(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0009301
(43) 공개일자 2010년01월27일

(51) Int. Cl.
H04L 9/14 (2006.01) *H04L 9/00* (2006.01)
(21) 출원번호 10-2008-0070139
(22) 출원일자 2008년07월18일
심사청구일자 2008년07월18일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가1 고려대학교 내
(72) 발명자
이동훈
서울특별시 종로구 내수동 72 경희궁의아침3단지 아파트 1404호
임종인
서울 종로구 내수동 95 삼성파크팰리스 101-901
(뒷면에 계속)
(74) 대리인
현종철

전체 청구항 수 : 총 17 항

(54) 모바일 기기에서의 통합형 데이터 관리 방법, 그 장치 및이를 기록한 기록 매체

(57) 요 약

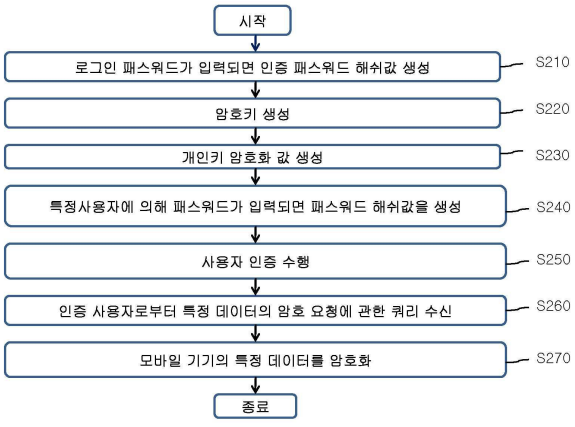
모바일 기기에서의 통합형 데이터 관리 방법, 그 장치 및 이를 기록한 기록 매체가 개시된다.

본 발명에 따른 모바일 기기에서의 통합형 데이터 관리 방법은,

인증 사용자에 의해 고유의 로그인 패스워드가 모바일 기기에 입력되면, 상기 로그인 패스워드, 상기 인증 사용자에 의해 미리 설정된 이터레이션(iteration) 값, 및 제 1 솔트(salt)값을 입력값으로 하여 해쉬 연산에 의해 인증 패스워드 해쉬값을 생성하고, 상기 모바일 기기의 단말 데이터베이스에 저장하는 단계; 상기 로그인 패스워드, 상기 이터레이션 값 및 제 2 솔트값을 이용하여 암호키를 생성하는 단계; 상기 인증 사용자의 모바일 기기에서 랜덤 생성된 비밀키를 상기 생성된 암호키를 이용하여 암호화함으로써 비밀키 암호화값을 생성하여 상기 단말 데이터베이스에 저장하는 단계; 특정 사용자에 의해 패스워드가 입력되면, 상기 이터레이션 값, 상기 제 1 솔트값을 이용하여 패스워드 해쉬값을 생성하고, 상기 인증 패스워드 해쉬값과 비교하여 사용자 인증을 수행하는 단계; 및 상기 인증 사용자로부터 특정 데이터의 암호 요청에 관한 쿼리를 수신하면, 상기 단말 데이터베이스에 저장된 상기 비밀키 암호화값을 복호화하여 상기 비밀키를 추출하고, 상기 추출된 비밀키를 이용하여 상기 모바일 기기의 특정 데이터를 암호화하는 단계를 포함한다.

본 발명에 의하면, 모바일 기기, 어플리케이션, OS/Platform 및 저장 장치의 종류에 독립적인 통합적 데이터 관리 구조를 제공할 수 있으며, 응용프로그램이 아닌 보안 플랫폼 구조 자체에 따라 모바일 기기에서 안전한 통합형 데이터 관리 구조를 제공함으로써, 기기의 도난, 분실, 인증되지 않은 사용자로부터의 접근, 각종 해킹, 악성코드로부터의 노출 등의 보안 위협으로부터 향상된 보안성을 제공할 수 있는 효과가 있다.

대 표 도 - 도2



(72) 발명자

김범한

서울 송파구 방이1동 130-16호 201호

이준호

서울특별시 강남구 논현동 160-15

백정하

서울 송파구 가락동 금호아파트 105동 802호

김현철

서울특별시 은평구 신사2동 현대아파트 103동 1501호

김윤규

경기도 용인시 처인구 김량장동 337-1번지 청광가든빌리지 2차108호

특허청구의 범위

청구항 1

인증 사용자에 의해 고유의 로그인 패스워드가 모바일 기기에 입력되면, 상기 로그인 패스워드, 상기 인증 사용자에 의해 미리 설정된 이터레이션(iteration) 값, 및 제 1 솔트(salt)값을 입력값으로 하여 해쉬 연산에 의해 인증 패스워드 해쉬값을 생성하고, 상기 모바일 기기의 단말 데이터베이스에 저장하는 단계;

상기 로그인 패스워드, 상기 이터레이션 값 및 제 2 솔트값을 이용하여 암호키를 생성하는 단계;

상기 인증 사용자의 모바일 기기에서 랜덤 생성된 비밀키를 상기 생성된 암호키를 이용하여 암호화함으로써 비밀키 암호화값을 생성하여 상기 단말 데이터베이스에 저장하는 단계;

특정 사용자에 의해 패스워드가 입력되면, 상기 이터레이션 값, 상기 제 1 솔트값을 이용하여 패스워드 해쉬값을 생성하고, 상기 인증 패스워드 해쉬값과 비교하여 사용자 인증을 수행하는 단계; 및

상기 인증 사용자로부터 특정 데이터의 암호 요청에 관한 쿼리를 수신하면, 상기 단말 데이터베이스에 저장된 상기 비밀키 암호화값을 복호화하여 상기 비밀키를 추출하고, 상기 추출된 비밀키를 이용하여 상기 모바일 기기의 특정 데이터를 암호화하는 단계를 포함하는 모바일 기기에서의 통합형 데이터 관리 방법.

청구항 2

제 1 항에 있어서,

상기 특정 데이터를 암호화하는 단계는

상기 추출된 비밀키에 따라 암호화된 특정 데이터가 상기 인증 사용자의 요청에 의해 로드되면, 상기 인증 사용자의 로그인 패스워드 입력에 따라 상기 암호키를 생성하는 단계; 및

상기 생성된 암호키를 이용하여 상기 암호화된 특정 데이터를 복호화하는 단계를 더 포함하는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 방법.

청구항 3

제 2 항에 있어서,

상기 특정 데이터의 암호화 및 복호화는

128, 192 또는 256 비트의 에이티에스(AES) 암호화 알고리즘 및 피비이(PBE) 암호화 알고리즘에 의해 수행되는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 방법.

청구항 4

제 1 항에 있어서,

상기 암호키를 생성하는 단계는

상기 로그인 패스워드, 상기 이터레이션 값 및 상기 제 2 솔트값을 입력값으로 하여 해쉬 연산을 수행하는 단계; 및

상기 해쉬 연산의 결과값의 MSB 16바이트(byte)를 취하여 상기 암호키를 생성하는 단계를 포함하는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 방법.

청구항 5

제 4 항에 있어서,

상기 암호키는

하기의 식 1에 의해 생성되는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 방법.

$$KEK = H^{iteration}(password \parallel salt_2) \quad (1)$$

(단, KEK는 암호키이고, $iteration$은 이터레이션 값이며, $password$가 로그인 패스워드이며, $salt_2$는 제 2 솔트값임.)

청구항 6

제 1 항에 있어서,

상기 사용자 인증을 수행하는 단계는

상기 패스워드 해쉬값과 상기 인증 패스워드 해쉬값이 동일하면 사용자 인증을 수행하는 단계; 및

상기 패스워드 해쉬값과 상기 인증 패스워드 해쉬값이 동일하지 않을 경우, 사용자 인증이 실패된 것으로 판단하여 상기 패스워드 해쉬값을 삭제하는 단계를 포함하는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 방법.

청구항 7

제 1 항에 있어서,

상기 모바일 기기의 특정 데이터는

캐쉬(cache) 정보, 상기 모바일 기기의 파일 시스템의 각각의 정보 및 상기 인증 사용자의 입력에 의해 생성된 텍스트 정보를 포함하는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 방법.

청구항 8

제 1 항에 있어서,

상기 모바일 기기는

휴대폰, 스마트폰, 피디에이(Personal Data Assistant:PDA) 및 네비게이션 중에서 선택된 어느 하나를 포함하는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 방법.

청구항 9

제 1 항 내지 제 8 항 중 어느 한 항의 방법을 컴퓨터에서 수행할 수 있도록 프로그램으로 기록된 기록 매체.

청구항 10

인증 사용자로부터 입력 데이터를 수신받고, 상기 인증 사용자의 쿼리에 의해 생성된 정보를 출력하도록 하는 사용자 인터페이스를 제공하는 사용자 계층;

상기 사용자 계층에 입력된 상기 인증 사용자의 입력 데이터에 의해 암호화 및 복호화를 수행하는 관리 계층; 및

상기 인증 사용자의 모바일 기기의 어플리케이션에서 생성된 데이터, 상기 사용자 계층 및 상기 관리 계층에서 생성된 데이터를 저장하는 모바일 기기의 단말 데이터베이스를 포함하고,

상기 사용자 계층은

상기 인증 사용자로부터 로그인 패스워드를 수신하고, 특정 사용자로부터 인증을 위한 패스워드를 수신하는 패스워드 수신부; 및

상기 인증 사용자 고유의 비밀키를 생성하는 비밀키 생성부를 포함하고,

상기 관리 계층은

상기 로그인 패스워드, 상기 인증사용자에 의해 미리 설정된 이티레이션(iteration) 값, 및 제 1 솔트(salt)값을 입력값으로 하여 해쉬 연산에 의해 인증 패스워드 해쉬값을 생성하는 인증 패스워드 해쉬값 생성부;

특정 사용자에 의해 상기 패스워드 수신부에 패스워드가 입력되면, 상기 이티레이션 값, 상기 제 1 솔트값을 이용하여 패스워드 해쉬값을 생성하고, 상기 인증 패스워드 해쉬값과 비교하여 사용자 인증을 수행하는 인증부;

상기 로그인 패스워드, 상기 이터레이션 값 및 제 2 솔트값을 이용하여 암호키를 생성하는 암호키 생성부;

상기 비밀키를 상기 암호키를 이용하여 암호화함으로써 비밀키 암호화값을 생성하는 비밀키 암호화값 생성부; 및

상기 인증 사용자로부터 특정 데이터의 암호 요청에 관한 쿼리를 수신하며, 상기 단말 데이터베이스에 저장되는 상기 비밀키 암호화값을 복호화하여 상기 비밀키를 추출하고, 상기 추출된 비밀키를 이용하여 상기 모바일 기기의 특정 데이터를 암호화하는 데이터 암호화부를 포함하는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 장치.

