(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년03월27일
(11) 등록번호 10-1130415
(24) 등록일자 2012년03월19일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
H04L 9/30 (2006.01)
(21) 출원번호 10-2005-0027654
(22) 출원일자 2005년04월01일
심사청구일자 2010년03월23일
(65) 공개번호 10-2006-0045440
(43) 공개일자 2006년05월17일
(30) 우선권주장
10/816,756 2004년04월02일 미국(US)
(56) 선행기술조사문헌
US6160891 A
KR1020030083857 A
KR1020000006633 A
KR1020030069545 A
전체 청구항 수 : 총 21 항

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
백 아담
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
드함아라잔 배스크아란
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
(뒷면에 계속)
(74) 대리인
제일특허법인

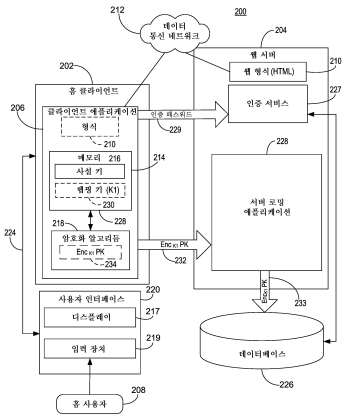
심사관 : 양종필

(54) 발명의 명칭 **비밀 데이터의 노출 없이 통신 네트워크를 통해 패스워드 보호된 비밀 데이터를 복구하는 방법 및 시스템**

(57) 요 약

통신 네트워크를 통해 링크된 제1 클라이언트 컴퓨터로부터 제2 클라이언트 컴퓨터로 안전하게 비밀 데이터를 로밍하는 시스템 및 방법이 개시된다. 제1 클라이언트 컴퓨터의 사용자는 홈 클라이언트 애플리케이션을 실행하고 로밍용 비밀 데이터를 지정한다. 홈 클라이언트 애플리케이션은 패스워드에 응답하여 제1 키를 생성하고, 지정된 비밀 데이터를 제1 키의 함수로서 암호화한다. 서버는 암호화된 비밀 데이터를 수신하여 저장한다. 제2 컴퓨터의 사용자는 로밍 클라이언트 애플리케이션을 실행하고, 서버로부터 암호화된 비밀 데이터의 전송을 요청한다. 로밍 클라이언트 애플리케이션은 패스워드에 응답하여 제1 키를 생성하고, 서버로부터 전송된 암호화된 비밀 데이터를 암호해독하여 비밀 데이터를 얻는다. 본 발명은 또한 사용자가 제1 키와 연관된 패스워드를 기억하지 못할 때 서버로부터 암호화된 비밀 데이터를 검색하는 능력을 사용자에게 제공할 수 있다. 또한, 서버는 비밀 데이터 또는 키를 알지 못한다.

대 표 도 - 도2



(72) 발명자

톤체바 다피나 이바노바

미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내

찬 콕 와이

미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내

뉴아스카 라훌 셔이칸트

미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내

특허청구의 범위

청구항 1

데이터 통신 네트워크에 연결된 컴퓨터들 사이에서 비밀 데이터(private data)를 통신하는 방법 - 상기 컴퓨터들은 상기 데이터 통신 네트워크에 연결된 제1 클라이언트 및 제2 클라이언트를 포함함 - 으로서,

네트워크 서버에서, 비밀 키를 로밍(roam)하라는 상기 제1 클라이언트의 사용자로부터의 요청에 응답하여 상기 제1 클라이언트에 의해 암호화된 복수의 키를 수신하는 단계 - 상기 복수의 키는 상기 비밀 키와, 상기 사용자로부터 수신된 암호화 패스워드에 응답하여 상기 제1 클라이언트에 의해 생성된 랩핑 키(wrapping key)와, 상기 제1 클라이언트에 의해 생성된 복구 키(recovery key)를 포함하고, 상기 비밀 키는 상기 랩핑 키의 함수로서 암호화되고, 상기 랩핑 키 및 상기 복구 키는 상기 서버에 알려지지 않고, 상기 서버는 상기 데이터 통신 네트워크에 연결됨 - ;

상기 서버에서, 상기 제1 클라이언트로부터 수신되는 상기 암호화된 복수의 키에 응답하여 백업 키를 생성하는 단계;

수신된 상기 암호화된 복수의 키 및 생성된 상기 백업 키를 상기 서버에 저장하는 단계;

상기 서버에서, 제2 클라이언트로부터 백업 데이터에 대한 요청을 수신하는 단계; 및

수신된 상기 요청에 응답하여, 암호화된 상기 복구 키 및 상기 백업 키를 상기 서버로부터 상기 제2 클라이언트에 전송하는 단계 - 상기 제2 클라이언트는 상기 제2 클라이언트에의 저장을 위해 전송된 상기 백업 키의 함수로서 암호화된 상기 복구 키를 나타내는 백업 암호화된 복구 키를 생성함 -

를 포함하는 방법.

청구항 2

제1항에 있어서,

상기 암호화된 복구 키를 상기 제2 클라이언트에서 상기 랩핑 키의 함수로서 암호해독하는 단계 - 상기 랩핑 키는 상기 제2 클라이언트의 사용자로부터 수신되는 상기 암호화 패스워드에 응답하여 상기 제2 클라이언트 상에 생성됨 - 를 더 포함하는 방법.

청구항 3

제1항에 있어서,

상기 복구 키는 상기 사용자에 의해서 선택된 복구 옵션에 응답하여 상기 제1 클라이언트 상에 생성되는 방법.

청구항 4

제1항에 있어서,

수신된 복구 요청에 응답하여 상기 서버로부터 상기 제2 클라이언트에 암호화된 비밀 키와 암호화된 랩핑 키를 전송하는 단계 - 상기 제2 클라이언트 상에 저장된 상기 백업 암호화된 복구 키는 전송된 백업 키의 함수로서 상기 제2 클라이언트에서 암호해독되어 상기 복구 키가 얻어 지고, 상기 암호화된 랩핑 키는 얻어진 상기 복구 키의 함수로서 상기 제2 클라이언트에서 암호해독되어 상기 랩핑 키가 얻어지며, 상기 암호화된 비밀 키는 상기 제2 클라이언트에서 얻어진 상기 랩핑 키의 함수로서 암호해독되어 상기 비밀 키가 얻어짐 - 를 더 포함하는 방법.

청구항 5

제1항에 있어서,

상기 제1 클라이언트의 사용자로부터 수신되는 백업 요청에 응답하여 상기 제1 클라이언트에 상기 암호화된 복구 키와 상기 백업 키를 전송하는 단계 - 전송된 상기 암호화된 복구 키는 상기 제1 클라이언트 상에 생성되는 상기 랩핑 키의 함수로서 상기 제1 클라이언트에서 암호해독되어 복구 키가 얻어지고, 상기 제1 클라이언트는 얻어진 상기 복구 키를 전송된 상기 백업 키의 함수로서 암호화하여 상기 제1 클라이언트와 연관된 메모리에 저

장하기 위한 상기 백업 암호화된 복구 키를 생성함 - 를 더 포함하는 방법.

청구항 6

제5항에 있어서,

상기 데이터 통신 네트워크를 통해 상기 제1 클라이언트로부터 수신되는 복구 요청에 응답하여 상기 서버로부터 상기 제1 클라이언트에 상기 암호화된 비밀 키와 상기 암호화된 랩핑 키를 전송하는 단계 - 상기 제1 클라이언트 상에 저장된 상기 백업 암호화된 복구 키는 상기 전송된 백업 키의 함수로서 상기 제1 클라이언트에서 암호해독되어 상기 복구 키가 얻어지고, 상기 암호화된 랩핑 키는 얻어진 상기 복구 키의 함수로서 상기 제1 클라이언트에서 암호해독되며, 상기 암호화된 비밀 키는 얻어진 상기 랩핑 키의 함수로서 상기 제1 클라이언트에서 암호해독되어 상기 비밀 키가 얻어짐 - 를 더 포함하는 방법.

청구항 7

제1항에 있어서,

상기 제2 클라이언트의 사용자로부터 수신되는 복구 요청에 응답하여 상기 서버와 연관된 데이터베이스로부터 저장된 백업 키를 검색하는 단계; 및

수신된 상기 복구 요청에 응답하여 상기 서버로부터 상기 제2 클라이언트에 상기 백업 키를 전송하는 단계

를 더 포함하는 방법.

청구항 8

제1항에 있어서,

상기 제2 클라이언트는 상기 데이터 통신 네트워크에 연결된 로밍 클라이언트 컴퓨터(roaming client computer)인 방법.

청구항 9

제1항의 방법을 수행하는 컴퓨터 실행가능 명령어들을 갖는 컴퓨터 판독가능 저장 매체.

청구항 10

데이터 통신 네트워크 상에서 비밀 데이터를 통신하기 위한 시스템으로서,

비밀 키를 로밍하라는 요청을 사용자로부터 수신하고 상기 요청에 응답하기 위해 상기 데이터 통신 네트워크에 연결된 제1 클라이언트 - 상기 제1 클라이언트에 의한 상기 응답은,

상기 사용자에 의해 제공된 암호화 패스워드의 함수로서 랩핑 키를 생성하는 것;

복구 키를 생성하는 것;

상기 랩핑 키의 함수로서 상기 비밀 키를 암호화하는 것;

상기 복구 키의 함수로서 상기 랩핑 키를 암호화하는 것; 및

상기 랩핑 키의 함수로서 상기 복구 키를 암호화하는 것을 포함함 - ;

제1 클라이언트에 의해 암호화된 비밀 키, 랩핑 키, 및 복구 키를 수신하고, 상기 암호화된 키들의 수신에 응답하여 백업 키를 생성하는 서버 - 상기 서버는 상기 데이터 통신 네트워크에 연결됨 -;

상기 서버와 연관된 데이터베이스 - 상기 서버는, 수신된 상기 암호화된 키들 및 생성된 상기 백업 키를 상기 데이터베이스에 저장하고, 백업 데이터에 대한 요청을 수신하는 것에 응답하여 상기 백업 데이터를 전송하도록 구성되고, 상기 백업 데이터는 저장된 상기 암호화된 복구 키 및 저장된 상기 백업 키를 포함함 - ; 및

서버로부터의 상기 백업 데이터를 요청하고 상기 서버로부터의 상기 백업 데이터 수신에 응답하여 백업 암호화된 복구 키를 생성하기 위해 상기 데이터 통신 네트워크에 연결되는 제2 클라이언트 - 상기 제2 클라이언트에 의한 상기 생성은,

상기 사용자로부터 암호화 패스워드를 수신하는 것,

상기 암호화된 복구 키를 수신된 상기 암호화 패스워드의 함수로서 암호해독하는 것,

상기 백업 키를 상기 복구 키의 함수로서 암호해독하는 것, 및

상기 제2 클라이언트와 연관된 메모리에 상기 백업 암호화된 복구 키를 저장하는 것을 포함함 -

를 포함하는 시스템

청구항 11

제10항에 있어서,

상기 제1 클라이언트는, 생성된 상기 복구 키를 상기 제1 클라이언트 상에 저장하도록 구성되는 시스템.

청구항 12

제10항에 있어서,

상기 백업 키는 상기 제1 클라이언트로부터 복수의 상기 암호화된 키를 수신하는 것에 응답하여 상기 서버에 의해 랜덤하게 생성되는 시스템.

청구항 13

제10항에 있어서,

상기 서버는 상기 제2 클라이언트로부터 수신되는 복구 요청에 응답하여 상기 암호화된 비밀 키, 생성된 상기 백업 키, 및 상기 암호화된 랩핑 키를 상기 제2 클라이언트에 전송하도록 더 구성되고,

상기 제2 클라이언트와 연관된 메모리에 저장된 상기 백업 암호화된 복구 키는 상기 제2 클라이언트에서, 전송된 상기 백업 키의 함수로서 암호해독되어 상기 복구 키가 얻어지고, 전송된 상기 암호화된 랩핑 키는, 상기 제2 클라이언트에서, 얻어진 상기 복구 키의 함수로서 암호해독되어 상기 랩핑 키가 얻어지고, 전송된 상기 암호화된 비밀 키는 상기 제2 클라이언트에서 획득된 상기 랩핑 키의 함수로서 암호해독되어 상기 비밀 키가 얻어지는, 시스템.

청구항 14

데이터 통신 네트워크에 연결된 컴퓨터들 사이에서 비밀 데이터를 통신하기 위한 컴퓨터 실행가능 명령어들을 포함하는 컴퓨터 판독가능 저장 매체 - 상기 컴퓨터들은 상기 데이터 통신 네트워크에 연결된 제1 클라이언트 및 제2 클라이언트를 포함함 - 로서,

네트워크 서버에서, 비밀 키를 로밍하라는 제1 클라이언트의 사용자로부터의 요청에 응답하여 상기 제1 클라이언트에 의해 암호화된 복수의 키를 수신하는 제1 수신 명령어 - 상기 복수의 키는 상기 비밀 키와, 상기 사용자로부터 수신된 암호화 패스워드에 응답하여 상기 제1 클라이언트에 의해 생성된 랩핑 키와, 상기 제1 클라이언트에 의해 생성된 복구 키를 포함하고, 상기 비밀 키는 상기 랩핑 키의 함수로서 암호화되고, 상기 랩핑 키 및 상기 복구 키는 상기 서버에 알려지지 않고, 상기 서버는 상기 데이터 통신 네트워크에 연결됨 - ;

상기 서버에 의해, 상기 제1 클라이언트로부터 수신되는 상기 암호화된 복수의 키에 응답하여 백업 키를 생성하는 생성 명령어;

수신된 상기 암호화된 복수의 키 및 생성된 상기 백업 키를 상기 서버에 저장하는 저장 명령어;

상기 서버에서, 제2 클라이언트로부터 백업 데이터에 대한 요청을 수신하는 제2 수신 명령어; 및

수신된 상기 요청에 응답하여, 암호화된 상기 복구 키 및 상기 백업 키를 상기 서버로부터 상기 제2 클라이언트에 전송하는 전송 명령어 - 상기 제2 클라이언트는 전송된 상기 백업 키의 함수로서 암호화된 상기 복구 키를 나타내는 백업 암호화된 복구 키를 생성함 -

를 포함하는 컴퓨터 판독가능 저장 매체.

청구항 15

제14항에 있어서,

상기 전송 명령어는 상기 암호화된 비밀 키를 전송하는 명령어를 포함하고,

상기 암호화된 비밀 키는 상기 제2 클라이언트에서 상기 랩핑 키의 함수로서 암호해독되고, 상기 랩핑 키는 상기 제2 클라이언트의 사용자로부터 수신되는 암호화 패스워드에 응답하여 상기 제2 클라이언트상에 생성되는

컴퓨터 판독가능 저장 매체.

청구항 16

제14항에 있어서,

상기 제1 수신 명령어는, 상기 서버에서, 상기 서버에 알려지지 않은 복구 키의 함수로서 상기 제1 클라이언트에 의해 암호화된 상기 랩핑 키를 수신하고 - 상기 복구 키는 상기 제1 클라이언트를 통해 상기 사용자에 의해 선택된 복구 옵션에 응답하여 상기 제1 클라이언트 상에 생성됨 - , 상기 서버에서 상기 랩핑 키의 함수로서 상기 제1 클라이언트에 의해 암호화된 상기 복구 키를 수신하는 명령어를 더 포함하는, 컴퓨터 판독가능 저장 매체.

