(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년12월01일
(11) 등록번호 10-1803651
(24) 등록일자 2017년11월24일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)
H04W 12/08 (2009.01)
(52) CPC특허분류
H04L 9/3226 (2013.01)
H04L 9/30 (2013.01)
(21) 출원번호 10-2016-0077896
(22) 출원일자 2016년06월22일
심사청구일자 2016년06월22일
(56) 선행기술조사문헌
Y. Sun, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Perservation for Vehicular Communication, IEEE Transactions on Vehicular Technology (2010)
한국정보통신기술협회, 차량 간 통신 인증 서비스 구조, TTAK.KO-13.xxxx (2013.12.)
KR1020160060683 A
US6640145 B2

(73) 특허권자
부경대학교 산학협력단
부산광역시 남구 신선로 365 (용당동, 부경대학교)
(72) 발명자
이경현
부산광역시 남구 수영로 345, 104동 1803호
박영호
부산광역시 사상구 모라로52번길 9, 102호
서철
부산광역시 해운대구 청사포로 12, 111동 902호
(74) 대리인
특허법인이상

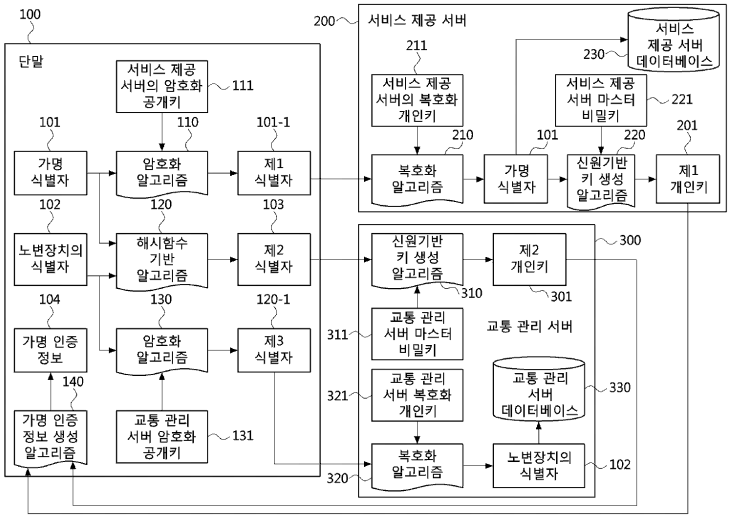
전체 청구항 수 : 총 20 항 심사관 : 양종필

(54) 발명의 명칭 **차량 클라우드 서비스 접속을 위한 인증 방법**

(57) 요 약

차량 클라우드 서비스에 접속하는 단말의 인증 방법이 개시된다. 단말의 인증 방법은 차량 클라우드 서비스에 접속하는 단말에서 수행되는 인증 방법으로서, 단말의 가명 식별자를 암호화하여 제1 식별자를 생성하는 단계, 가명 식별자 및 단말이 차량 클라우드 서비스에 접속하기 위한 노변 장치의 식별자를 암호화하여 제2 식별자를 생성하는 단계, 제1 식별자 및 제2 식별자를 기반으로 단말 및 노변 장치 간의 인증을 위해 가명 식별자 및 노변 장치의 식별자가 서로 연계된 가명 인증 정보를 생성하는 단계 및 가명 인증 정보를 기반으로 노변 장치와 인증을 수행하는 단계를 포함한다.

대 표 도



(52) CPC특허분류
H04L 9/3247 (2013.01)
H04W 12/06 (2013.01)
H04W 12/08 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 2014R1A2A1A11052981
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 도약연구지원사업
연구과제명 V-클라우드 환경에서 서비스 지향적 어플리케이션을 위한 프라이버시 보호 및 인증 기술 개발
기 여 율 1/1
주관기관 부경대학교
연구기간 2015.11.01 ~ 2016.10.31
공지예외적용 : 있음

명 세 서

청구범위

청구항 1

차량 클라우드 서비스(vehicle cloud service)에 접속하는 단말에서 수행되는 인증(authentication) 방법으로서,

상기 단말의 가명 식별자(pseudonym identity)를 암호화(encryption)하여 제1 식별자를 생성하는 단계;

상기 가명 식별자 및 상기 단말이 상기 차량 클라우드 서비스에 접속하기 위한 노변 장치(roadside unit)의 식별자를 암호화하여 제2 식별자를 생성하는 단계;

상기 제1 식별자 및 상기 제2 식별자를 기반으로 상기 단말 및 상기 노변 장치 간의 인증을 위해 상기 가명 식별자 및 상기 노변 장치의 식별자가 서로 연계된 가명 인증 정보를 생성하는 단계; 및

상기 가명 인증 정보를 기반으로 상기 노변 장치와 인증을 수행하는 단계를 포함하는 단말의 인증 방법.

청구항 2

청구항 1에 있어서,

상기 제1 식별자는,

상기 가명 식별자를 상기 차량 클라우드 서비스를 제공하는 서비스 제공 서버의 암호화 공개키를 기반으로 암호화된 식별자인 단말의 인증 방법.

청구항 3

청구항 1에 있어서,

상기 제2 식별자는,

상기 가명 식별자 및 상기 노변 장치의 식별자를 일방향 해시함수(one-way hash function)를 기반으로 암호화된 식별자인 단말의 인증 방법.

청구항 4

청구항 1에 있어서,

상기 단말의 인증 방법은,

상기 노변 장치의 식별자를 암호화하여 제3 식별자를 생성하는 단계;

상기 제3 식별자가 포함된 메시지를 상기 차량 클라우드 서비스를 관리하는 교통 관리 서버로 전송하는 단계를 더 포함하는 단말의 인증 방법.

청구항 5

청구항 4에 있어서,

상기 제3 식별자는,

상기 교통 관리 서버의 암호화 공개키를 기반으로 암호화된 식별자인 단말의 인증 방법.

청구항 6

청구항 1에 있어서,

상기 가명 인증 정보를 생성하는 단계는,

상기 제1 식별자가 포함된 메시지를 상기 차량 클라우드 서비스를 제공하는 서비스 제공 서버로 전송하는 단계;

상기 제2 식별자가 포함된 메시지를 상기 차량 클라우드 서비스를 관리하는 교통 관리 서버로 전송하는 단계;

상기 서비스 제공 서버로부터 상기 단말의 가명 식별자에 대응되는 상기 단말의 제1 개인키가 포함된 메시지를 수신하는 단계;

상기 교통 관리 서버로부터 상기 제2 식별자에 대응되는 상기 단말의 가명 식별자 및 상기 노변 장치의 식별자가 서로 연계된 제2 개인키가 포함된 메시지를 수신하는 단계; 및

상기 제1 개인키 및 상기 제2 개인키를 기반으로 상기 가명 인증 정보를 생성하는 단계를 포함하는 단말의 인증 방법.

청구항 7

청구항 6에 있어서,

상기 가명 인증 정보는,

상기 제1 개인키 및 상기 제2 개인키를 기반으로 겹선형 페어링(bilinear pairing) 연산하여 생성되는 단말의 인증 방법.

청구항 8

청구항 6에 있어서,

상기 제1 개인키는,

상기 단말의 가명 식별자가 상기 서비스 제공 서버의 마스터 비밀키를 기반으로 암호화된 키인 단말의 인증 방법.

청구항 9

청구항 6에 있어서,

상기 제2 개인키는,

상기 제2 식별자가 상기 교통 관리 서버의 마스터 비밀키를 기반으로 암호화된 키인 단말의 인증 방법.

청구항 10

차량 클라우드 서비스(vehicle cloud service)에 접속하는 단말에서 수행되는 인증(authentication) 방법으로서,

상기 단말의 가명 식별자(pseudonym identity) 및 상기 차량 클라우드 서비스의 접속을 위한 노변 장치(roadside unit)의 식별자가 서로 연계된 가명 인증 정보 및 상기 가명 식별자를 기반으로 상기 단말 및 상기 노변 장치 간의 인증을 요청하는 인증 요청 메시지를 생성하는 단계;

상기 인증 요청 메시지를 상기 노변 장치로 전송하는 단계; 및

상기 노변 장치로부터 상기 인증 요청 메시지에 대한 응답이 포함된 인증 응답 메시지를 수신하는 단계를 포함하는 단말의 인증 방법.

청구항 11

청구항 10에 있어서,

상기 단말의 인증 방법은,

상기 가명 식별자를 상기 노변 장치의 암호화 공개키를 기반으로 암호화(encryption)하여 암호화 가명 식별자를 생성하는 단계; 및

상기 암호화 가명 식별자가 포함된 메시지를 상기 노변 장치로 전송하는 단계를 더 포함하는 단말의 인증 방법.

청구항 12

청구항 10에 있어서,

상기 인증 요청 메시지는,

상기 가명 인증 정보의 소유에 대한 증명을 위해 상기 가명 인증 정보 및 상기 가명 식별자를 기반으로 생성되는 상기 가명 인증 정보의 서명(signature)을 포함하는 단말의 인증 방법.

청구항 13

청구항 10에 있어서,

상기 인증 응답 메시지는,

상기 차량 클라우드 서비스에 대한 접속의 허용 및 거부 중 하나를 나타내는 응답 정보를 포함하는 단말의 인증 방법.

청구항 14

차량 클라우드 서비스(vehicle cloud service)를 제공하는 노변 장치(roadside unit)에서 수행되는 인증(authentication) 방법으로서,

단말로부터 상기 차량 클라우드 서비스에 접속을 위한 상기 단말 및 상기 노변 장치 간의 인증을 요청하는 인증 요청 메시지를 수신하는 단계;

상기 인증 요청 메시지에 포함된 상기 단말의 가명 식별자 및 상기 노변 장치의 식별자가 서로 연계된 가명 인증 정보의 서명(signature)을 기반으로 상기 차량 클라우드 서비스의 접속 가능 여부를 판단하는 단계; 및

상기 접속 가능 여부의 결과를 포함하는 인증 응답 메시지를 상기 단말로 전송하는 단계를 포함하는 단말의 인증 방법.

청구항 15

청구항 14에 있어서,

상기 단말의 인증 방법은,

상기 단말로부터 암호화 가명 식별자가 포함된 메시지를 수신하는 단계; 및

상기 암호화 가명 식별자를 상기 노변 장치의 복호화(decryption) 개인키를 기반으로 복호화하여 상기 단말의 가명 식별자를 획득하는 단계를 더 포함하는 단말의 인증 방법.

