



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0058140
(43) 공개일자 2018년05월31일

(51) 국제특허분류(Int. Cl.)
E05B 47/00 (2018.01) E05B 49/00 (2006.01)
H04L 9/32 (2006.01) H04M 1/725 (2006.01)
(52) CPC특허분류
E05B 47/0001 (2013.01)
E05B 49/00 (2013.01)
(21) 출원번호 10-2016-0156883
(22) 출원일자 2016년11월23일
심사청구일자 2016년11월23일

(71) 출원인
한국기술교육대학교 산학협력단
충남 천안시 동남구 병천면 충절로 1600, 내 (한국기술교육대학교)
(72) 발명자
강형주
대전광역시 서구 둔산북로 160, 4동 1204호 (둔산동, 한마루아파트)
이현수
대전광역시 중구 동서대로 1388, 104동 205호 (목동, 금호한사랑아파트)
(뒷면에 계속)
(74) 대리인
특허법인 남앤드남

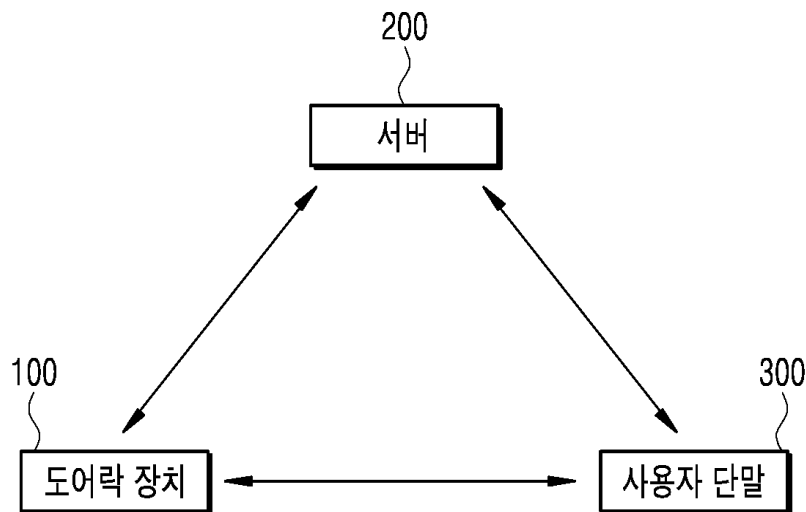
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **도어락제어시스템 및 그 방법**

(57) 요약

본 발명은 사물인터넷 기술을 기반으로 보다 스마트한 기능을 제공할 수 있도록 도어락을 제어함으로써, 기존 도어락 보다 보안성을 향상시키면서도 차별화된 기능을 제공하는 새로운 스마트 도어락 서비스가 실현되도록 하는 도어락제어시스템 및 그 방법을 제안한다.

대표도 - 도1



(52) CPC특허분류

H04L 9/3228 (2013.01)

H04M 1/72519 (2013.01)

H04M 1/72533 (2013.01)

E05B 2047/0095 (2013.01)

(72) 발명자

김재휘

경기도 성남시 중원구 도촌남로 22, 114동 502호
(도촌동, 휴먼시아섬마을1단지아파트)

이주명

충청북도 청주시 흥덕구 장구봉로101번길 27, 1동
408호(복대동, 형석아파트)

명세서

청구범위

청구항 1

비밀번호 입력과 관련되는 키패드의 배열을 랜덤하게 생성하는 도어락장치;

상기 도어락장치와의 통신연결상태를 주기적으로 확인한 결과에 기초하여 상기 도어락장치와 관련되는 특정상황 발생여부를 모니터링 하는 서버; 및

상기 도어락장치를 원격에서 제어하기 위한 적어도 하나의 원격제어기능을 수행하는 사용자단말

을 포함하는 것을 특징으로 하는 도어락제어시스템.

청구항 2

제 1 항에 있어서,

상기 서버는,

상기 도어락장치와의 최초 통신 시, 상기 도어락장치로부터 식별정보를 포함하는 특정비트를 수신하고, 상기 식별정보의 저장여부를 확인한 결과에 기초하여 상기 통신연결상태를 주기적으로 확인하기 위한 타이머를 지정하는 것을 특징으로 하는 도어락제어시스템.

청구항 3

제 2 항에 있어서,

상기 서버는,

상기 타이머에 의해 지정된 시간 동안 상기 특정비트가 주기적으로 수신되면, 상기 통신연결상태를 정상으로 판단하며,

상기 타이머에 의해 지정된 시간 동안 상기 특정비트가 주기적으로 수신되지 않으면, 상기 통신연결상태를 비정상으로 판단하는 것을 특징으로 하는 도어락제어시스템.

청구항 4

제 3 항에 있어서,

상기 특정상황은,

상기 통신연결상태가 비정상인 경우, 상기 도어락장치의 고장/파손, 상기 도어락장치와 상기 서버 간의 네트워크 이상발생 및 상기 도어락장치의 기본동작 수행 중 적어도 하나를 포함하는 것을 특징으로 하는 도어락제어시스템.

청구항 5

제 3 항에 있어서,

상기 사용자단말은,

상기 통신연결상태가 비정상인 경우, 상기 적어도 하나의 원격제어기능 중 임시비밀번호를 생성하는 것과 관련되는 특정원격제어기능을 차단하는 것을 특징으로 하는 도어락제어시스템.

청구항 6

제 1 항에 있어서,

상기 사용자단말은,

상기 도어락장치를 통한 출입이 차단될 수 있도록 보안시간을 설정하며, 상기 보안시간 동안 출입시도가 감지되는 경우에는 부정출입알림정보를 상기 서버로부터 수신하는 것을 특징으로 하는 도어락제어시스템.

청구항 7

제 6 항에 있어서,

상기 도어락장치는,

상기 보안시간 동안 입력된 비밀번호가 소정의 횟수이상 일치하지 않는 경우, 카메라를 통해 사진촬영을 수행하는 것을 특징으로 하는 도어락제어시스템.

청구항 8

제 1 항에 있어서,

상기 도어락장치는,

근거리 무선통신을 통해 상기 사용자단말로부터 특정태그정보가 확인되면, 상기 특정태그정보와 기 저장된 태그정보를 비교한 결과에 기초하여 해당 문의 개폐여부를 결정하는 것을 특징으로 하는 도어락제어시스템.

청구항 9

서버가, 비밀번호 입력과 관련되는 키패드의 배열을 랜덤하게 생성하는 도어락장치와의 통신연결상태를 주기적으로 확인한 결과에 기초하여 상기 도어락장치와 관련되는 특정상황 발생여부를 모니터링 하는 모니터링단계; 및

사용자단말이, 상기 도어락장치를 원격에서 제어하기 위한 적어도 하나의 원격제어기능을 수행하는 원격제어단계를 포함하는 것을 특징으로 하는 도어락제어시스템의 동작방법.

청구항 10

제 9 항에 있어서,

상기 모니터링단계에서 서버가,

상기 도어락장치와의 최초 통신 시, 상기 도어락장치로부터 식별정보를 포함하는 특정비트를 수신하고, 상기 식별정보의 저장여부를 확인한 결과에 기초하여 상기 통신연결상태를 주기적으로 확인하기 위한 타이머를 지정하는 것을 특징으로 하는 도어락제어시스템의 동작방법.

청구항 11

제 10 항에 있어서,

상기 모니터링단계에서 서버가,

상기 타이머에 의해 지정된 시간 동안 상기 특정비트가 주기적으로 수신되면, 상기 통신연결상태를 정상으로 판단하며,

상기 타이머에 의해 지정된 시간 동안 상기 특정비트가 주기적으로 수신되지 않으면, 상기 통신연결상태를 비정상으로 판단하는 것을 특징으로 하는 도어락제어시스템의 동작방법.

청구항 12

제 11 항에 있어서,

상기 특정상황은,

상기 통신연결상태가 비정상인 경우, 상기 도어락장치의 고장/파손, 상기 도어락장치와 상기 서버 간의 네트워크 이상발생 및 상기 도어락장치의 기본동작 수행 중 적어도 하나를 포함하는 것을 특징으로 하는 도어락제어시스템의 동작방법.

청구항 13

제 9 항에 있어서,

상기 원격제어단계에서 상기 사용자단말이,

상기 통신연결상태가 비정상인 경우, 상기 적어도 하나의 원격제어기능 중 임시비밀번호를 생성하는 것과 관련되는 특정원격제어기능을 차단하는 단계를 포함하는 것을 특징으로 하는 도어락제어시스템의 동작방법.

