(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년05월29일
(11) 등록번호 10-2101246
(24) 등록일자 2020년04월09일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 16/00* (2019.01)
(21) 출원번호 10-2014-0121845
(22) 출원일자 2014년09월15일
심사청구일자 2019년07월11일
(65) 공개번호 10-2015-0032189
(43) 공개일자 2015년03월25일
(30) 우선권주장
14/028,208 2013년09월16일 미국(US)
(56) 선행기술조사문헌
US20090064290 A1
US20090077638 A1
US20130086210 A1
US20040210771 A1

(73) 특허권자
엑시스 에이비
스웨덴왕국 룬트 에스-223 69, 엠달라베겐 14
(72) 발명자
마티어스 브루스
스웨덴왕국 룬트 엘지에치 1202,222 37 록포라레가탄 17비
니클라스 한손
스웨덴왕국 홀비 242 30, 스메디제가탄 4에이
(74) 대리인
특허법인가산

전체 청구항 수 : 총 15 항 심사관 : 양종필

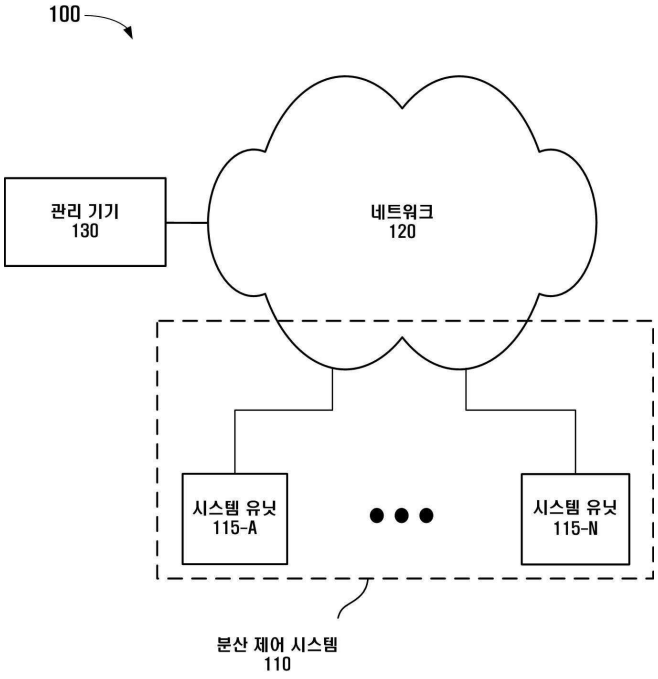
(54) 발명의 명칭 **사용자 크리덴셜들의 배포**

(57) 요 약

본 방법은 분산된 물리적 접근 제어 시스템에서 사용자 크리덴셜들을 배포하는 것에 관한 것으로, 보다 일반적으로는 분산된 시스템에서 사용자 크리덴셜들을 배포하는 것에 관한 것이다. 본 방법은, 상기 기기(115)에 의해 제공되는 제1 및 제2 서비스(332, 334)에 접근하는 사용자를 인증하기 위해, 사용자 크리덴셜 DB(360), 제1 변환된

(뒷면에 계속)

대 표 도 - 도1



크리덴셜 DB(356), 및 제2 변환된 크리덴셜 DB(358)를 포함한다. 상기 방법은 상기 사용자 크리덴셜 DB(360)에 기초하여 제1 변환된 크리덴셜 DB(356) 및 제2 변환된 크리덴셜 DB(358)를 생성하는 단계와, 제1 또는 제2 서비스(332, 334)에 대한 접근을 허용할지를 결정하기 위해, 사용자로부터 수신된 크리덴셜을 제1 또는 제2 변환된 크리덴셜 DB(356, 358)와 비교하는 단계를 포함할 수 있다. 상기 방법은, 서비스들에 접근하는 사용자들을 인증하기 위해, 상기 다른 기기들이 변환된 크리덴셜 DB들을 생성할 수 있도록, 네트워크 내에서 연결된 복수의 다른 기기들(115/210)에게 상기 사용자 크리덴셜 DB를 배포하는 단계를 포함할 수 있다.

명 세 서

청구범위

청구항 1

사용자 크리덴셜 데이터베이스(360), 기기(115/210)에 의해 제공되는 제1 서비스(332)에 접근하는 사용자들을 인증하기 위한 제1 변환된 크리덴셜 데이터베이스(356), 및 상기 기기(115/210)에 의해 제공된 제2 서비스(334)에 접근하는 사용자들을 인증하기 위한 제2 변환된 크리덴셜 데이터베이스(358)를 저장하는 메모리(350);

변환되지 않은 크리덴셜을 수신하는 통신 인터페이스(218);

상기 사용자 크리덴셜 데이터베이스(360)에 기초하여, 상기 제1 변환된 사용자 크리덴셜 데이터베이스(356) 및 상기 제2 변환된 사용자 크리덴셜 데이터베이스(360)를 업데이트하고, 상기 제1 서비스(332)에 접근하는 사용자를 인증하기 위하여 상기 수신된 변환되지 않은 크리덴셜이 정확한지를 판단하기 위해, 상기 수신된 변환되지 않은 크리덴셜을 상기 제1 변환된 크리덴셜 데이터베이스(356)에 저장된 제1 변환된 크리덴셜과 비교하거나, 상기 제2 서비스(334)에 접근하는 사용자를 인증하기 위하여 상기 수신된 변환되지 않은 크리덴셜이 정확한지를 판단하기 위해, 상기 수신된 변환되지 않은 크리덴셜을 상기 제2 변환된 크리덴셜 데이터베이스(358)에 저장된 제2 변환된 크리덴셜과 비교하는 프로세서(214);

피어-투-피어 네트워크 내에 연결된 복수의 다른 기기들에 의해 제공되는 서비스들에 접근하는 사용자들을 인증하기 위한, 다른 변환된 크리덴셜 데이터베이스들을 상기 복수의 다른 기기들이 생성하도록, 상기 복수의 다른 기기들(115/210)에게 상기 사용자 크리덴셜 데이터베이스(360)를 배포하고, 상기 피어-투-피어 네트워크 내의 다른 기기들로부터 상기 사용자 크리덴셜 데이터베이스(360)를 수신하는 통신 인터페이스(218)를 포함하는 사용자 크리덴셜 배포 기기(115/210).

청구항 2

제1항에 있어서,

상기 사용자 크리덴셜 데이터베이스는 암호화된 사용자 크리덴셜 데이터베이스이고, 상기 프로세서는 상기 암호화된 사용자 크리덴셜 데이터베이스를 복호화하고 상기 복호화된 사용자 크리덴셜 데이터베이스에 기초하여, 상기 제1 및 제2 변환된 크리덴셜 데이터베이스를 생성하도록 구성되며,

상기 다른 기기들이, 상기 다른 기기들에 의해 제공되는 서비스들에 접근하는 사용자를 인증하기 위한, 상기 다른 변환된 크리덴셜 데이터베이스들을 생성하도록, 상기 통신 인터페이스는 상기 다른 변환된 크리덴셜 데이터베이스들을 상기 다른 기기들에 배포하도록 구성되는 사용자 크리덴셜 배포 기기.

청구항 3

제1항 또는 제2항에 있어서,

상기 제1 서비스는 시큐어 쉘(SSH) 서버, 파일 전송 프로토콜(FTP) 서버, 원격 데스크탑 프로토콜(ROP) 서버, 가상 사설 네트워크(VPN) 서버, 또는 가상 네트워크 채널(VNC) 서버 중에서 하나를 포함하고,

상기 제2 서비스는 상기 제1 서비스와 다르고, 시큐어 쉘(SSH) 서버, 파일 전송 프로토콜(FTP) 서버, 원격 데스크탑 프로토콜(ROP) 서버, 가상 사설 네트워크(VPN) 서버, 또는 가상 네트워크 채널(VNC) 서버 중에서 하나를 포함하는 사용자 크리덴셜 배포 기기.

청구항 4

제2항에 있어서,

상기 프로세서는 암호 일방향 함수를 사용하여 상기 복호화된 사용자 크리덴셜 데이터베이스로부터, 크리덴셜들을 변환함에 의해 상기 제1 변환된 크리덴셜 데이터베이스를 생성하고,

상기 프로세서는 암호 일방향 함수를 사용하여 상기 복호화된 사용자 크리덴셜 데이터베이스로부터, 크리덴셜들을 변환함에 의해 상기 제2 변환된 크리덴셜 데이터베이스를 생성하도록 구성되는 사용자 크리덴셜 배포 기기.

청구항 5

제1항에 있어서,

상기 제1 변환된 크리덴셜 데이터베이스 및 상기 제2 변환된 크리덴셜 데이터베이스는 각각 동일한 크리덴셜로 동일한 사용자를 인증하도록 구성되는 사용자 크리덴셜 배포 기기.

청구항 6

제1항에 있어서,

상기 프로세서는 관리자로부터 업데이트된 사용자 크리덴셜들을 수신하고, 상기 사용자 크리덴셜 데이터베이스를 업데이트하며, 상기 업데이트된 사용자 크리덴셜 데이터베이스에 기초하여 상기 제1 변환된 크리덴셜 데이터베이스와 상기 제2 변환된 크리덴셜 데이터베이스를 생성하고,

상기 다른 기기들이, 상기 다른 기기들에 의해 제공된 서비스들에 접근하는 사용자들을 인증하기 위한, 상기 다른 변환된 크리덴셜 데이터베이스들을 생성하도록, 상기 통신 인터페이스는 상기 업데이트된 사용자 크리덴셜 데이터베이스를 다른 기기들에 배포하도록 구성되는 사용자 크리덴셜 배포 기기.

청구항 7

제2항에 있어서, 상기 프로세서는,

관리자로부터 상기 통신 인터페이스를 통하여 수신되는 패스워드에 기초하여, 암호화된 키를 복호화하여 키를 생성하고;

상기 키에 기초하여 상기 암호화된 사용자 크리덴셜 데이터베이스를 복호화하여 복호화된 관리자 패스워드를 생성하며;

상기 관리자로부터 수신된 패스워드가 상기 복호화된 관리자 패스워드와 동일하면 접근을 인증하는 사용자 크리덴셜 배포 기기.

청구항 8

상기 사용자 크리덴셜 데이터베이스를 배포하기 위해 상기 피어-투-피어 네트워크를 통해 통신하는, 제1항에 기재된 복수의 기기들을 포함하는 시스템.

청구항 9

변환되지 않은 크리덴셜을 저장하는 사용자 크리덴셜 데이터베이스, 기기에 의해 제공되는 제1 서비스에 접근하는 사용자들을 인증하기 위한 제1 변환된 크리덴셜 데이터베이스, 및 상기 기기에 의해 제공된 제2 서비스에 접근하는 사용자들을 인증하기 위한 제2 변환된 크리덴셜 데이터베이스를 저장하는 단계;

상기 사용자 크리덴셜 데이터베이스에 기초하여, 상기 제1 변환된 크리덴셜 데이터베이스 및 상기 제2 변환된 크리덴셜 데이터베이스를 생성하는 단계;

변환되지 않은 크리덴셜을 상기 기기가 수신하고, 상기 변환되지 않은 크리덴셜을 변환함으로써 수신되어 변환된 크리덴셜을 생성하는 단계;

상기 제1 서비스에 접근하는 사용자를 인증하기 위하여 상기 수신되어 변환된 크리덴셜이 정확한지를 판단하기 위해, 상기 수신되어 변환된 크리덴셜을 상기 제1 변환된 크리덴셜 데이터베이스에 저장된 제1 변환된 크리덴셜과 비교하거나, 상기 제2 서비스에 접근하는 사용자를 인증하기 위하여 상기 수신되어 변환된 크리덴셜이 정확한지를 판단하기 위해, 상기 수신되어 변환된 크리덴셜을 상기 제2 변환된 크리덴셜 데이터베이스에 저장된 제2 변환된 크리덴셜과 비교하는 단계;

피어-투-피어 네트워크 내에 연결된 복수의 다른 기기들에 의해 제공되는 서비스들에 접근하는 사용자들을 인증하기 위한, 다른 변환된 크리덴셜 데이터베이스들을 상기 복수의 다른 기기들이 생성하도록, 상기 복수의 다른 기기들에게 상기 사용자 크리덴셜 데이터베이스를 배포하는 단계; 및

상기 피어-투-피어 네트워크 내의 다른 기기들로부터 상기 사용자 크리덴셜 데이터베이스를 수신하는 단계를 포함하는 사용자 크리덴셜 배포 방법.

청구항 10

제9항에 있어서,

상기 사용자 크리덴셜 데이터베이스는 암호화된 사용자 크리덴셜 데이터베이스이며,

상기 암호화된 사용자 크리덴셜 데이터베이스를 복호화하고 상기 복호화된 사용자 크리덴셜 데이터베이스에 기초하여, 상기 제1 및 제2 변환된 크리덴셜 데이터베이스를 생성하는 단계; 및

상기 다른 기기들 각각이, 대응하는 기기들에 의해 제공되는 서비스들에 접근하는 사용자를 인증하기 위한, 대응하는 변환된 크리덴셜 데이터베이스들을 생성하도록, 통신 인터페이스는 상기 다른 변환된 크리덴셜 데이터베이스들을 상기 다른 기기들에 배포하는 단계를 더 포함하는 사용자 크리덴셜 배포 방법.

청구항 11

제10항에 있어서,

암호 일방향 함수를 사용하여 상기 복호화된 사용자 크리덴셜 데이터베이스로부터, 크리덴셜들을 변환함에 의해 상기 제1 변환된 크리덴셜 데이터베이스를 생성하는 단계; 및

암호 일방향 함수를 사용하여 상기 복호화된 사용자 크리덴셜 데이터베이스로부터, 크리덴셜들을 변환함에 의해 상기 제2 변환된 크리덴셜 데이터베이스를 생성하는 단계를 더 포함하는 사용자 크리덴셜 배포 방법.

청구항 12

제9, 10 또는 11항에 있어서,

상기 제1 변환된 크리덴셜 데이터베이스 및 상기 제2 변환된 크리덴셜 데이터베이스는 각각 동일한 크리덴셜로 동일한 사용자를 인증하도록 구성되는 사용자 크리덴셜 배포 방법.

청구항 13

제9, 10 또는 11항에 있어서,

관리자로부터 업데이트된 사용자 크리덴셜들을 수신하고, 상기 사용자 크리덴셜 데이터베이스를 업데이트하는 단계;

상기 업데이트된 사용자 크리덴셜 데이터베이스에 기초하여 상기 제1 변환된 크리덴셜 데이터베이스와 상기 제2 변환된 크리덴셜 데이터베이스를 업데이트하는 단계; 및

상기 다른 기기들 각각이, 대응하는 기기들에 의해 제공된 서비스들에 접근하는 사용자들을 인증하기 위한, 대응하는 변환된 크리덴셜 데이터베이스들을 생성하도록, 상기 업데이트된 사용자 크리덴셜 데이터베이스를 다른 기기들에 배포하는 단계를 포함하는 사용자 크리덴셜 배포 방법.

청구항 14

제10항에 있어서,

관리자로부터 수신되는 패스워드에 기초하여, 상기 암호화된 사용자 크리덴셜 데이터베이스를 복호화하는 단계를 더 포함하는 사용자 크리덴셜 배포 방법.

청구항 15

제14항에 있어서,

상기 관리자로부터 수신된 패스워드에 기초하여, 상기 암호화된 사용자 크리덴셜 데이터베이스를 복호화하는 단계는,

상기 관리자로부터 수신된 패스워드에 기초하여, 암호화된 키를 복호화하여 키를 생성하는 단계;

상기 키에 기초하여 상기 암호화된 사용자 크리덴셜 데이터베이스를 복호화하는 단계를 포함하고,

상기 방법은,

복호화된 관리자 패스워드를 생성하기 위해, 상기 키에 기초하여 암호화된 관리자 패스워드를 복호화하는 단계; 및

상기 관리자로부터 수신된 패스워드가 상기 복호화된 관리자 패스워드와 동일하면 접근을 인증하는 단계를 더 포함하는 사용자 크리덴셜 배포 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 분산된 물리적 접근 제어 시스템에서 사용자 크리덴셜들을 배포하는 것에 관한 것으로, 보다 일반적으로는 분산된 시스템에서 사용자 크리덴셜들을 배포하는 것에 관한 것이다.

배 경 기 술

[0002] 접근 제어 시스템들은 시설에 대한 물리적 접근을 제어하기 위하여 사용될 수 있다. 접근 제어 시스템(및 다른 종류의 제어 시스템들)은, 각각 다양한 서비스들을 사용자들에게 제공하는 다수의 컨트롤러들을 포함할 수 있다. 각각의 컨트롤러에 대한 각각의 서비스는 사용자가 상기 서비스에 접근하는 권한을 갖도록 인증하기 위한 크리덴셜들을 필요로 할 수 있다.

[0003] 결과적으로, 사용자들은 각각의 기기 상에서 각각의 서비스에 대한 그들의 크리덴셜들을 기억할 필요가 있을 수 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명은 분산된 시스템에서 사용자 크리덴셜들을 배포하는 것에 관한 것이다.

[0005] 본 발명의 목적은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0006] 일 실시예에서, 기기는 사용자 크리덴셜 DB, 상기 기기에 의해 제공되는 제1 서비스에 접근하는 사용자를 인증하기 위한 제1 변환된 크리덴셜 DB, 및 상기 기기에 의해 제공되는 제2 서비스에 접근하는 사용자를 인증하기 위한 제2 변환된 크리덴셜 DB를 포함할 수 있다. 상기 기기는 상기 사용자 크리덴셜 데이터베이스에 기초하여, 상기 제1 변환된 사용자 크리덴셜 데이터베이스 및 상기 제2 변환된 사용자 크리덴셜 데이터베이스를 업데이트하고, 상기 제1 서비스에 접근하는 사용자를 인증하기 위하여, 사용자로부터 수신된 크리덴셜을 상기 제1 변환된 크리덴셜 데이터베이스와 비교하거나, 상기 제2 서비스에 접근하는 사용자를 인증하기 위하여, 상기 수신된 크리덴셜을 상기 제2 변환된 크리덴셜 데이터베이스와 비교하는 프로세서를 포함할 수 있다. 상기 기기는, 상기 다른 기기들이, 상기 다른 기기들에 의해 제공된 서비스들에 접근하는 사용자들을 인증하기 위한, 다른 변환된 크리덴셜 데이터베이스들을 생성하도록, 피어-투-피어 네트워크 내에 연결되는 복수의 다른 기기들에게 상기 사용자 크리덴셜 데이터베이스를 배포하는 통신 인터페이스를 포함할 수 있다. 상기 프로세서는 상기 피어-투-피어 네트워크 내의 다른 기기들로부터 상기 사용자 크리덴셜 데이터베이스를 수신할 수 있다.

[0007] 일 실시예에서, 상기 사용자 크리덴셜 DB는 암호화된 사용자 크리덴셜 데이터베이스이고, 상기 프로세서는 상기 암호화된 사용자 크리덴셜 데이터베이스를 복호화하고 상기 복호화된 사용자 크리덴셜 데이터베이스에 기초하여, 상기 제1 및 제2 변환된 크리덴셜 데이터베이스를 생성한다. 상기 다른 기기들이, 상기 다른 기기들에 의해 제공되는 서비스들에 접근하는 사용자를 인증하기 위한, 상기 다른 변환된 크리덴셜 데이터베이스들을 생성하도록, 상기 통신 인터페이스는 상기 다른 변환된 크리덴셜 데이터베이스들을 상기 다른 기기들에 배포한다.

[0008] 일 실시예에서, 상기 제1 서비스는 시큐어 쉘(SSH) 서버, 파일 전송 프로토콜(FTP) 서버, 원격 데스크탑 프로토콜(ROP) 서버, 가상 사설 네트워크(VPN) 서버, 또는 가상 네트워크 채널(VNC) 서버 중에서 하나를 포함할 수 있다. 이 실시예에서, 상기 제2 서비스는 상기 제1 서비스와 다르고, 시큐어 쉘(SSH) 서버, 파일 전송 프로토콜(FTP) 서버, 원격 데스크탑 프로토콜(ROP) 서버, 가상 사설 네트워크(VPN) 서버, 또는 가상 네트워크 채널(VNC)

서버 중에서 하나를 포함할 수 있다.

[0009] 일 실시예에서, 상기 프로세서는 암호 일방향 함수(cryptographic one-way function)을 사용하여 상기 복호화된 사용자 크리덴셜 데이터베이스로부터, 크리덴셜들을 변환함에 의해 상기 제1 변환된 크리덴셜 데이터베이스를 생성할 수 있다. 상기 프로세서는 상기 암호 일방향 함수를 사용하여 상기 복호화된 사용자 크리덴셜 데이터베이스로부터, 크리덴셜들을 변환함에 의해 상기 제2 변환된 크리덴셜 데이터베이스를 생성할 수도 있다.