청구항 16

청구항 14에 있어서,

상기 단말의 인증 방법은,

상기 차량 클라우드 서비스를 제공하는 서비스 제공 서버로부터 적어도 하나의 취소 식별자를 포함하는 취소 식별자 목록이 포함된 메시지를 수신하는 단계를 더 포함하는 단말의 인증 방법.

청구항 17

청구항 16에 있어서,

상기 차량 클라우드 서비스의 접속 가능 여부를 판단하는 단계는,

상기 단말의 가명 식별자를 상기 적어도 하나의 취소 식별자와 비교하여 상기 적어도 하나의 취소 식별자 중 상기 단말의 가명 식별자와 동일한 식별자가 존재하지 않는 경우, 상기 단말의 가명 식별자가 취소 식별자의 대상이 아닌 것으로 판단하는 단계;

상기 서명을 상기 노변 장치의 암호화 공개키를 기반으로 복호화하여 상기 가명 인증 정보를 획득하는 단계;

상기 가명 인증 정보의 생성에 사용된 마스터 비밀키와 상기 노변 장치에 미리 저장된 마스터 공개키를 비교하는 단계; 및

상기 단말의 가명 인증 정보의 생성에 사용된 마스터 비밀키가 상기 노변 장치에 미리 저장된 마스터 공개키에 상응하는 마스터 비밀키인 경우, 상기 차량 클라우드 서비스의 접속이 가능한 것으로 판단하는 단계를 포함하는 단말의 인증 방법.

청구항 18

청구항 16에 있어서,

상기 단말의 인증 방법은,

상기 적어도 하나의 취소 식별자 중 상기 단말의 가명 식별자와 동일한 식별자가 존재하는 경우, 상기 단말의 가명 식별자가 취소 식별자의 대상인 것으로 판단하는 단계; 및

상기 차량 클라우드 서비스의 접속이 불가능한 것으로 판단하는 단계를 포함하는 단말의 인증 방법.

청구항 19

청구항 16에 있어서,

상기 단말의 인증 방법은,

상기 가명 인증 정보의 생성에 사용된 마스터 비밀키가 상기 노변 장치에 미리 저장된 마스터 공개키에 상응하는 마스터 비밀키가 아닌 경우, 상기 차량 클라우드 서비스의 접속이 불가능한 것으로 판단하는 단계를 포함하는 단말의 인증 방법.

청구항 20

청구항 16에있어서,

상기 단말의 인증 방법은,

상기 노변 장치의 데이터베이스(database)에 저장된 적어도 하나의 가명 식별자 중 상기 적어도 하나의 취소 식별자와 동일한 식별자인 취소 대상 식별자가 존재하는 경우, 상기 취소 대상 식별자가 포함된 메시지를 상기 서비스 제공 서버로 전송하는 단계를 더 포함하는 단말의 인증 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 차량 클라우드 서비스 접속을 위한 인증 방법에 대한 것으로, 더욱 상세하게는 차량 클라우드 서비스를 제공하는 외부장치 및 차량 내의 단말 간의 익명 인증 방법에 관한 것이다.

배 경 기 술

[0002] 스마트 자동차(smart car) 혹은 지능형 자동차(smart vehicle) 기술의 발전에 따라 차량에 탑재되는 컴퓨팅(computing) 기술과 무선 통신(wireless communication) 기술, GPS(global positioning system) 기술 및 내비게이션(navigation) 기술 등이 발전하고 있다. 또한, 이러한 기술들을 기반으로 제공되는 차량의 주행안전 및 편의성을 위한 지능형 교통정보시스템(Intelligent Transportation System, ITS), 위치기반서비스(Location-Based Service, LBS) 및 멀티미디어 콘텐츠를 포함하는 다양한 인포테인먼트(Infotainment) 서비스를 위한 기술과 차량 네트워크 서비스 모델들이 연구되고 있다.

[0003] 이와 관련하여, 대량의 도로교통정보의 수집과 처리, 대용량 멀티미디어 데이터의 저장과 공유 등과 같은 응용서비스는 복잡하고 많은 계산적 처리와 고용량의 저장 공간이 요구된다. 이러한 요구에 대해, 차량 네트워크 기술과 클라우드 컴퓨팅 기술을 결합함으로써, 차량 네트워크 응용서비스에 필요한 컴퓨팅 자원을 효과적으로 공유하고 처리하기 위한 차량 클라우드 컴퓨팅(vehicular cloud computing)에 대한 연구가 활발히 진행되고 있다.

[0004] 차량 클라우드 컴퓨팅 모델은 인터넷에서 구현되는 중앙 클라우드(Central Cloud)와 노변 장치들의 컴퓨팅 시스템을 활용한 노변 클라우드(Roadside Cloud)로 구분된다. 중앙 클라우드는 통상적인 상용 클라우드와 동일하게 고성능의 분산 컴퓨팅과 대용량의 스토리지 서비스를 위한 다양한 플랫폼(platform)을 제공한다. 노변 클라우드는 노변 장치들이 연결된 각각의 로컬 서버들을 결합하여 구성된다. 또한, 노변 클라우드는 각 노변 장치가 설

치된 지역을 통과하는 차량들에게 V2I(vehicle to infrastructure) 통신을 이용하여 주행 차량에게 필요한 지역적 정보(예를 들어, 주변 도로 교통상황 정보 및 편의시설 정보 등) 서비스 또는 멀티미디어 콘텐츠 다운로드 등을 제공하기 위해 차량을 중앙 클라우드의 서비스에 연결하는 중계 기능을 수행한다.

[0005] 차량 네트워크를 기반으로 도로상의 노변 장치를 통해 중앙 클라우드에 접속되는 차량 클라우드 서비스는 보안에 대한 안정성이 요구된다. 즉, 차량 클라우드 서비스의 접속이 허가되지 않은 차량(혹은 사용자)의 부당한 접속을 방지하기 위해, 노변 장치를 통한 차량의 V2I 인증(V2I authentication) 과정이 선행되어야 한다. 이때, 차량과 운전자의 프라이버시 보호를 위해 노변 장치를 통한 차량의 인증과정에서 차량의 실제 식별정보의 노출과 이동경로 추적을 예방할 수 있는 익명 인증 방법이 도입될 필요가 있다.

[0006] 차량 클라우드 서비스에서 차량의 익명 인증을 위한 종래의 연구들에 따르면, 대부분 차량의 인증에 사용될 신분증명으로 실제 차량의 식별정보 대신 시스템 관리자 또는 서비스 관리자가 발급한 복수의 가명 기반의 신분증명(Pseudonym Credential)을 사용하는 방법을 통해, 차량의 실제 식별정보의 노출을 방지한다. 여기서, 차량의 가명 신분증명은 차량 내에서 실제로 통신을 수행하는 단말의 가명 식별자를 의미할 수 있다. 또한, 차량에서 사용되는 가명 신분증명을 일정한 시간 동안 사용하도록 설정하고, 가명 신분증명을 주기적으로 교체하여 사용함으로써 동일한 신분증명을 사용하는 차량의 이동경로의 추적을 방지하는 방법들을 사용하고 있다.

[0007] 이러한 방법들은 차량의 익명성 보장을 악용하여 차량 클라우드 서비스를 부정적이나 악의적으로 사용하는 경우, 부정행위가 의심스러운 가명 신분증명을 사용한 차량을 추적하고 해당 가명 신분증명이 시스템에서 더 이상 사용되지 못하도록 취소(Revocation)시켜야 하는 상황이 발생될 수 있다. 따라서, 시스템에 등록된 차량들에게 발급한 복수의 가명 신분증명들에 대한 취소 발생 시 취소된 가명 신분증명들의 목록을 차량의 인증을 처리하는 노변 장치들에게 효율적으로 배포하기 위한 방법이 필요하다.

[0008] 일반적으로 차량 클라우드 서비스의 익명 인증 방법은 차량에서 사용되는 가명 신분증명들을 특별한 의미가 없는 임의적인 값으로 생성하고, 각 가명 신분증명을 사용하는 차량과 각 차량이 사용하는 노변 장치와의 연관성을 부여하지 않는다. 따라서, 각 가명 신분증명을 사용하는 차량이 차량 클라우드 서비스 상의 어떤 노변 장치에서 사용되는지 예측이 불가능한 문제가 있다.

[0009] 또한, 시스템은 취소된 가명 신분증명을 사용하는 차량의 접속을 허용하지 않도록 하기 위해 취소된 모든 가명 신분증명의 목록을 모든 노변 장치들에게 배포해야 한다. 이에 따라, 취소된 가명 신분증명의 수가 많아질수록 취소 목록의 크기가 커지고, 노변 장치들에게 목록을 전송하는데 오버헤드(overhead)가 발생하는 문제가 있다. 또한, 노변 장치는 잠재적으로 자신의 서비스 제공 영역에서 사용되지 않을 수도 있는 취소된 가명 신분증명 목록을 불필요하게 보관하게 되므로, 취소된 가명 신분증명의 목록의 검사에 소요되는 시간이 증가하는 문제가 있다.

발명의 내용

해결하려는 과제

[0010] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은 차량 클라우드 서비스 환경에서 차량 클라우드 서비스를 사용하는 차량 내의 단말들과 노변 클라우드 서비스를 제공하는 노변 장치들 간의 익명 인증 방법을 제공하는 데 있다.

과제의 해결 수단

[0011] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 단말의 인증 방법은 차량 클라우드 서비스(vehicle cloud service)에 접속하는 단말에서 수행되는 인증(authentication) 방법으로서, 상기 단말의 가명 식별자(pseudonym identity)를 암호화(encryption)하여 제1 식별자를 생성하는 단계, 상기 가명 식별자 및 상기 단말이 상기 차량 클라우드 서비스에 접속하기 위한 노변 장치(roadside unit)의 식별자를 암호화하여 제2 식별자를 생성하는 단계, 상기 제1 식별자 및 상기 제2 식별자를 기반으로 상기 단말 및 상기 노변 장치 간의 인증을 위해 상기 가명 식별자 및 상기 노변 장치의 식별자가 서로 연계된 가명 인증 정보를 생성하는 단계 및 상기 가명 인증 정보를 기반으로 상기 노변 장치와 인증을 수행하는 단계를 포함한다.

[0012] 여기서, 상기 제1 식별자는 상기 가명 식별자를 상기 차량 클라우드 서비스를 제공하는 서비스 제공 서버의 암호화 공개키를 기반으로 암호화된 식별자일 수 있다.

[0013] 여기서, 상기 제2 식별자는 상기 가명 식별자 및 상기 노변 장치의 식별자를 일방향 해시함수(one-way hash

function)를 기반으로 암호화된 식별자일 수 있다.

