



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2016년01월15일

(11) 등록번호 10-1585985

(24) 등록일자 2016년01월11일

(51) 국제특허분류(Int. Cl.)

H04L 9/32 (2006.01)

(52) CPC특허분류

H04L 9/3228 (2013.01)

(21) 출원번호 10-2015-0008460

(22) 출원일자 2015년01월19일

심사청구일자 2015년01월19일

(56) 선행기술조사문헌

KR1020120139844 A

KR1020140135244 A

JP2002268950 A

JP2005234866 A

(73) 특허권자

경희대학교 산학협력단

경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)

(72) 발명자

진창호

경기도 성남시 분당구 수내로192번길 25, 402동 1505호(수내동)

(74) 대리인

김홍석, 이강녕, 김등용

전체 청구항 수 : 총 15 항

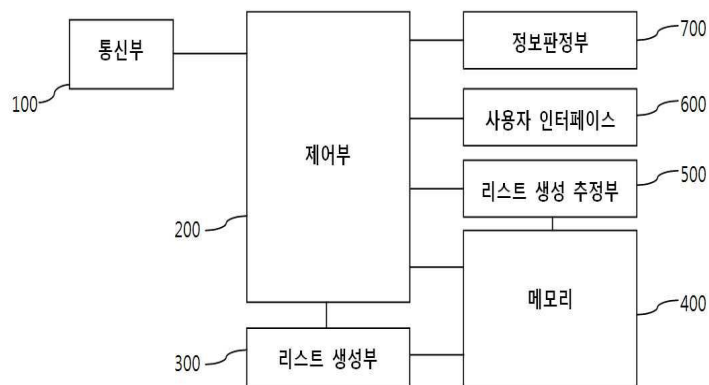
심사관 : 양종필

(54) 발명의 명칭 개인정보 비식별화 전송장치 및 전송방법

(57) 요약

본 발명의 실시예에 따른 개인정보 비식별화 전송장치는 외부 단말들과 네트워크로 연결되어 통신을 수행하는 통신부, 장치의 비식별화를 위한 아이디를 생성하고, 전송주기, 리스트 수집구간 또는 노출구간을 설정하는 제어부, 상기 통신부를 통해 상기 외부 단말의 노출용 아이디 리스트를 수신하여, 보관용 아이디 리스트, 수집구간 아이디 리스트, 노출용 아이디 리스트 및 전송용 아이디 리스트를 생성하는 리스트 생성부 및 상기 리스트 생성부로부터 생성된 보관용 아이디 리스트, 수집구간 아이디 리스트, 노출용 아이디 리스트 및 전송용 아이디 리스트를 저장하는 메모리를 포함한다.

대표도 - 도2



명세서

청구범위

청구항 1

개인정보 비식별화 전송장치에 있어서,

외부 단말들과 네트워크로 연결되어 통신을 수행하는 통신부;

상기 개인정보 비식별화 전송장치의 비식별화를 위한 아이디를 생성하고, 전송용 아이디 리스트의 전송주기, 외부 단말의 노출용 아이디 리스트를 수신하는 구간인 리스트 수집구간 또는 상기 개인정보 비식별화 전송장치의 노출용 아이디 리스트를 외부 단말로 노출시키는 노출구간을 설정하는 제어부;

상기 통신부를 통해 상기 외부 단말의 노출용 아이디 리스트를 수신하여, 보관용 아이디 리스트, 수집구간 아이디 리스트, 노출용 아이디 리스트 및 전송용 아이디 리스트를 생성하는 리스트 생성부; 및

상기 리스트 생성부로부터 생성된 보관용 아이디 리스트, 수집구간 아이디 리스트, 노출용 아이디 리스트 및 전송용 아이디 리스트를 저장하는 메모리를 포함하는 것을 특징으로 하는 개인정보 비식별화 전송장치.

청구항 2

제1항에 있어서,

상기 수집구간 아이디 리스트 생성시점과 생성위치를 추정하는 리스트 생성 추정부; 및

사용자 인터페이스를 더 포함하는 것을 특징으로 하는 개인정보 비식별화 전송장치.

청구항 3

제2항에 있어서,

상기 사용자 인터페이스를 통해 입력되는 사용자의 제1정보와 서버로부터 전송되는 제2정보가 일치하는지를 판정하는 정보 판정부를 더 포함하는 것을 특징으로 하는 개인정보 비식별화 전송장치.

청구항 4

제1항에 있어서,

상기 통신부는 Wi-Fi Direct, 와이파이(Wi-Fi) 또는 비콘(Beacon)통신을 위한 모듈을 포함하는 것을 특징으로 하는 개인정보 비식별화 전송장치.

청구항 5

제1항에 있어서,

상기 제어부는 상기 전송주기를 결정하고, 외부 단말의 노출용 아이디 리스트를 수신하는 리스트 수집구간을 결정하며, 상기 개인정보 비식별화 전송장치의 노출용 아이디 리스트를 노출시키는 노출구간을 결정하는 시스템 설정모듈;

상기 개인정보 비식별화 전송장치의 비식별화를 위한 아이디를 생성하는 아이디 생성모듈; 및

전송용 아이디 리스트를 서버로 전송할지 결정하는 전송결정모듈을 포함하는 것을 특징으로 하는 개인정보 비식별화 전송장치.

청구항 6

제5항에 있어서,

상기 시스템 설정모듈은 상기 리스트 수집구간과 상기 노출구간을 상기 전송주기 내 단수 또는 복수 구간이 할당하며, 상기 리스트 수집구간과 상기 노출구간의 시점과 종점은 전송주기 내에서 임의로 설정되거나 또는 수집

구간의 시작시점은 노출구간의 시작시점으로부터 정해진 시간 이전으로 설정되며, 상기 전송주기는 외부 단말과 동일한 것을 특징으로 하는 개인정보 비식별화 전송장치.

청구항 7

제5항에 있어서,

상기 아이디 생성모듈은 문자나 숫자나 기호의 임의 조합에 의한 아이디를 생성하는 것을 특징으로 하는 개인정보 비식별화 전송장치.

청구항 8

제5항에 있어서,

상기 전송결정모듈은 전송용 아이디 리스트에 생성위치정보가 포함되어 있는 경우에는 외부 단말로 수집구간 아이디 리스트와 생성위치정보를 포함하는 전송용 아이디 리스트를 노출시키도록 제어하는 것을 특징으로 하는 개별정보 비식별화 전송장치.

청구항 9

제1항에 있어서,

상기 리스트 생성부는 상기 통신부가 수신하는 외부 단말들의 노출용 아이디 리스트를 수신하여 보관용 아이디 리스트를 생성하는 보관용 아이디 리스트 생성모듈;

상기 메모리에 저장된 보관용 아이디 리스트에서 아이디 리스트 순서를 재배열하거나 추출하여 노출구간에 외부 단말로 노출시키기 위한 노출용 아이디 리스트를 생성하는 노출용 아이디 리스트 생성모듈;

상기 리스트 수집구간에 외부 단말로부터 수신한 외부단말의 노출용 감염자 리스트를 저장 또는 갱신하여 수집구간 아이디 리스트를 생성하고, 수집구간 아이디 리스트의 생성시점과 위치정보를 추정하는 수집구간 아이디 리스트 생성 추정부; 및

상기 전송주기 종료시점에 서버로 전송할 전송용 아이디 리스트를 생성하는 전송용 아이디 리스트 생성모듈을 포함하는 것을 특징으로 하는 개인정보 비식별화 전송장치.

청구항 10

개인정보 비식별화 전송장치로 구현되는 전송방법으로서,

- (a) 상기 개인정보 비식별화 전송장치의 아이디를 생성하는 단계;
- (b) 외부 단말로부터 노출용 아이디 리스트를 수신하여 수집구간 아이디 리스트를 생성하는 단계;
- (c) 상기 수집구간 아이디 리스트를 이용하여 보관용 아이디 리스트를 업데이트하는 단계;
- (d) 상기 보관용 아이디 리스트에 포함된 아이디 리스트 순서를 재배열하거나 추출하여 노출용 아이디 리스트를 생성하는 단계; 및
- (e) 상기 노출용 아이디 리스트를 외부 단말에 노출시키는 단계를 포함하는 것을 특징으로 하는 개인정보 비식별화 전송방법.

청구항 11

제10항에 있어서,

상기 (a)단계 이후에 상기 노출용 아이디 리스트의 노출구간을 결정하는 단계를 더 포함하는 것을 특징으로 하는 개인정보 비식별화 전송방법.

청구항 12

제10항에 있어서,

상기 (c)단계는 상기 외부 단말로부터 수신된 노출용 아이디 리스트를 상기 개인정보 비식별화 전송장치의 수집구간 아이디 리스트와 비교하여 중복 아이디가 포함되어 있는지를 판정하고, 중복 아이디를 제거하는 단계를 포

합하는 것을 특징으로 하는 개인정보 비식별화 전송방법.

청구항 13

제10항에 있어서,

상기 (e)단계 이후, 전송용 아이디 리스트의 전송주기 종료시점에 서버로 전송할 전송용 아이디 리스트를 생성하는 단계를 더 포함하는 것을 특징으로 하는 개인정보 비식별화 전송방법.

청구항 14

제13항에 있어서,

상기 전송용 아이디 리스트를 생성하는 단계 이후, 상기 개인정보 비식별화 전송장치의 전송주기 종료시점에 상기 전송용 아이디 리스트를 서버로 전송하는 단계를 더 포함하는 것을 특징으로 하는 개인정보 비식별화 전송방법.