[0010] 일 실시예에서, 상기 제1 변환된 크리덴셜 데이터베이스 및 상기 제2 변환된 크리덴셜 데이터베이스는 각각 동일한 크리덴셜로 동일한 사용자를 인증하도록 구성될 수 있다. 일 실시예에서, 상기 프로세서는 관리자로부터 업데이트된 사용자 크리덴셜들을 수신하고, 상기 사용자 크리덴셜 데이터베이스를 업데이트하며, 상기 업데이트된 사용자 크리덴셜 데이터베이스에 기초하여 상기 제1 변환된 크리덴셜 데이터베이스와 상기 제2 변환된 크리덴셜 DB를 생성할 수 있다. 상기 다른 기기들이, 상기 다른 기기들에 의해 제공된 서비스들에 접근하는 사용자들을 인증하기 위한, 상기 다른 변환된 크리덴셜 DB들을 생성하도록, 상기 통신 인터페이스는 상기 업데이트된 사용자 크리덴셜 DB를 다른 기기들에 배포할 수 있다.

[0011] 일 실시예에서, 상기 프로세서는 관리자로부터 상기 통신 인터페이스를 통해 수신되는 패스워드에 기초하여 암호화된 사용자 크리덴셜 DB를 복호화할 수 있다. 일 실시예에서, 상기 프로세서는 상기 관리자로부터 상기 통신 인터페이스를 통하여 수신되는 패스워드에 기초하여, 암호화된 키를 복호화하여 키를 생성할 수 있다. 상기 프로세서는 상기 키에 기초하여 상기 암호화된 사용자 크리덴셜 DB를 복호화할 수도 있다. 일 실시예에서, 상기 프로세서는 복호화된 관리자 패스워드를 생성하기 위해, 상기 키에 기초하여 암호화된 관리자 패스워드를 복호화할 수 있다. 상기 프로세서는 상기 관리자로부터 수신된 패스워드가 상기 복호화된 관리자 패스워드와 동일하면 접근을 인증할 수도 있다.

[0012] 일 실시예는 방법을 포함한다. 상기 방법은 사용자 크리덴셜 데이터베이스, 기기에 의해 제공되는 제1 서비스에 접근하는 사용자들을 인증하기 위한 제1 변환된 크리덴셜 데이터베이스, 및 상기 기기에 의해 제공된 제2 서비스에 접근하는 사용자들을 인증하기 위한 제2 변환된 크리덴셜 데이터베이스를 저장하는 단계를 포함할 수 있다. 상기 방법은 상기 사용자 크리덴셜 DB에 기초하여, 상기 제1 변환된 크리덴셜 DB 및 상기 제2 변환된 크리덴셜 DB를 생성하는 단계를 포함할 수 있다. 상기 방법은 상기 제1 서비스에 접근하는 사용자를 인증하기 위하여, 수신된 크리덴셜을 상기 제1 변환된 크리덴셜 데이터베이스와 비교하거나, 상기 제2 서비스에 접근하는 사용자를 인증하기 위하여, 상기 수신된 크리덴셜을 상기 제2 변환된 크리덴셜 데이터베이스와 비교하는 단계를 포함할 수 있다. 상기 방법은, 상기 다른 기기들이 상기 다른 기기들에 의해 제공된 서비스들에 접근하는 사용자들을 인증하기 위한, 다른 변환된 크리덴셜 데이터베이스들을 생성하도록, 피어-투-피어 네트워크 내에 연결되는 복수의 다른 기기들에게 상기 사용자 크리덴셜 데이터베이스를 배포하는 단계를 포함할 수 있다. 상기 방법은 상기 피어-투-피어 네트워크 내의 다른 기기들로부터 상기 사용자 크리덴셜 데이터베이스를 수신하는 단계를 포함할 수도 있다.

[0013] 일 실시예에서, 상기 사용자 크리덴셜 DB는 암호화된 사용자 크리덴셜 데이터베이스이며, 상기 방법은 상기 암호화된 사용자 크리덴셜 데이터베이스를 복호화하고 상기 복호화된 사용자 크리덴셜 데이터베이스에 기초하여, 상기 제1 및 제2 변환된 크리덴셜 데이터베이스를 생성하는 단계를 포함할 수 있다. 상기 방법은 상기 다른 기기들이, 상기 다른 기기들에 의해 제공되는 서비스들에 접근하는 사용자를 인증하기 위한, 상기 다른 변환된 크리덴셜 데이터베이스들을 생성하도록, 상기 통신 인터페이스는 상기 다른 변환된 크리덴셜 데이터베이스들을 상기 다른 기기들에 배포하는 단계를 포함할 수도 있다.

[0014] 일 실시예에서, 상기 방법은 암호 일방향 함수를 사용하여 상기 복호화된 사용자 크리덴셜 데이터베이스로부터, 크리덴셜들을 변환함에 의해 상기 제1 변환된 크리덴셜 데이터베이스를 생성하는 단계를 포함할 수 있다. 암호 일방향 함수를 사용하여 상기 복호화된 사용자 크리덴셜 데이터베이스로부터, 크리덴셜들을 변환함에 의해 상기 제2 변환된 크리덴셜 데이터베이스를 생성할 수 있다.

[0015] 일 실시예에서, 상기 제1 변환된 크리덴셜 데이터베이스 및 상기 제2 변환된 크리덴셜 데이터베이스는 각각 동일한 크리덴셜로 동일한 사용자를 인증하도록 구성될 수 있다. 일 실시예에서, 상기 방법은 관리자로부터 업데이트된 사용자 크리덴셜들을 수신하고, 상기 사용자 크리덴셜 데이터베이스를 업데이트하고, 상기 업데이트된 사용자 크리덴셜 데이터베이스에 기초하여 상기 제1 변환된 크리덴셜 데이터베이스와 상기 제2 변환된 크리덴셜 DB를 업데이트하는 단계를 포함할 수 있다. 상기 방법은 상기 다른 기기들 각각이, 상기 다른 기기들에 의해 제공된 서비스들에 접근하는 사용자들을 인증하기 위한, 대응되는 다른 변환된 크리덴셜 DB들을 생성하도록, 상기 업데이트된 사용자 크리덴셜 DB를 다른 기기들에 배포할 수도 있다.

[0016] 일 실시예에서, 상기 방법은 관리자로부터 상기 통신 인터페이스를 통하여 수신되는 패스워드에 기초하여, 상기 암호화된 사용자 크리덴셜 DB를 복호화하는 단계를 포함할 수 있다. 일 실시예에서, 상기 방법은 상기 관리자로부터 상기 통신 인터페이스를 통하여 수신되는 패스워드에 기초하여, 암호화된 키를 복호화하여 키를 생성하고, 상기 키에 기초하여 상기 암호화된 사용자 크리덴셜 DB를 복호화하는 단계를 포함할 수 있다.

[0017] 일 실시예에서, 상기 방법은 관리자로부터 수신된 패스워드에 기초하여, 상기 암호화된 사용자 크리덴셜 데이터베이스를 복호화하는 단계를 포함할 수 있다. 일 실시예에서, 상기 방법은 상기 관리자로부터 수신된 패스워드에 기초하여, 암호화된 키를 복호화하여 키를 생성하고, 상기 키에 기초하여 상기 암호화된 사용자 크리덴셜 데이터베이스를 복호화하는 단계를 포함할 수 있다.

[0018] 일 실시예는 시스템을 포함할 수 있다. 상기 시스템은 네트워크 내에서 통신하는 복수의 기기들을 포함할 수 있다. 각각의 기기는 사용자 크리덴셜 데이터베이스, 기기에 의해 제공되는 제1 서비스에 접근하는 사용자들을 인증하기 위한 제1 변환된 크리덴셜 데이터베이스, 및 상기 기기에 의해 제공된 제2 서비스에 접근하는 사용자들을 인증하기 위한 제2 변환된 크리덴셜 데이터베이스를 저장하는 메모리를 포함할 수 있다. 각각의 기기는 상기 사용자 크리덴셜 데이터베이스에 기초하여, 상기 제1 변환된 사용자 크리덴셜 데이터베이스 및 상기 제2 변환된 사용자 크리덴셜 데이터베이스를 업데이트하는 프로세서를 포함할 수 있다. 상기 제1 또는 제2 서비스에 대한 접근을 허용할지를 결정하기 위하여, 상기 프로세서는 사용자로부터 수신된 크리덴셜을, 상기 제1 또는 제2 변환된 크리덴셜 DB와 비교할 수 있다. 각각의 기기는 다른 기기들 각각이, 상기 다른 기기들에 의해 제공된 서비스들에 접근하는 사용자들을 인증하기 위한, 대응되는 변환된 크리덴셜 데이터베이스들을 생성하도록, 상기 다른 기기들에게 상기 사용자 크리덴셜 데이터베이스를 배포하는 통신 인터페이스를 포함할 수 있다.

[0019] 상기 시스템의 일 실시예에서, 상기 기기들은 상기 피어-투-피어 네트워크 내에서 연결되고 상기 피어-투-피어 네트워크 내에의 기기들 간에 상기 사용자 크리덴셜 DB를 배포한다. 일 실시예에서, 상기 사용자 크리덴셜 DB는 암호화된 사용자 크리덴셜 DB이고, 상기 프로세서는 상기 암호화된 사용자 크리덴셜 DB를 복호화하며, 상기 복호화된 사용자 크리덴셜 DB에 기초하여 상기 제1 및 제2 변환된 크리덴셜 DB를 생성하도록 구성된다.

[0020] 상기 시스템의 일 실시예에서, 상기 다른 기기들 각각이 상기 대응되는 기기에 의해 제공된 서비스들에 접근하는 사용자들을 인증하기 위한, 대응되는 변환된 크리덴셜 DB들을 생성하도록, 상기 통신 인터페이스는 상기 암호화된 사용자 크리덴셜 DB를 상기 다른 기기들에 배포할 수 있다.

[0021] 상기 시스템의 일 실시예에서, 상기 프로세서는 암호 일방향 함수를 사용하여 상기 복호화된 사용자 크리덴셜 DB로부터 크리덴셜들을 변환함에 의해, 상기 제1 변환된 크리덴셜 DB를 생성할 수 있고, 암호 일방향 함수를 사용하여 상기 복호화된 사용자 크리덴셜 DB로부터 크리덴셜들을 변환함에 의해, 상기 제2 변환된 크리덴셜 DB를 생성할 수 있다.

[0022] 다른 실시예들은 이하에서 설명된다. 즉, 전술한 실시예들은 예시로서 제공될 뿐이다.

도면의 간단한 설명

[0023] 도 1은 여기에 기술된 실시예에 따른 예시적인 환경을 도시하는 블록도이다.

도 2a 및 2b는 도 1의 시스템 유닛의 예시적인 요소들을 도시하는 블록도들이다.

도 3a 및 3b는 도 1의 시스템 유닛의 기능적 요소들을 도시하는 블록도들이다.

도 3c는 도 3b의 컨트롤러에서 관리 로직의 기능적 요소들을 도시하는 블록도이다.

도 4는 도 1의 시스템의 예시적인 물리적 레이아웃을 도시하는 평면도이다.

도 5는 도 1의 분산 제어 시스템의 예시적인 물리적 레이아웃을 도시하는 평면도이다.

도 6은 도 1의 관리 기기의 예시적인 요소들을 도시하는 블록도이다.

도 7a는 예시적인 관리 크리덴셜 DB의 블록도이다.

도 7b 및 7c는 예시적인 사용자 크리덴셜 DB의 블록도들이다.

도 7d 내지 7g는 예시적인 서비스 크리덴셜 DB의 블록도들이다.

도 8a는 제어 유닛에서 서비스에 접근하는 권한을 갖는 사용자를 인증하는 예시적인 절차의 흐름도이다.

도 8b는 관리자가 도 7b 및 7c의 사용자 크리덴셜 DB와 도 7d 내지 7g의 서비스 크리덴셜 DB를 업데이트하는 예시적인 절차의 흐름도이다.

도 8c는 관리자를 인증하는 예시적인 절차의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0024] 다음의 상세한 설명은 수반되는 도면들을 참조한다. 다른 도면들에서 동일한 참조 번호는 동일하거나 유사한 요소들을 나타낸다.

[0025] 아래에 기재된 일 실시예는 물리적 접근 제어 시스템(PACS) 내의 컨트롤러들과 관련된다. 다른 실시예들은 빌딩 관리, 감시 및 보안 시스템 내에서 다른 어플리케이션들을 제어하기 위한 시스템 내의 컨트롤러들과 같이, PACS와 다른 환경들을 포함할 수 있다. 일 실시예는 예를 들어 홈 자동화 시스템 내의 컨트롤러들을 포함할 수 있다.

[0026] 위에서 언급된 바와 같이, 사용자들은 각각의 컨트롤러에 의해 제공되는 각각의 서비스에 대해 크리덴셜들을 기억할 것이 요구될 수 있다. 이것은 사용자에 대해서는 부담이 될 수 있다. 아래에 설명된 실시예에서, 관리자는 다중 서비스들을 위한 다중 컨트롤러들에서와 마찬가지로 사용자 크리덴셜들을 관리할 수 있다. 다른 실시예에서, 관리자는 예를 들어 다른 컨트롤러로부터 하나의 컨트롤러 내에 저장된 사용자 크리덴셜들을 관리할 수도 있다. 아래의 하나 이상의 실시예들은 특정 환경에서 물리적 접근 제어 시스템(예를 들어, 분산된 물리적 접근 제어 시스템) 내에서 사용자 크리덴셜들의 배포와 관련된다. 설명된 바와 같이, 다른 실시예들은 다른 종류의 시스템들(물리적 접근 제어 시스템과 다른 시스템) 내에서의 사용자 크리덴셜의 배포와 관련될 수 있다. 일 실시예는 그러한 크리덴셜들을 다른 기기들에 배포하지 않고도, 기기 상에 사용자 크리덴셜들을 저장하는 방법 및 기기와 관련될 수 있다.

[0027] 도 1은 이하에서 설명된 시스템들 및 방법들이 구현되는 예시적인 환경(100)의 블록도이다.

[0028] 도 1에 도시된 바와 같이, 환경(100)은 분산 제어 시스템(110)(예를 들어, 분산된 물리적 접근 제어 시스템), 네트워크(120) 및 관리 기기(130)를 포함할 수 있다.

[0029] 분산 제어 시스템(110)은 시스템 유닛들(115-A 내지 115-N)(통합적으로 "시스템 유닛들(115)" 또는 "유닛들(115)" 및 개별적으로 "유닛(115)"으로 기재됨)을 포함하는 분산된 컴퓨팅 시스템을 포함할 수 있다. 일 실시예에서, 시스템 유닛(115)은 물리적 접근 제어 기기를 포함한다. 예를 들어, 시스템 유닛(115)은 방이나 여러 방들과 같은, 보안 영역에 대한 접근을 제어하는 컨트롤러를 포함할 수 있다. 시스템 유닛(115)은 상기 크리덴셜들이 진정하며 상기 보안 영역에 접근할 권한과 관련되는지를 판단하기 위해 리더 기기(reader device)를 통해 크리덴셜들(예를 들어, 억세스 카드 크리덴셜들)을 수신할 수 있다. 그러하다면, 상기 컨트롤러는 도어 록을 개방하거나 상기 보안 영역에 접근을 허용하는 것과 관련된 다른 동작을 수행하기 위한 명령을 발행할 수 있다.

[0030] 분산 제어 시스템(110)은 하나 이상의 분산된 데이터세트들을 포함할 수 있다. 분산된 데이터세트는, 상기 분산된 데이터세트와 관련된 시스템 유닛들(115) 내에 분산된(그리고 중복된) 형태로 저장되는 데이터를 포함한다. 일 실시예에서, 분산된 데이터세트들은 하나 이상의 기기 상에 복제된다. 예를 들어, 전체의 분산된 데이터세트는 모든 유닛들(115) 내에 저장될 수 있다. 다른 실시예에서, 하나 이상의 유닛들(115)은 상기 분산된 데이터세트의 서브세트를 저장할 수 있다. 또한, 분산된 데이터세트는 모든 시스템 유닛들(115)과 관련되거나, 시스템 유닛들(115)의 서브세트와 관련될 수 있다.

[0031] 일 실시예에서, 상기 분산된 데이터세트(예를 들어, 합의-기반의 분산 데이터베이스) 내에서 변경이 이루어지기 위해, 유닛들(115) 간에 합의(consensus)에 도달한다. 시스템 유닛(115)은 합의-기반의 분산 데이터세트에 대한 변경을 제안할 수 있다. 상기 분산된 데이터세트와 관련된 유닛들(115)의 정족수(quorum) 에 의해 변경이 받아들여지면, 합의는 성립되고, 변경은 각각 관련된 유닛(115) 내에 분산된 데이터세트의 각각의 로컬 사본에 전파될 수 있다. 따라서, 상기 관련된 유닛들(115)의 정족수가 상기 변경에 동의하는 것으로 투표하면, 상기 분산된 데이터세트 내의 변경과 관련된 합의는 성립될 수 있다. 정족수는 상기 관련된 유닛들(115)의 최소 다수(smallest majority)에 해당할 수 있다. 따라서, 분산된 데이터세트가 N개의 유닛들(115)과 관련된다고 하면, N이 짝수인 경우, N/2+1의 관련된 유닛들(115)이 상기 변경에 동의하는 것으로 투표하면 정족수는 달성될 수 있고, N이 홀수인 경우 (N-1)/2+1의 관련된 유닛들(115)이 상기 변경에 동의하는 것으로 투표하면 정족수는 달성될 수 있다. 정족수에 달하는 최소 다수를 요구하는 것은, 두 개의 상충된 제안들이 고려될 때, 적어도 하나의 시스템 유닛(115)이 양자의 제안을 수신하고 합의를 위해 그 중 하나를 선택하는 것을 보장할 수 있다.

[0032] 합의-기반의 분산된 데이터세트는 상기 분산된 데이터세트와 관련된 시스템 유닛(115)이 상기 분산된 데이터세트에 의해 관련되는 정보(예를 들어, 일 실시예에서의 모든 정보)를 포함하는 것을 보장할 수 있다. 예를 들면, 분산된 데이터세트는 접근 규칙들을 포함할 수 있고, 상기 접근 규칙들은 상기 분산된 데이터세트와 관련된 시스템 유닛(115)에서 가용할 수 있다. 따라서, 하나 이상의 분산된 데이터세트들의 결과로서, 일 실시예에서는, 제어 시스템(110)이 서버 기기와 같은 중앙 제어 기기가 없는, 분권화된 시스템에 대응될 수 있다. 다른 실시예들에서, 제어 시스템(110)은 분권화된 시스템 및 서버 기기와 같은 중앙 제어 기기 모두를 포함할 수 있다. 제어 시스템(110)에 대한 변경들은 임의의 시스템 유닛(115)에서 설정될 수 있고, 상기 변경이 분산된 데이터세트와 관련되면, 상기 변경은 상기 분산된 데이터세트와 관련된 다른 시스템 유닛들(115)로 전파될 수 있다. 또한, 고장의 단일 지점이 회피될 수 있기 때문에, 제어 시스템(110)은 기기 고장에 관한 강인성을 제공할 수 있다. 예를 들어, 특정 시스템 유닛(115)이 고장 나더라도, 다른 유닛들(115)은 데이터의 손실 없이(또는 최소한의 데이터 손실로) 계속하여 작동할 수 있다. 다른 실시예에서, 합의 없이 분산된 데이터베이스에 변경이 이루어질 수 있다.

[0033] 네트워크(120)는 유닛들(115)이 서로 통신할 수 있거나 관리 기기(130)가 특정 유닛들(115)와 통신할 수 있게 할 수 있다. 네트워크(120)는 하나 이상의 회로-스위치 네트워크 및/또는 패킷 스위치 네트워크를 포함할 수 있다. 예를 들어, 네트워크(120)는 LAN(local area network), WAN(wide area network), Man(metropolitan area network), PSTN(Public Switched Telephone Network), 애드혹 네트워크, 인터넷, 광섬유 기반의 네트워크, 무선 네트워크 및/또는 이러한 종류의 네트워크들의 조합을 포함할 수 있다.