[0014] 여기서, 상기 단말의 인증 방법은 상기 노변 장치의 식별자를 암호화하여 제3 식별자를 생성하는 단계, 상기 제3 식별자가 포함된 메시지를 상기 차량 클라우드 서비스를 관리하는 교통 관리 서버로 전송하는 단계를 더 포함할 수 있다.

[0015] 여기서, 상기 제3 식별자는 상기 교통 관리 서버의 암호화 공개키를 기반으로 암호화된 식별자일 수 있다.

[0016] 여기서, 상기 가명 인증 정보를 생성하는 단계는 상기 제1 식별자가 포함된 메시지를 상기 차량 클라우드 서비스를 제공하는 서비스 제공 서버로 전송하는 단계, 상기 제2 식별자가 포함된 메시지를 상기 차량 클라우드 서비스를 관리하는 교통 관리 서버로 전송하는 단계, 상기 서비스 제공 서버로부터 상기 단말의 가명 식별자에 대응되는 상기 단말의 제1 개인키가 포함된 메시지를 수신하는 단계, 상기 교통 관리 서버로부터 상기 제2 식별자에 대응되는 상기 단말의 가명 식별자 및 상기 노변 장치의 식별자가 서로 연계된 제2 개인키가 포함된 메시지를 수신하는 단계 및 상기 제1 개인키 및 상기 제2 개인키를 기반으로 상기 가명 인증 정보를 생성하는 단계를 포함할 수 있다.

[0017] 여기서, 상기 가명 인증 정보는 상기 제1 개인키 및 상기 제2 개인키를 기반으로 겹선형 페어링(bilinear pairing) 연산하여 생성될 수 있다.

[0018] 여기서, 상기 제1 개인키는 상기 단말의 가명 식별자가 상기 서비스 제공 서버의 마스터 비밀키를 기반으로 암호화된 키일 수 있다.

[0019] 여기서, 상기 제2 개인키는 상기 제2 식별자가 상기 교통 관리 서버의 마스터 비밀키를 기반으로 암호화된 키일 수 있다.

[0020] 상기 목적을 달성하기 위한 본 발명의 다른 실시예에 따른 단말의 인증 방법은 차량 클라우드 서비스(vehicle cloud service)에 접속하는 단말에서 수행되는 인증(authentication) 방법으로서, 상기 단말의 가명 식별자(pseudonym identity) 및 상기 차량 클라우드 서비스의 접속을 위한 노변 장치(roadside unit)의 식별자가 서로 연계된 가명 인증 정보 및 상기 가명 식별자를 기반으로 상기 단말 및 상기 노변 장치 간의 인증을 요청하는 인증 요청 메시지를 생성하는 단계, 상기 인증 요청 메시지를 상기 노변 장치로 전송하는 단계 및 상기 노변 장치로부터 상기 인증 요청 메시지에 대한 응답이 포함된 인증 응답 메시지를 수신하는 단계를 포함한다.

[0021] 여기서, 상기 단말의 인증 방법은 상기 가명 식별자를 상기 노변 장치의 암호화 공개키를 기반으로 암호화(encryption)하여 암호화 가명 식별자를 생성하는 단계 및 상기 암호화 가명 식별자가 포함된 메시지를 상기 노변 장치로 전송하는 단계를 더 포함할 수 있다.

[0022] 여기서, 상기 인증 요청 메시지는 상기 가명 인증 정보의 소유에 대한 증명을 위해 상기 가명 인증 정보 및 상기 가명 식별자를 기반으로 생성되는 상기 가명 인증 정보의 서명(signature)을 포함할 수 있다.

[0023] 여기서, 상기 인증 응답 메시지는 상기 차량 클라우드 서비스에 대한 접속의 허용 및 거부 중 하나를 나타내는 응답 정보를 포함할 수 있다.

[0024] 상기 목적을 달성하기 위한 본 발명의 또 다른 실시예에 따른 단말의 인증 방법은 차량 클라우드 서비스(vehicle cloud service)를 제공하는 노변 장치(roadside unit)에서 수행되는 인증(authentication) 방법으로서, 단말로부터 상기 차량 클라우드 서비스에 접속을 위한 상기 단말 및 상기 노변 장치 간의 인증을 요청하는 인증 요청 메시지를 수신하는 단계, 상기 인증 요청 메시지에 포함된 상기 단말의 가명 식별자 및 상기 노변 장치의 식별자가 서로 연계된 가명 인증 정보의 서명(signature)을 기반으로 상기 차량 클라우드 서비스의 접속 가능 여부를 판단하는 단계 및 상기 접속 가능 여부의 결과를 포함하는 인증 응답 메시지를 상기 단말로 전송하는 단계를 포함한다.

[0025] 여기서, 상기 단말의 인증 방법은 상기 단말로부터 암호화 가명 식별자가 포함된 메시지를 수신하는 단계 및 상기 암호화 가명 식별자를 상기 노변 장치의 복호화(decryption) 개인키를 기반으로 복호화하여 상기 단말의 가명 식별자를 획득하는 단계를 더 포함할 수 있다.

[0026] 여기서, 상기 단말의 인증 방법은 상기 차량 클라우드 서비스를 제공하는 서비스 제공 서버로부터 적어도 하나의 취소 식별자를 포함하는 취소 식별자 목록이 포함된 메시지를 수신하는 단계를 더 포함할 수 있다.

[0027] 여기서, 상기 차량 클라우드 서비스의 접속 가능 여부를 판단하는 단계는 상기 단말의 가명 식별자를 상기 적어도 하나의 취소 식별자와 비교하여 상기 적어도 하나의 취소 식별자 중 상기 단말의 가명 식별자와 동일한 식별

자가 존재하지 않는 경우, 상기 단말의 가명 식별자가 취소 식별자의 대상이 아닌 것으로 판단하는 단계, 상기 서명을 상기 노변 장치의 암호화 공개키를 기반으로 복호화하여 상기 가명 인증 정보를 획득하는 단계, 상기 가명 인증 정보의 생성에 사용된 마스터 비밀키와 상기 노변 장치에 미리 저장된 마스터 공개키를 비교하는 단계 및 상기 단말의 가명 인증 정보의 생성에 사용된 마스터 비밀키가 상기 노변 장치에 미리 저장된 마스터 공개키에 상응하는 마스터 비밀키인 경우, 상기 차량 클라우드 서비스의 접속이 가능한 것으로 판단하는 단계를 포함할 수 있다.

[0028] 여기서, 상기 단말의 인증 방법은 상기 적어도 하나의 취소 식별자 중 상기 단말의 가명 식별자와 동일한 식별자가 존재하는 경우, 상기 단말의 가명 식별자가 취소 식별자의 대상인 것으로 판단하는 단계 및 상기 차량 클라우드 서비스의 접속이 불가능한 것으로 판단하는 단계를 포함할 수 있다.

[0029] 여기서, 상기 단말의 인증 방법은 상기 가명 인증 정보의 생성에 사용된 마스터 비밀키와 상기 노변 장치에 미리 저장된 마스터 공개키에 상응하는 마스터 비밀키가 아닌 경우, 상기 차량 클라우드 서비스의 접속이 불가능한 것으로 판단하는 단계를 포함할 수 있다.

[0030] 여기서, 상기 단말의 인증 방법은 상기 노변 장치의 데이터베이스(database)에 저장된 적어도 하나의 가명 식별자 중 상기 적어도 하나의 취소 식별자와 동일한 식별자인 취소 대상 식별자가 존재하는 경우, 상기 취소 대상 식별자가 포함된 메시지를 상기 서비스 제공 서버로 전송하는 단계를 더 포함할 수 있다.

발명의 효과

[0031] 본 발명에 의하면, 차량 클라우드 서비스에 접속하는 차량의 단말은 노변 장치를 통해 차량 클라우드 서비스 접속 시 인증을 위한 가명 인증 정보를 생성하는 단계에서, 노변 장치의 식별자가 암호화된 형태로 포함된 단말의 식별자 및 노변 장치의 식별자가 서로 연계된 식별자를 서비스 제공 서버 및 교통 관리 서버로 제공할 수 있다. 이에 따라, 차량 클라우드 서비스에 접속하는 단말은 서비스 제공 서버에게 접속하는 노변 장치의 정보를 노출시키지 않을 수 있고, 교통 관리 서버에는 단말의 가명 식별자를 노출시키지 않음으로써 해당 단말의 가명 식별자 및 노변 장치의 연계에 대한 정보를 노출시키지 않을 수 있다.

[0032] 또한, 본 발명에 따른 익명 인증 방법은 단말의 가명 인증 정보를 이용한 단말 및 노변 장치 간의 인증을 수행하는 단계에서, 단말에서 전송되는 노변 장치와의 인증을 요청하는 인증 요청 메시지는 가명 인증 정보의 소유를 증명하는 서명을 포함하고, 노변 장치가 가명 인증 정보의 서명에 대한 검증을 통해 차량 클라우드 서비스 접속을 요청하는 단말의 정당성을 인증함으로써, 서비스 제공 서버 및 교통 관리 서버를 통해 가명 인증 정보가 생성되지 않은 단말의 부당한 차량 클라우드 서비스 접속을 차단할 수 있다.

[0033] 또한, 본 발명에 따른 익명 인증 방법은 노변 장치에 의한 단말의 인증을 위해 V2I 통신을 통해 전송되는 단말의 가명 식별자는 일방향성을 제공하는 암호 해시함수를 이용하여 암호화된 형태의 식별자를 사용하므로, V2I 통신을 이용하여 차량 클라우드 서비스에 접속하는 단말을 사용하는 차량(혹은 사용자)의 익명성을 보장할 수 있다.

[0034] 또한, 본 발명에 따른 익명 인증 방법은 가명 인증 정보를 위한 차량 내의 단말의 가명 식별자를 자신이 접속할 노변 장치의 식별자와 연계함으로써, 해당 가명 식별자는 오직 특정 노변 장치에서만 사용할 수 있으므로 다른 노변 장치에서의 중복적인 가명 식별자 사용을 예방할 수 있고, 서로 다른 가명 식별자를 사용하여 차량 클라우드 서비스에 접속하는 단말에 대한 동일 여부의 예측을 방지할 수 있다.

