(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년05월11일
(11) 등록번호 10-2108783
(24) 등록일자 2020년05월04일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *G06Q 30/02* (2012.01)
H04W 12/00 (2019.01) *H04W 4/38* (2018.01)
(52) CPC특허분류
H04L 63/0876 (2013.01)
G06Q 30/0241 (2013.01)
(21) 출원번호 10-2019-0126774
(22) 출원일자 2019년10월14일
심사청구일자 2019년10월14일
(56) 선행기술조사문헌
JP2015148896 A*
KR1020160009084 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
김두란
서울특별시 송파구 문정로 83, 117동 1301호 (문정동, 문정래미안아파트)
(72) 발명자
김두란
서울특별시 송파구 문정로 83, 117동 1301호 (문정동, 문정래미안아파트)
(74) 대리인
최훈식

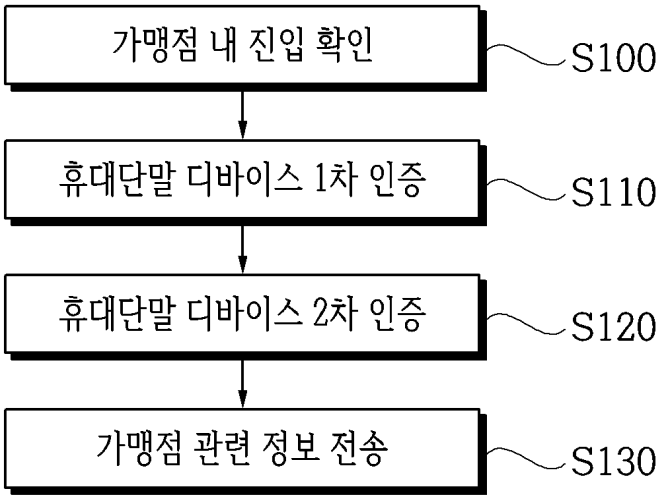
전체 청구항 수 : 총 1 항 심사관 : 문형섭

(54) 발명의 명칭 **비콘을 이용한 마케팅 시스템의 보안 인증 방법**

(57) 요 약

본 발명은 비콘을 이용하여 복수의 가맹점을 광고하기 위한, 비콘을 이용한 마케팅 시스템의 보안 인증 방법으로서, 비콘이, 휴대단말 디바이스의 가맹점 내 진입을 확인하는 제1 단계; 서비스 서버가, 휴대단말 디바이스의 디바이스 ID와 비콘의 마이너(MINOR) 값을 이용하여 1차 인증을 수행하는 제2 단계; 1차 인증을 패스한 후에, 서비스 서버가, 휴대단말 디바이스의 디바이스 ID와 비콘의 마이너 값과, 메이저(MAJOR) 값을 이용하여 2차 인증을 수행하는 제3 단계; 및 2차 인증을 패스한 후에, 서비스 서버가, 휴대단말 디바이스로 방문한 가맹점 관련 정보 - 메뉴 정보, 상품 할인정보 및 광고 중 적어도 하나를 포함함 - 를 전송하는 제4 단계를 포함하는 것을 특징으로 한다.

대 표 도 - 도2



(52) CPC특허분류
H04W 12/00503 (2019.01)
H04W 4/38 (2018.02)
H04L 2463/082 (2013.01)

명 세 서

청구범위

청구항 1

비콘을 이용하여 복수의 가맹점을 광고하기 위한, 비콘을 이용한 마케팅 시스템의 보안 인증 방법으로서,

비콘이, 휴대단말 디바이스의 가맹점 내 진입을 확인하는 제1 단계;

서비스 서버가, 휴대단말 디바이스의 디바이스 ID와 비콘의 마이너 값을 이용하여 1차 인증을 수행하는 제2 단계;

1차 인증을 패스한 후에, 서비스 서버가, 휴대단말 디바이스의 디바이스 ID와 비콘의 마이너 값과, 메이저 값을 이용하여 2차 인증을 수행하는 제3 단계; 및