[0034] 관리 기기(130)는 제어 시스템(110)을 설정하기 위해, 관리자가 특정 기기(115)에 연결하도록 허용하고, 제어 시스템(110)의 설정을 변경하고, 제어 시스템(110) 및/또는 다른 관리 제어 시스템(110)으로부터 정보를 수신하도록 허용한다. 제어 기기(130)는 하나 이상의 유닛들(115)과 통신하도록 설정된 임의의 기기를 포함할 수 있다. 예를 들어, 관리 기기(130)는 휴대용 통신 기기(예를 들어, 모바일 폰, 스마트 폰, 패블릿(phablet) 기기, GPS(global positioning system) 기기, 및/또는 다른 종류의 무선 기기들); 개인용 컴퓨터나 워크스테이션; 서버 기기; 랩톱, 태블릿 또는 다른 종류의 휴대용 컴퓨터; 및/또는 통신 기능을 갖는 다른 종류의 기기를 포함할 수 있다. 일 실시예에서, 관리 기기(130)는 유닛(115)의 일부가 될 수 있다. 따라서, 관리자는 하나 이상의 유닛들(115)로부터 제어 시스템(110)을 관리할 수 있다.

[0035] 도 1은 환경(100)의 예시적 구성요소들을 보여주지만, 다른 실시예들에서, 환경(100)은 도 1에 도시된 것과 달리 더 적은 구성요소들, 다른 구성요소들, 다르게 배치된 구성요소들 또는 추가적인 구성요소들을 포함할 수 있다. 추가적으로 또는 대안적으로, 환경(100) 내의 어떤 하나의 기기는 환경(100)(또는 기기들의 임의의 그룹) 내의 하나 이상의 다른 기기들에 의해 수행되는 것으로 설명된 기능들을 수행할 수 있다.

[0036] 도 2a 및 2b는 유닛(115)의 예시적인 구성요소를 도시하는 블록도이다.

[0037] 도 2a에 도시된 바와 같이, 유닛(115)은 컨트롤러(210)와 하나 이상의 주변 기기들(230)을 포함할 수 있다. 컨트롤러(210)는 유닛(115)의 동작을 제어하거나, 다른 유닛들(115)과 통신하거나, 관리 기기(130)와 통신하거나, 주변 기기들(230)을 제어할 수 있다. 주변 기기들(230)은 컨트롤러(210)에 정보를 제공하거나, 컨트롤러(210)에 의해 제어되거나, 아니면 컨트롤러(210)와 통신하는 기기들을 포함할 수 있다. 일 실시예에서, 주변 기기들(230)은 어떠한 종류의 보안 기기를 포함할 수 있다. 예를 들어, 주변 기기들(230)은 판독 기기(240), 잠금 기기(250), 센서(260)(예: 카메라) 및/또는 액츄에이터(270)와 같은 보안 기기들을 포함할 수 있다.

[0038] 도 2b에 도시된 바와 같이, 컨트롤러(210)는 버스(212), 프로세서(214), 메모리(216), 네트워크 인터페이스(218), 주변 인터페이스(220) 및 하우징(222)을 포함할 수 있다. 버스(212)는 컨트롤러(210)의 구성요소들 간에 통신을 허용하는 경로를 포함한다. 프로세서(214)는 단일 코어 프로세서, 다중 코어 프로세서, 마이크로 프로세서, 래치 기반의 프로세서 및/또는 인스트럭션들을 해석하고 실행하는 프로세싱 로직(또는 프로세서들, 마이크로 프로세서들 및/또는 프로세싱 로직들의 집합) 중 임의의 종류를 포함할 수 있다. 다른 실시예들에서, 프로세서(214)는 IC(integrated circuit), ASIC(application-specific integrated circuit), FPGA(field-programmable gate array) 및/또는 다른 종류의 IC나 프로세싱 로직을 포함할 수 있다. 프로세서(214)는 각각 다른 기능을 수행하는 다중 프로세서들(예를 들어, 동일하거나 분리된 칩들 내의 프로세서들)을 포함할 수 있다. 예를 들어, 프로세서(214)는 마이크로프로세서와 더불어, 데이터를 암호화 및 복호화하기 위한 전용의 회로(예: ASIC)를 포함할 수 있다.

[0039] 메모리(216)는 정보, 데이터 및/또는 인스트럭션들을 저장한다. 메모리(216)는 동적, 휘발성 및/또는 비휘발성 저장 기기의 종류를 포함할 수 있다. 메모리(216)는 프로세서(214)에 의한 실행을 위해 인스트럭션들을 저장하

거나, 프로세서(214)에 의한 사용을 위해 정보를 저장할 수 있다. 예를 들어, 메모리(216)는 RAM(random access memory) 또는 다른 종류의 동적 저장 소자, ROM(read-only memory) 기기 또는 다른 종류의 정적 저장 소자, CAM(content addressable memory), 자력 및/또는 광학 기록 메모리 소자와 그에 대응되는 드라이브(예: 하드 디스크 드라이브, 광학 드라이브 등), 및/또는 플래시 메모리와 같이 제거 가능한 형태의 메모리를 포함할 수 있다.

[0040] 네트워크 인터페이스(218)는 컨트롤러(210)가, 유선 통신 링크들 (예: 전도성 와이어, 트위스트 페어 케이블, 동축 케이블, 전송선, 광학 케이블 및/또는 웨이브 가이드 등), 무선 통신 링크들(RF, 적외선 및/또는 시각적 옵틱스), 또는 무선 및 유선 통신 링크들의 조합을 통해, 다른 기기들 및/또 시스템들과 통신(데이터의 송신 및/또는 수신)할 수 있게 하는 트랜시버(예: 송신기 및/또는 수신기)를 포함한다. 네트워크 인터페이스(218)는 기저대역 신호들을 RF 신호들로 변환하거나, RF 신호들을 기저대역 신호들로 변환하는 수신기를 포함할 수 있다. 네트워크 인터페이스(218)는 RF 신호들의 송수신을 위해 안테나에 결합될 수 있다.

[0041] 네트워크 인터페이스(218)는 입력 및/또는 출력 포트들, 입력 및/또는 출력 시스템들, 및/또는 다른 기기들로의 데이터의 전송을 용이하게 하는 다른 입력 및 출력 구성요소들을 포함하는 논리적 구성요소(logical component)를 포함할 수 있다. 예를 들면, 네트워크 인터페이스(218)는 유선 통신을 위한 네트워크 인터페이스 카드(예: 이더넷 카드) 및/또는 무선 통신을 위한 무선 네트워크 인터페이스 카드(예: WiFi)를 포함할 수 있다. 네트워크 인터페이스(218)는 케이블을 통한 통신을 위한 USB(universal serial bus) 포트, 블루투스 무선 인터페이스, RFID(radiofrequency identification) 인터페이스, NFC(near-field communications) 무선 인터페이스 및/또는 하나의 형태에서 다른 형태로 변환하는 다른 종류의 인터페이스를 포함할 수 있다.

[0042] 주변 인터페이스(220)는 하나 이상의 주변 기기들(230)과 통신하도록 구성될 수 있다. 예를 들어, 주변 인터페이스(220)는, 입력 및/또는 출력 포트들, 입력 및/또는 출력 시스템들, 및/또는 주변 기기들(230)로의 데이터 전송을 용이하게 하는 다른 입력 및 출력 구성요소들을 포함하는 하나 이상의 논리적 구성요소들을 포함할 수 있다. 예를 들면, 주변 인터페이스(220)는 직렬 주변기기 인터페이스 버스(Serial Peripheral Interface Bus) 프로토콜(예: 위건드(Wiegand) 프로토콜및/또는 RS-485 프로토콜)를 사용하여 주변 기기들(230)과 통신할 수 있다. 다른 실시예로서, 주변 인터페이스(220)는 다른 종류의 프로토콜을 사용할 수 있다. 일 실시예에서, 네트워크 인터페이스(218)는 주변 기기들(230)을 컨트롤러(210)에 결합하기 위한 주변 인터페이스로서 동작할 수도 있다.

[0043] 하우징(222)은 컨트롤러(210)의 구성요소들을 수용하고 상기 환경으로부터 컨트롤러(210)의 구성요소들을 보호할 수 있다. 일 실시예에서, 하우징(222)은 하나 이상의 주변 기기들(230)을 포함할 수 있다. 다른 실시예에서, 하우징(222)은 관리 기기(130)를 포함할 수 있다. 하나 이상의 시스템 유닛(115) 및/또는 하나 이상의 컨트롤러(210) 내에서, 하우징(222)은 다른 시스템 유닛(115) 및/또는 컨트롤러들(210)로부터, 하나의 시스템 유닛(115) 및/또는 컨트롤러(210)의 경계들을 정의할 수 있다.

[0044] 이하에서 설명되는 바와 같이, 컨트롤러(210)는 하나 이상의 기기들 상에 하나 이상의 서비스들에 대한 사용자 크리덴셜들을 배포하는 것과 관련된 동작들을 수행할 수 있다. 컨트롤러(210)는 ASIC의 하드 와이어 회로의 결과로서 이러한 동작들을 수행할 수 있다. 컨트롤러(210)는 대안적으로, 메모리(216)와 같은 컴퓨터로 읽을 수 있는 매체에 포함된 소프트웨어 인스트럭션들을 실행하는 프로세서(214)에 응답하여, 이러한 동작들을 수행할 수도 있다. 컴퓨터로 읽을 수 있는 매체는 비-임시적(non-transitory) 메모리 기기를 포함할 수 있다. 메모리(216)는 단일의 물리적 메모리 기기 내에 구현되거나, 다중 물리적 메모리 기기들에 걸쳐 분포될 수 있다. 상기 소프트웨어 인스트럭션들은 다른 컴퓨터로 읽을 수 있는 매체나 다른 기기들로부터 메모리(216) 내로 읽혀질 수 있다. 상기 메모리(216) 내에 포함된 소프트웨어 인스트럭션들은 프로세서(214)가 여기에 기술된 프로세스들을 수행하도록 유도할 수 있다. 따라서, 여기에 설명된 구현들은 하드웨어 회로 및 소프트웨어의 특정 조합에 한정되지 않는다.

[0045] 주변 기기들(230)로 돌아가면, 판독 기기(240)는 사용자로부터 크리덴셜들을 읽고 상기 크리덴셜들을 컨트롤러(210)에 제공하는 기기를 포함할 수 있다. 예를 들어, 판독 기기(240)는 사용자로부터 PIN(alphanumeric personal identification number)을 수신하도록 구성된 키보드; RFID 태그와 같은, 자력 스트립 또는 다른 종류의 저장 기기 상에 카드 코드를 저장하는 카드를 설정하는 카드 판독기; 사용자의 지문을 인식하도록 구성된 지문 판독기; 사용자의 홍채를 판독하도록 구성된 홍채 판독기; 사용자의 음성 특성을 기록하도록 구성된 마이크로폰 및 음성 특성 식별기; NFC 판독기; 얼굴 인식 소프트웨어와 관련된 카메라; 및/또는 다른 종류의 판독 기기를 포함할 수 있다. 판독 기기(240)는 크리덴셜들을 제공할 수 있는 임의의 종류의 보안 기기를 포함할 수

있고, 하나 이상의 센서 기기들(센서(260)을 참조하여 설명되는 어떠한 센서 기기)을 포함할 수 있다. 예를 들어, 판독 기기(240)는 얼굴 인식을 위해 사용되는 카메라 및/또는 음성 인식을 위해 사용되는 마이크로폰을 포함할 수 있다. 이 경우에, 사용자의 음성 또는 얼굴은 예를 들어, 상기 사용자의 크리덴셜들이 될 수 있다.

[0046] 잠금 기기(250)는 컨트롤러(210)에 의해 제어되는 자물쇠(lock)를 포함할 수 있다. 잠금 기기(250)는 도어(예: 도어를 열고 닫는 것을 방지함), 윈도우, HVAC 벤트 및/또는 보안 영역에 개방된 다른 종류의 접근을 잠글 수 있다. 예를 들어, 잠금 기기(250)는 전자기 자물쇠; 컨트롤러(210)에 의해 제어되는 모터를 갖는 기계적 자물쇠; 전자기계적 자물쇠; 및/또는 다른 종류의 자물쇠를 포함할 수 있다.

[0047] 센서(260)는 센싱 기기를 포함할 수 있다. 예를 들면, 센서(260)는 도어가 열려있는지 닫혀있는지를 감지하기 위한 도어 센서; 가시광 감시 기기(예: 카메라), 적외선 감시 기기, 열 특성 감지 기기, 오디오 감시 기기(예: 마이크로폰), 및/또는 다른 종류의 감시 기기; 모션 센서, 열 센서, 압력 센서 및/또는 다른 종류의 알람 센서와 같은 알람 센서; 유닛(115) 내에 위치하는 위치 센서와 같은 탬퍼(tamper) 센서; 유닛(115)와 관련된 보안 영역 내에 위치하는 "탈출 요청" 버튼; 및/또는 다른 종류의 센서 기기를 포함할 수 있다. 아래의 예에서, 센서(260)는 "카메라(260)"로 언급될 수 있다.

[0048] 액츄에이터(270)는 액츄에이터 기기를 포함할 수 있다. 일 예로서, 액츄에이터(270)는 조명 기기를 제어할 수 있다. 다른 예로서, 액츄에이터(270)는 침입자 알람 활성화기; 메시지를 재생하거나 알람 신호들을 생성하는 스피커; 디스플레이 기기; 센서(260)를 이동시키는 모터(예를 들어, 카메라나 다른 감시 기기의 시야를 제어함); 도어, 윈도우, HVAC 벤트 및/또는 보안 영역과 관련된 다른 개방부를 열거나 닫기 위한 모터; 잠금 기기(250)를 잠금 또는 비잠금 위치에 놓여지게 하기 위한 모터; 소화 기기; 및/또는 다른 종류의 액츄에이터 기기를 포함할 수 있다.

[0049] 도 2a 및 2b가 유닛(115)의 예시적인 구성요소들을 보여주지만, 다른 실시예들에서, 유닛(115)은 도 2a, 2b에 도시된 것보다 더 적은 구성요소들, 다른 구성요소들, 추가적인 구성요소들 또는 다르게 배치된 구성요소들을 포함할 수 있다. 예를 들어, 단일의 판독 기기(240), 단일의 잠금 기기(250), 단일의 센서(260) 및 단일의 액츄에이터(270)가 도 2a에 도시되어 있지만, 실제로 주변 기기들(230)은 다중 판독 기기들(240), 다중 잠금 기기들(250), 다중 센서들(260) 및/또는 다중 액츄에이터들(270)을 포함할 수 있다. 주변 기기들(230)는 도 2a에 도시된 하나 이상의 기기들을 포함하지 않을 수도 있다. 추가적으로 또는 대안적으로, 유닛(115)의 구성요소(또는 구성요소들의 어떠한 그룹)는 유닛(115)의 하나 이상의 구성요소들에 의해 수행되는 것으로 기술된 태스크나 태스크들을 수행할 수 있다.

[0050] 또한, 예시적인 분산 제어 시스템(110)이 물리적 제어 분산 제어 시스템을 포함하지만, 다른 구현 예들은 물리적 접근 이외의 시스템들을 제어할 수 있다. 반면에, 분산 제어 시스템(110)은, 도어를 개폐하거나 빌딩 또는 시설에 대한 물리적 접근을 제어하는 제어 시스템과 같은, 어떠한 종류의 물리적 접근 제어 시스템들(예: 동작적 환경에서)을 포함할 수 있다. 분산 제어 시스템(110)은 팬(fan)을 제어하거나, 빌딩 관리 시스템(예: 인증 실패, 인증 성공 등)에서 알람을 발생하거나, 산업 자동화 시스템에서 로봇 아암(arm)을 제거하기 위한 시스템을 포함할 수도 있다.

[0051] 도 3a는 시스템 유닛(115)의 예시적인 기능적 계층들을 도시하는 블록도이다.

[0052] 도 3a에 도시된 바와 같이, 유닛(115)은 API(application program interface) 계층(310), 어플리케이션 계층(320), 분배 계층(340) 및 스토리지 계층(350)을 포함할 수 있다.

[0053] API 계층(310)은 예컨대, 관리 기기(130)와 통신하도록 구성된 API를 포함한다. 관리자가 관리자 기기(130)를 사용하여 유닛(115)에 로그인할 때, API 계층(310)은 상기 관리자를 인증하기 위해 관리자 기기(130)와 통신할 수 있다. 다른 실시예로서, API 계층(310)은 유닛(115)의 설정을 변경하기 위해 관리자 기기(130)와 통신할 수 있다. API 계층(310)은 관리자 기기(130)로부터 데이터를 수신하고 상기 데이터를 분배 계층(340) 및/또는 스토리지 계층(350)에 제공할 수 있다. API 계층(310)은 어플리케이션 계층(320)에 어플리케이션을 설치하기 위해 관리자 기기(130)와 통신할 수도 있다. API 계층(310)은 다른 관리자 종류들을 처리하도록 구성될 수 있다. 예를 들어, API 계층(310)은 웹 서비스 관리자, 리눅스 관리자, ONVIF(Open Network Video Interface Forum) 관리자 및/또는 다른 종류의 API를 처리하는 API를 포함할 수 있다.

[0054] 어플리케이션 계층(320)은 유닛(115) 내에 설치된 하나 이상의 어플리케이션들을 포함한다. 어플리케이션들은 제어 로직 어플리케이션, 도어들을 개폐하기 위한 도어 제어 어플리케이션, 다른 어플리케이션들 사이에서 사용자 크리덴셜들을 수신하는 판독기 제어 어플리케이션을 포함할 수 있다. 어플리케이션들은 도 3b를 참조하여 보

다 자세히 설명된다.

[0055] 배포 계층(340)은 유닛들(115)와 관련된 하나 이상의 분산 데이터세트들을 관리할 수 있다. 예를 들어, 분배 계층(340)은 데이터세트들의 분산을 위해, P2P(peer-to-peer) 네트워크 내에서 컨트롤러들(210)을 연결할 수 있다. 분배 계층(340)은 특정 합의-기반의 분산된 데이터세트의 변경에 관한 합의를 수립하기 위한 프로토콜(예: PAXOS 프로토콜)을 사용할 수 있다. 예로서, 분배 계층(340)은 상기 분산된 데이터세트와 관련된 다른 시스템 유닛들(115)에 대한 변경 제안을 전송하고, 상기 다른 시스템 유닛들(115)로부터 상기 변경에 대한 정족수를 수신할 수 있다. 다른 예로서, 분배 계층(340)은 다른 유닛(115)로부터 수신된 제안에 대해 투표할 수 있다. 또 다른 실시예로서, 분배 계층(340)은 상기 변경에 대한 투표 없이, 상기 변경에 대한 합의에 도달하였다는 표지를 수신할 수 있다. 변경에 대한 합의의 표지가 수신되면, 분배 계층(340)은 상기 분산된 데이터세트의 로컬 사본에 변경을 가할 수 있다. 분배 계층(340)은 네트워크(120)를 통해 다른 유닛들(115)과의 보안 연결(예: TLS(Transport Layer Security) 연결)을 유지할 수 있다.

[0056] 스토리지 계층(350)은 유닛(115)과 관련된 하나 이상의 데이터세트들을 저장할 수 있다. 스토리지 계층(350)에 저장된 데이터세트는 로컬 데이터세트에 대응되거나 분산된 데이터세트에 대응될 수 있다. 로컬 데이터세트는 상기 로컬 데이터세트를 저장하는 특정 유닛(115)와 관련된(또는 특정 유닛(115)에만 관련된) 정보를 저장할 수 있다. 분산된 데이터세트는 상기 분산된 데이터세트와 관련된 다른 시스템 유닛들(115)과 관련된 정보를 저장할 수 있다.

[0057] 도 3b는 어플리케이션 계층(320) 및 스토리지 계층(350)에 대해 보다 상세히 제공되는, 컨트롤러(310)의 예시적인 기능적 구성요소들의 블록도이다.

[0058] 도 3b에 보여진 바와 같이, 어플리케이션 계층(320)은 제어 로직 어플리케이션(322)(내지 "제어 로직(322)"), 관리자 인증 로직(323), 도어 제어 어플리케이션(324), 판독기 제어 어플리케이션(326), 이벤트 처리 어플리케이션(328), 스케쥴 처리 어플리케이션(330), 제1 서비스 어플리케이션(332)(또는 "제1 서비스(332)"), 및/또는 제2 서비스 어플리케이션(334)(또는 "제2 서비스(334)")를 포함할 수 있다. 다른 어플리케이션들은 예를 들면, 알람 및 제어 어플리케이션들을 포함할 수 있다. 이러한 기능적 구성요소들을 처리하는 로직은 컨트롤러(210) 및/또는 시스템 유닛(115)의 다른 부분들을 포함할 수 있다. 즉, 이러한 기능적 구성요소들을 처리하는 로직은 예를 들면, 단일의 하드웨어 모듈에 연결되지 않을 수 있다.