[0035] 또한, 본 발명에 따른 익명 인증 방법은 부정행위 등으로 인해 차량 클라우드 서비스의 접속이 거부된 단말들의 취소 식별자 목록을 배포하는 단계에 있어서, 부정행위가 발견된 단말의 가명 식별자 및 노변 장치의 식별자가 연계된 정보를 기반으로 단말 및 노변 장치의 관계를 구분할 수 있다. 이에 따라, 시스템 환경에서 취소된 모든 취소 식별자 목록들을 도로상에 설치된 모든 노변 장치들에게 배포할 필요 없이, 노변 장치와 관련된 취소 식별자 목록만을 해당 노변 장치로 배포하므로 다른 노변 장치들에게 불필요한 취소 식별자 목록을 배포하지 않아 관리적 부담을 줄일 수 있다.

도면의 간단한 설명

[0036] 도 1은 본 발명의 일 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법이 수행되는 차량 네트워크를 도시한 개념도이다.

도 2는 본 발명의 일 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법을 도시한 개념도이

다.

도 3은 본 발명의 일 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법을 도시한 흐름도이다.

도 4는 본 발명의 일 실시예에 따른 차량 클라우드 서비스에 접속을 위한 가명 인증 정보를 생성하는 방법을 도시한 흐름도이다.

도 5는 본 발명의 다른 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법을 도시한 개념도이다.

도 6은 본 발명의 다른 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법을 도시한 흐름도이다.

도 7은 본 발명의 또 다른 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0037] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0038] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0039] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0040] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0041] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0042] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0044] 도 1은 본 발명의 일 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법이 수행되는 차량 네트워크를 도시한 개념도이다.

[0045] 도 1을 참조하면, 본 발명의 일 실시예에 따른 차량 클라우드 서비스(vehicle cloud service)에 접속을 위한 단말의 인증(authentication) 방법이 수행되는 차량 네트워크는 차량 클라우드(10) 및 노변 클라우드(20)를 포함할 수 있다. 구체적으로, 차량 클라우드(10)는 다양한 서비스들과 관련된 서버(server)들을 포함할 수 있다.

[0046] 예를 들어, 차량 클라우드(10)는 교통 관리 서버(11), 멀티미디어 서비스 제공 서버(12) 및 위치 기반 서비스 제공 서버(13) 등과 같은 서버들을 포함할 수 있다. 노변 클라우드(20)는 복수의 로컬 서버(local server)들(예

를 들어, 제1 로컬 서버(21) 및 제2 로컬 서버(22) 등)을 포함할 수 있다. 노변 클라우드(20)에 포함된 각 로컬 서버는 적어도 하나의 노변 장치(roadside unit)(예를 들어, 제1 노변 장치(31) 및 제2 노변 장치(32)들과 연결될 수 있다. 여기서, 노변 장치는 자신이 설치된 지점을 중심으로 일정한 영역(노변 장치가 서비스 제공 가능한 서비스 영역) 내를 통과하는 차량의 단말(이하, '단말'이라 함)과 통신을 수행할 수 있다. 여기서, 노변 장치 및 단말 간에 수행되는 통신은 V2I(vehicle to infrastructure) 통신을 의미할 수 있다. 노변 장치는 V2I 통신을 통해 단말로 차량 클라우드(10)에서 제공 가능한 다양한 서비스들을 제공할 수 있다.

[0047] 예를 들어, 제1 단말(31-1)은 제1 노변 장치(31)가 서비스의 제공이 가능한 서비스 영역 내에 위치할 수 있고, 이러한 경우 제1 노변 장치(31)에 연결될 수 있다. 제1 단말(31-1)은 제1 노변 장치(31)를 통해서 제1 로컬 서버(21)에 접속할 수 있다. 또한, 제1 로컬 서버(21)는 제1 단말(31-1)에서 요청하는 서비스에 기초하여 차량 클라우드(10)에 포함된 적어도 하나의 서버 중 해당하는 서버(예를 들어, 제1 단말(31-1)에서 요청하는 서비스가 지도와 관련된 서비스인 경우, 위치 기반 서비스 제공 서버)로 서비스 제공을 요청할 수 있다. 이후, 제1 단말(31-1)은 제1 로컬 서버(21)와 연결된 제1 노변 장치(31)를 통해 원하는 서비스를 이용할 수 있다.

[0048] 또한, 제2 단말(32-1) 및 제3 단말(32-2)은 제2 노변 장치(32)의 서비스 영역 내에 위치할 수 있고, 제2 노변 장치(32)를 통해 차량 클라우드(10)에서 제공되는 다양한 서비스들을 이용할 수 있다. 제2 단말(32-1) 및 제3 단말(32-2)이 서비스를 이용하는 방법은 제1 단말(31-1)이 서비스를 이용하는 방법과 동일할 수 있다.

[0049] 상술한 바와 같은 과정을 통해 단말은 이동하는 경로 상에 위치한 노변 장치로 접속할 수 있고, 해당 노변 장치와 연동된 로컬 서버를 통해 차량 클라우드에서 제공하는 다양한 서비스들을 이용할 수 있다. 단말은 이러한 과정 중 자신이 접속하는 노변 장치와 인증 과정을 우선적으로 수행해야 할 수 있다. 즉, 단말은 노변 장치와의 인증을 통해 차량 클라우드 서비스에 접속이 가능한(허가된) 단말임을 증명해야 할 수 있다. 이를 위해, 도 2 내지 도 7을 참조하여 본 발명에서 제안하는 차량 클라우드 서비스에 접속하는 단말의 인증 방법의 실시예들이 설명될 수 있다.

[0051] 먼저, 도 2 내지 도 4를 참조하여 본 발명의 일 실시예에 따른 단말의 인증 방법이 설명될 수 있다.

[0052] 도 2는 본 발명의 일 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법을 도시한 개념도이고, 도 3은 본 발명의 일 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법을 도시한 흐름도이고, 도 4는 본 발명의 일 실시예에 따른 차량 클라우드 서비스에 접속을 위한 가명 인증 정보를 생성하는 방법을 도시한 흐름도이다.

[0053] 도 2를 참조하면, 본 발명의 일 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법은 단말(100), 서비스 제공 서버(200) 및 교통 관리 서버(300) 간의 연동을 기반으로 수행될 수 있다. 여기서, 단말(100)은 차량 내에 위치하여 노변 장치와 통신을 수행하는 단말을 의미할 수 있다. 예를 들어, 단말(100)은 스마트 폰(smart phone) 및 내비게이션(navigation) 등과 같은 단말을 의미할 수 있다. 서비스 제공 서버(200)는 차량 클라우드 서비스를 제공하는 서버를 의미할 수 있고, 교통 관리 서버는 차량 클라우드 서비스를 이용하는 단말 및 차량 클라우드 서비스를 제공하는 노변 장치를 관리하는 서버를 의미할 수 있다.

[0054] 도 2는 단말(100) 및 노변 장치(400, 도 5 참조) 간의 인증에 사용되는 가명 인증 정보(104)가 단말(100)에서 생성되는 방법을 나타낼 수 있다. 구체적으로, 도 3을 참조하여 단말(100)에서 가명 인증 정보가 생성되는 방법이 설명될 수 있다.

[0055] 도 3을 참조하면, 본 발명의 일 실시예에 따른 차량 클라우드 접속을 위한 단말의 인증 방법은 단말(100)에서 수행될 수 있다. 여기서, 단말(100)은 프로세서(processor) 및 프로세서를 통해 실행되는 적어도 하나의 프로그램 명령(program command)이 저장되는 메모리(memory)를 포함할 수 있다. 단말(100)은 본 발명의 일 실시예에 따른 인증 방법을 수행하기 위한 프로그램 명령을 프로세서를 통해 수행할 수 있다.

[0056] 단말(100)의 메모리는 적어도 하나의 가명 식별자(pseudonym identity)를 저장할 수 있다. 여기서, 단말(100)은 메모리에 저장된 적어도 하나의 가명 식별자 중 노변 장치와 인증을 수행하기 위해 사용되는 가명 식별자(101)를 선택할 수 있다. 즉, 가명 식별자(101)는 단말(100)의 실제적인 식별자를 노출시키지 않기 위한 익명이 보장되는 식별자를 의미할 수 있다.

[0057] 이후, 단말(100)은 단말(100)의 가명 식별자(101)를 암호화(encryption)하여 제1 식별자(101-1)를 생성할 수 있다(S100). 즉, 단말(100)은 단말(100)의 가명 식별자(101)에 대하여 암호기술(cryptography)을 이용하여 제1 식별자(101-1)를 생성할 수 있다. 구체적으로, 단말(100)은 서비스 제공 서버(200)의 암호화 공개키를 기반으로 암호화하는 암호화 알고리즘(110)을 통해 제1 식별자(101-1)를 생성할 수 있다. 여기서, 단말(100)은 서비스 제

공 서버(200)의 암호화 공개키를 미리 가지는 것으로 가정될 수 있다.

[0058] 이후, 단말(100)은 차량 클라우드 서비스에 접속하기 위한 노변 장치를 선택할 수 있다. 즉, 단말(100)이 선택하는 노변 장치는 단말(100)의 이동 예정인 경로상에 위치하는 노변 장치 또는 단말(100)의 현재 위치를 기반으로 서비스 제공이 가능한 노변 장치를 의미할 수 있다.

[0059] 이후, 단말(100)은 단말(100)의 가명 식별자(101) 및 차량 클라우드 서비스에 접속하기 위한 노변 장치의 식별자(102)를 암호화하여 제2 식별자(103)를 생성할 수 있다(S110). 즉, 단말(100)은 단말(100)의 가명 식별자(101) 및 차량 클라우드 서비스에 접속하기 위한 노변 장치의 식별자(102)에 대하여 암호기술을 이용하여 제2 식별자(103)를 생성할 수 있다. 구체적으로, 단말(100)은 가명 식별자(101) 및 노변 장치의 식별자(102)를 일방향 해시함수(one-way hash function)를 기반으로 암호화하는 해시함수 기반 알고리즘(120)을 통해 제2 식별자(103)를 생성할 수 있다(S120).

[0060] 이후, 단말(100)은 제1 식별자(101-1) 및 제2 식별자(103)를 기반으로 가명 인증 정보(104)를 생성할 수 있다(S130). 여기서, 가명 인증 정보는 단말(100)의 가병 식별자(101) 및 노변 장치의 식별자(102)가 서로 연계된 정보를 의미할 수 있다. 이하에서, 도 4를 참조하여 가명 인증 정보(104)가 생성되는 구체적인 방법이 설명될 수 있다.

[0062] 도 4를 참조하면, 단말(100)은 제1 식별자(101-1)가 포함된 메시지(message)를 생성할 수 있다. 이후, 단말(100)은 제1 식별자(101-1)가 포함된 메시지를 서비스 제공 서버(200)로 전송할 수 있다(S121). 또한, 단말(100)은 제2 식별자(103)가 포함된 메시지를 생성할 수 있다. 이후, 단말(100)은 제2 식별자(103)가 포함된 메시지를 교통 관리 서버(300)로 전송할 수 있다(S122).

