(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06F 15/00 (2006.01)
H04L 9/32 (2006.01)
H04L 9/30 (2006.01)
H04L 12/22 (2006.01)

(45) 공고일자 2007년01월19일
(11) 등록번호 10-0670832
(24) 등록일자 2007년01월11일

(21) 출원번호 10-2005-0121986
(22) 출원일자 2005년12월12일
심사청구일자 2005년12월12일

(65) 공개번호
(43) 공개일자

(73) 특허권자 한국전자통신연구원
대전 유성구 가정동 161번지

(72) 발명자 노종혁
대전 유성구 반석동 양지마을 2단지 203-1804

김승현
대구 달서구 도원동 1439 가람마을아파트 105-804

최대선
대전 서구 월평3동 누리아파트 108-1101

조상래
대전 서구 월평동 진달래아파트 103-1505

조영섭
대전 서구 월평3동 하나로아파트 107-902

진승헌
대전 서구 월평동 백합아파트 104-1405

(74) 대리인 리앤목특허법인

(56) 선행기술조사문헌
JP2001331446 A
JP2002305513 A
KR1020030066134 A
JP2002297385 A
JP2004135004 A
* 심사관에 의하여 인용된 문헌

심사관 : 여원현

전체 청구항 수 : 총 18 항

(54) 에이전트를 이용한 사용자 개인정보 송수신 방법 및 장치

(57) 요약

본 발명은 에이전트를 이용한 사용자 개인정보 송수신 방법 및 장치에 관한 것으로, 개인정보를 관리하는 서버는 개인정보 요청을 받으면 개인정보를 에이전트에 담아서 제공하고, 에이전트를 수신한 호스트는 필요한 개인정보를 에이전트에 요청하며, 에이전트는 요청한 호스트가 정당한 사용자인지를 판단한 후 개인정보를 제공함으로써 개인정보가 안전하게 관리되고 유통되도록 하는 것이다.

대표도

도 1

특허청구의 범위

청구항 1.

(a) 클라이언트로부터 사용자 개인정보를 요청하는 요청 메시지를 전송받은 정보 관리 서버는 상기 사용자 개인정보를 검출하는 단계;

(b) 상기 검출된 사용자 개인정보를 암호화하기 위한 암호화키와 이를 복호화하기 위한 복호화키를 각각 생성하는 단계;

(c) 상기 검출된 사용자 개인정보를 상기 암호화키로 암호화하고, 암호화된 사용자 개인정보를 서명하는 단계;

(d) 상기 암호화된 사용자 개인정보와 암호화된 사용자 개인정보의 서명값 및 상기 사용자 개인정보가 정당한 클라이언트에게만 제공되도록 하는 검증 정보를 포함하는 에이전트를 생성하는 단계; 및

(e) 상기 정보 관리 서버는 상기 생성된 에이전트와 복호화키를 상기 클라이언트로 전송하는 단계;를 포함하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 송신 방법.

청구항 2.

제 1 항에 있어서,

상기 요청 메시지에는 상기 사용자 개인정보를 사용하고자 하는 목적 정보가 포함되되,

상기 정보 관리 서버는 상기 목적 정보가 기 설정된 목적에 해당하는 경우에 한하여 상기 사용자 개인정보를 검출하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 송신 방법.

청구항 3.

제 2 항에 있어서,

상기 검증 정보는 상기 요청 메시지에 포함된 목적 정보를 포함하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 송신 방법.

청구항 4.

제 1 항에 있어서,

상기 검증 정보는 상기 사용자 개인정보를 사용할 수 있는 기한 정보 및/또는 횟수 정보를 포함하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 송신 방법.

청구항 5.

제 1 항에 있어서,

상기 검증 정보는 상기 클라이언트의 공개키를 포함하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 송신 방법.

청구항 6.

제 1 항에 있어서,

상기 에이전트는 상기 정보 관리 서버에서 상기 클라이언트로 전송되는 소프트웨어 이동 에이전트인 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 송신 방법.

청구항 7.

(a) 클라이언트는 암호화된 사용자 개인정보, 사용자 개인정보의 서명값 및 정당한 클라이언트에게만 사용자 개인정보가 제공되도록 하는 검증 정보를 포함하는 에이전트와 상기 암호화된 사용자 개인정보를 복호화할 수 있는 복호화키를 정보 관리 서버로부터 전송받는 단계;

(b) 상기 클라이언트는 상기 에이전트로 상기 사용자 개인정보를 요청하는 단계;

(c) 상기 에이전트는 상기 검증 정보를 통하여 상기 클라이언트가 상기 사용자 개인정보를 정당하게 이용할 수 있는지 판단하는 단계;

(d) 상기 사용자 개인정보를 정당하게 이용할 수 있다고 판단된 경우에, 상기 에이전트는 상기 암호화된 사용자 개인정보 및 사용자 개인정보 서명값을 상기 클라이언트로 제공하는 단계; 및

(e) 상기 클라이언트는 상기 사용자 개인정보 서명값을 상기 정보 관리 서버의 공개키로 검증하고 검증이 이루어지는 경우에 상기 암호화된 사용자 개인정보를 상기 복호화키로 복호화하여 상기 사용자 개인정보를 추출하는 단계;를 포함하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 수신 방법.

청구항 8.

제 7 항에 있어서,

상기 검증 정보는 상기 사용자 개인정보를 사용하고자 하는 목적 정보를 포함하되,

상기 (b)단계에서 상기 클라이언트는 상기 에이전트로 상기 사용자 개인정보를 사용하고자 하는 목적 정보를 포함하여 요청하고,

상기 (c)단계는 상기 사용자 개인정보를 사용하고자 하는 목적 정보가 동일한지 여부를 통하여 상기 클라이언트가 상기 사용자 개인정보를 정당하게 이용할 수 있는지 판단하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 수신 방법.

청구항 9.

