(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0092471
(43) 공개일자 2020년08월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06F 16/21* (2019.01)
G06F 21/60 (2013.01) *H04L 29/06* (2006.01)
H04L 9/06 (2006.01)
(52) CPC특허분류
H04L 9/0866 (2013.01)
G06F 16/21 (2019.01)
(21) 출원번호 10-2019-0002567
(22) 출원일자 2019년01월09일
심사청구일자 없음

(71) 출원인
현대자동차주식회사
서울특별시 서초구 헌릉로 12 (양재동)
기아자동차주식회사
서울특별시 서초구 헌릉로 12 (양재동)
(72) 발명자
류중희
경기도 화성시 남양읍 현대연구소로 150 전자네트워크개발팀
박승욱
경기도 용인시 수지구 태봉로 17, 403동 302호
임화평
경기도 성남시 분당구 불정로 219, 115-301
(74) 대리인
이철희

전체 청구항 수 : 총 16 항

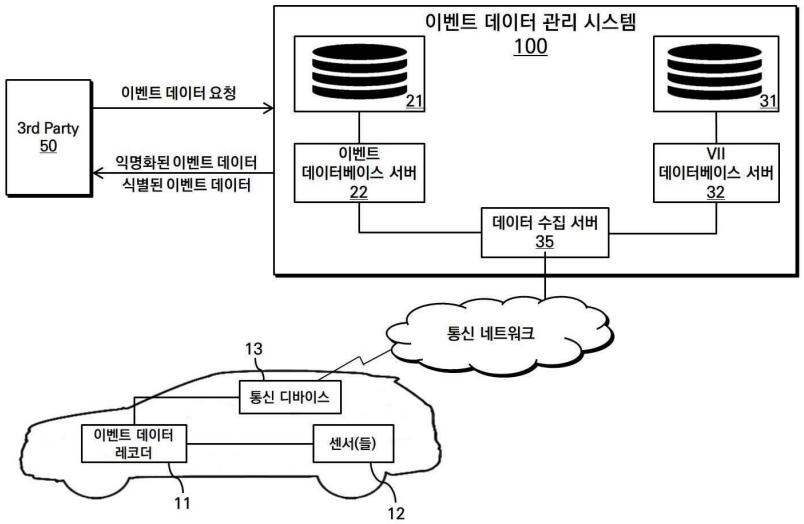
(54) 발명의 명칭 **클라우드 기반의 EDR 데이터 관리 방법 및 시스템**

(57) 요 약

클라우드 기반의 EDR 데이터 관리 방법 및 시스템을 개시한다.

각 차량에서 기록된 이벤트 데이터는 네트워크 상의 데이터베이스에 저장되고 관리된다. 개인의 프라이버시 보호를 위해, 제3자가 관련 차량을 식별하거나 추적할 수 있게 하는 차량 식별 정보가 이벤트 데이터로부터 분리된다. 그리고 분리된 차량 식별 정보와 이벤트 데이터를 각각 상이한 데이터베이스로 관리한다.

대 표 도



(52) CPC특허분류
G06F 21/60 (2013.01)
H04L 63/10 (2013.01)
H04L 9/0643 (2013.01)
H04L 2209/84 (2013.01)

명 세 서

청구범위

청구항 1

하나 이상의 컴퓨팅 시스템에 의해 수행되는, 차량의 이벤트 데이터를 수집 및 관리하는 방법에 있어서,

차량으로부터 이벤트 리포트 메시지를 수신하는 단계, 상기 이벤트 리포트 메시지는 차량 식별 정보와 상기 차량에서 기록된 이벤트 데이터를 포함함;

상기 차량 식별 정보로부터 가명 식별자를 생성하는 단계;

상기 이벤트 데이터를 상기 가명 식별자에 연관시켜, 제 1 데이터베이스에 저장하는 단계; 및

상기 차량 식별 정보를 제 2 데이터베이스에 저장하는 단계;

를 포함하는 방법.

청구항 2

제 1 항에 있어서,

상기 가명 식별자는,

상기 차량 식별 정보에 대해 단방향 해시 알고리즘(one-way hash algorithm)을 적용하여 생성되는 것을 특징으로 하는, 방법.

청구항 3

제 1 항에 있어서,

상기 가명 식별자는,

상기 차량 식별 정보와 난수(random number)에 대해 단방향 해시 알고리즘을 적용하여 생성되는 것을 특징으로 하는, 방법.

청구항 4

제 3 항에 있어서,

상기 난수는,

상기 차량 식별 정보에 연관되어 상기 제 2 데이터베이스에 저장되는 것을 특징으로 하는, 방법.

청구항 5

제 3 항에 있어서,

상기 난수는,

상기 제 1 데이터베이스 및 제 2 데이터베이스와는 독립적으로 관리되는 것을 특징으로 하는, 방법.

청구항 6

제 1 항에 있어서,

상기 가명 식별자는,

VII 인덱스에 대해 단방향 해시 알고리즘을 적용하여 생성되며, 상기 VII 인덱스는 상기 제 2 데이터베이스에서 상기 차량 식별 정보를 고유하게 식별시키는데 사용되는 것을 특징으로 하는, 방법.

청구항 7

제 1 항에 있어서,

상기 이벤트 리포트 메시지는,

이벤트가 발생한 지리적 위치, 날짜, 및 시각 중 적어도 하나에 관한 부가 정보를 더 포함하며, 상기 부가 정보는 상기 제 1 데이터베이스 또는 상기 제 2 데이터베이스에 저장되는 것을 특징을 하는, 방법.

청구항 8

제 1 항에 있어서,

상기 제 1 데이터베이스와 상기 제 2 데이터베이스는 서로 상이한 사업자에 의해 관리되는 것을 특징으로 하는, 방법.

청구항 9

차량의 이벤트 데이터를 수집 및 관리하는 시스템에 있어서,

제 1 데이터베이스;

상기 제 1 데이터베이스를 관리하는 제 1 데이터베이스 서버;

제 2 데이터베이스;

상기 제 2 데이터베이스를 관리하는 제 2 데이터베이스 서버; 및

상기 제 1 데이터베이스 서버와 상기 제 2 데이터베이스서버에 통신적으로 연결된 데이터 수집 서버를 포함하고,

상기 데이터 수집 서버는,

차량으로부터, 차량 식별 정보와 상기 차량에서 기록된 이벤트 데이터를 포함하는, 이벤트 리포트 메시지를 수신하고, 상기 차량 식별 정보로부터 가명 식별자를 생성하도록 구성되고,

상기 제 1 데이터베이스 서버는,

상기 이벤트 데이터를 상기 가명 식별자에 연관시켜, 상기 제 1 데이터베이스에 저장하도록 구성되고,

상기 제 2 데이터베이스 서버는,

상기 차량 식별 정보를 상기 제 2 데이터베이스에 저장하도록 구성된 것을 특징으로 하는, 시스템.

청구항 10

제 9 항에 있어서,

상기 데이터 수집 서버는,

상기 차량 식별 정보에 대해 단방향 해시 알고리즘을 적용하여 상기 가명 식별자를 생성하도록 구성된 것을 특징으로 하는, 시스템.

청구항 11

제 9 항에 있어서,

상기 데이터 수집 서버는,

상기 차량 식별 정보와 난수(random number)에 대해 단방향 해시 알고리즘을 적용하여 상기 가명 식별자를 생성하도록 구성된 것을 특징으로 하는, 시스템.