[0063] 한편, 서비스 제공 서버(200)는 단말(100)로부터 제1 식별자(101-1)가 포함된 메시지를 수신할 수 있다. 이후, 서비스 제공 서버(200)는 수신된 메시지에 포함된 제1 식별자(101-1)를 획득할 수 있다. 이후, 서비스 제공 서버(200)는 제1 식별자(101-1)를 서비스 제공 서버(200)의 복호화(decryption) 개인키(211)를 기반으로 복호화하는 복호화 알고리즘(210)을 통해 가명 식별자(101)를 획득할 수 있다.

[0064] 이후, 서비스 제공 서버(200)는 획득된 가명 식별자(101)를 서비스 제공 서버(200)의 데이터베이스(database)(230)에 저장할 수 있다. 구체적으로, 서비스 제공 서버(200)는 동일한 단말로부터 수신되는 가명 식별자에 대하여 동일한 인덱스(index) 번호를 매핑(mapping)하여 데이터베이스(230)에 저장할 수 있다.

[0065] 예를 들어, 제1 단말로부터 수신되는 제1 가명 식별자 및 제2 가명 식별자는 제1 인덱스 번호와 매핑되어 데이터베이스에 저장될 수 있다. 또한, 제2 단말로부터 수신되는 제3 가명 식별자 및 제4 가명 식별자는 제2 인덱스 번호와 매핑되어 데이터베이스에 저장될 수 있다.

[0066] 또한, 서비스 제공 서버(200)는 가명 식별자(101)를 서비스 제공 서버(200)의 마스터 비밀키를 기반으로 암호화하는 신원기반 키 생성 알고리즘(220)을 통해 제1 개인키(201)를 생성할 수 있다.

[0067] 이후, 서비스 제공 서버(200)는 생성된 제1 개인키(201)가 포함된 메시지를 생성할 수 있다. 이후, 서비스 제공 서버(200)는 제1 개인키(201)가 포함된 메시지를 단말(100)로 전송할 수 있다.

[0068] 한편, 단말(100)에서 수행되는 단계(S122)에 따르면, 교통 관리 서버(300)는 단말(100)로부터 제2 식별자(103)가 포함된 메시지를 수신할 수 있다. 이후, 교통 관리 서버(300)는 수신된 메시지에 포함된 제2 식별자(103)를 획득할 수 있다. 또한, 교통 관리 서버(300)는 제2 식별자(103)를 교통 관리 서버(300)의 마스터 비밀키를 기반으로 암호화하는 신원기반 키 생성 알고리즘(310)을 통해 제2 개인키(301)를 생성할 수 있다.

[0069] 이후, 교통 관리 서버(300)는 생성된 제2 개인키(301)가 포함된 메시지를 생성할 수 있다. 이후, 교통 관리 서버(300)는 제2 개인키(301)가 포함된 메시지를 단말(100)로 전송할 수 있다.

[0070] 한편, 단말(100)은 서비스 제공 서버(200)로부터 제1 개인키(201)가 포함된 메시지를 수신할 수 있다(S123). 이후, 단말(100)은 수신된 메시지에 포함된 제1 개인키(201)를 획득할 수 있다. 또한, 단말(100)은 교통 관리 서버(200)로부터 제2 개인키(301)가 포함된 메시지를 수신할 수 있다(S124). 이후, 단말(100)은 수신된 메시지에 포함된 제2 개인키(301)를 획득할 수 있다.

[0071] 이후, 단말(100)은 제1 개인키(201) 및 제2 개인키(301)를 기반으로 가명 인증 정보(104)를 생성할 수 있다(S125). 구체적으로, 단말(100)은 제1 개인키(201) 및 제2 개인키(301)를 결합하는 가명 인증 정보 생성 알고리즘을 기반으로 가명 인증 정보(104)를 생성할 수 있다.

[0072] 이후, 단말(100)은 생성된 가명 인증 정보(104)를 기반으로 노변 장치와 인증을 수행할 수 있다(S130). 또한, 단말(100)은 노변 장치의 식별자(102)를 교통 관리 서버(300)의 암호화 공개키를 기반으로 암호화하는 암호화 알고리즘(130)을 통해 제3 식별자(120-1)를 생성할 수 있다(S140). 이후, 단말(100)은 제3 식별자가 포함된 메시지를 생성할 수 있고, 생성된 메시지를 교통 관리 서버(300)로 전송할 수 있다(S150). 여기서, 단말(100)에서 수행되는 단계 S100 내지 S150가 수행되는 순서는 상기에서 설명되는 순서에 한정되지 않을 수 있다. 즉, 단말(100)은 제3 식별자를 생성하고, 제3 식별자가 포함된 메시지의 생성하여 교통 관리 서버로 전송한 후 제1 식별자 또는 제2 식별자를 생성할 수도 있다.

[0073] 한편, 교통 관리 서버(300)는 단말(100)로부터 제3 식별자(120-1)가 포함된 메시지를 수신할 수 있다. 이후, 교통 관리 서버(300)는 수신된 메시지에 포함된 제3 식별자(120-1)를 획득할 수 있다. 이후, 교통 관리 서버(300)는 제3 식별자(120-1)를 교통 관리 서버(300)의 복호화 개인키를 기반으로 복호화하는 복호화 알고리즘(320)을 통해 노변 장치의 식별자(102)를 획득할 수 있다.

[0074] 이후, 교통 관리 서버(300)는 획득된 노변 장치의 식별자(102)를 교통 관리 서버(300)의 데이터베이스(330)에 저장할 수 있다. 구체적으로, 교통 관리 서버(300)는 동일한 단말로부터 수신되는 노변 장치의 식별자에 대하여 동일한 인덱스 번호를 매핑하여 데이터베이스(330)에 저장할 수 있다.

[0075] 예를 들어, 제1 단말로부터 수신되는 제1 노변 장치의 식별자 및 제2 노변 장치의 식별자는 제1 인덱스 번호와 매핑되어 데이터베이스에 저장될 수 있다. 또한, 제2 단말로부터 수신되는 제3 노변 장치의 식별자 및 제4 노변 장치의 식별자는 제2 인덱스 번호와 매핑되어 데이터베이스에 저장될 수 있다.

[0076] 도 2 내지 도 4를 참조하여 설명한 바와 같이, 본 발명의 일 실시예에 따른 차량 클라우드 접속을 위한 단말의 인증 방법은 단말(100), 서비스 제공 서버(200) 및 교통 관리 서버(300)의 연동을 기반으로 단말(100) 및 노변 장치 간의 인증을 위한 가명 인증 정보(104)가 생성될 수 있다. 또한, 단말(100)은 가명 인증 정보(104)를 기반으로 노변 장치와 인증을 수행할 수 있다. 이하에서는, 도 5 내지 도 7을 참조하여 가명 인증 정보(104)를 기반으로 단말(100) 및 노변 장치 간에 인증이 수행되는 구체적인 방법이 설명될 수 있다.

[0078] 도 5는 본 발명의 다른 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법을 도시한 개념도이고, 도 6은 본 발명의 다른 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법을 도시한 흐름도이고, 도 7은 본 발명의 또 다른 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법을 도시한 흐름도이다.

[0079] 도 5를 참조하면, 본 발명의 다른 실시예에 따른 차량 클라우드 서비스에 접속을 위한 단말의 인증 방법은 단말(100) 및 노변 장치(400) 간에 수행될 수 있다. 먼저, 단말(100)은 차량 클라우드 서비스의 접속에 대한 필요가 발생하는 경우, 접속 가능한 노변 장치의 유무를 판단할 수 있다. 예를 들어, 노변 장치는 자신의 서비스 영역 내에 위치하는 적어도 하나의 단말이 존재하는 경우, 해당하는 단말로 주기적인 신호를 전송할 수 있다. 또한, 노변 장치는 단말의 존재 여부와 관계 없이 주기전인 신호를 전송할 수 있다. 단말(100)은 노변 장치로부터 신호를 수신하는 경우, 해당 노변 장치의 서비스 영역 내에 위치하는 것으로 판단할 수 있다. 이를 통해, 단말(100)은 접속 가능한 노변 장치의 유무를 판단할 수 있고, 접속하고자 하는 노변 장치를 결정할 수 있다.

[0080] 또는, 단말(100)은 이동 예정인 경로 상에 위치하는 노변 장치들의 정보를 미리 가질 수 있다. 이러한 경우, 단말(100)은 미리 가지는 노변 장치들의 정보를 기반으로 접속하고자 하는 노변 장치(400)를 결정할 수도 있다. 이와 같이, 단말(100)은 차량 클라우드 서비스 접속을 위한 노변 장치를 결정할 수 있다. 이하에서, 단말(100)이 인증을 수행하는 노변 장치(400)는 차량 클라우드 서비스 접속을 위한 노변 장치를 의미할 수 있다. 이후, 단말(100)은 해당 노변 장치(400)와 인증을 수행하기 위한 가명 인증 정보(104)를 도 2 내지 도 4를 참조하여 설명한 방법을 기반으로 생성할 수 있다. 이하에서, 도 6을 참조하여 본 발명의 다른 실시예에 따른 차량 클라우드 서비스 접속을 위한 단말의 인증 방법이 구체적으로 설명될 수 있다.

[0081] 도 6을 참조하면, 단말(100)은 가명 인증 정보(104) 및 가명 식별자(101)를 기반으로 인증 요청 메시지를 생성할 수 있다(S200). 여기서, 가명 인증 정보(104)는 단말의 가명 식별자(101) 및 노변 장치(400)의 식별자(401)가 서로 연계되어 미리 생성된 정보일 수 있다. 또한, 단말(100)이 생성하는 인증 요청 메시지는 가명 인증 정보(104)의 소유에 대한 증명을 위해 가명 인증 정보(104) 및 가명 식별자(101)를 기반으로 생성되는 가명 인증 정보(104)에 대한 서명(signature)(104-1)을 포함할 수 있다.

[0082] 구체적으로, 단말(100)은 인증 요청 메시지(105)에 대해 가명 인증 정보(104) 및 가명 식별자(101)를 이용하여 가명 인증 정보(104)의 소유 증명을 위한 서명 알고리즘(150)을 통해 가명 인증 정보(104)의 서명(104-1)을 생

성할 수 있다.