제 7 항에 있어서,

상기 검증 정보는 상기 사용자 개인정보를 사용할 수 있는 기한 정보 및/또는 횟수 정보를 포함하되,

상기 (c)단계는 상기 사용자 개인정보를 사용할 수 있는 기한 및/또는 횟수가 유효한지 여부를 통하여 상기 클라이언트가 상기 사용자 개인정보를 정당하게 이용할 수 있는지 판단하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 수신 방법.

청구항 10.

제 7 항에 있어서,

상기 검증 정보는 상기 클라이언트의 공개키를 더 포함하되,

상기 (c)단계는 상기 클라이언트의 공개키를 이용하여 상기 클라이언트가 상기 사용자 개인정보를 정당하게 이용할 수 있는지 판단하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 수신 방법.

청구항 11.

제 7 항에 있어서,

상기 에이전트는 상기 정보 관리 서버에서 상기 클라이언트로 전송되는 소프트웨어 이동 에이전트인 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 수신 방법.

청구항 12.

사용자 개인정보를 기 저장하고 클라이언트로부터 사용자 개인정보를 요청받아 송신하는 장치에 있어서,

상기 클라이언트로부터 사용자 개인정보를 요청하는 요청 메시지를 입력받아 기 저장되어 있는 사용자 개인정보를 검출하는 정보 검출부;

상기 검출된 사용자 개인정보를 암호화하기 위한 암호화키와 이를 복호화하기 위한 복호화키를 각각 생성하는 키생성부;

상기 검출된 사용자 개인정보를 상기 암호화키로 암호화하고, 암호화된 사용자 개인정보를 서명하는 암호화부;

상기 암호화된 사용자 개인정보와 사용자 개인정보 서명값 및 상기 사용자 개인정보가 정당한 클라이언트에게만 제공되도록 하는 검증 정보를 포함하는 에이전트를 생성하는 에이전트 생성부; 및

상기 클라이언트로부터 상기 요청 메시지를 전송받아 상기 정보 검출부로 출력하고, 상기 생성된 에이전트와 상기 복호화키를 상기 클라이언트로 전송하는 송수신부;를 포함하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 송신 장치.

청구항 13.

제 12 항에 있어서,

상기 요청 메시지에는 상기 사용자 개인정보를 사용하고자 하는 목적 정보가 포함되되,

상기 정보 검출부는 상기 목적 정보가 기 설정된 목적에 해당하는 경우에 한하여 상기 사용자 개인정보를 검출하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 송신 장치.

청구항 14.

제 12 항에 있어서,

상기 검증 정보는 상기 사용자 개인정보를 사용하고자 하는 목적 정보, 상기 사용자 개인정보를 사용할 수 있는 기한 정보, 상기 사용자 개인정보를 사용할 수 있는 횟수 정보 및 상기 클라이언트의 공개키 중 적어도 어느 하나를 포함하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 송신 장치.

청구항 15.

제 12 항에 있어서, 상기 생성된 에이전트는

상기 암호화된 사용자 개인정보, 사용자 개인정보 서명값 및 검증 정보를 저장하고 있는 저장부;

상기 클라이언트로부터 상기 요청 메시지를 입력받고 상기 검증 정보를 통하여 상기 사용자 개인정보를 정당하게 이용할 수 있다고 판단된 경우에 암호화된 사용자 개인정보와 사용자 개인정보 서명값을 검출하는 개인정보 제어부; 및

상기 클라이언트로부터 상기 요청 메시지를 전송받아 상기 개인정보 제어부로 출력하고, 상기 암호화된 사용자 개인정보 및 사용자 개인정보 서명값을 상기 클라이언트로 전송하는 인터페이스부를 포함하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 송신 장치.

청구항 16.

정보 관리 서버로 사용자 개인정보 요청 메시지를 전송하고, 상기 정보 관리 서버로부터 암호화된 사용자 개인정보, 사용자 개인정보 서명값 및 정당한 사용자 개인정보 수신 장치에게만 사용자 개인정보가 제공되도록 하는 검증 정보를 포함하는 에이전트와 상기 암호화된 사용자 개인정보를 복호화할 수 있는 복호화키를 전송받는 송수신부;

상기 전송받은 에이전트로 사용자 개인정보를 요청하고, 상기 에이전트에서 상기 검증 정보를 통하여 상기 사용자 개인정보를 정당하게 이용할 수 있다고 판단된 경우에 상기 에이전트로부터 상기 암호화된 사용자 개인정보를 전송받는 에이전트 인터페이스부; 및

상기 에이전트 인터페이스부를 통하여 전송받은 상기 사용자 개인정보의 서명값을 상기 정보 관리 서버의 공개키로 검증하고, 상기 암호화된 사용자 개인정보를 상기 복호화키로 복호화하여 상기 사용자 개인정보를 추출하는 복호화부;를 포함하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 수신 장치.

청구항 17.

제 16 항에 있어서,

상기 검증 정보는 상기 사용자 개인정보를 사용하고자 하는 목적 정보, 상기 사용자 개인정보를 사용할 수 있는 기한 정보, 상기 사용자 개인정보를 사용할 수 있는 횟수 정보 및 상기 클라이언트의 공개키 중 적어도 어느 하나를 포함하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 수신 장치.

청구항 18.

제 16 항에 있어서, 상기 에이전트는

상기 암호화된 사용자 개인정보, 사용자 개인정보 서명값 및 검증 정보를 저장하고 있는 저장부;

상기 요청 메시지를 입력받고 상기 검증 정보를 통하여 상기 사용자 개인정보를 정당하게 이용할 수 있다고 판단된 경우에 암호화된 사용자 개인정보와 사용자 개인정보 서명값을 검출하는 개인정보 제어부; 및

상기 에이전트 인터페이스부로부터 상기 요청 메시지를 전송받아 상기 개인정보 제어부로 출력하고, 상기 암호화된 사용자 개인정보 및 사용자 개인정보 서명값을 상기 에이전트 인터페이스부로 전송하는 인터페이스부를 포함하는 것을 특징으로 하는 에이전트를 이용한 사용자 개인정보 수신 장치.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 에이전트를 이용한 사용자 개인정보 송수신 방법 및 장치에 관한 것으로, 더욱 상세하게는 사용자 개인정보를 소프트웨어 이동 에이전트에 포함시켜 전송함으로써, 외부의 공격으로부터 사용자 개인정보를 안전하게 전송하고자 하는 에이전트를 이용한 사용자 개인정보 송수신 방법 및 장치에 관한 것이다.