[0059] 제어 로직(322)은 수신된 크리덴셜들과 저장된 접근 규칙들에 기초하여, 사용자에 대한 물리적 접근을 허용할지를 판단할 수 있다. 관리 로직(323)는 관리자에 대한 접근(예: 원격 로그인과 같은 원격 접근)을 허용하고 다른 관리자 프로세서들을 제공할 수 있다. 예를 들면, 관리 로직(323)은 크리덴셜들(예: 사용자명 및 패스워드)에 기초하여 관리자를 인증할 수 있고, 관리자가 사용자 크리덴셜들에 접근하고 업데이트할 수 있도록 권한을 부여한다(예: 다른 관리자들 및/또는 물리적 접근이 허가되기를 원하는 사용자들에 대해). 일 실시예에서, 관리 로직(323)은 관리자가 특정 시스템 유닛(115)에 대한 사용자 크리덴셜들에 접근하고 업데이트하도록 인증하거나, 다른 또는 모든 시스템 유닛들(115)에 대한 크리덴셜들을 업데이트 할 수 있도록 권한을 부여할 수 있다. 관리 로직(323)의 이러한 기능들은 도 3c을 참조하여 아래에서 설명된다.

[0060] 도어 제어 어플리케이션(324)은 하나 이상의 도어들 및/또는 관련 잠금 기기들(250)을 제어할 수 있다. 예를 들면, 도어 제어 어플리케이션(324)은 도어가 열렸는지 닫혔는지, 및/또는 잠겼는지 잠기지 않았는지를 판단할 수 있고, 하나 이상의 기기가 상기 도어를 개폐하거나 잠금 또는 잠금 해제할 수 있도록 할 수 있다. 판독기 제어 어플리케이션(326)은 하나 이상의 판독 기기들(240)을 제어할 수 있고, 상기 하나 이상의 판독 기기들(240)로부터 수신된 크리덴셜들을 획득하고 처리할 수 있다. 이벤트 처리 어플리케이션(328)은 도어 열림 이벤트, 알람 이벤트, 센서 이벤트 및/또는 다른 종류의 로그 이벤트와 같은, 유닛(115)에 의해 기록되는 이벤트들을 처리할 수 있다. 이벤트 처리 어플리케이션(328)은 보고 및/또는 알람을 생성하고 상기 보고 및/또는 알람을 관리자 기기(130)(및/또는 다른 유닛들(115)과 같은, 다른 지정된 기기)에 전송할 수 있다. 스케쥴 처리 어플리케이션(330)은 유닛(115)와 관련된 하나 이상의 일정들을 관리할 수 있다. 예를 들어, 사용자들의 특정 그룹에 대한 접근 규칙들은 하루 중 특정한 시간에 기초하여 변경될 수 있다.

[0061] 제1 서비스 어플리케이션(332) 및 제2 서비스 어플리케이션(334)은 서비스들을 인증된 관리자들에게 제공할 수 있다. 서비스의 예들은, SSH(secure shell) 서버, FTP(file transfer protocol) 서버, RDP(remote desktop protocol) 서버, VPN(virtual private network) 서버, VNC(virtual network channel) 서버 등을 포함한다. 각각의 컨트롤러(210)는 서비스 어플리케이션들의 다른 세트를 포함한다. 예를 들어, 하나의 컨트롤러(210)는 SSH 서버 및 RDP 서버를 제공하고, 다른 컨트롤러(210)는 SSH 서버 및 VPN 서버를 제공할 수 있다.

[0062] 도 3b에 보여진 바와 같이, 스토리지 계층(350)은 설정 데이터(352), 관리자 크리덴셜 DB (354), 제1 서비스 크리덴셜 DB (356), 제2 서비스 크리덴셜 DB (358) 및/또는 사용자 크리덴셜 DB (360)를 저장할 수 있다.

[0063] 설정 데이터(352)는 컨트롤러(210), 상기 컨트롤러(210)에 연결된 주변 기기들(230), 어플리케이션 계층(320)에 설치된 어플리케이션의 하드웨어 설정, 또는 다른 종류의 설정 정보와 같은, 특정 유닛(115)과 관련된 설정 데이터를 저장한다. 일 실시예에서, 설정 데이터(352)는 그것이 특정 컨트롤러(210)에 한정된 것일 때, 다른 컨트롤러(210)에는 배포되지 않는다. 다른 실시예들에서, 설정 데이터(352)는 다른 컨트롤러들(210)에 사용되는 설정 데이터(352) 없이 다른 컨트롤러들(210)에 대한 백업으로서 배포될 수 있다.

[0064] 관리자 크리덴셜 DB (352)는 시스템 유닛(115)을 예컨대, 원격 로그인으로 관리할 수 있는 인증된 사용자들에 대한 크리덴셜들(예: 사용자명 및 패스워드)을 저장한다. 관리자 크리덴셜 DB (354)는 도 7a를 참조하여 아래에서 설명된다. 일 실시예에서, 관리자 크리덴셜 DB (354)는 다른 컨트롤러들(210) 간에 배포되어, 동일한 관리자들이 컨트롤러들(210) 또는 유닛들(115)로부터 시스템(110)을 관리할 수 있도록 허용한다.

[0065] 제1 서비스 크리덴셜 DB (356)(또는 제1 변환된 크리덴셜 DB (356)) 및 제2 서비스 크리덴셜 DB (358)(또는 제2 변환된 크리덴셜 DB (358))는 컨트롤러(210)에 의해 제공되는 서비스들(예: 제1 서비스(332) 또는 제2 서비스(334))에 접근하는 사용자들(예: 추가적 관리자들)을 인증하기 위한 크리덴셜들(예: 사용자명 및 패스워드)을 저장한다. 제1 서비스(332)는 예를 들어, 제1 서비스(332)에 접근을 시도하는 사용자를 인증하기 위해 제1 서비스 크리덴셜 DB (356)를 사용할 수 있다. 마찬가지로, 제2 서비스(334)는 제2 서비스(334)에 접근을 시도하는 사용자를 인증하기 위해 제2 서비스 크리덴셜 DB (358)를 사용할 수 있다.

[0066] 일 실시예에서, DB들(356 및/또는 358) 내의 크리덴셜들은 일반 텍스트로 저장되지 않을 수 있다(예를 들어, 상기 크리덴셜들을 노출하지 않는 비암호화 포맷 또는 방식). 이 실시예에서, 크리덴셜 DB들(356 및/또는 358)은 변환된 사용자 크리덴셜들을 저장할 수 있다. 예를 들어, 하나의 실시예에서, 제1 서비스 크리덴셜 DB (356)는 암호 일방향 함수(cryptographic one-way function)(예: 해쉬)으로 변환된 크리덴셜들을 저장할 수 있다. 이 실시예에서, 제1 서비스 크리덴셜 DB (356)는 상기 사용자명과 대응되는 패스워드의 해쉬를 저장할 수 있다. 다른 실시예로서, 제1 서비스 크리덴셜 DB (356)는 상기 사용자명 및 대응되는 패스워드의 솔티드 해쉬(salted hash)를 저장할 수 있다. 제1 서비스 크리덴셜 DB (356) 및 제2 서비스 크리덴셜 DB (358)는 도 7d 내지 7g를 참조하여 이하에서 설명된다.

[0067] 사용자 크리덴셜 DB (360)는 시스템 유닛(115)에 의해 제공되는 서비스들(예: 제1 서비스(332) 및/또는 제2 서비스(334))에 접근할 수 있는 사용자의 크리덴셜들(예: 사용자명과 패스워드)을 저장할 수 있다. 일 실시예에서, 사용자 크리덴셜 DB (360)는 서비스 크리덴셜 DB들(예: 제1 서비스 크리덴셜 DB (356) 및/또는 제2 서비스 크리덴셜 DB (358))에 저장된 것과 동일한 사용자(또는 사용자들)에 대한 동일한 크리덴셜(또는 크리덴셜들)을 저장할 수 있다. 일 실시에에서, 사용자 크리덴셜 DB (360)는 크리덴셜 DB들(356, 358)과 다른 방식으로 크리덴셜들을 저장한다. 예를 들어, 사용자 크리덴셜 DB (360)는, 변환된 크리덴셜들을 저장하는 서비스 크리덴셜 DB들(356 및/또는 358)과는 반대로, 상기 크리덴셜들 자체를 노출하기 위한 방식으로 크리덴셜들을 저장할 수 있다. 일 실시예에서, 서비스 크리덴셜 DB들(356, 358)은 사용자 크리덴셜 DB (360)로부터 변환되거나 도출될 수 있다.

[0068] 도 3c는 관리 로직(323)의 예시적 구성요소들의 블록도인데, 상기 관리 로직(323)은 관리자 인증기(382), 사용자 크리덴셜 업데이트 로직(384), 변환된 크리덴셜 생성기(386) 및/또는 크리덴셜 변환 규칙 DB (388)을 포함할 수 있다. 관리자 인증기(382)는 컨트롤러(210)에 접속하려 하는 관리자들에 대한 크리덴셜들을 수신하고, 상기 크리덴셜들이 진짜인지를 판단하며, 컨트롤러(210)에 대한 접근(예를 들어, 사용자 크리덴셜 DB (360)를 편집하고 변경하는 능력을 포함함)을 인증할 수 있다. 사용자 크리덴셜 업데이트 로직(384)은 컨트롤러(210)의 서비스들의 사용자들과 관련된 크리덴셜들에 대한 변경들 및/또는 업데이트들을 (사용자 크리덴셜 DB (360)에 저장하기 위해 관리자로부터) 수신할 수 있다 변환된 크리덴셜 생성기(386)는 사용자 크리덴셜 DB (360)에 대한 변경들 및/또는 업데이트들에 기초하여, 서비스 크리덴셜 DB들(예: 제1 서비스 크리덴셜 DB (356) 및 제2 서비스 크리덴셜 DB (358))을 생성하거나 업데이트할 수 있다. 변환된 크리덴셜 생성기(386)는 크리덴셜 변환 규칙 DB (388)에 저장된 정보(예: 규칙들 및 기기에 특화된 정보)에 기초하여 크리덴셜들을 변환할 수 있다. 예를 들면, 규칙 DB (388)는 SSH 서비스에 대해, 패스워드는 로컬 머신의 하드웨어 주소(예: 기기에 특화된 정보 또는 MAC 주소)로 SHA-224 알고리즘을 사용하여 해쉬되어야 한다는 것을 나타낼 수 있다. 또한, 일 실시예에서, 규칙 DB (388)는 제어 시스템(110) 내의 다른 컨트롤러들(210)에 대한 규칙들 및 기기에 특화된 정보를 저장할 수 있다.

[0069] 도 3a, 3b 및 3c가 유닛(115)의 예시적인 기능적 구성요소들을 보여주지만, 다른 실시예들에서는, 유닛(115)가

도 3a, 3b 및 3c에 도시된 것과 달리 더 적은 구성요소들, 다른 구성요소들, 다르게 배치된 구성요소들 또는 추가적인 구성요소들을 포함할 수 있다. 또한, 유닛(115)의 상기 구성요소들(다른 구성요소들의 어떤 그룹) 중 어느 하나는 유닛(115)의 하나 이상의 다른 기능적 구성요소들에 의해 수행되는 것으로 설명된 기능들을 수행할 수 있다. 또한, 유닛(115)의 상기 기능적 구성요소들은 예를 들어, 하나 이상의 ASIC들의 하드-와이어 회로로 구현될 수 있다. 추가적으로 또는 대안적으로, 유닛(115)의 기능적 구성요소들은 메모리(216)로부터 인스트럭션들을 실행하는 프로세서(214)에 의해 구현될 수 있다.

[0070] 도 4는 유닛(115)의 예시적인 물리적 레이아웃(400)을 도시하는 평면도 이다.

[0071] 도 4에 도시된 바와 같이 물리적 레이아웃(400)은 벽(410), 도어(420), 컨트롤러(210), 판독 기기(240), 잠금 기기(250), 센서(260) 및 액츄에이터(270)를 포함할 수 있다.

[0072] 벽(410)은 빌딩 내의 방과 같은 보안 영역(440)을 둘러싼다. 도어(420)는 사용자의 보안 영역(440)으로의 접근을 제공한다. 이 실시예에서, 컨트롤러(210)는 보안 영역(440) 내부에 설치된다. 다른 실시예들에서, 컨트롤러(210)는 비보안 영역(450) 내에 설치될 수 있다. 판독 기기(240)는 보안 영역(440)의 외부에 설치되고, 잠금 기기(250)는 보안 영역(440) 내에서 벽(410) 및 도어(420)에까지 설치된다. 센서(260)는 예를 들면, 비보안 영역(450) 내에서 보안 영역(440)의 외부에 장착된 감시 기기이다. 액츄에이터(270)는 이 실시예에서, 상기 감시 기기의 시야를 제거하기 위해 사용되는 모터를 포함한다.

[0073] 사용자가 크리덴셜들을 판독 기기(240)(예를 들어, PIN을 입력하거나, 억세스 카드를 스캐닝 하거나, 홍채를 스캐닝 하는 등에 의해)에 입력할 때, 컨트롤러(210)는 사용자의 동일성을 인증하기 상기 크리덴셜들을 사용할 수 있고, 상기 사용자의 동일성 및 접근 규칙들에 기초하여 상기 사용자에 대한 접근을 허용할지를 판단하는 접근 규칙 테이블 내에서 룩업(lookup)을 수행할 수 있다. 컨트롤러(210)가 접근이 허용되어야 한다고 판단하면, 컨트롤러(210)는 도어(420)의 잠금을 해제하기 위해 잠금 기기(250)를 활성화하고, 사용자의 보안 영역(440)에 대한 접근을 허용한다.

[0074] 도 4는 물리적 레이아웃(400)의 예시적인 구성요소들을 보여주지만, 다른 실시예들에서, 물리적 레이아웃(400)은 도 4에 도시된 것과 달리 더 적은 구성요소들, 다른 구성요소들, 다르게 배치된 구성요소들 또는 추가적인 구성요소들을 포함할 수 있다. 추가적으로 또는 대안적으로, 물리적 레이아웃(400) 내의 어떤 하나의 구성요소(또는 구성요소들의 그룹)는 물리적 레이아웃(400)의 하나 이상의 다른 구성요소들에 의해 수행되는 것으로 설명되는 태스크 또는 태스크들을 수행할 수 있다.

[0075] 도 5는 제어 시스템(110)의 예시적인 물리적 레이아웃(500)을 도시하는 평면도이다.

[0076] 도 5에 도시된 바와 같이, 물리적 레이아웃(500)은 방들(520-A 내지 520-F)를 갖는 빌딩(510)을 포함할 수 있다. 이더넷 네트워크와 같은 로컬 네트워크(530)는, 시스템 유닛들(115-A 내지 115-F)를 상호 연결할 수 있다. 이 실시에에서, 시스템 유닛(115-A)은 방(520-A) 내부로 두 개의 도어를 제어한다; 시스템 유닛(115-B)는 방(520-B) 내부로 외부의 도어를 제어한다; 시스템 유닛(115-C)은 방(520-B)으로부터 (520-C)까지 하나의 도어를 제어한다; 시스템 유닛(115-D)는 방(520-C)에서 방(520-D)까지 하나의 도어를 제어한다; 시스템 유닛(115-E)은 방(520-D)에서 방(520-E)까지 하나의 도어를 제어한다; 그리고 유닛(520-F)은 방(520-F) 내부로 외부 도어를 제어한다.

[0077] 이 실시에에서, 시스템 유닛들(115-A 내지 115-F)은 중앙 제어 기기(예: 서버)를 포함하지 않고, 하나 이상의 분산된 데이트세트들을 포함할 수 있다. 예를 들어, 시스템 유닛들(115-A 내지 115-F)은 분산된 크리덴셜 테이블, 분산된 접근 규칙 데이블 및/또는 분산된 이벤트 로그를 유지할 수 있다. 관리자가 사용자를 추가하고 사용자와 관련된 크리덴셜들을 추가하기 위해, 시스템 유닛(115- A)으로 로그인하려고 관리 기기(130)를 사용한다고 가정한다. 그와 같이 추가된 크리덴셜들은 사용자가 접근하는 방들 내로 도어들을 제어하는 다른 시스템 유닛들(115)로 분산될 수 있다. 시스템 유닛(115-B)이 고장나면, 예를 들어, 시스템 유닛(115-B)에 의해 수집된 데이터는 상기 다른 시스템 유닛 내에 포함된 분산된 이벤트 로그의 결과로서 지속적으로 가용화될 수 있다.

[0078] 도 5에서, 각각의 유닛(115)은 컨트롤러(210)와 관련된다. 또한, 도 5의 실시예에서, 각각의 컨트롤러(210)는 다른 컨트롤러들(210)과 다른 위치(예: 다른 방(520))에 있다. 다른 구현 예들에서, 몇몇 컨트롤러들(210) 및 유닛들(115)은 다른 컨트롤러들 및 유닛들(115)과 다른 빌딩들, 다른 지리적 지역들, 다른 국가들, 다른 대륙들 등에 위치할 수 있다. 그것들의 다양한 위치에도 불구하고 일 실시예에서, 유닛들(115) 및 컨트롤러들(210)은 서로를 발견하고(또는 발견하기 위해 최선을 다하고), P2P 네트워크를 형성하며 데이트세트들을 배포할 수 있다.

[0079] 도 5는 물리적 레이아웃(500)의 예시적인 구성요소들을 보여주지만, 다른 구현 예들에서, 물리적 레이아웃(500)은 도 5에 도시된 것과 달리 더 적은 구성요소들, 다른 구성요소들, 다르게 배치된 구성요소들 또는 추가적인 구성요소들을 포함할 수 있다. 예를 들어, 다른 실시예에서, 중앙 제어 기기(예: 서버)는 하나 이상의 분산된 데이터세트들과 함께 사용될 수 있다. 추가적으로 또는 대안적으로, 물리적 레이아웃(500)의 적어도 하나의 구성요소들은 물리적 레이아웃(500)의 하나 이상의 구성요소들에 의해 수행되는 것으로 기술된 태스크나 태스크들을 수행할 수 있다.

[0080] 도 6은 관리 기기(130)의 예시적인 구성요소들을 도시하는 블록도이다.

[0081] 도 6에 나타난 바와 같이, 관리 기기(130)는 버스(610), 프로세서(620), 메모리(630), 입력 기기(640), 출력 기기(650) 및 통신 인터페이스(660)을 포함할 수 있다.

[0082] 버스(610)는 관리 기기(130)의 구성요소들 간의 통신을 허용하는 경로를 포함한다. 프로세서(620)는 단일 코어 프로세서, 다중 코어 프로세서, 마이크로 프로세서, 래치 기반의 프로세서 및/또는 인스트럭션들을 해석하고 실행하는 프로세싱 로직(또는 프로세서들, 마이크로 프로세서들 및/또는 프로세싱 로직들의 집합) 중 임의의 종류를 포함할 수 있다. 다른 실시예들에서, 프로세서(620)는 IC, ASIC, FPGA 및/또는 다른 종류의 IC나 프로세싱 로직을 포함할 수 있다.

[0083] 메모리(630)는 정보, 데이터 및/또는 인스트럭션들을 저장한다. 메모리(630)는 동적, 휘발성 및/또는 비휘발성 저장 기기의 종류를 포함할 수 있다. 메모리(630)는 프로세서(620)에 의한 실행을 위해 인스트럭션들을 저장하거나, 프로세서(620)에 의한 사용을 위해 정보를 저장할 수 있다. 예를 들어, 메모리(630)는 RAM 또는 다른 종류의 동적 저장 소자, ROM 기기 또는 다른 종류의 정적 저장 소자, CAM, 자력 및/또는 광학 기록 메모리 소자와 그에 대응되는 드라이브(예: 하드 디스크 드라이브, 광학 드라이브 등), 및/또는 플래시 메모리와 같이 제거 가능한 형태의 메모리를 포함할 수 있다.

[0084] 입력 기기(640)는 운전자가 정보를 관리 기기(130)에 입력하도록 허용한다. 입력 기기(640)는 예를 들어, 키보드, 마우스, 펜, 마이크로폰, 터치 스크린 디스플레이 등을 포함할 수 있다. 출력 기기(650)는 관리 기기의 운전자에게 정보를 출력할 수 있다. 출력 기기(650)는 디스플레이, 프린터, 스피커 및/또는 다른 종류의 출력 기기를 포함할 수 있다.

[0085] 통신 인터페이스(660)는 컨트롤러(210)가, 유선 통신 링크들, 무선 통신 링크들, 또는 무선 및 유선 통신 링크들의 조합을 통해, 다른 기기들 및/또 시스템들과 통신(데이터의 송신 및/또는 수신)할 수 있게 하는 트랜시버(예: 송신기 및/또는 수신기)를 포함할 수 있다. 통신 인터페이스(660)는 유선 통신을 위한 네트워크 인터페이스 카드(예: 이더넷 카드) 및/또는 무선 통신을 위한 무선 네트워크 인터페이스 카드(예: WiFi)를 포함할 수 있다.