[0083] 이후, 단말(100)은 가명 식별자(101)를 노변 장치(400)의 암호화 공개키(402)를 기반으로 암호화하는 암호화 알고리즘(160)을 통해 암호화 가명 식별자(101-1)를 생성할 수 있다(S210). 여기서, 암호화 가명 식별자(101-1)는 도 2를 참조하여 설명된 제1 식별자(101-1)와 동일한 식별자를 의미할 수 있다.

[0084] 이후, 단말(100)은 암호화 가명 식별자(101-1)가 포함된 메시지를 생성할 수 있다. 이후, 단말(100)은 생성된 메시지를 노변 장치(400)로 전송할 수 있다(S220). 또한, 단말(100)은 단계 S200에서 생성된 인증 요청 메시지를 노변 장치(400)로 전송할 수 있다(S230). 여기서, 단말(100)이 인증 요청 메시지 및 암호화 가명 식별자(101-1)가 포함된 메시지를 노변 장치(400)로 전송하는 순서는 상기의 설명에 한정되는 것은 아니다. 즉, 단말(100)은 암호화 가명 식별자가 포함된 메시지를 노변 장치(400)로 전송한 후 인증 요청 메시지를 생성하여, 이를 노변 장치로(400) 전송할 수도 있다.

[0085] 이후, 단말(100)은 노변 장치(400)로부터 인증 요청 메시지에 대한 응답이 포함된 인증 응답 메시지를 수신할 수 있다(S240). 여기서, 인증 응답 메시지는 차량 클라우드 서비스에 대한 접속의 허용 및 거부 중 하나를 나타내는 응답 정보를 포함할 수 있다. 단말(100)로부터 인증 요청 메시지를 수신한 노변 장치(400)에서 인증 요청 메시지에 대한 응답으로 인증 응답 메시지를 생성 및 전송하는 방법은 도 7을 참조하여 구체적으로 설명될 수 있다.

[0087] 도 7을 참조하면, 도 5에 도시된 노변 장치(400)에서 수행되는 인증 방법이 설명될 수 있다. 즉, 도 7은 도 6에 도시된 단말(100)에서 수행되는 단계 S220 및 단계 S230에 대응되는 노변 장치(400)의 동작을 의미할 수 있다.

[0088] 먼저, 노변 장치(400)는 단말(100)로부터 차량 클라우드 서비스에 접속을 위한 노변 장치(400) 및 단말(100)간의 인증을 요청하는 인증 요청 메시지를 수신할 수 있다(S300). 여기서, 인증 요청 메시지는 가명 인증 정보(104)의 서명(104-1)을 포함할 수 있다. 또한, 노변 장치(400)는 단말(100)로부터 암호화 가명 식별자(101-1)가 포함된 메시지를 수신할 수 있다(S310). 여기서, 노변 장치(400)가 단말(100)로부터 인증 요청 메시지 및 암호화 가명 식별자(101-1)가 포함된 메시지를 수신하는 순서는 단말(100)에서 수행되는 단계 S220 및 단계 S230에 기초하여 결정될 수 있다.

[0089] 이후, 노변 장치(400)는 암호화 가명 식별자(101-1)를 노변 장치(400)의 복호화 개인키(403)를 기반으로 복호화하는 복호화 알고리즘(420)을 통해 가명 식별자(101)를 획득할 수 있다(S320). 이때, 노변 장치(400)는 차량 클라우드 서비스를 제공하는 서비스 제공 서버로부터 적어도 하나의 취소(revocation) 식별자를 포함하는 취소 식별자 목록이 포함된 메시지를 수신할 수 있다. 이후, 노변 장치(400)는 수신된 메시지에서 적어도 하나의 취소 식별자를 포함하는 취소 식별자 목록을 획득할 수 있다. 즉, 노변 장치(400)는 서비스 제공 서버로부터 취소 식별자 목록을 미리 수신함으로써, 적어도 하나의 취소 식별자에 대한 정보를 미리 가질 수 있다.

[0090] 또한, 노변 장치(400)는 적어도 하나의 취소 식별자를 데이터베이스에 저장할 수 있다. 여기서, 데이터베이스는 단말(100)의 가명 식별자(101) 및 이후에 획득되는 적어도 하나의 가명 식별자를 저장할 수도 있다.

[0091] 이때, 노변 장치(400)는 데이터베이스에 저장된 적어도 하나의 가명 식별자 중 적어도 하나의 취소 식별자와 동일한 취소 대상 식별자가 존재하는 경우, 해당하는 취소 대상 식별자가 포함된 메시지를 생성할 수 있다. 이후, 노변 장치(400)는 생성된 메시지를 서비스 제공 서버로 전송할 수 있다.

[0092] 이후, 노변 장치(400) 인증 요청 메시지에 포함된 가명 인증 정보(104)의 서명(104-1)을 기반으로 차량 클라우드 서비스의 접속 가능 여부를 판단할 수 있다(S330). 여기서, 노변 장치(400)는 인증 요청 메시지(105)에 대해 단말(100)의 가명 인증 정보(104)의 서명(104-1), 가명 식별자(101) 및 노변 장치(400)의 식별자(401)를 기반으로 수행되는 가명 인증 정보(104)의 서명(104-1)에 대한 검증 알고리즘(410)을 통해 단말(100)의 차량 클라우드 서비스의 접속 가능 여부를 판단할 수 있다.

[0093] 구체적으로, 노변 장치(400)는 단말(100)의 가명 식별자(101)를 서비스 제공서버로부터 수신된 취소 식별자 목록에 포함된 적어도 하나의 취소 식별자와 비교하여 적어도 하나의 취소 식별자 중 단말(100)의 가명 식별자(101)와 동일한 식별자가 존재하는지 확인할 수 있다. 이후, 노변 장치(400)는 적어도 하나의 취소 식별자 중 단말(100)의 가명 식별자(101)와 동일한 식별자가 존재하는 경우, 해당하는 단말(100)의 가명 식별자(101)가 취소 식별자인 것으로 판단할 수 있다. 즉, 노변 장치(400)는 단말(100)이 차량 클라우드 서비스의 접속에 대해 차단된(차량 클라우드 서비스의 접속이 불가능) 것으로 판단할 수 있다. 이러한 경우, 노변 장치(400)는 단말(100)로부터 수신된 인증 요청 메시지에 대한 응답으로 차량 클라우드 서비스의 접속이 불가능함을 나타내는 지시자가 포함된 인증 응답 메시지를 생성할 수 있다. 이후, 노변 장치(400)는 생성된 인증 응답 메시지를 단말

(100)로 전송할 수 있다.

[0094] 반면, 노변 장치(400)는 가명 식별자(101)와 동일한 식별자가 존재하지 않는 경우, 해당하는 단말(100)의 가명 식별자(101)가 취소 식별자가 아닌 것으로 판단할 수 있다. 즉, 노변 장치(400)는 단말(100)이 차량 클라우드 서비스의 접속에 대해 차단된 단말이 아닌 것으로 판단할 수 있다.

[0095] 이후, 노변 장치(400)는 단말(100)로부터 수신된 가명 인증 정보(104)의 서명(104-1)을 노변 장치(400)의 암호화 공캐기(104)를 기반으로 복호화하여 가명 인증 정보(104)를 획득할 수 있다. 이후, 노변 장치(400)는 가명 인증 정보(104)의 생성에 사용된 마스터 비밀키와 노변 장치(400)에 미리 저장된 마스터 공개키를 비교할 수 있다. 즉, 노변 장치(400)는 가명 인증 정보(104)의 생성에 사용된 서비스 제공 서버의 마스터 비밀키가 노변 장치(400)에 미리 저장된 서비스 제공 서버의 마스터 공개키(221)에 상응하는 마스터 비밀키인지 확인할 수 있다. 또한, 노변 장치(400)는 가명 인증 정보(104)의 생성에 사용된 교통 관리 서버의 마스터 비밀키가 노변 장치(400)에 미리 저장된 교통 관리 서버의 마스터 공개키(311)에 상응하는 마스터 비밀키인지 확인할 수 있다.

[0096] 이후, 노변 장치(400)는 단말(100)의 가명 인증 정보(104)의 생성에 사용된 마스터 비밀키가 노변 장치(400)에 미리 저장된 마스터 공개키에 상응하는 마스터 비밀키인 경우, 차량 클라우드 서비스의 접속이 가능한 것으로 판단할 수 있다. 즉, 노변 장치(400)는 단말(100)이 서비스 제공 서버 및 교통 관리 서버를 통해 정상적으로 가명 인증 정보(104)를 생성한 것으로 판단할 수 있다.

[0097] 이후, 노변 장치(400)는 단말(100)로부터 수신된 인증 요청 메시지에 대한 응답으로 차량 클라우드 서비스의 접속에 대하여 허용함을 나타내는 지시자가 포함된 인증 응답 메시지를 생성할 수 있다. 이후, 노변 장치(400)는 생성된 인증 응답 메시지를 단말(100)로 전송할 수 있다.

[0099] 이하에서는, 도 2 내지 도 7을 참조하여 설명된 본 발명의 일 실시예 및 다른 실시예에 따른 차량 클라우드 서비스의 접속을 위한 단말의 인증 방법을 사용하는 차량 네트워크 환경에서, 차량 클라우드 서비스의 접속의 차단이 필요한 단말이 발생한 경우가 설명될 수 있다.

[0100] 먼저, 노변 장치에서 차량 클라우드 서비스의 접속의 차단이 필요한 단말의 가명 식별자가 감지된 경우, 해당하는 가명 식별자가 포함된 메시지를 서비스 제공 서버로 전송할 수 있다. 여기서, 차량 클라우드 서비스의 접속의 차단이 필요한 단말은 이미 노변 장치와 인증을 수행한 후 차량 클라우드 서비스에 접속하여 서비스를 이용하고 있는 상태에서 더 이상 차량 클라우드 서비스를 이용하지 못하도록 접속의 취소가 필요한 단말을 의미할 수 있다.

[0101] 한편, 서비스 제공 서버는 노변 장치로부터 수신된 메시지에서 차량 클라우드 서비스의 접속에 대한 취소가 필요한 가명 식별자에 대한 인덱스 번호를 데이터베이스에 저장된 적어도 하나의 가명 식별자에 대한 인덱스 번호에서 검색할 수 있다. 이후, 서비스 제공 서버는 검색된 인덱스 번호에 해당하는 노변 장치의 식별자에 대한 정보를 요청하는 메시지를 생성할 수 있다. 즉, 서비스 제공 서버는 요청하는 노변 장치의 식별자에 해당하는 인덱스 번호가 포함된 메시지를 생성할 수 있다. 이후, 서비스 제공 서버는 생성된 메시지를 교통 관리 서버로 전송할 수 있다.