청구항 17

데이터 통신 네트워크에 연결된 컴퓨터들 사이에서 비밀 데이터를 통신하는 방법 - 상기 컴퓨터들은 상기 데이터 통신 네트워크에 연결된 제1 클라이언트 및 제2 클라이언트를 포함함 - 으로서,

서버에서, 로밍 클라이언트로부터 백업 데이터에 대한 요청을 수신하는 단계 - 상기 요청은 인증 패스워드의 다이제스트 값 또는 해쉬 값을 포함하고, 상기 서버는 상기 데이터 통신 네트워크에 연결됨 -;

상기 로밍 클라이언트로부터 수신된 상기 인증 패스워드의 형태가 유효한지 를 판정하는 단계;

상기 인증 패스워드의 형태가 유효한 경우, 상기 백업 데이터를 검색하는 단계 - 상기 백업 데이터는 백업 키 및 암호화된 복구 키를 포함하고, 상기 복구 키는 랩핑 키의 함수로서 암호화되고, 상기 랩핑 키는 암호화 패스워드의 함수로서 사전에 생성되어 있음 - ; 및

백업 암호화된 복구 키를 생성하기 위해 상기 검색된 백업 데이터를 상기 서버로부터 상기 로밍 클라이언트에 전송하는 단계

를 포함하는 방법.

청구항 18

제17항에 있어서,

전송된 상기 암호화된 복구 키를 상기 로밍 클라이언트에서 상기 랩핑 키의 함수로서 암호해독하는 단계를 더 포함하고,

상기 랩핑 키는 상기 로밍 클라이언트의 사용자로부터 수신된 상기 암호화 패스워드에 응답하여 상기 로밍 클라이언트 상에 생성되는 방법.

청구항 19

제17항에 있어서,

상기 전송된 백업 키의 함수로서 암호화된 상기 복구 키를 나타내는 상기 백업 암호화된 복구 키를 상기 로밍 클라이언트 상에 저장하는 단계

를 더 포함하는 방법.

청구항 20

제17항에 있어서,

상기 로밍 클라이언트의 사용자로부터 수신되는 복구 요청에 응답하여 저장된 백업 키를 검색하는 단계 - 상기 백업 키는 홈 클라이언트로부터 암호화된 비밀 데이터를 수신하는 것에 응답하여 상기 서버에 생성됨 - ;

상기 수신된 복구 요청에 응답하여 상기 백업 키를 상기 데이터 통신 네트워크를 통해 상기 서버로부터 상기 로

밍 클라이언트에 안전한 방식으로 전송하는 단계 - 상기 로밍 클라이언트는 상기 백업 암호화된 복구 키를 암호해독하여 상기 복구 키를 얻어냄 - ;

를 더 포함하는 방법.

청구항 21

제20항에 있어서,

수신된 상기 복구 요청에 응답하여 상기 서버로부터 상기 로밍 클라이언트에 암호화된 비밀 키와 암호화된 랩핑 키를 전송하는 단계를 더 포함하고,

상기 암호화된 랩핑 키는 얻어진 상기 복구 키의 함수로서 상기 로밍 클라이언트에서 암호해독되어 상기 랩핑 키가 얻어지고, 상기 암호화된 비밀 키는 얻어진 상기 랩핑 키의 함수로서 상기 로밍 클라이언트에서 암호해독되어 상기 비밀 키가 얻어지는, 방법.

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0018] 본 발명은 컴퓨터 네트워크 환경에 관한 것이다. 특히, 본 발명은 통신 네트워크을 통해 연결된 하나 이상의 클라이언트 컴퓨터들 사이에서 로밍 가능한 비밀 데이터의 백업 및 복구를 위한 시스템 및 방법에 관한 것이다.

[0019] 인터넷 사이트와 같은 웹 서비스들은 종종 그들의 사용자들에게 정보, 제품, 서비스 등을 제공한다. 그러나 사용자 및 웹 서비스의 같은 주요 관심사는, 특히 민감한 정보를 전송할 때의 인터넷의 보안이었다. 정보 보안은 종종 암호화 프로세스를 통해 사용자 및/또는 웹 서비스에 제공된다. 예컨대, 공개 키 기반구조(PKI) 및 공개 키 암호 시스템은 통신 보안을 위한 키 관리 서비스로서 알려져 있다. 이들 서비스는 대개, 프라이버시를 유지하기 위하여 비밀 키가 안전하게 저장되어야 하므로 단일 컴퓨터 상에서만 이용 가능하다. 따라서, 비밀 키를 로밍, 백업 및 복구할 수 있는 것이 바람직하다.

[0020] 기존의 비밀 키 로밍 프로토콜은 사용자가 주 패스워드를 기억할 수 없을 때 단말 대 단말 보안 관계 및 데이터의 복구를 해결하지 못한다. 따라서, 사용자 데이터 및 사용자 통신의 기밀, 프라이버시, 무결성 및 인증을 해결하면서 비밀 사용자 데이터를 로밍하기 위한 시스템이 요구된다.

발명이 이루고자 하는 기술적 과제

[0021] 본 발명은 통신 네트워크을 통해 연결된 하나 이상의 클라이언트들 사이에서의 비밀 정보의 개선된 로밍에 관한 것이다. 구체적으로, 본 발명은 서버가 비밀 정보(예컨대 비밀 키)에 대한 지식을 갖거나 심지어 비밀 정보를 수신하지 않고도 서버에 연결된 클라이언트들 사이에서 비밀 정보를 로밍할 수 있는 능력을 사용자에게 제공한다. 더욱이, 본 발명은, 심지어 사용자가 비밀 키의 암호화와 관련된 패스워드를 기억할 수 없을 때에도 클라이언트 상에서의 해독을 위해 서버로부터 비밀 키의 암호화 버젼을 검색할 수 있는 능력을 사용자에게 제공한다. 클라이언트들 사이에서 비밀 정보를 로밍하고 서버로부터 이러한 정보를 숨길 수 있는 능력을 사용자에게 제공함으로써, 통신 네트워크 보안성이 크게 향상되며, 따라서 악의 사용자들의 보안 통신을 방해하는 능력이 크게 감소된다.

[0022] 본 발명의 일 양태에 따르면, 데이터 통신 네트워크에 결합된 컴퓨터들 사이에 비밀 데이터를 통신하기 위한 방법이 제공된다. 이 방법은 통신 네트워크 서버에게 알려지지 않은 랩핑 키(wrapping key)의 함수로서 제1 클라이언트에 의해 암호화된 비밀 데이터를 통신 네트워크 서버에서 수신하는 단계를 포함한다. 서버 및 제1 클라이언트는 데이터 통신 네트워크에 결합된다. 이 방법은 수신된 암호화된 비밀 데이터를 서버에서 저장하는 단계를 더 포함한다. 이 방법은 암호화된 비밀 데이터에 대한 제2 클라이언트로부터의 요구를 서버에서 수신하는 단계를 더 포함한다. 이 방법은 수신된 요구에 응답하여 랩핑 키의 함수로서 해독하기 위해 암호화된 비밀 데이터를 서버에서 제2 클라이언트로 전송하는 단계를 더 포함한다.

[0023] 본 발명의 다른 양태에 따르면, 데이터 통신 네트워크에서 비밀 데이터를 통신하기 위한 시스템이 제공된다. 서버는 서버에게 알려지지 않은 랩핑 키의 함수로서 제1 클라이언트에 의해 암호화된 비밀 데이터를 수신한다. 서버 및 제1 클라이언트는 데이터 통신 네트워크에 결합된다. 하나의 데이터베이스가 서버와 연관된다. 서버는 수신된 암호화된 비밀 데이터를 데이터베이스에 저장하도록 구성된다. 서버는 또한 제2 클라이언트로부터 수신된 암호화된 비밀 데이터에 대한 요구에 응답하여 랩핑 키의 함수로서 해독하기 위해, 저장된 암호화된 비밀 데이터를 데이터 통신 네트워크에 결합된 제2 클라이언트에게 전송하도록 구성된다.

[0024] 본 발명의 또 다른 양태에 따르면, 데이터 통신 네트워크에 결합된 컴퓨터들 사이에 비밀 데이터를 통신하기 위한 컴퓨터 실행 가능 명령들을 구비한 컴퓨터 판독 가능 매체가 제공된다. 제1 수신 명령들이 서버에게 알려지지 않은 랩핑 키의 함수로서 제1 클라이언트에 의해 암호화된 비밀 데이터를 통신 네트워크 서버에서 수신한다. 서버 및 제1 클라이언트는 데이터 통신 네트워크에 결합된다. 저장 명령들이 수신된 암호화된 비밀 데이터를 서버에서 저장한다. 제2 수신 명령들이 암호화된 비밀 데이터에 대한 제2 클라이언트로부터의 요구를 서버에서 수신한다. 전송 명령들이, 수신된 요구에 응답하여 랩핑 키의 함수로서 해독하기 위해, 암호화된 비밀 데이터를 서버에서 제2 클라이언트로 전송한다.

[0025] 본 발명의 또 다른 양태에 따르면, 데이터 통신 네트워크에 결합된 컴퓨터들 사이에 비밀 데이터를 통신하기 위한 방법에 제공된다. 이 방법은 암호화된 비밀 데이터에 대한 로밍 클라이언트로부터의 요구를 서버에서 수신하는 단계를 포함한다. 요구는 인증 패스워드의 다이제스트 또는 해쉬 값을 포함한다. 서버 및 로밍 클라이언

트는 데이터 통신 네트워크에 결합된다. 이 방법은 로밍 클라이언트로부터 수신된 인증 패스워드의 형태가 유효한지를 판정하는 단계를 더 포함한다. 이 방법은 또한 인증 패스워드의 형태가 유효한 때 암호화된 비밀 데이터를 검색하는 단계를 더 포함하는데, 이 비밀 데이터는 서버에게 알려지지 않은 암호화 패스워드의 함수로서 이전에 암호화되었다. 이 방법은 또한 랩핑 키의 함수로서 해독하기 위해, 수신된 암호화된 비밀 데이터를 서버에서 로밍 클라이언트로 전송하는 단계를 더 포함한다.

[0026] 본 발명의 또 다른 양태에 따르면, 데이터 구조가 저장된 컴퓨터 판독 가능 매체가 제공된다. 제1 데이터 필드가 비밀 데이터를 포함한다. 제2 데이터 필드가 사용자로부터 수신된 입력 데이터 스트림을 표현하는 키 데이터를 포함한다. 제3 함수 필드가 키 데이터의 함수로서 비밀 데이터를 암호화하고, 암호화된 비밀 데이터를 저장을 위해 중앙 위치로 전송한다.

[0027] 대안으로, 본 발명은 다양한 다른 방법 및 장치를 포함할 수 있다.

발명의 구성 및 작용

[0028] 이제 도 1을 참조하면, 홈 또는 로컬 클라이언트 컴퓨터(102)가 데이터 통신 네트워크(104)에 결합된다. 이 예에서, 통신 네트워크(104)은 인터넷(또는 WWW)이다. 그러나, 본 발명의 가르침은 어떠한 데이터 통신 네트워크에도 적용될 수 있다. 다수의 로밍 또는 원격 클라이언트 컴퓨터(106, 108)도 통신 네트워크(104)에 결합된다. 또한, 홈 클라이언트 컴퓨터(102)는 통신 네트워크(104)을 통해 로밍 클라이언트 컴퓨터(106, 108)와 통신할 수 있다. 홈 클라이언트 컴퓨터(102)는, 사용자가 믿을만한 이유를 가진 컴퓨터를 나타내는데, 이는 믿지 못할 제3자가 그에 대해 무제한으로 또는 쉽게 액세스할 수 없기 때문이다. 로밍 클라이언트 컴퓨터(106, 108)는 보다 제한된 믿음을 가진 컴퓨터를 나타내는데, 이는 이 컴퓨터가 제3자에 의해 소유되고 물리적으로 제어되기 때문이다. 통신 네트워크(104)에 결합된 인증 서버(11)는 그 자체와 홈 클라이언트 컴퓨터(102) 및 로밍 클라이언트 컴퓨터(106, 108) 사이의 통신을 허용한다. "인증 서버"로 지칭되지만, 실시예에서의 인증 서버(110)는 단지, 사용자를 인증하는 것은 물론 웹 브라우저 및 다른 웹 서버와 상호작용할 수 있는 웹 서버이다.

[0029] 이 예에서, 데이터는 정보를 안전하게 교환하기 위해 인터넷에서 일반적으로 사용되는 프로토콜인 보안 소켓 계층(SSL)을 이용하여 인증 서버(110), 클라이언트 컴퓨터 시스템(102) 및 로밍 클라이언트 컴퓨터(106, 108) 사이에서 통신된다. 구체적으로, SSL은 공개 키 암호화를 구현하는 데 사용될 수 있다. 이 분야의 전문가에게 알려진 바와 같이, 공개 키 암호화는 비밀 키를 가진 개인(또는 컴퓨터)만이 정보를 디코딩할 수 있는 방식으로 정보를 인코딩하는 것을 포함한다. 오늘날 사용되는 컴퓨터 암호화 시스템들은 대칭 키 암호화 및 공개 키 암호화를 포함한다.

[0030] 대칭 키 암호화에 있어서, 각각의 컴퓨터는 비밀 키(코드)를 갖는데, 이 키는 통신 네트워크을 통해 다른 컴퓨터에 전송되기 전에 정보의 패킷을 암호화하는 데 사용될 수 있다. 대칭 키는 어느 컴퓨터들과 통신하고 있는지, 그래서 그 각각의 컴퓨터에 키를 설치할 수 있어야 함을 알 것을 요구한다. 이러한 타입의 암호화가 성공적이기 위해, 양 컴퓨터는 정보를 디코딩할 수 있도록 비밀 코드를 알아야 한다.

[0031] 공개 키 암호화에 있어서, 비밀 키 및 공개 키의 조합이 정보를 코딩 및 디코딩하는 데 사용된다. 예를 들어, 특정 발신 컴퓨터(예컨대, 홈 클라이언트)는 공개/비밀 키 쌍을 가진 로밍 클라이언트(예컨대 로밍 클라이언트)로 정보를 보안 전송한다. 발신 컴퓨터는 암호화된 메시지를 생성하기 위해 정보에 대해 행해지는 수학적 연산에서 로밍 클라이언트의 공개 키를 사용하며, 메시지의 무결성을 표명하기 위해 그 자신의 비밀 키로 이 메시지에 서명할 수 있다. 발신 컴퓨터는 또한 그의 공개 키를 로밍 클라이언트에 제공하지만, 비밀 키는 발신 컴퓨터에 비밀로 유지된다. 암호화된 메시지를 디코딩하기 위해, 수신자는 그 자신의 비밀 키를 사용해야 하며, 메시지 상의 서명을 확인하기 위해 송신자로부터 제공된 공개 키를 사용한다. 따라서, 수신자, 즉 홈 클라이언트(102)의 사용자가 로밍 클라이언트(106, 108)를 통해 암호화된 메시지를 디코딩할 수 있는 능력을 원하는 경우, 사용자는 비밀 키를 로밍 클라이언트로 전송해야 한다.