청구항 11

제 10 항에 있어서,

상기 관리 계층은

상기 비밀키에 따라 암호화된 특정 데이터가 상기 인증 사용자의 쿼리에 의해 로드되면, 상기 인증 사용자의 로그인 패스워드 입력에 따라 상기 암호키를 생성하고, 상기 생성된 암호키를 이용하여 상기 암호화된 특정 데이터를 복호화하는 데이터 복화화부를 더 포함하는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 장치.

청구항 12

제 11 항에 있어서,

상기 관리 계층은

128, 192 또는 256 비트의 에이티에스(AES) 암호화 알고리즘 및 피비이(PBE) 암호화 알고리즘에 따라 암호화 또는 복호화를 수행하는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 장치.

청구항 13

제 10 항에 있어서,

상기 암호키 생성부는

상기 로그인 패스워드, 상기 이터레이션 값 및 상기 제 2 솔트값을 입력값으로 하여 해쉬 연산을 수행하고, 상기 해쉬 연산의 결과값의 MSB 16바이트(byte)를 취하여 상기 암호키를 생성하는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 장치.

청구항 14

제 13 항에 있어서,

상기 암호키는

하기의 식 2에 의해 생성되는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 장치.

$$KEK = H^{iteration}(password \parallel salt_2) \quad (2)$$

(단, KEK는 암호키이고, $iteration$은 이터레이션 값이며, $password$가 로그인 패스워드이며, $salt_2$는 제 2 솔트값임.)

청구항 15

제 10 항에 있어서,

상기 인증부는

상기 패스워드 해쉬값과 상기 인증 패스워드 해쉬값이 동일하면 사용자 인증을 수행하고, 상기 패스워드 해쉬값과 상기 인증 패스워드 해쉬값이 동일하지 않을 경우, 사용자 인증이 실패된 것으로 판단하여 상기 패스워드 해

쉬값을 삭제하는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 장치.

청구항 16

제 10 항에 있어서,

상기 모바일 기기의 특정 데이터는

캐쉬(cache) 정보, 상기 모바일 기기의 파일 시스템의 각각의 정보 및 상기 인증 사용자의 입력에 의해 생성된 텍스트 정보를 포함하는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 장치.

청구항 17

제 10 항에 있어서,

상기 모바일 기기는

휴대폰, 스마트폰, 피디에이(Personal Data Assistant:PDA) 및 네비게이션 중에서 선택된 어느 하나를 포함하는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 장치.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 모바일 기기에서의 데이터 관리에 관한 것으로서, 특히 모바일 기기의 데이터에 물리적인 접근뿐만 아니라, 네트워크를 통한 통합 침투에 대하여 안전하면서도 통합적인 데이터 관리 기법인 모바일 기기에서의 통합형 데이터 관리 방법, 그 장치 및 이를 기록한 기록 매체에 관한 것이다.

배 경 기 술

<2> 최근 정보화 시대가 도래하면서, 휴대폰의 기능은 전화를 걸기 위한 목적 이외에 부가적인 기능으로서 그 위치를 자리 잡기 시작했으며, 현대를 살아가는 사람들에게 없어서는 안될 필수품이 되었다. 바로 인터넷이 가지고 있는 장점을 살리면서도 또 하나의 새로운 산업적, 문화적인 가치를 만들어 나가고 있는 것이다.

<3> 현재 모바일 기기에서 가능한 서비스로는 이메일 서비스, 위치 정보 서비스, 게임 서비스, 무선 금융 서비스, 무선 전자 상거래, 무선 정보 서비스 등 다양하다.

<4> 그러나, 향후 이보다 많은 서비스가 실현될 것으로 보이며, 현재 유선 인터넷으로 가능한 모든 서비스는 모바일 기기에서 그대로 실현되고 있는 실정이다.

<5> 더욱이, 최근 몇 년 동안 컴퓨터의 초소형화 및 무선 통신의 범용화에 따른 유비쿼터스 환경이 급격히 발전하고 있다.

<6> 핸드폰, PDA(Personal Digital Assistants), 스마트폰의 판매 수는 급증되고 있으며, 이 모바일 기기들은 다양한 어플리케이션과 저장 인터페이스를 갖추고 있어 여러 가지 정보 노출의 가능성이 열려 있는 실정이다.

<7> 한편, 유비쿼터스 환경에서의 사용자들은 다양하고 통합적인 서비스를 이용하기를 원하고 있으며, 이를 위하여 다양한 데이터의 저장 및 관리는 필수적인 요소이다.

<8> 이러한 다양한 데이터들 중에는 민감한 정보들도 많이 존재하게 되어 유비쿼터스 환경에서 사용자 데이터의 안전한 관리가 중요한 요소로 부각되고 있다.

<9> 최근에는 핸드폰뿐만 아니라 PDA나 스마트폰의 사용자가 급증하면서 모바일 기기에 저장되어 있는 데이터 유출의 위험성이 점점 증가하고 있는 추세이다.

<10> 또한 모바일 기기의 크기가 점점 작아지고 경량화되면서 분실 및 도난의 위험성이 커지고 있으며, 기기에 저장된 개인 정보가 유출되어 범죄에 악용될 우려가 커지고 있다.

<11> 실제로, 모바일 기기내에는 사용자의 다양한 개인정보(주민등록번호, 금융 거래 정보, 일정, 주소록, 메일, 메모 뿐만 아니라, 기업의 망에 연결하여 이용할 경우 기업 내부의 기밀정보도 저장되어 있으므로 데이터의 관리

는 반드시 필요한 요소이다.

<12> 현재, 대부분의 모바일 기기들은 데이터를 저장할 때에 기본적으로 암호화를 하지 않고 있으며, 핸드폰의 경우에 문자 메시지를 인코딩하여 저장하는 경우 외에는 데이터를 곧 바로 저장장치에 저장한다.

<13> 그 중에서도 일부 모델만 인코딩을 적용할 뿐이고, 인코딩 방식을 알아내는 것 또한 그리 어려운 문제가 아니다.

<14> 이런 데이터를 제3자가 접근하지 못하게 하기 위하여, 보통 패스워드를 통하여 접근 제한 기능을 제공하지만 일반적으로 패스워드가 네자리 이고, 숫자 입력만 지원하기 때문에 전수 조사로 쉽게 패스워드를 알아내는 것이 가능하다.

<15> 또한, 패스워드를 알아낼 수 없는 환경이라 하더라도, 조인트 테스트 액션 그룹(Joint Test Action Group:JTAG)과 같은 하드웨어적인 방법이나, 퀄컴 프러덕트 서포트 툴(Qualcomm Product Support Tool:QPST)와 같은 소프트웨어 적인 방법으로 모바일 기기 내부의 데이터를 추출하는 것이 가능하기 때문에 데이터가 원본 그대로 저장되어 있다면 정보의 유출은 쉽게 이루어질 수 있다.

<16> 더군다나, 이런 모바일 기기들이 기업의 업무에 사용될 경우에 기업의 고객 정보, 기밀 문서 등이 유출되면 기업의 경제적인 손실 및 이미지 실추로 인하여 큰 타격이 예상된다.

<17> 이와 같은 하기의 표 1은 모바일 기기에 대한 위협과 공격으로 인한 소요 비용들을 정리한 것이다.

표 1

개인	· 감염된 핸드셋의 환불 보증 · 감염된 장치로 인한 시장 평판 손상
기업	· 영업권 상실, 고객 불만족, 고객 이탈 증가 · 장치의 바이러스 감염으로 인한 과금 가능 시간 손실 · 바이러스 감염으로 인한 고객 서비스 요청 · 서비스 중단
모바일 사업자	· 직원 생산성 손실 · 치료 비용 · 데이터/개인 정보 손실 위험 · 인트라넷 감염으로 기업 생산성 저하 · 감염으로 인해 발생된 메시지/전화에 대한 MMS 또는 SMS 비용을 돌려받는데 시간 허비
핸드셋 제조업체	· 사용할 수 없는 장치 · 생산성 손실 · 데이터/개인 정보 손실 위험 · 장치를 제거하거나 수리를 받기 위해 반환해야 하는 번거로움 · 감염으로 인해 발생된 메시지/전화에 대한 MMS 또는 SMS 비용을 돌려받아야 하는 번거로움

<18>

<19> 현재, 모바일 기기들은 데이터를 저장할 때에 내부의 메모리에 저장을 하거나, 모바일용 데이터베이스에 저장을 하고 옵션으로 외부의 저장 장치를 따로 두는 방식을 취하고 있다.

<20> 또한, 접근 제어 방식으로 사용자가 패스워드를 설정해 놓아 모바일 기기 자체에 잠금 설정을 할 수도 있다.

<21> 이러한 잠금 기능을 통하여 원하지 않는 사용자로부터 데이터 접근을 제한한다.

<22> 그러나, 이러한 패스워드를 통한 접근 제한은 큰 문제점이 있다. 일단 가장 큰 문제점은 패스워드가 4자리로 제한되어 있고, 숫자만을 패스워드로 입력받기 때문에 전수조사로 쉽게 파악될 수 있다.