[0102] 한편, 교통 관리 서버는 서비스 제공 서버로부터 인덱스 번호가 포함된 메시지를 수신할 수 있다. 이후, 교통 관리 서버는 인덱스 번호에 해당하는 노변 장치의 식별자를 데이터베이스에 저장된 적어도 하나의 노변 장치의 식별자에서 검색할 수 있다. 이후, 교통 관리 서버는 검색된 노변 장치의 식별자가 포함된 메시지를 생성할 수 있다. 이후, 교통 관리 서버는 생성된 메시지를 서비스 제공 서버로 전송할 수 있다.

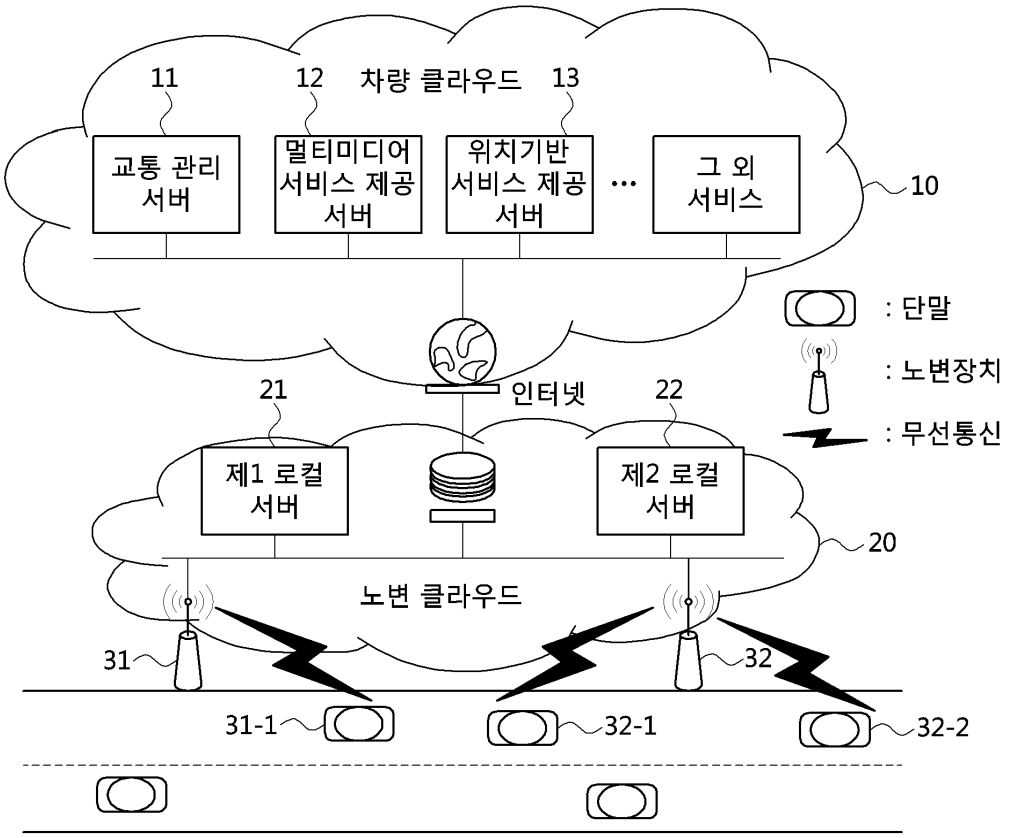
[0103] 이와 같은 방법을 통해, 서비스 제공 서버는 교통 관리 서버로부터 차량 클라우드 서비스의 접속에 대해 취소가 필요한 단말의 가명 식별자와 연계된 노변 장치의 식별자에 대한 정보를 획득할 수 있다. 이후, 서비스 제공 서버는 획득된 노변 장치의 식별자에 상응하는 노변 장치로 취소가 필요한 단말의 가명 식별자가 포함된 메시지를 생성할 수 있다. 즉, 서비스 제공 서버는 취소가 필요한 단말의 가명 식별자에 해당하는 단말의 차량 클라우드 접속을 취소시킬 것을 지시하는 지시자가 포함된 메시지를 생성할 수 있다. 이후, 서비스 제공 서버는 생성된 메시지를 해당하는 노변 장치로 전송할 수 있다. 즉, 서비스 제공 서버는 차량 클라우드 서비스의 접속에 대해 취소가 필요한 단말이 발생하는 경우, 해당 단말이 사용하는 노변 장치로만 차량 클라우드 서비스의 접속에 대해 취소를 지시하는 메시지를 전송할 수 있다.

[0105] 이상 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을

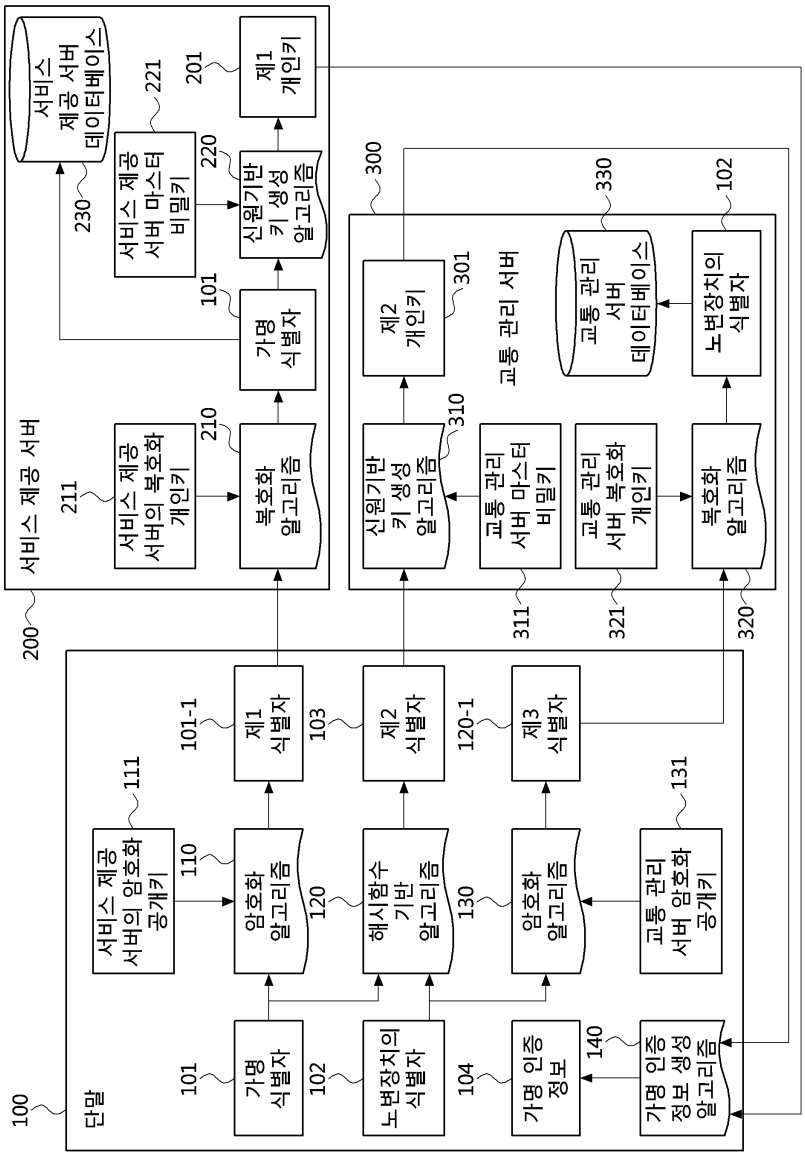
이해할 수 있을 것이다.