[0032] 인증 데이터베이스(112)는 인증 서버(110)에 결합되며, 클라이언트 컴퓨터 시스템(102)의 사용자를 인증하는 데 필요한 정보, 및 홈 클라이언트 컴퓨터 또는 로밍 클라이언트 컴퓨터의 사용자가 데이터베이스에 암호화 데이터를 저장할 수 있는 권한을 갖는지, 그리고/또는 데이터베이스(11)로부터 암호화 데이터를 수신하는지를 판정하는 데 필요한 정보를 갖는다.

[0033] 이제 도 2를 참조하면, 도 2의 블록도는 본 발명의 일 실시예에 따라 홈 클라이언트(202)(예컨대 홈 클라이언트 컴퓨터 102)와 웹 서버(204)(예컨대 인증 서버 110) 사이에서 암호화된 비밀 데이터를 통신하기 위한 시스템

(200)을 나타낸다.

[0034] 홈 클라이언트 애플리케이션(206)은 사용자(208)가 비밀 데이터를 암호화하고 통신 네트워크(212)(예를 들어 통신 네트워크 104)을 통해 암호화된 비밀 데이터를 웹 서버(204)로 전송하는 것을 허용한다. 홈 클라이언트 애플리케이션(206)은 홈 클라이언트(202)에 의해, 비밀 데이터의 암호화를 개시하기 위한 사용자 입력, 및 암호화된 비밀 데이터의 웹 서버(204)로의 전송에 응답하여 실행될 수 있다. 이 실시예에서, 홈 클라이언트 애플리케이션(206)은 도 1을 참조하여 전술한 바와 같이 공개 키 암호화 프로세스 동안 사용되는 비밀 키(216)를 저장하는 메모리(214)를 포함한다. 홈 클라이언트 애플리케이션(206)은 비밀 데이터를 암호화된 비밀 데이터로 변환하기 위해 비밀 데이터에 대한 수학적 연산을 수행하기 위한 암호화 알고리즘(218)을 포함한다. 구체적으로, 암호화 알고리즘(218)은 비밀 데이터를 변환하기 위한 키 데이터와 함께 사용된다. 이 분야의 전문가들에게 알려진 바와 같이, 많은 암호화 알고리즘(예컨대, 3DES 및 HMAC-RC4)이 암호화 키를 알지 않고는 컨텐츠를 거의 해독할 수 없도록 데이터를 암호화하는 데 사용될 수 있다.

[0035] 홈 클라이언트(202)의 사용자는 하나 이상의 로밍 클라이언트(예를 들어, 로밍 클라이언트 106, 108)를 통해 웹 서비스들과 보안 통신하기 위하여 비밀 키(216)를 로밍할 수 있는 능력을 원할 수 있다. 그러나 이러한 비밀 키의 로밍은 비밀 키(216)가 악의 자에 의해 가로채이는 결과를 낳을 수 있다. 결과적으로, 특정 비밀 키(216)로 데이터를 안전하게 해독하거나 서명할 수 있는 사용자(208)의 능력이 크게 손상될 수 있다.

[0036] 홈 클라이언트(202)에 연결된 사용자 인터페이스(UI; 220)는 사용자가 웹 서버(204)와 상호작용하는 것을 허용한다. 예를 들어, UI(214)는 데이터 및/또는 입력 양식을 보기 위한 컴퓨터 모니터와 같은 디스플레이(217), 데이터를 입력 양식(도시되지 않음)에 입력하기 위한 키보드 또는 포인팅 장치(예컨대, 마우스, 트랙볼, 펜 또는 터치 패드)와 같은 입력 장치(219)를 포함할 수 있다. 즉, UI(214)는 사용자(208)가 암호화를 위해 홈 클라이언트(210) 상에 데이터를 입력하는 것을 허용하고, 사용자(208)가 저장을 위해 암호화된 데이터를 홈 클라이언트(202)에서 웹 서버(204)로 전송하려는 요구를 제출하는 것을 허용한다.

[0037] 데이터베이스(226)(예컨대, 110)는 웹 서버(204)에 결합되며, 암호화된 비밀 데이터를 데이터베이스(226)에 저장하기 위해 홈 클라이언트(202)(통신 네트워크 상의 다른 사용자들도 포함)로부터의 요구를 검증하는 데 필요한 정보를 포함한다. 데이터베이스(210)가 인증 서버(204)와 분리되어 도시되어 있지만, 본 발명의 다른 실시예에서 데이터베이스(210)는 웹 서버(208) 내에 포함될 수 있다는 것을 이해해야 한다.

[0038] 일 실시예에서, 웹 서버(204)는 서버(204)에 대한 액세스를 요구하는 사용자(208)를 인증하기 위한 인증 서비스(227)를 실행하는 로그인 서버이다. 이 실시예에서, 웹 서버(204)는 사용자가 웹 서버(204)에 의해 제공되는 웹 서비스에 액세스하는 것을 허용하기 전에 참조 문자(229)에 의해 지시되는 바와 같이 인증 패스워드와 같은 사용자로부터의 인증 정보를 먼저 요구한다.

[0039] 도 2를 더 참조하면, 홈 클라이언트(202)는 홈 클라이언트 애플리케이션(206)을 이용하여 암호화된 비밀 키를 서버(204) 상에 저장하기를 원한다. 이를 행하기 전에, 홈 클라이언트 애플리케이션(206)은 서버(204)에 대해 사용자(208)를 인증/허가하는 것을 필요로 한다. 이 실시예에서, 사용자(208)에 의해 제공되는 인증 패스워드는 서버(204)에 대해 사용자(208)를 인증하는 데 사용된다.

[0040] 비밀 데이터를 안전하게 전송 및 저장하기 위하여, 홈 클라이언트 애플리케이션(206)은 사용자(208)로부터의 암호화 패스워드와 같은 입력 데이터를 요구한다. 홈 클라이언트 애플리케이션(206) 및 UI(220)는 사용자(208)가 암호화 패스워드를 입력하는 것을 허용한다. 홈 클라이언트 애플리케이션(206)은 사용자(208)에 의한 암호화 패스워드 입력에 응답하여 비밀 키를 암호화하는 데 사용되는 랩핑 키(K1 230)를 생성한다. 이 실시예에서, 랩핑 키(K1)는 비밀 키를 암호화하는 데 사용되는 대칭 키이다(예를 들어 해쉬 값 생성). 홈 클라이언트 애플리케이션(206)은 참조 문자(232)에 의해 지시되는 바와 같이 암호화된 비밀 데이터를 서버 로밍 애플리케이션(228)으로 전송한다. 인증 패스워드 및 암호화 패스워드는 사용자 데이터의 프라이버시를 보호하기 위하여 개별 패스워드들로서 도시되어 있다. 그러나 이들은 단일 패스워드일 수 있다는 점을 이해해야 한다. 또한, 웹 서버(204)는 스마트 카드, 1회용 패스워드는 물론 바이오메트릭스와 같은, 사용자(208)를 인증하기 위한 다른 인증 메카니즘들을 사용할 수 있다는 것을 이해해야 한다.

[0041] 서버(204)에 의해 실행되는 서버 로밍 애플리케이션(208)(즉, 웹 서비스)은 참조 문자에 의해 지시되는 바와 같이 수신된 암호화된 비밀 데이터를 데이터베이스(226)에 저장한다. 이 예에서, 비밀 데이터는 메모리(216)에 저장된 비밀 키(216)이고, 이 비밀 키는 암호화된 비밀 키(E_{k1}PK 234)를 생성하기 위해 생성된 랩핑 키(230)의 함수로서 암호화 알고리즘(218)에 의해 암호화된다. 더욱이, 서버는 랩핑 키(230)를 생성하는 데 사용되는 암

호화 패스워드를 소유하지 않으므로, 서버 로밍 애플리케이션은 암호화된 비밀 키(234)를 해독할 수 없다.

[0042] 이제 도3을 참조하면, 도 3의 블록도는 본 발명의 일 실시예에 따라 로밍 클라이언트(302)와 웹 서버(204) 사이에서 암호화된 비밀 데이터를 통신하기 위한 시스템을 나타낸다.

[0043] 이 실시예에서, 서버 로밍 애플리케이션(228)은 데이터베이스(226)로부터 저장된 암호화된 비밀 데이터를 검색하기 위한 로밍 클라이언트(302)로부터의 요구를 로밍 클라이언트 애플리케이션(304) 및 통신 네트워크(213)을 통해 수신한다. 서버 로밍 애플리케이션(228)은 수신된 요구에 응답하여, 로밍 사용자(306)를 인증하기 위해 웹 서버(204)에 의해 실행될 수 있다. 이 실시예에서, 서버(204)는 도 2a에 도시된 바와 같은 입력 양식을 통해 로밍 사용자(306)로부터 인증 패스워드를 요구한다.

[0044] 도 2를 참조하여 전술한 것과 실질적으로 동일한 방식으로, 서버 로밍 애플리케이션(228)은 로밍 서버(306)가 데이터베이스로부터 암호화된 데이터를 검색하도록 허가되는지를 판정하기 위해 클라이언트로부터 수신된 인증 패스워드의 양식을 검증한다. 인증 패스워드가 유효하지 않은 경우, 서버 로밍 애플리케이션(228)은 데이터베이스(226)에 저장된 암호화된 비밀 데이터에 대한 로밍 클라이언트(302) 액세스를 거부한다. 대안으로, 인증 패스워드가 유효한 경우에는, 서버 로밍 애플리케이션(228)은 참조 문자(310)에 의해 지시되는 바와 같이 데이터베이스(226)로부터 암호화된 데이터를 검색하여, 참조 문자(311)에 의해 지시되는 바와 같이 암호화된 데이터를 로밍 클라이언트(302)로 전송한다. 로밍 클라이언트 애플리케이션(304)은 수신된 암호화된 비밀 데이터에 응답하여, 사용자로부터 암호화 패스워드(308)를 요구하여 랩핑 키(K1)를 생성하고, 해독 알고리즘(312)(308은 도 3에서 틀리게 도시되어 있다)을 실행한다. 이 경우, 해독 알고리즘(312)은 로밍 클라이언트(302) 상에 생성된 랩핑 키(230)의 함수로서 수신된 암호화된 비밀 데이터를 해독하여 홈 클라이언트(202)와 관련된 비밀 키를 얻는다. 이후, 로밍 클라이언트 애플리케이션(304)은 얻어진 비밀 키를 로밍 클라이언트(302)와 관련된 메모리(314)에 저장할 수 있다.

[0045] 이제 도 4를 참조하면, 도 4의 블록도는 본 발명의 다른 바람직한 실시예에 따라 홈 클라이언트 컴퓨터(202)와 서버(204) 사이에서 암호화된 비밀 데이터 및 복구 데이터를 통신하기 위한 시스템(400)을 나타낸다.

[0046] 이 실시예에서, 홈 사용자(208)는 UI(220)를 사용하여, 사용자가 암호화 패스워드를 기억할 수 없는 경우에도 서버(204) 상에 저장된 암호화된 비밀 데이터를 복구할 수 있는 능력을 갖는 복구 옵션을 선택한다. 이 실시예에서, 도 2를 참조하여 전술한 바와 같이 암호화 패스워드의 함수로서 랩핑 키(K1)를 생성하는 것 외에, 로밍 클라이언트 애플리케이션(212)은 복구 키 요구에 응답하여, 새로운 암호화 키(즉, 복구 키 K2)를 임의로 생성한다. 예를 들어, 사용자(208)가 암호화 패스워드를 양식(도시되지 않음)에 입력한 후, 사용자는 예를 들어 마우스를 이용하여 "암호화 패스워드없이 비밀 데이터 복구를 가능하게 함" 메시지를 표시하는 대화 상자와 함께 사용자에게 제공되는 "예" 버튼을 클릭한다. 홈 클라이언트 애플리케이션(206)은 사용자에 의한 "예" 선택에 응답하여, 복구 키(K2)를 임의로 생성한다. K2는 어떠한 방식으로도 암호화 패스워드에 연결되지 않는다는 점은 주목할 만하다. 서버 로밍 애플리케이션(228)은 클라이언트로부터 수신된 인증 패스워드를 검증함으로써 사용자(208)를 인증한다. 인증 패스워드가 유효한 경우, 사용자(208)는 랩핑 키(E_{k1}PK 234)에 의해 암호화된 비밀 키, 복구 키(E_{k2}K1 414)에 의해 암호화된 랩핑 키, 및 랩핑 키(E_{k1}K2 416)에 의해 암호화된 복구 키를 포함하는 암호화된 비밀 데이터를 418, 419 및 420에 의해 각각 지시된 바와 같이 서버(204)로 전송하는 것이 허용된다. 서버 로밍 애플리케이션(228)은 수신된 암호화된 비밀 데이터에 응답하여, E_{k1}PK, E_{k2}K1 414 및 E_{k1}K2를 421, 422 및 423에 각각 지시된 바와 같이 데이터베이스(226)에 저장한다. 더욱이, 서버 로밍 애플리케이션(228)은 홈 클라이언트(202)로부터 수신된 암호화된 데이터에 응답하여, 425에 의해 지시되는 바와 같이 데이터베이스(226)에 저장하기 위해 백업 키(K3 424)를 임의로 생성하고, 생성된 백업 키(424)를 426에 의해 지시되는 바와 같이 홈 클라이언트(226)로 전송한다. K3의 전송은 보안 채널을 통해(예를 들어 SSL을 통해) 발생한다는 점에 유의한다. 보안 채널이 없는 경우, 그 값은 복구 키가 쉽게 발견될 수 있도록 변경될 수 있다. 홈 클라이언트 애플리케이션(206)은 수신된 백업 키(424)에 응답하여, 제2의 암호화된 복구 키(E_{k3}K2 428)를 생성하여 메모리 및/또는 홈 클라이언트(202)와 관련된 디스크 상에 저장한다.

[0047] 이 실시예에서, 암호화 알고리즘(216)은 암호화된 비밀 키(234), 암호화된 랩핑 키(414), 제1 암호화된 복구 키(416) 및 제2 암호화된 복구 키(428)를 생성하는 데 사용된다. 암호화된 비밀 키(234)는 랩핑 키의 함수로서 암호화된 비밀 키를 나타내고, 암호화된 랩핑 키(414)는 복구 키(K2)의 함수로서 암호화된 랩핑 키를 나타내며, 제1 암호화된 복구 키(416)는 랩핑 키(K1)의 함수로서 암호화된 복구 키(408)를 나타내고, 제2 암호화된 복구 키(428)는 백업 키(424)의 함수로서 암호화된 복구 키(408)를 나타낸다. 본 발명이 본 명세서에서 동일한 암호

화 알고리즘을 이용하는 것으로 설명되지만, 상이한 암호화 알고리즘들이 상이한 암호화된 키들 각각을 생성하는 데 사용될 수 있다는 점이 고려된다.

[0048] 이제 도 5를 참조하면, 본 발명의 일 실시예에 따라 서버(204)로부터 로밍 클라이언트(302)로 복구 데이터를 전송하는 시스템(500)에 대한 블럭도가 도시되어 있다.