청구항 12

제 11 항에 있어서,

상기 데이터 수집 서버는,

상기 난수를 자체적으로 안전하게 보관하도록 구성된 것을 특징으로 하는, 시스템.

청구항 13

제 11 항에 있어서,

상기 데이터 수집 서버는,

상기 난수가 상기 차량 식별 정보에 연관되어 상기 제 2 데이터베이스에 저장되도록, 상기 제 2 데이터베이스 서버에 상기 난수를 제공하도록 구성된 것을 특징으로 하는, 시스템.

청구항 14

제 9 항에 있어서,

상기 데이터 수집 서버는,

상기 제 2 데이터베이스에서 상기 차량 식별 정보를 고유하게 식별시키는데 사용되는 VII 인덱스에 대해 단방향 해시 알고리즘을 적용하여 상기 가명 식별자를 생성하도록 구성된 것을 특징으로 하는, 시스템.

청구항 15

제 9 항에 있어서,

상기 이벤트 리포트 메시지는,

이벤트가 발생한 지리적 위치, 날짜, 및 시각 중 적어도 하나에 관한 부가 정보를 더 포함하며, 상기 부가 정보는 상기 제 1 데이터베이스 또는 상기 제 2 데이터베이스에 저장되는 것을 특징을 하는, 시스템.

청구항 16

제 9 항에 있어서,

상기 데이터 수집 서버, 상기 제 1 데이터베이스 서버, 및 상기 제 2 데이터베이스 서버 중 적어도 일부는 서로 상이한 사업자에 의해 운영되는 것을 특징으로 하는, 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 다수의 차량들에서 생성된 이벤트 데이터를 수집 및 저장하는 것과 관련되어 있다.

배 경 기 술

[0002] 이 부분에 기술된 내용은 단순히 본 발명에 대한 배경 정보를 제공할 뿐 종래기술을 구성하는 것은 아니다.

[0003] 일반적으로 이벤트 데이터 레코더(Event Data Recorder: EDR)는 사고 등을 검출하여 그 시점의 전후 소정 시간 내의 차량의 주행 상태나 운전자에 의한 조작 등에 관한 정보를 기억하도록 구성되어 있다. 속도, 안전 벨트 상태 및 에어백 전개 상태를 포함하는 적어도 여러 파라미터들이 포렌식 조사 과정에서 복구될 수 있도록 저장된다.

[0004] 포렌식 조사는, 일반적으로, OBD-II 포트를 통해 혹은 이벤트 데이터 레코더 의 데이터 메모리를 물리적으로 추출하여 데이터를 판독함으로써 수행된다. 이벤트 데이터 레코더 내의 데이터는 잘못된 판독 기술로 인해 손상되거나 변경될 수 있으며, 저장 후에 악의적으로 조작되거나 삭제될 수도 있는 바, 저장된 데이터에 대한 무결성이 완벽히 보장된다고 보기 어렵다.

[0005] 한편, 정부 기관이나 보험 회사, 자동차 제조사 등의 민간 조직의 조사자들은 교통 이벤트(예컨대, 교통 사고)를 둘러싼 상황을 조사하기 위해, 특정 데이터 소스(예컨대, 사고 차량)를 식별 및 추적한 다음 사고의 원인, 결함, 악화 요인, 완화 요인 등을 파악하는 데 필요한 정보를 각 데이터 소스에서 독자적으로 수집한다. 이러한 정보에는 이벤트 데이터 레코더 내의 데이터를 포함할 수 있다. 불행하게도, 위와 같은 방식으로 정보를 수집하는 데에는 많은 노력과 시간이 소요될 수 있다. 더욱이, 일부 데이터 소스는 식별되지 않거나 식별된 때에 더 이상 데이터를 사용할 수 없거나 이미 삭제되었을 수도 있다. 따라서, 교통 이벤트에 관한 데이터를 갖는 데이

터 소스를 자동으로 식별하고, 그러한 데이터를 적시에 획득할 수 있도록, 차량의 이벤트 데이터 레코더 내의 데이터를 수집 저장하는 시스템 및 관련 방법이 필요하다.

발명의 내용

해결하려는 과제

[0006] 클라우드 저장소 혹은 원격 서버는 권한없는 접근을 막고 데이터의 훼손을 방지할 수 있는 안전한 공간이 될 수 있다. 즉, EDR 데이터의 무결성 유지 등을 위해, 신뢰할 수 있는 클라우드 저장소에 EDR 데이터를 저장하는 것이 고려될 수 있다. 그러나, 클라우드 저장소에 EDR 데이터를 저장하는 데에는 개인의 프라이버시를 보호하기 위한 방안이 함께 고려되어야 한다. 이에, 본 발명은 개인의 프라이버시를 보호할 수 있는 클라우드 기반의 EDR 데이터 관리 시스템을 제안한다.

과제의 해결 수단

[0007] 본 발명의 일 측면에 의하면, 하나 이상의 컴퓨팅 시스템에 의해 수행되는, 차량의 이벤트 데이터를 수집 및 관리하는 방법으로서, 차량으로부터 이벤트 리포트 메시지를 수신하는 단계, 상기 이벤트 리포트 메시지는 상기 차량 식별 정보와 상기 차량에서 기록된 이벤트 데이터를 포함함; 상기 차량 식별 정보로부터 가명 식별자를 생성하는 단계; 상기 이벤트 데이터를 상기 가명 식별자에 연관시켜, 제 1 데이터베이스에 저장하는 단계; 및 상기 차량 식별 정보를 제 2 데이터베이스에 저장하는 단계를 포함한다.

[0008] 상기 방법의 실시예들은 다음의 특징들을 하나 이상 더 포함할 수 있다.

[0009] 일부 실시예에서, 상기 가명 식별자는 상기 차량 식별 정보에 대해 단방향 해시 알고리즘(one-way hash algorithm)을 적용하여 생성될 수 있다.

[0010] 일부 실시예에서, 상기 가명 식별자는 상기 차량 식별 정보와 난수(random number)에 대해 단방향 해시 알고리즘을 적용하여 생성될 수 있다. 상기 난수는 상기 차량 식별 정보에 연관되어 상기 제 2 데이터베이스에 저장되거나, 상기 제 1 데이터베이스 및 제 2 데이터베이스와는 독립적으로 관리될 수 있다.

[0011] 일부 실시예에서, 상기 가명 식별자는 VII 인덱스에 대해 단방향 해시 알고리즘을 적용하여 생성될 수 있다. 여기서 VII 인덱스는 상기 제 2 데이터베이스에서 상기 차량 식별 정보를 고유하게 식별시키는데 사용된다.

[0012] 일부 실시예에서, 상기 이벤트 리포트 메시지는 이벤트가 발생한 지리적 위치, 날짜, 및 시각 중 적어도 하나에 관한 부가 정보를 더 포함하며, 상기 부가 정보는 상기 제 1 데이터베이스 또는 상기 제 2 데이터베이스에 저장될 수 있다.

[0013] 일부 실시예에서, 상기 제 1 데이터베이스와 상기 제 2 데이터베이스는 서로 상이한 사업자에 의해 관리될 수 있다.