인터넷에서 많은 사이트들은 사용자들에게 서비스를 제공하면서 사용자들에게 등록을 요구하고 있다. 사용자들은 서비스를 이용하기 위해 사이트에 가입할 때, 이름, 주민등록번호, 주소, 전화번호, 전자우편 등 자신의 중요한 개인정보를 입력한다. 사용자들은 너무 많은 사이트에 가입을 하다 보니, 자신의 정보가 어느 곳에 있는지, 어떤 정보를 입력하였는지 기억하기 쉽지 않다. 그리고 인터넷의 수많은 영세 사이트들은 고객의 정보를 관리함에 있어 정보보호 및 프라이버시 보호 문제들을 전혀 고려하고 있지 않다. 심지어 고객의 정보를 불법으로 판매하는 일도 벌어지고 있다.

이러한 환경에서 사용자의 정보를 안전하게 관리하고 유통시키기 위한 기술들이 제안되고 있다. 대표적으로 인터넷 Identity 관리 시스템이 있다. 인터넷 Identity 관리 시스템은 사용자가 인터넷을 사용함에 있어 보다 편하고 안전한 환경을 제공하는 것을 목표로 한다. 즉, 한번의 로그인 과정으로 인터넷의 많은 사이트들을 자유롭게 사용할 수 있는 SSO (Single Sign On) 서비스를 제공하고, 사용자의 정보를 안전한 사이트에 저장함으로써 자신의 정보를 최신의 상태로 유지하고 안전하게 관리할 수 있게 해준다. 이와 관련된 많은 표준과 기술이 개발되고 있다. 대표적으로, OASIS 그룹의 SAML, Liberty Alliance의 ID-FF, ID-WSF, ID-SIS, 그리고 IBM과 Microsoft의 WS-Security가 있다.

또한, 사용자 개인정보를 안전하게 관리하기 위한 표준으로, W3C의 P3P, OASIS의 XACML, IBM의 EPAL 등이 있다.

인터넷 Identity 관리 시스템과 개인정보 기술 외에 본 발명의 핵심이 되는 기술로 소프트웨어 이동 에이전트가 있다. 소프트웨어 에이전트를 한마디로 표현하면 사용자를 대신해서 사용자가 원하는 작업을 자동적으로 해결하여 주는 소프트웨어라고 할 수 있다. 에이전트 기술은 인공지능 분야에서 오래전부터 연구되어 온 개념이다. 80년대 말부터 인공지능과 분리되어 독립적인 연구 주제로 대두되었고, 90년대 중반에 들어서는 인터넷의 등장으로 인해 다양한 형태의 에이전트 기술들이 등장하였다. 인터넷의 정보를 수집하는 정보 검색, 온라인 쇼핑 등의 전자상거래, 메시징과 같은 이동 컴퓨팅 분야에서 에이전트가 활용되고 있다. 에이전트는 서비스 환경에 따라 다양한 형태로 존재할 수 있다. 본 발명에서는 에이전트가 다른 호스트로 이동하여 작업할 수 있는 이동 에이전트이고, 사용자의 정보를 안전하게 보호할 수 있도록 암호화 모듈을 탑재하고 있다.

발명이 이루고자 하는 기술적 과제

상기 종래 기술의 문제점을 해결하기 위한 본 발명은 사용자 개인정보를 인터넷상에서 그대로 전송하는 것이 아니라 사용자 개인정보를 필요로 하는 클라이언트에게 사용자 개인정보를 포함하고 있는 에이전트를 전송하여 사용자 개인정보를 안전하게 전송하고자 하는 사용자 개인정보 송수신 방법 및 장치를 제공한다.

또한, 본 발명은 클라이언트가 불법적으로 타 클라이언트에게 에이전트를 제공하거나, 공격자가 네트워크 상에서 불법적으로 에이전트를 취득하더라도 사용자 개인정보를 취득하지 못하도록 하는 사용자 개인정보 송수신 방법 및 장치를 제공한다.

발명의 구성

상기 기술적 과제를 해결하기 위한 본 발명의 에이전트를 이용한 사용자 개인정보 송신 방법은, (a) 클라이언트로부터 사용자 개인정보를 요청하는 요청 메시지를 전송받은 정보 관리 서버는 상기 사용자 개인정보를 검출하는 단계; (b) 상기 검출된 사용자 개인정보를 암호화하기 위한 암호화키와 이를 복호화하기 위한 복호화키를 각각 생성하는 단계; (c) 상기 검출된 사용자 개인정보를 상기 암호화키로 암호화하고, 암호화된 사용자 개인정보를 서명하는 단계; (d) 상기 암호화된 사용자 개인정보와 암호화된 사용자 개인정보의 서명값 및 상기 사용자 개인정보가 정당한 클라이언트에게만 제공되도록 하는 검증 정보를 포함하는 에이전트를 생성하는 단계; 및 (e) 상기 정보 관리 서버는 상기 생성된 에이전트와 복호화키를 상기 클라이언트로 전송하는 단계;를 포함하는 것을 특징으로 가진다.