<23> 그러므로, 패스워드를 알아내기만 한다면 내부의 데이터는 바로 공개가 되어 버린다.

<24> 또한, 패스워드를 전수조사로 알아낼 수 없는 상황이라 할지라도, 내부의 메모리를 추출하는 도구를 통하여 데이터의 추출이 가능하다면 내부의 데이터는 공개가 되어 버린다.

<25> 여기서, 가장 큰 문제점은 데이터를 원본 그대로 메모리나 데이터베이스에 저장한다는 점에 있다.

<26> 또한, 모바일 기기의 사용이 높아져 가면서 모바일 기기내의 저장 정보는 해커와 악성 코드 사용자들의 새로운

공격대상으로 떠오르고 있다.

<27> 2004년 6월 처음 발견된 카비르 웜은 자기 복제와 네트워크를 통해 전파되는 최초의 웜 형태의 악성코드로, 삼성, 노키아, 지멘스, 소니에릭슨 등의 생산한 스마트 폰에 사용되는 심비안 운영체제에 침투하여 단말기 전원을 켤때마다 액정화면에 'Caribe'라는 메시지를 보이게 하며, 이는 주로 근거리 무선통신규격인 블루투스(Bluetooth)를 이용하여 전염된다.

<28> 이외에도, 전 세계적으로 다양한 모바일 악성코드가 보고되고 있다.

<29> 도 1은 다양한 경로의 모바일 기기의 감염 경로를 도시하고 있다. 이러한 모바일 기기에 대한 위협과 공격은 핸드셋 제조업체, 모바일 사업자, 기업, 개인 등에게 상당한 비용의 위험을 초래할 수 있다. 이와 같이, 모바일 기기의 데이터에 물리적인 접근 뿐만 아니라, 네트워크를 통한 침투도 일어나고 있기 때문에 데이터를 저장하고 관리하는데 있어서 새로운 구조를 가지는 프라이버시 보호 아키텍처가 필요하다.

<30> 즉, 종래의 휴대 단말에서의 프라이버시 보호 방법은 단말 내부의 관리 프로그램을 응용한 것으로, 기존의 솔루션 제품들은 보통 클라이언트 서버 모델로 중앙 집중식 관리 모델이어서 내부 관리자의 해킹 위험이 있고, 단일 응용 프로그램이 아닌 보안 플랫폼 아키텍처는 암호화 기능을 제공하는 모바일 데이터베이스거나 단말 위에 올라가는 보안 솔루션 응용프로그램으로 모바일 기기의 데이터에 물리적인 접근 뿐만 아니라, 네트워크를 통한 침투도 일어나고 있기 때문에 데이터를 저장하고 관리하는데 있어서 모바일 기기에 개인 프라이버시 보호에 문제가 있다.

발명의 내용

해결 하고자하는 과제

<31> 따라서, 본 발명이 해결하고자 하는 첫 번째 과제는 단말 내부의 온 디바이스 보안 아키텍처를 제공하여 단말기 자체적으로 독립적인 보안환경을 제공할 수 있는 모바일 기기에서의 통합형 데이터 관리 방법을 제공하는 것이다.

<32> 본 발명이 해결하고자 하는 두 번째 과제는 상기 모바일 기기에서의 통합형 데이터 관리 방법을 적용한 모바일 기기에서의 통합형 데이터 관리 장치를 제공하는 것이다.

<33> 그리고 본 발명이 해결하고자 하는 세 번째 과제는 상기 모바일 기기에서의 통합형 데이터 관리 방법을 컴퓨터에서 수행할 수 있도록 프로그램으로 기록된 기록매체를 제공하는 것이다.

과제 해결수단

<34> 상기 첫 번째 과제를 해결하기 위하여 본 발명은,

<35> 인증 사용자에 의해 고유의 로그인 패스워드가 모바일 기기에 입력되면, 상기 로그인 패스워드, 상기 인증 사용자에 의해 미리 설정된 이터레이션(iteration) 값, 및 제 1 솔트(salt)값을 입력값으로 하여 해쉬 연산에 의해 인증 패스워드 해쉬값을 생성하고, 상기 모바일 기기의 단말 데이터베이스에 저장하는 단계; 상기 로그인 패스워드, 상기 이터레이션 값 및 제 2 솔트값을 이용하여 암호키를 생성하는 단계; 상기 인증 사용자의 모바일 기기에서 랜덤 생성된 비밀키를 상기 생성된 암호키를 이용하여 암호화함으로써 비밀키 암호화값을 생성하여 상기 단말 데이터베이스에 저장하는 단계; 특정 사용자에 의해 패스워드가 입력되면, 상기 이터레이션 값, 상기 제 1 솔트값을 이용하여 패스워드 해쉬값을 생성하고, 상기 인증 패스워드 해쉬값과 비교하여 사용자 인증을 수행하는 단계; 및 상기 인증 사용자로부터 특정 데이터의 암호 요청에 관한 쿼리를 수신하면, 상기 단말 데이터베이스에 저장된 상기 비밀키 암호화값을 복호화하여 상기 비밀키를 추출하고, 상기 추출된 비밀키를 이용하여 상기 모바일 기기의 특정 데이터를 암호화하는 단계를 포함하는 모바일 기기에서의 통합형 데이터 관리 방법을 제공한다.

<36> 여기서, 상기 특정 데이터를 암호화하는 단계는 상기 추출된 비밀키에 따라 암호화된 특정 데이터가 상기 인증 사용자의 요청에 의해 로드되면, 상기 인증 사용자의 로그인 패스워드 입력에 따라 상기 암호키를 생성하는 단계; 및 상기 생성된 암호키를 이용하여 상기 암호화된 특정 데이터를 복호화하는 단계를 더 포함할 수 있다.

<37> 그리고, 상기 특정 데이터의 암호화 및 복호화는 128, 192 또는 256 비트의 에이티에스(AES) 암호화 알고리즘 및 피비이(PBE) 암호화 알고리즘에 의해 수행되는 것을 특징으로 한다.

<38> 아울러, 상기 암호키를 생성하는 단계는 상기 로그인 패스워드, 상기 이티레이션 값 및 상기 제 2 솔트값을 입력값으로 하여 해쉬 연산을 수행하는 단계; 및 상기 해쉬 연산의 결과값의 MSB 16바이트(byte)를 취하여 상기 암호키를 생성하는 단계를 포함할 수 있다.

<39> 또한, 상기 암호키는 KEK는 암호키이고, $iteration$은 이티레이션 값이며, $password$가 로그인 패스워드이며, $salt_2$는 제 2 솔트값일 때, 수학식 $KEK = H^{iteration}(password \| salt_2)$에 의해 생성될 수 있다.

<40> 한편, 상기 사용자 인증을 수행하는 단계는 상기 패스워드 해쉬값과 상기 인증 패스워드 해쉬값이 동일하면 사용자 인증을 수행하는 단계; 및 상기 패스워드 해쉬값과 상기 인증 패스워드 해쉬값이 동일하지 않을 경우, 사용자 인증이 실패된 것으로 판단하여 상기 패스워드 해쉬값을 삭제하는 단계를 포함할 수 있다.

<41> 그리고, 상기 모바일 기기의 특정 데이터는 캐쉬(cache) 정보, 상기 모바일 기기의 파일 시스템의 각각의 정보 및 상기 인증 사용자의 입력에 의해 생성된 텍스트 정보를 포함할 수 있다.

<42> 한편, 상기 모바일 기기는 휴대폰, 스마트폰, 피디에이(Personal Data Assistant:PDA) 및 네비게이션 중에서 선택된 어느 하나를 포함할 수 있다.

<43> 상기 두 번째 과제를 해결하기 위하여 본 발명은,

<44> 인증 사용자로부터 입력 데이터를 수신받고, 상기 인증 사용자의 쿼리에 의해 생성된 정보를 출력하도록 하는 사용자 인터페이스를 제공하는 사용자 계층; 상기 사용자 계층에 입력된 상기 인증 사용자의 입력 데이터에 의해 암호화 및 복호화를 수행하는 관리 계층; 및 상기 인증 사용자의 모바일 기기의 어플리케이션에서 생성된 데이터, 상기 사용자 계층 및 상기 관리 계층에서 생성된 데이터를 저장하는 모바일 기기의 단말 데이터베이스를 포함하고, 상기 사용자 계층은 상기 인증 사용자로부터 로그인 패스워드를 수신하고, 특정 사용자로부터 인증을 위한 패스워드를 수신하는 패스워드 수신부; 및 상기 인증 사용자 고유의 비밀키를 생성하는 비밀키 생성부를 포함하고, 상기 관리 계층은 상기 로그인 패스워드, 상기 인증사용자에 의해 미리 설정된 이티레이션(iteration) 값, 및 제 1 솔트(salt)값을 입력값으로 하여 해쉬 연산에 의해 인증 패스워드 해쉬값을 생성하는 인증 패스워드 해쉬값 생성부; 특정 사용자에 의해 상기 패스워드 수신부에 패스워드가 입력되면, 상기 이티레이션 값, 상기 제 1 솔트값을 이용하여 패스워드 해쉬값을 생성하고, 상기 인증 패스워드 해쉬값과 비교하여 사용자 인증을 수행하는 인증부; 상기 로그인 패스워드, 상기 이티레이션 값 및 제 2 솔트값을 이용하여 암호키를 생성하는 암호키 생성부; 상기 비밀키를 상기 암호키를 이용하여 암호화함으로써 비밀키 암호화값을 생성하는 비밀키 암호화값 생성부; 및 상기 인증 사용자로부터 특정 데이터의 암호 요청에 관한 쿼리를 수신하며, 상기 단말 데이터베이스에 저장되는 상기 비밀키 암호화값을 복호화하여 상기 비밀키를 추출하고, 상기 추출된 비밀키를 이용하여 상기 모바일 기기의 특정 데이터를 암호화하는 데이터 암호화부를 포함하는 것을 특징으로 하는 모바일 기기에서의 통합형 데이터 관리 장치를 제공한다.

