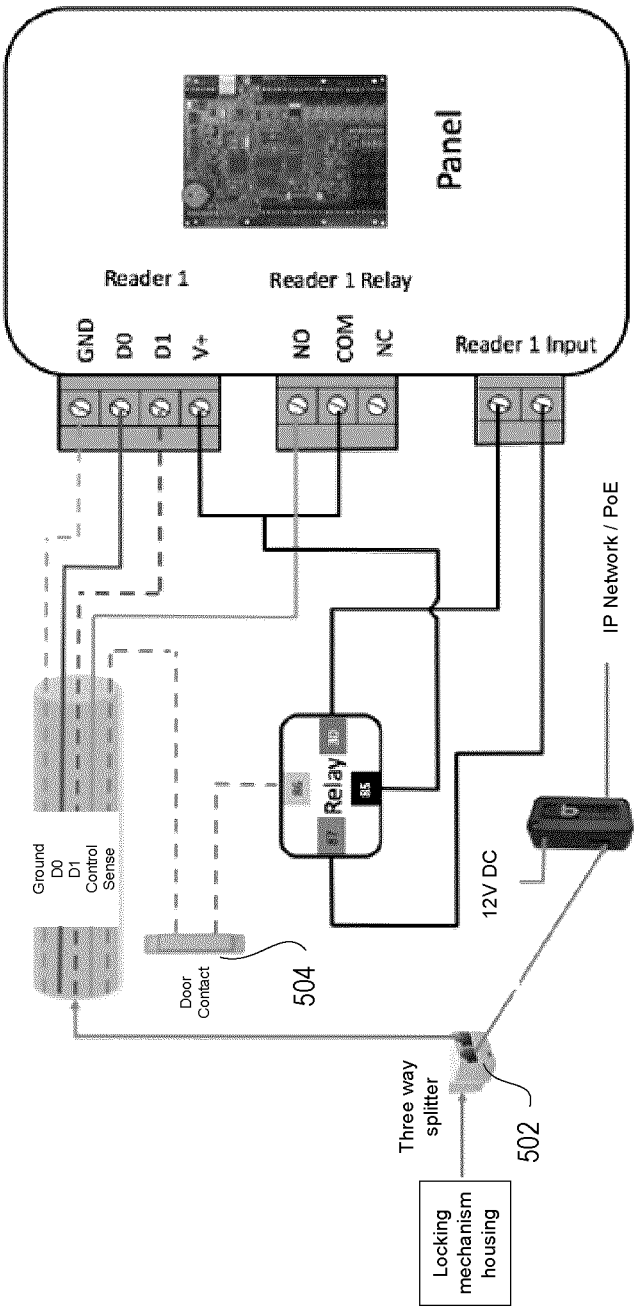
Panel
Reader 1
Reader 1 Relay
GND
D0
D1
V+
NO
COM
NC
Reader 1 Input
IP Network / PoE
Relay
12V DC
Ground
D0
D1
Control Sense
Door Contact
504
Three way splitter
502
Locking mechanism housing