청구항 14

제 9 항에 있어서,

상기 원격제어단계에서 상기 사용자단말이,

상기 도어락장치를 통한 출입이 차단될 수 있도록 보안시간을 설정하며, 상기 보안시간 동안 출입시도가 감지되는 경우에는 부정출입알림정보를 상기 서버로부터 수신하는 단계를 더 포함하는 것을 특징으로 하는 도어락제어시스템의 동작방법.

청구항 15

제 14 항에 있어서,

상기 도어락장치가, 상기 보안시간 동안 입력된 비밀번호가 소정의 횟수이상 일치하지 않는 경우, 카메라를 통해 사진촬영을 수행하는 단계; 및

상기 도어락장치가, 근거리 무선통신을 통해 상기 사용자단말로부터 특정태그정보가 확인되면, 상기 특정태그정보와 기 저장된 태그정보를 비교한 결과에 기초하여 상기 도어락장치가 설치된 문의 개폐여부를 결정하는 단계를 더 포함하는 것을 특징으로 하는 도어락제어시스템의 동작방법.

발명의 설명

기술 분야

[0001] 본 발명은 스마트 도어락 기술에 관한 것으로, 더욱 상세하게는, 사물인터넷 기술을 기반으로 보다 스마트한 기능을 제공하기 위한 도어락 제어 방안에 관한 것이다.

배경 기술

[0002] 최근 사물 인터넷(Internet of Things, IoT) 기술에 대한 관심이 높아지면서, 실생활에서 사용할 IoT 기기의 종류도 점차 다양화되는 추세에 있다.

[0003] 여기서, 사물인터넷이란, 각종 사물에 센서와 통신 기능을 내장하여 인터넷에 연결하는 기술을 말하는 것으로, 웨어러블 디바이스를 비롯한 가전제품, 모바일 장치 등 다양한 사물을 일컫는다.

[0004] 이러한 사물인터넷 기술은, 스마트 카, 스마트 홈, 헬스케어 등 다양한 분야에서 사용되고 있으며, 특히 실생활에 가장 밀접한 스마트 홈에 대한 사용자의 관심이 집중적으로 증가하고 있다.

[0005] 한편, 현대 사회에서 점차 1인가구가 늘어나면서 사람들이 집에서 보내는 시간이 줄어들고 있으며, 이러한 변화에 따라 주거침입과 관련되는 범죄 건수도 함께 증가하는 추세이다.

[0006] 따라서, 사물인터넷 기술을 적용하여 주거침입과 관련되는 범죄를 예방을 위해 도어락의 보안성을 보다 향상시키면서도 기존 도어락과 다른 스마트한 기능을 제공할 수 있는 스마트 도어락과 관련되는 기술이 요구된다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 상기한 사정을 감안하여 창출된 것으로서, 본 발명에서 도달하고자 하는 목적은, 사물인터넷 기술을 기반으로 보다 스마트한 기능을 제공할 수 있도록 도어락을 제어함으로써, 기존 도어락 보다 보안성을 향상시키면서도 차별화된 기능을 제공할 수 있는, 새로운 스마트 도어락 서비스가 실현되도록 하는데 있다.

과제의 해결 수단

- [0008] 상기 목적을 달성하기 위한 본 발명에 따른 도어락제어시스템은, 비밀번호 입력과 관련되는 키패드의 배열을 랜덤하게 생성하는 도어락장치; 상기 도어락장치와의 통신연결상태를 주기적으로 확인한 결과에 기초하여 상기 도어락장치와 관련되는 특정상황 발생여부를 모니터링 하는 서버; 및 상기 도어락장치를 원격에서 제어하기 위한 적어도 하나의 원격제어기능을 수행하는 사용자단말을 포함하는 것을 특징으로 한다.
- [0009] 상기 서버는, 상기 도어락장치와의 최초 통신 시, 상기 도어락장치로부터 식별정보를 포함하는 특정비트를 수신하고, 상기 식별정보의 저장여부를 확인한 결과에 기초하여 상기 통신연결상태를 주기적으로 확인하기 위한 타이머를 지정하는 것을 특징으로 한다.
- [0010] 상기 서버는, 상기 타이머에 의해 지정된 시간 동안 상기 특정비트가 주기적으로 수신되면, 상기 통신연결상태를 정상으로 판단하며, 상기 타이머에 의해 지정된 시간 동안 상기 특정비트가 주기적으로 수신되지 않으면, 상기 통신연결상태를 비정상으로 판단하는 것을 특징으로 한다.
- [0011] 상기 특정상황은, 상기 통신연결상태가 비정상인 경우, 상기 도어락장치의 고장/파손, 상기 도어락장치와 상기 서버 간의 네트워크 이상발생 및 상기 도어락장치의 기본동작 수행 중 적어도 하나를 포함하는 것을 특징으로 한다.
- [0012] 상기 사용자단말은, 상기 통신연결상태가 비정상인 경우, 상기 적어도 하나의 원격제어기능 중 임시비밀번호를 생성하는 것과 관련되는 특정원격제어기능을 차단하는 것을 특징으로 한다.
- [0013] 상기 사용자단말은, 상기 도어락장치를 통한 출입이 차단될 수 있도록 보안시간을 설정하며, 상기 보안시간 동안 출입시도가 감지되는 경우에는 부정출입알림정보를 상기 서버로부터 수신하는 것을 특징으로 한다.
- [0014] 상기 도어락장치는, 상기 보안시간 동안 입력된 비밀번호가 소정의 횟수이상 일치하지 않는 경우, 카메라를 통해 사진촬영을 수행하는 것을 특징으로 한다.
- [0015] 상기 도어락장치는, 근거리 무선통신을 통해 상기 사용자단말로부터 특정태그정보가 확인되면, 상기 특정태그정보와 기 저장된 태그정보를 비교한 결과에 기초하여 해당 문의 개폐여부를 결정하는 것을 특징으로 한다.
- [0016] 상기 목적을 달성하기 위한 본 발명에 따른 도어락제어시스템의 동작방법은, 서버가, 비밀번호 입력과 관련되는 키패드의 배열을 랜덤하게 생성하는 도어락장치와의 통신연결상태를 주기적으로 확인한 결과에 기초하여 상기 도어락장치와 관련되는 특정상황 발생여부를 모니터링 하는 모니터링단계; 및 사용자단말이, 상기 도어락장치를 원격에서 제어하기 위한 적어도 하나의 원격제어기능을 수행하는 원격제어단계를 포함하는 것을 특징으로 한다.
- [0017] 상기 모니터링단계에서 서버가, 상기 도어락장치와의 최초 통신 시, 상기 도어락장치로부터 식별정보를 포함하는 특정비트를 수신하고, 상기 식별정보의 저장여부를 확인한 결과에 기초하여 상기 통신연결상태를 주기적으로 확인하기 위한 타이머를 지정하는 것을 특징으로 한다.
- [0018] 상기 모니터링단계에서 서버가, 상기 타이머에 의해 지정된 시간 동안 상기 특정비트가 주기적으로 수신되면, 상기 통신연결상태를 정상으로 판단하며, 상기 타이머에 의해 지정된 시간 동안 상기 특정비트가 주기적으로 수신되지 않으면, 상기 통신연결상태를 비정상으로 판단하는 것을 특징으로 한다.
- [0019] 상기 특정상황은, 상기 통신연결상태가 비정상인 경우, 상기 도어락장치의 고장/파손, 상기 도어락장치와 상기 서버 간의 네트워크 이상발생 및 상기 도어락장치의 기본동작 수행 중 적어도 하나를 포함하는 것을 특징으로 한다.
- [0020] 상기 원격제어단계에서 상기 사용자단말이, 상기 통신연결상태가 비정상인 경우, 상기 적어도 하나의 원격제어기능 중 임시비밀번호를 생성하는 것과 관련되는 특정원격제어기능을 차단하는 단계를 포함하는 것을 특징으로 한다.
- [0021] 상기 원격제어단계에서 상기 사용자단말이, 상기 도어락장치를 통한 출입이 차단될 수 있도록 보안시간을 설정하며, 상기 보안시간 동안 출입시도가 감지되는 경우에는 부정출입알림정보를 상기 서버로부터 수신하는 단계를 더 포함하는 것을 특징으로 한다.
- [0022] 상기 도어락장치가, 상기 보안시간 동안 입력된 비밀번호가 소정의 횟수이상 일치하지 않는 경우, 카메라를 통해 사진촬영을 수행하는 단계; 및 상기 도어락장치가, 근거리 무선통신을 통해 상기 사용자단말로부터 특정태그정보가 확인되면, 상기 특정태그정보와 기 저장된 태그정보를 비교한 결과에 기초하여 상기 도어락장치가 설치된 문의 개폐여부를 결정하는 단계를 더 포함하는 것을 특징으로 한다.