[0086] 관리 기기(130)는 시스템(11) 내의 유닛들(115)을 관리하는 것과 관련된 동작들을 수행할 수 있다. 관리 기기(130)는 메모리(630)와 같은, 컴퓨터로 읽을 수 있는 매체에 포함된 소프트웨어 인스트럭션들을 실행하는 프로세서(620)에 대한 응답으로, 이러한 동작들을 수행할 수 있다. 메모리(630) 내에 포함된 소프트웨어 인스트럭션들은 프로세서(620)가 이러한 동작들을 수행할 수 있게 한다.

[0087] 위에서 언급된 바와 같이 컨트롤러(210)는 관리자가 상기 유닛(115)을 관리할 수 있도록 인증할 수 있다.

[0088] 도 7a는 일 실시예에서 이러한 목적을 위한 관리 크리덴셜 DB(354)를 도시하는 블록도이다. 관리자 크리덴셜 DB(354)는 관리자를 인증하기 위하여 사용되는 크리덴셜 정보와 더불어 사용자 크리덴셜 DB (360)를 복호화하기 위한 마스터 키(예: 암호화된 마스터 키)를 저장할 수 있다. 일 실시예에서, 상기 마스터 키는 제어 시스템(110) 내의 분산된 DB (들)을 복호화하기 위하여 사용될 수도 있다. "마스터"라는 용어는 여기에 설명된 다른 키들과 구별하기 위하여 사용된다.

[0089] 도 7a에 도시된 바와 같이, 관리자 크리덴셜 DB (354)는 관리자 사용자명 필드(702), 암호화된 패스워드 필드(704) 및 암호화된 마스터 키 필드(706)를 포함할 수 있다. 관리자 사용자명 필드(702)는 상기 관리자의 사용자명을 저장한다. 예를 들어, 도 7a의 관리자 크리덴셜 DB (354)는 두 개의 관리자 사용자명(admin 1 및 admin2)을 보여준다. 다수의 관리자 사용자명도 관리자 크리덴셜 DB (354) 내에 리스트될 수 있다(즉, 다수의 레코드들 또는 행들이 관리 크리덴셜 DB (354)에 나타날 수 있다).

[0090] 암호화된 패스워드 필드(704)는 대응되는 사용자명을 위한 패스워드를 저장한다. 이 실시예에서, 필드(704) 내의 패스워드는 암호화된 마스터 키 필드(706) 내에 저장된 마스터 키로 암호화되어 있다. 다른 실시예들에서,

패스워드 필드(704)는 비암호화 포맷으로 되거나 상기 마스터 키와 다른 키로 암호화된 대응되는 패스워드를 저장할 수 있다. 필드(704)는 도 7a에서 암호화된 패스워드를 보여주기 보다는, 상기 암호화된 패스워드가 생성되는 함수 C(오퍼랜드 1(operand1), 오퍼랜드 2(operand2))를 보여준다. 함수 C는 암호화 키로서 오퍼랜드 2를 사용하여 오퍼랜드 1을 암호화한다. 함수 C는 어떠한 다른 암호화 함수가 될 수 있다. 예를 들면, 패스워드 필드(704)는 제1 함수(C1)를 사용하여 마스터 키로 암호화될 수 있다.

[0091] 암호화된 마스터 키 필드(706)는 상기 암호화된 마스터 키를 저장한다. 이 실시예에서, 마스터 키는 대응되는 관리자의 패스워드로 암호화되어 있다. 관리자 크리덴셜 DB (354)는 도 8c를 참조하여 이하에서 설명된다. 상기 마스터 키 필드(706)는 제2 함수(C2)를 사용하여 상기 패스워드로 암호화될 수 있다. 일 실시예에서, 프로세서(214)는 컨트롤러(210) 내의 다른 프로세서들에 대해 외부에 있는 전용 회로(예: ASIC) 내에서 함수 C를 수행한다.

[0092] 관리자 크리덴셜 DB (354)는 도 7a에 도시된 것보다 더 많거나, 더 적거나 다른 필드들을 포함할 수 있다. 예를 들어, 일 실시예에서, 관리자 사용자명 필드(702)는 생략될 수 있다. 다른 실시예에서, 관리자 크리덴셜 DB (354) 내에서 저장되거나 사용되는 크리덴셜은, 사용자명 및 패스워드와 다른 또는 이에 추가된 종류의 크리덴셜들을 포함할 수 있다. 예를 들어, 크리덴셜은 생체정보 크리덴셜(예: 지문 또는 홍채 스캔)을 포함할 수 있다.

[0093] 이상에서 언급된 바와 같이, 관리자는 사용자 크리덴셜 DB (360)를 업데이트하는 기능을 포함하는 관리 유닛(115)을 관리하기 위해 컨트롤러(210)에 로그인할 수 있다. 사용자 크리덴셜 DB는 다른 사용자들 또는 관리자들이 컨트롤러(210)에 의해 제공된 서비스들에 접근하기 위한 크리덴셜들을 저장한다. 도 7b 및 7c는 일 실시예에서 예시적인 사용자 크리덴셜 DB (예: 2개의 다른 시간에서의 사용자 크리덴셜 DB (360))의 블록도이다. 사용자 크리덴셜 DB (360)는 사용자명 필드(742), 서비스 필드(744), 기기 필드(746) 및/또는 크리덴셜 필드(748)를 포함할 수 있다. 이러한 필드들은 아래에서 설명된다.

[0094] 사용자명 필드(742)는 제1 서비스(332) 및 제2 서비스(334)와 같은, 컨트롤러(210) 내의 서비스들에 접근하도록 인증된 사용자를 식별한다. 사용자 크리덴셜 DB (360)(도 7b에 도시됨)에서, 사용자명은 Magnus 및 Sabina이다. 어떠한 수의 사용자명도 가능하다(예: 다수의 엔트리들 및 레코드들).

[0095] 서비스 필드(744)는 대응되는 사용자명의 접근이 허용되는 서비스들을 식별한다(예를 들어, 기기 필드(746)에서 식별된 기기 상의 크리덴셜 필드(748) 내에서 식별된 크리덴셜을 이용하여). 서비스 필드(744)에서 식별된 서비스들은 SSH 서버("SSH") 및 VPN 서버("VPN")를 포함한다. 어떠한 수의 서비스들도 어떠한 컨트롤러들(210)에 의해 제공될 수 있다.

[0096] 기기 필드(746)는 대응되는 사용자명 필드(742)에 식별된 사용자들에게, 서비스 필드(744)에 식별된 서비스를 제공하는 기기들(예: 컨트롤러(210)을 식별한다. 이상에서 언급된 바와 같이, 모든 컨트롤러들(210)이 동일한 (또는 심지어 임의의) 서비스들을 제공할 수 있는 것은 아니다. 또한, 몇몇 기기들에 대한 몇몇 서비스들은 예를 들어, 크리덴셜 필드(748)에 나열된 크리덴셜들과 관련되지 않을 수 있다. 예를 들어, 크리덴셜 필드(748) 내의 크리덴셜이 대응되는 사용자명 및 대응되는 서비스를 갖는 모든 기기들과 관련되어야 한다면, 기기 필드(746)는 "모두"를 식별할 수 있다. 크리덴셜 필드(748)에 저장된 상기 크리덴셜이 특정 기기(예: 카메라(260)) 내에서 대응되는 서비스 및 대응되는 사용자명과 관련되지 않아야 한다면, 기기 필드(746)는 상기 기기를 배제할 수 있다(예: "카메라(260) 아님"). 기기 필드(746)는 판독기(240), 자물쇠(250) 및 액츄에이터(270)와 같이, 개별적으로 기기들을 식별할 수 있다.

[0097] 크리덴셜 필드(748)는 대응되는 기기 또는 기기들(예: 기기 필드(746)에서 식별된 기기) 상에서 대응되는 서비스 또는 서비스들(예: 서비스 필드(744)에서 식별된 서비스)에 대해 대응되는 사용자(예: 사용자명 필드(742)에서 식별된 사용자)를 인증하기 위하여 사용되는 크리덴셜을 저장한다.

[0098] 일 실시예에서, 단일의 또는 동일한 크리덴셜(크리덴셜 필드(748)에서 식별됨) 및/또는 단일의 또는 동일한 사용자명(사용자명 필드(742)에서 식별됨)은, 하나 이상의 기기들(기기 필드(746)에서 식별됨)에 걸쳐, 다중 서비스들(서비스 필드(744)에서 식별됨)과 관련될 수 있다. 일 실시예에서, 단일의 또는 동일한 크리덴셜(크리덴셜 필드(748)에서 식별됨) 및/또는 단일의 또는 동일한 사용자명(사용자명 필드(742)에서 식별됨)은, 하나 이상의 서비스들(서비스 필드(744)에서 식별됨)에 걸쳐, 다중 기기들(기기 필드(746)에서 식별됨)과 관련될 수 있다.

[0099] 다른 실시예에서, 크리덴셜(크리덴셜 필드(748)에서 정의됨)(및 대응되는 패스워드)은 네트워크 내의 모든 기기들(예: 제어 시스템(110)과 같은 분산된 물리적 접근 제어 시스템)과 관련될 수 있다. 대안적으로, 크리덴셜(크

리덴셜 필드(748)에서 정의됨)(및 대응되는 패스워드)는 네트워크 내의 모든 기기들보다 적은 기기들(예: 카메라(260) 아님)과 관련될 수 있다. 즉, 몇몇 컨트롤러(210)는 다중 기기들 및/또는 다중 서비스들에 걸쳐, 크리덴셜과 관련되는 것(크리덴셜 필드(748)에서 식별되는 것)으로부터 배제될 수 있다.

[0100] 크리덴셜 필드(748)는 변환되지 않은 방식으로 크리덴셜을 저장할 수 있다. 예를 들어, 상기 크리덴셜이 패스워드이면, 상기 패스워드는 사용자에 의해 입력될 때 저장될 수 있다. 크리덴셜 필드(748)는 암호화된 포맷으로 상기 크리덴셜을 저장할 수도 있지만, 일 실시예에서는 비변환된 크리덴셜(예: 바이젝티브(bijective) 암호화 기능)을 노출하기 위해 복호화될 수 있는 포맷으로 상기 크리덴셜을 저장할 수 있다. 또 다른 실시예에서, 크리덴셜 필드(748)는 예를 들어, 모든 컨트롤러들(210)에 의해 제공되는 모든 서비스들에 대해, 모든 관련된 변환들을 포함하는, 하나 이상의 변환된 포맷들로 상기 크리덴셜을 저장할 수 있다.

[0101] 도 8b에 관하여 아래의 예에서 설명되는 바와 같이, 사용자 크리덴셜 DB (360)(도 7b에 도시됨)는 사용자 크리덴셜 DB (360')(도 7c에 도시됨)를 생성하기 위하여 업데이트된다. 업데이트된 사용자 크리덴셜 DB (360')에 대한 변경(사용자 크리덴셜 DB (360)와 비교할 때)은, 볼드체 및 화살표들로 도시된다. 예를 들어, 업데이트된 사용자 크리덴셜 DB (360')에서는, 사용자명들은 Magnus, Sabina, 및 Gunnar를 포함한다. 즉, Gunnar는 사용자명으로서 사용자 크리덴셜 DB (360)에 추가되었다.

[0102] 사용자 크리덴셜 DB (360)는 도 7b 및 도 7c에 도시된 것에 비해 더 많은, 더 적은 또는 다른 필드들을 포함할 수 있다. 예를 들어, 일 실시예에서, 사용자명 필드(742)는 생략될 수 있고 크리덴셜 필드(748)는 사용자를 인증함과 함께 식별하기 위하여 사용될 수 있다. 사용자 크리덴셜 DB (360)에 저장된 크리덴셜들은 사용자명 및 패스워드와 다른 또는 그에 추가된 종류들의 크리덴셜들을 포함할 수 있다. 예를 들어, 사용자 크리덴셜 DB (360)는 생체정보 크리덴셜(예: 지문 또는 홍채 스캔)을 저장할 수 있다.

[0103] 위에 언급된 바와 같이, 컨트롤러(210)는 사용자들 또는 관리자들이 컨트롤러(210)에 의해 제공되는 서비스들에 접근하도록 인증할 수 있다. 컨트롤러(210)(및 대응되는 서비스)는 이러한 사용자들을 인증하기 위해 서비스 크리덴셜 DB들을 사용할 수 있다. 도 7d 내지 7g는 일 실시예에서 서비스 크리덴셜 DB들(예: 2개의 다른 시간에서의 제1 서비스 크리덴셜 DB (356) 및 제2 서비스 크리덴셜 DB (358))을 나타내는 블록도이다.

[0104] 도 7d 및 7e에 도시된 바와 같이, 제1 서비스 크리덴셜 DB (356)는 사용자명(722) 및 변환된 크리덴셜 필드(724)를 포함할 수 있다. 사용자명 필드(722)는 제1 서비스(332)에 접근하는 권한을 갖는 사용자들을 식별한다. 변환된 크리덴셜 필드(724)는 예를 들면, 솔트(salt)와 연접된 패스워드의 해쉬와 같은 크리덴셜의 암호 일방향 변환을 포함할 수 있다. 하나의 구현 예에서, 상기 변환은 대응되는 기기(예: 컨트롤러(210))의 하드웨어 주소(예: MAC 주소)가 되는 솔트와 같은, 제1 서비스(332)를 제공하는 기기에 특화될 수도 있다. 다른 구현 예에서, 제1 서비스 크리덴셜 DB (356)는 변환된 크리덴셜들을 저장하지 않지만, 원시 크리덴셜들(raw credentials) 자체 또는 원래의 크리덴셜들이 획득되는 방식(예: 양방향 해쉬, 암호화 또는 바이젝티브 변환)으로 변환된 크리덴셜들을 저장한다.

[0105] 마찬가지로, 제2 서비스 크리덴셜 DB (358)는 사용자명 필드(732) 및 변환된 크리덴셜 필드(734)을 포함할 수 있다. 사용자명 필드(732)는 제2 서비스(334)에 접근할 권한이 있는 사용자들을 식별할 수 있다. 변환된 크리덴셜 필드(734)는 예를 들면, 크리덴셜(예: 솔트와 연접된 패스워드)의 암호 일방향 변환을 포함할 수 있다. 일 구현 예에서, 필드(734) 내에서 변환된 크리덴셜을 생성하기 위해 사용되는 변환 함수는 필드(724) 내에서 변환된 크리덴셜을 생성하는 데에 사용되는 변환 함수와 다르다. 즉, 상기 변환 함수는 서비스(예를 들어, 상기 서비스가 제1 서비스(332)인지 제2 서비스(334)인지 여부)에 특화될 수 있다. 또한, 상기 변환은 대응되는 컨트롤러(210)의 하드웨어 주소(예: MAC 주소)가 되는 솔트와 같은, 제2 서비스(334)를 제공하는 기기에 특화될 수 있다. 다른 구현 예에서, 제2 서비스 크리덴셜 DB (358)는 변환된 크리덴셜들을 저장하지 않지만, 상기 크리덴셜들 자체 또는 원래의 크리덴셜들이 획득되는 방식(예: 양방향 해쉬, 암호화 또는 바이젝티브 변환)으로 변환된 크리덴셜들을 저장한다.

[0106] 제1 서비스 크리덴셜 DB (356)(SSH를 위한 도 7d에서의 UYDAG)에서 Sabina에 대한 상기 변환된 크리덴셜은 제2 서비스 크리덴셜 DB (358)(VPN을 위한 도 7g에서의 UHYRV)에서 Sabina에 대한 상기 변환된 크리덴셜과 다르지만, 이것은 두 서비스들에 대해 동일한 변환되지 않은 크리덴셜(예: 패스워드 LETMEIN)에 대응된다. 따라서, Sabina는 동일한 크리덴셜들(예: 사용자명 및 패스워드)을 사용하여 특정 컨트롤러(210-A) 상에서 상기 SSH 서버 및 상기 VPN 서버로 로그인할 수 있다. 또한, 설령 제1 서비스 크리덴셜 DB (356) 및 제2 서비스 크리덴셜 DB(358) 내의 상기 변환된 크리덴셜들은, 다른 컨트롤러(210)(예: 컨트롤러들(210-B 내지 210-F)) 상에서는 다를 수 있다고 하더라도, 이러한 변환된 크리덴셜들은 동일한 변환되지 않은 크리덴셜들(예: 사용자명 및 패스워

드)에 대응될 수도 있다. 따라서, Sabina는 동일한 크리덴셜(예: 사용자명 및 패스워드)를 사용하여 다른 컨트롤러들(210-B 내지 210-F) 상에서 상기 SSH 서버 및 상기 VPN 서버에 로그인할 수 있다.

[0107] 도 8b에 관하여 아래의 예에서 설명된 바와 같이, 제1 서비스 크리덴셜 DB (356)(도 7d에 도시됨)는 업데이트된 제1 서비스 크리덴셜 DB (356')(도 7e에 도시됨)를 생성하기 위해 업데이트된다. 또한, 제2 서비스 크리덴셜 DB (358)(도 7f에 도시됨)는 (업데이트 된) 제2 서비스 크리덴셜 DB (358')(도 7g에 도시됨)를 생성하기 위하여 업데이트된다. 업데이트 된 제1 서비스 크리덴셜 DB (356') 및 제2 서비스 크리덴셜 DB (358')에 대한 변경은 (제1 서비스 크리덴셜 DB (356) 및 제2 서비스 크리덴셜 DB (358)와 비교할 때) 볼드체 및 화살표들로 도시된다.

[0108] 제1 서비스 크리덴셜 DB (356) 및 제 2 크리덴셜 DB (358)는 도 7d 내지 7g에 도시된 것에 비해 더 많은, 더 적은 또는 다른 필드들을 포함할 수 있다. 예를 들어, 일 실시예에서, 사용자명 필드(722 또는 734)는 생략될 수 있고 크리덴셜 필드(724 또는 734)는 사용자를 인증함과 함께 식별하기 위하여 사용될 수 있다. 다른 실시예에서, 사용자 크리덴셜 DB들(356 및/또는 358)에 저장된 크리덴셜들은 사용자명 및 (변환된) 패스워드와 다른 또는 그에 추가된 종류들의 크리덴셜들을 포함할 수 있다. 예를 들어, 사용자 크리덴셜 DB들(356 및 358)은 생체정보 크리덴셜(예: 지문 또는 홍채 스캔)을 저장할 수 있다.

[0109] 위에 언급된 바와 같이, 일 실시예는 사용자가 동일한 크레덴셜(들)(예: 동일한 사용자명 및 패스워드)을 사용하면서, 다중 기기들에 걸쳐 다중 서비스들에 접근하도록 허용한다. 또한, 일 실시예는 제어 시스템(110)의 유닛들(115) 내의 컨트롤러들(210)과 같은, 분산된 네트워크 내의 기기들 사이에서 전파될 크리덴셜(들)에 대한 변경을 허용한다.

[0110] 도 8a는 컨트롤러들(210) 내의 서비스에 접근할 권한을 갖는 사용자를 인증하기 위한, 예시적인 프로세스(800A)의 흐름도이다. 프로세스(800)는 예를 들어, 컨트롤러(210) 내에서 실행중인 서비스 또는 서비스들(예: 제1 서비스(332) 및/또는 제2 서비스(334))에 의해 수행될 수 있다. 각각의 서비스는 하나 이상의 사용자가 그러한 특정 서비스에 접근하도록 인증하기 위한, 그 자신의 버전의 프로세스(800)를 실행할 수 있다. 이하의 예에서, 제1 서비스(332)는 SSH 서버이고 제2 서비스(334)는 VPN 서버이다. 또한, 상기 특정 컨트롤러(210)는 도 7b에 도시된 바와 같은 사용자 크리덴셜 DB (360), 도 7d에 도시된 바와 같은 제1 서비스(SSHO 크리덴셜 DB (356), 및 도 7f에 도시된 바와 같은 VPN 크리덴셜 DB (358)을 포함한다.

[0111] 이 실시예에서, 프로세스(800A)는 사용자로부터 서비스의 요청을 수신함과 함께 시작된다(블록 802). 상기 요청된 서비스가 인증을 위한 사용자명 및 패스워드를 요구하는 SSH 서버이고, 상기 사용자가 관리 기기(130)(사용자가 원격으로 위치하는 곳) 내에서 실행 중인 SSH 클라이언트를 사용하여 컨트롤러(210)에 로그인하기를 원한다고 가정한다. 이 경우에, 상기 서비스(SSH 서버)는 크리덴셜(들)(예: 사용자명 및 패스워드)에 대해 사용자에게 프롬프트를 표시한다(블록 804). 상기 서비스(SSH 서버)는 사용자 크리덴셜(들)을 수신하고(블록 806), 일 실시예에서, 상기 사용자 크리덴셜(들)을 변환한다(블록 808). 크리덴셜들의 변환의 예는 변환된 크리덴셜 생성기(386)에 관하여 위와 같이 설명된다.