[0014] 본 발명의 다른 측면에 의하면, 차량의 이벤트 데이터를 수집 및 관리하는 시스템을 제공한다. 상기 시스템은 제 1 데이터베이스; 상기 제 1 데이터베이스를 관리하는 제 1 데이터베이스 서버; 제 2 데이터베이스; 상기 제 2 데이터베이스를 관리하는 제 2 데이터베이스 서버; 및 상기 제 1 데이터베이스 서버와 상기 제 2 데이터베이스서버에 통신적으로 연결된 데이터 수집 서버를 포함한다.

[0015] 상기 데이터 수집 서버는, 차량으로부터 이벤트 리포트 메시지를 수신한다. 이벤트 리포트 메시지는 상기 차량의 차량 식별 정보와 상기 차량에서 기록된 이벤트 데이터를 포함한다. 상기 데이터 수집 서버는, 상기 차량 식별 정보로부터 가명 식별자를 생성하도록 구성된다.

[0016] 상기 제 1 데이터베이스 서버는 상기 이벤트 데이터를 상기 가명 식별자에 연관시켜 상기 제 1 데이터베이스에 저장하도록 구성되고, 상기 제 2 데이터베이스 서버는 상기 차량 식별 정보를 상기 제 2 데이터베이스에 저장하도록 구성된다.

[0017] 상기 시스템의 실시예들은 다음의 특징들을 하나 이상 더 포함할 수 있다.

[0018] 일부 실시예에서, 상기 데이터 수집 서버는 상기 차량 식별 정보에 대해 단방향 해시 알고리즘을 적용하여 상기 가명 식별자를 생성하도록 구성될 수 있다.

[0019] 일부 실시예에서, 상기 데이터 수집 서버는 상기 차량 식별 정보와 난수(random number)에 대해 단방향 해시 알고리즘을 적용하여 상기 가명 식별자를 생성하도록 구성될 수 있다. 상기 데이터 수집 서버는 상기 난수를 자체

적으로 안전하게 보관하도록 구성될 수 있다. 대안적으로, 상기 데이터 수집 서버는, 상기 난수가 상기 차량 식별 정보에 연관되어 상기 제 2 데이터베이스에 저장되도록, 상기 제 2 데이터베이스 서버에 상기 난수를 제공하도록 구성될 수 있다.

[0020] 일부 실시예에서, 상기 데이터 수집 서버는, 상기 제 2 데이터베이스에서 상기 차량 식별 정보를 고유하게 식별시키는데 사용되는 VII 인덱스에 대해 단방향 해시 알고리즘을 적용하여, 상기 가명 식별자를 생성하도록 구성될 수 있다.

[0021] 일부 실시예에서, 상기 이벤트 리포트 메시지는 이벤트가 발생한 지리적 위치, 날짜, 및 시각 중 적어도 하나에 관한 부가 정보를 더 포함하며, 상기 부가 정보는 상기 제 1 데이터베이스 또는 상기 제 2 데이터베이스에 저장될 수 있다.

[0022] 일부 실시예에서, 상기 데이터 수집 서버, 상기 제 1 데이터베이스 서버, 및 상기 제 2 데이터베이스 서버 중 적어도 일부는 서로 상이한 사업자에 의해 운영될 수 있다.

발명의 효과

[0023] 제안된 방법 및 시스템에 따르면, 각 차량에서 기록된 이벤트 데이터는 네트워크 상의 데이터베이스에 저장되고 관리된다. 개인의 프라이버시 보호를 위해, 제3자가 관련 차량을 식별하거나 추적할 수 있게 하는 차량 식별 정보가 이벤트 데이터로부터 분리된다. 그리고 분리된 차량 식별 정보와 이벤트 데이터는 각각 상이한 데이터베이스로 관리된다. 어떠한 데이터베이스에도 이벤트 데이터와 그와 관련된 차량 식별 정보가 함께 저장되지 않는다. 이를 통해 개인의 프라이버시가 보호될 수 있다. 나아가, 각 데이터베이스에 상이한 액세스 권한 정책을 적용함으로써, 개인의 프라이버시의 보호는 한층 더 강화될 수 있다.

[0024] 또한, 제안된 방법 및 시스템에 따르면, 개인이나 기관은 이벤트 데이터가 저장된 네트워크 상의 데이터베이스를 검색하여, 관심 있는 이벤트에 관한 데이터(예컨대, EDR 데이터)를 적시에 쉽게 얻을 수 있다. 또한, 신뢰할 수 있는 네트워크 상의 저장소에 저장된 이벤트 데이터는 이벤트 데이터의 무결성 보장이 요구되는 포렌식 조사에 유용할 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 일 실시예에 따른, 클라우드 기반으로 이벤트 데이터를 저장하고 관리하는 전체 시스템을 도식화한 도면이다.

도 2는 도 1에 도시된 시스템의 이벤트 데이터 수집 프로세스를 예시하기 위한 흐름도이다.

도 3은 도 1에 예시된 이벤트 데이터 관리 시스템이 익명화된 이벤트 데이터를 제공하는 프로세스를 예시한 흐름도이다.

도 4는 도 1에 예시된 이벤트 데이터 관리 시스템이 특정한 차량과 관련된 이벤트 데이터를 제공하는 프로세스를 예시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 이하, 본 발명의 일부 실시예들을 예시적인 도면을 통해 상세하게 설명한다. 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[0027] 또한, 본 발명의 구성 요소를 설명하는 데 있어서, 제 1, 제 2, A, B, (a), (b) 등의 용어를 사용할 수 있다. 이러한 용어는 그 구성 요소를 다른 구성 요소와 구별하기 위한 것일 뿐, 그 용어에 의해 해당 구성 요소의 본질이나 차례 또는 순서 등이 한정되지 않는다. 명세서 전체에서, 어떤 부분이 어떤 구성요소를 '포함', '구비'한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 '…부,' '모듈' 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0029] 본 발명의 적어도 일부 실시예에 따르면, 각 차량에서 기록된 이벤트 데이터는 네트워크 상의 데이터베이스에 저장되고 관리된다. 제3자가 관련 차량이나 개인을 식별하거나 추적할 수 있게 하는 차량 식별 정보를 이벤트 데이터로부터 분리된다. 그리고 분리된 차량 식별 정보와 이벤트 데이터를 각각 상이한 데이터베이스로 관리한다.

[0030] 도 1은 본 발명의 일 실시예에 따른, 클라우드 기반으로 이벤트 데이터를 저장하고 관리하는 전체 시스템을 도식화한 도면이다.

[0031] 차량 탑재 모니터링 시스템은 이벤트 발생 시점의 전후 소정 시간 내의 차량의 주행 상태나 운전자에 의한 조작 등에 관한 데이터를 기록할 수 있다. 차량 탑재 모니터링 시스템은 기록된 데이터를 클라우드 기반의 이벤트 데이터 관리 시스템(100)에 무선 송신할 수 있다.

[0032] 차량 탑재 모니터링 시스템은 이벤트 데이터 레코더(Event Data Recorder: EDR; 11), 적어도 하나의 센서(12) 및 통신 디바이스(Telecommunication device; 13)를 포함할 수 있다. 이들은 차량 데이터 버스(예컨대, CAN(Controller Area Network), LIN(Local Interconnect Network), MOST(Medium Oriented Systems Transport), Ethernet 등)에 연결될 수 있다.