FIG. 5

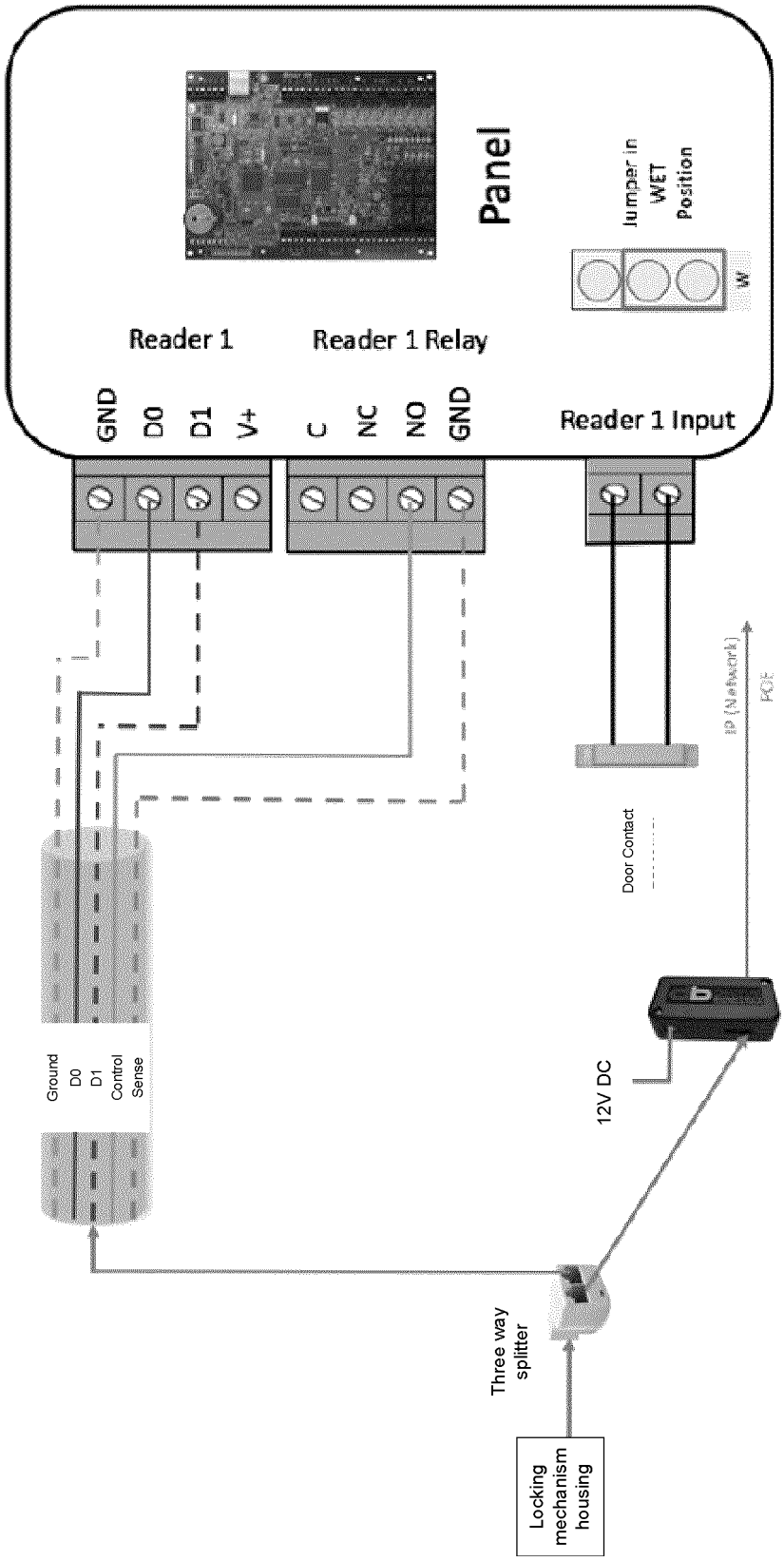
Panel
Jumper in WET Position
W
Reader 1
Reader 1 Relay
GND
D0
D1
V+
C
NC
NO
GND
Reader 1 Input
Door Contact
IP (Network)
POE
12V DC
Ground
D0
D1
Control
Sense
Three way splitter
Locking mechanism housing