청구항 15

제14항에 있어서,

상기 전송용 아이디 리스트를 서버로 전송하는 단계는 상기 수집구간 아이디 리스트와 생성위치정보를 포함하는 전송용 아이디 리스트를 전송하는 경우에는 상기 수집구간 아이디 리스트와 생성위치정보를 포함하는 상기 전송용 아이디 리스트를 외부 단말로 노출시킨 이후, 외부 단말이 서버로 전송하는 단계를 포함하는 것을 특징으로 하는 개인정보 비식별화 전송방법.

발명의 설명

기술 분야

[0001]

본 발명은 개인정보 비식별화 전송장치 및 전송방법에 관한 발명으로서, 보다 상세하게는 개인정보보호법에 저촉되지 않고 개인활동내역 및 개인정보를 외부장치로 전송하는 전송장치 및 전송방법에 관한 발명이다.

배경 기술

[0002]

현대 사회에서는, 특정의 개인에 관한 정보가 수많은 단체로부터 얻을 수 있다. 병원, 연구소, 은행, 보험 회사 및 소매업자 등의 건강, 금융 및 영리 단체는 연구 및 개발, 마케팅 및 다른 상업 목적을 위해서 이용 가능한 데이터를 소유하고 있다. 그러나, 이러한 데이터에 관계하는 개인의 프라이버시 보호가 필요하다라는 의식이 높아지고 있다. 특히, 개인의 건강 또는 재정상태에 관한 정보는 극히 기밀성이 높다고 말할 수 있다.

[0003]

개인정보를 수많은 공인된 단체에서 저장하고 있다고 하더라도 이를 사용하는 것은 국가기관의 승인이 필요하다거나 지극히 제한적으로 가능하다. 그러나 컴퓨터 기술의 발달로 인하여 저장되어 있는 개인정보는 해킹 등과 같은 범죄행위를 통해서 공연히 유출되고 있으며, 또 다른 범죄행위에 악용되고 있다.

[0004]

최근 빅데이터와 관련된 기술의 등장으로 이와 같은 정보를 분석할 필요성이 커지고 있다. 데이터의 분석을 위해서는 많은 경우 복수의 소스로부터 데이터에 액세스 할 필요가 있다. 예를 들면, 특정의 약물 요법의 효능을 관정하는 연구에는 약물 요법을 처방하는 개인의 그룹이나 약물을 처방하는 약국의 해당하는 그룹의 레코드에 액세스 할 필요가 있다. 그러나 넘쳐나는 정보의 홍수에도 불구하고 이를 분석하여 유용한 결과를 도출하기 위해서는 개인정보보호의 패러다임과 절충이 필요한 실정이다.

[0005]

특히 질병의 감염과 관련된 정보는 지극히 개인적인 정보에 해당할 뿐만 아니라, 개인정보보호에 관한 법률의 제정을 통해 비밀유지의무를 갖는 자를 제외하고 이를 유통시키거나 전파하는 것은 절대적으로 금지되어 있다. 이에 반해 질병의 감염을 예측하고 경보를 발하는 시스템의 도입은 공익을 위해서 절대적으로 필요한 실정이다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 목적은 개인정보를 보호하면서 사람간에 전파 가능한 사회유행이나 소문 또는 질병 등 사회 현상의 동화나 동조나 전파 또는 감염된 개체수나 지역 내지는 경로를 예측하기 위한 개인정보 비식별화 장치 및 그 방법을 제공하는데 있다.

[0007] 또한 본 발명의 목적은 개인정보를 수집하거나 저장하지 않고, 활용이 가능하여 관리자의 실수나 범죄행위로 인한 개인정보 노출위험이 전혀 없는 개인정보 비식별화 장치 및 그 방법을 제공하는데 있다.

과제의 해결 수단

[0008] 본 발명의 실시예에 따른 개인정보 비식별화 전송장치는 외부 단말들과 네트워크로 연결되어 통신을 수행하는 통신부, 장치의 비식별화를 위한 아이디를 생성하고, 전송주기, 리스트 수집구간 또는 노출구간을 설정하는 제어부, 상기 통신부를 통해 상기 외부 단말의 노출용 아이디 리스트를 수신하여, 보관용 아이디 리스트, 수집구간 아이디 리스트, 노출용 아이디 리스트 및 전송용 아이디 리스트를 생성하는 리스트 생성부 및 상기 리스트 생성부로부터 생성된 보관용 아이디 리스트, 수집구간 아이디 리스트, 노출용 아이디 리스트 및 전송용 아이디 리스트를 저장하는 메모리를 포함한다.

[0009] 본 발명의 실시예에 따른 개인정보 비식별화 전송장치는 상기 수집구간 아이디 리스트 생성시점과 생성위치를 추정하는 리스트 생성 추정부 및 사용자 인터페이스를 더 포함할 수 있다.

[0010] 또한, 상기 사용자 인터페이스를 통해 입력되는 사용자의 제1정보와 서버로부터 전송되는 제2정보가 일치하는지를 판정하는 정보 판정부를 더 포함할 수 있다.

[0011] 여기서, 상기 통신부는 Wi-Fi Direct, 와이파이(wifi) 또는 비콘(Beacon)통신을 위한 모듈을 포함할 수 있다.

[0012] 여기서, 상기 제어부는 상기 전송주기를 결정하고, 외부 단말로부터 아이디 리스트를 수신하는 리스트 수집구간을 결정하며, 상기 노출용 아이디 리스트를 노출시키는 노출구간을 결정하는 시스템 설정모듈, 장치의 비식별화를 위한 아이디를 생성하는 아이디 생성모듈 및 전송용 아이디 리스트를 서버로 전송할지 결정하는 전송결정모듈을 포함할 수 있다.

[0013] 여기서, 상기 시스템 설정모듈은 상기 리스트 수집구간과 상기 노출구간을 상기 전송주기 내 단수 또는 복수 구간이 할당하며, 상기 리스트 수집구간과 상기 노출구간의 시점과 종점은 전송주기 내에서 임의로 설정되거나 또는 수집구간의 시작시점은 노출구간의 시작시점으로부터 정해진 시간 이전으로 설정되며, 상기 전송주기는 외부 단말과 동일하다.

[0014] 여기서, 상기 아이디 생성모듈은 문자나 숫자나 기호의 임의 조합에 의해 아이디를 생성한다.

[0015] 여기서, 상기 전송결정모듈은 전송용 아이디 리스트에 생성위치정보가 포함되어 있는 경우에는 다른 단말로 수집구간 아이디 리스트와 생성위치정보를 포함하는 전송용 아이디 리스트를 노출시키도록 제어한다.

[0016] 또한, 상기 리스트 생성부는 상기 통신부가 수신하는 외부 단말들의 노출용 아이디 리스트를 수신하여 보관용 아이디 리스트를 생성하는 보관용 아이디 리스트 생성모듈, 상기 메모리에 저장된 보관용 아이디 리스트에서 아이디 리스트 순서를 재배열하거나 추출하여 노출구간에 외부 단말로 노출시키기 위한 노출용 아이디 리스트를 생성하는 노출용 아이디 리스트 생성모듈, 상기 리스트 수집구간에 외부 단말로부터 수신한 외부단말의 노출용 아이디 리스트를 저장 또는 갱신하여 수집구간 아이디 리스트를 생성하고, 수집구간 아이디 리스트의 생성시점과 위치정보를 생성하는 수집구간 아이디 리스트 생성모듈 및 상기 전송주기 종료시점에 서버로 전송할 전송용 아이디 리스트를 생성하는 전송용 아이디 리스트 생성모듈을 포함할 수 있다.

[0017] 본 발명의 또 다른 양태에 따른 개인정보 비식별화 전송방법은 개인정보 비식별화 전송장치로 구현되는 전송방법으로서, (a) 장치의 아이디를 생성하는 단계, (b) 외부 단말로부터 노출용 아이디 리스트를 수신하여 수집구간 아이디 리스트를 생성하는 단계, (c) 상기 수집구간 아이디 리스트를 이용하여 보관용 아이디 리스트를 업데이트하는 단계, (d) 상기 보관용 아이디 리스트에 포함된 아이디 리스트 순서를 재배열하거나 추출하여 노출용 아이디 리스트를 생성하는 단계 및 (e) 상기 노출용 아이디 리스트를 외부 단말에 노출시키는 단계를 포함한다.

[0018] 여기서, 상기 (a)단계 이후에 상기 노출용 아이디 리스트의 노출구간을 결정하는 단계를 더 포함할 수 있다.

[0019] 또한, 상기 (c)단계는 상기 외부 단말로부터 수신된 아이디 리스트에 중복 아이디가 포함되어 있는지를 판정하고, 중복 아이디를 제거하는 단계를 포함할 수 있다.

[0020] 또한, 상기 (e)단계 이후, 상기 전송주기의 종료시점에 서버로 전송할 전송용 아이디 리스트를 생성하는 단계를

더 포함할 수 있다.

[0021] 여기서, 상기 전송용 아이디 리스트를 생성하는 단계 이후, 상기 장치의 전송주기 종료시점에 상기 전송용 아이디 리스트를 서버로 전송하는 단계를 더 포함할 수 있다.

[0022] 여기서, 상기 전송용 아이디 리스트를 서버로 전송하는 단계는 상기 수집구간 아이디 리스트와 생성위치정보를 포함하는 전송용 아이디 리스트를 전송하는 경우에 상기 수집구간 아이디 리스트와 생성위치정보를 포함하는 상기 전송용 아이디 리스트를 다른 단말로 노출시킨 이후, 다른 단말이 서버로 전송하는 단계를 포함할 수 있다.