[0033] 이벤트 데이터 레코더(EDR; 11)는 하나 이상의 미리 정의된 이벤트의 발생이 검출되면, 그 검출 전후 소정 시간 내의 데이터를 기록하고 저장하도록 설계된다. 그러한 이벤트는 특히 충돌 사고(traffic collision)일 수 있다. 충돌 사고는, 예를 들어, 에어백의 전개가 트리거되는 때에 감지될 수 있다. 또한, 이벤트는 차량의 주요 기능의 고장을 더 포함할 수도 있다. 주요 기능의 고장은, 예컨대, 사전 정의된 임계 값을 초과하는 가/감속이 발생할 때 감지될 수 있다. 이벤트 데이터 레코더(11)는 적어도 하나의 센서(12)에 의해 측정된 값들에 접근 가능할 수 있다. 적어도 하나의 센서(12)는 차량 속도/가감속/이동 거리 등을 감지하도록 설계될 수 있다. 이벤트 데이터 레코더(11)에 의해 기록되는 데이터는, 예컨대, 차량의 동역학(dynamics), 운전자의 행동, 차량의 안전 시스템의 작동 상태 등과 같은 충돌 사고를 추적하기에 적합한 데이터일 수 있다. 이벤트 데이터 레코더(11)는 기록된 EDR 데이터를 통신 디바이스(13)에 제공한다.

[0034] 통신 디바이스(13)는, 이벤트 데이터 레코더(11)로부터 EDR 데이터가 수신되면, 위치 결정 디바이스(미도시), 시간 결정 디바이스(미도시) 등으로부터 이벤트가 발생한 날짜, 시각, 및 지리적 위치를 획득할 수 있다. 위치 결정 디바이스는 GPS, GNSS와 같은 위성 지원 위치 결정 시스템으로부터 지리적 위치 정보 및/또는 시간 정보를 수신하는 수신기를 포함할 수 있다. 통신 디바이스(13)는 위치 결정 디바이스 및/또는 시간 결정 디바이스를 포함하도록 구성될 수 있다. 대안적으로, 이벤트 데이터 레코더(11)에 의해 기록되는 이벤트 데이터 그 자체에 이벤트가 발생한 날짜, 시각, 및 지리적 위치가 포함될 수도 있다.

[0035] 통신 디바이스(13)는, 차량 내부 네트워크를 외부의 통신 네트워크에 연결하는 유선 혹은 무선 통신기기이다. 통신 디바이스(13)는, 예컨대, 텔레매틱스 유닛(Telematics Unit; TMU), OBD-Ⅱ 포트에 플러그 되는 유무선 동글일 수 있다. 통신 디바이스(13)는, 예를 들어, GSM/WCDMA/LTE/5G와 같은 셀룰러 통신 혹은 WLAN, c-V2X, WAVE, DSRC, 블루투스와 같은 단거리 무선 통신이 가능한 무선 송수신기를 포함하도록 구성될 수도 있다.

[0036] 통신 디바이스(13)는, 통신 네트워크를 거쳐, 이벤트 데이터 관리 시스템(100)에, 이벤트 리포트 메시지를 전송할 수 있다. 이벤트 리포트 메시지는 차량 식별 정보(Vehicle identifiable information: VII)와 이벤트 데이터 레코더(11)에 의해 이벤트 전후에 기록된 이벤트 데이터를 포함한다. 여기서, 차량 식별 정보는 해당 차량을 고유하게 식별할 수 있는 정보로서, 예컨대, 차량 내 ECU들로부터 수집될 수 있는 차량 식별 번호(vehicle identification number: VIN), 통신 디바이스(13)가 통신에 사용하는 고유 식별자, V2X 통신을 위해 차량에 부여된 (장기 혹은 단기) 인증서 등을 포함할 수 있다. 대안적으로, 개인(즉, 차량의 소유자 혹은 운전자)를 식별할 수 있는 개인 식별 정보(예컨대, 주민등록번호, 운전면허번호 등)가 차량 식별 정보에 대용하여 사용될 수도 있다.

[0037] 또한, 이벤트 리포트 메시지는 이벤트가 발생한 지리적 위치, 날짜, 시각, 차량 모델, 제조 년도, 제조사 등의 부가 정보를 더 포함할 수 있다. 이들 부가 정보 중 적어도 일부는 이벤트 데이터와 함께 이벤트 데이터베이스(21)에 저장되거나, 차량 식별 정보와 함께 VII 데이터베이스(31)에 저장되거나, 혹은 이들 데이터베이스(21, 31) 양쪽에 저장될 수도 있다.

[0038] 이벤트 데이터 관리 시스템(100)은 다수의 차량들로부터 이벤트 리포트 메시지를 수신할 수 있다. 개인의 프라이버시를 보호하기 위해, 이벤트 데이터 관리 시스템(100)은 차량으로부터 수신된 이벤트 리포트 메시지에 대해, 후술하는 바와 같이 비식별화 처리를 수행하여, 제3자가 관련 차량이나 관련된 개인을 식별하거나 추적할

수 있게 하는 차량 식별 정보를 이벤트 데이터로부터 분리한다. 그리고 분리된 차량 식별 정보와 이벤트 데이터를 각각 상이한 데이터베이스로 관리한다.

[0039] 이벤트 데이터 관리 시스템(100)은 이벤트 데이터베이스(21), 이벤트 데이터베이스(21)를 관리하는 이벤트 데이터베이스 서버(22), VII 데이터베이스(31), 및 VII 데이터베이스(31)를 관리하는 VII 데이터베이스 서버(32)를 포함한다. 이벤트 데이터 관리 시스템(100)은 이벤트 데이터베이스 서버(22)와 VII 데이터베이스 서버(32)에 통신 가능하게 연결된 데이터 수집 서버(35)를 더 포함한다. 도 1에는 이벤트 데이터베이스 서버(22)와 VII 데이터베이스 서버(32)가 별개의 서버로 구분되어 있으나, 이들 서버는 주지의 가상화 기술을 통해 컴퓨팅 자원을 공유하는 방식으로 구현될 수도 있다.

[0040] 데이터 수집 서버(35)는, 다수의 차량들로부터 이벤트 리포트 메시지들을 수신한다. 데이터 수집 서버(35)는 차량으로부터 수신된 이벤트 리포트 메시지에 대해 비식별화 처리를 수행하여, 제3자가 관련 차량이나 개인을 식별하거나 추적할 수 없는, 익명화된 이벤트 데이터를 생성할 수 있다. 전술한 바와 같이, 이벤트 리포트 메시지는 이벤트 데이터와 차량 식별 정보를 포함한다.

[0041] 데이터 수집 서버(35)는 이벤트 리포트 메시지에 포함된 정보들을 2개의 데이터 셋으로 분할할 수 있다. 하나의 데이터 셋(제 1 데이터 셋)은 이벤트 데이터가 포함하지만 차량 식별 정보를 포함하지 않으며, 다른 하나의 데이터 셋(제 2 데이터 셋)은 차량 식별 정보를 포함하지만 이벤트 데이터를 포함하지 않는다. 즉, 이벤트 데이터의 관련 차량이나 개인을 식별하거나 추적할 수 있게 하는 VIN 데이터 또는 임의의 다른 고유 데이터가 이벤트 데이터로부터 분리된다.

[0042] 데이터 수집 서버(35)는 이벤트 데이터를 위한 가명 식별자(pseudonymous identifier)를 생성한다. 생성된 가명 식별자는 이벤트 데이터베이스에서 관련 이벤트 데이터를 고유하게 식별시키는데 사용된다. 그러나 차량이나 개인을 식별하게 하는 어떠한 의미 있는 정보도 포함되어 있지 않다. 데이터 수집 서버(35)는 가명 식별자가 추가된 제 1 데이터 셋, 즉 익명화된 이벤트 데이터를 이벤트 데이터베이스 서버(22)에 전달한다.