상기 기술적 과제를 해결하기 위한 본 발명의 에이전트를 이용한 사용자 개인정보 수신 방법은, (a) 클라이언트는 암호화된 사용자 개인정보, 사용자 개인정보의 서명값 및 정당한 클라이언트에게만 사용자 개인정보가 제공되도록 하는 검증 정보를 포함하는 에이전트와 상기 암호화된 사용자 개인정보를 복호화할 수 있는 복호화키를 정보 관리 서버로부터 전송받는 단계; (b) 상기 클라이언트는 상기 에이전트로 상기 사용자 개인정보를 요청하는 단계; (c) 상기 에이전트는 상기 검증 정보를 통하여 상기 클라이언트가 상기 사용자 개인정보를 정당하게 이용할 수 있는지 판단하는 단계; (d) 상기 사용자 개인정보를 정당하게 이용할 수 있다고 판단된 경우에, 상기 에이전트는 상기 암호화된 사용자 개인정보 및 사용자 개인정보 서명값을 상기 클라이언트로 제공하는 단계; 및 (e) 상기 클라이언트는 상기 사용자 개인정보 서명값을 상기 정보 관리 서버의 공개키로 검증하고 검증이 이루어지는 경우에 상기 암호화된 사용자 개인정보를 상기 복호화키로 복호화하여 상기 사용자 개인정보를 추출하는 단계;를 포함하는 것을 특징으로 가진다.

상기 기술적 과제를 해결하기 위한 본 발명의 에이전트를 이용한 사용자 개인정보 송신 장치는, 사용자 개인정보를 기 저장하고 클라이언트로부터 사용자 개인정보를 요청받아 송신하는 장치에 있어서, 상기 클라이언트로부터 사용자 개인정보를 요청하는 요청 메시지를 입력받아 기 저장되어 있는 사용자 개인정보를 검출하는 정보 검출부; 상기 검출된 사용자 개인정보를 암호화하기 위한 암호화키와 이를 복호화하기 위한 복호화키를 각각 생성하는 키생성부; 상기 검출된 사용자 개인정보를 상기 암호화키로 암호화하고, 암호화된 사용자 개인정보를 서명하는 암호화부; 상기 암호화된 사용자 개인정보와 사용자 개인정보 서명값 및 상기 사용자 개인정보가 정당한 클라이언트에게만 제공되도록 하는 검증 정보를 포함하는 에이전트를 생성하는 에이전트 생성부; 및 상기 클라이언트로부터 상기 요청 메시지를 전송받아 상기 정보 검출부로 출력하고, 상기 생성된 에이전트와 상기 복호화키를 상기 클라이언트로 전송하는 송수신부;를 포함하는 것을 특징으로 가진다.

상기 기술적 과제를 해결하기 위한 본 발명의 에이전트를 이용한 사용자 개인정보 수신 장치는, 정보 관리 서버로 사용자 개인정보 요청 메시지를 전송하고, 상기 정보 관리 서버로부터 암호화된 사용자 개인정보, 사용자 개인정보 서명값 및 정당한 사용자 개인정보 수신 장치에게만 사용자 개인정보가 제공되도록 하는 검증 정보를 포함하는 에이전트와 상기 암호화된 사용자 개인정보를 복호화할 수 있는 복호화키를 전송받는 송수신부; 상기 전송받은 에이전트로 사용자 개인정보를 요청하고, 상기 에이전트에서 상기 검증 정보를 통하여 상기 사용자 개인정보를 정당하게 이용할 수 있다고 판단된 경우에 상기 에이전트로부터 상기 암호화된 사용자 개인정보를 전송받는 에이전트 인터페이스부; 및 상기 에이전트 인터페이스부를 통하여 전송받은 상기 사용자 개인정보의 서명값을 상기 정보 관리 서버의 공개키로 검증하고, 상기 암호화된 사용자 개인정보를 상기 복호화키로 복호화하여 상기 사용자 개인정보를 추출하는 복호화부;를 포함하는 것을 특징으로 가진다.

이하에서, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 대하여 상세히 설명한다.

도 1은 본 발명의 바람직한 일 실시예에 따른 에이전트를 이용한 사용자 개인정보 송수신 시스템에 대한 블럭도이다. 도 1을 참조하면, 에이전트를 이용한 사용자 개인정보 송수신 시스템은 정보 관리 서버(100)와 클라이언트(120)를 포함하여 구성된다.

정보 관리 서버(100)는 사용자 개인정보를 관리하는 서버로써, 사용자 개인정보를 외부의 공격으로부터 안전하게 보관하는 역할을 수행한다.

클라이언트(120)는 정보 관리 서버(100)로 사용자 개인정보를 요청하고 사용자 개인정보를 사용하고자 하는 객체로써, 사용자가 요구하는 서비스를 수행하기 위해서 또는 정책적인 이유 등 다양한 목적(예를 들어, 광고 전송, 사은품 증정, 사용자 통계 등)으로 정보 관리 서버(100)로 사용자 개인정보를 요청하고 전송받은 사용자 개인정보를 사용하는 역할을 수행한다.

정보 관리 서버(100)는 송수신부(101), 정보 검출부(102), 저장부(103), 암호화부(104), 키생성부(105) 및 에이전트 생성부(106)를 포함하여 구성된다.

송수신부(101)의 수신 모듈은 클라이언트(120)로부터 사용자 개인정보를 요청하는 요청 메시지를 수신한다. 여기에서, 사용자 개인정보를 요청하는 요청 메시지에는 사용자 개인정보를 사용하고자 하는 사용 목적 정보가 포함된다.

저장부(103)는 사용자 개인정보를 기 저장하고 있다. 여기에서, 사용자 개인정보를 기 저장하고 있다는 것은 사용자가 정보 관리 서버(100)에 사용자 자신의 개인정보들을 미리 등록하여 관리를 위탁한다는 것을 의미한다. 사용자 개인정보들로는 가신의 주민등록번호, 주소, 전화번호 등 다양한 정보를 포함할 수 있다.

정보 검출부(102)는 송수신부(101)를 통하여 입력받은 요청 메시지를 통하여 저장부(102)에 저장되어 있는 사용자 개인정보를 검출하여 암호화부(104)로 전송한다. 또한, 정보 검출부(102)는 입력받은 요청 메시지에 포함되어 있는 사용 목적 정보를 검출하여 에이전트 생성부(106)로 전송한다.

키생성부(105)는 사용자 개인정보를 암호화하기 위한 암호화키와 암호화된 사용자 개인정보를 복호화하기 위한 복호화키를 생성한다. 키생성부(105)는 생성된 암호화키를 암호화부(104)로 전송하고 복호화키를 송수신부(101)로 전송한다.