발명의 효과

[0023] 본 발명의 실시예에 따른 개인정보 비식별화 장치 및 방법에 의하면 개인정보를 보호하면서, 사회유행이나 소문 또는 질병 등 사회 현상의 동화, 동조, 전파, 감염 여부, 위치와 관련된 개인정보를 다름에도 불구하고 노출의 위험이 없으며, 사회 현상의 동화나 동조나 전파 또는 감염된 개체수, 지역 및 경로에 대한 보다 정확한 정보를 얻을 수 있다.

도면의 간단한 설명

[0024] 도1은 본 발명의 실시예에 따른 전송장치의 활용 개념도이다.

도2는 본 발명의 실시예에 따른 전송장치의 블록도이다.

도3은 본 발명의 실시예에 따른 제어부의 상세블록도이다.

도4는 전송주기내의 수집구간, 노출구간을 설명하기 위한 다이어그램이다.

도5는 실제 장치에서 노출된 노출용 아이디 리스트를 도시한 그림이다.

도6은 본 발명의 실시예에 따른 리스트 생성부의 블록도이다.

도7은 본 발명이 실시예에 따른 전송장치의 동작흐름도이다.

도8은 본 발명의 실시예에 따른 개인정보 비식별화 전송방법의 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0025] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0026] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0027] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0028] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0029] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구

성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0030] 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 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0031] 이하 첨부된 도면을 참고하여 본 발명의 실시예에 따른 개인정보 비식별화 전송장치에 대해서 상세히 설명한다.

[0032] 도1은 본 발명의 실시예에 따른 전송장치의 활용 개념도이다.

[0033] 일반적으로 개인정보가 포함되어 있는 정보를 활용하기 위해서 각 개인이 소지하고 있거나 관리영역내에 있는 단말에 개인정보를 저장시킨다. 단말에 저장되어 있는 개인정보는 다수의 단말이 접속가능한 서버로 전송되고, 서버는 다량의 개인정보를 저장하여 공적인 결과데이터를 생성하기 위해서 개인정보를 분석한다. 그러나 이와 같은 방법은 앞서 언급한 바와 같이 식별가능한 개인정보를 활용하기 때문에 접근이 제한된 서버에 저장되어 있다고 하더라도 개인정보의 유출위험은 항상 내포하고 있다. 단말기에 저장된 개인정보를 암호화하더라도 그 암호화의 체계를 이해하면, 암호화된 개인 정보를 다시 해독하여 해당 개인을 식별할 수 있는 가능성이 있다. 또한 단말기에 저장된 개인정보를 비식별화하더라도 비식별화 과정이 해당 단말기 외부에서 진행된다면 일단은 식별 가능한 개인정보가 외부로 전송되어야 함으로 외부 장치에 의해 비식별화 전에 식별된 개인정보가 기록에 남을 수 있다.

[0034] 이에 도1과 같은 개념의 시스템을 통해서 다량의 개인정보를 저장하지 않고, 식별된 개인정보가 아닌 비식별된 개인정보로 데이터를 가공하여 서버로 전송함으로써 서버로 하여금 개인정보를 저장하거나 유출하지 않고도 분석이 가능하도록 한다.

[0035] 도1을 통해 본 발명의 실시예에 따른 전송장치의 활용 개념을 상세히 설명하면, 제1단말과 제2단말은 서로 유무선통신을 통해서 데이터를 주고 받을 수 있으며, 제1단말 및 제2단말은 제3단말, 제4단말 ... 등과도 상호 연결되어 데이터를 주고 받을 수 있다. 제2단말과 제4단말이 특정 이벤트에 대한 정보를 포함하고 있다고 가정하고, 특정 이벤트를 독감감염이라 설정한다. 독감감염정보는 각 단말의 사용자가 현재 독감에 감염되어 있는지에 대한 정보를 의미한다. 도1에 도시된 서버는 독감의 감염정보, 확산경로, 감염자수 등을 수집하고 예측하기 위한 장치로 설정하고, 각 단말에 저장되어 있는 독감감염정보와 단말의 위치정보를 바로 서버에 전송하게 되면, 특정 단말의 사용자가 독감에 감염되었다는 정보가 서버로 유출되는 결과를 초래하게 되고, 사용자의 위치정보가 서버로 노출된다. 그러나 이러한 독감감염정보나 위치정보는 지극히 개인적인 정보에 해당하여 전송이나 수집이 엄격히 금지되어 있으며, 노출시에 다양한 형태로 범죄에 악용될 우려가 있다.

[0036] 본 발명의 실시예에 따른 전송장치는 도1에서 도시된 각 단말을 의미한다. 제2단말과 제4단말은 특정 이벤트에 대한 정보인 독감감염정보를 포함하고 있다. 제1단말 내지 제4단말은 고유식별번호가 아닌 비식별 아이디를 생성한다. 비식별 아이디는 문자나 기호나 숫자의 임의 조합일 수 있다. 도1과 같이 제1단말이 단말의 고유식별정보를 제공하지 않고 제2단말로부터 정보를 획득할 수 있는 통신반경 내에 제2단말이 놓여져 있고, 제2단말이 단말의 고유식별정보를 제공하지 않고 다른 단말에게 정보를 노출할 수 있는 통신반경 내에 제1단말이 놓여져 있고, 제2단말이 노출한 제2단말의 비식별 아이디를 제1단말이 수신한다. 마찬가지로 제4단말의 비식별 아이디를 제3단말이 수신한다. 독감감염정보를 포함하고 있지 않는 제3단말은 제3단말의 비식별 아이디는 노출하지 않고 제4단말로부터 수신한 제4단말의 비식별 아이디만 노출하여 다시 제1단말이 수신한다.

[0037] 제1단말에는 독감감염정보를 최초로 포함하고 있던 단말의 비식별 아이디 정보와 그 비식별 아이디 정보가 제1단말로 수신되기까지 거쳐왔던 단말들 중에서 가장 최근에 해당 비식별 아이디의 단말로부터 비식별 아이디를 수신했던 단말의 수신시점과 그 당시 그 비식별 아이디의 단말의 위치에 대해 추정된 정보가 저장되어 있게 된다. 즉, 제1단말에는 독감감염정보를 포함하고 있던 제4단말의 비식별 아이디 정보와 그 정보가 제3단말로 수신된 시점과 그 당시 제4단말의 위치에 대해 추정된 정보가 저장되어 있게 된다. 그 수신시점과 비식별 아이디의 단말의 당시 위치는 해당 비식별 아이디를 수신했던 제1단말의 수신시점과 제1단말의 위치정보와 그 위치정보를 파악한 시점으로 추정될 수 있다. 또한 제1단말에는 독감감염정보를 포함하고 있던 제2단말의 비식별 아이디 정보와 그 정보가 제1단말로 수신된 시점과 그 당시 제2단말의 위치에 대해 추정된 정보가 저장되어 있게 된다. 그러나 제1단말에 저장되어 있는 독감감염정보가 어느 단말의 것인지를 비식별 아이디를 통해서 판별할 수 없으

며, 단순히 제1단말이 노출 및 수신 과정의 거쳐 정보를 획득할 수 있는 단말들 중에서 두 개의 단말의 사용자가 독감에 감염되었다는 정보만 알 수 있다. 제1단말 또한 마찬가지로 제2단말로부터 수신한 비식별 아이디를 통해서 제2단말의 사용자가 독감감염자일 것으로 예상할 수도 있으나 제2단말과 인접해 있는 또 다른 단말의 사용자로부터 수신한 정보일 가능성도 있어 앞선 가정과 달리 제1단말은 제2단말의 사용자가 독감감염자임을 확인할 수 없다. 제1단말은 이와 같은 정보를 서버로 전송함으로써 서버는 도1에 도시된 영역 내에 두 명의 독감감염자가 있는 것과 그 위치에 대한 정보만을 알 수 있을 뿐, 구체적으로 어느 단말의 사용자가 독감에 감염되었는지를 파악할 수가 없다.

[0038] 본 발명의 실시예에 따른 개인정보 비식별화 전송장치는 도1과 같은 개념의 시스템을 구축하기 위해 필요한 장치로서 자세한 설명을 하기한다.

[0039] 설명의 편의상 앞선 예와 같이 단말에 저장되는 개인정보를 질병감염정보로 가정하고 설명한다.

[0040] 도2는 본 발명의 실시예에 따른 전송장치의 블록도이다.

[0041] 도2와 같이 본 발명이 실시예에 따른 전송장치(10)는 외부 단말과 네트워크로 연결되어 통신을 수행하는 통신부(100), 장치(10)의 비식별화를 위한 아이디를 생성하고, 전송주기, 리스트 수집구간 또는 노출구간을 설정하는 제어부(200), 통신부(100)를 통해 외부 단말의 노출용 아이디 리스트를 수신하여 보관용 아이디 리스트, 수집구간 아이디 리스트, 노출용 아이디 리스트 및 전송용 아이디 리스트를 생성하는 리스트 생성부(300) 및 리스트 생성부(300)로부터 생성된 보관용 아이디 리스트, 수집구간 아이디 리스트, 노출용 아이디 리스트 및 전송용 아이디 리스트를 저장하는 메모리(400)를 포함한다.

[0042] 또한 본 발명의 실시예에 따른 전송장치(10)는 수집구간 아이디 리스트 생성시점과 생성위치를 추정하는 리스트 생성 추정부(500) 및 사용자 인터페이스(600)와 상기 사용자 인터페이스(600)를 통해 입력되는 사용자의 제1정보와 서버로부터 전송되는 제2정보가 일치하는지를 판정하는 정보 판정부(700)를 더 포함한다.