<45> 또한, 상기 관리 계층은 상기 비밀키에 따라 암호화된 특정 데이터가 상기 인증 사용자의 쿼리에 의해 로드되면, 상기 인증 사용자의 로그인 패스워드 입력에 따라 상기 암호키를 생성하고, 상기 생성된 암호키를 이용하여 상기 암호화된 특정 데이터를 복호화하는 데이터 복화화부를 더 포함할 수 있다.

<46> 아울러, 상기 관리 계층은 128, 192 또는 256 비트의 에이티에스(AES) 암호화 알고리즘 및 피비이(PBE) 암호화 알고리즘에 따라 암호화 또는 복호화를 수행할 수 있다.

<47> 그리고, 상기 암호키 생성부는 상기 로그인 패스워드, 상기 이티레이션 값 및 상기 제 2 솔트값을 입력값으로 하여 해쉬 연산을 수행하고, 상기 해쉬 연산의 결과값의 MSB 16바이트(byte)를 취하여 상기 암호키를 생성할 수 있다.

<48> 또한, 상기 암호키는 KEK는 암호키이고, $iteration$은 이티레이션 값이며, $password$가 로그인 패스워드이며, $salt_2$는 제 2 솔트값일 경우 수학식 $KEK = H^{iteration}(password \| salt_2)$에 의해 연산되는 것을 특징으로 한다.

<49> 그리고, 상기 인증부는 상기 패스워드 해쉬값과 상기 인증 패스워드 해쉬값이 동일하면 사용자 인증을

수행하고, 상기 패스워드 해쉬값과 상기 인증 패스워드 해쉬값이 동일하지 않을 경우, 사용자 인증이 실패된 것으로 판단하여 상기 패스워드 해쉬값을 삭제하는 것을 특징으로 한다.

<50> 아울러, 상기 모바일 기기의 특정 데이터는 캐쉬(cache) 정보, 상기 모바일 기기의 파일 시스템의 각각의 정보 및 상기 인증 사용자의 입력에 의해 생성된 텍스트 정보를 포함하는 것을 특징으로 한다.

<51> 그리고, 상기 모바일 기기는 휴대폰, 스마트폰, 피디에이(Personal Data Assistant:PDA) 및 네비게이션 중에서 선택된 어느 하나를 포함하는 것을 특징으로 한다.

<52> 상기 세 번째 과제를 해결하기 위하여 본 발명은,

<53> 상기 모바일 기기에서의 통합형 데이터 관리 방법을 컴퓨터에서 수행할 수 있도록 프로그램으로 기록된 기록매체를 제공한다.

효 과

<54> 본 발명에 의하면, 모바일 기기, 어플리케이션, OS/Platform 및 저장 장치의 종류에 독립적인 통합적 데이터 관리 구조를 제공할 수 있으며, 응용프로그램이 아닌 보안 플랫폼 구조 자체에 따라 모바일 기기에서 안전한 통합형 데이터 관리 구조를 제공함으로써, 기기의 도난, 분실, 인증되지 않은 사용자로부터의 접근, 각종 해킹, 악성코드로부터의 노출 등의 보안 위협으로부터 향상된 보안성을 제공할 수 있는 효과가 있다.

발명의 실시를 위한 구체적인 내용

<55> 본 발명은 휴대 단말, 즉 모바일 기기에 저장되는 사용자 프라이버시와 관련된 모든 정보를 안전하게 암호화하여 저장하고, 이를 필요에 따라 효율적으로 복호화할 수 있는 통합형 사용자 프라이버시 관리 모델을 제공한다.

<56> 즉, 모바일 기기 및 사용자 정보를 저장하고, 이를 기반으로 동작하는 모바일 기기의 애플리케이션에서 안전한 사용자 정보 저장 모델을 본 발명은 제공할 수 있다.

<57> 이를 위하여 모바일 기기는 사용자에게 사용자 인터페이스(User Interface:UI)를 제공하고, 사용자가 필요한 정보를 사용자의 패스워드를 입력받아 필요한 서비스를 진행한다.

<58> 그리고, 사용자가 입력한 로그인 패스워드를 기반으로 하여 대칭키를 생성하고, 모바일 기기에 저장된 정보를 암호화하여 저장하거나, 복호화하여 참조한다.

<59> 이에 의하여 사용자 정보는 본인 이외에 어떠한 제3자도 사용자의 정보를 열람할 수 없으며, 기존의 모바일 기기에서의 사용자 정보 관리는 암호화 없이 단말의 파일시스템에 그래도 저장하고, 제3자가 휴대단말 메모리부에 직접적으로 접근할 경우에 사용자 정보가 그래도 노출되는데 반하여, 본 발명에 의하면 사요자 정보는 정확한 사용자 패스워드를 알지 못하는 한 자신이 원하는 정보를 열람할 수 없게 된다.

<60> 이와 같은 방식을 적용하면, 기본적으로 휴대 단말에서 제공하는 전화번호부, 문자 메시지뿐만 아니라 사용자의 사진, 위치정보, 파일 관리 등의 휴대 단말기의 모든 서비스 어플리케이션에 필요한 사용자 정보를 통합적으로 안전하게 관리할 수 있게 된다.

<61> 한편, 하기에 상술되는 인증 사용자란 모바일 기기에 자신의 정보를 등록한 자로, 합법적인 소유권을 가지거나, 상기 합법적인 소유권을 가진자로부터 사용에 대한 허락을 받은 자를 의미한다.

<62> 그리고, 하기에 상술되는 본 발명의 통합형 데이터 관리 방법은 모바일 기기에 한정되었으나, 이에 구애받지 않고, 인증 사용자의 로그인 정보를 이용하는 통신 분야에서의 암호화에 효율적으로 적용될 수 있음은 물론이다.

<63> 이하, 본 발명의 바람직한 실시예를 첨부도면에 의거하여 상세하게 설명하기로 한다.

<64> 그러나, 다음에 예시하는 본 발명의 실시예는 여러 가지 다른 형태로 변형할 수 있으며, 본 발명의 범위가 하기에 상술되는 실시예에 한정되는 것은 아니다. 본 발명의 실시예는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 더욱 완전하게 설명하기 위하여 제공된다.

<65> 도 2는 본 발명의 일 실시예에 따른 모바일 기기에서의 통합형 데이터 관리 방법의 흐름도를 도시한 것이다.

<66> 도 2를 참조하면, 우선 인증 사용자에 의해 고유의 로그인 패스워드가 모바일 기기에 입력되면, 로그인 패스워드, 인증 사용자에 의해 미리 설정된 이티레이션(iteration) 값 및 제 1 솔트(salt)값을 입력값으로 하여 해쉬 연산에 의해 인증 패스워드 해쉬값을 생성하고, 모바일 기기의 단말 데이터베이스에 저장한다(S210).

<67> 즉, 이는 로그인 패스워드 생성과정으로, 인증 사용자의 로그인 패스워드를 기반으로 인증 사용자인지의 여부를 확인하기 위한 인증 패스워드 해쉬값을 생성하는 과정이다.

<68> 이를 위하여, 입력값으로 인증 사용자에 의해 설정되거나, 관리자에 의해 미리 결정된 로그인 패스워드, 시스템 상에서 미리 결정된 이티레이션 값, 제 1 솔트값을 입력값으로 하여 해쉬 연산을 수행함으로써 인증 패스워드 해쉬값을 생성한다.

<69> 여기서, 추가적으로 제 1 솔트값이 사용되는 것은 패스워드 만으로 인증 패스워드 해쉬값을 생성하는 것보다 더욱 결과값의 복잡도를 높이기 위함이다.

<70> 그 다음, 상기 로그인 패스워드, 상기 이티레이션 값 및 제 2 솔트값을 이용하여 암호키를 생성한다(S220).

<71> 여기서, 암호키를 생성하는 이유는 상기 과정(S210)과는 달리, 인증 사용자에 의해 특정 데이터를 암호화하기 위함이며, 사용자의 인증을 위하여 사용되는 제 1 솔트값과는 별도로 데이터의 암호화를 위하여 제 2 솔트값을 별도로 사용함으로써 암호화의 복잡도를 더욱 증가시킬 수 있다.

<72> 그 다음, 상기 인증 사용자의 모바일 기기에서 비밀키를 랜덤 생성하고, 생성된 비밀키를 상기 과정(S220)에서 생성된 암호키를 이용하여 암호화함으로써 비밀키 암호화값을 생성하고, 비밀키 암호화값을 단말 데이터베이스에 저장한다.

<73> 여기서, 비밀키 암호화값을 생성하는 이유는 전술한 바와 같이, 모바일 기기에서 생성되거나, 사용자의 조작에 의해 생성된 데이터를 암호화하는 암호키를 암호화하여 모바일 기기의 단말 데이터베이스에 저장하기 위함이며, 상기 비밀키 암호화값이 유출된다고 하더라도, 타 사용자가 상기 로그인 패스워드, 인증 사용자에 의해 미리 설정된 이티레이션(iteration) 값 및 제 1 솔트(salt)을 모두 알지 못하는 한 로그인을 수행할 수 없고, 더불어 상기 로그인 패스워드, 이티레이션 값, 제 2 솔트값을 모두 알지 못하는 한 상기 암호키를 알 수 없으며, 이에 따라 상기 암호키에 의해 암호화된 모바일 기기의 특정 데이터를 복호화 할 수 없다.

<74> 그 다음, 특정 사용자에 의해 패스워드가 입력되면, 상기 이티레이션 값, 상기 제 1 솔트값을 이용하여 패스워드 해쉬값을 생성(S240)하고, 상기 인증 패스워드 해쉬값과 비교하여 사용자 인증을 수행한다(S250).