2차 인증을 패스한 후에, 서비스 서버가, 휴대단말 디바이스로 방문한 가맹점 관련 정보 - 메뉴 정보, 상품 할인정보 및 광고 중 적어도 하나를 포함함 - 를 전송하는 제4 단계를 포함하며,

상기 제1 단계는,

비콘이, 휴대단말 디바이스로 디바이스 GPS 정보를 요청하는 단계;

휴대단말 디바이스가, 자신의 GPS 정보를 비콘으로 전송하는 단계;

비콘이, 자신의 GPS 정보와 디바이스 GPS 정보를 비교하는 단계; 및

비콘이, 비콘 GPS 정보와 디바이스 GPS 정보가 일치할 경우, 휴대단말 디바이스의 가맹점 내 진입으로 확인하고, 서비스 서버로 디바이스 GPS 정보를 전송하는 단계를 포함하고, 서비스 서버는 휴대단말 디바이스의 디바이스 GPS 정보를 수신한 후에 서비스 서버에 저장된 데이터베이스의 디바이스 GPS 정보와 비교하여 휴대단말 디바이스의 추가적인 인증을 수행할 수 있는 것을 특징으로 하는 비콘을 이용한 마케팅 시스템의 보안 인증 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 비콘을 이용한 마케팅 시스템에 관한 것으로, 보다 상세하게는 보안이 취약한 비콘을 이용한 마케팅 시스템에서 휴대단말 디바이스의 디바이스 ID와 비콘의 고유값을 조합하여 이중 암호화 함으로써 보안성을 강화할 수 있는 비콘을 이용한 마케팅 시스템의 보안 인증 방법에 관한 것이다.

배 경 기 술

[0002] 최근에는 RFID(Radio-Frequency Identification)칩, NFC, 비콘, QR코드 등의 근거리 무선통신기술에 의한 인식기술과 스마트 기기에 부착된 장치들의 다양한 부가기능과 연동하는 기술이 발달함에 따라 다양한 분야에 무선통신기술을 이용한 정보제공기술이 응용되어 실생활에 구현되고 있다.

[0003] 이러한 무선인식기술 중에서, 대표적인 기술로 비콘이 있다. 비콘은 블루투스나 인간이 들을 수 없는 비가청영역의 주파수를 활용해 단말과 정보를 주고받는 디바이스로서, 스마트폰이나 태블릿 등의 사용자 디바이스를 소지한 고객이 커버리지 내에 진입할 경우 해당 단말을 감지하여 정보를 제공하는 방식을 취한다.

[0004] 가장 최근에는 비콘이 마케팅 분야에 시도되고 있는데, 비콘을 통해 무선으로 광고 데이터나 쿠폰 데이터를 브로드캐스팅하면 그 주변을 지나는 사람들의 스마트폰에서 이들 무선신호를 식별하여 광고 페이지나 쿠폰을 사용자에게 표시하는 것이다.

[0005] 하지만, 비콘은 사용자 디바이스와 단순히 저전력 블루투스(BLE: bluetooth low energy) 기술에 기반하여 인증을 하기 때문에 해킹에 취약한 단점이 있다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) KR 10-2012-0101244 A1

발명의 내용

해결하려는 과제

[0007] 본 발명의 목적은 보안이 취약한 비콘을 이용한 마케팅 시스템에서 휴대단말 디바이스의 디바이스 ID와 비콘의 고유값을 조합하여 이중 암호화 함으로써 보안성을 강화할 수 있는 비콘을 이용한 마케팅 시스템의 보안 인증 방법을 제공하는 것이다.

[0008] 본 발명의 다른 목적 및 장점들은 하기에 설명될 것이며, 본 발명의 실시예에 의해 알게 될 것이다. 또한, 본 발명의 목적 및 장점들은 청구범위에 나타낸 수단 및 조합에 의해 실현될 수 있다.