[0043] 통신부(100)는 Wi-Fi Direct, 와이파이(Wi-Fi) 또는 비콘(Beacon)통신을 위한 모듈을 포함하고 있으며, 통신부(100)를 통해 전송장치(10)는 부근에 있는 다른 단말들과 데이터를 주고 받을 수 있다. 전송장치(10)와 다른 단말간의 통신 프로토콜은 모두 동일할 수 있으며, 단말의 고유식별번호의 형식도 모두 동일할 수 있다.

[0044] 통신부(100)는 다양한 정보를 전송하거나 수신할 수 있다. 일례로, 단말의 사용자 요청에 의해서 특정 질병 관련 정보를 수신할 수 있다. 단말 사용자의 요청없이 범용적 질병관련 정보를 수신할 수도 있다. 범용적 질병 관련 정보는 일반적인 질병대처법이나 생활예방수칙 등을 포함한다. 특정 질병 관련 정보는 단말기 사용자들이 입력하는 개인정보인 감염정보를 이용하여 도출된 특정 질병 관련 감염지도와 같은 정보를 수신하여 단말 사용자에게 디스플레이할 수 있다.

[0045] 제어부(200)는 장치의 비식별화를 위한 아이디를 생성하고 전송주기, 리스트 수집구간 또는 노출구간을 설정한다.

[0046] 도3은 본 발명의 실시예에 따른 제어부의 상세블록도이다.

[0047] 도3과 같이 제어부(200)는 시스템 설정모듈(210)과 아이디 생성모듈(220), 전송결정모듈(230)을 포함한다.

[0048] 시스템 설정모듈(210)은 장치의 전송주기를 결정하고, 외부 단말로부터 노출용 아이디 리스트를 수신하는 리스트 수집구간을 결정하며, 노출용 아이디 리스트를 노출시키는 노출구간을 결정한다.

[0049] 본 발명의 실시예에 따른 전송장치는 시스템 설정모듈(210)에 의해 설정된 전송주기별로 반복된 절차를 수행한다. 예를 들어, 1시간 또는 30분, 10분, 1분마다 전송할 수 있고, 설정된 전송주기를 참고해서 장치에 저장된 정보의 전송시점을 결정한다.

[0050] 전송주기, 수집구간, 노출구간에 대한 설명은 도4를 참고하여 설명한다.

[0051] 도4는 전송주기내의 수집구간, 노출구간을 설명하기 위한 다이어그램이다.

[0052] 전송주기는 전송용 아이디 리스트를 서버로 전송하는 주기를 의미한다.

[0053] 전송주기의 시작시점과 종료시점은 모든 단말기가 동일하다. 전송주기의 시작시점에 각 단말기의 아이디가 생성되어 전송주기의 종료시점까지 유지되기 때문에 전송주기를 길게 하면 그 동안은 하나의 단말기 아이디로 이동 경로 추적이 가능하다. 이는 질병의 감염경로 파악을 위해 사용될 수 있다.

[0054] 수집구간은 외부 단말기로부터 노출용 아이디 리스트를 수신하는 구간이다. 수집구간의 시작시점과 종료시점은

각 단말기가 임의로 결정한다. 수집구간의 시작시점을 전송장치의 노출구간의 시작시점을 기준으로 일정시간(T_1) 이전으로 설정할 수 있으며, 노출구간의 시작시점과 무관하게 주기적으로 또는 임의로 수집구간 시작시점을 결정하여 전송주기 내에서 일정구간(T_1-T_2) 동안 다른 단말기로부터 노출용 아이디 리스트를 수집할 수 있다. 이때 첫 번째 노출용 아이디 리스트 수집 구간의 시작시점은 임의로 결정되도록 할 수 있으며, 난수발생 등을 통해 첫 번째 수집구간의 시작시점이 결정되도록 할 수 있다. 수집하는 횟수는 단수 또는 복수로 설정할 수 있으며, 복수회로 설정된 경우 첫 번째 수집구간의 시작시점이 임의로 결정되고 그 다음 수집구간의 시작시점은 첫 번째 수집구간의 시작시점을 기준으로 일정간격을 두고 설정되어 전송주기의 종료시점을 초과하지 않는 범위내에서 설정될 수 있다. 또한 노출구간의 시작시점을 전송주기 내에 복수회 결정하는 절차와 유사하게 리스트 수집 구간의 시작시점을 전송주기 내에서 복수로 결정할 수 있다.

- [0055] 노출구간은 본 발명의 실시예에 따른 전송장치(10)가 저장하고 있는 보관용 아이디 리스트를 이용하여 생성된 노출용 아이디 리스트를 다른 단말로 노출시켜 수신할 수 있도록 하는 구간이다. 노출구간의 시작시점과 종료시점은 각 단말기가 임의로 결정할 수 있다.
- [0056] 노출구간의 시작시점은 전송주기 내에 1회 또는 복수로 결정될 수 있다. 노출구간의 시작 시점과 전송주기내 1회 결정되는 절차는 0 ~ 100사이 랜덤 숫자를 발생시킨다. 발생된 랜덤 숫자를 r 이라 하면 노출구간 시작시점은 전송주기 시작시점 + (전송주기 - 노출구간의 길이)* $r/100$ 일 수 있다. 예를 들어 전송주기가 30분이고 전송주기 시작시점이 오후 2시이고 노출구간의 최소길이가 10분이며, $r=75$ 이면 해당 전송주기의 노출구간의 시작시점은 0시를 기점으로 분단위로 산출하면 855분이 된다.
- [0057] 전송주기 동안 노출구간의 시작시점을 1회 결정하여 노출구간의 시작시점 이후로 노출용 아이디 리스트를 노출구간의 최소 길이만큼만 노출하거나 서버로 전송될 때까지 노출을 지속할 수 있다. 노출 구간의 최소길이에 해당하는 시간 동안만 노출하도록 설정될 경우에 노출지속시간이 노출구간의 최소길이를 초과하기 전에 서버로 전송용 아이디 리스트가 전송되는 시점이 도래하면 최소 노출 지속시간이 충족된 것으로 처리할 수 있다.
- [0058] 노출구간의 시작시점을 전송주기 내에 복수회로 결정하는 절차는 다음과 같다.
- [0059] 첫 노출구간의 시작시점이 결정된 이후로 해당 전송주기의 종료시점 전까지 다음의 과정을 반복하여 1회 또는 복수로 노출시점의 시작구간을 결정할 수 있다. 먼저 0~100사이 랜덤한 숫자를 발생시킨다. 발생된 랜덤숫자를 r 이라 한다. 전송주기 내 첫 노출시점의 시작구간은 (전송주기 시작시점 + (전송주기 - 노출구간의 길이)* $r/100$)으로 산출한다. ($j-1$)번째 노출구간의 종료시점(S) = ($j-1$)번째 노출구간의 시작시점 + 노출구간의 길이이고, j 번째 노출시점의 시작구간은 $S + S$ 이후로 남겨진 해당 전송주기의 잔여시간* $r/100$ 으로 정할 수 있다. j 번째 노출구간 시작시점이 전송주기의 종료시점으로부터 노출구간의 길이를 뺀 시점 이전에 위치한다면 다시 이전 과정을 반복하여 ($j+1$)번째 노출시점의 시작구간을 산출한다. 그렇지 않으면 더 이상 노출시점의 시작구간을 산출하지 않는다.
- [0060] 이외에 전송주기 내 갱신주기는 수집 구간 내에서 수집구간 아이디 리스트를 갱신하는 주기를 의미하고 갱신주기는 모든 단말기에서 동일할 수도 있고 그렇지 않을 수도 있다.
- [0061] 아이디 생성모듈(220)은 장치의 비식별화를 위한 아이디를 생성한다. 본 발명의 실시예에 따른 전송장치 뿐만 아니라 주변의 다른 모든 단말에서 비식별화된 아이디를 생성한다. 아이디 생성모듈(220)은 문자나 숫자나 기호를 임의 조합하여 아이디를 생성할 수도 있다.
- [0062] 도5는 실제 장치에서 노출된 노출용 아이디 리스트를 도시한 그림이다.
- [0063] 도5에 도시된 바와 같이 4*1, 67&, a6#, 5%a, 7d@, 17?, s21, #!7, slk, *#1 등 10개 아이디로 구성된 Wi-Fi Direct 단말 아이디가 노출되어 있음을 확인할 수 있다. 즉 아래 설명할 노출용 아이디 리스트가 앞서 설명한 노출구간의 시작시점부터 도5와 같은 형태의 데이터로 노출되고 장치의 근처에 외부 단말은 이 정보를 읽어들이 수 있다.
- [0064] 전송결정모듈(230)은 전송주기의 종료시점에 전송용 아이디 리스트를 서버로 전송할지 말지를 결정한다. 단말이 고유식별정보를 제공하고 전송용 아이디 리스트를 서버로 전송할 경우 부득이 전송한 단말을 특정할 수 있는 경우가 발생한다.
- [0065] 예를 들어 설명하면 복수의 수집구간이 있는 전송주기 내에서 개인이 특정되는 경우를 설정해본다. 하나의 전송주기 내에 복수의 수집구간이 발생하였을 때 그 수집구간들에서 복수의 수집구간 아이디 리스트들에 특정 아이

다가 반복적으로 등재되면 개인이 특정되는 상황이 발생할 수 있다.

표 1

[0066]

수집구간 No	1		
스캔가능단말	A	B	C
생성된 단말 아이디	#11	#22	#33
감염유무	0	X	X

표 2

[0067]

수집구간 No	2		
스캔가능단말	A	E	D
생성된 단말 아이디	#11	&44	&55
감염유무	0	X	X

[0068]

위 표1, 2은 첫 번째 수집구간과 두 번째 수집구간에 대한 정보를 보여주고 있다. 단말 A만 감염자의 단말기이며 그 이외의 단말은 모두 비감염자의 단말이다. 첫 번째 수집구간의 종료시점에 단말기 A, B 와 C는 아래 표3과 같은 전송용 아이디 리스트를 서버로 전송할 수 있다.