<75> 이 과정은 상기 모바일 기기를 사용하는 사용자가 인증 사용자인지의 여부를 확인하는 과정으로, 이는 모바일 기기에 접근하는 사용자에게 패스워드를 입력하도록 하여, 패스워드가 입력되면 이를 기반으로 모바일 기기에 미리 설정된 이티레이션 값과 제 1 솔트값을 기반으로 패스워드 해쉬값을 생성하고, 패스워드 해쉬값이 생성되면, 상기 패스워드 해쉬값과 상기 모바일 기기의 단말 데이터베이스에 저장된 인증 패스워드 해쉬값과 비교하여, 이의 동일성 여부에 따라 사용자를 인증한다.

<76> 그 다음, 인증 사용자로부터 특정 데이터의 암호 요청에 관한 쿼리를 수신하면(S260), 최종적으로 상기 단말 데이터베이스에 저장된 상기 비밀키 암호화값을 복호화하여 상기 비밀키를 추출하고, 상기 추출된 비밀키를 이용하여 상기 모바일 기기의 특정 데이터를 암호화한다(S270).

<77> 이 과정은 인증 과정을 수행한 인증 사용자에 의해 특정 데이터를 암호화하는 과정으로, 암호화하고자 하는 단말 데이터베이스에 저장된 특정 데이터를 로드하면, 인증 사용자의 로그인 패스워드 입력에 따라 상기 과정(S220)을 수행하여 암호키를 생성한다.

<78> 그러면, 상기 생성된 암호키를 기반으로 단말 데이터베이스에 저장된 개인키 암호화 값을 복호화하여 상기 비밀키를 추출하고, 추출된 비밀키를 이용하여 상기 특정 데이터를 암호화할 수 없다.

<79> 따라서, 인증 과정을 수행하지 못한 외부 사용자는 비밀키를 추출하기 위한 여타의 키 값을 알 수 없으므로, 특정 데이터를 암호화할 수 없을 뿐만 아니라, 복호화도 수행할 수 없다.

<80> 여기서, 암호화 및 복호화 알고리즘은 128, 192 또는 256 비트의 에이이에스(AES) 암호화 알고리즘을 적용할 수 있고, 피비이(PBE) 알고리즘을 적용할 수 있다.

<81> 여기서, 에이이에스(AES) 암호화 알고리즘은 개선된 암호화 표준(Advanced Encryption Standard:AES)으로 대칭키 암호화 규격(Data Encryption Standard:DES)과 같이 128, 192 또는 256 비트의 블럭 암호를 이용하는 대칭키 암호 시스템이다.

<82> 그리고, 피비이(PBE) 암호화 알고리즘은 패스워드 기반의 암호화 알고리즘(Password-Based Encryption:PBE)으로, RSA사가 제시한 공개 키 암호 표준(Public-Key Cryptography Standard:PKCS)의 하나인

PKCS #5를 적용할 수 있고, 이를 기반으로, 개인 키 정보를 사용자의 패스워드에 기반하여 암호화하는 암호화 알고리즘을 적용할 수 있다.

<83> 한편, 상기 과정(S270)은 상기 추출된 비밀키에 따라 암호화된 특정 데이터가 상기 인증 사용자의 요청에 의해 로드되면, 상기 인증 사용자의 로그인 패스워드 입력에 따라 암호키를 생성하고, 상기 생성된 암호키를 이용하여 상기 암호화된 특정 데이터를 복호화하는 단계를 더 포함할 수 있다.

<84> 즉, 암호화 뿐만 아니라 복호화 과정에서도 인증 사용자의 패스워드가 입력되어야 하며, 잘못된 패스워드가 입력될 경우, 전술한 바와 같은 방법으로 생성되는 암호키의 키 값이 달라지므로 암호화된 특정 데이터를 복호화할 수 없다.

<85> 도 3은 도 2의 인증 패스워드 해쉬값 생성 과정(S210)의 상세 흐름도이다.

<86> 도 3을 참조하면, 우선 인증 사용자에 의해 패스워드(password)가 입력되면(S211), 인증 사용자의 모바일 기기에서 미리 설정된 이터레이션 값(iteration)과 제 1 솔트값을 로드(S212)하여, 인증 패스워드 해쉬값 $H^{iteration}(password \parallel salt_1)$을 생성한다(S213).

<87> 여기서, 상기 미리 설정된 이터레이션 값은 인증 패스워드의 해쉬값을 생성하기 위하여 해쉬 연산의 반복 수행 횟수를 의미하여, 상기 제 1 솔트값을 기반으로 패스워드의 암호화의 복잡도를 더욱 증가시킨다.

<88> 그리고, 상기 연산된 인증 패스워드 해쉬값을 단말 데이터베이스에 저장(S214)함으로써, 추후 사용자의 인증에 상기 인증 패스워드 해쉬값을 사용하게 된다.

<89> 도 4는 상기 도 2의 암호키 생성과정(S220)의 상세 흐름도이다.

<90> 도 4를 참조하면, 인증 사용자에 의해 인증 패스워드(password)가 입력(S421)되면, 인증 사용자의 모바일 기기에서 미리 설정된 이터레이션 값(iteration)과 제 2 솔트값($salt_2$)을 로드(S422)하여, 상기 인증 패스워드, 이터레이션 값 및 제 2 솔트값을 기반으로 해쉬 연산을 수행하여 해쉬연산의 결과값을 생성한다(S423).

<91> 마지막으로, 상기 해쉬연산의 결과값에서 최상위 비트(Most Significant Bit:MSB) 16비트를 취하여 암호키 $H^{iteration}(password \parallel salt_2)$를 생성한다(S424).

<92> 즉, KEK는 암호키이고, $iteration$은 이터레이션 값이며, $password$가 로그인 패스워드이며, $salt_2$는 제 2 솔트값일 때, 상기 암호키는 하기의 수학식 1에 의해 생성될 수 있다.

수학식 1

<93> $$KEK = H^{iteration}(password \parallel salt_2)$$

<94> 도 5는 상기 도 2의 패스워드 해쉬값 생성 과정(S240) 및 사용자 인증 수행 과정(S250)의 상세 흐름도이다.

<95> 도 5를 참조하면, 특정 사용자에 의해 패스워드(password')가 입력되면(S541), 단말 데이터베이스에 저장된 이터레이션 값(iteration) 및 제1솔트값($salt_1$) 을 로드(S542)하여 해쉬연산에 의해 패스워드 해쉬값을 생성한다(S543).

<96> 그런 다음, 생성된 패스워드 해쉬값과 인증 사용자의 패스워드에 의해 연산된 인증 패스워드 해쉬값과 비교하여(S544), 양자가 동일할 경우, 사용자 인증을 완료(S545)하고, 동일하지 않을 경우 상기 생성된 패스워드 해쉬값을 삭제(S546)하고 상기 특정 사용자에 의해 패스워드가 재입력되거나, 전체 과정을 종료한다.

<97> 도 6은 상기 도 2의 특정 데이터의 암호화 과정(S270)의 상세흐름도이다.

<98> 도 6을 참조하면, 인증 사용자로부터 특정 데이터(data)의 암호화 요청에 대한 쿼리를 수신(S671)하면, 단말 데이터베이스에 저장된 비밀키 암호화값 $E_{KEK}(key)$을 로드(S672)하고, 로드된 비밀키 암호화값을 상기 암호키 KEK를 이용하여 복호화함으로써 비밀키를 추출한다(S673).

<99> 상기 비밀키를 추출하는 연산은 하기의 수학식 2와 같다.

수학식 2

<100> $$D_{KEK}(E_{KEK}(key)) = key$$

<101> 상기 수학식 2에서 D는 복호화 알고리즘을 의미하고, $E_{KEK}(key)$는 비밀키 암호화값을 의미하고, key는 비밀키를 의미한다

<102> 그런 다음, 상기 추출된 비밀키를 이용하여 특정 데이터를 암호화한다(S674).

<103> 한편, 여기서 특정 데이터는 모바일 기기의 특정 데이터를 의미하고, 이는 캐쉬(cache) 정보, 상기 모바일 기기의 파일 시스템의 각각의 정보 및 상기 인증 사용자의 입력에 의해 생성된 텍스트 정보를 포함할 수 있고, 상기 모바일 기기는 휴대폰, 스마트폰, 피디에이(Pesonal Data Assitant:PDA)를 포함할 수 있다.

<104> 한편, 상기 비밀키를 추출하는 과정(S673) 및 특정 데이터를 암호화하는 과정(S674)에서 암호화 및 복호화 알고리즘은 전술한 128, 192 또는 256 비트의 에이이에스(AES) 암호화 알고리즘을 적용할 수 있고, 피비이(PBE) 알고리즘을 적용할 수 있다.

<105> 도 7은 본 발명에 적용되는 암호화된 특정 데이터의 복호화 과정의 상세 흐름도이다.

<106> 도 7을 참조하면, 우선 비밀키에 따라 암호화된 특정 데이터 $E_{key}(data)$가 인증 사용자의 요청에 의해 로드되면(S781), 인증 사용자의 로그인 패스워드 입력에 따라 암호키 KEK를 생성한다(S782). 상기 암호키 생성 과정은 전술한 바와 동일하므로 중복된 설명은 과감히 생략하기로 한다.

<107> 그런 다음, 상기 생성된 암호키 KEK에 따라 비밀키 암호화값을 복호화하여 비밀키를 획득한다(S783). 이는 상기 수학식 2에 기재된 바와 동일하다.

<108> 그 다음, 상기 비밀키를 이용하여 암호화된 특정 데이터를 복호화한다(S784).

<109> 이는 하기의 수학식 3과 같다.