[0049] 본 실시예에서, 서버 로밍 애플리케이션(228)은 원격 로밍 클라이언트 애플리케이션(304) 및 통신 네트워크를 통해서 로밍 클라이언트(302)로부터 요청을 수신하여 데이터베이스(226)로부터 백업 데이터를 검색한다. 이러한 경우에 있어서, 백업 데이터는 제1 암호화된 복구 키(416) 및 백업 키(424)이다. 서버 로밍 애플리케이션(228)은 클라이언트로부터 수신된 인증 패스워드의 형식의 유효성을 검사하여 사용자(208)를 인증한다. 인증 패스워드가 유효한 경우에는, 참조 부호(506,508)로 각각 나타난 바와 같이 서버 로밍 애플리케이션(228)은 데이터베이스(226)로부터 제1 암호화된 복구 키(416) 및 백업 키(424)를 검색하고, 참조 부호(510,512)로 각각 나타난 바와 같이 $E_{K1}K2$ 및 K3를 로밍 클라이언트 애플리케이션(304)에 전송한다. 이와 달리, 인증 패스워드가 유효하지 않은 경우에는 서버 로밍 애플리케이션(228)은 데이터베이스(226)에의 액세스를 거부한다.

[0050] 로밍 클라이언트 애플리케이션(304)은 수신된 제1 암호화된 복구 키(416)에 응답하여 사용자로부터 암호화 패스워드(504)를 요청하고, 랩핑 키(K1)를 생성하고 암호해독 알고리듬(312)을 실행한다. 이 경우에, 암호해독 알고리듬(312)은 수신된 제1 암호화된 복구 키(416)를 로밍 클라이언트(302)상에 생성되는 랩핑 키(230)의 함수로서 암호해독하여 홈 클라이언트 컴퓨터(202)와 관련된 복구 키(408)를 획득한다. 로밍 클라이언트 애플리케이션(304)은 수신된 백업 키(424)에 응답하여 암호화 알고리듬(218)을 실행한다. 이 경우에, 암호화 알고리듬(218)은 획득된 복구 키(408)를 수신된 백업 키(424)의 함수로서 암호화하여 제2 암호화된 복구 키(428)를 생성한다. 그 후에, 로밍 클라이언트 애플리케이션(304)은 제2 암호화된 복구 키(428)를 메모리(314) 및 로밍 클라이언트(302)와 관련된 디스크에 저장한다. 제2 암호화된 복구 키(428), 백업 키(424) 및 암호화된 랩핑 키를 서버로부터 메모리(314)에 저장한 결과로서, 로밍 클라이언트(302)는 랩핑 키(K1)를 생성하는 데에 이용된 패스워드(즉, 암호화 패스워드)를 알지 못하여도 데이터베이스(226)에 저장되는 비밀 키(234)를 복구하고 암호해독할 수 있다.

[0051] 이제 도 6을 참조하면, 본 발명의 일 실시예에 따라 암호화 패스워드를 알지 못하여도 로밍 클라이언트(302)에서 웹 서버(204)로부터 암호화된 비밀 데이터를 복구하는 시스템(600)을 도시하는 블럭도가 나타나 있다.

[0052] 본 실시예에서, 상기된 백업 프로세스는 로밍 클라이언트(302) 상에서 수행되어 로밍 클라이언트(302)는 제2 암호화된 복구 키(428)를 메모리(314) 내에 가진다. 서버 로밍 애플리케이션(228)은 로밍 클라이언트 애플리케이션(304) 및 통신 네트워크(212)를 통해서 로밍 클라이언트(302)로부터 요청을 수신하여 데이터베이스(226)로부터 비밀 키(216)와 같은 암호화된 비밀 데이터를 검색한다. 서버 로밍 애플리케이션(228)은 클라이언트로부터 수신된 인증 패스워드의 유효성을 검사하여 사용자(302)를 인증한다. 사용자가 성공적으로 인증된 경우에는 서버 애플리케이션은 암호화된 비밀 데이터(216)를 로밍 클라이언트 애플리케이션(304)에 전송한다. 도 3 및 도 5를 참조하여 상기된 바와 같이, 로밍 클라이언트 애플리케이션(304)은 암호화된 비밀 데이터에 응답하여 랩핑 키(K1)를 생성하기 위하여 암호화 패스워드를 로밍 사용자(306)에 요청한다.

[0053] 사용자(306)가 암호화 패스워드를 기억하지 못하는 경우에는, 예컨대 사용자는 UI를 이용하여 "암호화 패스워드를 입력하지 않고서 비밀 데이터를 복구"라는 메시지를 디스플레이하는 다른 대화 박스(도시되지 않음)와 함께 사용자에게 제공되는 "예" 옵션을 선택한다. 서버 로밍 애플리케이션(228)은 참조 부호 610, 612 및 614에 의해서 각각 나타난 바와 같이 복구 요청에 응답하여 백업 키(424), 암호화된 비밀 키(234) 및 암호화된 랩핑 키(414)를 데이터베이스(226)로부터 검색하고, 검색된 K3, $E_{K1}PK$ 및 $E_{K2}K1$을 로밍 클라이언트 애플리케이션(304)에 전송한다.

[0054] 로밍 클라이언트 애플리케이션(304)은 수신된 백업 키(424), 암호화된 비밀 키(234) 및 암호화된 랩핑 키(414)에 응답하여 암호해독 알고리듬(312)을 실행한다. 이 경우에, 암호해독 알고리듬(312)은 메모리에 이전에 저장된 제2 암호화된 복구 키(428)(도 5 참조)를 수신된 백업 키(424)의 함수로서 암호해독하여 홈 클라이언트(202)와 관련된 복구 키(408)를 획득한다. 그런 다음, 암호해독 알고리듬(312)은 수신된 암호화 랩핑 키(414)를 획득된 복구 키(408)의 함수로서 암호해독하여 랩핑 키(230)를 획득한다. 그런 다음, 암호해독 알고리듬(312)은 수신된 암호화된 비밀 키(234)를 획득된 랩핑 키(230)의 함수로서 암호해독하여 홈 클라이언트(202)와 관련된 비밀 키(216)를 획득한다. 그 후에, 로밍 클라이언트 애플리케이션(304)은 획득된 비밀 키(PK)를 로밍 클라이언트(302)와 관련된 메모리(214)에 저장한다.

[0055] 이제 도 7을 참조하면, 본 발명의 일 실시예에 따라 로밍 클라이언트 컴퓨터에 의해서 비밀 데이터 복구를 돕는, 홈 클라이언트 컴퓨터와 서버 사이의 비밀 데이터의 통신 방법의 예시적인 흐름도가 도시되어 있다. 단계 702에서, 홈 클라이언트 컴퓨터의 사용자는 홈 클라이언트 애플리케이션을 실행하고 홈 클라이언트 컴퓨터와 관련된 메모리내에 저장된 비밀 데이터(예컨대, 비밀 키)를 지정하여 암호화하고 서버에 전송한다. 단계 704에서, 홈 클라이언트 애플리케이션은 사용자에 암호화 패스워드를 요청한다. 단계 706에서, 랩핑 키가 사용자로부터 수신된 암호화 패스워드의 함수로서 생성된다. 단계 708에서, 지정된 비밀 데이터는 생성된 랩핑 키의 함수로서 암호화된다. 단계 710에서, 홈 클라이언트 애플리케이션은 암호화된 데이터를 서버 로밍 애플리케이션을 실행하는 서버에 전송한다. 단계 712에서, 서버 애플리케이션은 전송된 암호화된 비밀 데이터에 응답하여 암호화된 비밀 데이터가 서버에 연결된 데이터베이스에 저장된다.

[0056] 이제 도 8을 참조하면, 본 발명의 일 실시예에 따라 암호화된 비밀 데이터를 서버로부터 로밍 클라이언트 컴퓨터에 전송하는 방법을 도시하는 예시적인 흐름도가 나타나 있다.

[0057] 단계 802에서, 로밍 클라이언트 애플리케이션을 실행하는 로밍 클라이언트 컴퓨터는 서버 로밍 애플리케이션을 실행하는 서버에 암호화된 비밀 데이터의 전송을 요청한다. 본 예에서, 사용자는 도 7을 참조하여 상기 설명된 바와 같은 방법에 의해서 서버에 연결된 데이터베이스 내에 이전에 저장된 암호화된 비밀 키($E_{K1}PK$)의 전송을 요청한다. 단계 804에서, 로밍 클라이언트 애플리케이션은 암호화 패스워드를 사용자에 요청한다. 단계 806에서, 랩핑 키는 로밍 클라이언트 애플리케이션에 의해서 사용자로부터 수신된 암호화 패스워드의 함수로서 생성된다. 인증 서비스는 먼저 패스워드 매칭과 같은 소정의 인증 메카니즘을 이용하여 사용자를 인증한다. 단계 808의 인증에 실패하는 경우에, 단계 809에서 서버 로밍 애플리케이션은 요청된 암호화된 데이터에의 사용자 액세스를 거부한다. 단계 808의 인증에 성공하는 경우에, 단계 810에서 서버 로밍 애플리케이션은 데이터베이스로부터 요청된 암호화된 비밀 키($E_{K1}PK$)를 검색하고, 검색된 암호화된 비밀 키를 로밍 클라이언트 컴퓨터에 전송한다. 단계 812에서, 로밍 클라이언트 애플리케이션은 수신된 암호화된 비밀 키($E_{K1}PK$)를 생성된 랩핑 키(230)의 함수로서 암호해독하여 비밀 키(PK)를 획득한다.

[0058] 이제 도 9a 및 도 9b를 참조하면, 본 발명의 일 실시예에 따라 홈 클라이언트 컴퓨터와 서버 사이에 비밀 데이터와 복구 데이터의 통신 방법을 도시하는 예시적인 흐름도가 나타나 있다.

[0059] 단계 902에서, 홈 클라이언트 컴퓨터의 사용자는 로밍 클라이언트 애플리케이션을 수행하고 홈 클라이언트 컴퓨터의 메모리 내에 저장된 비밀 데이터를 지정하여 암호화하고 지정된 비밀 데이터를 서버에 전송하는 요청을 제기한다. 단계 904에서, 도 8을 참조하여 상기 논의된 바와 같이 요청이 인증된 경우에, 서버는 로밍 서버 애플리케이션을 실행한다. 단계 906에서 서버 로밍 애플리케이션이 이것이 처음 실행인 것으로 판정하거나, 또는 백업 키(K3)가 이 사용자에 대한 데이터베이스에서 발견될 수 없는 경우에, 단계 908에서 서버 로밍 애플리케이션은 랜덤 백업 키(K3)를 생성한다. 단계 910에서, 서버 로밍 애플리케이션은 백업 키(K3)를 데이터베이스에 저장하고, 단계 912에서 복구 데이터를 암호화하는 데에 이용하기 위하여 백업 키(K3)를 홈 클라이언트 애플리케이션에 제공한다. 단계 907에서 서버 로밍 애플리케니션이 이것이 처음의 실행이 아닌 것으로 판정한 경우에, 단계 909에서 서버 로밍 애플리케이션은 데이터베이스로부터 백업 키를 검색하고, 단계 912에서 복구 데이터를 암호화하는 데에 이용하기 위하여 백업 키(K3)를 홈 클라이언트 애플리케이션에 제공한다.

[0060] 이제 도 9b를 참조하면, 단계 914에서, 홈 클라이언트 애플리케이션은 랩핑 키(K1)를 사용자에 의해서 제공되는 암호화 패스워드의 함수로서 생성한다. 단계 916에서, 홈 클라이언트 애플리케이션은 복구 키(K2)가 홈 클라이언트 컴퓨터 상에 저장되는지 여부를 판정한다. 단계 916에서, 홈 플라이언트 애플리케이션이 복구 키(K2)가 홈 클라이언트와 관련된 메모리내에 저장되지 않으며, 제1 암호화된 복구 키($E_{K1}K2$)가 서버 상에 존재하지 않는 것으로 판정하는 경우에, 단계 918에서 홈 클라이언트 애플리케이션은 랜덤 복구 키(K2)를 생성한다. 예컨대, 이것이 홈 클라이언트 애플리케이션의 제1 실행인 경우에, 복구 키는 홈 클라이언트 컴퓨터 상에 존재하지 않을 것이다. 단계 916의 홈 클라이언트 애플리케이션이 복구 키(K2)가 홈 클라이언트와 관련된 메모리 내에 저장된 것으로 판정한 경우에, 단계 920에서 홈 클라이언트 애플리케이션은 메모리로부터 복구 키(K2)를 검색한다. 단계 922에서, 홈 클라이언트 애프리케이션은 암호화된 비밀 키를 생성하고, 랩핑 키(K1), 제1 암호화된 복구키 및 제2 암호화된 복구 키를 생성한다. 암호화된 비밀 키는 비밀 키(PK)가 생성된 랩핑 키(K1)의 함수로서 암호화되었음을 나타낸다. 암호화된 랩핑 키($E_{K2}K1$)는 랩핑 키(K1)가 복구 키(K2)의 함수로서 암호화되었음을 나타낸다. 제1 암호화된 복구 키($E_{K1}K2$)는 복구 키(K2)가 랩핑 키(K1)의 함수로서 암호화되었음을 나타낸다. 제2 암호화된 복구 키($E_{K3}K2$)는 복구 키(K2)가 서버로부터 전송된 백업 키(K3)의 함수로서 암호화되었음을 나타낸다.

단계 924에서, 홈 클라이언트 애플리케이션은 제2 암호화된 복구 키($E_{K3}K2$)를 홈 클라이언트 컴퓨터와 관련된 메모리에 저장한다. 단계 926에서, 홈 클라이언트 애플리케이션은 암호화된 비밀 키, 암호화된 랩핑 키 및 제1 암호화된 복구 키 및 제1 암호화된 복구 키를 서버에 전송한다. 도 9a를 다시 참조하면, 단계 928에서 서버 로밍 애플리케이션은 전송된 암호화된 비밀 키, 암호화된 랩핑 키 및 제1 암호화된 복구 키를 수신하여 데이터베이스내에 저장한다.

[0061] 이제 도 10을 참조하면, 로밍 클라이언트가 암호화 패스워드없이 비밀 데이터를 검색할 수 있도록 하기 위하여 서버로부터 로밍 클라이언트로 복구 데이터를 전송하는 방법을 도시하는 예시적인 흐름도가 나타난다. 단계 1002에서, 로밍 서버 애플리케이션을 실행하는 서버는 로밍 클라이언트 애플리케이션을 시행하는 로밍 클라이언트의 사용자로부터 인증 패스워드를 수신하고, 복구 데이터를 이동시키거나 백업하도록 요청한다. 단계 1004에서, 로밍 클라이언트는 인증된 사용자에 의해서 제공되는 암호화된 패스워드에 응답하여 랩핑 키(K1)를 생성한다. 단계 1006에서, 백업 키(K3) 및 제1 암호화된 복구 키($E_{K1}K2$)가 로밍 서버 애플리케이션에 의해서 로밍 클라이언트 애플리케이션에 전송된다. 로밍 클라이언트 애플리케이션은 수신된 제1 암호화된 복구 키($E_{K1}K2$)를 생성된 랩핑 키(K1)의 함수로서 암호해독하여 K2를 획득한다. 단계 1010에서, 클라이언트 애플리케이션은 획득된 복구 키(K2)를 수신된 백업 키(K3)의 함수로서 암호화하여 제2 암호화된 복구 키($E_{K3}K2$)를 생성한다. 단계 1012에서, 로밍 클라이언트 애플리케이션은 생성된 제2 암호화된 복구 키를 로밍 클라이언트 컴퓨터와 관련된 메모리에 저장한다.