발명의 효과

[0023] 이에, 본 발명의 도어락제어시스템 및 그 방법에 의하면, 사물인터넷 기술을 기반으로 보다 스마트한 기능을 제공할 수 있도록 도어락을 제어함으로써, 기존 도어락 보다 보안성을 향상시키면서도 차별화된 기능을 제공하는 새로운 스마트 도어락 서비스를 실현시킬 수 있다.

도면의 간단한 설명

[0024] 도 1은 본 발명의 실시예에 따른 도어락제어시스템을 나타내는 도면이다.
 도 2는 본 발명의 실시예에 따른 도어락장치의 개략적인 구성도를 나타내는 도면이다.
 도 3은 본 발명의 실시예에 따른 서버의 개략적인 구성도를 나타내는 도면이다.
 도 4는 본 발명의 실시예에 따른 임시비밀번호를 생성하여 친구초대를 수행하는 일례를 나타내는 도면이다.
 도 5는 본 발명의 실시예에 따른 사용자단말의 개략적인 구성도를 나타내는 도면이다.
 도 6은 본 발명의 실시예에 따른 원격 제어를 위해 애플리케이션을 통해 제공되는 화면의 일례를 나타내는 도면이다.
 도 7은 본 발명의 실시예에 따른 스마트 도어락 서비스를 제공하는 흐름을 나타내는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0025] 본 명세서에서 사용되는 기술적 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아님을 유의해야 한다. 또한, 본 명세서에서 사용되는 기술적 용어는 본 명세서에서 특별히 다른 의미로 정의되지 않는 한, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 의미로 해석되어야 하며, 과도하게 포괄적인 의미로 해석되거나, 과도하게 축소된 의미로 해석되지 않아야 한다. 또한, 본 명세서에서 사용되는 기술적인 용어가 본 발명의 사상을 정확하게 표현하지 못하는 잘못된 기술적 용어일 때에는, 당업자가 올바르게 이해할 수 있는 기술적 용어로 대체되어 이해되어야 할 것이다. 또한, 본 발명에서 사용되는 일반적인 용어는 사전에 정의되어 있는 바에 따라, 또는 전후 문맥상에 따라 해석되어야 하며, 과도하게 축소된 의미로 해석되지 않아야 한다.

[0026] 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시예를 상세히 설명하되, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 또한, 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 발명의 사상을 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 발명의 사상이 제한되는 것으로 해석되어서는 아니됨을 유의해야 한다. 본 발명의 사상은 첨부된 도면 외에 모든 변경, 균등물 내지 대체물에 까지도 확장되는 것으로 해석되어야 한다.

[0027] 이하, 첨부된 도면을 참조하여 본 발명의 일 실시예에 대하여 설명한다.

[0028] 먼저, 도 1을 참조하여 본 발명의 도어락제어시스템을 설명하도록 하겠다.

[0029] 도 1에 도시된 바와 같이, 본 발명의 도어락제어시스템은, 비밀번호 입력과 관련되는 키패드의 배열을 랜덤하게 생성하는 도어락장치(100), 도어락장치(100)와의 통신연결상태를 주기적으로 확인한 결과에 기초하여 도어락장치(100)와 관련되는 특정상황 발생여부를 모니터링 하는 서버(200), 및 도어락장치(100)를 원격에서 제어하기 위한 적어도 하나의 원격제어기능을 수행하는 사용자단말(300)을 포함하는 것을 특징으로 한다.

[0030] 이러한 도어락제어시스템의 각 장치들은, 사물인터넷(Internet of Things, 이하 IoT) 기술을 기반으로 보다 스마트한 기능을 제공할 수 있도록 네트워크를 통해 서로 연동하여 동작한다.

[0031] 여기서, 네트워크는 근거리 통신망(Local Area Network; LAN), 광역 통신망(Wide Area Network; WAN) 또는 부가가치 통신망(Value Added Network; VAN) 등과 같은 유선 네트워크나 이동 통신망(mobile radio communication network), 위성 통신망, 블루투스(Bluetooth), Wibro(Wireless Broadband Internet), HSDPA(High Speed Downlink Packet Access) 등과 같은 모든 종류의 무선 네트워크로 구현될 수 있으며, IoT 기술에 적용될 수만 있다면 특별한 제한을 두지 않는다.

[0032] 이에, 본 발명의 도어락제어시스템은, IoT 기술을 기반으로 도어락장치(100)를 제어함으로써, 기존 도어락 보다

보안성을 향상시키면서도 차별화된 기능에 따른 도어락 서비스(이하, 스마트 도어락 서비스)를 제공할 수 있는데, 이하에서는 이러한 스마트 도어락 서비스를 제공하기 위한 각 장치의 특징에 대하여 보다 구체적으로 설명하도록 하겠다.

- [0033] 먼저, 도어락장치(100)의 구성에 대하여 보다 구체적으로 설명하도록 하겠다.
- [0034] 도어락장치(100)는, 도어락에서 일반적으로 제공하는 문의 개폐, 오작동 알림 등의 기본동작을 수행하는 한편, 네트워크를 통해 서버(200) 및 사용자단말(300)과 연동하여 스마트 도어락 서비스를 제공하는 장치일 수 있다. 이때, 문의 개폐를 위해 비밀번호뿐만 아니라 음성인식, 지문인식 등과 같은 다양한 수단이 이용될 수도 있다.
- [0035] 이러한 도어락장치(100)는, 도 2에 도시된 바와 같이, 키패드관리부(110), 기능제어부(120), 카메라부(130), 저장부(140), 표시부(150) 및 근거리통신부(160)를 포함하는 구성을 가질 수 있다.
- [0036] 키패드관리부(110)는, 보안성을 향상을 위해 비밀번호 입력과 관련되는 키패드의 배열을 랜덤으로 생성한다.
- [0037] 보다 구체적으로, 키패드관리부(110)는, 사용자가 비밀번호를 입력하기 위해 키패드의 표시와 관련되는 제어(예: 키 누름/터치)를 수행하는 경우, 키패드의 배열을 랜덤으로 생성한다.
- [0038] 즉, 키패드관리부(110)는, 사용자가 비밀번호를 입력할 때 타인이 키패드의 위치를 외우지 못하도록 키패드 상에 출력되는 숫자들의 위치를 매번 새로운 위치로 배열하게 된다.
- [0039] 이에, 사용자가 비밀번호를 입력할 때, 비밀번호에 대응하는 키패드의 위치가 외부에 노출되더라도 랜덤하게 배열되는 키패드에 의해 부정출입 자체를 미연에 차단할 수 있게 되는 것이다.
- [0040] 기능제어부(120)는, 도어락에서 일반적으로 제공하는 문의 개폐, 오작동 알림 등의 기본동작이 수행될 수 있도록 제어한다.
- [0041] 보다 구체적으로, 기능제어부(120)는, 사용자가 문을 열기 위해 비밀번호를 입력하는 경우, 입력된 비밀번호와 기 설정된 비밀번호를 비교한 결과에 기초하여 문의 개폐여부를 결정한다.
- [0042] 즉, 입력된 비밀번호와 기 설정된 비밀번호가 일치하면, 기능제어부(120)는, 정상적인 출입인 것으로 판단하여 문의 열리도록 제어한다.
- [0043] 한편, 입력된 비밀번호와 기 설정된 비밀번호가 일치하지 않으면, 기능제어부(120)는, 비정상적인 출입을 시도하는 것으로 판단하여 문의 열리지 않도록 제어한다.
- [0044] 이후, 비정상적인 출입이 소정의 횟수이상 시도되는 경우, 기능제어부(120)는, 카메라를 통해 전방을 촬영하여 부정시도영상을 생성하고, 출입로그를 확인한다. 이어서, 기능제어부(120)는, 부정시도영상 및 출입로그를 포함하는 부정출입판단정보를 서버(200)로 전달한다.
- [0045] 이에, 서버(200)는, 푸시서버(Firebase Cloud Messaging Server)로서의 기능을 수행하여, 부정출입판단정보를 기반으로 부정출입알림정보인 푸시 메시지를 생성하고, 이를 사용자단말(300)로 전송하게 된다. 본 발명의 실시예에서는 서버(200)에 푸시서버의 기능이 포함되는 것으로 언급하였으나, 이에 한정되지 않으며, 서버(200)와 푸시서버가 별도의 장치로 구분되도록 구현할 수도 있음은 물론이다.
- [0046] 그러면, 사용자단말(300)은, 푸시 메시지를 수신하게 되며, 도어락장치(100)로부터 수신된 부정출입판단정보를 확인할 수 있게 되는 것이다. 여기서, 푸시 메시지는, 기본적으로 특정 사용자에게 전송되나, 도어락장치(100)를 이용하는 다수의 사용자에게 전송될 수도 있다.
- [0047] 전술에 따라 부정출입이 감지된 경우, 기존에는 도어락장치(100)가 단순히 경보를 발생시켜 부정출입을 알리는 방식이었기 때문에택내에 사용자가 없는 경우에는 경보를 확인할 수 없어 부정출입에 용이하게 대처할 수 없었으나, 본 발명에서는 부정출입판단정보, 즉 부정시도영상과 출입로그를 푸시 메시지 형식으로 실시간으로 제공할 수 있으므로, 부정출입에 대해 신속하고 용이하게 대처할 수 있게 되는 것이다.
- [0048] 한편, 기능제어부(120)는, 사용자단말(300)로부터 도어락장치(100)를 통한 출입이 차단될 수 있도록 보안시간이 설정되는 경우, 보안시간 동안 출입이 시도되었는지를 감시한다.
- [0049] 여기서, 보안시간이라 함은, 도어락장치(100)를 통한 모든 출입이 차단될 수 있도록 사용자가 설정한 시간이며, 이 시간 동안에 키패드가 동작하는 것을 부정출입으로 간주하게 된다.
- [0050] 즉, 기능제어부(120)는, 보안시간 동안 출입을 위해 도어락장치(100)의 키패드가 동작하게 되면, 부정출입으로