[0112] 사용자를 인증하기 위해, 서비스(SSH 서버)는 상기 수신된 크리덴셜들(예: 변환된 크리덴셜들)을 상기 저장된 크리덴셜(들)과 비교한다(블록 810). 상기 수신된 크리덴셜들을 상기 저장된 크리덴셜(들)과 비교하는 단계는 상기 수신된 크리덴셜들을 변환하는 단계를 포함할 수 있다. 위에서 설명된 바와 같이, 상기 서비스에 대한 크리덴션들은, 컨트롤러(210)의 스토리지 계층(350) 내의 제1 서비스(제1 변환된) 크리덴셜 DB (356)에 저장된다. 상기 크리덴셜들이 동일하지 않으면(예를 들어, 상기 수신된 크리덴셜이 정확하지 않으면)(블록 812의 아니오), 인증은 실패하고 서비스(SSH 서버)에 대한 접근은 허용되지 않는다(블록 814). 상기 수신된 크리덴셜(들)(변환되어 있는 크리덴셜들)이 정확하면(즉, 매칭되면)(블록 812의 예), 인증은 성공하고 상기 서비스(SSH 서버)에 대한 접근이 허용된다(블록 816).

[0113] 예를 들어, 사용자 Sabina는 SSH 클라이언트를 갖는 유닛(115-A)의 컨트롤러(210-A)(도 5 참조)로의 로그인을 시도하기 위해, 관리 기기(130)를 사용할 수 있다. 그녀에게는 사용자명(Sabina)과 패스워드(LETMEIN)을 입력하도록 프롬프트가 표시되고, 그것들을 입력한다. 도 7d에 도시된 바와 같이, 컨트롤러(210-A)가 제1 서비스(SSH) 크리덴셜 DB (356)를 저장한다고 가정한다. 컨트롤러(210-A)의 서비스(332)(SSH)는 패스워드 "LETMEIN"을, 크리덴셜 DB (356) 내에 저장되는 변환된 크리덴셜과 매칭되는 UYDAG로 변환하고, 사용자 Sabina는 성공적으로 인증되고 컨트롤러(210-A) 내에서 SSH 서비스에 접근할 권한을 갖는다. 이 실시예에서, 컨트롤러(210-B) 내의 SSH 크리덴셜 DB (356)은 이러한 방식으로 설정되기 때문에, Sabina는 동일한 사용자명 및 패스워드로 컨트롤러(210-B) 상에서 SSH 서버로 로그인할 수도 있다. 사실, 각각의 컨트롤러(210) 내에 저장된 상기 VPN 크리덴셜

DB (358)는 이러한 방식으로 설정되기 때문에, Sabina는 동일한 사용자명 및 패스워드(Sabina, LETMEIN)로 다중 컨트롤러들(210) 상에서 VPN 서버로 로그인할 수 있다. 예를 들어, 상기 SSH 크리덴셜 테이블(제1 서비스 크리덴셜 DB (356)) 내의 변환된 크리덴셜은 상기 VPN 크리덴셜 테이블(제2 서비스 크리덴셜 DB (358)) 내의 변환된 크리덴셜과 동일한 패스워드에 대응된다. 그러나, Sabina는 컨트롤 시스템(110) 내의 모든 서비스들(SSH 및 VPN)과 모든 컨트롤러들(210-A 내지 210-F)에 대해, 그녀의 패스워드를 "LETMEIN"에서 "GOTLAND"로 변환하기를 원한다. 그러나, 관리자(또는 Sabina)가 각각의 기기 및 각각의 서비스에 대해 패스워드를 변경해야 한다면, Sabina의 희망은 잠재적으로 부담을 야기한다.

[0114] 여기에 설명된 실시예들은 Sabina(또는 관리자)가 서비스(들)에 대해 컨트롤러(210) 상에서 사용자 크리덴셜 DB (360) 내에 있는 그녀의 패스워드를 변경하고 그러한 변경이 다른 컨트롤러들(210)로 전파될 수 있게 하는 것을 허용할 수 있다. 이 경우에, 관리자 인증 로직(382)은 다중 서비스들 및/또는 다중 기기들 상의 다중 서비스들에 대해 동일한 크리덴셜로 동일한 사용자(예: Sabina)를 인증할 수 있다.

[0115] 도 8b는 사용자 크리덴셜 DB (360) 및 서비스 크리덴셜 DB들(예: DB 들(356 및 358))을 업데이트하기 위해 관리자에 대한 예시적인 프로세스(800B)의 흐름도이다. 아래의 예에서, 관리자는 컨트롤러(210)에 대한 로그인을 위해 관리 기기(130)를 사용한다. 일 실시예에서, 상기 사용자 크리덴셜 DB에 대한 변경들은 필요한 다른 컨트롤러들(210)(및 다른 서비스 DB들)로 배포될 수 있기 때문에, 상기 관리자는 상기 컨트롤러들(310) 중 어느 하나에 로그인할 수 있다. 이러한 예에서, 관리자는 컨트롤러(210-A)에 로그인하고 프로세스(800B)는 유닛(115-A)의 컨트롤러(210-A) 내에서 사용자 크리덴셜 업데이트 로직(384)에 의해 수행된다.

[0116] 프로세스(800B)는 컨트롤러(210)에 로그인하는 관리자로부터 크리덴셜(들)을 수신함과 함께 시작되고 상기 관리자를 인증한다(블록 822). 상기 관리자는 예를 들면, Sabina의 패스워드(예를 들어, 컨트롤러(210-A) 내에 저장된 사용자 크리덴셜 DB (360) 내에 있는 패스워드)를 업데이트 하기 위한 목적으로 컨트롤러(210-A)에 로그인한다. 상기 관리자를 인증하기 위한 방법 및 프로세스는 도 8c에 관하여 아래에서 설명된다. 이 예에서, 상기 관리자는 성공적으로 인증되었고 프로세스(800B)는 블록(824)로 진행하는 것을 가정한다. 사용자 크리덴셜 DB(360)가 암호화되었으면 그것은 복호화된다(블록 824). 도 8c에 관하여 설명된 일 실시예에서, 사용자 크리덴셜 DB (360)를 복호화하기 위해 사용되는 키는 상기 관리자가 성공적으로 인증되었을 때에만 가용하다. 사용자 크리덴셜 DB (360)를 복호화하는 것은 상기 관리자가 상기 DB 내의 엔트리들을 편집하고 변경할 수 있게 허용하는 것이다. 다른 실시예들에서, 사용자 크리덴셜 DB (360)를 복호화하기 위해 사용되는 키는 암호화 없이 컨트롤러(210) 내에 저장된다.

[0117] 상기 관리자는 일단 인증되면, 필드(748) 내의 크리덴셜(들), 사용자명 필드(742) 내의 사용자명(들), 서비스 필드(744) 내의 서비스(들) 및/또는 기기 필드(746) 내의 기기(들)을 포함하는, 사용자 크리덴셜 DB (360) 내의 정보를 편집하고 변경할 수 있다. 이러한 새롭고 업데이트된 크리덴셜(들)(사용자명들을 포함하는)은 컨트롤러(210-A)에 의해 수신된다(블록 826). 상기 크리덴셜(들)에 대응되는 상기 식별된 서비스들 및 기기들도 수신되며(블록 828), 컨트롤러(210-A) 내의 상기 사용자 크리덴셜 DB (360)가 업데이트 된다(블록 830). 예를 들면, 상기 관리자는 컨트롤러(210-A)에 의해 제공되는 특정 서비스 또는 다른 컨트롤러(210-B 내지 210-F) 중 하나에 의해 제공되는 서비스에 접근할 권한을 갖는 사용자를 추가하거나 삭제할 수 있다. 상기 관리자는 예를 들어 크리덴셜 필드(748) 내에 저장된 크리덴셜(예: 패스워드)를 변경할 수 있다. 또한, 상기 관리자는 상기 대응되는 크리덴셜들이 적용되는 컨트롤러(들)(210)을 변경할 수 있다.

[0118] 예를 들어, 도 7a 및 7b에 도시된 바와 같이, 상기 관리자는 사용자 크리덴셜 DB (360')(도 7b)를 생성하기 위해, 사용자명 Gunnar를 사용자 크리덴셜 DB (360)(도 7a)에 추가한다. 업데이트 된 사용자 크리덴셜 DB (360')는 컨트롤러들(210-A, 210-B 및 210-C) 상에서 VPN 서비스에 대한 접근권을 갖지만, 이 예에서 컨트롤러를 포함하는 카메라(260) 내에서는 아니다(기기 필드(746)에서 정의된 바와 같이). 이러한 식별된 컨트롤러들(기기 필드(746) 내의)에 의해 제공되는 VPN 서비스에 대해, Gunnar는 인증을 위해 사용자명 "Gunnar" 및 패스워드 "MUNKKALLAREN"를 사용할 수 있다. 또한, 상기 관리자는 제어 시스템(110) 내의 모든 기기들에 대한 SSH 및 VPN 서비스들을 위한, 사용자명 Sabina에 대해 상기 크리덴셜(즉, 패스워드)을 "LETMEIN"에서 "GOTLAND"로 변경한다.

[0119] 사용자 크리덴셜 DB (360)에 대한 변경이 있으면, 변환된 사용자 크리덴셜들이 생성되고(예를 들어, 상기 업데이트된 또는 비암호화된 사용자 크리덴셜들에 기초하여), 상기 서비스 크리덴셜 DB들(예: 제1 서비스 크리덴셜 DB (356) 및/또는 제2 서비스 크리덴셜 DB (358))은 업데이트된다(블록 832). 사용자 크리덴셜 DB (360)에 저장된 크리덴셜들은 상기 서비스 및 기기에 대해 적절하게 변환된다. 이상에서 설명된 바와 같이, 변환된 크리덴셜

생성기(386)는 크리덴셜 변환 규칙 DB (388)에 저장된 규칙들(및 다른 정보)에 기초하여 상기 크리덴셜을 변환할 수 있다. 예를 들어, 생성기(386)는 상기 변환된 크리덴셜을 생성하기 위해 SSH 서비스에 대해 암호 일방향 함수(예: 상기 로컬 기기의 이더넷 MAC 주소로 솔트된(salted) SHA-224 암호 해쉬 함수)를 사용할 수 있다. 이 경우에, 프로세스(800B)(예를 들어, 변환된 크리덴셜 생성기(386)를 채용하는 크리덴셜 업데이트 로직(384)을 실행하는 컨트롤러(210))는 상기 기기 상에서 SSH 서버에 대한 업데이트된 또는 새로운 변환된 크리덴셜들을 생성한다.

[0120] 일 실시예에서, 상기 사용자 크리덴셜 DB (360)는, 예를 들어, 서비스 크리덴셜 DB들이 업데이트된 후 상기 관리자가 로그아웃할 때, 암호화되고(블록 834), 컨트롤러(210-A)의 스토리지 계층(350) 내에 저장된다. 상기 사용자 크리덴셜 DB (360)는 컨트롤러들(210-B 내지 210-F)(예: P2P 네트워크에 연결되는)와 같은 다른 컨트롤러들(210)로 배포될 수도 있다(블록 836). 아래에서 설명되는 바와 같이, 사용자 크리덴셜 DB (360)는, 대응되는 다른 기기들에 의해 제공되는 서비스들에 접근하는 사용자를 인증하기 위한 변환된 크리덴셜 DB들을 상기 다른 기기들이 생성할 수 있도록, 다른 컨트롤러들에 배포될 수 있다. 이 경우에, 배포 계층(340)은 사용자 크리덴셜 DB (360)를 위에서 설명된 다른 기기들에 배포할 수 있다. 일 실시예에서, 예를 들어 컨트롤러들(210) 중 하나가 비보안 영역에 위치하면, 사용자 크리덴셜 DB (360)는 모든 컨트롤러들(210)보다 적은 수에 배포된다.

[0121] 일 실시예에서, 사용자 크리덴셜 DB (360)는 암호화된 포맷으로 배포된다. 이 경우에, 사용자 크리덴셜 DB (360)를 암호화하기 위해 사용되는 키(상기 "마스터 키")는 저장되고 다른 컨트롤러들(210)에 의해 사용될 수도 있다. 이 경우에, 사용자 크리덴셜 DB (360)가 암호화된 포맷으로 배포된다고 하더라도, 다른 컨트롤러들(210)은 상기 사용자 크리덴셜 DB (360)를 사용할 수 있다. 대안적인 실시예에서, 사용자 크리덴셜 DB (360)는 비암호화된 포맷으로 배포되지만, 컨트롤러들(210) 간의 링크들은 암호화될 수도 있다.

[0122] 컨트롤러(210-A) 내의 사용자 크리덴셜 DB (360)의 변경은, 다른 컨트롤러들(210)(예: 컨트롤러들(210-B 내지 210-F)) 내의 서비스 크리덴셜 DB들에 대한 변경으로 귀결될 수도 있다. 예를 들어, 컨트롤러(210-B)는 컨트롤러(210-A)에 의해 배포된 사용자 크리덴셜 DB (360)에 대한 업데이트들을 수신할 수 있다. 즉, 추가적인 변환된 사용자 크리덴셜들이 생성될 수 있고, 다른 컨트롤러들(210) 내의 서비스 크리덴셜 DB들이 업데이트될 수 있다(블록 838). 이것은 아래에 설명된 것과 같은 다양한 방법으로 수행될 수 있다. 마찬가지로 다른 예에서, 컨트롤러(210-A)는 다른 컨트롤러(210)(예: P2P 네트워크 내의 컨트롤러들(210-B 내지 210-F))에 의해 배포된 사용자 크리덴셜 DB (360)에 대한 업데이트들을 수신할 수 있고(블록 836), 변환된 사용자 크리덴셜들을 생성하고 컨트롤러(210-A) 내의 서비스 크리덴셜 DB들을 업데이트할 수 있다(블록 838). 다른 예에서, 관리자는 사용자 크리덴셜 DB (360)를 업데이트하기 위해 컨트롤러(210-B)에 로그인할 수 있다.

[0123] 일 실시예에서, 크리덴셜 변환 규칙 DB (388)(예: 컨트롤러(210-A)에 저장됨)는 자신과 더불어 다른 컨트롤러들(210)(예: 컨트롤러(210-B 내지 210-F)) 상의 서비스들에 대한 규칙들 및 정보(예: 기기에 특화된 정보)를 저장할 수 있다. 따라서, 컨트롤러(210-A) 내에서 변환된 크리덴셜 생성기(386)는 자신과 더불어 다른 컨트롤러들(210)(예: 컨트롤러(210-B 내지 210-F)) 상의 다른 서비스들에 대해 변환된 크리덴셜들을 생성할 수 있다. 이 경우에, 서비스 크리덴셜 DB들은 상기 관리자가 로그인하는 컨트롤러로부터 적절한 컨트롤러(210)에 배포될 수 있다. 또한, 상기 크리덴셜들은 이미 변환되었기 때문에, 상기 서비스 크리덴셜 DB들은 비암호화된 형태로 배포될 수 있다. 그러나, 상기 서비스 크리덴셜 DB들은 암호화된 형태로 배포될 수 있다고 하더라도, 컨트롤러들(210) 간의 통신 링크들은 여전히 암호화될 수 있다(예: SSL/TLS에 의해).

[0124] 다른 실시예에서, 각각의 컨트롤러(210)는 자신의 서비스 크리덴셜 DB들을 생성하는 것을 담당할 수 있다. 이 경우에, 변환된 크리덴셜 생성기(386)(컨트롤러(210-A)와 다른 컨트롤러 상에 있음)는, 사용자 크리덴셜 DB (360)가 변경되었다는 것을 감지하고 그 자신의 로컬 서비스 크리덴셜 DB들을 업데이트할 수 있다. 이 경우에, 사용자 크리덴셜 DB (360) 및 마스터 키가 암호화되었으면, 컨트롤러(210)(예: 컨트롤러(210-B 내지 210-F))는 상기 마스터 키 없이는 크리덴셜 DB (360)에 접근할 수 없다. 일 실시예에서, 관리자가 컨트롤러(210-A)에 로그인할 때, 다른 컨트롤러들(210)(예: 컨트롤러(210-B 내지 210-F))이 상기 마스터 키를 결정하거나 복호화하기에 충분한 정보가 상기 다른 컨트롤러들(210)에 전달된다(예: 암호화된 링크들을 사용함). 따라서, 다른 컨트롤러들(210)(예: 컨트롤러(210-B 내지 210-F))은 상기 관리자가 로그인하는 컨트롤러(210)(예: 컨트롤러(210-A))로부터 수신되는 크리덴셜 DB (360)에 대한 배포된 업데이트들을 복호화할 수 있다. 일 실시예에서, 상기 마스터 키는 어떠한 컨트롤러(210) 내의 비휘발성 메모리 내에도 결코 저장되지 않는다. 다른 실시예들에서, 상기 마스터 키는 비휘발성 메모리 내에 저장될 수 있다. 대안적으로, 상기 대응되는 로컬 서비스 크리덴셜 DB들이 업데이트될 수 있도록, 상기 관리자는 각각의 컨트롤러(210)로 로그인하도록 요구될 수 있다. 다른 실시예에서, 사용자 크리덴셜 DB (360)가 컨트롤러(210-A) 내에서 업데이트된 후에, 그리고 사용자 크리덴셜 DB (360)가 다른

컨트롤로들(210-B)에 배포된 후에, 예를 들면 컨트롤러(210-A)는 상기 관리자가 제공하는 패스워드를 사용하여, 다른 컨트롤러들(210-B)내로 관리자가 로그인하게 할 수 있다. 이러한 방식으로, 상기 관리자로부터 사용자 크리덴셜 DB (360)에 대한 업데이트들을 수신한 컨트롤러(210-A)는, 다른 컨트롤러들(210-B 내지 210-F)이 자신의 각각의 크리덴셜 DB들을 업데이트하는 것을 보장할 수 있다.

[0125] 도 8b에 관해 설명된 바와 같이, 관리자는 관리 기기(130)를 사용하여 컨트롤러(210)에 로그인 할 수 있다.

[0126] 도 8c는 일 실시예에서 관리자를 인증하기 위한 프로세스(822)의 흐름도이다. 프로세스(822)가 사용자 크리덴셜 DB (360)를 업데이트하려는 관리자를 인증하는 데에 사용될 수 있지만, 인증 프로세스(822)는 컨트롤러(210)에 관한 다른 태스크들을 수행하려는 관리자를 인증하기 위해서 사용될 수도 있다.

[0127] 프로세스(822)는 유닛(115)의 컨트롤러(210)로 로그인하는 관리자로부터, 관리자 사용자명 및 패스워드(즉, 크리덴셜들)를 수신함과 함께 시작된다(블록 842). 상기 입력된 사용자명과 일치하는 사용자명이 존재하는지를 판단하기 위해, 프로세스(822)는 크리덴셜 DB (354)에 질의한다. 일치된 사용자명이 관리자 크리덴셜 DB (354)에서 발견되지 않으면(블록 844의 아니오), 인증은 실패하고 컨트롤러(210)에 대한 접근은 허용되지 않는다(블록 846). 일치된 사용자명이 관리자 크리덴셜 DB (354)에서 발견되면(블록 844의 예), 프로세스(822)는 블록(848)로 진행하여 인증이 성공인지 아닌지를 판단한다.

[0128] 상기 수신된 관리자 패스워드가 당분간 대략적으로(probably) 정확하다는 것만 전제된다면, 소위 "대략적(probable) 마스터 키"를 생성하기 위해 상기 수신된 관리자 패스워드에 기초하여 상기 저장된 암호화된 마스터 키(암호화된 마스터 키 필드(706) 내에 저장됨)가 복호화된다. 소위 "대략적 마스터 키"를 생성하기 위해, 상기 저장된 관리자 패스워드는 그 후 대략적 마스터 키에 기초하여 복호화된다(블록 850). 상기 수신된 관리자 패스워드가 상기 대략적 관리자 패스워드와 동일하지 않으면(블록 852의 아니오), 인증은 실패하고 컨트롤러(210)에 대한 접근은 허용되지 않는다(블록 846). 상기 수신된 관리자 패스워드가 상기 대략적 관리자 패스워드와 일치하면(블록 852의 예), 인증은 성공하고 상기 컨트롤러(210)에 대한 접근이 허용된다(블록 854). 이 경우에(블록 854의 예), 도 8b로 돌아가면(블록 824), 사용자 크리덴셜 DB (360)가 암호화되었다면, 관리 로직(323)은 상기 마스터 키(이 경우에는 상기 대략적 마스터 키와 동일함)에 기초하여 사용자 크리덴셜 DB (360)를 복호화할 수 있다. 이 실시예에서 상기 암호화된 마스터 키는 상기 관리자 패스워드에 기초하여 복호화되기 때문에, 관리 로직(323)은 상기 입력된 관리자 패스워드(이 경우에는 상기 대략적 관리자 패스워드와 동일함)에도 기초하여 상기 사용자 크리덴셜 DB (360)를 복호화한다.