[0062] 이제 도 11을 참조하면, 암호화 패스워드 없이 서버로부터 비밀 데이터를 로밍 클라이언트에 복구하는 방법을 나타내는 예시적인 흐름도가 도시되어 있다. 단계 1102에서, 서버는 로밍 클라이언트 애플리케이션을 실행하는 로밍 클라이언트로부터 인증된 패스워드를 수신하고, 암호화 패스워드 없이 암호화된 비밀 키의 전송을 요청한다. 단계 1104에서, 로밍 서버 애플리케이션은 백업 키, 암호화된 랩핑 키($E_{K2}K1$) 및 암호화된 비밀 키($E_{K1}PK$)를 데이터베이스로부터 검색한다. 단계 1106에서, 로밍 서버 애플리케이션은 검색된 백업 키, 암호화된 랩핑 키 및 암호화된 비밀 키를 로밍 클라이언트에 전송한다. 단계 1108에서, 로밍 클라이언트 애플리케이션은 이전에 로밍 클라이언트상에 저장된(도 10 참조) 제2 암호화된 복구 키($E_{K3}K2$)를 검색된 백업 키(K3)의 함수로서 암호해독하여 복구 키(K2)를 획득한다. 단계 1110에서, 로밍 클라이언트 애플리케이션은 암호화된 랩핑 키($E_{K2}K1$)를 획득된 복구 키(K2)의 함수로서 암호해독하여 랩핑 키(K1)를 획득한다. 단계 1112에서, 로밍 클라이언트 애플리케이션은 암호화된 비밀 키를 획득된 랩핑 키의 함수로서 암호해독한다.

[0063] 특히, 클라이언트 상에 K2를 생성하고 이를 서버에 노출하지 않음으로써, 서버 상의 암호화된 패스워드 키(K1)와 복구 키(K2)를 알려지지 않은 상태에서도 백업할 수 있게 된다. 동시에, 클라이언트는 2개의 키중 적어도 하나를 알고 있으므로, 즉 사용자가 암호화 패스워드 K1 또는 이전에 클라이언트에 저장된 K2를 입력하면, 클라이언트는 $E_{K1}K2$ 및 $E_{K2}K1$를, 비밀 데이터를 복원하고 또한 백업을 수행하는 데에 이용할 수 있다.

[0064] 도 12는 컴퓨터(130) 형태의 범용 컴퓨팅 장치의 일 예를 나타낸다. 본 발명의 일 실시예에서, 컴퓨터(130)와 같은 컴퓨터는 본 명세서에 도시되고 설명되는 다른 도면에서 이용하기에 적당하다. 컴퓨터(130)는 하나 이상의 프로세서 또는 처리 유닛(132) 및 시스템 메모리(134)를 포함한다. 도시된 실시예에서, 시스템 버스(136)는 시스템 메모리(134)를 포함하는 다양한 시스템 컴포넌트를 프로세서(132)에 접속시킨다. 버스(136)는 메모리 버스 또는 메모리 제어기, 주변 버스, 가속화된 그래픽 포트 및 프로세서 또는 임의의 다양한 버스 구조를 이용하는 로컬 버스를 포함하는 임의의 다수의 타입의 버스 구조를 나타낸다. 한정적인 것이 아니라 예시적으로, 이러한 구조는 ISA(Industry Standard Architecture) 버스, MCA(Micro Channel Architecture) 버스, EISA(Enhanced ISA) 버스, VESA(Video Electronics Standards Association) 로컬 버스 및 메자닌(Mezzanine) 버스로도 알려진 PCI(Peripheral Component Interconnect) 버스를 포함한다.

[0065] 컴퓨터(130)는 전형적으로 적어도 몇몇 형태의 컴퓨터 판독가능 매체를 포함한다. 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함하는 컴퓨터 판독 가능 매체는 컴퓨터(130)에 의해서 액세스될 수 있는 임의의 이용가능한 매체일 수 있을 것이다. 한정적인 것이 아니라 예시적으로, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 포함한다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령, 데이터 구조, 프로그램 모듈 또는 다른 데이터와 같은 정보의 저장을 위해서 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 포함한다. 예컨대, 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래쉬 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital versatile disks) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치 또는 원하는 정보를 저장하는 데에 이용될 수 있으며, 컴퓨터

(130)에 의해서 액세스될 수 있는 임의의 기타 매체를 포함한다. 통신 매체는 전형적으로 반송파 또는 기타 전송 메카니즘과 같은 변조된 데이터 신호에 컴퓨터 판독 가능 명령, 데이터 구조, 프로그램 모듈 또는 기타 데이터를 구현하며, 임의의 정보 전달 매체를 포함한다. 본 발명의 기술 분야의 당업자는 신호 내에 정보를 인코딩하기 위하여 하나 이상의 특성 세트를 가지거나 그러한 방식으로 변경되는 변조된 데이터 신호라는 용어에 익숙할 것이다. 유선 네트워크 또는 직접 유선 접속과 같은 유선 매체와, 음향, RF, 적외선 및 기타 무선 매체와 같은 무선 매체는 통신 매체의 일 예이다. 상술한 것들 중 임의의 조합이 컴퓨터 판독가능 매체의 범위 내에 포함된다.

[0066] 시스템 메모리(134)는 분리형 및/또는 비분리형, 휘발성 및/또는 비휘발성 메모리 형태의 컴퓨터 저장 매체를 포함한다. 도시된 실시예에서, 시스템 메모리(134)는 ROM(138) 및 RAM(140)을 포함한다. 가령, 시동중에 컴퓨터(130) 내의 요소들 간의 정보의 전송을 돕는 기본 루틴을 포함하는 BIOS(142)는 전형적으로 ROM(138) 내에 저장된다. RAM(140)은 전형적으로 즉각적으로 액세스가능하며/액세스가능하거나 현재 프로세싱 유닛(132) 상에서 처리되는 데이터 및/또는 프로그램 모듈을 포함한다. 한정적인 것이 아니라 예시적으로, 도 12는 오퍼레이팅 시스템(144), 애플리케이션 프로그램(146), 기타 프로그램 모듈(148) 및 프로그램 데이터(150)를 도시한다.

[0067] 컴퓨터(130)는 기타 분리형/비분리형, 휘발성/비휘발성 컴퓨터 저장 매체를 포함할 수 있을 것이다. 예컨대, 도 12는 비분리형, 비휘발성 자기 매체로부터 판독하거나, 이들에 기록하는 하드 디스크 드라이브(154)를 포함한다. 또한, 도 12는 분리형, 비휘발성 자기 디스크(158)로부터 판독하거나 이에 기록하는 자기 디스크 드라이브(156)와, CD-ROM 또는 기타 광 매체와 같은 분리형, 비휘발성 광 디스크(162)로부터 판독하거나 이에 기록하는 광 디스크 드라이브(160)를 도시한다. 예시적인 오퍼레이팅 환경에서 이용될 수 있는 기타 분리형/비분리형, 휘발성/비휘발성 컴퓨터 저장 매체는 자기 테이프 카세트, 플래쉬 메모리 카드, DVD, 디지털 비디오 테이프, 반도체 RAM, 반도체 ROM 등을 포함하며, 이에 한정되는 것은 아니다. 하드 디스크 드라이브(154), 자기 디스크 드라이브(156) 및 광 디스크 드라이브(160)는 전형적으로 인터페이스(166)와 같은 비휘발성 메모리 인터페이스에 의해서 시스템 버스(136)에 접속된다.

[0068] 상기 논의되고 도 12에 도시된 드라이브 또는 기타 대량 저장 장치 및 그와 관련된 컴퓨터 저장 매체는 컴퓨터 판독가능 명령, 데이터 구조, 프로그램 모듈 및 기타 데이터를 제공한다. 도 12에서, 예컨대 하드 디스크 드라이브(154)는 오퍼레이팅 시스템(170), 애플리케이션 프로그램(172), 기타 프로그램 모듈 및 프로그램 데이터(176)를 저장하는 것으로 도시되어 있다. 이들 컴포넌트들은 오퍼레이팅 시스템(144), 애플리케이션 프로그램(146), 기타 프로그램 모듈(148) 및 프로그램 데이터(150)와 동일할 수도, 혹은 상이할 수도 있다. 오퍼레이팅 시스템(170), 애플리케이션 프로그램(172), 기타 프로그램 모듈(174) 및 프로그램 데이터(176)에는 본 명세서에서는 상이한 참조 부호가 부여되었는데, 이는 최소한 이들이 상이한 복사본임을 나타내기 위함이다.

[0069] 사용자는 키보드(180) 및 포인팅 장치(182)(예컨대, 마우스, 트랙볼, 펜 또는 터치 패드)와 같은 입력 장치 또는 사용자 안터페이스 선택 장치를 통해서 커맨드 및 정보를 입력할 수 있을 것이다. 기타 입력 장치들(도시되지 않음)은 마이크로폰, 조이스틱, 게임 패드, 위성 안테나, 스캐너 등을 포함할 수 있을 것이다. 이들 및 기타 입력 장치들은 시스템 버스(136)에 결합되는 사용자 입력 인터페이스(184)를 통해서 프로세싱 유닛(132)에 접속되지만, 병렬 포트, 게임 포트 또는 USB와 같은 다른 인터페이스 및 버스 구조에 의해서 접속될 수 있을 것이다. 모니터(188) 또는 다른 타입의 디스플레이 장치 또한 비디오 인터페이스(190)와 같은 인터페이스를 통해서 시스템 버스(136)에 접속될 수 있을 것이다. 모니터(188)에 추가하여, 컴퓨터는 종종 프린터 및 스피커와 같은 기타 주변 출력 장치(도시되지 않음)를 포함하며, 이들은 출력 주변 인터페이스(도시되지 않음)를 통해서 접속될 수 있을 것이다.

[0070] 컴퓨터(130)는 로밍 클라이언트(194)와 같은 하나 이상의 로밍 클라이언트에의 논리 접속을 이용하여 네트워킹된 환경에서 동작할 수 있을 것이다. 로밍 클라이언트(194)는 퍼스널 컴퓨터, 서버, 라우터, 네트워크 PC, 피어 장치 또는 기타 공통 네트워크 노드일 수 있으며, 전형적으로 컴퓨터(130)와 관련하여 상기된 대부분의 요소 또는 모든 요소를 포함한다. 도 12에 도시된 논리 접속은 LAN(196) 및 WAN(198)을 포함하며, 다른 네트워크를 포함할 수도 있을 것이다. 이러한 네트워킹 환경은 사무실, 기업형 컴퓨터 네트워크, 인트라넷 및 글로벌 컴퓨터 네트워크에서 통상적인 것이다.

[0071] 네트워킹 환경에서 이용되는 경우에, 컴퓨터(130)는 네트워크 인터페이스 또는 어댑터(186)를 통해서 LAN(196)에 접속된다. WAN 환경에서 이용되는 경우에, 컴퓨터(130)는 전형적으로 모뎀(178) 또는 인터넷과 같이 WAN(198)을 통해서 통신을 확립하는 다른 수단을 포함한다. 내장형 또는 외장형일 수 있는 모뎀은 사용자 입력 인터페이스(184) 또는 다른 적절한 메카니즘을 통해서 시스템 버스(136)에 접속될 수 있을 것이다. 네트워킹된

환경에서, 컴퓨터(130)와 관련하여 도시된 프로그램 모듈, 또는 그 일부는 원격 메모리 저장 장치(도시되지 않음)에 저장될 수 있을 것이다. 한정적인 것이 아니라 예시적으로, 도 12는 원격 애플리케이션 프로그램(192)이 메모리 장치 상에 상주하는 것으로 나타나 있다. 도시된 네트워킹 환경은 예시적이며, 컴퓨터들간의 통신 연결을 확립하는 다른 수단이 이용될 수 있음을 이해할 수 있을 것이다.

[0072] 통상적으로, 컴퓨터(130)의 데이터 프로세서는 컴퓨터의 다양한 컴퓨터 판독가능 저장 매체에 상이한 시간에 저장된 명령에 의해서 프로그래밍된다. 프로그램 및 오퍼레이팅 시스템은 전형적으로, 예컨대 플로피 디스크 또는 CD-ROM 상에 분산된다. 이들로부터 프로그램 또는 오퍼레이팅 시스템은 컴퓨터의 부차적 메모리내에 설치되거나 로딩된다. 실행시에, 이들은 컴퓨터의 주메모리에 적어도 부분적으로 로딩된다. 본 명세서에 기재된 발명은 이들 및 다른 다양한 타입의 컴퓨터 판독가능 저장 매체가 마이크로 프로세서 또는 기타 데이터 프로세서와 관련하여 아래에 기술되는 단계를 수행하는 명령 또는 프로그램을 포함하는 경우에 이들을 포함한다. 본 발명은 본 명세서에 기술되는 방법 및 기술에 따라 프로그램되는 경우에 컴퓨터 자체를 또한 포함한다.

[0073] 설명을 위하여, 오퍼레이팅 시스템과 같은 프로그램 또는 기타 실행가능 프로그램 컴포넌트가 본 명세서에서 이산 블록으로 나타나 있다. 그러나, 컴퓨터의 상이한 저장 컴포넌트에 다양한 시간에 상주하는 이러한 프로그램 및 컴포넌트는 컴퓨터의 데이터 프로세서에 의해서 실행된다.

[0074] 컴퓨터(130)를 포함하는 예시적인 컴퓨터 시스템 환경과 결합하여 기술되었지만, 본 발명은 많은 다른 범용 또는 특수 목적 컴퓨팅 시스템 환경 또는 구성에서도 동작가능하다. 이러한 컴퓨팅 시스템 환경은 본 발명의 이용 범위 또는 기능에 관하여 어떠한 제한을 암시하기 위한 것은 아니다. 더우기, 이러한 컴퓨팅 시스템 환경은 예시적인 오퍼레이팅 환경에 나타난 임의의 컴포넌트 또는 컴포넌트의 조합과 관련된 임의의 의존성 또는 요구사항을 가지는 것으로 해석되어서는 안된다. 본 발명을 이용하기에 적합한 잘 알려진 컴퓨팅 시스템, 환경 및/또는 구성은 퍼스널 컴퓨터, 서버 컴퓨터, 핸드헬드 또는 랩탑 장치, 멀티프로세서 시스템, 마이크로프로세서 기반 시스템, 셋톱 박스, 프로그래밍가능한 가전제품, 네트워크 PC , 미니컴퓨터, 메인프레임 컴퓨터, 상기된 시스템 또는 장치 중 임의의 것을 포함하는 분산 컴퓨팅 환경 등을 포함하며, 이에 한정되는 것은 아니다.

[0075] 본 발명은 하나 이상의 컴퓨터 또는 다른 장치에 의해서 실행되는 프로그램 모듈과 같은 컴퓨터 실행가능 명령의 통상적인 컨텍스트로 기술될 수 있을 것이다. 통상적으로, 프로그램 모듈은 루틴, 프로그램, 오브젝트, 컴포넌트 및 특정 업무를 수행하거나 특정한 추상 데이터 타입을 실행하는 데이터 구조를 포함하며, 이에 한정되는 것은 아니다. 본 발명은 통신 네트워크를 통해서 연결된 원격 프로세싱 장치에 의해서 업무가 수행되는 분산 컴퓨팅 환경에서 실시될 수 있을 것이다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 메모리 저장 장치를 포함하는 로컬 및 로밍 클라이언트 저장 매체 내에 위치할 수 있을 것이다.