간주하고 전술에서 언급한 바와 같이 비정상적인 출입을 알리기 위한 부정출입판단정보를 생성하여 서버(200)로 전달한다.

- [0051] 그러면, 서버(200)에서는 부정출입판단정보를 기반으로 푸시 메시지를 생성하여 사용자단말(300)로 전송하게 된다. 이에, 사용자단말(300)은, 푸시 메시지를 수신하게 되며, 도어락장치(100)로부터 수신된 부정출입판단정보를 확인할 수 있게 된다.
- [0052] 저장부(140)는, 스마트 도어락 서비스를 제공하기 위해 송수신되는 모든 정보(예: 기 설정된 비밀번호, 출입로그, 부정시도영상 등)를 저장한다.
- [0053] 표시부(150)는, 도어락장치(100)의 구동 시 사용자에게 정보를 출력하여 표시하기 위한 영역일 수 있으며, 액정 표시장치(Liquid Crystal Display, LCD) 등과 같은 표시장치일 수 있다.
- [0054] 근거리통신부(160)은, 근거리 무선통신을 통해 입력된 특정태그정보를 확인하여 문의 개폐여부를 결정한다.
- [0055] 보다 구체적으로, 근거리통신부(160)은, 근거리 무선통신을 통해 사용자단말(300)로부터 특정태그정보가 확인되면, 특정태그정보와 기 저장된 태그정보를 비교한 결과에 기초하여 해당 문의 개폐여부를 결정한다.
- [0056] 즉, 근거리통신부(160)은, 근거리 무선통신을 통해 사용자단말(300)이 접속한 것으로 확인되면, 사용자단말(300)로부터 태그식별자(user identifier, 이하 UID)를 검출한다. 이어서, 근거리통신부(160)은, 서버(200)로 기 저장된 태그식별자(UID)를 수신한다.
- [0057] 이후, 근거리통신부(160)은, 기 저장된 태그식별자(UID)와 검출한 태그식별자(UID)를 비교한다.
- [0058] 즉, 기 저장된 태그식별자(UID)와 검출한 태그식별자(UID)가 일치하면, 근거리통신부(160)은, 정상적인 출입인 것으로 판단하여 서버(200)에 출입로그를 남기고 문을 연다. 한편, 기 저장된 태그식별자(UID)와 검출한 태그식별자(UID)가 일치하지 않으면, 근거리통신부(160)은, 비정상적인 출입을 시도하는 것으로 판단하여 문의 열리지 않도록 제어한다.
- [0059] 다음은, 서버(200)의 구성에 대하여 보다 구체적으로 설명하도록 하겠다.
- [0060] 서버(200)는, 스마트 도어락 서비스를 제공하는 것과 관련되는 전반적인 관리/제어 및 네트워크의 연결을 유지하는 기능을 수행하게 된다.
- [0061] 특히, 서버(200)는, 도어락장치(100)와의 통신연결상태를 주기적으로 확인한 결과에 기초하여 도어락장치(100)와 관련되는 특정상황 발생여부를 모니터링 하는 기능을 수행한다.
- [0062] 이러한 서버(200)는, 도 3에 도시된 바와 같이, 모니터링부(210), 서비스관리부(220) 및 저장부(230)를 포함하는 구성을 가질 수 있다.
- [0063] 모니터링부(210)는, 도어락장치(100)와의 통신연결상태를 주기적으로 확인한다.
- [0064] 보다 구체적으로, 모니터링부(210)는, 도어락장치(100)와의 최초 통신 시, 도어락장치(100)로부터 식별정보를 포함하는 특정비트를 수신하고, 식별정보의 저장여부를 확인한 결과에 기초하여 통신연결상태를 주기적으로 확인하기 위한 타이머를 지정한다.
- [0065] 여기서, 특정비트는, 서버 프로그램에서 수행하는 "하트비트(HeartBeat)"라는 기능에 의해 송수신되며, 심장 박동과 같이 서버(200)와 도어락장치(100) 사이의 통신연결이 지속되고 있는 지를 확인할 수 있는 신호일 수 있다. 이러한 특정비트에는, 서버(200)가 다수의 도어락장치를 구분할 수 있도록 각 도어락장치 별 식별정보, 즉 IP 주소(Address)가 포함되게 된다.
- [0066] 즉, 모니터링부(210)는, 도어락장치(100)로부터 식별정보를 포함하는 특정비트가 수신되면, 특정비트로부터 식별정보를 검출한다. 이후, 모니터링부(210)는, 저장부(230)에 기 저장된 사용자정보데이터를 기반으로 식별정보의 존재여부를 확인한 결과에 기초하여 타이머를 지정하게 된다.
- [0067] 이때, 기 저장된 사용자정보데이터에 식별정보가 저장되어 있지 않은 경우에는, 도어락장치(100)가 신규 등록하는 것으로 판단하여 검출된 식별정보를 사용자정보데이터에 저장하는 과정을 먼저 수행하게 될 것이다.
- [0068] 만일, 기 저장된 사용자정보데이터에 식별정보가 저장되어 있으면, 모니터링부(210)는, 도어락장치(100)가 신규 등록을 완료한 이후 특정비트를 전송한 것이므로, 통신연결상태를 주기적으로 확인하기 위한 타이머를 지정하게 된다.