FIG. 6

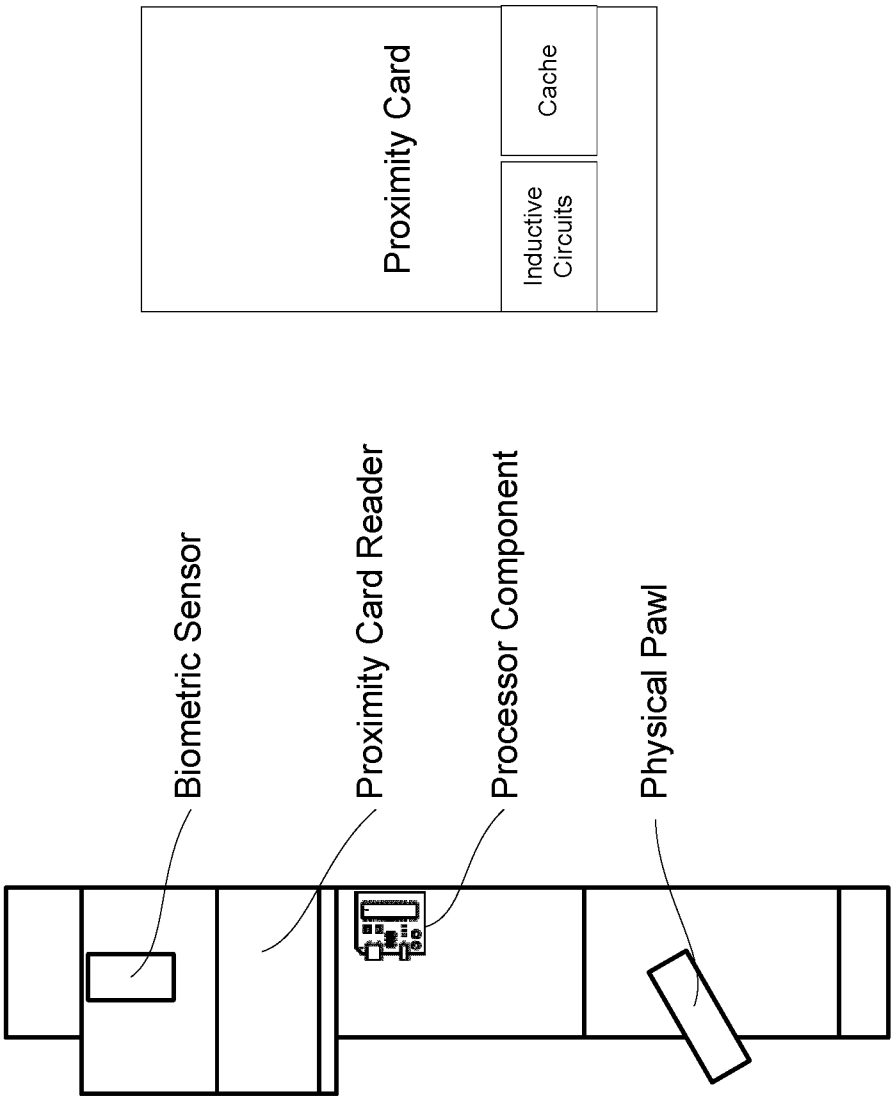
Proximity Card
Cache
Inductive Circuits
Biometric Sensor
Proximity Card Reader
Processor Component
Physical Pawl