[0076] 동작시에, 컴퓨터(130)는 비밀 데이터를 암호화 및 전송하고/전송하거나 비밀 데이터를 검색 및 암호해독하도록 도 7 내지 도 11에 나타난 것과 같은 컴퓨터 실행가능 명령을 실행한다.

[0077] 본 발명의 요소 또는 그 실시예를 설명하는 경우에, "하나의", "그" 및 "상기"라는 용어는 하나 이상의 요소가 존재함을 의미하기 위한 것이다. "포함하는" 및 "구비하는"이라는 용어는 포함하는 것을 의미하는 것이며 이는 열거된 요소외의 추가적인 요소가 존재할 수 있음을 의미한다.

[0078] 상기된 바에 의해서, 본 발명의 몇몇 목적들이 달성되며, 다른 장점들이 결과적으로 얻어질 것이다.

[0079] 본 발명의 범위를 벗어나지 않고서 구성 및 방법에 있어서 다양한 변경이 이루어질 수 있으므로, 상기 설명에 포함되고, 첨부된 도면에 도시된 모든 사항은 한정적인 의미로 사용된 것이 아니라, 예시적인 의미로 사용된 것으로 해석되어야 할 것이다.

발명의 효과

[0080] 본 발명은 사용자 데이터 및 사용자 통신의 기밀, 프라이버시, 무결성 및 인증을 해결하면서 비밀 사용자 데이터를 로밍하기 위한 시스템을 제공한다.

도면의 간단한 설명

[0001] 도 1은 본 발명이 이용될 수 있는 예시적인 통신 네트워크 환경의 블록도.

[0002] 도 2는 본 발명의 일 실시예에 따라 홈 클라이언트와 서버 사이에서 암호화된 비밀 데이터를 통신하기 위한 시스템의 블록도.

[0003] 도 3은 본 발명의 일 실시예에 따라 로밍 클라이언트 컴퓨터와 서버 사이에서 암호화된 비밀 데이터를 통신하기 위한 시스템의 블록도.

[0004] 도 4는 본 발명의 일 실시예에 따라 홈 클라이언트와 서버 사이에서 암호화된 비밀 데이터 및 복구 데이터를 통신하기 위한 시스템의 블록도.

[0005] 도 5는 본 발명의 일 실시예에 따라 서버에서 로밍 클라이언트로 복구 데이터를 전송하기 위한 시스템의 블록도.

[0006] 도 6은 본 발명의 일 실시예에 따라 암호 패스워드 없이 서버에서 로밍 클라이언트로 암호화된 비밀 데이터를 복구하기 위한 시스템의 블록도.

[0007] 도 7은 본 발명의 일 실시예에 따라 홈 클라이언트와 서버 사이에서 비밀 데이터를 통신하기 위한 방법의 흐름도.

[0008] 도 8은 본 발명의 일 실시예에 따라 서버에서 로밍 클라이언트로 암호화된 비밀 데이터를 전송하기 위한 방법의 흐름도.

[0009] 도 9a 및 9b는 본 발명의 일 실시예에 따라 서버와 홈 클라이언트 사이에서 암호화된 비밀 데이터 및 복구를 통신하기 위한 방법의 흐름도.

[0010] 도 10은 본 발명의 일 실시예에 따라 서버와 로밍 클라이언트 사이에서 복구 데이터를 통신하는 방법의 흐름도.

[0011] 도 11은 본 발명의 일 실시예에 따라 암호 패스워드 없이 서버에서 로밍 클라이언트로 암호화된 비밀 데이터를 복구하는 방법의 흐름도.

[0012] 도 12는 본 발명이 구현될 수 있는 적절한 컴퓨팅 시스템 환경의 일례를 나타내는 블록도.

[0013] 도면들에서 대응하는 참조 문자들은 대응하는 부분들을 나타낸다.

[0014] <도면의 주요부분에 대한 부호의 설명>

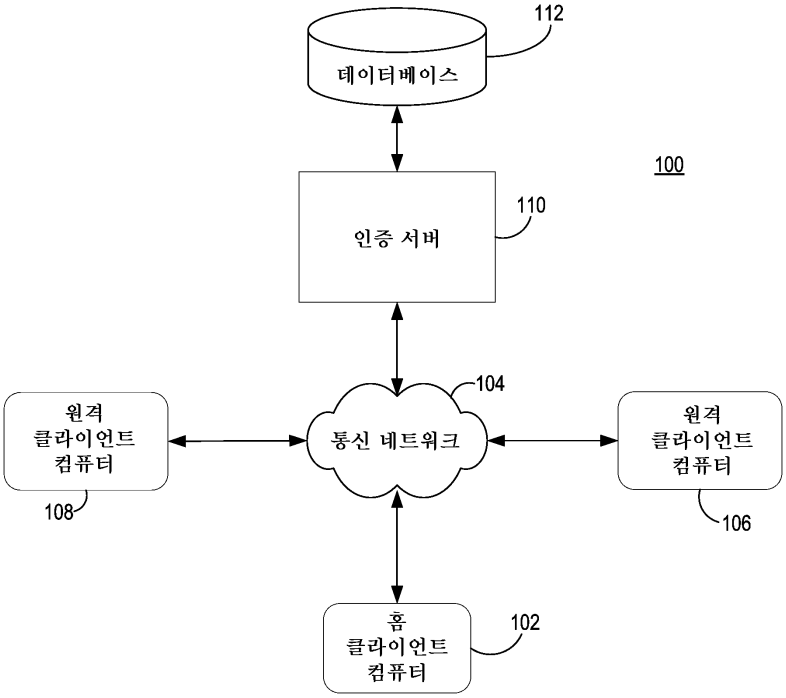
[0015] 102 : 홈 클라이언트 104 : 통신 네트워크

[0016] 110 : 인증 서버 106, 108 : 원격 클라이언트 컴퓨터

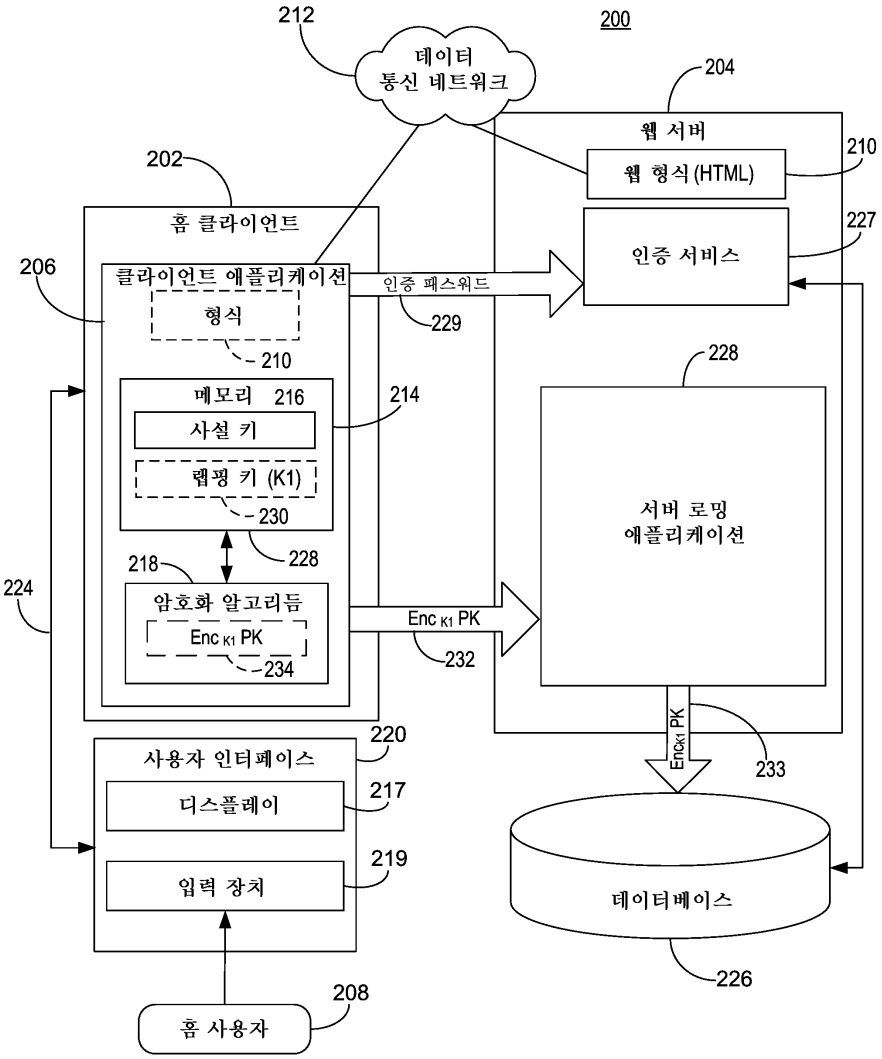
[0017] 112 : 데이터베이스

도면

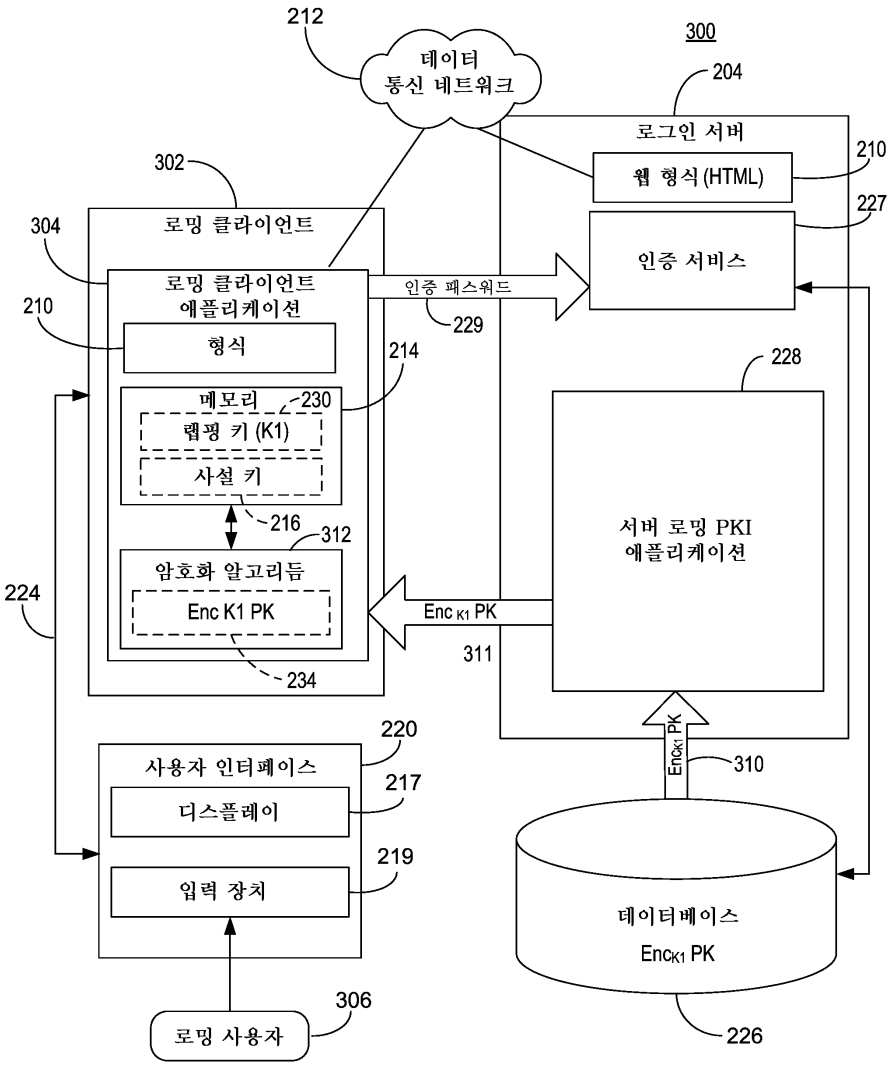
도면1


112
데이터베이스
100
110
인증 서버
104
원격
클라이언트
컴퓨터
108
통신 네트워크
원격
클라이언트
컴퓨터
106
홈
클라이언트
컴퓨터
102

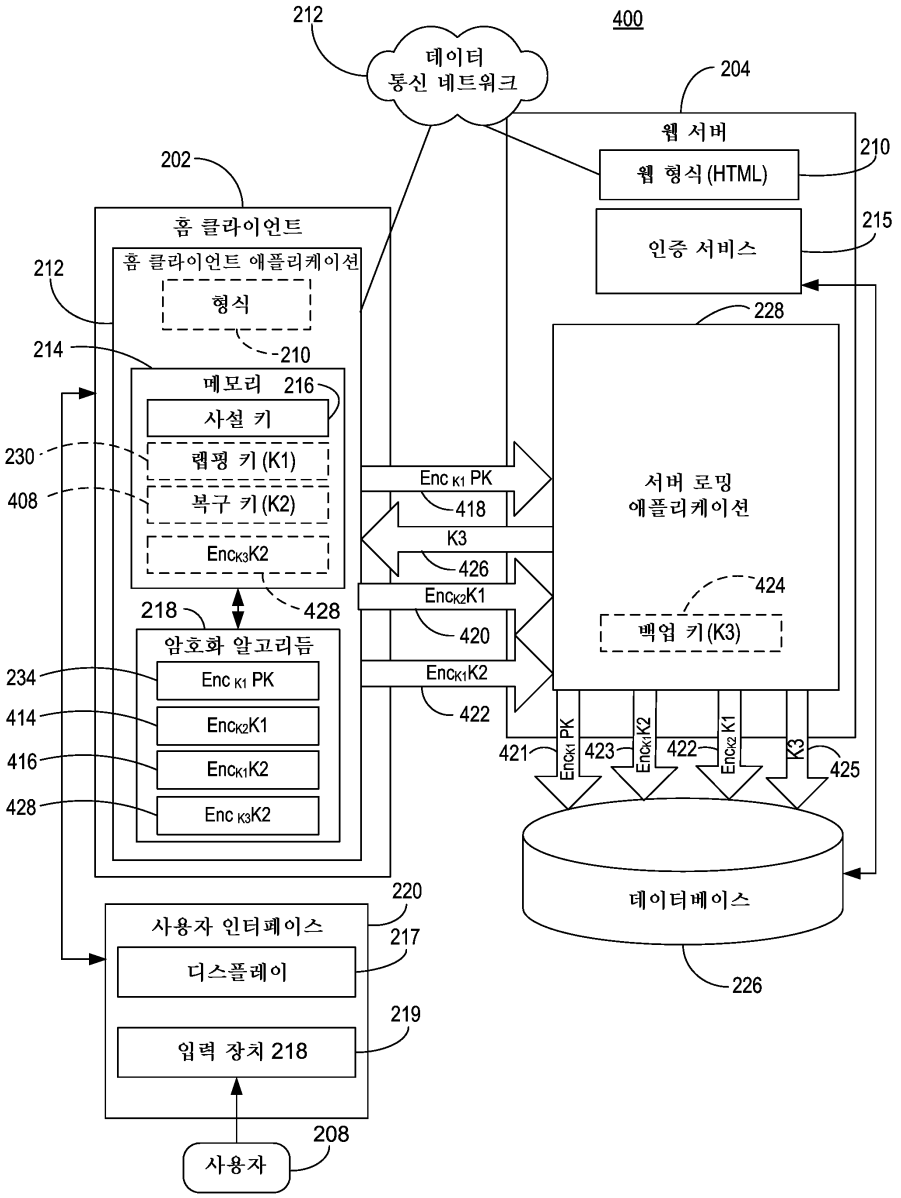
도면2


212
데이터
통신 네트워크
200
204
웹 서버
웹 형식(HTML)
210
202
홈 클라이언트
206
클라이언트 애플리케이션
형식
210
인증 패스워드
229
인증 서비스
227
228
서버 로밍
애플리케이션
메모리 216
사설 키
랩핑 키 (K1)
230
214
228
218
암호화 알고리듬
Enc K1 PK
234
224
Enc K1 PK
232
Enc K1 PK
233
220
사용자 인터페이스
디스플레이
217
입력 장치
219
데이터베이스
226
208
홈 사용자