- [0069] 전술에 따라 타이머가 지정되면, 모니터링부(210)는, 타이머에 의해 지정된 시간 동안 특정비트가 주기적으로 수신되는지의 여부를 확인한다.
- [0070] 즉, 타이머에 의해 지정된 시간 동안 특정비트가 주기적으로 수신되면, 모니터링부(210)는, 특정비트에 포함된 식별정보에 해당하는 도어락장치(100)와의 통신연결상태가 정상인 것으로 판단한다. 이후, 모니터링부(210)는, 타이머가 만료되기 이전에 이를 리셋하여 지속적으로 통신연결상태를 확인하게 된다.
- [0071] 한편, 타이머에 의해 지정된 시간 동안 특정비트가 주기적으로 수신되지 않으면, 모니터링부(210)는, 특정비트에 포함된 식별정보에 해당하는 도어락장치(100)와의 통신연결상태가 비정상인 것으로 판단하게 된다.
- [0072] 즉, 모니터링부(210)는, 식별정보에 해당하는 도어락장치(100)와의 통신연결이 특정상황에 의해 종료된 것으로 판단하고, 특정상황이 발생하였음을 사용자단말(300)로 알리게 된다.
- [0073] 여기서, 특정상황은, 식별정보에 해당하는 도어락장치(100)의 고장/파손, 식별정보에 해당하는 도어락장치(100)와 서버(200) 간의 네트워크 이상발생 및 도어락 기본동작 수행 중 적어도 하나를 포함하는 것일 수 있다.
- [0074] 이에, 사용자는 도어락장치(100)와 관련되는 특정상황의 발생여부를 원격에서 모니터링할 수 있게 되므로, 원격에 위치하는 도어락장치(100)의 물리적인 고장/파손 및 네트워크 이상발생여부를 실시간으로 확인하여 대처할 수 있음은 물론, 기존 보다 보안성이 강화된 도어락 서비스를 제공받을 수 있게 되는 것이다.
- [0075] 한편, 특정상황이 도어락 기본동작 수행(예: 문의 개폐)으로 발생한 경우에는 기본동작 수행(예: 문의 개폐) 이후 끊겼던 특정비트가 다시 정상적으로 수신되는지의 여부를 확인하고, 정상적으로 수신되는 경우에는 특정상황이 종료되었음을 사용자단말(300)로 알리는 것이 바람직할 것이다.
- [0076] 서비스관리부(220)는, 모니터링부(210)로부터 특정상황의 발생여부를 확인한 결과에 기초하여 서비스의 차단여부를 결정한다. 이하에서는 특정상황이 도어락 기본동작이 아닌, 도어락장치(100)의 고장/파손이나 네트워크 이상발생인 것으로 언급하여 설명하도록 하겠다.
- [0077] 보다 구체적으로, 서비스관리부(220)는, 모니터링부(210)에 의해 특정상황이 발생한 것이 확인되면, 통신연결상태가 비정상적인 상황이므로 원격제어기능의 일부가 수행되지 않도록 제어하게 된다.
- [0078] 즉, 서비스관리부(220)는, 통신연결상태가 비정상인 경우, 사용자단말(300)에서 수행 가능한 적어도 하나의 원격제어기능 중 임시비밀번호를 생성하는 것과 관련되는 특정원격제어기능을 차단하게 된다.
- [0079] 여기서, 임시비밀번호는, 사용자에게 의해 기 설정되는 비밀번호와 다르게 한번 사용이 이루어지게 되면, 더 이상 사용할 수 없게 삭제되는데, 삭제 방식의 경우, 사용자가 직접 사용자단말(300)을 이용하여 삭제할 수도 있으며, 소정의 시간 이후 자동적으로 삭제하는 방식 등으로 구현될 수 있다.
- [0080] 이와 관련하여, 도 4에는 임시비밀번호를 생성하여 친구초대를 수행하는 일례가 도시되어 있다.
- [0081] 도 4에 도시된 바와 같이, 사용자단말(300)로부터 임시비밀번호를 생성하는 것과 관련되는 특정원격제어기능이 요청되는 경우, 서버(200)는, 특정비트를 기반으로 도어락장치(100)와 서버(200) 사이의 통신연결상태가 정상적으로 지속되고 있는지를 확인한 결과에 기초하여 임시비밀번호를 생성하게 된다(S10-S12).
- [0082] 즉, 서버(200)는, 통신연결상태가 정상적인 경우에 한해 임시비밀번호를 생성하고, 이를 도어락장치(100)와 공유하게 된다. 이후, 서버(200)는, 임시비밀번호를 사용자단말(300)로 전송한다.
- [0083] 그러면, 사용자단말(300)에는 임시비밀번호가 표시되며, 사용자는 표시된 임시비밀번호를 다양한 메시지 전송방식(예: SMS, 카카오톡 등)을 통해 피초대자의 단말로 전송하게 된다(S13).
- [0084] 이처럼 피초대자의 단말로 임시비밀번호가 전송되어 피초대자가 도어락장치(100)의 키패드에 임시비밀번호를 입력하게 되면, 도어락장치(100)는, 서버(200)로부터 수신한 임시비밀번호와 피초대자에 의해 입력된 임시비밀번호의 일치 여부를 확인한 결과에 기초하여 도어락장치(100)가 설치된 해당 문의 개폐여부를 결정하게 된다(S14).
- [0085] 전술에서 확인한 바와 같이, 임시비밀번호를 생성하고 이를 이용하는 것은 보안에 있어서 중요한 부분이므로, 본 발명에서는 도어락장치(100)와 서버(200) 간의 통신연결상태가 비정상적인 경우에는 임시비밀번호를 생성하는 것과 관련되는 특정원격제어기능을 차단하게 되는 것이다.
- [0086] 다시 도 3을 참고하면, 저장부(230)는, 스마트 도어락 서비스를 제공하기 위한 모든 정보를 저장한다.

[0087] 즉, 저장부(230)는, 스마트 도어락 서비스를 제공하기 위해 도어락장치(100)와의 연동 시 송수신되는 모든 정보를 저장하는 한편, 사용자단말(300)과의 연동 시 송수신되는 모든 정보를 저장하게 된다.

[0088] 이러한 정보들은, PHP(Hypertext Preprocessor) 파일형식으로 저장되므로, 사용자단말(300)에서 PHP 파일을 호출하여 저장부(230)로부터 데이터를 가져오거나 변경할 수 있게 된다.

[0089] 본 발명의 실시예에서는 사용자단말(300)이 서버(200)를 통해 PHP 파일에 접근하고, 직접 서버(200)의 저장부(230)에 접속한 후 쿼리를 사용하여 정보를 전송하는 것으로 언급하였으나, 이에 한정되지 않으며, 클라우드 서버(예: 푸시서버)를 사용하여 서버(200)의 저장부(230)를 관리하는 방식으로 저장부(230)에 저장된 정보를 전송할 수도 있음은 물론이다.

[0090] 이하에서는 저장부(230)에 저장되는 정보에 대하여 표1 내지 표 7을 참고하여 보다 구체적으로 설명하도록 하겠다.

[0091] 먼저, 표 1은 사용자정보테이블이며, 사용자ID와 사용자 비밀번호, 도어락 비밀번호, 사용자 이름, 사용자 IP주소, 도어락 시리얼넘버 등과 같은 사용자정보가 저장되게 된다.

표 1

필드명	설명
id	사용자 ID
id_password	사용자 비밀번호
doorlock_password	도어락 비밀번호
user_name	사용자 이름
ip_address	사용자 IP주소
serial_number	도어락 시리얼넘버

[0092]

[0093] 즉, 사용자정보테이블에는, 도어락장치(100)를 사용하는 사용자가 사용자단말(300)에 설치된 어플리케이션을 이용하기 위한 ID와, 도어락장치(100)를 이용하기 위한 ID를 공유하고 있으며, 통신연결상태를 주기적으로 확인하기 위한 IP주소 등이 포함되게 된다.

[0094] 다음, 표 2는 보안정보테이블이며, 도어락장치(100)를 통한 출입이 차단될 수 있도록 보안시간 설정과 관련되는 정보들이 저장되게 된다.

표 2

필드명	설명
id	사용자 ID
st.mon.start	월요일 시작시간
st.mon.stop	월요일 종료시간
...	...
st.sun.start	일요일 시작시간
st.sun.stop	일요일 종료시간

[0095]

[0096] 즉, 보안정보테이블에는, 최초 회원가입으로 사용자ID가 생성되면, 보안시간이 디폴드(default) 값인 0:0(시간에 대한 디폴드 값)으로 저장된다.

[0097] 다음, 표 3은 로그(Logs)테이블이며, 도어락장치(100)의 출입로그에 해당하는 출입 시간, 출입 성공여부, 사용자ID 등이 저장되게 된다.

표 3

필드명	설명
enter_time	출입시간
access_check	출입 성공여부
id	사용자 ID

[0098]

[0099] 다음, 표 4은 임시비밀번호관련테이블이며, 사용자ID와 임시비밀번호가 저장되게 된다.

표 4

필드명	설명
id	사용자 ID
temp_password	임시비밀번호

[0100]

[0101] 이러한 임시비밀번호관련테이블에 저장된 임시비밀번호의 경우, 한번 출입을 하기 위해 이용되면 임시비밀번호 관련테이블로부터 즉시 삭제되도록 구현되게 된다.