표 3

[0069]

단말A의 전송용 아이디 리스트	단말B의 전송용 아이디 리스트	단말C의 전송용 아이디 리스트
#11	#11	#11

[0070]

두 번째 수집구간의 종료시점에 단말 A, D, E는 아래 표4와 같은 전송용 아이디 리스트를 서버로 전송할 수 있다.

표 4

[0071]

단말A의 전송용 아이디 리스트	단말D의 전송용 아이디 리스트	단말E의 전송용 아이디 리스트
#11	#11	#11

[0072]

단말들이 서버에 접속 했을때는 단말의 고유 식별번호가 서버에 의해서 인식된다. 따라서 첫 번째 수집구간과 두 번째 수집구간에 각 1명의 감염자가 존재하고 두 수집구간에 공통적으로 참여하고 있는 단말은 A 한 대이며, 두 구간에서 전송되는 전송용 아이디 리스트에 감염자로서 #11이라는 하나의 아이디만 등재되어 있다. 이러한 정보는 두 구간에 감염자 단말 1대가 존재하고, 두 구간에 공통으로 참여하고 있음을 확인할 수 있어 감염자 단말은 A임을 알 수 있다.

[0073]

물론 첫 번째 수집구간과 두 번째 수집구간 각각에서 3대의 단말기 외에 제4의 단말기가 존재하여 감염자 정보 노출 및 공유과정에만 참여하고 전송을 하지 않았을 경우가 있으므로 단말 A가 감염자 단말로 100%확신할 수는 없는 상황이다.

[0074]

이 상황에 착안하여 본 발명의 실시예에 따른 전송결정모듈(230)은 하나의 전송주기 내에 복수의 수집구간을 사용할 때에 개인 식별화 문제를 해결하기 위해서 복수의 수집 구간을 가진 전송 주기의 종료시점에 감염자 단말은 전송용 감염자 ID 리스트를 서버로 전송하지 않도록 한다. 따라서 서버는 감염자 단말기의 존재를 파악할 수 없다. 또한 비감염자 단말기들도 일부만 서버로 전송할 수 있도록 설정한다. 예를 들어, 난수를 발생시켜 비감염자 단말기들이 각각 전송시킬 확률 P를 가질 수 있도록 설정할 수 있다. P=70%라고 하자. 난수 r을 0에서 1 사이에서 발생시켜 r=0.8을 얻었다고 하자. r>P이므로 해당 단말기는 서버로 전송용 감염자 ID 리스트를 전송하지 않는다. 이와 유사하게 다른 비감염자 단말도 전송 여부를 결정한다. 감염자 단말을 제외한 전체 단말의 일부만 전송하여, 감염자 단말이 식별화 되는 경우를 방지한다. P값은 스캔되는 단말의 수에 따라 자동 결정되게

설정할 수 있다. 스캔되는 단말의 수가 많을수록 P값은 낮아지고, 반대의 경우 높아져서 충분한 수의 단말이 해당 지역의 감염 정보를 서버로 전송할 수 있도록 하는 것이 바람직하다.

[0075] 도6은 본 발명의 실시예에 따른 리스트 생성부의 블록도이다.

[0076] 도6에 도시된 바와 같이 리스트 생성부(300)는 보관용 아이디 리스트 생성모듈(310)과 수집구간 아이디 리스트 생성모듈(320), 노출용 아이디 리스트 생성모듈(330) 및 전송용 아이디 리스트 생성모듈(340)을 포함한다.

[0077] 보관용 아이디 리스트 생성모듈(310)은 통신부(100)를 통해 다른 단말의 노출용 아이디 리스트를 수신하여 보관용 아이디 리스트를 생성한다. 보관용 아이디 리스트는 네트워크 검색반경 내의 다른 단말의 노출용 아이디 리스트에 기재된 감염자 아이디로 구성되는 리스트일 수 있으며 장치 사용자 본인이 감염되었을 경우 장치의 아이디도 기록한다. 보관용 아이디 리스트는 전송주기의 시작시점에 백지화된다.

[0078] 수집구간 아이디 리스트 생성모듈(320)은 리스트 수집구간에 외부 단말로부터 수신한 노출용 감염자 리스트를 저장 또는 갱신하여 수집구간 아이디 리스트를 생성한다. 수집구간 아이디 리스트는 아래 설명할 리스트 생성 추정부에서 추정된 수집구간 아이디 리스트 생성시점 및 생성위치와 함께 메모리에 저장된다.

[0079] 노출용 아이디 리스트 생성모듈(330)은 보관용 아이디 리스트에서 추출한 아이디들의 순서를 재배열하여 노출구간에 외부 단말로 노출시키기 위한 노출용 아이디 리스트를 생성한다. 보다 상세하게는 보관용 아이디 리스트는 수집구간 아이디 리스트로 구성되어 있고, 수집구간 아이디 리스트의 일부 또는 전부로부터 아이디를 추출하여 노출용 아이디 리스트를 생성한다. 노출용 아이디 리스트는 보관용 아이디 리스트의 일부 또는 전부를 가공하여 노출시키고, 리스트의 길이는 임의로 설정이 가능하다.

[0080] 설정된 노출용 아이디 리스트의 길이를 초과하지 않는 범위 내에서 노출시점의 시작구간 이전에 생성된 가장 최근 보관용 아이디 리스트의 일부 또는 전부를 추출하고 그 추출된 리스트에 등재된 아이디의 순서를 재배열하여 구성하는 방식으로 노출용 아이디 리스트를 생성한다. 이때 전송장치의 사용자가 감염자일 경우에는 전송장치의 아이디를 포함하여 노출용 아이디 리스트를 노출한다. 노출방식은 여러 통신모듈을 이용해서 결정될 수 있다. 앞서 설명한 도5에 도시된 Wi-Fi Direct 기기명을 리스트에 포함된 감염자 단말 아이디를 일렬로 나열하여 노출하는 방식이 그 예이다.

[0081] 전송용 아이디 리스트 생성모듈(340)은 전송주기 종료시점에 서버로 전송할 전송용 아이디 리스트를 생성한다. 전송용 아이디 리스트는 보관용 아이디 리스트의 일부 또는 전부를 추출하여 생성된다. 이때 생성된 전송용 아이디 리스트의 서버로 전송여부와 전송시에 동반 전송할 추가 정보의 종류를 결정하는 방법은 다양하게 설정될 수 있다. 특히 전송용 아이디 리스트와 함께 전송될 수집구간 아이디 리스트의 생성시점과 생성위치의 추정값에 대한 정확도에 따라 서버로 전송여부 및 동반 전송될 추가정보를 결정할 수 있다. 생성시점과 생성위치 추정방법에 대해서는 실제 생성시점과 생성위치 추정을 수행하는 아래 리스트 생성 추정부에서 설명한다.

[0082] 리스트 생성 추정부(500)는 수집구간 아이디 리스트 생성시점과 생성위치를 추정한다. k번째 수집구간 아이디 리스트의 생성시점과 생성위치를 리스트 생성 추정부에서 추정한다고 가정한다. 가능한 추정방법은 다양하다. k번째 수집구간 아이디 리스트를 구성하고 있는 감염자 아이디들은 대부분 타 단말로부터 수집한 것이기 때문에 생성시점과 위치정보를 알 수 없지만 수집한 단말의 수집시점을 기준으로 추정을 시도한다.

[0083] 추정방법으로는 k번째 수집구간 아이디 리스트의 최종 갱신시점에서 가장 근접한 시점에 파악된, 수집에 사용된 단말(여기서는 본 발명의 실시예에 따른 전송장치)의 위치정보와 그 위치정보가 파악된 시점을 해당 수집구간 아이디 리스트의 생성위치와 생성시점으로 추정할 수 있다. 또한 수집에 사용된 단말의 수집구간 내에 파악된 모든 위치정보의 위경도들의 중심점과 생성 시점들의 중심점을 해당 수집구간 아이디 리스트의 생성위치와 시점으로 추정이 가능하다. 이와 같은 방법 중 하나로 추정된 k번째 수집구간 아이디 리스트의 생성시점과 생성위치 정보는 수집구간 아이디 리스트 생성정보로 메모리에 저장된다. 또는 그 대신에 수집에 사용된 단말의 수집구간 내에 파악된 모든 위치정보의 위경도들과 생성시점들로 데이터셋을 구성하여 "수집구간 아이디 리스트 생성모듈"로 메모리에 저장할 수 있다.

[0084] 사용자 인터페이스(600)는 본 발명의 실시예에 따른 전송장치에 구비되어 있는 사용자에게 의한 데이터의 입력이 가능하도록 하는 장치이다. 전송장치에 사용자의 질병감염여부 등에 대한 정보를 입력하는 장치로서 사용가능한 모든 인터페이스를 포함한다.

[0085] 정보관정부(700)는 사용자 인터페이스(600)를 통해 입력되고, 메모리(400)에 저장된 사용자의 제1정보와 이를 확인하기 위해 통신력이 보장된 기관이나 단체의 서버에서 전송되는 제2정보가 일치하는지를 확인한다. 예를 들

어 전송장치(10)의 사용자가 질병에 감염이 되지 않았으나 사용자가 전송장치(10)에 감염되었다고 입력한 경우, 건강보험심사평가원 DB나 질병관리본부 DB로부터 수신한 정보와 비교해서 허위입력임을 확인하고 더 이상 전송장치(10)의 서비스 사용을 허용하지 않을 수 있다.