FIG. 7

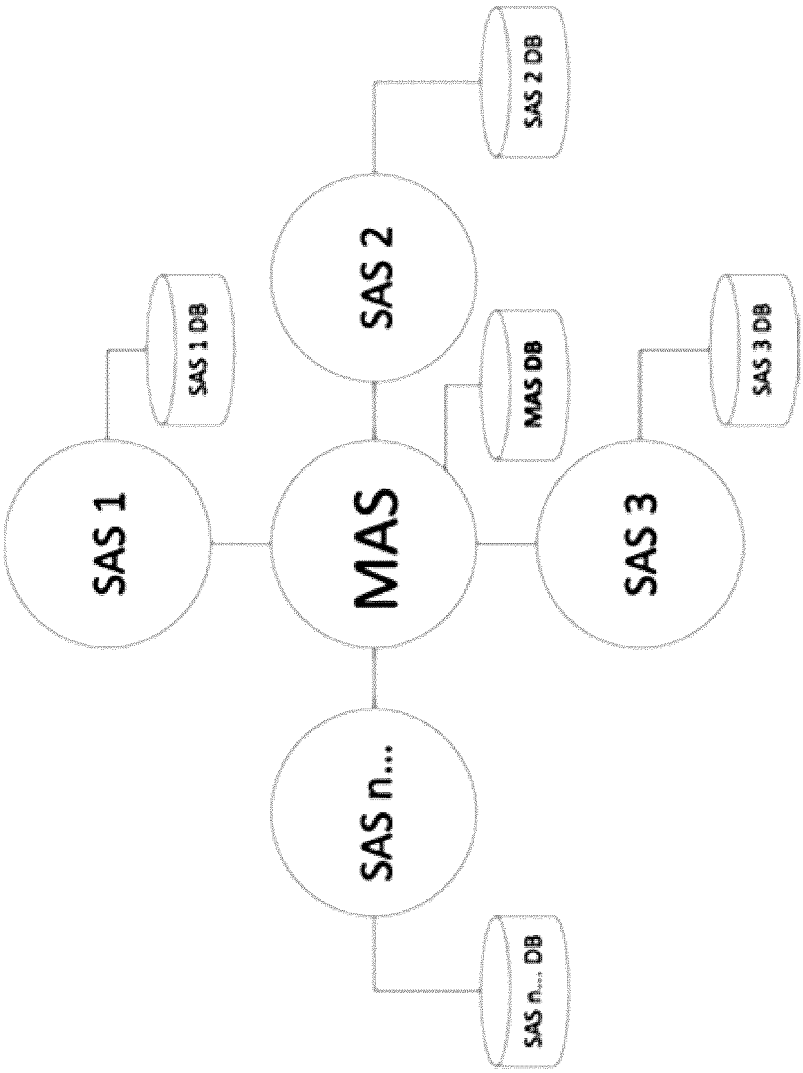

FIG. 8

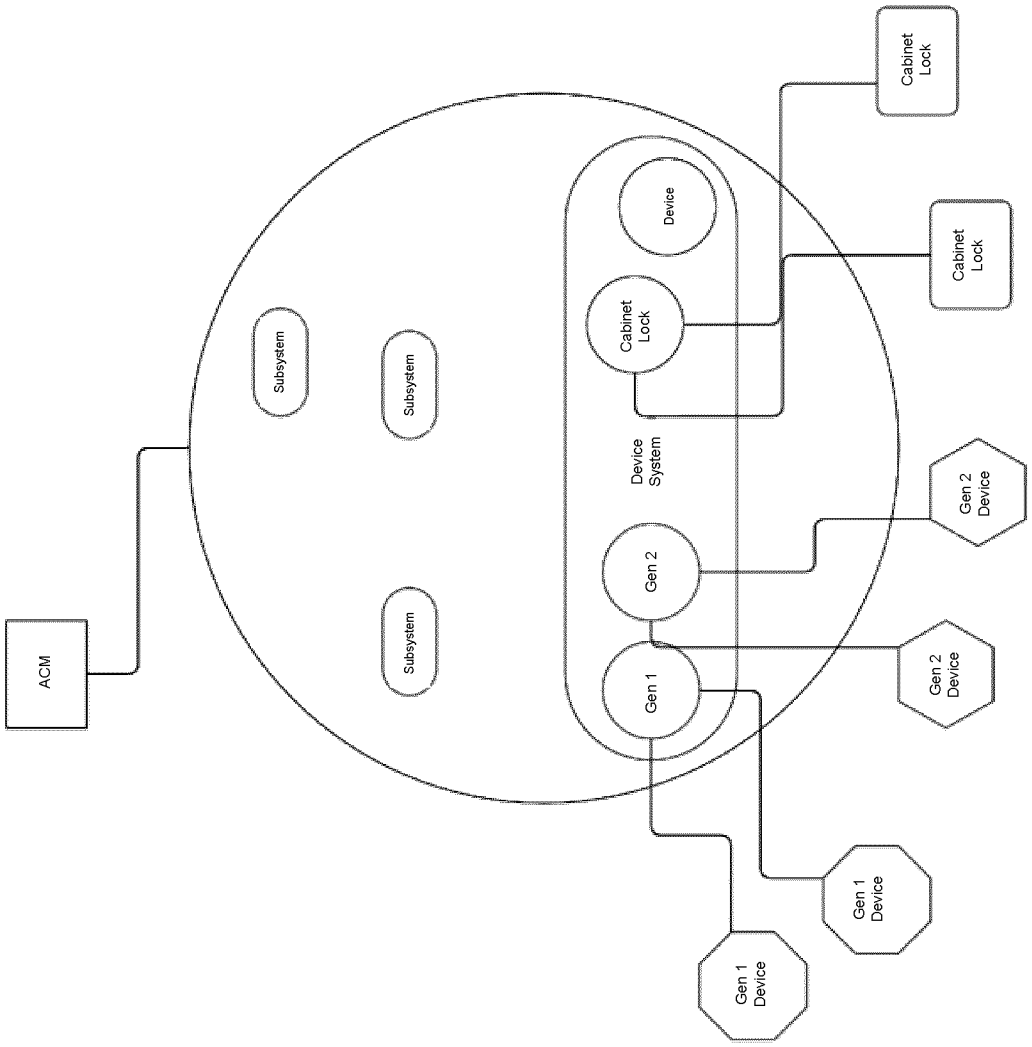
ACM
Subsystem
Subsystem
Subsystem
Device System
Gen 1
Gen 2
Cabinet Lock
Device
Cabinet Lock
Cabinet Lock
Gen 1 Device
Gen 1 Device
Gen 2 Device
Gen 2 Device