[0102] 다음, 표 5는 푸시관련테이블이며, 사용자ID와 사용자단말(300)의 애플리케이션에서 사용되는 토큰(Token)이 저장되게 된다.

표 5

필드명	설명
id	사용자 ID
token	안드로이드 토큰

[0103]

[0104] 즉, 푸시관련테이블에는, 사용자단말(300)에 애플리케이션이 최초 설치가 되었을 때 생성되는 일종의 애플리케이션 ID인 토큰이 저장된다. 이러한 토큰은, 애플리케이션의 삭제여부에 따라 삭제되거나 재설치 되게 된다.

[0105] 다음, 표 6은 태그식별자(UID)테이블이며, 근거리 무선통신(예: NFC)을 통해 접속하는 특정태그(Tag)에 대응하는 태그식별자(UID)가 저장되게 된다.

표 6

필드명	설명
id	사용자 ID
uid_num	nfc uid 정보

[0106]

[0107] 다음, 표 7은 부정출입관련테이블이며, 카메라를 통해 전방을 촬영하여 생성된 부정시도영상, 저장부(230)에서의 파일명, 업로드 시간, 사용자 ID 등이 포함되게 된다. 이때, 업로드 시간은, 카메라로부터 촬영된 시간에 대응하는 시간일 수 있다.

표 7

필드명	설명
upload_filename	사진파일명
db_filename	Db파일저장명
File_type	확장자
Upload_date	업로드 시간
Id	사용자 ID

[0108]

[0109]

[0110]

[0111]

[0112]

[0113]

[0114]

[0115]

[0116]

[0117]

[0118]

[0119]

[0120]

[0121]

[0122]

[0123]

다음은, 사용자단말(300)의 구성에 대하여 보다 구체적으로 설명하도록 하겠다.

사용자단말(300)은, 도어락장치(100)를 원격에서 제어하기 위한 적어도 하나의 원격제어기능을 수행한다.

이러한 사용자단말(200)은, 상대방과의 통화를 시도(발신)하거나 또는 상대방으로부터 시도되는 통화를 수신(착신)하는 등 기본적인 통화 서비스를 이용할 수 있는 디바이스로서, 유선 단말일 수도 있고 무선 단말일 수도 있다.

물론, 사용자단말(300)은, 기본적인 통화 서비스 외에도, 메시지(예: SMS, MMS 등)를 발/착신하는 등의 메시지 서비스와, 데이터 다운로드 및 정보 검색 등의 데이터 서비스를 이용할 수도 있다.

예를 들어, 위 사용자단말(300)로는 예컨대, 스마트 폰, 태블릿 PC, 및 PDA 등이 해당될 수 있으며, 이에 제한되는 것이 아닌 도어락장치(100)의 원격 제어가 가능한 장치는 모두 포함될 수 있다.

한편, 사용자단말(300)에서의 스마트 도어락 서비스가 가능하게 하는 매체로는 예컨대, 사용자단말(300) 자체에서 실행되는 애플리케이션 또는 사용자단말(300)에서 브라우저를 호출하여 접속할 수 있는 온라인 서비스페이지가 해당될 수 있는 데, 본 발명의 실시예에서는 사용자단말(300)에서 스마트 도어락 서비스를 가능하게 하는 매체가 애플리케이션임을 전제 하기로 한다.

이처럼 스마트 도어락 서비스를 위한 애플리케이션이 설치된 사용자단말(300)은, 도 5에 도시된 바와 같이, 원격제어부(310), 근거리통신부(320) 및 표시관리부(330)를 포함하는 구성을 가질 수 있다.

원격제어부(310)는, 사용자가 도어락장치(100)의 원격 제어를 위해 애플리케이션을 실행하면, 원격 제어를 위한 관련 화면을 애플리케이션을 통해 제공하게 된다.

이와 관련하여, 도 6의 (㉠ 내지 ㉦)에는 원격 제어를 위해 애플리케이션을 통해 제공되는 화면의 일례가 도시되어 있다.

사용자에 의해 원격 제어를 위해 애플리케이션이 실행되면, 원격제어부(310)는, 도 6의 (㉠)에 도시된 바와 같이, 사용자단말(300)의 표시부(예: LCD)에 메인 화면을 표시하게 된다.

이러한 메인 화면을 통해 사용자는, 원클릭으로 로그인을 수행할 수도 있으며, 다수의 사용자ID도 저장할 수 있게 된다. 만일, 스마트 도어락 서비스를 최초 이용하는 사용자인 경우에는 회원가입을 수행할 수도 있다.

전술에 따라 로그인이 완료되면, 원격제어부(310)는, 도 6의 (㉡)에 도시된 바와 같이, 원격 제어를 위한 메뉴 화면을 표시하게 된다. 이러한 메뉴 화면에는, 사용자가 이용 가능한 적어도 하나의 원격제어기능과 관련되는 원격제어메뉴목록(400)이 포함된다.

여기서, 원격제어메뉴목록(400)은, 원격개폐제어(410), 출입로그확인(420), 친구초대(430), 기능설정(440) 및 보안시간설정(450) 중 적어도 하나를 포함할 수 있다.

이러한 원격제어메뉴목록(400) 중 원격개폐제어(410)가 선택되면, 원격제어부(310)는, 도 6의 (㉢)에 도시된 바와 같이, 원격에서 도어락장치(100)의 개폐동작을 제어하기 위한 버튼(411)을 제공하고, 사용자에 의해 버튼(411)이 터치되었는지의 여부를 확인한 결과에 기초하여 도어락장치(100)의 문을 열 것을 요청하기 위한 오픈메시지를 생성하여 전송하게 된다.

한편, 원격제어메뉴목록(400) 중 출입로그확인(420)가 선택되면, 원격제어부(310)는, 도 6의 (㉣)에 도시된 바와 같이, 서버(200)로부터 수신된 출입로그와 부정출입알림정보를 표시하여 출입로그 화면을 제공하게 된다.