[0086] 또 다른 예로 정보관정부(700)는 12월 현재, 지난 10월에 자발적으로 입력한 장치 사용자 본인의 감염정보와 11월에 건강보험심사평가원 DB나 질병관리본부 DB로부터 입수한 10월 실제 감염여부를 비교해서 10월 입력한 감염정보의 진위여부를 판단하여 10월의 입력정확성을 산출하고, 일정수준 이상일 경우에만 12월의 서비스 사용을 허가할 수 있다.

[0087] 이상 본 발명의 실시예에 따른 전송장치의 각 구성에 대해서 살펴보았다. 다음으로 전송장치의 동작에 따른 리스트 생성 및 리스트 전송과정을 도7을 통해 설명한다.

[0088] 도7은 본 발명이 실시예에 따른 전송장치의 동작흐름도이다.

[0089] 도7에 도시된 바와 같이 수집구간의 시작시점을 사용자 전송장치(10)의 노출구간의 시작시점을 기준으로 일정시간(D)이전으로 설정된 경우를 도식화하여 설명한다. 설정에 따라서는 수집구간들이 겹칠 수도 있으나 이때 별도의 수집구간 아이디 리스트를 생성하여 갱신할 수 있다. 설명의 편의상 특정 이벤트를 질병감염으로 설정하고 보관용 아이디 리스트를 보관용 감염자 ID리스트로, 노출용 아이디 리스트를 노출용 감염자 ID리스트로, 전송용 아이디 리스트를 전송용 감염자 ID리스트로 정의하고 설명한다.

[0090] 본 발명의 실시예에 따른 전송장치(10)와 모든 단말은 동일한 전송주기의 시작시점과 종료시점을 가진다. 만약 전송주기의 시작시점이 서로 다르다면 한 단말의 전송주기 동안 타 단말의 전송주기가 연속으로 2번 걸치는 상황이 발생하여 하나의 단말임에도 불구하고 다른 아이디의 생성으로 별개 단말로 인식할 수 있게 된다.

[0091] 앞서 설명한 바와 같이 전송주기별로 반복된 절차를 수행하고 전송주기는 1시간 또는 30분 또는 10분 등 다양하게 설정이 가능하다.

[0092] 전송주기의 시작시점에 전송장치의 아이디를 생성한다. 전송주기 시작시점에 보관용 감염자 ID리스트는 백지상태로 데이터가 담겨 있지 않다. 기 입력된 정보에 의해서 제어부(200)는 노출구간과 수집구간을 설정한다.

[0093] 보관용 감염자 ID리스트는 리스트 수집구간별로 생성된 수집구간 감염자 ID리스트를 추가하는 방식으로 생성된다. 1번째 수집구간의 시작시점에 백지상태인 1번째 수집구간 감염자 ID리스트를 생성한다. 그리고 1번째 리스트 수집구간의 시작시점에 스캔 가능한 반경 내에 위치한 타 단말의 노출용 감염자 ID리스트에 등재된 감염자 ID를 읽어 들여 1번째 수집구간 감염자 ID리스트에 추가한다. 설정된 갱신주기마다 스캔 가능한 반경 내에 위치한 타 단말의 노출용 감염자 ID리스트에 등재된 감염자 ID를 읽어 들여 1번째 수집구간 감염자 ID리스트에 추가하는 과정을 1번째 리스트 수집구간의 종료시점까지 반복한다. 이때 중복된 ID의 하나만 등재한다. 1번째 리스트 수집구간의 종료시점까지 갱신된 1번째 수집구간 감염자 ID리스트를 1번째 수집구간 감염자 ID리스트라고 명명하여 보관용 감염자 ID리스트에 추가한다. 전송주기의 종료시점까지 k번째 수집구간 감염자 ID리스트를 위 방법과 유사하게 생성하여 보관용 감염자 ID리스트에 추가한다. ($k=2, 3, \dots$)

[0094] 노출용 감염자 ID리스트를 읽어 들일 단말의 수가 많은 환경에 위치할 경우에 스캔 반경 내에 위치한 단말의 ID의 중복가능성을 줄이기 위해 단말 스캔반경을 줄일 수 있다. 예를 들어 지하철과 같은 스캔가능 반경 내에 많은 수의 단말이 존재하는 경우 단말의 스캔 반경을 줄여서 타 단말들의 ID가 중복될 가능성을 줄일 수 있다. 여기서 타 단말의 ID는 단말의 고유식별번호가 아니라 앞서 생성된 비식별화 ID를 의미하는 자명하다.

[0095] k번째 수집구간 감염자 ID리스트는 보관용 감염자 ID리스트에 k번째로 추가되는 감염자 ID리스트가 된다. 단 k번째 수집구간 감염자 ID리스트로 개인을 특정할 수 있는 상황이라 판단될 때는 보관용 감염자 ID리스트에 추가하지 않는다.

[0096] 개인을 특정할 수 있는 상황은 제1단말의 스캔반경 내에 타 단말이 존재하지 않고 제1단말에 그 사용자가 감염자라고 입력되는 상황이거나 스캔 반경 내의 타 단말의 수와 k번째 수집구간 감염자 ID리스트에 등재된 ID들 중에서 해당 단말기 ID를 제외한 ID들의 수가 일치하는 상황, 즉 면적이 1km^2 의 공터에 두 대의 단말만 있어서 서로의 스캔 반경 내에서 상대 단말만 검색되고 그 단말들의 사용자 두 사람 모두 감염자여서 각 단말에 사용자 감염자라고 입력되어 있고, 두 사람 중 제1단말만 노출을 허용하는 상황을 가정해 볼 수 있다. 이때 제1단말의 수집구간 감염자 ID리스트에는 두 단말의 ID들이 등재되고 제2단말의 수집구간 감염자 ID리스트에는 제2단말의 ID만 등재된다. 여기서 제1단말의 스캔반경 내의 타 단말의 수는 0개, 제1단말의 수집구간 감염자 ID리스트에 등재된 ID들 중에서 제1단말의 자체 ID를 제외한 ID의 수는 0개이고, 제2단말의 스캔반경 내의 타 단말의 수는

1개이고, 제2단말의 수집구간 감염자 ID리스트에 등재된 ID들 중에서 제2단말의 자체 ID를 제외한 ID의 수는 1개이다. 제1단말과 제2단말 각각에 스캔 반경내의 타 단말의 수와 해당 수집구간 감염자 ID리스트에 등재된 ID들 중에서 해당 단말기 ID를 제외한 ID들의 수가 일치하는 상황이 발생한다. 따라서 각 단말의 해당 수집구간 감염자 ID리스트는 각 단말의 보관용 감염자 ID리스트에 추가하지 않는다.

[0097] k번째 수집구간 감염자 ID리스트의 생성시점과 생성위치는 리스트 생성 추정부(500)에서 추정한다.

[0098] 1번째 수집구간에 수집된 다른 단말에서 노출되는 노출용 감염자 ID리스트를 수신하여 보관용 감염자 ID리스트에 추가한다. 이후 노출구간에 본 발명의 실시예에 따른 노출용 감염자 ID리스트를 노출시킨다. 노출용 감염자 ID리스트는 보관용 감염자 ID리스트의 수집구간 감염자 ID리스트들 중에서 생성시점의 최신성에 따라 우선순위를 두어 사용하는 것이 바람직하다. 가장 최근에 생성된 수집구간 감염자 ID리스트를 최우선적으로 사용하는 것이 수집구간 감염자 ID리스트의 생성시점과 생성위치를 추정하는데 유리하다.

[0099] 만약 보관용 감염자 ID리스트를 구성하고 있는 특정 수집구간 감염자 ID리스트의 추정된 생성시점이나 생성위치가 노출에 사용될 단말의 노출시점이나 노출위치와 일정수준 이상 상이하다고 판단되면, 그 수집구간 감염자 ID리스트는 노출용 감염자 ID리스트를 생성할 때 사용하지 않도록 설정할 수 있다.

[0100] 만약 보관용 감염자 ID리스트를 구성하고 있는 수집구간 감염자 ID리스트의 추정된 생성시점이나 생성위치가 노출에 사용될 단말의 노출시점이나 노출위치와 일정수준 이상 상이하지 않아서 노출용 감염자 ID리스트에 사용될 수 있음에도 불구하고 노출용 감염자 ID리스트의 길이제한으로 인해 노출용 감염자 ID리스트 생성에 사용되지 못할 경우도 있다. 이때 시작시점이 일정수준 이상 상이하지 않는 연속된 두 노출구간들에 대해 선행 노출구간의 시작시점의 단말 위치와 후행 노출구간의 시작시점의 단말 위치가 일정수준 이상 상이하지 않을 경우에는 가장 최근에 생성된 수집구간 감염자 ID리스트를 최우선적으로 사용하는 방식을 취하되 바로 이전 노출구간에 사용되었던 노출용 감염자 ID리스트에 등재되지 않은 ID에 우선순위를 뒤서 노출용 감염자 ID리스트를 생성할 수 있다. 이는 노출용 감염자 ID리스트의 길이제한으로 인해 수집되는 정보의 범위가 제한 받는 것을 완화하기 위함이다.

[0101] 2번째 리스트 수집구간에서도 앞서 설명한 1번째 리스트 수집구간과 같은 프로세스를 거쳐 보관용 감염자 ID리스트를 갱신하여 최종 리스트를 생성한다.