[0043] 일부 실시예에서, 가명 식별자는 차량 식별 정보(예컨대, VIN 데이터)에 대해 단방향 해시 알고리즘(one-way hash algorithm)을 적용하여 생성될 수 있다. 단방향 해시 알고리즘은 생성된 가명 식별자로부터 차량 식별 정보 혹은 다른 유용한 정보를 추출하는 것을 불가능하게 한다. 바람직하게는, 가명 식별자는 차량 식별 정보와 데이터 수집 서버(35)에 의해 생성된 난수(random number)의 조합에 대해 일방향 해시 알고리즘을 적용하여 생성될 수 있다. 가명 식별자의 생성에 사용된 난수는 데이터 수집 서버(35) 내에 안전하게 관리되거나 관련된 차량 식별 정보와 함께 VII 데이터베이스(31)에 저장될 수 있다. 여기서, 단방향 해시 알고리즘이 일 예로 설명되었으나, 익명 식별자를 생성하는 다른 유형의 암호학적 알고리즘의 사용될 수도 있다.

[0044] 다른 실시예에서, 가명 식별자는 VII 데이터베이스에서 차량 식별 정보를 고유하게 식별시키는데 사용되는 VII 인덱스에 대해 단방향 해시 알고리즘을 적용하여 생성될 수 있다. 이를 위해, 데이터 수집 서버(35)는 차량 식별 정보를 포함하는 제 2 데이터 셋을 이벤트 데이터베이스 서버(22)에 제공하고, 이벤트 데이터베이스 서버(22)로부터 VII 인덱스를 획득할 수도 있다.

[0045] 이벤트 데이터베이스 서버(22)는 데이터 수집 서버(35)로부터 전달되는 익명화된 이벤트 데이터를 이벤트 데이터베이스(21)에 저장할 수 있다. 전술한 바와 같이, 익명화된 이벤트 데이터는 가명 식별자로 식별되는 이벤트 데이터이거나 이를 포함할 수 있다.

[0046] VII 데이터베이스 서버(32)는 데이터 수집 서버(35)로부터 전달되는 차량 식별 정보를 VII 데이터베이스(31)에 저장할 수 있다. 만약 가명 식별자가 차량 식별 정보와 난수의 조합에 대해 일방향 해시 알고리즘을 적용하여 생성되었다면, VII 데이터베이스 서버(32)는 데이터 수집 서버(35)로부터 전달되는 차량 식별 정보와 난수를 VII 데이터베이스(31)에 저장할 수도 있다. 전술한 바와 같이, 가명 식별자들의 생성에 사용된 난수들은 VII 데이터베이스 서버(32)에 제공되지 않을 수도 있다.

[0047] 이와 같이, 개인의 프라이버시는 가명 식별자의 사용으로 보호될 수 있다. 가명 식별자 그 자체는 차량이나 개인을 식별하게 하는 어떠한 의미 있는 정보도 포함하고 있지 않으나, 가명 식별자는 VII 데이터베이스(31)에 저장된 차량 식별 정보에 적어도 부분적으로 기초하여 암호학적으로 (재)생성될 수 있다. 따라서, 개인의 프라이버시 보호를 더욱 강화하기 위해, 가명 식별자를 생성하는 데이터 수집 서버(35)는 이벤트 데이터베이스 서버(22) 혹은 VII 데이터베이스 서버(32)와는 상이한 사업자에 의해 관리되거나, 이들 서버(22, 32, 35)는 서로 상이한 사업자에 의해 관리되는 것이 바람직하다. 또한, 가명 식별자의 생성에 사용되는 암호학적 알고리즘이나 난수는 이들 데이터베이스 서버(22, 32)의 사업자(들)로부터 안전하게 관리되는 것이 바람직하다.

[0048] 이벤트 데이터 관리 시스템(100)은, 제3자(50)의 요청에 응답하여, 특정 차량이나 개인과 식별되지 않는 익명화된 이벤트 데이터를 제공하거나 특정 차량이나 개인이 식별된 이벤트 데이터를 제공할 수 있다. 제3자(50)는 이벤트 데이터를 활용하고자 하는 서비스 이용자, 예컨대, 보험사 혹은 정부기관, 연구자, 차량 제조사, 차량 소유자 등일 수 있다. 제3자(50)는 이벤트 발생 위치, 날짜, 시각, 연루된 차량의 모델, 차량 식별 번호(VIN) 등과 같은 검색 조건을 특정할 수 있다. 이벤트 데이터 관리 시스템(100)은 제3자의 요청에 특화된 이벤트 데이터를 추출하기 위해, 이벤트 데이터베이스 서버(22), 이벤트 데이터베이스 서버(22), 및 데이터 수집 서버(35) 중 적어도 하나를 이용할 수 있다. 이벤트 데이터 관리 시스템(100)이 이벤트 데이터를 제공하는 구체적인 프로세스는 도 3 및 도 4를 참조하여 후술한다.

[0049] 개인의 프라이버시의 추가적인 보호를 위해, VII 데이터베이스 서버(32)는 기 설정된 액세스 권한 정책에 기초하여 VII 데이터베이스(31)에 저장된 데이터에 대한 액세스를 더 제어할 수 있다. 예를 들어, 액세스 권한 정책은 법원 명령, 수색 영장 및/또는 다른 적용 가능한 법률 및 규정에 의해 달리 승인되지 않는 한, 각각의 차량 소유자에 의해 허가된 조사자 혹은 다른 사용자에 의한 액세스만을 허용할 수 있다. 즉, 기 설정된 권한 부여 정책은 VII 데이터베이스(31)의 상이한 사용자들에 대해 상이한 레벨의 액세스를 제공할 수 있다. 유사하게, 데이터 수집 서버(35)는, 이벤트 데이터베이스(21)로부터 특정 차량과 관련된 이벤트 데이터를 검색하는 데 사용될 가명 식별자를 (재)생성하기에 앞서, 요청자가 정당한 권한을 가지는 자인지 여부를 판단할 수 있다.

[0050] 반면, 익명화된 이벤트 데이터베이스(22)를 관리하는 이벤트 데이터베이스 서버(22)는, VII 데이터베이스 서버(32)에 비해 덜 엄격한 액세스 권한 정책을 사용할 수 있다. 예컨대, 이벤트 데이터베이스 서버(22)는 익명화된 이벤트 데이터를 요청하는 제3자에 대해 단지 과금(billing) 시스템에 기반한 액세스 권한 정책을 사용할 수 있다. 그러나 특정한 가명 식별자에 대응하는 이벤트 데이터(즉, 식별된 이벤트 데이터)의 요청을 받는 경우에는, 이벤트 데이터베이스 서버(22)는 요청자가 정당한 권한을 가지는 자인지 여부를 판단하여야 할 것이다.

[0051] 또한, 데이터베이스 서버(22, 32)에 방화벽(firewall)이 사용되거나 데이터베이스(21, 31)에 데이터베이스 암호화 기법들이 적용될 수도 있으며, 특히, VII 데이터의 안전한 관리를 위해, VII 데이터베이스 서버(32) 및/또는 VII 데이터베이스(31)에는 보다 강화된 보안 기술들이 적용되는 것이 바람직하다.