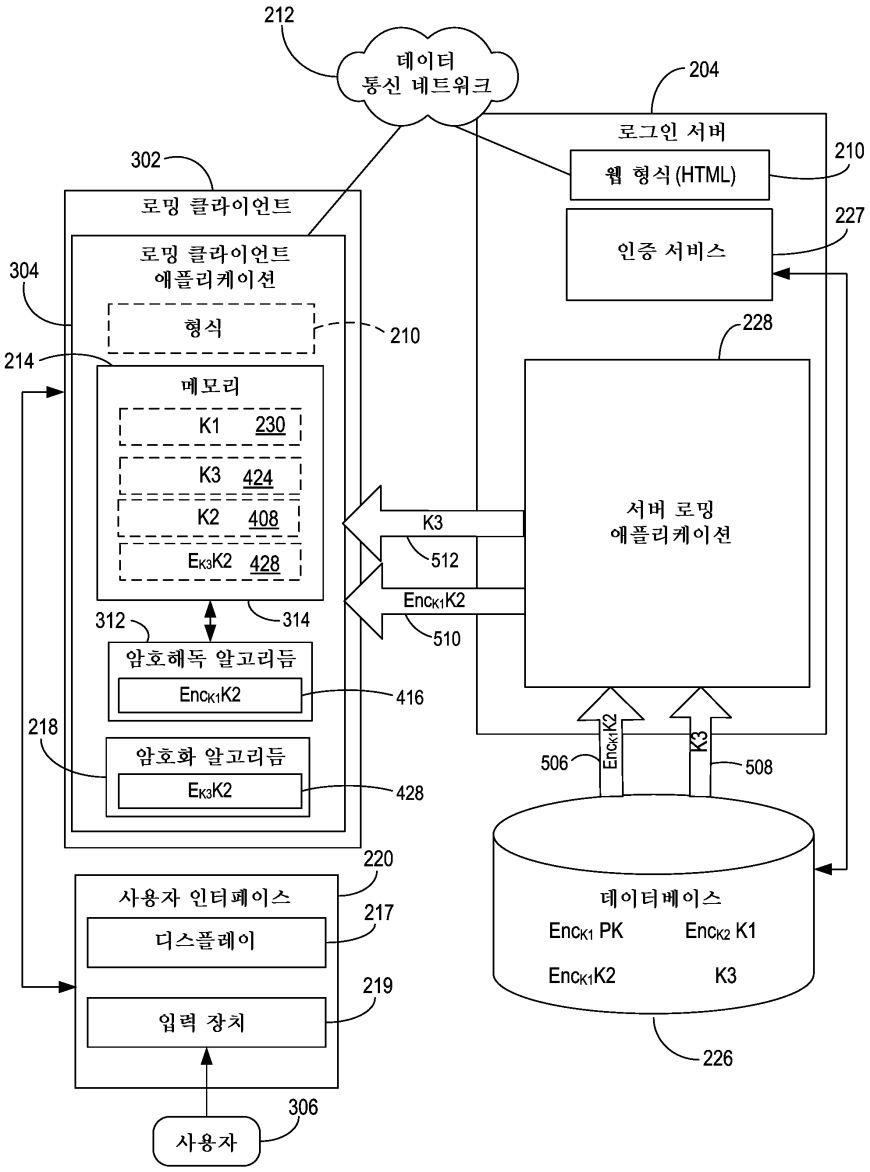
도면3


212
데이터
통신 네트워크
300
204
로그인 서버
웹 형식 (HTML)
210
227
인증 서비스
302
로밍 클라이언트
304
로밍 클라이언트
애플리케이션
210
형식
인증 패스워드
229
214
228
메모리
230
랩핑 키 (K1)
사설 키
216
312
암호화 알고리듬
Enc K1 PK
224
Enc K1 PK
311
서버 로밍 PKI
애플리케이션
234
220
사용자 인터페이스
217
디스플레이
219
입력 장치
Enc K1 PK
310
데이터베이스
Enc K1 PK
306
로밍 사용자
226

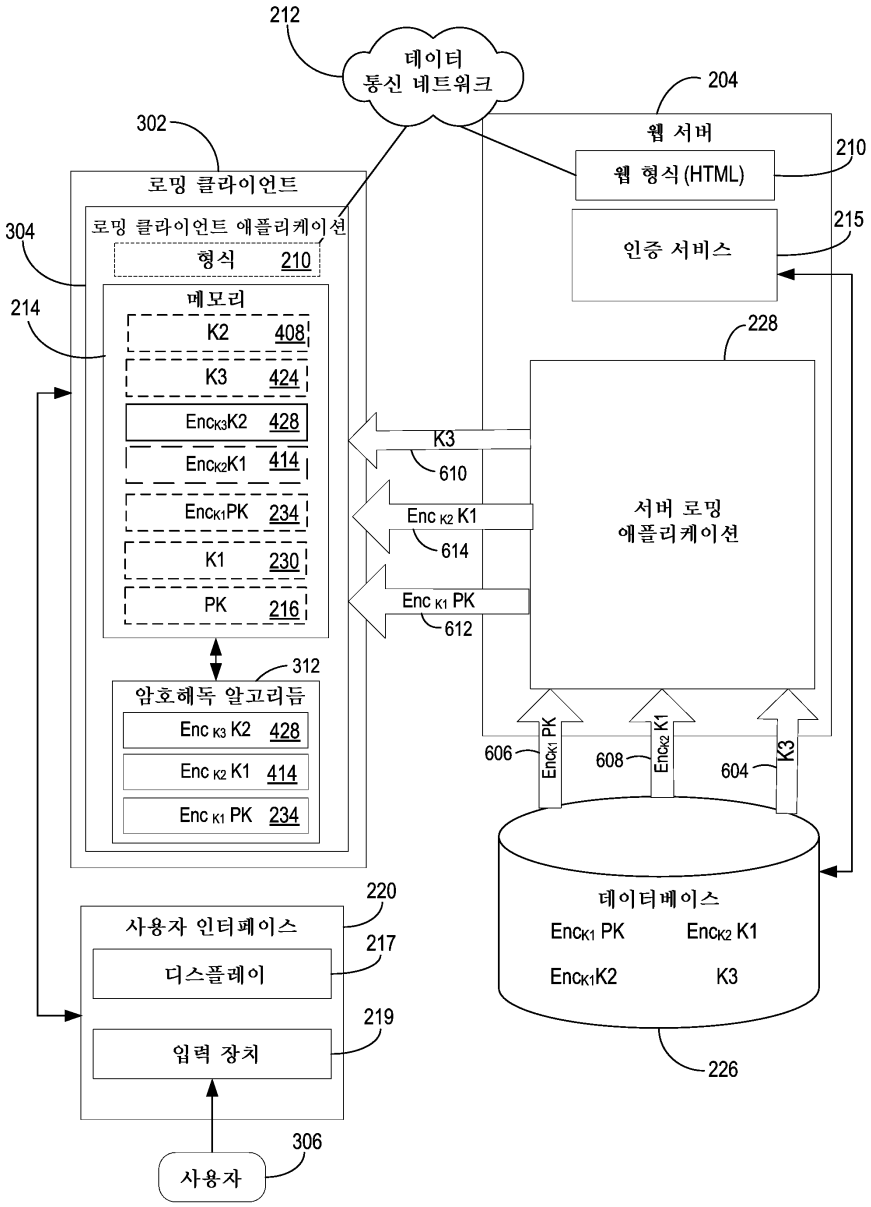
도면4


400
212
데이터
통신 네트워크
204
웹 서버
웹 형식 (HTML)
210
215
인증 서비스
202
홈 클라이언트
홈 클라이언트 애플리케이션
212
형식
210
214
228
메모리
216
사설 키
230
랩핑 키 (K1)
408
복구 키 (K2)
Enc K3K2
428
218
암호화 알고리듬
Enc K1 PK
Enc K2K1
Enc K1K2
Enc K3K2
234
414
416
428
Enc K1 PK
418
K3
426
Enc K2K1
420
Enc K1K2
422
서버 로밍
애플리케이션
424
백업 키 (K3)
421
Enc K1 PK
423
Enc K1K2
422
Enc K2 K1
K3
425
데이터베이스
226
220
사용자 인터페이스
217
디스플레이
219
입력 장치 218
208
사용자

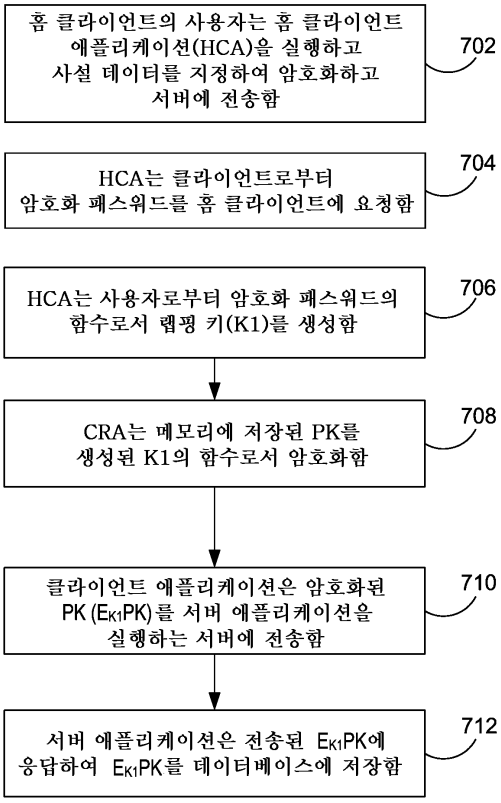
도면5


212
데이터
통신 네트워크
204
로그인 서버
웹 형식 (HTML)
210
227
인증 서비스
228
서버 로밍
애플리케이션
302
로밍 클라이언트
로밍 클라이언트
애플리케이션
304
형식
210
214
메모리
K1 230
K3 424
K2 408
EK3K2 428
K3
512
EncK1K2
510
312
314
암호해독 알고리듬
EncK1K2
416
218
암호화 알고리듬
EK3K2
428
506
EncK1K2
K3
508
220
사용자 인터페이스
217
디스플레이
219
입력 장치
306
사용자
데이터베이스
EncK1 PK
EncK2 K1
EncK1K2
K3
226

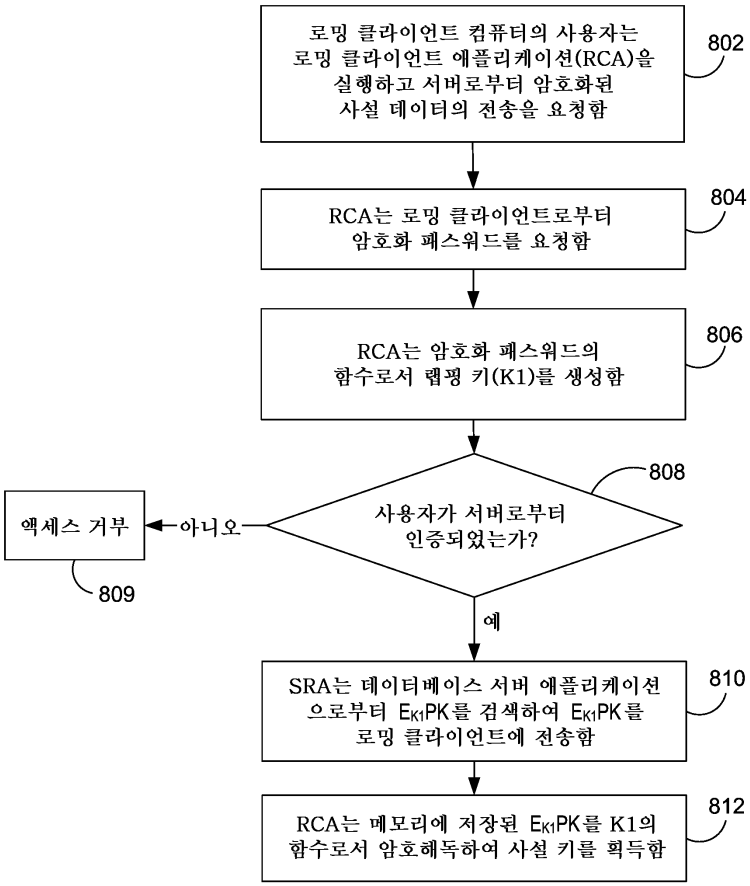
도면6


212
데이터
통신 네트워크
204
웹 서버
웹 형식(HTML)
210
215
인증 서비스
302
로밍 클라이언트
로밍 클라이언트 애플리케이션
304
형식 210
214
메모리
K2 408
K3 424
EncK3K2 428
EncK2K1 414
EncK1PK 234
K1 230
PK 216
228
서버 로밍
애플리케이션
K3
610
Enc K2 K1
614
Enc K1 PK
612
312
암호해독 알고리듬
Enc K3 K2 428
Enc K2 K1 414
Enc K1 PK 234
606
608
604
데이터베이스
EncK1 PK
EncK2 K1
EncK1K2
K3
226
220
사용자 인터페이스
217
디스플레이
219
입력 장치
306
사용자

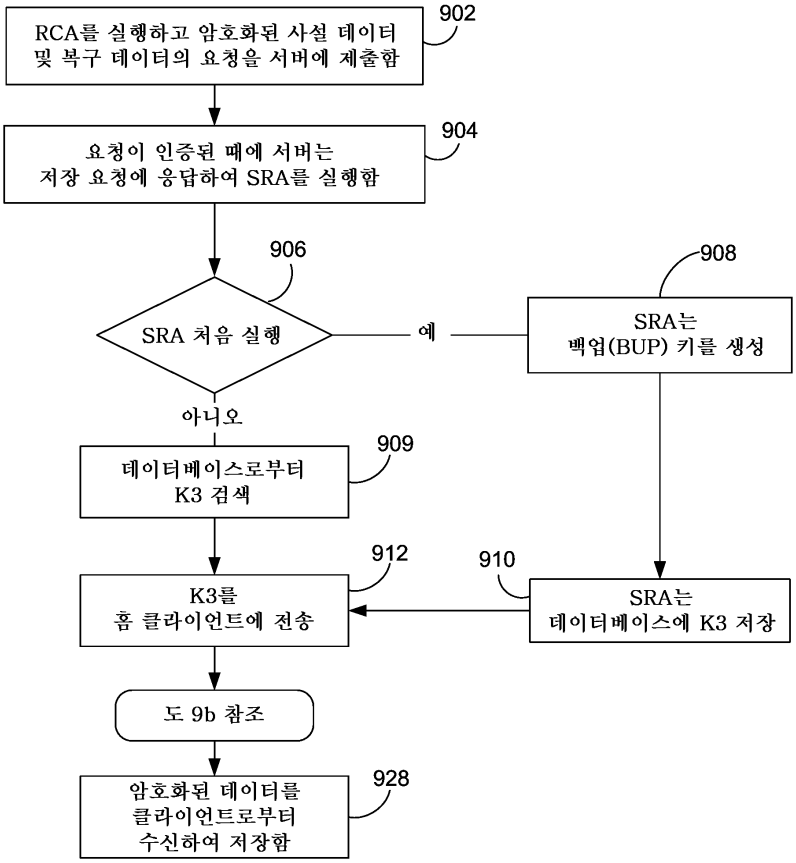
도면7


홈 클라이언트의 사용자는 홈 클라이언트 애플리케이션(HCA)을 실행하고 사설 데이터를 지정하여 암호화하고 서버에 전송함
702
HCA는 클라이언트로부터 암호화 패스워드를 홈 클라이언트에 요청함
704
HCA는 사용자로부터 암호화 패스워드의 함수로서 랩핑 키(K1)를 생성함
706
CRA는 메모리에 저장된 PK를 생성된 K1의 함수로서 암호화함
708
클라이언트 애플리케이션은 암호화된 PK ($E_{K1}PK$)를 서버 애플리케이션을 실행하는 서버에 전송함
710
서버 애플리케이션은 전송된 $E_{K1}PK$에 응답하여 $E_{K1}PK$를 데이터베이스에 저장함
712