과제의 해결 수단

[0009] 본 발명의 일측면에 따르면, 비콘을 이용하여 복수의 가맹점을 광고하기 위한, 비콘을 이용한 마케팅 시스템의 보안 인증 방법으로서, 비콘을 이용하여 복수의 가맹점을 광고하기 위한, 비콘을 이용한 마케팅 시스템의 보안 인증 방법으로서, 비콘이, 휴대단말 디바이스의 가맹점 내 진입을 확인하는 제1 단계; 서비스 서버가, 휴대단말 디바이스의 디바이스 ID와 비콘의 마이너 값을 이용하여 1차 인증을 수행하는 제2 단계; 1차 인증을 패스한 후에, 서비스 서버가, 휴대단말 디바이스의 디바이스 ID와 비콘의 마이너 값과, 메이저 값을 이용하여 2차 인증을 수행하는 제3 단계; 및 2차 인증을 패스한 후에, 서비스 서버가, 휴대단말 디바이스로 방문한 가맹점 관련 정보 - 메뉴 정보, 상품 할인정보 및 광고 중 적어도 하나를 포함함 - 를 전송하는 제4 단계를 포함하며, 상기 제1 단계는, 비콘이, 휴대단말 디바이스로 디바이스 GPS 정보를 요청하는 단계; 휴대단말 디바이스가, 자신의 GPS 정보를 비콘으로 전송하는 단계; 비콘이, 자신의 GPS 정보와 디바이스 GPS 정보를 비교하는 단계; 및 비콘이, 비콘 GPS 정보와 디바이스 GPS 정보가 일치할 경우, 휴대단말 디바이스의 가맹점 내 진입으로 확인하고, 서비스 서버로 디바이스 GPS 정보를 전송하는 단계를 포함하고, 서비스 서버는 휴대단말 디바이스의 디바이스 GPS 정보를 수신한 후에 서비스 서버에 저장된 데이터베이스의 디바이스 GPS 정보와 비교하여 휴대단말 디바이스의 추가적인 인증을 수행할 수 있는 것을 특징으로 한다.

[0010] 삭제

[0011] 삭제

[0012] 삭제

[0013] 삭제

[0014] 삭제

[0015] 삭제

발명의 효과

[0016] 본 발명에 의하면, 보안이 취약한 비콘을 이용한 마케팅 시스템에서 휴대단말 디바이스의 디바이스 ID와 비콘의 고유값을 조합하여 이중 암호화 함으로써 보안성을 강화할 수 있는 효과가 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 일실시예에 따른 비콘을 이용하여 복수의 가맹점을 광고하기 위한 비콘을 이용한 마케팅 시스템의 개략적인 구성도이고,

도 2는 본 발명의 일실시예에 따른 비콘을 이용한 마케팅 시스템의 보안 인증 방법을 설명하기 위한 순서도이고,

도 3은 1차 및 2차 인증의 암호화를 설명하기 위한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하에서는 도면을 참조하여 본 발명의 구체적인 실시예를 상세하게 설명한다. 다만, 본 발명의 사상은 제시되는 실시예에 제한되지 아니하고, 본 발명의 사상을 이해하는 당업자는 동일한 사상의 범위 내에서 다른 구성요소를 추가, 변경, 삭제 등을 통하여, 퇴보적인 다른 발명이나 본 발명 사상의 범위 내에 포함되는 다른 실시예를 용이하게 제안할 수 있을 것이나, 이 또한 본원 발명 사상 범위 내에 포함된다고 할 것이다.

[0019] 또한, 각 실시예의 도면에 나타나는 동일한 사상의 범위 내의 기능이 동일한 구성요소는 동일한 참조부호를 사용하여 설명한다.

[0020] 이하 바람직한 실시예를 도시한 첨부 도면을 통해 본 발명을 상세히 설명한다.

[0021] 본 발명을 설명함에 있어, 관련된 공지 기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그에 대한 상세한 설명은 생략하기로 한다.

[0022] 도 1은 본 발명의 일실시예에 따른 비콘을 이용하여 복수의 가맹점을 광고하기 위한 비콘을 이용한 마케팅 시스템의 개략적인 구성도이고, 도 2는 본 발명의 일실시예에 따른 비콘을 이용한 마케팅 시스템의 보안 인증 방법을 설명하기 위한 순서도이고, 도 3은 1차 및 2차 인증의 암호화를 설명하기 위한 순서도이다.