암호화부(104)는 정보 검출부(102)로부터 검출된 사용자 개인정보를 입력받고, 키생성부(105)로부터 암호화키를 입력받는다. 그리고, 암호화부(104)는 키생성부(105)로부터 입력받은 암호화키로 정보 검출부(102)로부터 입력받은 검출된 사용자 개인정보를 암호화한다.

또한, 암호화부(104)는 정보 관리 서버(100)의 개인키로 암호화된 사용자 개인정보를 서명한다. 상기와 같은 서명을 하는 이유는 아래에서 설명할 에이전트가 포함하고 있는 사용자 개인정보가 정보 관리 서버(100)의 저장부(103)에 기 저장되어 있는 정당한 사용자 개인정보인지를 증명하기 위한 것이다.

에이전트 생성부(106)는 암호화부(104)로부터 암호화된 사용자 개인정보와 사용자 개인정보 서명값을 입력받고, 정보 검출부(102)로부터 사용자 개인정보를 사용하고자 하는 사용 목적 정보를 입력받는다.

그리고, 에이전트 생성부(106)는 입력받은 암호화된 사용자 개인정보와 사용자 개인정보 서명값을 포함하는 에이전트를 생성한다.

여기에서, 에이전트 생성부(106)에서 생성된 에이전트는 암호화된 사용자 개인정보와 사용자 개인정보 서명값 이외에, 사용자 개인정보를 사용하고자 하는 사용 목적, 사용자 개인정보 사용 기한 및 제한 횟수, 그리고 클라이언트(120)의 공개키를 포함하는 검증 정보를 포함한다.

이와 같이 에이전트에 포함되는 정보들은 사용자의 개인정보가 불법적으로 타 개체에게 노출되는 것을 막기 위함이다. 예를 들어, 네트워크로 전송되는 에이전트를 불법적으로 취득한다던지, 클라이언트(120)가 서버(100)의 허가없이 타 개체에게 에이전트와 복호화키를 제공한다던지 하였을 때, 에이전트가 사용 목적을 확인하고 적법한 클라이언트인지를 인증하고 정보 사용 기한 및 횟수를 제한함으로써 이에 따른 피해를 최소화할 수 있다.

사용 목적은 클라이언트(120)가 개인정보를 제공하기에 앞서 사용 목적을 재확인할 때 사용된다.

개인정보의 사용 기한 및 제한 횟수는 적법하지 않은 객체가 에이전트를 취득하더라도 기한이 만료되거나 제한 횟수를 초과하게 되면 정보를 얻지 못하도록 하기 위해 사용된다. 예를 들어, 개인정보의 사용 기한 및 제한 회수는 "사용자 A의 주민등록번호는 x월 x일 까지만 노출하되 총 3회만 노출되도록 허용한다"와 같은 방식으로 표현될 수 있다.

클라이언트의 공개키는 에이전트가 정보를 요청하는 대상이 적법한 대상인지 인증할 때 사용된다.

또한, 송수신부(101)의 송신 모듈은 에이전트 생성부(106)에서 생성된 에이전트와 키생성부(105)에서 생성된 복호화키를 입력받아 이를 클라이언트(120)로 전송한다. 여기에서, 에이전트와 복호화키는 클라이언트(120)에게 보안 채널 등을 통하여 안전하게 전달되도록 한다.

클라이언트(120)는 송수신부(121), 에이전트 인터페이스부(122) 및 복호화부(123)를 포함하여 구성된다.

송수신부(121)의 송신 모듈은 정보 관리 서버(100)로 사용자 개인정보 요청 메시지를 전송한다. 상기에서 설명한 바와 같이 사용자 개인정보 요청 메시지는 사용자 개인정보를 사용하고자 하는 사용 목적 정보를 포함한다.

또한, 송수신부(121)의 수신 모듈은 정보 관리 서버(100)로부터 에이전트와 복호화키를 전송받는다. 송수신부(121)의 수신 모듈은 전송받은 에이전트를 에이전트 인터페이스부(122)로 출력하고, 전송받은 복호화키를 복호화부(123)로 출력한다.

에이전트 인터페이스부(122)는 입력받은 에이전트에게 사용자 개인정보를 요청하는 요청 메시지를 전송한다. 여기에서, 에이전트에게 요청하는 요청 메시지에는 사용자 개인정보를 사용하고자 하는 목적 정보를 함께 함께 전송한다.

또한, 에이전트 인터페이스부(122)는 요청 메시지를 생성할 때 클라이언트(120)의 개인키로 메시지를 서명하고 그 서명값을 메시지와 함께 에이전트에게 전송한다.

에이전트는 요청 메시지를 분석하여 정당한 요청인지 여부를 판단한다. 요청이 정당하다고 판단되면, 에이전트는 암호화되어 있는 사용자 개인정보와 암호화되어 있는 사용자 개인정보를 서명한 값을 에이전트 인터페이스부(122)에게 제공한다.

에이전트 인터페이스부(122)는 제공받은 정보를 복호화부(123)로 출력한다.

복호화부(123)는 사용자 개인정보 서명값을 정보 관리 서버(100)의 공개키로 검증한다. 여기에서 사용자 개인정보 서명값이 검증된 경우에 송수신부(121)의 수신 모듈로부터 직접 입력받은 복호화키로 암호화된 사용자 개인정보를 복호화하여 사용자 개인정보를 추출한다.

도 2는 도 1의 에이전트 생성부(106)에서 생성된 에이전트를 보다 구체적으로 나타낸 블록도이다. 에이전트(200)는 저장부(201), 개인정보 제어부(202), 인터페이스부(203)를 포함하여 구성된다.

저장부(201)는 암호화된 사용자 개인정보, 암호화된 사용자 개인정보를 정보 관리 서버(100)의 개인키로 서명한 사용자 개인정보 서명값, 클라이언트(120)의 공개키, 개인정보의 사용 목적, 사용 기한 및 제한 횟수를 저장하고 있다.