FIG. 9

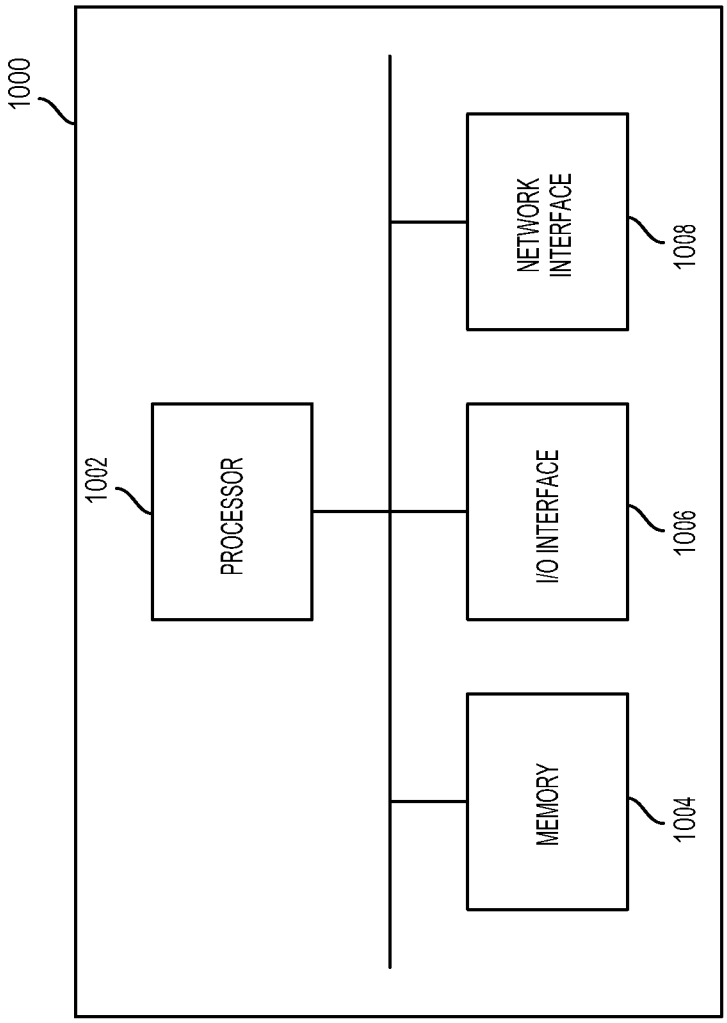
1000
1002
PROCESSOR
NETWORK INTERFACE
1008
I/O INTERFACE
1006
MEMORY
1004

FIG. 10

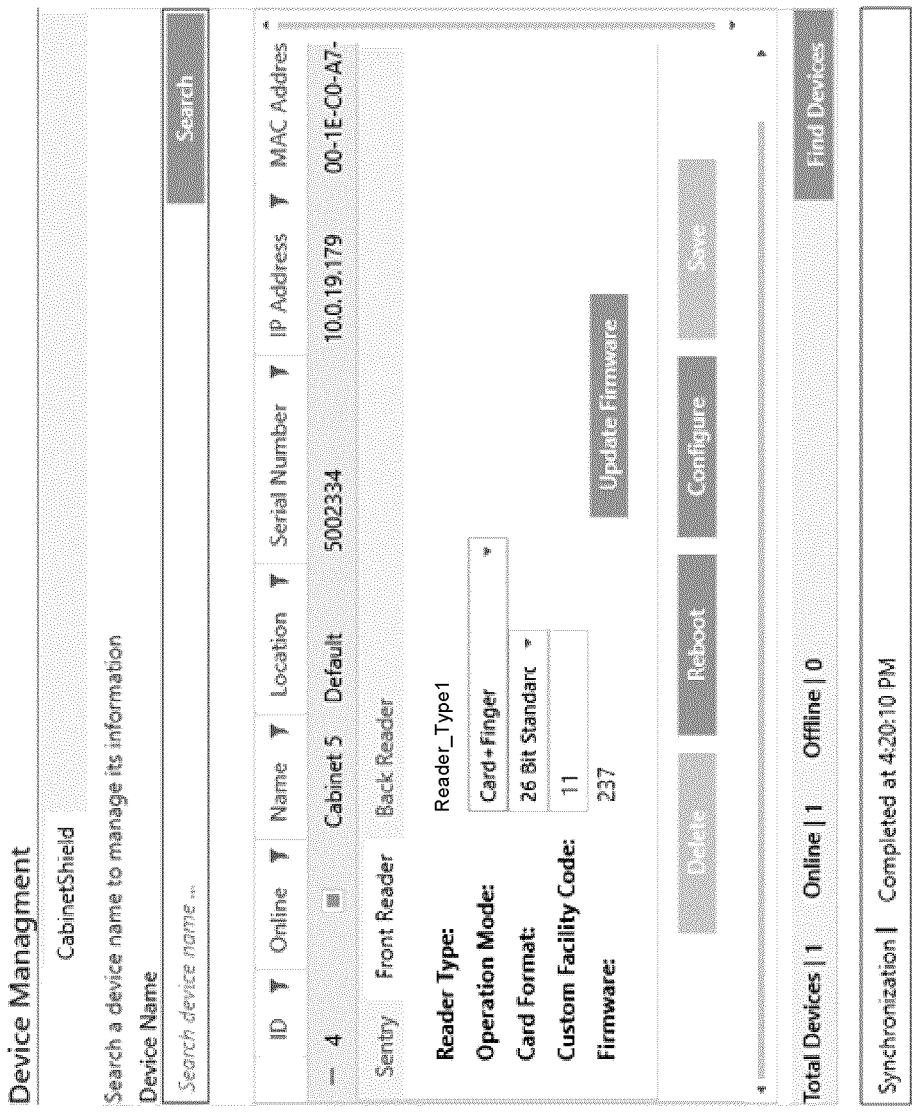
Device Managment
CabinetShield
Search a device name to manage its information
Device Name
Search device name ...
Search
ID
Online
Name
Location
Serial Number
IP Address
MAC Addres
4
Cabinet 5
Default
5002334
10.0.19.179
00-1E-C0-A7-
Sentry
Front Reader
Back Reader
Reader Type:
Reader_Type1
Operation Mode:
Card+Finger
Card Format:
26 Bit Standarc
Custom Facility Code:
11
Firmware:
237
Update Firmware
Delete
Reboot
Configure
Save
Total Devices | 1
Online | 1
Offline | 0
Find Devices
Synchronization |
Completed at 4:20:10 PM