[0023] 본 발명에서는 비콘이 전송하는 식별자 값이 보안적으로 취약한 점을 해결하기 위한 방안을 제시하고 있다.

[0024] 비콘이 갖는 3가지 식별자중 UUID 값은 위치를 확인하기 위해 사용하고, 메이저(MAJOR) 또는 마이너(MINOR) 값은 수신한 디바이스의 유효성을 확인하기 위해 사용되는 값이다. 사용자 디바이스가 비콘으로부터 메이저 또는 마이너 값을 획득후 서버로 전송하면, 서버는 비콘과 사용자 디바이스에서 수집된 메이저 또는 마이너 값을 비교하여 유효성 검사를 하고 검사가 통과되면 사용자 디바이스에서 특정 서비스가 이용 가능하도록 한다.

[0025] 이와 같이, 종래에는 비콘의 메이저 또는 마이너 값을 이용한 사용자 디바이스의 유효성 검사가 1차 인증으로만 행해지고 있으므로, 비콘 정보가 누출될 경우 보안에 미흡할 수 있는 단점이 있었다.

[0026] 이를 보완하기 위해서, 본 발명에서는 휴대단말 디바이스의 디바이스 ID와 비콘의 고유값들을 조합하여, 이중 암호화 하여 1차 및 2차에 걸쳐 인증과정을 수행하고 있으며, 따라서 비콘 정보가 누출되더라도 곧바로 서비스를 제한할 수 있게 되어 비콘을 이용한 마케팅 시스템의 보안성을 보장할 수 있게 된다.

[0027] 또한, 본 발명에서는 비콘 자신의 GPS 정보와 휴대단말 디바이스의 GPS 정보를 인증을 위해 추가로 이용함으로써 보안성을 더욱 증가시킬 수 있게 된다.

[0028] 도 1을 참조하면, 본 발명의 일실시예에 따른 비콘을 이용하여 복수의 가맹점을 광고하기 위한 비콘을 이용한 마케팅 시스템은 가맹점(100) 내 비콘(110) 및 포스단말기(120), 사용자가 휴대하는 휴대단말 디바이스(200), 서비스 제공을 위한 서비스 서버(300)를 포함할 수 있다.

[0029] "가맹점(100)"은 당업계에서 통상의 의미로 이해될 수 있는 바, 구체적으로 서비스 운영자와 특정 계약을 체결한 곳으로, 상품 또는 서비스를 판매하는 가게나 상점을 의미할 수 있다.

[0030] 또한, "가맹점 내"라는 용어 역시 통상의 의미로 이해될 수 있는데, 예를 들면 가맹점의 상품 또는 서비스 판매를 위한 공간(건축물 또는 시설)을 의미할 수 있다.

[0031] 비콘(110)은 적은 전력으로 고속전송이 가능한 블루투스 기반 무선통신기술이다. 기존에 사용되는 NFC의 송신거리가 20 cm이내였던 것에 비해, 비콘(110)은 최대 70 m까지 송신이 가능하며 저전력 블루투스(BLE)를 이용하기 때문에 배터리 교체 없이 약 2년간 동작이 가능한 장점을 가진다.

[0032] 포스단말기(120)는 일반적으로 금전 출납 등록 기능과 컴퓨터 기능을 보유한 판매시점 관리시스템으로서, 본 실시예에서는 서비스 서버(300)로부터 주문 정보나 결제 정보를 수신할 수도 있다.

[0033] 서비스 서버(300)는 휴대단말 디바이스(200)의 인증을 수행하고, 휴대단말 디바이스(200)로 가맹점 관련 정보를 전송하거나, 휴대단말 디바이스(200)로 결제정보를 전송할 수도 있다. 여기서, 가맹점 관련 정보는, 예를 들면 가맹점의 상품 정보, 메뉴 정보, 상품 할인 정보, 광고 등이며, 이들 중 적어도 하나 이상을 포함할 수 있다

[0034] 서비스 서버(300)는 비콘(110)의 GPS 정보를 기반으로 각 가맹점(100)을 식별할 수 있고, 가맹점(100)의 각종 정보가 미리 저장될 수 있다.