[0053] 도 2는 도 1에 도시된 시스템의 이벤트 데이터 수집 프로세스를 예시하기 위한 흐름도이다.

[0054] 먼저, 차량의 통신 디바이스(13)는 이벤트 데이터 레코더(11)를 포함하는 하나 이상의 모듈, ECU, 컴포넌트, 프로그램 등으로부터 이벤트 관련 데이터를 획득한다(S200). 예컨대, 통신 디바이스(13)는 이벤트 데이터 레코더(11)로부터 이벤트 전후에 기록된 이벤트 데이터를 수신하고, 이벤트가 발생한 지리적 위치, 날짜, 시각, 차량 모델, VIN 등을 수집할 수 있다.

[0055] 통신 디바이스(13)는 이벤트 데이터와 차량 식별 정보를 포함하는 이벤트 리포트 메시지를 네트워크 상의 데이터 수집 서버(35)에 무선 전송한다(S210). 전술한 바와 같이, 이벤트 리포트 메시지는 이벤트가 발생한 지리적 위치, 날짜, 시각, 차량 모델, 제조 년도, 제조사 등의 부가 정보를 더 포함할 수도 있다. 또한, 차량 식별 정보는 차량을 고유하게 식별할 수 있는 정보로서, 예컨대, 차량 내 ECU들로부터 수집될 수 있는 차량 식별 번호(vehicle identification number: VIN), 통신 디바이스(13)가 통신에 사용하는 고유 식별자 등을 포함할 수 있다.

[0056] 데이터 수집 서버(35)는, 차량으로부터 수신된 이벤트 리포트 메시지에 대해 비식별화 처리를 수행하여, 제3자가 관련 차량이나 개인을 식별하거나 추적할 수 없는, 익명화된 이벤트 데이터를 생성한다(220). 전술한 바와 같이, 이벤트 리포트 메시지는 이벤트 데이터와 차량 식별 정보를 포함한다. 데이터 수집 서버(35)는 이벤트 리포트 메시지에 포함된 정보들을 2개의 데이터 셋으로 분할할 수 있다. 하나의 데이터 셋(제 1 데이터 셋)은 이벤트 데이터가 포함하지만 차량 식별 정보를 포함하지 않으며, 다른 하나의 데이터 셋(제 2 데이터 셋)은 차량 식별 정보를 포함하지만 이벤트 데이터를 포함하지 않는다. 데이터 수집 서버(35)는 이벤트 데이터를 위한 가명 식별자(pseudonymous identifier)를 생성한다.

[0057] 데이터 수집 서버(35)는 가명 식별자가 추가된 제 1 데이터 셋, 즉 익명화된 이벤트 데이터를 이벤트 데이터베이스 서버(22)에 전달한다. 이벤트 데이터베이스 서버(22)는 데이터 수집 서버(35)로부터 전달되는 익명화된 이벤트 데이터를 이벤트 데이터베이스(21)에 저장할 수 있다. 전술한 바와 같이, 익명화된 이벤트 데이터는 가명 식별자로 식별되는 이벤트 데이터이거나 이를 포함할 수 있다.

[0058] 데이터 수집 서버(35)는 차량 식별 정보를 포함하는 제 2 데이터 셋을 VII 데이터베이스 서버(32)에 제공한다. VII 데이터베이스 서버(32)는 데이터 수집 서버(35)로부터 전달되는 차량 식별 정보를 VII 데이터베이스(31)에 저장할 수 있다. 만약 가명 식별자가 차량 식별 정보와 난수의 조합에 대해 일방향 해시 알고리즘을 적용하여 생성되었다면, VII 데이터베이스 서버(32)는 데이터 수집 서버(35)로부터 전달되는 차량 식별 정보와 난수를 VII 데이터베이스(31)에 저장할 수도 있다. 전술한 바와 같이, 가명 식별자들의 생성에 사용된 난수들은 VII 데이터베이스 서버(32)에 제공되지 않을 수도 있다.

[0060] 도 3은 도 1에 예시된 이벤트 데이터 관리 시스템(100)이 익명화된 이벤트 데이터를 제공하는 프로세스를 예시한 흐름도이다.

[0061] 이벤트 데이터 관리 시스템(100)은, 예컨대, 정부기관의 조사관 혹은 연구자들로부터 특정 지역에서 일정 기간 동안 발생한 이벤트들과 같이 특정 조건을 만족하는 익명화된 이벤트 데이터를 요청받을 수 있다(S310). 이벤트 데이터 관리 시스템(100)은 단계 S510 이전 또는 이후에 요청자가 액세스 권한을 가진 자인지 여부를 판단할 수도 있다. 이벤트 데이터 관리 시스템(100)은 이벤트 데이터베이스 서버(22)로 하여금 이벤트 데이터베이스(21)를 조회하여 관련된 이벤트 데이터들을 추출하도록 할 수 있다(S320). 본 예시에서, 이벤트 데이터를 추출하는 데에는 VII 데이터베이스(31)가 관여되지 않는다. 이벤트 데이터 관리 시스템(100)은 추출된 이벤트 데이터를 요청에 대한 응답으로서 제공할 수 있다(S330). 위와 같이, 단지 이벤트 데이터베이스(21)에 의존하여 추출된 이벤트 데이터들은 차량이나 개인과의 연관 관계가 제거된 상태인 바, 추출된 이벤트 데이터들의 제공은 관련된 차량 소유자의 프라이버시를 손상시키지 않는다.

[0063] 도 4는 도 1에 예시된 이벤트 데이터 관리 시스템(100)이 특정한 차량과 관련된 이벤트 데이터를 제공하는 프로세스를 예시한 흐름도이다.

[0064] 이벤트 데이터 관리 시스템(100)은, 예컨대, 차량 소유자, 보험사 혹은 수사기관의 조사관으로부터 특정한 차량 식별 번호(VIN)와 관련된 이벤트 데이터를 요청 받을 수 있다(S410).

[0065] 이벤트 데이터 관리 시스템(100)은 요청자가 법원 명령, 수색 영장 및/또는 다른 적용 가능한 법률 및 규정에 의해 혹은 관련 차량 소유자에 의해 액세스 권한을 가진 자인지 여부를 먼저 판단할 수 있다(S420).

[0066] VII 데이터베이스 서버(32)는 VII 데이터베이스(31)를 조회하여 차량 식별 번호(VIN)에 대응되는 차량 식별 정보와 난수를 추출한다(S430). 데이터 수집 서버(35)는 추출된 차량 식별 정보와 난수에 적어도 부분적으로 기초하여 차량 식별 번호(VIN)에 대응하는 가명 식별자를 생성한다(S440). 이벤트 데이터베이스 서버(22)는 이벤트 데이터베이스(21)를 조회하여, 생성된 가명 식별자에 대응되는 이벤트 데이터를 추출한다(S450). 이벤트 데이터 관리 시스템(100)은 추출된 이벤트 데이터를 요청에 대한 응답으로서 제공한다(S460).

[0067] 데이터 수집 서버(35)와 이벤트 데이터베이스(21)를 운용하는 사업자가 서로 상이한 경우에, 단계 S440에서 생성된 가명 식별자는, 이벤트 데이터베이스(21)의 조회에 사용될 수 있도록, 전술한 조사관들에 제공되거나 혹은 이벤트 데이터베이스(21)를 운용하는 사업자에게 곧바로 제공될 수도 있다.