- [0124] 이에, 사용자는, 도어락장치(100)에 비밀번호가 입력된 출입시각과 출입여부, 부정출입인 경우에는 부정시도영상을 원격에서도 확인할 수 있게 되는 것이다.
- [0125] 한편, 원격제어메뉴목록(400) 중 친구초대(430)가 선택되면, 원격제어부(310)는, 도 6의 (⑤)에 도시된 바와 같이, 임시비밀번호를 요청하기 위한 버튼(431)과, 피초대자에게 전송할 수 있도록 다양한 메시지 전송방식(예: SMS, 카카오톡 등)으로 연결되도록 하는 버튼(432)과, 임시비밀번호를 사용자가 직접 삭제할 수 있도록 하는 버튼(433)을 제공하게 된다.
- [0126] 한편, 원격제어메뉴목록(400) 중 기능설정(440)이 선택되면, 원격제어부(310)는, 도 6의 (⑥)에 도시된 바와 같이, 개인정보설정, 푸시 메시지 수신 설정등과 같은 기능설정을 수행할 수 있도록 하는 화면을 제공하게 된다.
- [0127] 한편, 원격제어메뉴목록(400) 중 보안시간설정(450)이 선택되면, 원격제어부(310)는, 도 6의 (⑦)에 도시된 바와 같이, 도어락장치(100)를 통한 출입이 차단될 수 있도록 보안시간을 설정하는 화면을 제공하게 된다.
- [0128] 이에, 사용자는, 보안시간 동안 키패드가 동작하게 되면 애플리케이션을 통해 부정출입 여부를 확인할 수 있게 되며, 도어락장치(100)에서 순간 알람이 울리도록 원격에서 제어할 수도 있게 된다.
- [0129] 다시 도 5를 참고하면, 근거리통신부(320)는, 근거리 무선통신을 통해 도어락장치(100)에 접속하게 되면, 태그 식별자(UID)를 포함하는 특정태그정보를 도어락장치(100)로 전달하여 해당 문을 열어줄 것을 요청하게 된다.
- [0130] 이에, 도어락장치(100)는, 근거리 무선통신을 통해 접속하는 사용자단말(300)로부터 특정태그정보를 수신한 후 특정태그정보와 기 저장된 태그정보를 비교한 결과에 기초하여 해당 문의 개폐여부를 결정할 수 있게 된다.
- [0131] 표시관리부(330)는, 원격제어부(310)의 제어에 따라 원격 제어를 위한 관련 화면이 애플리케이션을 통해 표시부(예: LCD)에 표시되도록 제어한다.
- [0132] 즉, 표시관리부(330)는, 사용자에게 의해 원격 제어를 위해 애플리케이션이 실행되면, 애플리케이션을 통해 출력되는 원격 제어를 위한 관련 화면이 사용자단말(300)의 표시부(예: LCD)에 표시되도록 제어한다.
- [0133] 이상에서 설명한 바와 같이, 본 발명에 따르면, 사물인터넷 기술을 기반으로 보다 스마트한 기능을 제공할 수 있도록 도어락을 제어함으로써, 기존 도어락 보다 보안성을 향상시키면서도 차별화된 기능을 제공하는 새로운 스마트 도어락 서비스를 실현할 수 있는 효과가 성취된다.
- [0134] 이하에서는, 도 7을 참조하여 본 발명의 실시예에 따른 스마트 도어락 서비스를 제공하는 흐름을 구체적으로 설명하도록 한다. 이하에서는 설명의 편의를 위해 전술의 도 1 내지 도 6에서 언급한 참조번호를 언급하여 설명하도록 하겠다.
- [0135] 도 7에 도시된 바와 같이, 본 발명의 서버(200)는, 도어락장치(100)와의 통신연결상태를 주기적으로 확인한다(S100).
- [0136] 보다 구체적으로, 서버(200)는, 도어락장치(100)와의 최초 통신 시, 도어락장치(100)로부터 식별정보를 포함하는 특정비트를 수신하고, 식별정보의 저장여부를 확인한 결과에 기초하여 통신연결상태를 주기적으로 확인하기 위한 타이머를 지정한다.
- [0137] 즉, 서버(200)는, 도어락장치(100)로부터 식별정보를 포함하는 특정비트가 수신되면, 특정비트로부터 식별정보를 검출한다. 이후, 서버(200)는, 기 저장된 사용자정보테이블을 기반으로 식별정보의 존재여부를 확인한 결과에 기초하여 타이머를 지정하게 된다.
- [0138] 이때, 기 저장된 사용자정보테이블에 식별정보가 저장되어 있지 않은 경우에는, 도어락장치(100)가 신규 등록하는 것으로 판단하여 검출된 식별정보를 사용자정보테이블에 저장하는 과정을 먼저 수행하게 될 것이다.
- [0139] 만일, 기 저장된 사용자정보테이블에 식별정보가 저장되어 있으면, 서버(200)는, 도어락장치(100)가 신규 등록을 완료한 이후 특정비트를 전송한 것이므로, 통신연결상태를 주기적으로 확인하기 위한 타이머를 지정하게 된다.
- [0140] 전술에 따라 타이머가 지정되면, 서버(200)는, 타이머에 의해 지정된 시간 동안 특정비트가 주기적으로 수신되는지의 여부를 확인한다(S101).
- [0141] S101 단계의 판단결과, 타이머에 의해 지정된 시간 동안 특정비트가 주기적으로 수신되면, 서버(200)는, 특정비트에 포함된 식별정보에 해당하는 도어락장치(100)와의 통신연결상태가 정상인 것으로 판단한다. 이후, 서버

(200)는, 타이머가 만료되기 이전에 이를 리셋하여 지속적으로 통신연결상태를 확인하게 된다.

- [0142] 한편, S101 단계의 판단결과, 타이머에 의해 지정된 시간 동안 특정비트가 주기적으로 수신되지 않으면, 서버(200)는, 특정비트에 포함된 식별정보에 해당하는 도어락장치(100)와의 통신연결상태가 비정상인 것으로 판단하게 된다.
- [0143] 즉, 서버(200)는, 식별정보에 해당하는 도어락장치(100)와의 통신연결이 특정상황에 의해 종료된 것으로 판단하고, 특정상황이 발생하였음을 사용자단말(300)로 알리게 된다(S102-S103).
- [0144] 여기서, 특정상황은, 식별정보에 해당하는 도어락장치(100)의 고장/파손, 식별정보에 해당하는 도어락장치(100)와 서버(200) 간의 네트워크 이상발생 및 도어락 기본동작 수행 중 적어도 하나를 포함하는 것일 수 있다.
- [0145] 보다 구체적으로, 서버(200)는, 특정상황의 발생여부를 확인한 결과에 기초하여 서비스의 차단여부를 결정한다. 이하에서는 특정상황이 도어락 기본동작이 아닌, 도어락장치(100)의 고장/파손이나 네트워크 이상발생인 것으로 언급하여 설명하도록 하겠다.
- [0146] 즉, 서버(200)는, 통신연결상태가 비정상인 경우, 사용자단말(300)에서 수행 가능한 적어도 하나의 원격제어기능 중 임시비밀번호를 생성하는 것과 관련되는 특정원격제어기능을 차단하게 된다.
- [0147] 이후, 서버(200)는, 특정원격제어기능을 차단할 것을 요청하는 차단요청메시지를 생성하고, 이를 사용자단말(300)로 전송한다.
- [0148] 전술에 따라 서버(200)로부터 차단요청메시지가 수신되면, 사용자단말(300)은, 사용자가 도어락장치(100)의 원격 제어를 위해 애플리케이션을 실행했을 때, 원격 제어를 위한 메뉴 화면의 원격제어메뉴목록(400) 중 친구초대(430)가 선택되더라도 해당 제어가 수행되지 않도록 차단하게 된다.
- [0149] 한편, 사용자단말(300)은, 원격제어메뉴목록(400) 중 보안시간설정(450)이 선택되는 경우, 도어락장치(100)를 통한 출입이 차단될 수 있도록 보안시간을 설정하는 화면을 제공하게 된다(S105).
- [0150] 이처럼 사용자가 보안시간을 설정하게 되면, 사용자단말(300)은, 설정된 보안시간 동안 도어락장치(100)를 통한 모든 출입이 차단될 수 있도록 보안시간알림메시지를 생성하고, 이를 도어락장치(100) 및 서버(200)로 전달한다(S106, S107).
- [0151] 그러면, 도어락장치(100)는, 사용자단말(300)로부터 수신된 보안시간을 저장하고, 보안시간 동안 출입이 시도되었는지의 여부를 감시한다(S108).
- [0152] S108 단계의 판단결과, 보안시간 동안 출입이 시도된 경우, 도어락장치(100)는, 카메라를 통해 전방을 촬영하여 부정시도영상을 생성하고, 출입로그를 확인한다. 이어서, 도어락장치(100)는, 부정시도영상 및 출입로그를 포함하는 부정출입판단정보를 서버(200)로 전달한다(S109, S110).
- [0153] 전술에 따라 도어락장치(100)로부터 부정출입판단정보가 수신되면, 서버(200)는, 부정출입판단정보를 기반으로 부정출입알림정보인 푸시 메시지를 생성하고, 이를 사용자단말(300)로 전송한다(S111, S112).
- [0154] 이에, 사용자단말(300)은, 푸시 메시지를 수신하게 되며, 도어락장치(100)로부터 수신된 부정출입판단정보를 확인하여 신속하게 대처할 수 있게 된다(S113).
- [0155] 이때, 사용자가 부정출입을 확인하여 신고하는 것으로 대처방식을 결정하게 되면, 신고 관련 처리가 용이하게 수행되도록 하는 기능을 더 제공하는 것이 바람직할 것이다.
- [0156] 한편, S108 단계의 판단결과, 보안시간 동안 출입이 시도되지 않은 경우, 도어락장치(100)는, 도어락에서 일반적으로 제공하는 문의 개폐, 오작동 알림 등의 기본동작을 수행하는 S114 단계 이후의 과정을 수행하게 될 것이다.
- [0157] 즉, 도어락장치(100)는, 사용자가 문을 열기 위해 비밀번호를 입력하는 경우, 입력된 비밀번호와 기 설정된 비밀번호를 비교한 결과에 기초하여 문의 개폐여부를 결정한다.
- [0158] 이때, 입력된 비밀번호와 기 설정된 비밀번호가 일치하면, 도어락장치(100)는, 정상적인 출입인 것으로 판단하여 문의 열리도록 제어한다.
- [0159] 한편, 입력된 비밀번호와 기 설정된 비밀번호가 일치하지 않으면, 도어락장치(100)는, 비정상적인 출입을 시도하는 것으로 판단하여 문의 열리지 않도록 제어한다.