[0035] 도 2를 참조하면, 본 발명의 일실시예에 따른 비콘을 이용한 마케팅 시스템의 보안 인증 방법은, 비콘(110)이, 휴대단말 디바이스(200)의 가맹점(100) 내 진입을 확인하는 단계(S100); 서비스 서버(300)가, 휴대단말 디바이스(200)의 디바이스 ID와 비콘(110)의 마이너 값을 이용하여 1차 인증을 수행하는 단계(S110); 1차 인증을 패스한 후에, 서비스 서버(300)가, 휴대단말 디바이스(200)의 디바이스 ID와 비콘의 마이너 값과, 메이저 값을 이용하여 2차 인증을 수행하는 단계(S120); 및 2차 인증을 패스한 후에, 서비스 서버(300)가, 휴대단말 디바이스(200)로 방문한 가맹점(100) 관련 정보 - 메뉴 정보, 상품 할인정보 및 광고 중 적어도 하나를 포함함 - 를 전송하는 단계(S130)를 포함할 수 있다.

[0036] 휴대단말 디바이스(200)의 가맹점(100) 내 진입을 확인하는 단계(S100)는, 비콘(110)이, 휴대단말 디바이스(200)로 디바이스 GPS 정보를 요청하는 단계; 휴대단말 디바이스(200)가, 자신의 GPS 정보를 비콘(110)으로 전송하는 단계; 비콘(110)이, 자신의 GPS 정보와 디바이스 GPS 정보를 비교하는 단계; 및 비콘 GPS 정보와 디바이스 GPS 정보가 일치할 경우 휴대단말 디바이스(200)가 가맹점(100) 내에 진입한 것으로 확인하고 서비스 서버(300)로 디바이스 GPS 정보를 전송하는 단계를 포함할 수 있다.

[0037] 이때, 서비스 서버(300)는 휴대단말 디바이스(200)의 디바이스 GPS 정보를 수신한 후에 서비스 서버(300)에 저장된 데이터베이스의 디바이스 GPS 정보와 비교하여 추가적인 인증을 수행할 수도 있다. 이를 위해서, 휴대단말 디바이스(200)는 주기적으로 자신의 디바이스 GPS 정보를 서비스 서버(300)로 전송하여 서비스 서버(300) 측의 디바이스 GPS 정보가 업데이트될 수 있도록 한다.

[0038] 이와 같이, 비콘 GPS 정보와 디바이스 GPS 정보를 이용하여 휴대단말 디바이스(200)의 가맹점(100) 내의 진입여부를 체크함으로써 보다 안전한 가맹점(100) 내에서의 서비스 제공이 가능해지며, 기존 비콘을 이용한 무작위 메시지 전송으로 인한 사용자의 불편도 해소할 수 있는 이점이 있다.

[0039] 그리고, 서비스 서버(300)가 1차 인증을 수행하는 단계(S110)는, 비콘(110)이, 센싱 계층을 통해 휴대단말 디바이스(200)를 1차 감지하면 해당 휴대단말 디바이스(200)로 마이너 값을 전송하는 단계; 휴대단말 디바이스(20

0)가, 디바이스 ID와 함께 비콘(110)으로부터 수신한 마이너 값을 서비스 서버로 전송하는 단계; 및 서비스 서버(300)가, 휴대단말 디바이스(200)로부터 디바이스 ID와 마이너 값을 수신한 후에 서비스 서버(300)에 저장된 데이터베이스의 디바이스 ID와 마이너 값을 비교하는 단계를 포함하는 것을 특징으로 한다.

[0040] 또한, 서비스 서버(300)가 2차 인증을 수행하는 단계(S120)는, 비콘(110)이, 센싱 계층을 통해 휴대단말 디바이스(200)를 2차 감지하면 해당 휴대단말 디바이스(200)로 메이저 값을 전송하는 단계; 휴대단말 디바이스(200)가, 디바이스 ID와 함께 비콘으로부터 수신한 마이너 값과, 메이저 값을 서비스 서버로 전송하는 단계; 및 서비스 서버(300)가, 휴대단말 디바이스(200)로부터 디바이스 ID와 마이너 값, 메이저 값을 수신한 후에 서비스 서버(300)에 저장된 데이터베이스의 디바이스 ID와 마이너 값, 메이저 값을 비교하는 단계를 포함하는 것을 특징으로 한다.