수학식 3

<110> $$D_{key}(E_{key}(data)) = data$$

<111> 상기 수학식 3에서 $E_{key}(data)$는 특정 데이터 $data$를 비밀키 key에 의해 암호화한 암호화된 특정 데이터를 의미하고, 이를 상기 과정(S783)에 의해 복호화함으로써 획득된 비밀키 key를 기반으로 특정 데이터 $data$를 복호화함을 나타내고 있다.

<112> 도 8은 본 발명에 따른 모바일 기기에서의 통합형 데이터 관리 방법의 개괄도를 도시한 것이다.

<113> 도 8을 참조하면, 우선 인증 사용자의 로그인 패스워드(810)를 기반으로 미리 설정된 이터레이션 값 및 제 1 솔트값을 이용하여 인증 패스워드 해쉬값(820)을 생성하여 사용자 인증용 인증 패스워드 해쉬값(820)을 단말 데이터베이스(870)에 저장한다.

<114> 또한, 인증 사용자의 로그인 패스워드(810)를 기반으로 미리 설정된 이터레이션 값 및 제 2 솔트값을 이용하여 해쉬 연산의 결과값(830)을 생성하고, 상기 해쉬 연산의 결과값 중 최상위 비트(MSB) 16비트를 취하여 암호키(840)를 생성한다.

<115> 그리고, 상기 암호키(840)를 이용하여 모바일 기기에서 랜덤 생성된 비밀키(850)을 암호화하여 비밀키 암호화값(860)을 생성하고, 이를 단말 데이터베이스(870)에 저장한다.

<116> 도 9는 본 발명의 일 실시예에 따른 모바일 기기에서의 통합형 데이터 관리 장치의 블록도를 도시한 것이다.

<117> 한편, 하기에 상술되는 본 발명의 일 실시예에 따른 모바일 기기에서의 통합형 데이터 관리 장치의 상술에 있어서, 전술한 모바일 기기에서의 통합형 데이터 관리 방법과 중복된 상술은 과감히 생략하기로 한다.

<118> 도 9를 참조하면, 본 발명의 일 실시예에 따른 모바일 기기에서의 통합형 데이터 관리 장치는 사용자 계층(910), 관리 계층(920) 및 모바일 기기의 단말 데이터베이스(930)을 포함할 수 있다.

<119> 한편, 상기 사용자 계층(910)은 인증 사용자로부터 입력 데이터를 수신받고, 상기 인증 사용자의 쿼리에 의해 생성된 정보를 출력하도록 하는 사용자 인터페이스를 제공하며, 이는 패스워드 수신부(911) 및 비밀키 생성부(912)를 포함할 수 있다.

<120> 그리고, 관리 계층(920)은 상기 사용자 계층(910)에 입력된 상기 인증 사용자의 입력 데이터에 의해 암호화 및 복호화를 수행하며, 이는 인증 패스워드 해쉬값 생성부(921), 인증부(922), 암호키 생성부(923), 비밀키 암호화값 생성부(924), 및 데이터 암호화부(925)를 포함할 수 있다.

<121> 또한, 단말 데이터베이스(930)은 상기 인증 사용자의 모바일 기기의 어플리케이션에서 생성된 데이터, 상기 사용자 계층(910) 및 상기 관리 계층(920)에서 생성된 데이터를 저장하며, 구체적으로는 인증 패스워드 해쉬값(931), 암호키(932) 및 비밀키 암호화 값(933)을 저장할 수 있다.

<122> 상기 패스워드 수신부(911)는 상기 인증 사용자로부터 로그인 패스워드를 수신하고, 특정 사용자로부터 인증을 위한 패스워드를 수신한다.

<123> 상기 비밀키 생성부는 인증 사용자 고유의 비밀키를 랜덤하게 생성한다.

<124> 인증 패스워드 해쉬값 생성부(921)는 상기 로그인 패스워드, 상기 인증 사용자에 의해 미리 설정된 이티레이션(iteration) 값, 및 제 1 솔트(salt)값을 입력값으로 하여 해쉬 연산에 의해 인증 패스워드 해쉬값을 생성한다.

<125> 인증부(922)는 특정 사용자에 의해 상기 패스워드 수신부에 패스워드가 입력되면, 상기 이티레이션 값, 상기 제 1 솔트값을 이용하여 패스워드 해쉬값을 생성하고, 상기 인증 패스워드 해쉬값과 비교하여 사용자 인증을 수행하게 된다.

<126> 여기서, 상기 인증부(922)는 상기 패스워드 해쉬값과 상기 인증 패스워드 해쉬값이 동일하면 사용자 인증을 수행하고, 상기 패스워드 해쉬값과 상기 인증 패스워드 해쉬값이 동일하지 않을 경우, 사용자 인증이 실패된 것으로 판단하여 상기 패스워드 해쉬값을 삭제할 수 있다.

<127> 이와 같이, 패스워드 해쉬값과 상기 인증 패스워드 해쉬값의 동일성 여부에 따라 사용자 인증을 수행함으로써, 한층 보안이 향상된 사용자 인증을 수행할 수 있게 된다.

<128> 암호키 생성부(923)는 상기 로그인 패스워드, 상기 이티레이션 값 및 제 2 솔트값을 이용하여 암호키를 생성한다.

<129> 여기서, 암호키 생성부(923)는 상기 로그인 패스워드, 상기 이티레이션 값 및 상기 제 2 솔트값을 입력값으로 하여 해쉬 연산을 수행하고, 상기 해쉬 연산의 결과값의 MSB 16바이트(byte)를 취하여 상기 암호키를 생성할 수 있다.

<130> 그리고, 상기 암호키는 전술한 바와 같이,

<131> 상기 암호키는

<132> KEK는 암호키이고, $iteration$은 이티레이션 값이며, $password$가 로그인 패스워드이며, $salt_2$는 제 2 솔트값일 때, 상기 수학식 1에 의해 연산될 수 있다.

<133> 또한, 비밀키 암호화값 생성부(924)는 상기 비밀키를 상기 암호키를 이용하여 암호화함으로써 비밀키 암호화값을 생성한다.

<134> 데이터 암호화부(925)는 상기 인증 사용자로부터 특정 데이터의 암호 요청에 관한 쿼리를 수신하며, 상기 단말 데이터베이스에 저장되는 상기 비밀키 암호화값을 복호화하여 상기 비밀키를 추출하고, 상기 추출된 비밀키를 이용하여 상기 모바일 기기의 특정 데이터를 암호화하는 역할을 수행한다.

<135> 여기서, 모바일 기기의 특정 데이터는 캐쉬(cache) 정보, 상기 모바일 기기의 파일 시스템의 각각의 정보 및 상기 인증 사용자의 입력에 의해 생성된 텍스트 정보를 포함하며, 상기 모바일 기기는 휴대폰, 스마트폰, 피디에

이(Personal Data Assistant:PDA) 및 네비게이션을 포함할 수 있다.

<136> 한편, 상기 관리 계층(930)은 상기 비밀키에 따라 암호화된 특정 데이터가 상기 인증 사용자의 쿼리에 의해 로드되면, 상기 인증 사용자의 로그인 패스워드 입력에 따라 상기 암호키를 생성하고, 상기 생성된 암호키를 이용하여 상기 암호화된 특정 데이터를 복호화하는 데이터 복화화부(미도시)를 더 포함할 수 있다.

<137> 그리고, 상기 관리 계층(930)은 전술한 바와 같이, 128, 192 또는 256 비트의 에이티에스(AES) 암호화 알고리즘 및 피비이(PBE) 암호화 알고리즘에 따라 암호화 또는 복호화를 수행한다.

<138> 본 발명에 따른 모바일 기기에서의 통합형 데이터 관리 방법은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터(정보처리 기능을 갖는 장치를 모두 포함한다)가 읽을 수 있는 코드로서 구현하는 것이 가능하다.

<139> 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 테이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광데이터 저장장치 등이 있다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<140> 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 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 등록청구범위의 기술적 사항에 의해 정해져야 할 것이다.

도면의 간단한 설명

<141> 도 1은 다양한 경로의 모바일 기기의 감염 경로를 도시한 것이다.

<142> 도 2는 본 발명의 일 실시예에 따른 모바일 기기에서의 통합형 데이터 관리 방법의 흐름도를 도시한 것이다.

<143> 도 3은 도 2의 인증 패스워드 해쉬값 생성 과정(S210)의 상세 흐름도이다.

<144> 도 4는 상기 도 2의 암호키 생성과정(S220)의 상세 흐름도이다.

<145> 도 5는 상기 도 2의 패스워드 해쉬값 생성 과정(S240) 및사용자 인증 수행 과정(S250)의 상세 흐름도이다.

<146> 도 6은 상기 도 2의 특정 데이터의 암호화 과정(S270)의 상세흐름도이다.

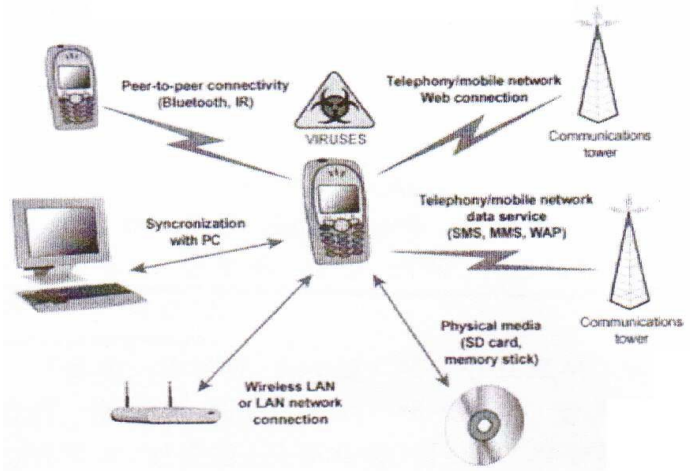
<147> 도 7은 본 발명에 적용되는 암호화된 특정 데이터의 복호화 과정의 상세 흐름도이다.