FIG. 11

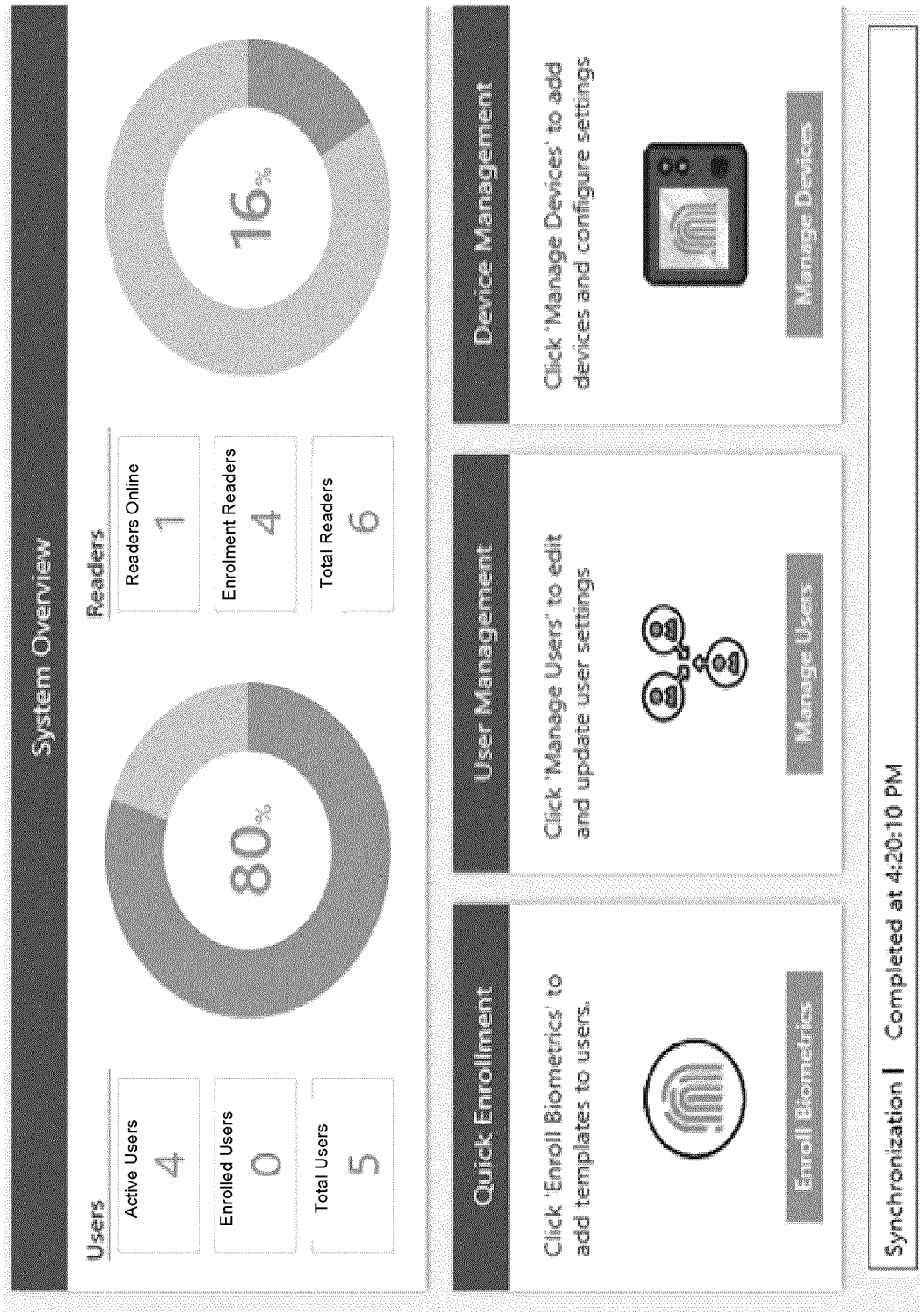
System Overview
Users
Active Users
4
Enrolled Users
0
Total Users
5
80%
Readers
Readers Online
1
Enrolment Readers
4
Total Readers
6
16%
Quick Enrollment
Click 'Enroll Biometrics' to add templates to users.
Enroll Biometrics
User Management
Click 'Manage Users' to edit and update user settings
Manage Users
Device Management
Click 'Manage Devices' to add devices and configure settings
Manage Devices
Synchronization | Completed at 4:20:10 PM

FIG. 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2018/050884

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***G07C 9/00*** (2006.01) , ***G06F 21/32*** (2013.01) , ***G06F 21/43*** (2013.01) , ***H04Q 1/04*** (2006.01) , *H04L 12/28* (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Keywords used across the whole IPC

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Databases: Questel-Orbit (FamPat), Canadian Patents Database, Google. Search terms: control, physical, access, entry, biometric, receiver, reader, authorize, premises, space, room, area, cabinet, rack, equipment, data center, storage, identity, profile, dual, second, authentication, identification, separate, segregate, splitter, sentry, server.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2017/0118206 A1 (Liu) 27 April 2017 (27-04-2017) *paragraphs [0010]-[0012], [0026], [0029], [0031], [0034]-[0038], [0040], [0041]* *Figures 3, 4*	1-42
Y	US 2016/0335427 A1 (Cornick et al.) 17 November 2016 (17-11-2016) *abstract* *paragraphs [0028]-[0030], [0036], [0037], [0040], [0041]* *Figures 1, 4*	1-42
A	US 2017/0124792 A1 (Schoenfelder et al.) 4 May 2017 (04-05-2017) *abstract* *paragraphs [0049]-[0052], [0057], [0060]* *Figures 1-3*	

☑ Further documents are listed in the continuation of Box C.