도면

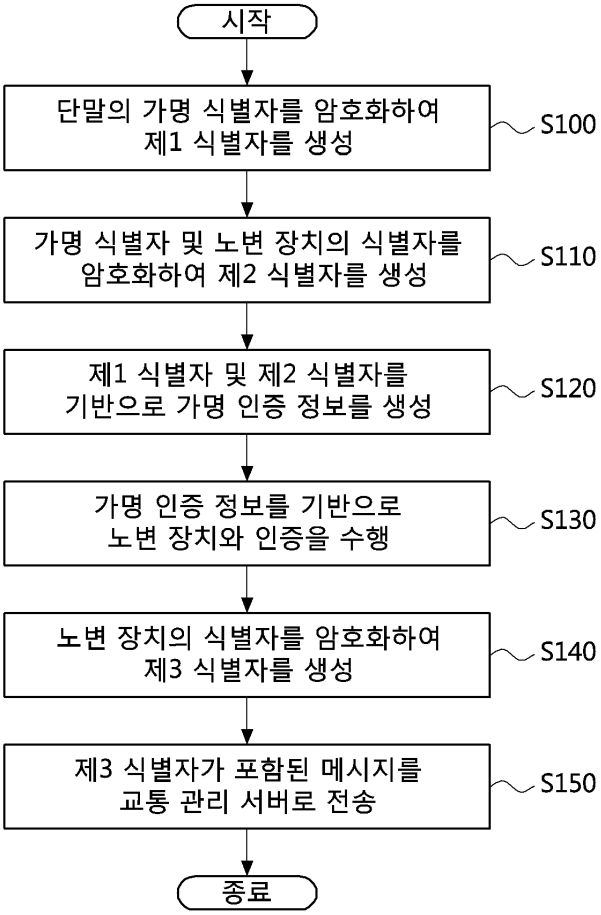
도면1



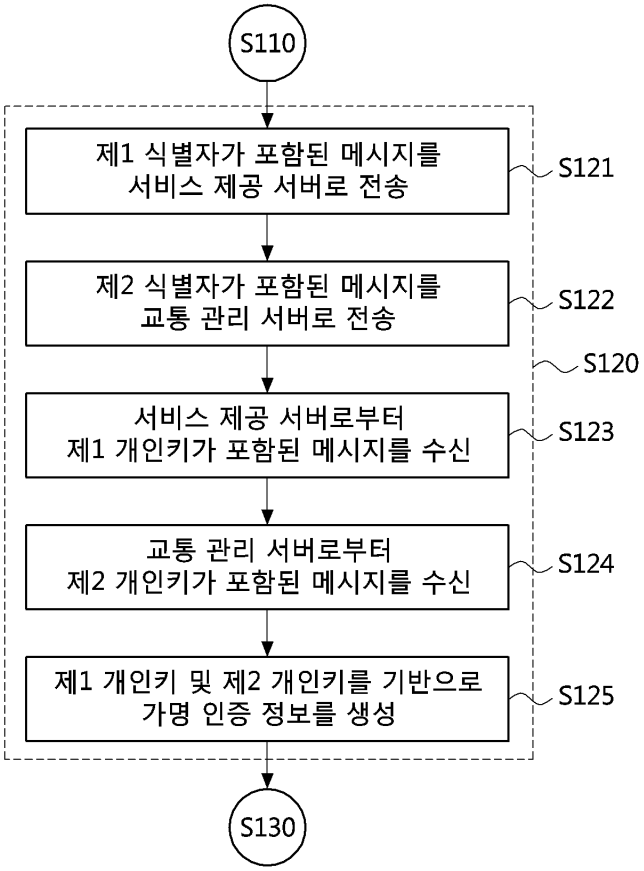
도면2


100
단말
101
가명 식별자
102
노변장치의 식별자
104
가명 인증 정보
140
가명 인증 정보 생성 알고리즘
111
서비스 제공 서버의 암호화 공개키
110
암호화 알고리즘
120
해시함수 기반 알고리즘
130
암호화 알고리즘
131
교통 관리 서버 암호화 공개키
101-1
제1 식별자
103
제2 식별자
120-1
제3 식별자
200
서비스 제공 서버
211
서비스 제공 서버의 복호화 개인키
210
복호화 알고리즘
101
가명 식별자
230
서비스 제공 서버 데이터베이스
221
서비스 제공 서버 마스터 비밀키
220
신원기반 키 생성 알고리즘
201
제1 개인키
300
교통 관리 서버
301
제2 개인키
310
신원기반 키 생성 알고리즘
311
교통 관리 서버 마스터 비밀키
321
교통 관리 서버 복호화 개인키
320
복호화 알고리즘
330
교통 관리 서버 데이터베이스
102
노변장치의 식별자

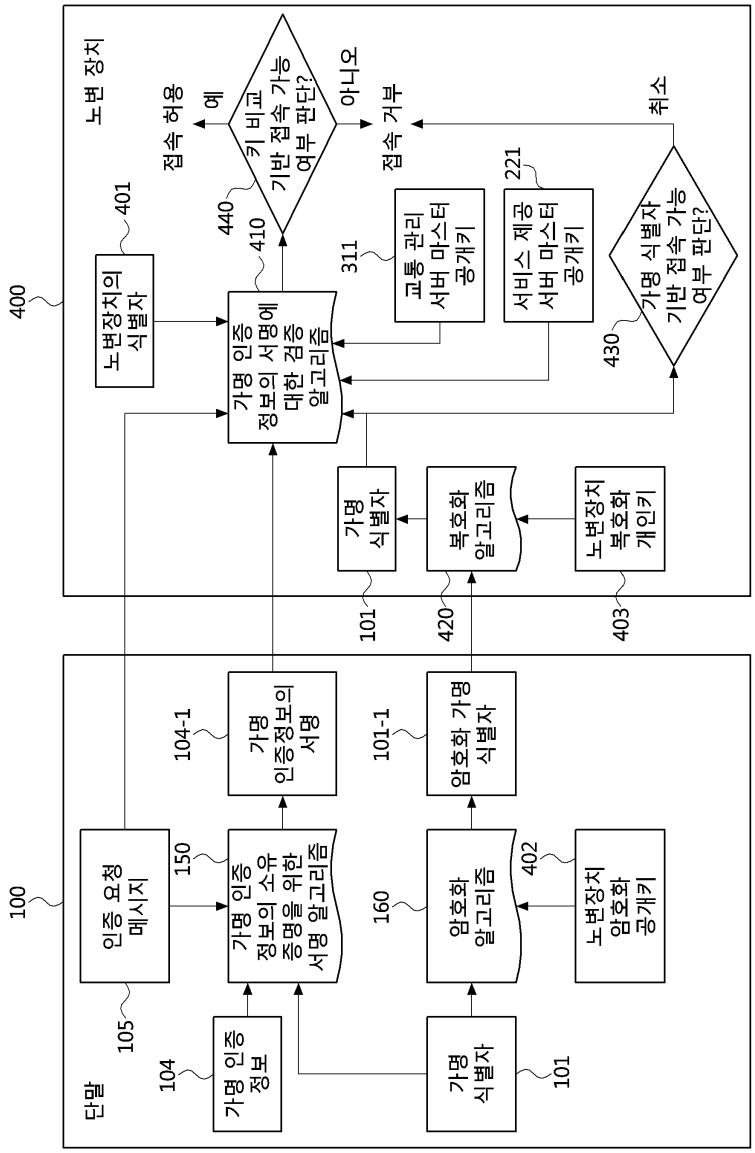
도면3


시작
단말의 가명 식별자를 암호화하여 제1 식별자를 생성
S100
가명 식별자 및 노변 장치의 식별자를 암호화하여 제2 식별자를 생성
S110
제1 식별자 및 제2 식별자를 기반으로 가명 인증 정보를 생성
S120
가명 인증 정보를 기반으로 노변 장치와 인증을 수행
S130
노변 장치의 식별자를 암호화하여 제3 식별자를 생성
S140
제3 식별자가 포함된 메시지를 교통 관리 서버로 전송
S150
종료

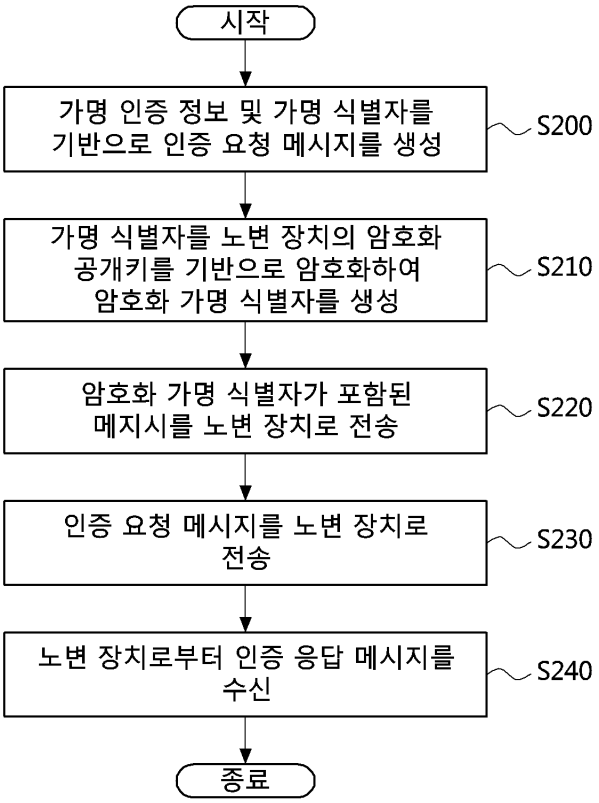
도면4


S110
제1 식별자가 포함된 메시지를
서비스 제공 서버로 전송
S121
제2 식별자가 포함된 메시지를
교통 관리 서버로 전송
S122
S120
서비스 제공 서버로부터
제1 개인키가 포함된 메시지를 수신
S123
교통 관리 서버로부터
제2 개인키가 포함된 메시지를 수신
S124
제1 개인키 및 제2 개인키를 기반으로
가명 인증 정보를 생성
S125
S130

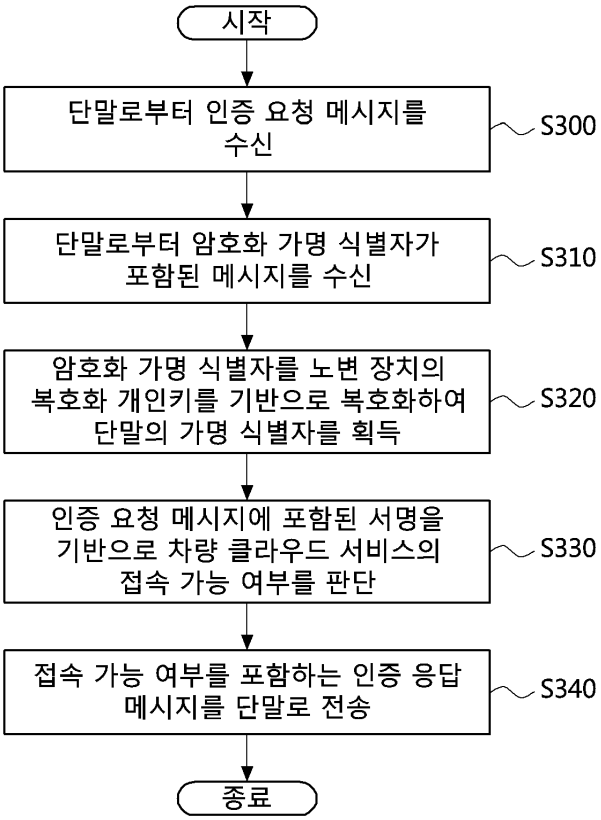
도면5


노변 장치
400
노변장치의 식별자
401
가명 인증 정보의 서명에 대한 검증 알고리즘
410
키 비교 기반 접속 가능 여부 판단?
440
예
접속 허용
아니오
접속 거부
교통 관리 서버 마스터 공개키
311
서비스 제공 서버 마스터 공개키
221
가명 식별자 기반 접속 가능 여부 판단?
430
취소
가명 식별자
101
복호화 알고리즘
420
노변장치 복호화 개인키
403
단말
100
인증 요청 메시지
105
가명 인증 정보
104
가명 인증 정보의 소유 증명을 위한 서명 알고리즘
150
가명 인증정보의 서명
104-1
가명 식별자
101
암호화 알고리즘
160
암호화 가명 식별자
101-1
노변장치 암호화 공개키
402

도면6


시작
가명 인증 정보 및 가명 식별자를 기반으로 인증 요청 메시지를 생성
S200
가명 식별자를 노변 장치의 암호화 공개키를 기반으로 암호화하여 암호화 가명 식별자를 생성
S210
암호화 가명 식별자가 포함된 메지시를 노변 장치로 전송
S220
인증 요청 메시지를 노변 장치로 전송
S230
노변 장치로부터 인증 응답 메시지를 수신
S240
종료

도면7


시작
단말로부터 인증 요청 메시지를 수신
S300
단말로부터 암호화 가명 식별자가 포함된 메시지를 수신
S310
암호화 가명 식별자를 노변 장치의 복호화 개인키를 기반으로 복호화하여 단말의 가명 식별자를 획득
S320
인증 요청 메시지에 포함된 서명을 기반으로 차량 클라우드 서비스의 접속 가능 여부를 판단
S330
접속 가능 여부를 포함하는 인증 응답 메시지를 단말로 전송
S340
종료