<148> 도 8은 본 발명에 따른 모바일 기기에서의 통합형 데이터 관리 방법의 개괄도를 도시한 것이다.

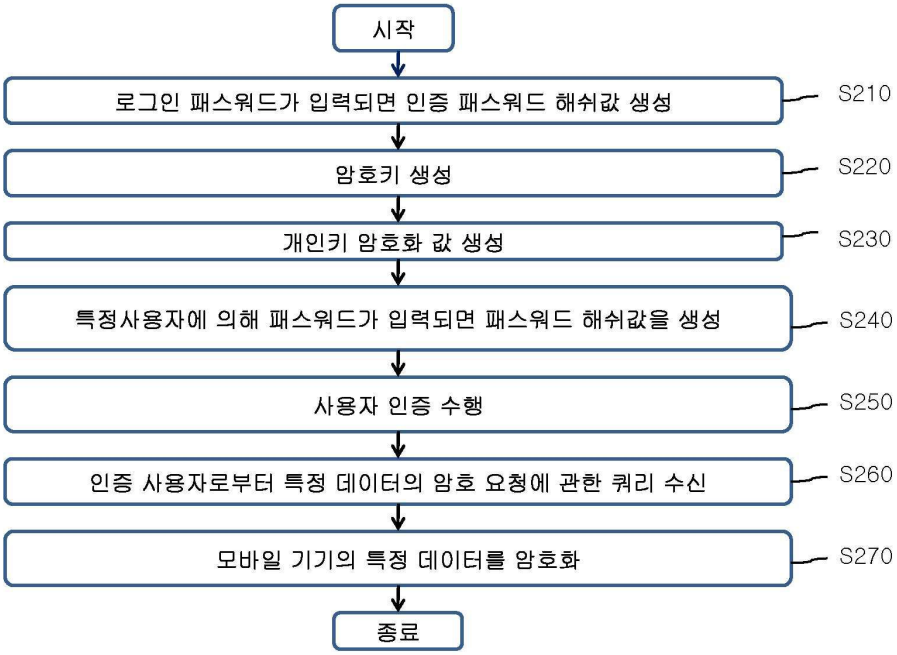
<149> 도 9는 본 발명의 일 실시예에 따른 모바일 기기에서의 통합형 데이터 관리 장치의 블록도를 도시한 것이다.

도면

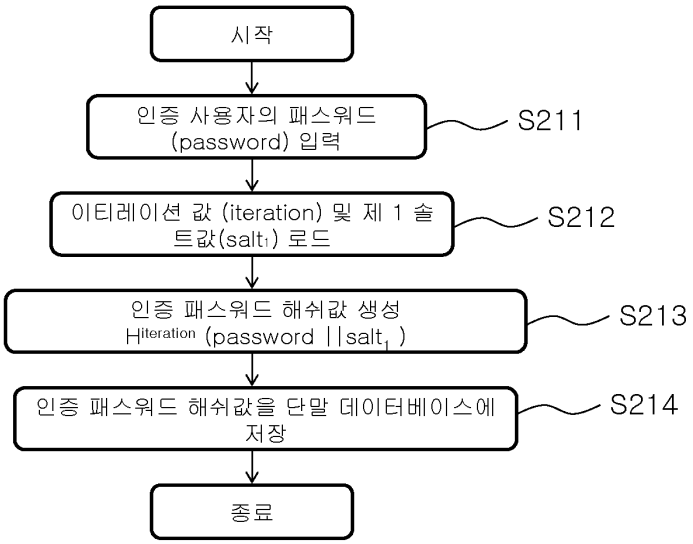
도면1



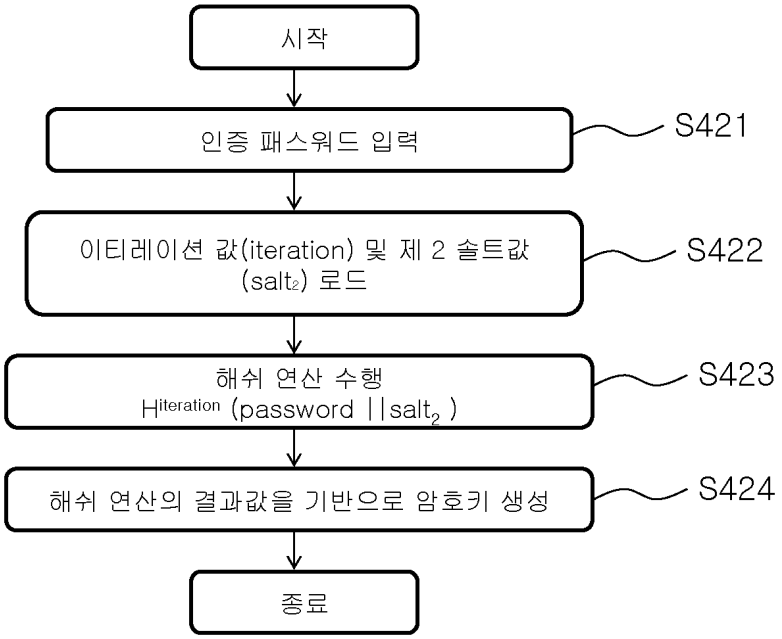
도면2


시작
로그인 패스워드가 입력되면 인증 패스워드 해쉬값 생성
S210
암호키 생성
S220
개인키 암호화 값 생성
S230
특정사용자에 의해 패스워드가 입력되면 패스워드 해쉬값을 생성
S240
사용자 인증 수행
S250
인증 사용자로부터 특정 데이터의 암호 요청에 관한 쿼리 수신
S260
모바일 기기의 특정 데이터를 암호화
S270
종료

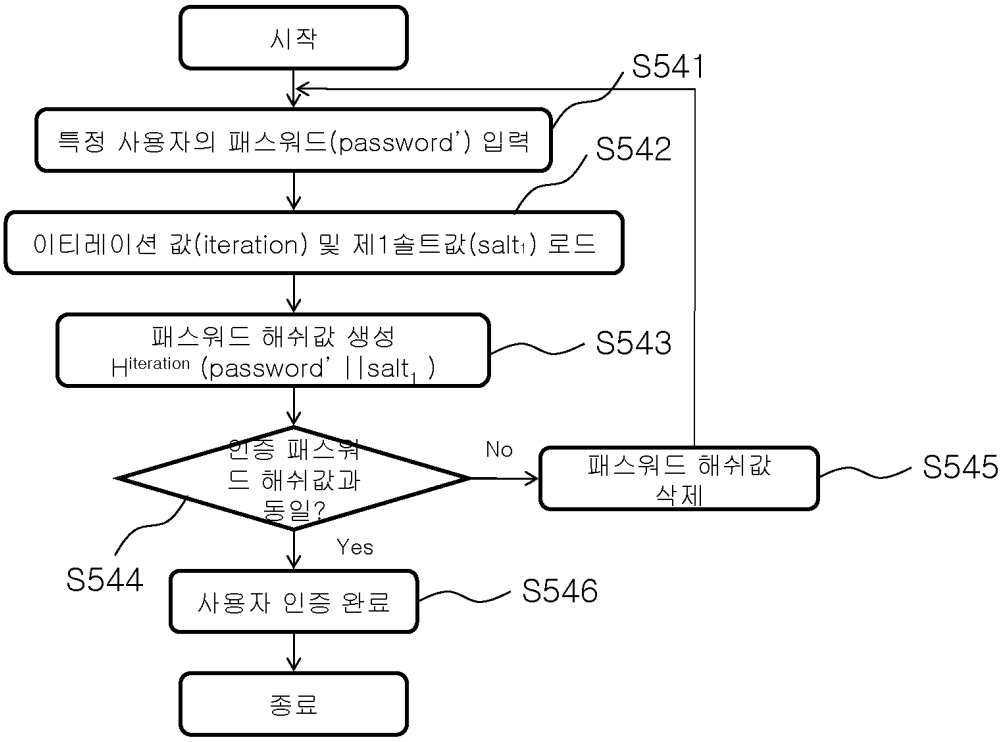
도면3


시작
인증 사용자의 패스워드 (password) 입력
S211
이터레이션 값 (iteration) 및 제 1 솔트값(salt1) 로드
S212
인증 패스워드 해쉬값 생성
H^iteration (password ||salt1)
S213
인증 패스워드 해쉬값을 단말 데이터베이스에 저장
S214
종료

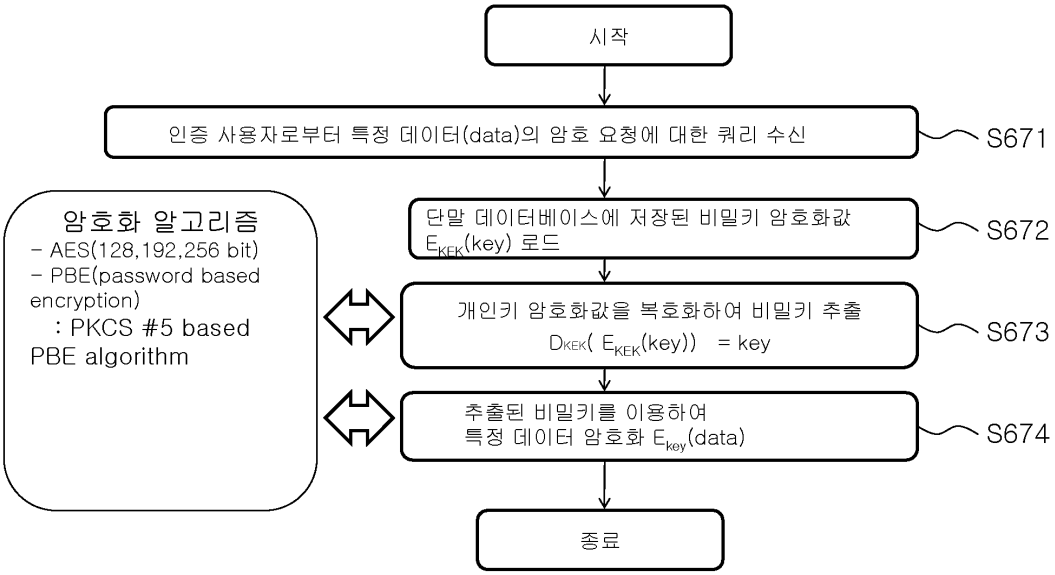
도면4


시작
인증 패스워드 입력
S421
이터레이션 값(iteration) 및 제 2 솔트값 ($salt_2$) 로드
S422
해쉬 연산 수행
$H^{iteration}$ (password ||$salt_2$)
S423
해쉬 연산의 결과값을 기반으로 암호키 생성
S424
종료