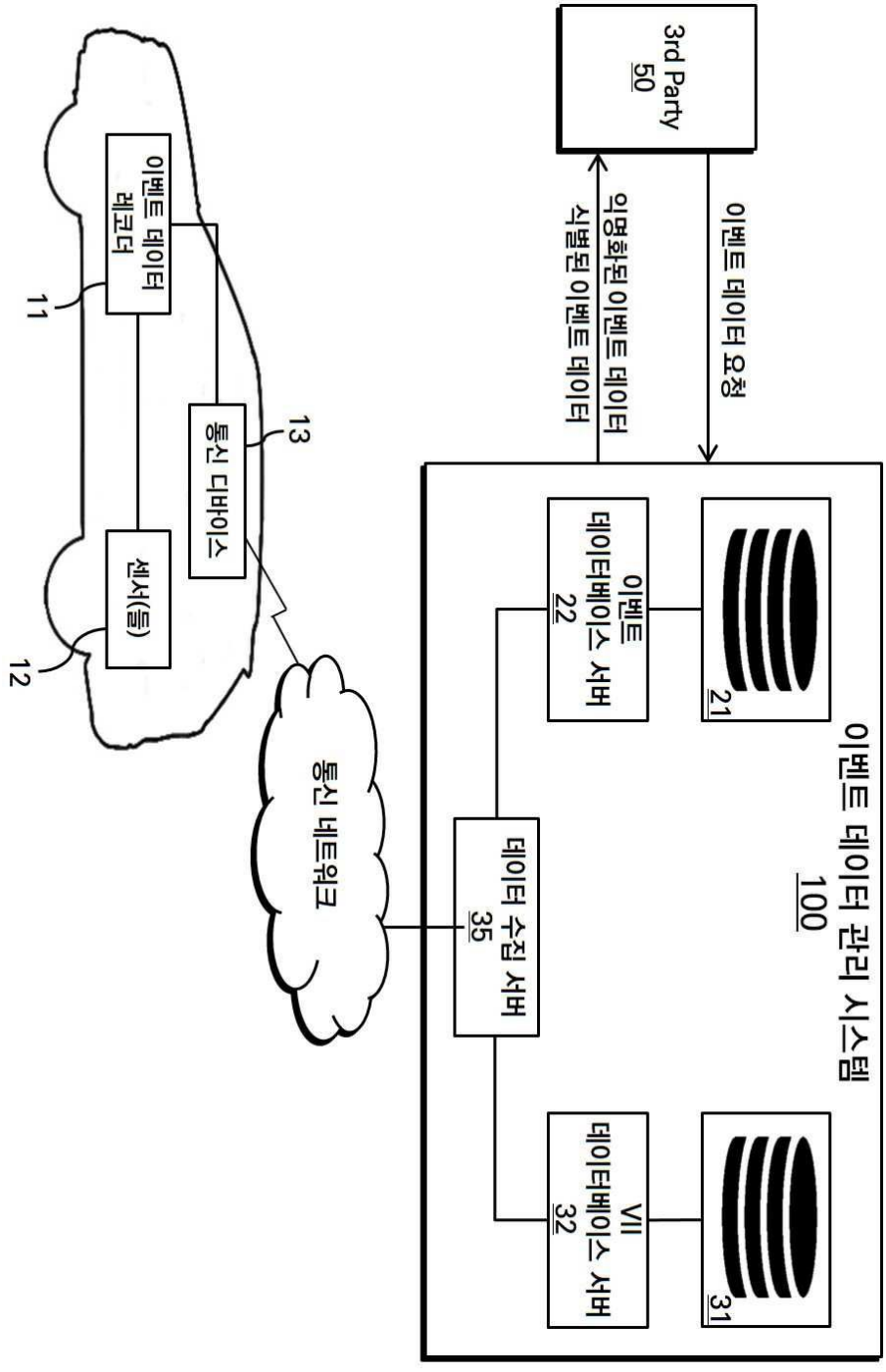
[0069] 전술한 예시적인 실시예는 많은 다른 방식으로 구현될 수 있다는 것을 이해해야 한다. 일부 예들에서, 본 개시에서 설명된 다양한 방법들, 장치들, 서버들, (서브) 시스템들은 프로세서, 메모리, 디스크 또는 다른 대용량 스토리지, 통신 인터페이스, 입/출력(I/O) 디바이스들 및 기타 주변 장치들을 가지는 적어도 하나의 범용 컴퓨터에 의해 구현될 수도 있다. 범용 컴퓨터는 소프트웨어 명령어들을 프로세서에 로딩한 다음, 본 개시에 설명된 기능을 수행하기 위해 명령들의 실행함으로써 상술한 방법을 실행하는 장치로 기능할 수 있다.

[0070] 한편, 본 개시에서 설명된 다양한 방법들은 하나 이상의 프로세서에 의해 판독되고 실행될 수 있는 비일시적 기록매체에 저장된 명령어들로 구현될 수도 있다. 비일시적 기록매체는, 예를 들어, 컴퓨터 시스템에 의하여 판독 가능한 형태로 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 예를 들어, 비일시적 기록매체는 EPROM(erasable programmable read only memory), EEPROM(Electrically Erasable Programmable Read-Only Memory), 플래시 드라이브, 광학 드라이브, 자기 하드 드라이브, 솔리드 스테이트 드라이브(SSD)와 같은 저장매체를 포함한다.

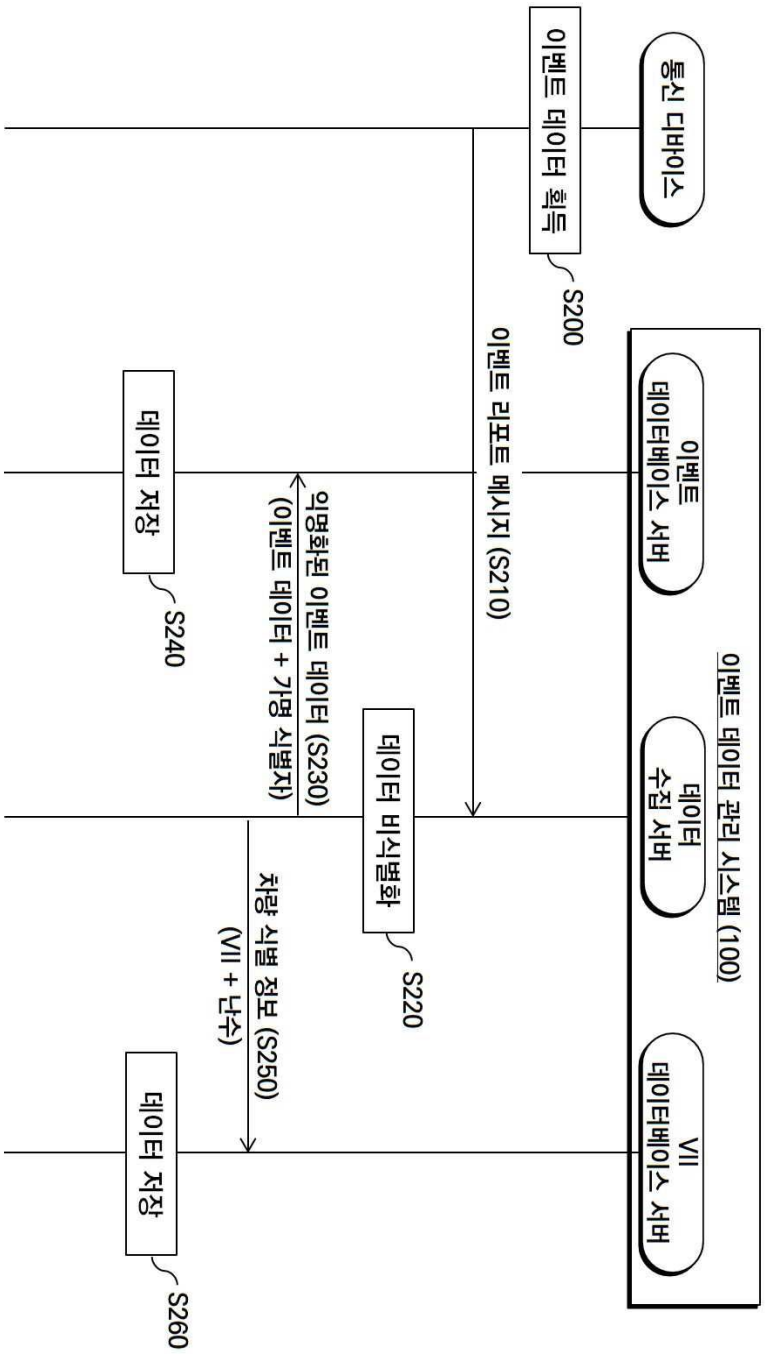
[0071] 이상의 설명은 본 실시예의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 실시예들은 본 실시예의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 실시예의 기술 사상의 범위가 한정되는 것은 아니다. 본 실시예의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 실시예의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