[0041] 그리고, 휴대단말 디바이스(200)에서 모바일 결제시, 서비스 서버(300)는 휴대단말 디바이스(200)로부터 모바일 결제 정보를 수신하고, 휴대단말 디바이스(200)에서 행한 모바일 결제 정보를 포스 단말기(120)로 전송할 수 있다.

[0042] 1차 인증에 실패하면, 휴대단말 디바이스(200)에는 '인증 실패'라는 음성과 함께 'FAILED' 메시지가 표시될 수 잇다.

[0043] 1차 인증이 성공하면, 사용자가 아무런 이벤트를 수행하지 않고 2차 인증으로 넘어가며, 1차 인증에서 수신한 디바이스 ID와 마이너 값을 삭제 후 다시 휴대단말 디바이스(200)의 디바이스 ID와 비콘(110)의 마이너, 메이저 값을 수신한다

[0044] 2차 인증에 성공하면, 휴대단말 디바이스(200)에는 '인증 성공'이라는 음성과 성공 메시지가 표시될 수 있다. 만약 2차 인증에 실패하는 경우, 1차 인증 실패와 마찬가지로 휴대단말 디바이스(200)에는 '인증 실패'라는 음성과 함께 'FAILED' 메시지가 표시될 수 잇다.

[0045] 도 3은 1차 및 2차 인증의 암호화를 설명하기 위한 순서도이다.

[0046] 도 3을 참조하면, 1차 인증을 수행하는 단계(S110)에서 전송되는 디바이스 ID와 마이너 값; 및 2차 인증을 수행하는 단계(S120)에서 전송되는 디바이스 ID와 마이너 값, 메이저 값은 암호화(복호화 포함)하는 것이 바람직하다. 이때, 1차 인증을 수행하는 단계(S110)에서의 암호화와 2차 인증을 수행하는 단계(S120)에서의 암호화는 서로 다른 암호화 방식을 사용할 수 있다.

[0047] 상기에서는 본 발명에 따른 실시예를 기준으로 본 발명의 구성과 특징을 설명하였으나 본 발명은 이에 한정되지 않으며, 본 발명의 사상과 범위 내에서 다양하게 변경 또는 변형할 수 있음은 본 발명이 속하는 기술분야의 당업자에게 명백한 것이며, 따라서 이와 같은 변경 또는 변형은 첨부된 특허청구범위에 속함을 밝혀둔다.