[0129] 다양한 프로세스(822)가 가능하다. 예를 들어 일 실시예에서, 관리자에 의해 입력되는 패스워드는 사용되지 않는다. 그 보다는, 상기 관리자는 다른 수단(예를 들어, 키 또는 패스워드 관리 시스템을 갖는 관리 기기(130) 내의 클라이언트 소프트웨어를 통해서)에 의해 비밀을 제공할 수 있다. 또한, 일 실시예에서 상기 관리자는 사용자명을 제공하지 않는다. 이 경우에, 프로세스(822)는, 예를 들어 인증이 성공인지 아닌지를 판단하기 위해, 관리자 크리덴셜 DB (354) 내에 각각의 엔트리 또는 레코드에 대해 실행될 수 있다.

[0130] 이전의 명세서에서, 다양한 실시예들이 수반하는 도면들을 참조하여 설명되었다. 그러나, 뒤따르는 청구항에 제시된 발명의 광범위한 범주를 일탈하지 않고도, 거기에 다양한 수정들 및 변경들이 가해질 수 있다는 것은 명백하다. 상기 명세서 및 도면들은 따라서 한정적인 의미보다는 예시적인 것으로 간주되어야 한다. 예를 들어, 일련의 블록들은 도 8a 내지 8c를 참조하여 설명되었지만, 상기 블록들 및/또는 신호 흐름들의 순서는 다른 구현예들에서는 수정될 수 있다. 또한, 비종속적 블록들 및/또는 신호 흐름들은 평행하게 수행될 수 있다.

[0131] 위에 설명된 바와 같은 시스템들 및/또는 수단들은, 도면들에 도시된 구현예들에서 소프트웨어, 펌웨어 및 하드웨어의 많은 다른 형태들로 구현될 수 있다. 이러한 시스템들 및 방법들을 구현하기 위한 실제 소프트웨어 코드나 특화된 제어 하드웨어는 상기 실시예들에 한정되지 않는다. 따라서, 상기 시스템들 및 방법들의 동작 및 거동은 특정 소프트웨어 코드를 참조하지 않고 설명되었다. 여기의 설명에 기초하여, 상기 시스템들 및 방법들을 구현하기 위해 소프트웨어 및 제어 하드웨어가 설계될 수 있다는 것을 이해될 수 있을 것이다.

[0132] 또한, 위에 설명된 어떤 부분들은 하나 이상의 기능들을 수행하는 구성요소로 구현될 수 있다. 여기에 사용된 구성요소는 프로세서, ASIC 또는 FPGA와 같은 하드웨어나 하드웨어 및 소프트웨어의 조합(예: 소프트웨어를 실행하는 프로세서)을 포함할 수 있다.

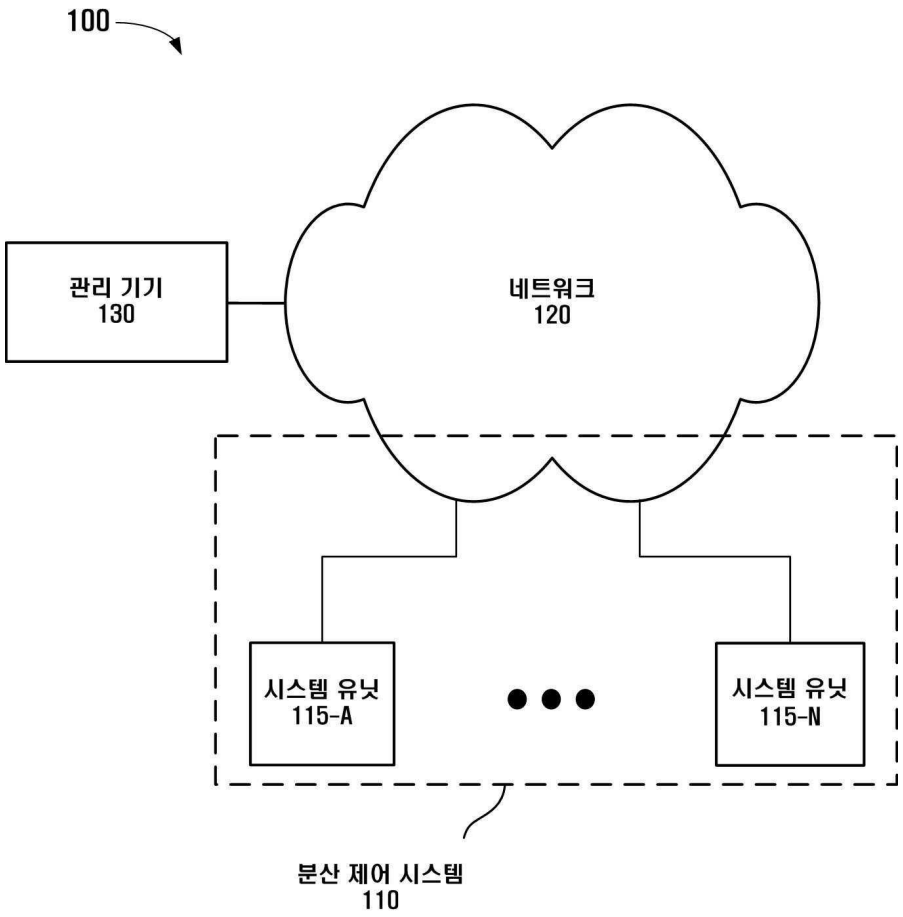
[0133] 여기에 사용된 "포함한다" 및/또는 "포함하는"이라는 용어는, 설명된 특징들, 정수들, 단계들 또는 구성요소들의 존재를 특정하지만, 하나 이상의 다른 특징들, 정수들, 단계들, 구성요소들 또는 그들의 그룹들의 존재나 추가를 배제하는 것은 아니다. 또한, "예시적인"(예: "예시적인 실시예", "예시적인 구성" 등)이라는 용어는

"예"를 의미하며 "선호", "최선" 등을 의미하지 않는다.

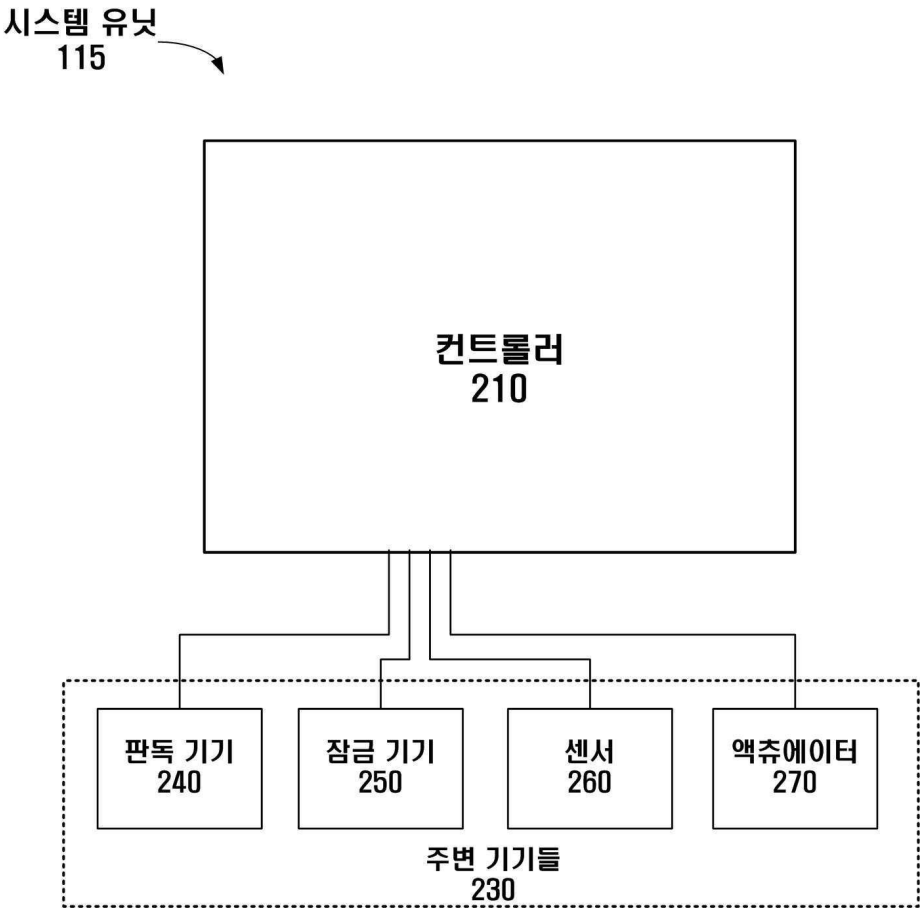
[0134] 본원에 사용되는 어떠한 요소, 동작 또는 인스트럭션도 명시적으로 기재되어 있지 않는 한, 실시예들에 대해 임계적이거나 필수적인 것으로 해석되어서는 아니된다. 또한, 여기에 사용된, 관사 "a"는 하나 이상의 항목들을 포함하도록 의도된 것이다. 예를 들어, 프로세서("a processor")는 하나 이상의 프로세서들(예: 암호화 및/또는 복호화를 위한 마이크로프로세서 및 전용 회로)을 포함한다. 또한, 복수의 기기들의 "각각"이 어떤 특징을 포함하는 것으로 기재되었더라도, 모든 기기들이 반드시 그 특징을 포함하는 것은 아니다. 즉, 다른 기기들(상기 특징을 갖는 것으로 정의된 기기 이외의 기기들)은 상기 특징을 포함하지 않을 수 있다. 또한, "기초하여"라는 문구는 명시적으로 반대로 기재되어 있지 않는 한, "적어도 부분적으로 기초하여"를 의미하도록 의도된 것이다.

도면

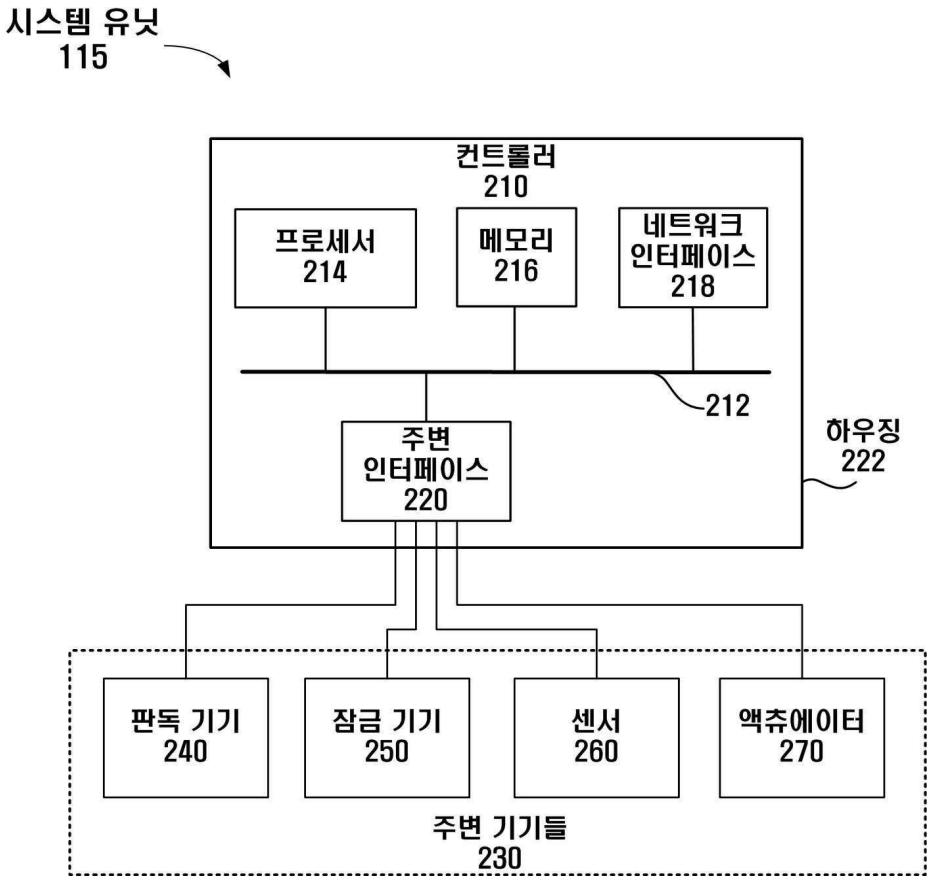
도면1



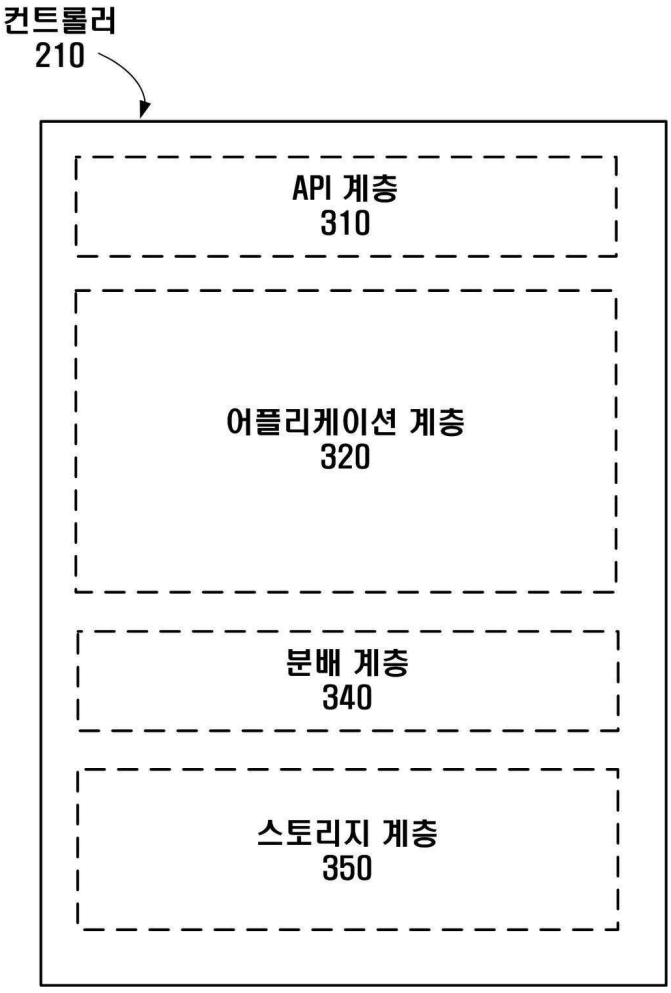
도면2a


시스템 유닛
115
컨트롤러
210
판독 기기
240
잠금 기기
250
센서
260
액츄에이터
270
주변 기기들
230

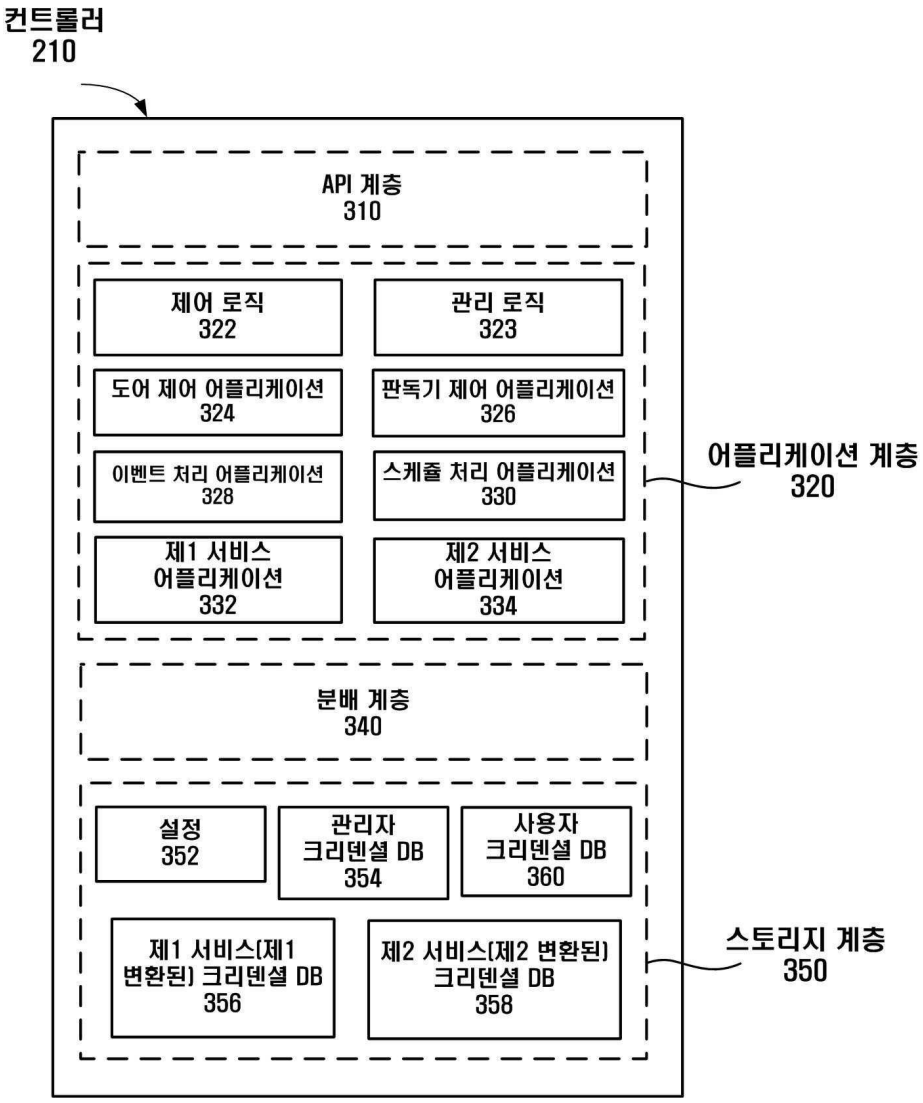
도면2b


시스템 유닛
115
컨트롤러
210
프로세서
214
메모리
216
네트워크
인터페이스
218
212
하우징
222
주변
인터페이스
220
판독 기기
240
잠금 기기
250
센서
260
액츄에이터
270
주변 기기들
230

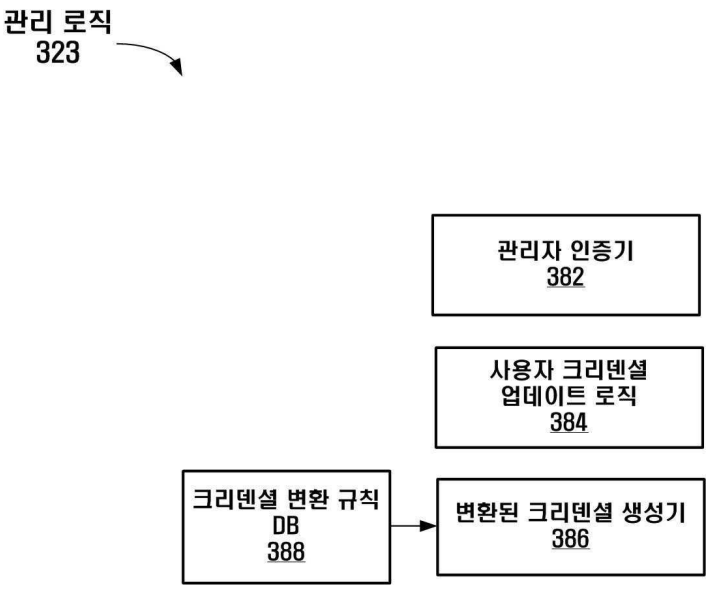
도면3a



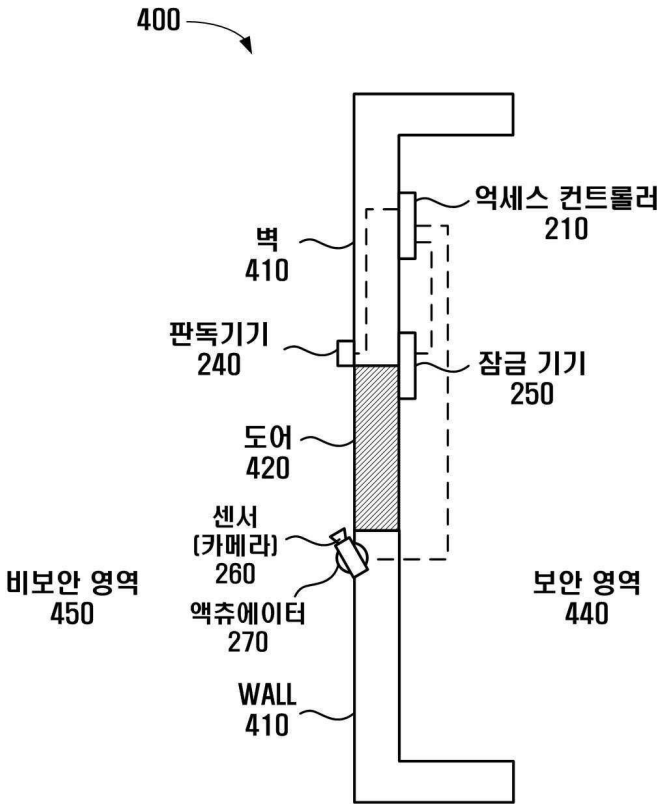
도면3b


컨트롤러
210
API 계층
310
제어 로직
322
관리 로직
323
도어 제어 어플리케이션
324
판독기 제어 어플리케이션
326
이벤트 처리 어플리케이션
328
스케줄 처리 어플리케이션
330
제1 서비스
어플리케이션
332
제2 서비스
어플리케이션
334
어플리케이션 계층
320
분배 계층
340
설정
352
관리자
크리덴셜 DB
354
사용자
크리덴셜 DB
360
제1 서비스(제1
변환된) 크리덴셜 DB
356
제2 서비스(제2 변환된)
크리덴셜 DB
358
스토리지 계층
350