인터페이스부(203)는 클라이언트의 에이전트 인터페이스부(122)로부터 사용자 개인정보 요청 메시지를 수신한다. 요청 메시지에는 요청하는 사용자 개인정보 항목, 사용자 개인정보를 사용하고자 하는 목적, 클라이언트(120)의 개인키로 요청 메시지를 서명한 값을 포함하고 있다. 인터페이스부(203)는 이러한 정보를 개인정보 제어부(202)로 출력한다.

개인정보 제어부(202)는 요청 메시지에 포함되어 있는 요청하는 사용자 개인정보 항목을 저장부(201)가 포함하고 있는지 확인한다. 그리고 요청 메시지에 포함되어 있는 개인정보 사용 목적이 저장부(201)가 저장하고 있는 사용 목적과 같은지 확인한다. 그리고 요청 메시지가 도착한 시간이 저장부(201)가 저장하고 있는 정보 사용 기한 내에 있는지 확인한다. 그리고 정보를 요청한 총 횟수가 저장부(201)가 저장하고 있는 정보 제한 횟수 내에 있는지 확인한다. 위 모든 과정이 적합하게 판정되면 요청 메시지에 포함되어 있는 사용자 개인정보 서명값을 검증하여 정보 요청자가 적법한 개체인지를 확인한다. 위 모든 과정이 적합하게 판정되면 요청 메시지에 포함되어 있는 요청 메시지 서명값을 클라이언트 공개키로 검증하여 정보 요청자가 적법한 개체인지를 확인한다.

사용자 개인정보 서명값이 검증되면 개인정보 제어부(202)는 암호화된 사용자 개인정보와 이를 서명한 사용자 개인정보 서명값을 인터페이스부(203)로 출력한다.

도 3은 본 발명의 바람직한 일 실시예에 따른 에이전트를 이용한 사용자 개인정보 송신 방법에 대한 흐름도이다.

도 3을 참조하면, 먼저, 정보 관리 서버(도 1의 참조번호 100)는 클라이언트(도 1의 참조번호 120)로부터 사용자 개인정보 요청 메시지를 전송받는다(S300). 여기에서, 사용자 개인정보를 요청하는 요청 메시지에는 사용자 개인정보를 사용하고자 하는 사용 목적 정보가 함께 포함된다.

다음으로, 정보 관리 서버(100)는 단계S300에서 전송받은 사용자 개인정보 요청 메시지에 따른 사용자 개인정보를 검출한다(S310). 여기에서, 사용자 개인정보는 정보 관리 서버(100)에 기 등록되어 있다.

다음으로, 단계S310에서 검출된 사용자 개인정보를 암호화하기 위한 암호화키와 이를 복호화하기 위한 복호화키를 생성한다(S320).

다음으로, 단계S310에서 검출된 사용자 개인정보를 단계S320에서 생성한 암호화키로 암호화한다(S330).

다음으로, 단계S330에서 암호화된 사용자 개인정보를 정보 관리 서버(100) 자신의 개인키로 서명하여 사용자 개인정보 서명값을 생성한다(S340).

다음으로 단계S330에서 암호화된 사용자 개인정보와 단계S340에서 사용자 개인정보 서명값을 포함하는 에이전트를 생성한다(S350). 단계S350에서 생성되는 에이전트는 암호화된 사용자 개인정보와 사용자 개인정보 서명값 외에, 사용자 개인정보를 사용하고자 하는 사용 목적, 사용자 개인정보 사용 기한 및 제한 횟수, 그리고 클라이언트(120)의 공개키로 이루어진 검증 정보를 포함한다.

다음으로, 단계S350에서 생성된 에이전트와 단계S320에서 생성된 복호화키를 클라이언트로 전송한다(S360).

도 4는 본 발명의 바람직한 일 실시예에 따른 클라이언트가 에이전트로부터 사용자 개인정보를 수신하는 방법에 대한 흐름도이다. 도 4를 참조하면, 먼저, 클라이언트(도 1의 참조번호 120)는 정보 관리 서버(도 1의 참조번호 100)로부터 암호화된 사용자 개인정보와 사용자 개인정보 서명값을 포함하는 에이전트 및 복호화키를 전송받는다(S400). 여기에서, 복호화키는 정보 관리 서버(100)에서 암호화키에 의하여 암호화된 사용자 개인정보를 복호화하기 위한 키이다.

다음으로, 에이전트로 사용자 개인정보 요청 메시지를 전송한다(S410).

다음으로, 에이전트는 사용자 개인정보 요청 메시지를 수신한다(S420).

다음으로, 에이전트는 요청 메시지에 포함되어 있는 요청하는 사용자 개인정보 항목을 저장부(도 2의 참조번호 201)가 포함하고 있는지 확인한다. 그리고 요청 메시지에 포함되어 있는 개인정보 사용 목적이 저장부(도 2의 참조번호 201)가 저장하고 있는 사용 목적과 같은지 확인한다. 그리고 요청 메시지가 도착한 시간이 저장부(도 2의 참조번호 201)가 저장하고 있는 정보 사용 기한 내에 있는지 확인한다. 그리고 정보를 요청한 총 횟수가 저장부(도 2의 참조번호 201)가 저장하고 있는 정보 제한 횟수 내에 있는지 확인한다. 상기와 같은 과정이 적합하게 판정되면 사용자 개인정보 요청 메시지에 포함되어 있는 요청 메시지 서명값을 클라이언트 공개키로 검증하여 클라이언트가 적법한 개체인지를 확인한다(S430).

단계S430에서의 결과가 정당하다고 판단되지 않는 경우에는 단계S445로 진행하여 오류메시지를 클라이언트에게 전송한다(S445).

한편, 단계S430에서의 판단결과 사용자 개인정보 요청이 정당하다고 판단되는 경우에는 단계S440으로 진행하여 암호화된 사용자 개인정보와 사용자 개인정보 서명값을 클라이언트에게 전송한다.