도면

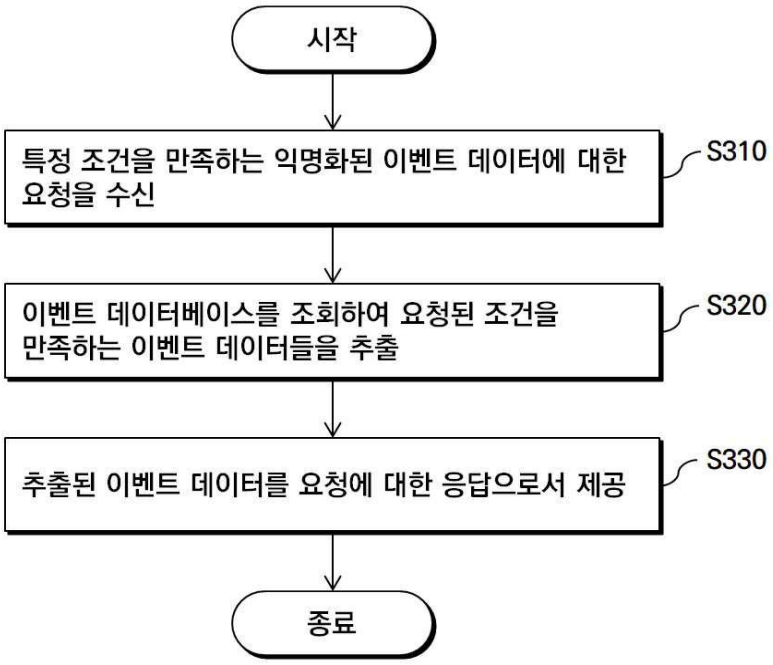
도면1



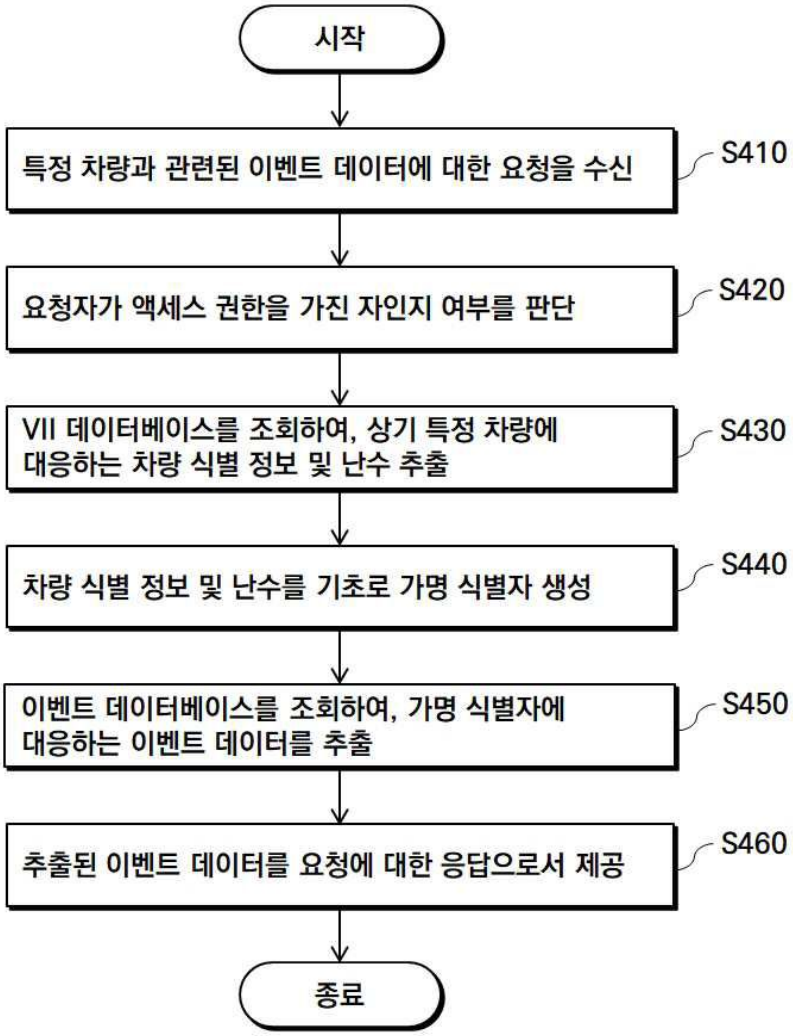
도면2


통신 디바이스
이벤트 데이터 획득
S200
이벤트 리포트 메시지 (S210)
이벤트 데이터 관리 시스템 (100)
이벤트 데이터베이스 서버
데이터 수집 서버
VII 데이터베이스 서버
데이터 저장
S240
익명화된 이벤트 데이터 (S230)
(이벤트 데이터 + 가명 식별자)
데이터 비식별화
S220
차량 식별 정보 (S250)
(VII + 난수)
데이터 저장
S260

도면3


시작
특정 조건을 만족하는 익명화된 이벤트 데이터에 대한 요청을 수신
S310
이벤트 데이터베이스를 조회하여 요청된 조건을 만족하는 이벤트 데이터들을 추출
S320
추출된 이벤트 데이터를 요청에 대한 응답으로서 제공
S330
종료

도면4


시작
특정 차량과 관련된 이벤트 데이터에 대한 요청을 수신
S410
요청자가 액세스 권한을 가진 자인지 여부를 판단
S420
VII 데이터베이스를 조회하여, 상기 특정 차량에 대응하는 차량 식별 정보 및 난수 추출
S430
차량 식별 정보 및 난수를 기초로 가명 식별자 생성
S440
이벤트 데이터베이스를 조회하여, 가명 식별자에 대응하는 이벤트 데이터를 추출
S450
추출된 이벤트 데이터를 요청에 대한 응답으로서 제공
S460
종료