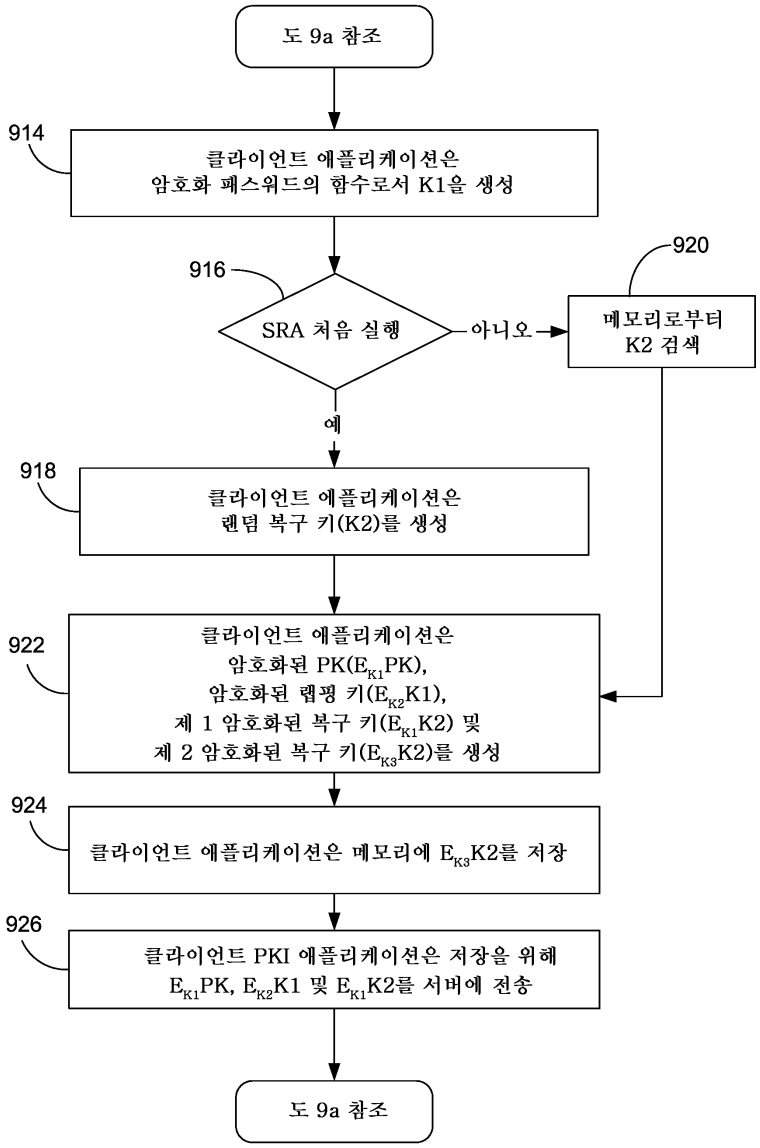
도면8


로밍 클라이언트 컴퓨터의 사용자는 로밍 클라이언트 애플리케이션(RCA)을 실행하고 서버로부터 암호화된 사설 데이터의 전송을 요청함
802
RCA는 로밍 클라이언트로부터 암호화 패스워드를 요청함
804
RCA는 암호화 패스워드의 함수로서 랩핑 키(K1)를 생성함
806
사용자가 서버로부터 인증되었는가?
808
아니오
액세스 거부
809
예
SRA는 데이터베이스 서버 애플리케이션으로부터 EK1PK를 검색하여 EK1PK를 로밍 클라이언트에 전송함
810
RCA는 메모리에 저장된 EK1PK를 K1의 함수로서 암호해독하여 사설 키를 획득함
812

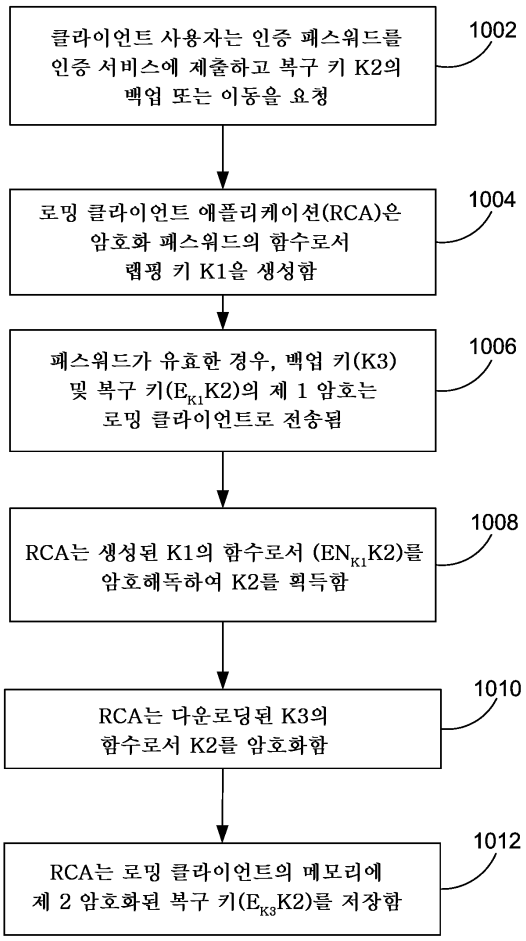
도면9a


RCA를 실행하고 암호화된 사설 데이터 및 복구 데이터의 요청을 서버에 제출함
902
요청이 인증된 때에 서버는 저장 요청에 응답하여 SRA를 실행함
904
906
SRA 처음 실행
예
908
SRA는 백업(BUP) 키를 생성
아니오
909
데이터베이스로부터 K3 검색
912
910
K3를 홈 클라이언트에 전송
SRA는 데이터베이스에 K3 저장
도 9b 참조
928
암호화된 데이터를 클라이언트로부터 수신하여 저장함

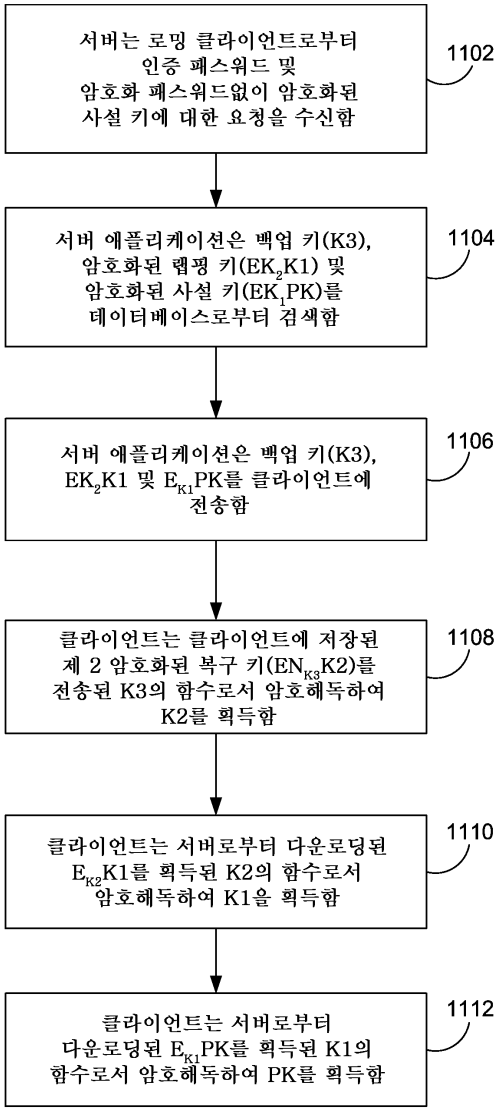
도면9b


도 9a 참조
914
클라이언트 애플리케이션은
암호화 패스워드의 함수로서 K1을 생성
916
SRA 처음 실행
아니오
920
메모리로부터
K2 검색
예
918
클라이언트 애플리케이션은
랜덤 복구 키(K2)를 생성
922
클라이언트 애플리케이션은
암호화된 PK(E_{K1}PK),
암호화된 랩핑 키(E_{K2}K1),
제 1 암호화된 복구 키(E_{K1}K2) 및
제 2 암호화된 복구 키(E_{K3}K2)를 생성
924
클라이언트 애플리케이션은 메모리에 E_{K3}K2를 저장
926
클라이언트 PKI 애플리케이션은 저장을 위해
E_{K1}PK, E_{K2}K1 및 E_{K1}K2를 서버에 전송
도 9a 참조

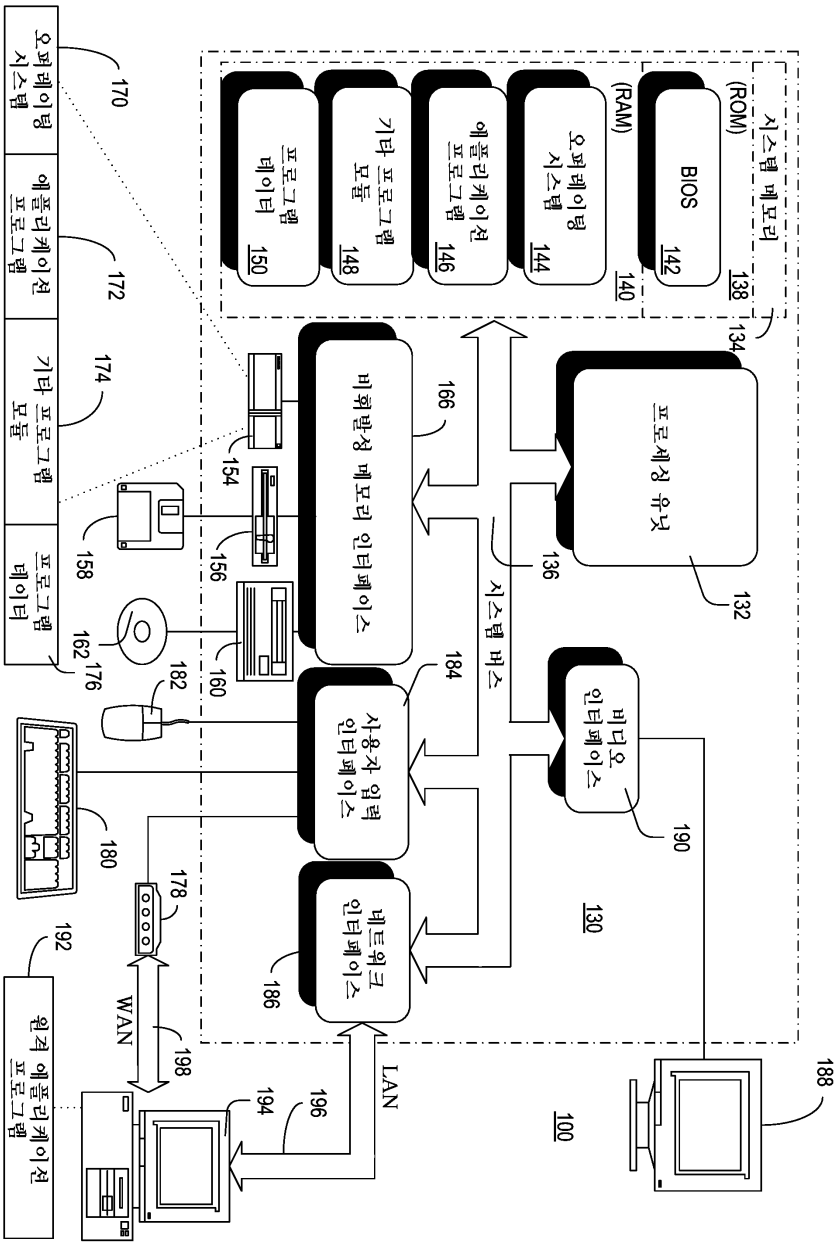
도면10


클라이언트 사용자는 인증 패스워드를 인증 서비스에 제출하고 복구 키 K2의 백업 또는 이동을 요청
1002
로밍 클라이언트 애플리케이션(RCA)은 암호화 패스워드의 함수로서 랩핑 키 K1을 생성함
1004
패스워드가 유효한 경우, 백업 키(K3) 및 복구 키(E_{K1}K2)의 제 1 암호는 로밍 클라이언트로 전송됨
1006
RCA는 생성된 K1의 함수로서 (EN_{K1}K2)를 암호해독하여 K2를 획득함
1008
RCA는 다운로딩된 K3의 함수로서 K2를 암호화함
1010
RCA는 로밍 클라이언트의 메모리에 제 2 암호화된 복구 키(E_{K3}K2)를 저장함
1012

도면11


서버는 로밍 클라이언트로부터 인증 패스워드 및 암호화 패스워드없이 암호화된 사설 키에 대한 요청을 수신함
1102
서버 애플리케이션은 백업 키(K3), 암호화된 랩핑 키(EK_2K1) 및 암호화된 사설 키(EK_1PK)를 데이터베이스로부터 검색함
1104
서버 애플리케이션은 백업 키(K3), EK_2K1 및 $E_{K1}PK$를 클라이언트에 전송함
1106
클라이언트는 클라이언트에 저장된 제 2 암호화된 복구 키($EN_{K3}K2$)를 전송된 K3의 함수로서 암호해독하여 K2를 획득함
1108
클라이언트는 서버로부터 다운로딩된 $E_{K2}K1$를 획득된 K2의 함수로서 암호해독하여 K1을 획득함
1110
클라이언트는 서버로부터 다운로딩된 $E_{K1}PK$를 획득된 K1의 함수로서 암호해독하여 PK를 획득함
1112

도면12


시스템 메모리 (ROM) 138
BIOS 142
(RAM) 140
오퍼레이팅 시스템 144
애플리케이션 프로그램 146
기타 프로그램 모듈 148
프로그램 데이터 150
프로세싱 유닛 132
134
136
시스템 버스
비휘발성 메모리 인터페이스
사용자 입력 인터페이스
네트워크 인터페이스
비디오 인터페이스
130
100
166
184
186
190
188
154
156
158
160
162
176
182
180
178
192
WAN
198
LAN
194
196
원격 애플리케이션 프로그램
오퍼레이팅 시스템
애플리케이션 프로그램
기타 프로그램 모듈
프로그램 데이터
170
172
174