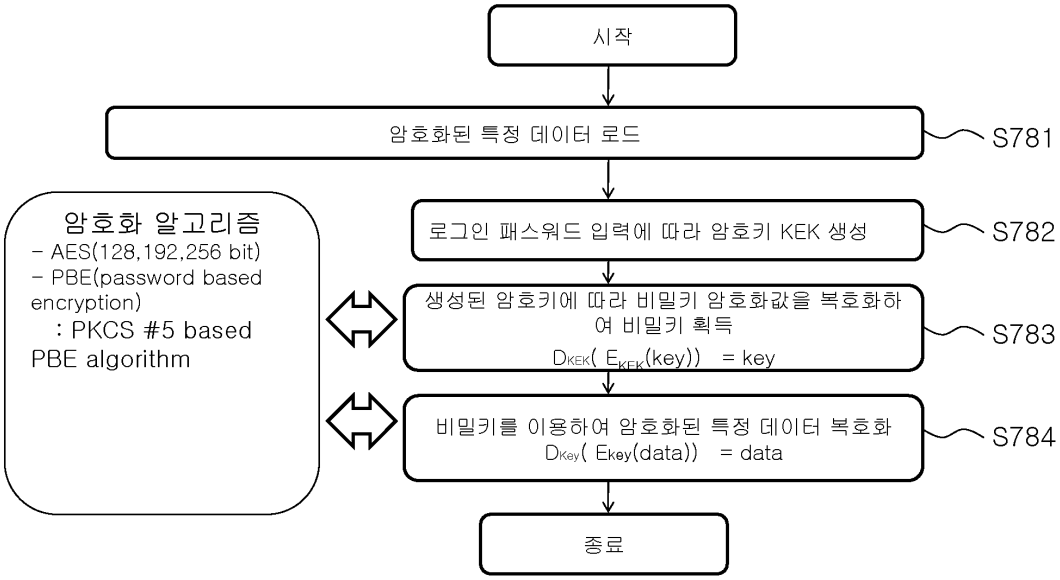
도면5


시작
S541
특정 사용자의 패스워드(password') 입력
S542
이터레이션 값(iteration) 및 제1솔트값($salt_1$) 로드
패스워드 해쉬값 생성
$H^{iteration}$ (password' ||$salt_1$)
S543
인증 패스워드 해쉬값과 동일?
No
패스워드 해쉬값 삭제
S545
S544
Yes
사용자 인증 완료
S546
종료

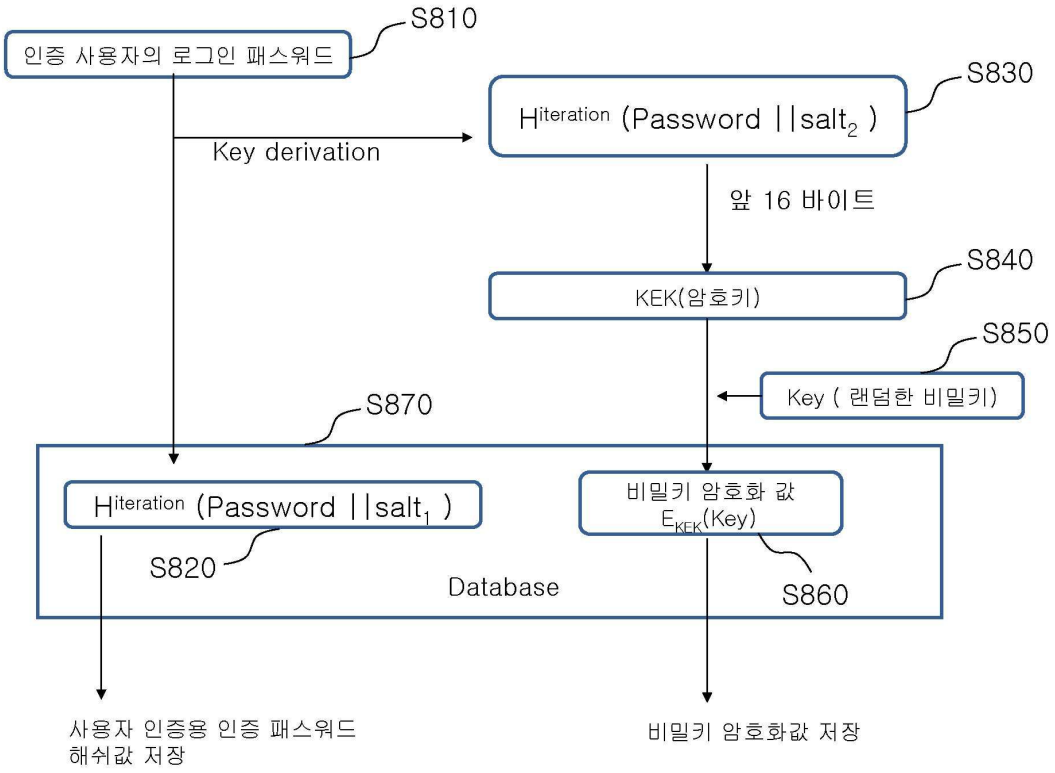
도면6


시작
인증 사용자로부터 특정 데이터(data)의 암호 요청에 대한 쿼리 수신
S671
단말 데이터베이스에 저장된 비밀키 암호화값 E_{KEK}(key) 로드
S672
개인키 암호화값을 복호화하여 비밀키 추출
$D_{KEK}(E_{KEK}(key)) = key$
S673
추출된 비밀키를 이용하여 특정 데이터 암호화 E_{key}(data)
S674
종료
암호화 알고리즘
- AES(128,192,256 bit)
- PBE(password based encryption)
: PKCS #5 based PBE algorithm

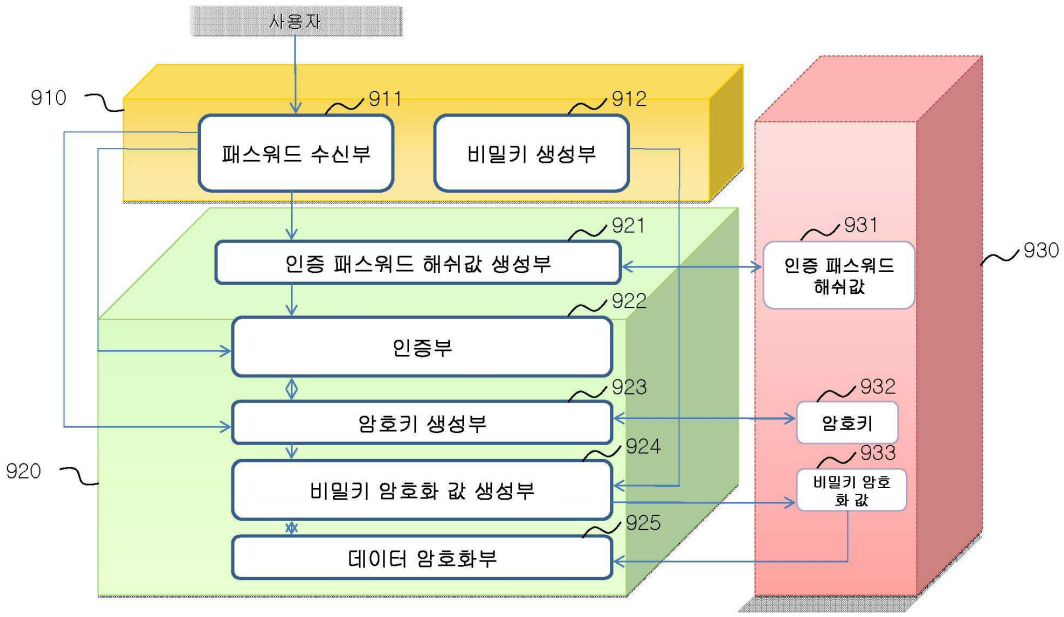
도면7


시작
암호화된 특정 데이터 로드
S781
로그인 패스워드 입력에 따라 암호키 KEK 생성
S782
생성된 암호키에 따라 비밀키 암호화값을 복호화하여 비밀키 획득
$D_{KEK}(E_{KEK}(key)) = key$
S783
비밀키를 이용하여 암호화된 특정 데이터 복호화
$D_{Key}(E_{key}(data)) = data$
S784
종료
암호화 알고리즘
- AES(128,192,256 bit)
- PBE(password based encryption)
: PKCS #5 based PBE algorithm

도면8


S810
인증 사용자의 로그인 패스워드
Key derivation
S830
Hiteration (Password ||salt2)
앞 16 바이트
S840
KEK(암호키)
S850
Key (랜덤한 비밀키)
S870
Hiteration (Password ||salt1)
S820
비밀키 암호화 값
EKEK(Key)
S860
Database
사용자 인증용 인증 패스워드
해쉬값 저장
비밀키 암호화값 저장

도면9


사용자
910
911
912
패스워드 수신부
비밀키 생성부
921
인증 패스워드 해쉬값 생성부
922
인증부
923
암호키 생성부
924
비밀키 암호화 값 생성부
925
데이터 암호화부
920
931
인증 패스워드 해쉬값
930
932
암호키
933
비밀키 암호화 값