[0102] 전송용 감염자 ID리스트는 전송주기의 종료시점 이전에 생성된 보관용 감염자 ID리스트의 일부 또는 전부를 추출하여 생성한다. 이때 생성된 전송용 감염자 ID리스트의 서버로 전송여부와 전송시에 동반 전송할 추가정보의 종류를 결정하는 방법은 다양하게 설정될 수 있다. 특히 전송용 감염자 ID리스트에 포함된 수집구간 감염자 ID리스트들의 생성시점과 생성위치의 추정값에 대한 정확도에 따라 서버로 전송여부 및 동반 전송될 추가정보를 결정할 수 있다.

[0103] 제어부(200)의 전송결정모듈(230)은 서버로 전송하기에 앞서 수집구간 감염자 ID리스트의 추정된 위치정보의 정확도에 따라 전송주기의 종료시점에 전송용 감염자 ID리스트로 변환하여 서버로 전송할지 여부를 결정할 수 있다. 예를 들어 전송주기가 30분이고 해당 전송주기의 시작시점과 종료시점에서만 전송장치의 사용자 위치정보만 파악되었으며, 시작시점의 위치와 종료시점의 위치가 번째 수집구간 감염자 ID리스트의 생성위치를 추정하기 어려울 정도로 충분히 상이하게 구성되어 있으면, 해당 전송주기에 전송용 감염자 ID리스트의 서버로의 전송을 결정하지 않을 수 있다. 또 다른 예시로 자동차나 지하철 등을 타고 이동하는 것은 자이로스코프나 가속도 센서를 이용해서 알 수 있고, 위치이동이 많은 상황이면 이를 고려해서 수집구간 감염자 ID리스트의 생성위치파악의 정확성을 판단할 수 있다. 위와 같은 과정이 전송주기의 시작시점과 종료시점 사이에 설정되는 수집구간에서 반복적으로 수행되어 종료시점 이전에 해당 전송주기의 보관용 감염자 ID리스트 최종본이 완성된다.

[0104] 전송결정모듈(230)은 위와 같이 서버로 전송할지 여부를 판단하는 기능 이외에 서버로 전송할지, 타 단말로 전송용 감염자 ID리스트를 노출시킬지를 결정한다. 즉 본 발명의 실시예에 따른 전송장치(10)에서 전송하게 될 전송용 감염자 ID리스트, 생성시점 및 생성위치에 대한 정보의 일부를 전송하는 경우를 가정해 볼 수 있다. 만일 생성위치정보를 전송하는 경우에는 전송자의 위치가 서버에 노출될 가능성이 있기 때문이다.

[0105] 자세한 설명을 위해 전송하게 될 전송용 아이디 리스트(전송용 감염자 ID리스트)에 포함되어 있는 정보를 각각 분류하여 서버로 전송할지 다른 단말로 노출시킨 후에 다른 단말을 통해서 서버로 전송할지를 결정하는 예를 살펴본다.

[0106] 첫째, 서버로 전송하게 될 전송용 감염자 ID리스트는 수집구간 감염자 ID리스트만을 서버로 전송할 수 있다. 이 경우는 생성시점과 생성위치에 대한 정보 없이 감염자 ID리스트만 전송하는 것으로 감염자의 위치 및 이동을 파악

할 수는 없지만 조사대상이 되는 전 지역내의 감염자 수 파악만으로도 의미가 있게 되고, 전송용 감염자 ID리스트를 서버로 전송하더라도 전송자의 위치가 노출될 위험은 없어 바로 서버로 전송한다.

[0107] 둘째, 전송용 감염자 ID리스트에 포함된 수집구간 감염자 ID리스트 중에서 생성시점의 추정값이 타당하다고 판단되고 생성위치 추정값이 타당하다고 판단되지 않는 수집구간 감염자 ID리스트만 추정된 생성시점과 함께 서버로 전송할 수 있다. 이 경우에는 생성시점 정보를 제공해서 감염자의 변동과악에 효율적인 자료로 사용이 가능하고, 생성위치에 대한 정보를 포함하고 있지 않는 관계로 전송자의 위치가 노출될 위험이 없어 바로 서버로 전송한다.

[0108] 셋째, 전송용 감염자 ID리스트에 포함된 수집구간 감염자 ID리스트 들 중에서 생성시점의 추정값이 타당하다고 판단되지 않고 생성위치의 추정값이 타당하다고 판단되는 수집구간 감염자 ID리스트만 추정된 생성위치정보와 함께 서버로 전송할 수 있는데 이 경우는 정확한 생성시점은 파악할 수 없으나 특정 기간에 대한 감염자들의 분포를 파악할 수 있으나, 전송단말이 서버로 직접 생성위치정보를 전송하는 경우에는 전송단말의 이동경로가 서버에 직접 노출될 위험이 있다. 이 경우에 전송결정모듈(230)은 수집구간 감염자 ID리스트와 생성위치정보가 포함된 전송용 감염자 ID리스트를 다른 단말이 수신할 수 있도록 노출시킨다. 전송용 감염자 ID리스트를 수신한 다른 단말은 서버로 전송용 감염자 ID리스트를 전송한다. 이때 다른 단말은 감염자 단말 일 수도 있고 피감염자 단말 일 수도 있다.

[0109] 이와 같은 과정을 거치게 되면 전송용 감염자 ID리스트상에 포함되어 있는 생성위치정보를 다른 단말이 수신하더라도 어느 전송장치(단말)의 정보인지를 알 수 없게 되어 다른 단말을 통해 서버로 전송하더라도 전송장치의 개인정보는 보호된다.

[0110] 다른 단말은 서버로 전송하기 이전에 전송용 감염자 ID리스트(전송용 아이디 리스트)에 포함되어 있는 수집구간 감염자 ID를 확인하여 중복여부를 필터링하고 서버로 전송할 수 있다.

[0111] 넷째, 전송용 감염자 ID리스트에 포함된 수집구간 감염자 ID리스트들 중에서 생성시점의 추정값이 타당하다고 판단되고 생성위치의 추정값이 타당하다고 판단되는 수집구간 감염자 ID리스트만 추정된 생성시점 정보와 생성위치정보를 서버로 전송할 수 있고, 이 경우에는 감염자수와 감염자의 위치, 시간별 변동사항의 파악이 가능하나, 위 세 번째 예와 마찬가지로 생성위치정보가 서버로 직접 전송될 경우 전송단말의 사용자의 이동경로가 서버로 노출된다. 이러한 위험으로 인해서 전송결정모듈(230)은 다른 단말이 수집구간 감염자 ID리스트와 생성시점, 생성위치정보를 포함하는 전송용 감염자 ID리스트를 수신할 수 있도록 노출시키고, 위 정보를 수신한 다른 단말이 서버로 전송한다. 마찬가지로 다른 단말은 감염자 단말일 수도 있고, 피감염자 단말일 수도 있다.

[0112] 상기 질병감염에 대한 예를 들어 본 발명의 실시예에 따른 전송장치(10)에 대해서 설명하였고, 이는 감염에 해당하는지 안하는지 2가지 형태로 답변이 가능한 문답으로서 감염자인 경우에만 아이디를 노출시키고 수신하는 프로세스를 거치게 되나 이와 달리 선거 지지도 조사와 같은 선다형(multiple choice)의 경우에도 본 발명의 실시예에 따른 전송장치(10)의 적용이 가능하다. 예를 들어 선다형의 경우에는 적용하기 위한 다양한 방법이 있겠으나 일례로 아이디를 생성하는 단계에서 아이디 앞에 숫자로 응답번호를 명시하고 이어서 아이디를 표시하는 방식(노출용 아이디 리스트가 1A@#E&F2ER#K@!으로 표시된 경우, 1번 후보를 선택한 단말의 아이디가 A@#, E&F이고 2번 후보를 선택한 단말의 아이디는 ER#, K@!)으로 아이디 리스트를 작성할 경우 개인정보 비식별화 전송장치에 적용이 가능하다.

[0113] 이상 본 발명의 실시예에 따른 개인정보 비식별화 전송장치에 대해서 살펴보았다. 이하 본 발명의 또 다른 양태에 따른 개인정보 비식별화 전송방법에 대해서 도8를 통해 살펴본다. 앞선 실시예와 중복되는 구성에 대한 설명은 생략한다.

[0114] 도8는 본 발명의 실시예에 따른 개인정보 비식별화 전송방법의 순서도이다.

[0115] 도8에 도시된 바와 같이 개인정보 비식별화 전송방법은 장치의 아이디를 생성하는 단계(S100), 노출용 아이디 리스트의 노출구간을 결정하는 단계(S200), 외부 단말로부터 노출용 아이디 리스트를 수신하여 수집구간 아이디 리스트를 생성하는 단계(S300), 상기 수집구간 아이디 리스트를 이용하여 보관용 아이디 리스트를 업데이트하는 단계(S400), 상기 보관용 아이디 리스트에 포함된 아이디 리스트 순서를 재배열하거나 추출하여 노출용 아이디 리스트를 생성하는 단계(S500), 노출용 아이디 리스트를 외부 단말에 노출시키는 단계(S600), 상기 전송주기의 종료시점에 서버로 전송할 전송용 아이디 리스트를 생성하는 단계(S700) 및 상기 장치의 전송주기 종료시점에 상기 전송용 아이디 리스트를 서버로 전송하는 단계(S800)를 포함한다.

[0116] 아이디를 생성하는 단계(S100)는 장치의 고유번호를 이용하여 조합가능한 아이디를 생성하는 단계이다. 생성되

는 아이디어는 인근의 다른 단말과의 구별을 위한 것일 뿐, 단말의 고유식별번호가 아니다.