다음으로, 클라이언트는 암호화된 사용자 개인정보와 사용자 개인정보 서명값을 수신한다(S450).

다음으로, 사용자 개인정보 서명값을 정보 관리 서버의 공개키를 이용하여 검증한다(S460). 단계S460에서 검증이 되지 않으면 오류메시지를 출력한다(S475).

한편, 단계S460에서 검증 작업을 성공하면, 암호화된 사용자 개인정보를 복호화키로 복호화하여 사용자 개인정보를 추출한다(S480).

본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD_ROM, 자기테이프, 플로피디스크 및 광데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드로 저장되고 실행될 수 있다.

이상에서와 같이 도면과 명세서에서 최적 실시예가 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

발명의 효과

본 발명은 사용자 개인정보를 소프트웨어 이동 에이전트에 포함시켜 전송함으로써, 외부의 공격으로부터 사용자 개인정보를 안전하게 보호하여 사용자 개인정보를 원하는 클라이언트로 전송할 수 있다.

또한, 소프트웨어 이동 에이전트는 사용자 개인정보를 사용하는 대상이 적합한지, 사용 목적 정보가 적합한지 및 사용 요건 정보가 적합한지 등을 확인한 상태에서 정당한 요청이라고 판단되는 경우에만 사용자 개인정보를 클라이언트에게 제공함으로써 사용자 개인정보가 오남용 되지 않도록 할 수 있다.

도면의 간단한 설명

도 1은 본 발명의 바람직한 일 실시예에 따른 에이전트를 이용한 사용자 개인정보 송수신 시스템에 대한 블럭도,

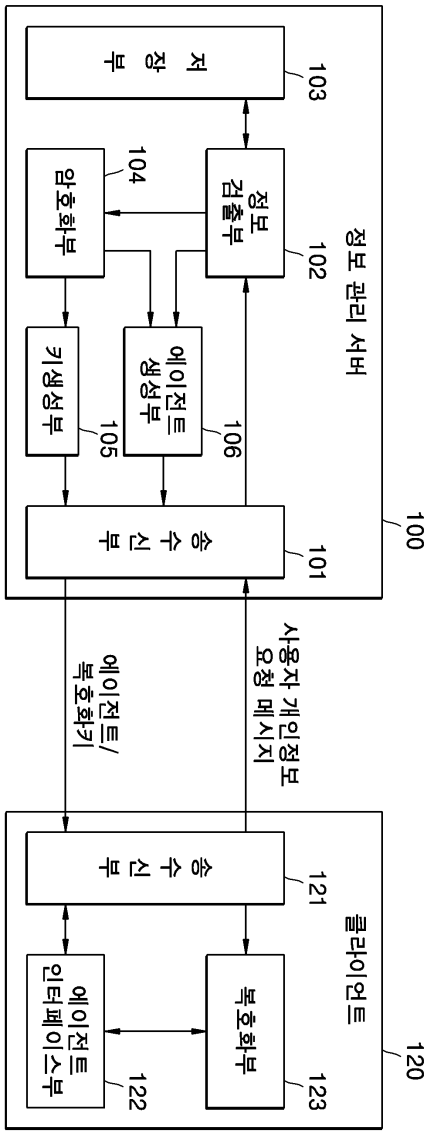
도 2는 도 1의 에이전트 생성부에서 생성된 에이전트를 보다 구체적으로 나타낸 블럭도,

도 3은 본 발명의 바람직한 일 실시예에 따른 에이전트를 이용한 사용자 개인정보 송신 방법에 대한 흐름도 및

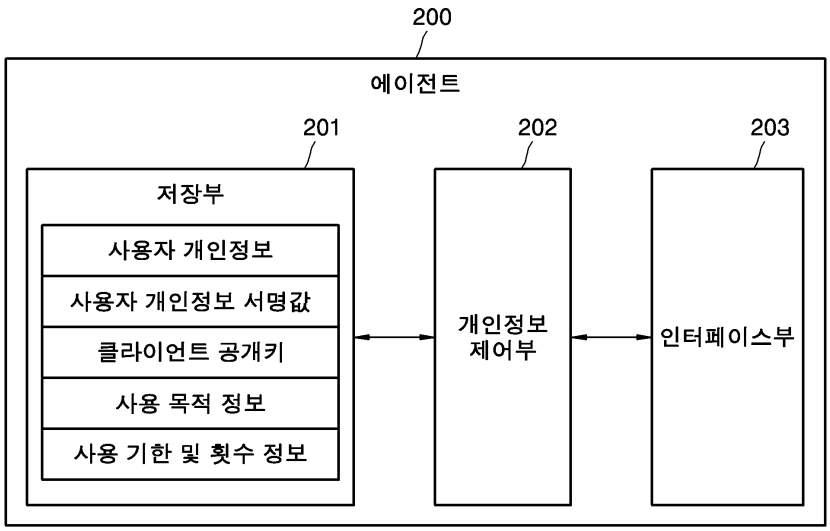
도 4는 본 발명의 바람직한 일 실시예에 따른 에이전트를 이용한 사용자 개인정보 수신 방법에 대한 흐름도이다.