☑ See patent family annex.

*	Special categories of cited documents:
"A"	document defining the general state of the art which is not considered to be of particular relevance
"E"	earlier application or patent but published on or after the international filing date
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O"	document referring to an oral disclosure, use, exhibition or other means
"P"	document published prior to the international filing date but later than the priority date claimed
"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&"	document member of the same patent family

Date of the actual completion of the international search 14 September 2018 (14-09-2018)	Date of mailing of the international search report 27 September 2018 (27-09-2018)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 819-953-2476	Authorized officer Georges Matar (819) 635-8043

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2011/0205016 A1 (Al-Azem et al.) 25 August 2011 (25-08-2011) *paragraphs [0031]-[0038], [0040], [0051], [0052]* *Figure 1*	
A	US 2010/0242102 A1 (Cross et al.) 23 September 2010 (23-09-2010) *abstract* *paragraphs [0021]-[0025]* *Figures 2, 3*	
A	US 2007/0094716 A1 (Farino et al.) 26 April 2007 (26-04-2007) *paragraphs [0061], [0062], [0094]-[0098]* *Figures 6, 10*	

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2018/050884

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US20170118206A1	27 April 2017 (27-04-2017)	CN106611116A	03 May 2017 (03-05-2017)
		EP3163485A1	03 May 2017 (03-05-2017)
		JP2017097857A	01 June 2017 (01-06-2017)
US20160335427A1	17 November 2016 (17-11-2016)	US9721081B2	01 August 2017 (01-08-2017)
		CA2986003A1	17 November 2016 (17-11-2016)
		EP3295420A1	21 March 2018 (21-03-2018)
		US2017277877A1	28 September 2017 (28-09-2017)
		US9870459B2	16 January 2018 (16-01-2018)
		US2018032713A1	01 February 2018 (01-02-2018)
		US10049201B2	14 August 2018 (14-08-2018)
		US2018247041A1	30 August 2018 (30-08-2018)
		WO2016183517A1	17 November 2016 (17-11-2016)
US20170124792A1	04 May 2017 (04-05-2017)	AU2016348413A1	26 April 2018 (26-04-2018)
		CA3003174A1	11 May 2017 (11-05-2017)
		CN108475447A	31 August 2018 (31-08-2018)
		WO2017079438A1	11 May 2017 (11-05-2017)
US20110205016A1	25 August 2011 (25-08-2011)	US8952781B2	10 February 2015 (10-02-2015)
US20100242102A1	23 September 2010 (23-09-2010)	AU2007345313A1	31 July 2008 (31-07-2008)
		AU2007345313B2	16 December 2010 (16-12-2010)
		CA2653615A1	31 July 2008 (31-07-2008)
		CN101479987A	08 July 2009 (08-07-2009)
		EP2033359A2	11 March 2009 (11-03-2009)
		EP2033359A4	31 May 2017 (31-05-2017)
		JP2010505286A	18 February 2010 (18-02-2010)
		KR20090041365A	28 April 2009 (28-04-2009)
		MX2008015958A	06 March 2009 (06-03-2009)
		NO20085023A	12 December 2008 (12-12-2008)
		RU2008152118A	10 July 2010 (10-07-2010)
		RU2434340C2	20 November 2011 (20-11-2011)
		WO2008091277A2	31 July 2008 (31-07-2008)
		WO2008091277A3	18 December 2008 (18-12-2008)
US20070094716A1	26 April 2007 (26-04-2007)	US7437755B2	14 October 2008 (14-10-2008)
		CN101297282A	29 October 2008 (29-10-2008)
		CN101297282B	26 October 2011 (26-10-2011)
		EP1941383A2	09 July 2008 (09-07-2008)
		EP1941383A4	22 June 2011 (22-06-2011)
		JP2009514100A	02 April 2009 (02-04-2009)
		JP5129148B2	23 January 2013 (23-01-2013)
		KR20080065299A	11 July 2008 (11-07-2008)
		KR101314445B1	21 November 2013 (21-11-2013)
		WO2007050481A2	03 May 2007 (03-05-2007)
		WO2007050481A3	22 November 2007 (22-11-2007)