- [0117] 전송용 감염리스트의 노출구간을 결정하는 단계(S200)는 앞서 설명한 바와 같이 전송주기와 임의의 랜덤넘버를 이용하거나 복수회 노출인 경우에는 노출지속시간 등을 고려하여 전송주기 종료시점까지의 노출시점의 시작구간을 결정한다.

[0118] 외부 단말로부터 노출용 아이디 리스트를 수신하여 수집구간 아이디 리스트를 생성하는 단계(S300)는 장치와 인접해 있는 외부 단말에서 생성된 노출용 아이디 리스트를 수신하는 단계이다.

[0119] 외부 단말로부터 노출용 아이디 리스트를 수신한 후에 보관용 아이디 리스트를 업데이트 한다(S400). 보관용 아이디 리스트는 전송주기 시작시점에 생성된다. 메모리에 저장된 보관용 아이디 리스트는 외부 단말로부터 수신된 노출용 아이디 리스트를 통해서 업데이트된다.

[0120] 업데이트시에 중복아이디는 제거한다.

[0121] 노출용 아이디 리스트를 생성하는 단계(S500)는 메모리에 저장되어 있는 보관용 감염리스트에서 아이디의 순서를 서로 바꾸거나 재조합하거나 일부 아이디만을 추출하여 노출용 아이디 리스트를 생성한다.

[0122] 노출용 아이디 리스트가 생성되면 기 결정된 노출구간에 노출용 아이디 리스트를 외부 단말로 노출시키는 단계(S600)를 거친다. 외부 단말은 본 발명에 따른 장치와 같은 동작을 수행하되, 중복아이디는 제거된다. 외부 단말의 노출구간의 시작시점이나 종료시점은 외부 단말 자체의 설정에 의해서 정해지므로 본 발명에 따른 장치와 같을 가능성은 크지 않다.

[0123] 전송주기 종료시점에 이른 경우 서버로 전송할 전송용 아이디 리스트를 생성한다.(S700) 전송용 아이디 리스트는 전송주기의 종료시점 이전에 생성된 보관용 아이디 리스트의 일부 또는 전부를 추출하여 생성된다.

[0124] 다음으로 전송할 전송용 아이디 리스트에 생성위치정보가 포함되어 있는지를 판단하고, 만일 생성위치 정보가 포함되어 있는 경우에는 직접 서버로 전송하지 않고, 다른 단말로 수집구간 아이디 리스트와 생성위치정보 및/또는 생성시점정보를 포함하는 전송용 아이디 리스트를 노출시킨다.(S800) 이후 다른 단말은 수신한 정보들을 서버로 전송한다.(S900)

[0125] 만일 전송할 전송용 아이디 리스트에 생성위치정보가 포함되어 있지 않은 경우에는 직접 서버로 수집구간 아이디 리스트 및/또는 생성시점정보를 포함하는 전송용 아이디 리스트를 전송한다.(S900)

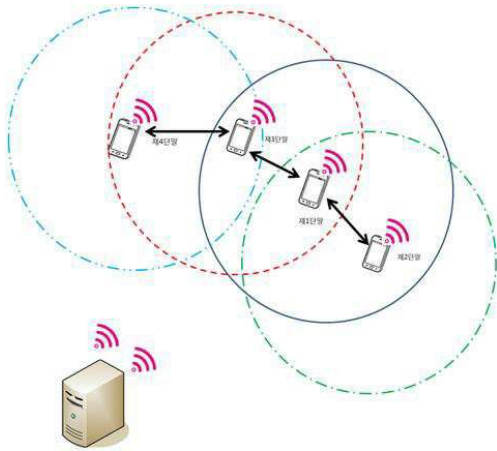
[0126] 결국 위와 같은 과정을 통해 구현되는 개인정보 비식별화 전송방법에 의해서 서버로 전송되는 정보는 개인정보를 담고 있으나 각 개인별로 매칭이 불가능한 정보로서 개인정보 노출위험이 없으며, 비식별 아이디를 생성하여 고유식별정보 없이도 단말기 간에 정보를 공유하거나 노출구간의 시작시점을 달리함으로써 자칫 발생할 수 있는 개인정보 식별위험을 차단하게 된다.

부호의 설명

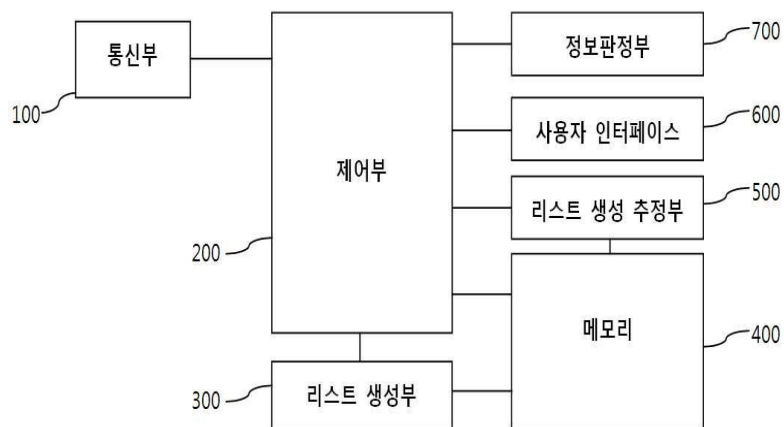
- | | | |
|--------|-----------------------|----------------------|
| [0127] | 10 전송장치 | 100 통신부 |
| | 200 제어부 | 210 시스템 설정모듈 |
| | 220 아이디 생성모듈 | 230 전송결정모듈 |
| | 300 리스트 생성부 | 310 보관용 아이디 리스트 생성모듈 |
| | 320 수집구간 아이디 리스트 생성모듈 | 330 노출용 아이디 리스트 생성모듈 |
| | 340 전송용 아이디 리스트 생성모듈 | 400 메모리 |
| | 500 리스트 생성 추정부 | 600 사용자 인터페이스 |
| | 700 정보관정부 | |

도면

도면1

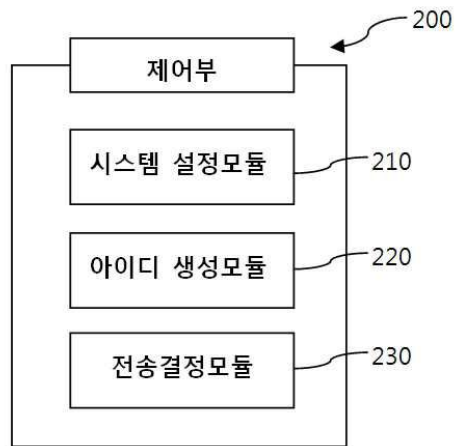


도면2

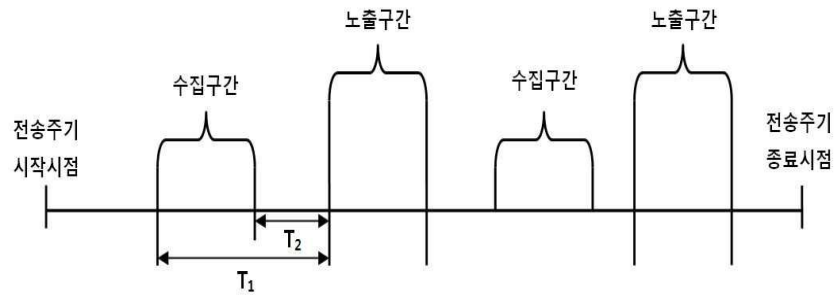


10

도면3



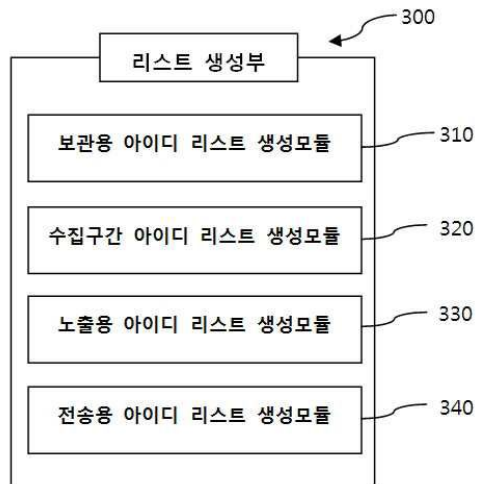
도면4



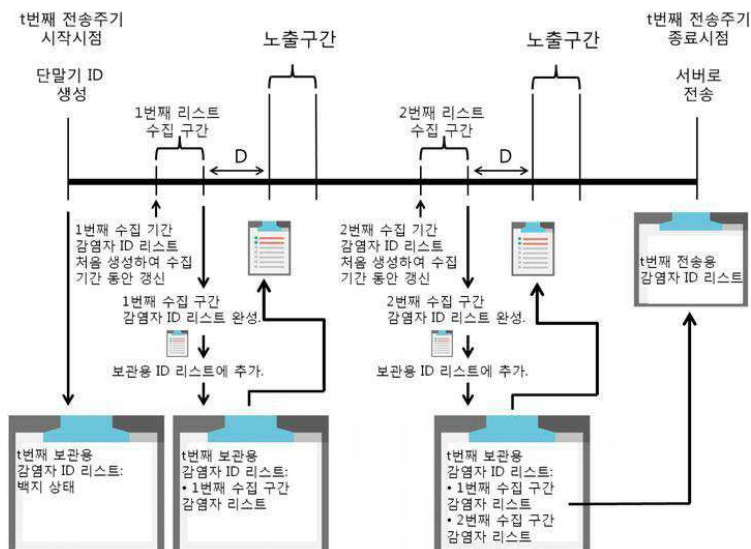
도면5



도면6



도면7



도면8