- [0160] 이후, 비정상적인 출입이 소정의 횟수이상 시도되는 경우, 도어락장치(100)는, 카메라를 통해 전방을 촬영하여 부정시도영상을 생성하고, 출입로그를 확인한다. 이어서, 도어락장치(100)는, 부정시도영상 및 출입로그를 포함하는 부정출입판단정보를 서버(200)로 전달하는 전술한 S109 단계 이후의 과정을 수행하게 될 것이다.
- [0161] 결국, 본 발명은 스마트 도어락 서비스의 제공을 위해 랜덤 키패드, 보안시간 설정, 특정비트(예: 하트비트)를 기반으로 도어락 사용의 보안성을 향상시킬 수 있게 된다. 또한, 기존 도어락과 달리 사용자의 단말을 통해 친구초대, 원격제어, 근거리 무선통신 등과 같은 편의 기능을 차별화하여 제공할 수 있게 됨에 따라 스마트 홈의 기능을 다양화하는데 기여할 수 있게 된다.
- [0162] 이상에서 설명한 바와 같이, 본 발명에 따르면, 사물인터넷 기술을 기반으로 보다 스마트한 기능을 제공할 수 있도록 도어락을 제어함으로써, 기존 도어락 보다 보안성을 향상시키면서도 차별화된 기능을 제공하는 새로운 스마트 도어락 서비스를 실현할 수 있는 효과가 성취된다.
- [0163] 본 발명의 실시예들은, 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0164] 지금까지 본 발명을 바람직한 실시 예를 참조하여 상세히 설명하였지만, 본 발명이 상기한 실시 예에 한정되는 것은 아니며, 이하의 특허청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 또는 수정이 가능한 범위까지 본 발명의 기술적 사상이 미친다 할 것이다.

산업상 이용가능성

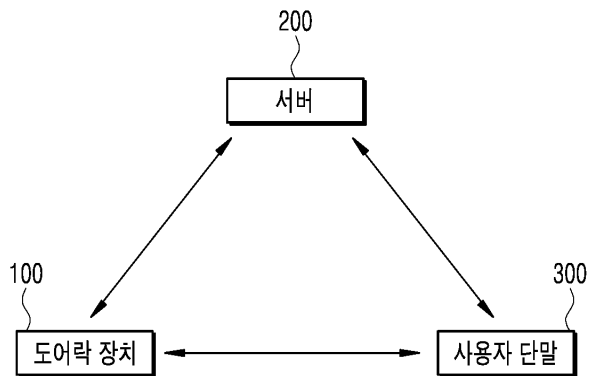
- [0165] 본 발명의 도어락제어시스템 및 그 방법에 따르면, 사물인터넷 기술을 기반으로 보다 스마트한 기능을 제공할 수 있도록 도어락을 제어함으로써, 기존 도어락 보다 보안성을 향상시키면서도 차별화된 기능을 제공하는 새로운 스마트 도어락 서비스가 실현되도록 할 수 있다는 점에서, 기존 기술의 한계를 뛰어 넘음에 따라 관련 기술에 대한 이용만이 아닌 적용되는 장치의 시판 또는 영업의 가능성이 충분할 뿐만 아니라 현실적으로 명백하게 실시할 수 있는 정도이므로 산업상 이용가능성이 있는 발명이다.

부호의 설명

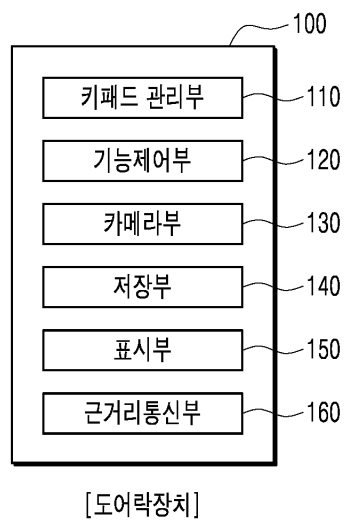
- [0166]
- | | |
|-------------|-------------|
| 100: 도어락장치 | |
| 110: 키패드관리부 | 120: 기능제어부 |
| 130: 카메라부 | 140: 저장부 |
| 150: 표시부 | 160: 근거리통신부 |
| 200: 서버 | |
| 210: 모니터링부 | 220: 서비스관리부 |
| 230: 저장부 | |
| 300: 사용자단말 | |
| 310: 원격제어부 | 320: 근거리통신부 |
| 330: 표시관리부 | |

도면

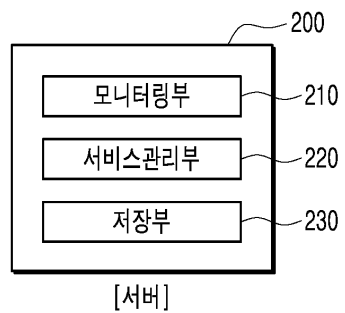
도면1



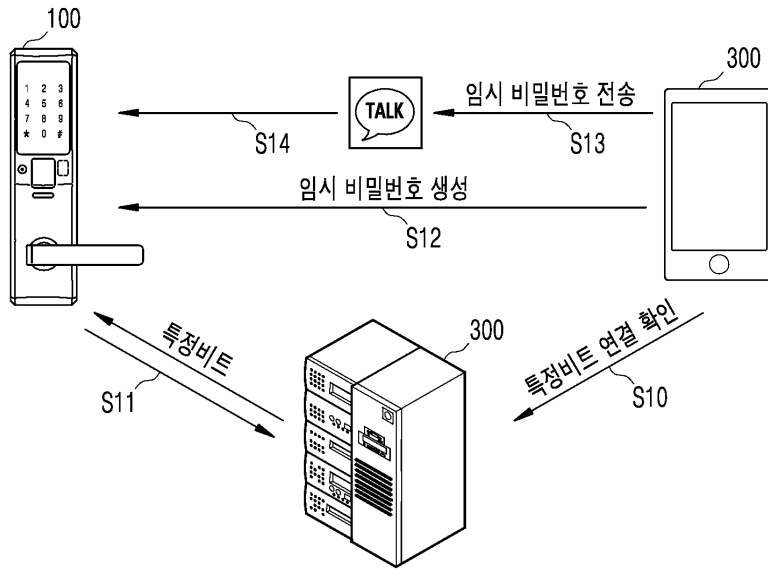
도면2



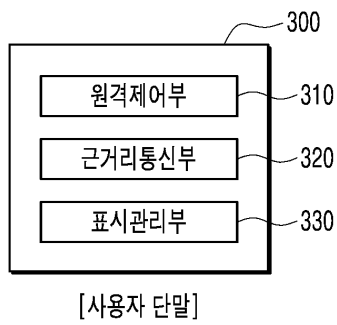
도면3



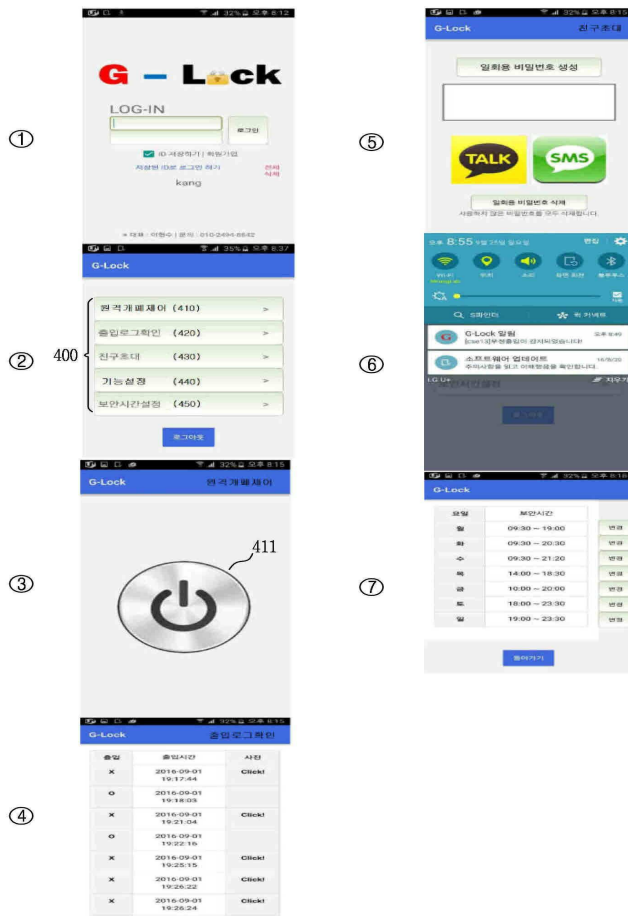
도면4



도면5



도면6



도면7