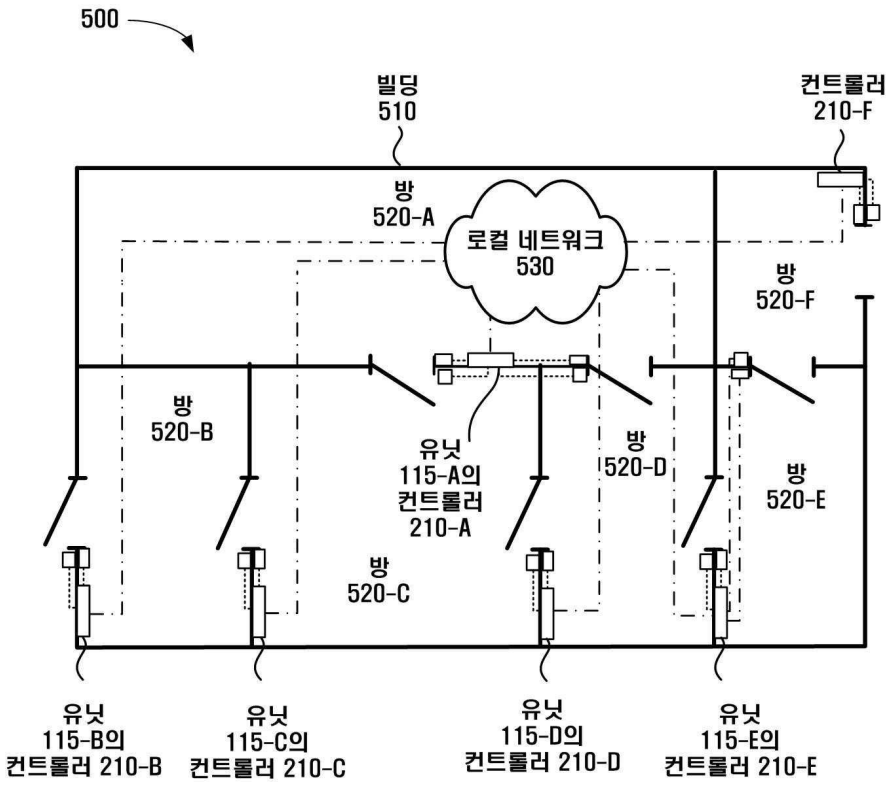
도면3c


관리 로직
323
관리자 인증기
382
사용자 크리덴셜
업데이트 로직
384
크리덴셜 변환 규칙
DB
388
변환된 크리덴셜 생성기
386

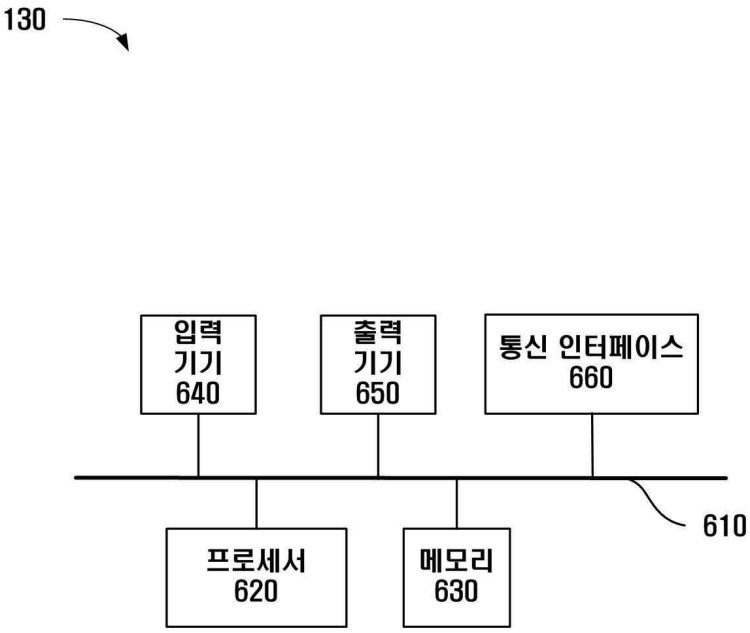
도면4


400
억세스 컨트롤러
210
벽
410
판독기기
240
잠금 기기
250
도어
420
센서
(카메라)
260
액츄에이터
270
비보안 영역
450
보안 영역
440
WALL
410

도면5


500
빌딩
510
컨트롤러
210-F
방
520-A
로컬 네트워크
530
방
520-F
방
520-B
유닛
115-A의
컨트롤러
210-A
방
520-D
방
520-E
방
520-C
유닛
115-B의
컨트롤러 210-B
유닛
115-C의
컨트롤러 210-C
유닛
115-D의
컨트롤러 210-D
유닛
115-E의
컨트롤러 210-E

도면6



도면7a

관리자 크리덴셜 DB 354

관리자 사용자명 702	암호화된 패스워드 704	암호화된 마스터 키 706
ADMIN1	C(PW1, MASTER KEY)	C(MASTER KEY, PW1)
ADMIN2	C(PW2, MASTER KEY)	C(MASTER KEY, PW2)

도면7b

사용자 크리덴셜 DB 360

사용자명 742	서비스 744	기기 746	크리덴셜 748
MAGNUS	SSH, VPN	ALL	MONKEY
SABINA	SSH, VPN	ALL, NOT CAMERA 260	LETMEIN

도면7c

(업데이트)사용자 크리덴셜 DB 360'

사용자명 742	서비스 744	기기 746	크리덴셜 748
MAGNUS	SSH, VPN	ALL	MONKEY
SABINA	SSH, VPN	ALL, NOT CONTROLLER 210-F	GOTLAND
GUNNAR	VPN	CONTROLLERS 210-A, 210-B, 210-C, NOT CAMERA 260	MUNKKALLAREN

도면7d

제1 서비스(제1 변환된) 크리덴셜 DB 356

SSH 크리덴셜 테이블

사용자명 722	변환된 크리덴셜 724
MAGNUS	SDFGH
SABINA	UYDAG

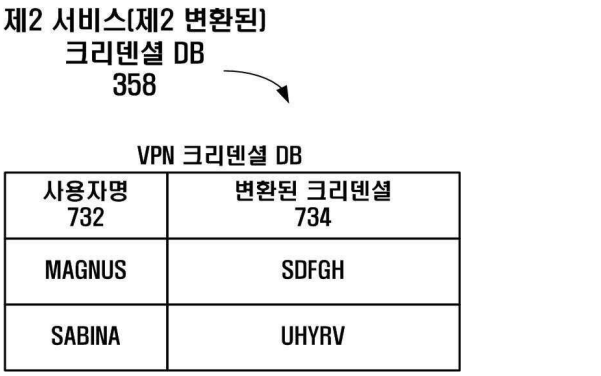
도면7e

(업데이트된) 제1 서비스 (제1 변환된) 크리덴셜 DB 356'

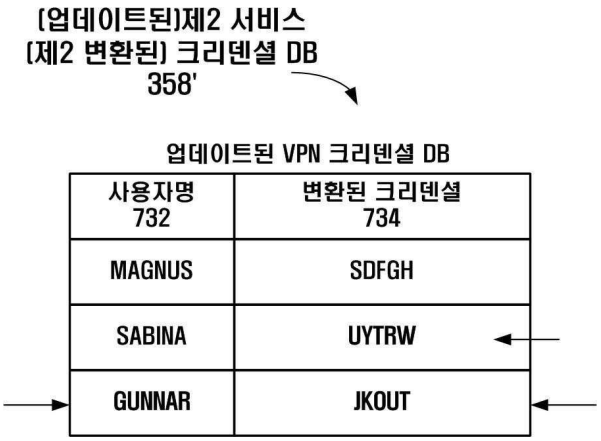
업데이트된 SSH 크리덴셜 테이블

사용자명 722	변환된 크리덴셜 724
MAGNUS	SDFGH
SABINA	DSISO

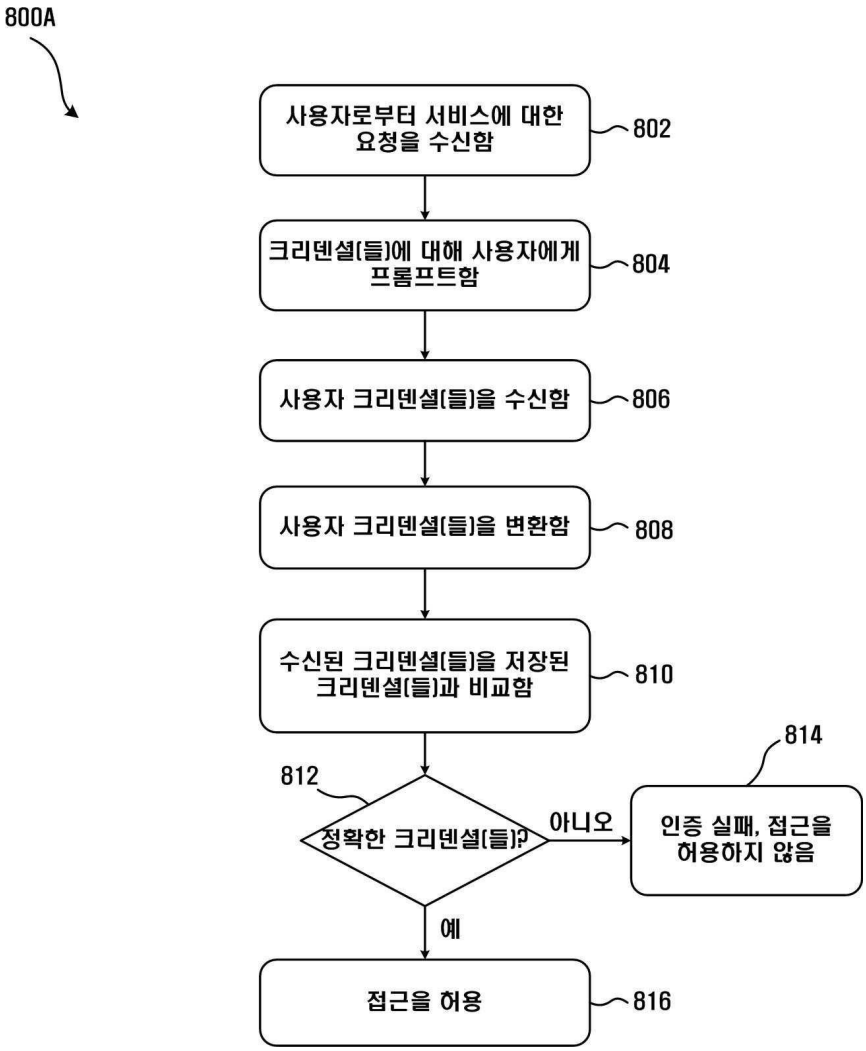
도면7f


제2 서비스(제2 변환된)
크리덴셜 DB
358
VPN 크리덴셜 DB
사용자명
732
변환된 크리덴셜
734
MAGNUS
SDFGH
SABINA
UHYRV

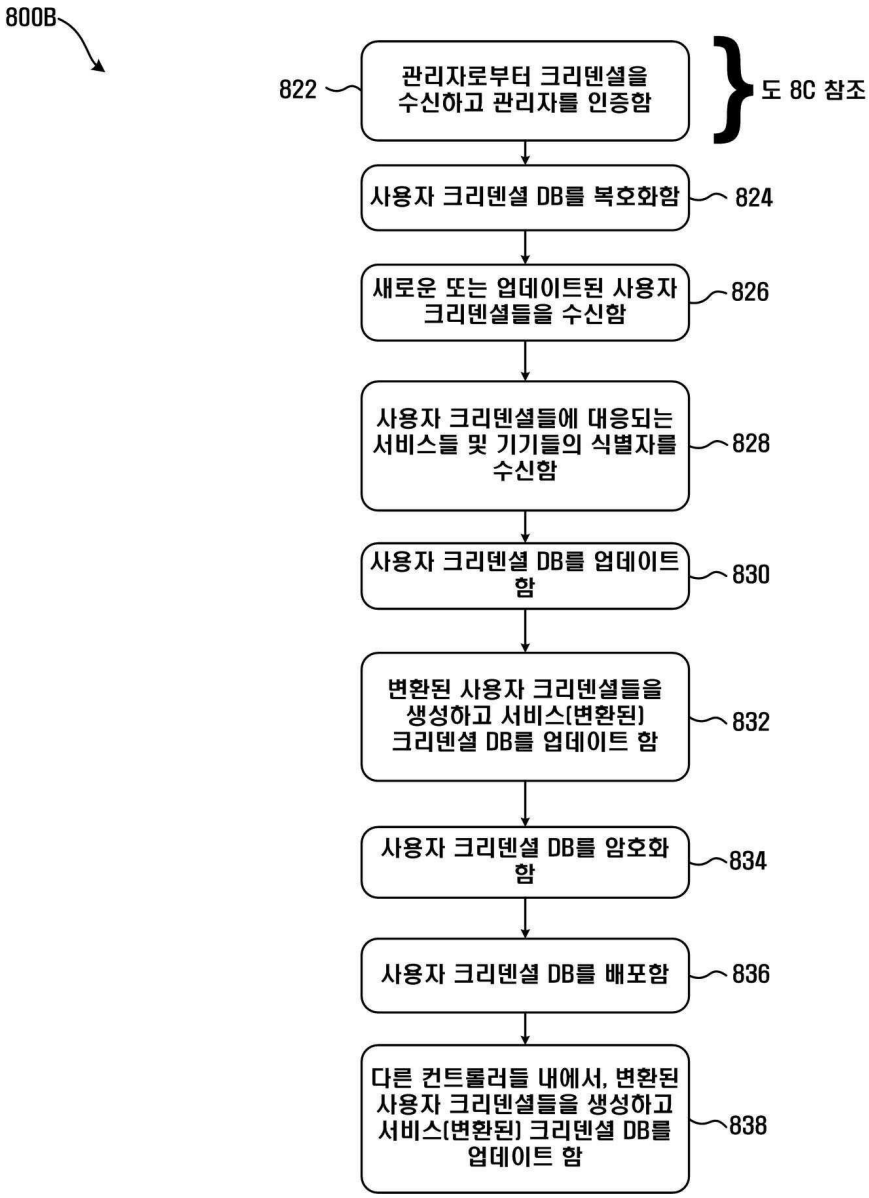
도면7g


(업데이트된)제2 서비스
(제2 변환된) 크리덴셜 DB
358'
업데이트된 VPN 크리덴셜 DB
사용자명
732
변환된 크리덴셜
734
MAGNUS
SDFGH
SABINA
UYTRW
GUNNAR
JKOUT

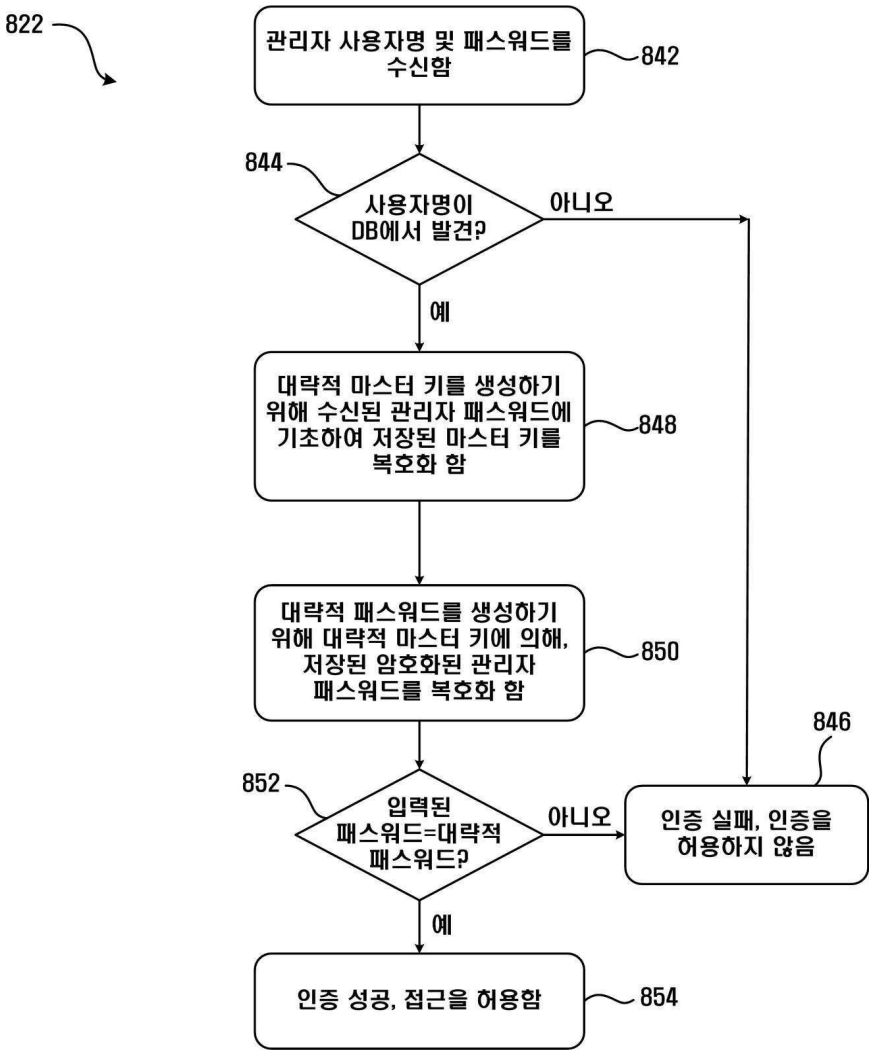
도면8a


800A
사용자로부터 서비스에 대한 요청을 수신함
802
크리덴셜(들)에 대해 사용자에게 프롬프트함
804
사용자 크리덴셜(들)을 수신함
806
사용자 크리덴셜(들)을 변환함
808
수신된 크리덴셜(들)을 저장된 크리덴셜(들)과 비교함
810
812
정확한 크리덴셜(들)?
아니오
814
인증 실패, 접근을 허용하지 않음
예
접근을 허용
816

도면8b


800B
822
관리자로부터 크리덴셜을 수신하고 관리자를 인증함
도 8C 참조
사용자 크리덴셜 DB를 복호화함
824
새로운 또는 업데이트된 사용자 크리덴셜들을 수신함
826
사용자 크리덴셜들에 대응되는 서비스들 및 기기들의 식별자를 수신함
828
사용자 크리덴셜 DB를 업데이트 함
830
변환된 사용자 크리덴셜들을 생성하고 서비스(변환된) 크리덴셜 DB를 업데이트 함
832
사용자 크리덴셜 DB를 암호화 함
834
사용자 크리덴셜 DB를 배포함
836
다른 컨트롤러들 내에서, 변환된 사용자 크리덴셜들을 생성하고 서비스(변환된) 크리덴셜 DB를 업데이트 함
838

도면8c



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제10항

【변경전】

상기 통신 인터페이스는 상기 다른 변환된 크리덴셜 데이터베이스들을 상기 다른 기기들에 배포

【변경후】

통신 인터페이스는 상기 다른 변환된 크리덴셜 데이터베이스들을 상기 다른 기기들에 배포

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 제7항

【변경전】

상기 관리자로부터 상기 통신 인터페이스를 통하여 수신되는 패스워드에 기초하여

【변경후】

관리자로부터 상기 통신 인터페이스를 통하여 수신되는 패스워드에 기초하여