도면

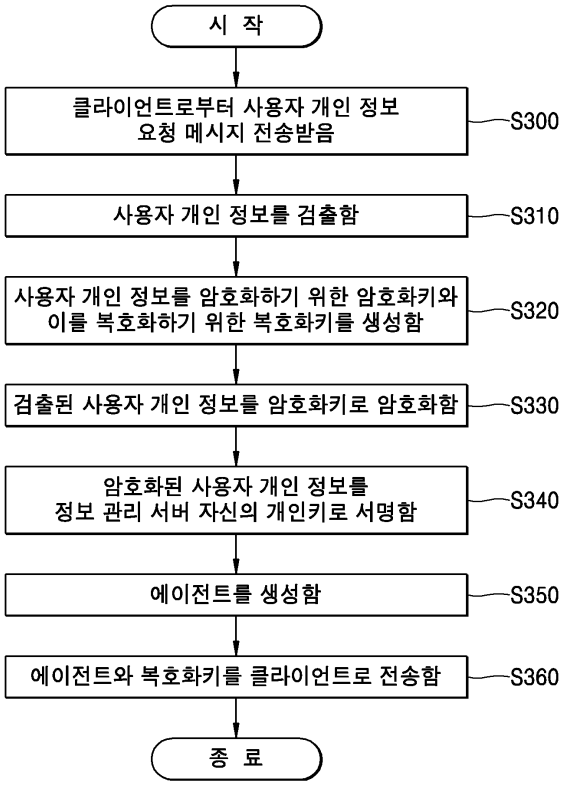
도면1


정보 관리 서버
저장부
103
정보 검출부
102
암호화부
104
키생성부
105
에이전트 생성부
106
송수신부
101
100
에이전트/ 복호화키
사용자 개인정보 요청 메시지
클라이언트
송수신부
121
에이전트 인터페이스부
122
복호화부
123
120

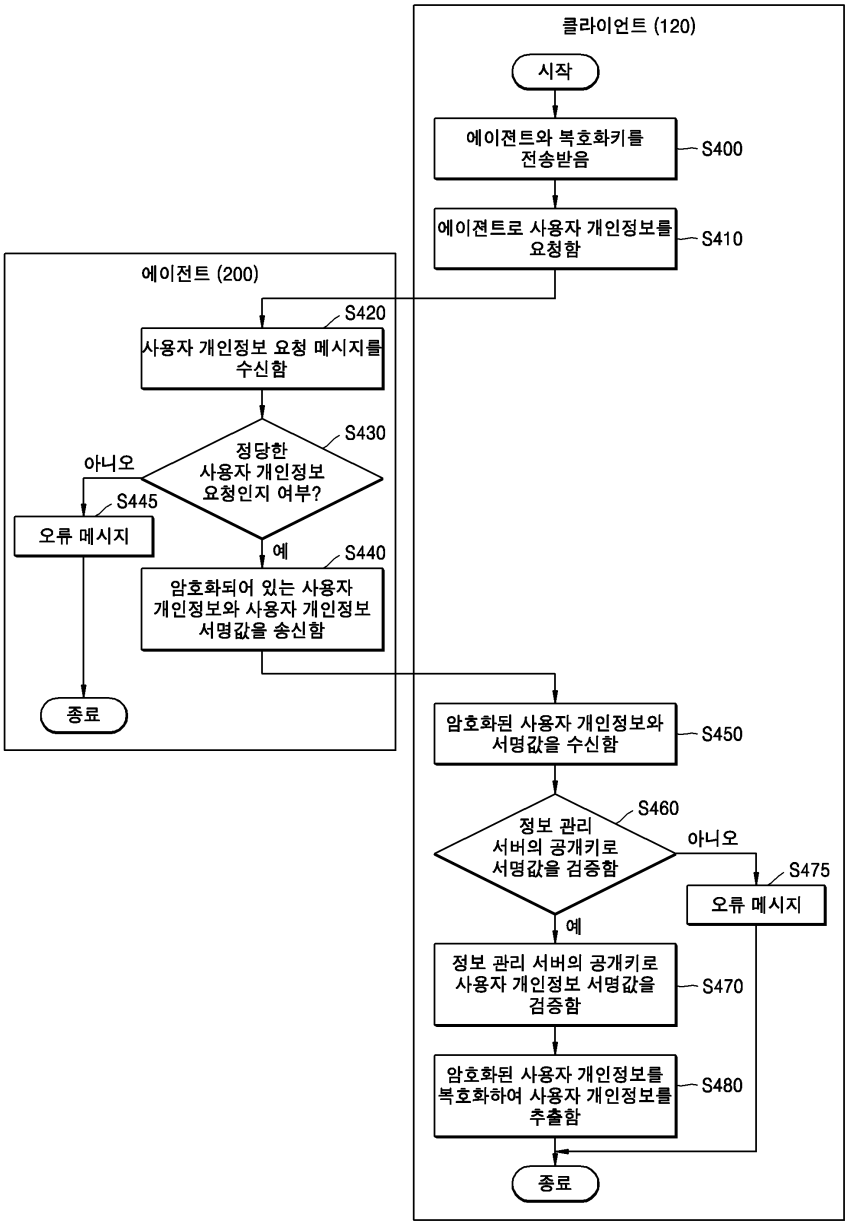
도면2


200
에이전트
201
202
203
저장부
사용자 개인정보
사용자 개인정보 서명값
클라이언트 공개키
사용 목적 정보
사용 기한 및 횟수 정보
개인정보 제어부
인터페이스부

도면3


시 작
클라이언트로부터 사용자 개인 정보 요청 메시지 전송받음
S300
사용자 개인 정보를 검출함
S310
사용자 개인 정보를 암호화하기 위한 암호화키와 이를 복호화하기 위한 복호화키를 생성함
S320
검출된 사용자 개인 정보를 암호화키로 암호화함
S330
암호화된 사용자 개인 정보를 정보 관리 서버 자신의 개인키로 서명함
S340
에이전트를 생성함
S350
에이전트와 복호화키를 클라이언트로 전송함
S360
종 료

도면4


클라이언트 (120)
시작
에이젼트와 복호화키를 전송받음
S400
에이젼트로 사용자 개인정보를 요청함
S410
에이전트 (200)
S420
사용자 개인정보 요청 메시지를 수신함
S430
정당한 사용자 개인정보 요청인지 여부?
아니오
S445
오류 메시지
예
S440
암호화되어 있는 사용자 개인정보와 사용자 개인정보 서명값을 송신함
종료
암호화된 사용자 개인정보와 서명값을 수신함
S450
S460
정보 관리 서버의 공개키로 서명값을 검증함
아니오
S475
오류 메시지
예
정보 관리 서버의 공개키로 사용자 개인정보 서명값을 검증함
S470
암호화된 사용자 개인정보를 복호화하여 사용자 개인정보를 추출함
S480
종료