부호의 설명

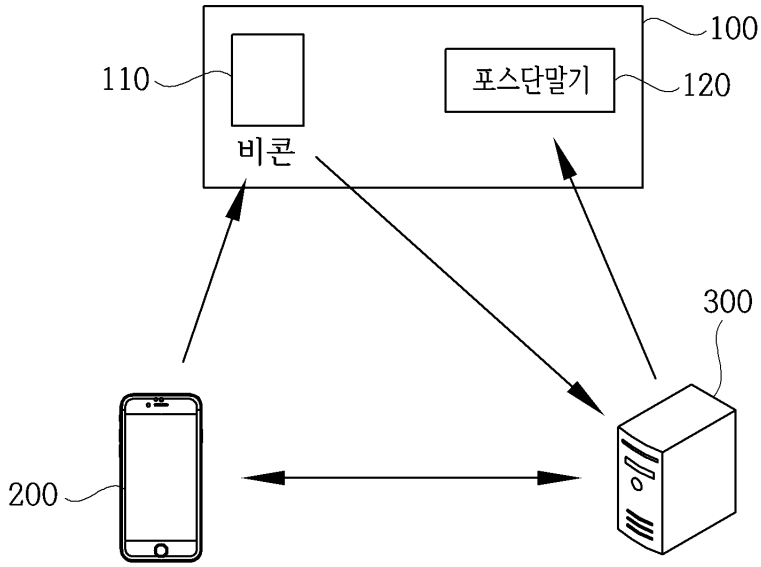
[0048] 100 : 가맹점 110 : 비콘

120 : 포스단말기 200 : 휴대단말 디바이스

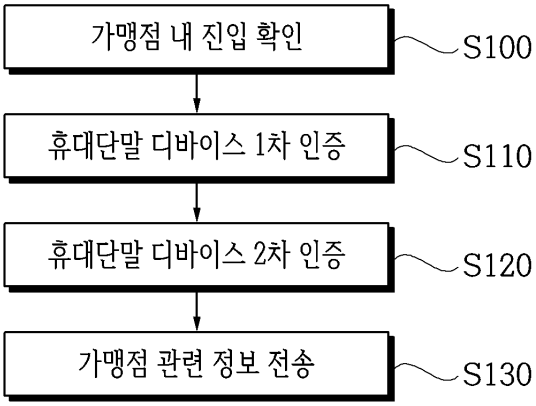
300 : 서비스 서버

도면

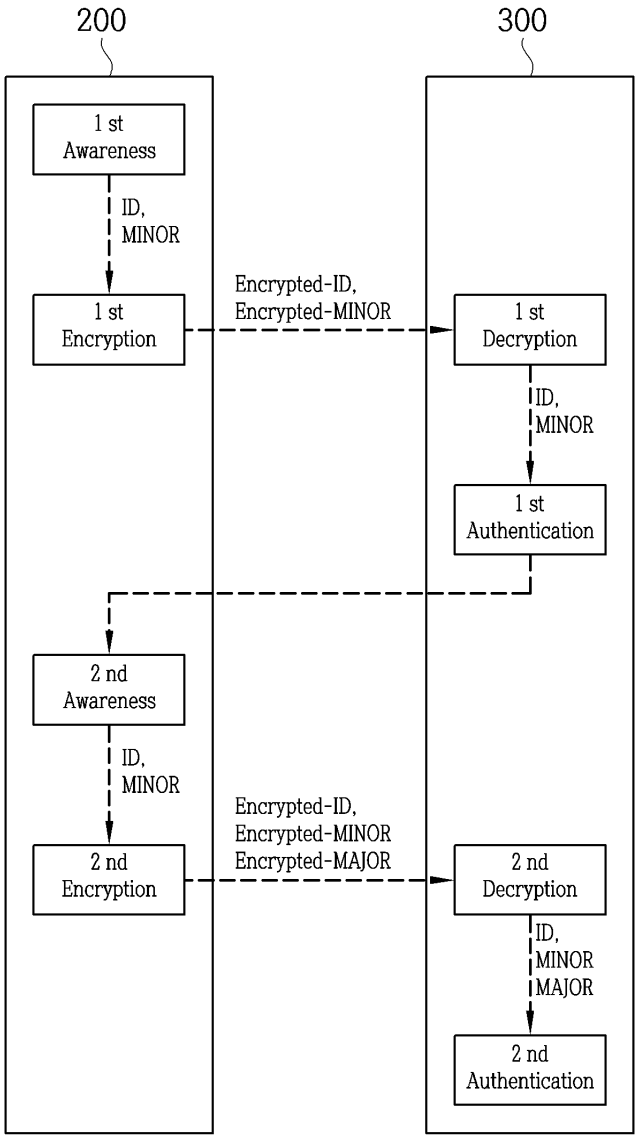
도면1


100
110
포스단말기
120
비콘
300
200

도면2


가맹점 내 진입 확인
S100
휴대단말 디바이스 1차 인증
S110
휴대단말 디바이스 2차 인증
S120
가맹점 관련 정보 전송
S130

도면3


200
300
1 st Awareness
ID, MINOR
1 st Encryption
Encrypted-ID, Encrypted-MINOR
1 st Decryption
ID, MINOR
1 st Authentication
2 nd Awareness
ID, MINOR
2 nd Encryption
Encrypted-ID, Encrypted-MINOR Encrypted-MAJOR
2 nd Decryption
ID, MINOR MAJOR
2 nd Authentication