(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2007-0109040
(43) 공개일자 2007년11월15일

(51) Int. Cl.
G06F 17/00 (2006.01)
(21) 출원번호 10-2006-0041504
(22) 출원일자 2006년05월09일
심사청구일자 2006년05월09일

(71) 출원인
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
유상봉
인천 부평구 산곡동 산37-4 현대아파트 305동 1404호
신우철
경기 평택시 서탄면 장등리 321
(74) 대리인
이원희

전체 청구항 수 : 총 10 항

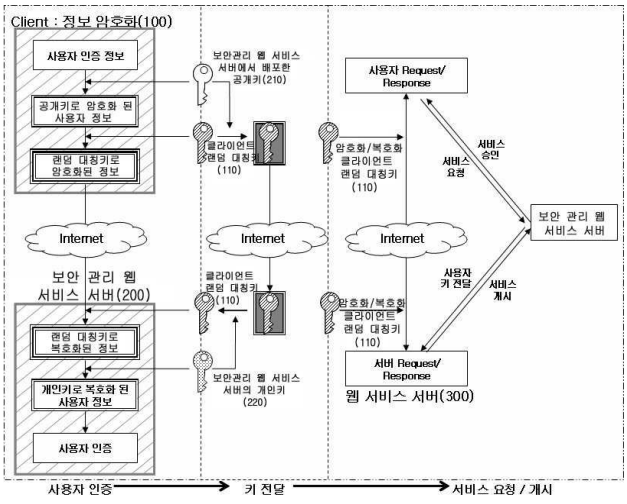
(54) 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스시스템 및 방법

(57) 요 약

본 발명은 통상의 웹 서비스와는 별도로 보안 관리 웹 서비스를 둠으로써 사용자 인증의 이중 강화 및 메시지 보안을 강화하고 이를 실제 웹 서비스와 분산처리 함으로써 그 부하를 줄여서 안전하고도 보다 효율적인 웹 서비스를 구현할 수 있도록 하는 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 시스템 및 방법을 제공한다.

본 발명의 보안 관리 웹 서비스 시스템은, 공개키로 사용자 인증 정보를 1차 암호화하며, 랜덤 대칭키로 상기 1차 암호화된 사용자 인증 정보를 2차 암호화하여 보안 관리 웹 서비스 서버로 제공하는 클라이언트; 상기 공개키를 클라이언트에 제공하며, 상기 클라이언트로부터 제공된 랜덤 대칭키를 바탕으로 상기 클라이언트로부터 제공된 암호화된 사용자 인증 정보를 1차 복호화한 후, 개인키로 2차 복호화하여 사용자를 인증하는 보안 관리 웹 서비스 서버; 및 사용자의 웹 서비스 요청시 상기 보안 관리 웹 서비스 서버로부터 랜덤 대칭키를 제공받아 상기 클라이언트와의 웹 서비스 메시지를 암호화하는 실제 웹 서비스 서버;로 구성됨을 특징으로 한다.

대표도 - 도4



특허청구의 범위

청구항 1

공개키로 사용자 인증 정보를 1차 암호화하며, 랜덤 대칭키로 상기 1차 암호화된 사용자 인증 정보를 2차 암호화하여 보안 관리 웹 서비스 서버로 제공하는 클라이언트;

상기 공개키를 클라이언트에 제공하며, 상기 클라이언트로부터 제공된 랜덤 대칭키를 바탕으로 상기 클라이언트로부터 제공된 암호화된 사용자 인증 정보를 1차 복호화한 후, 개인키로 2차 복호화하여 사용자를 인증하는 보안 관리 웹 서비스 서버; 및

사용자의 웹 서비스 요청시 상기 보안 관리 웹 서비스 서버로부터 랜덤 대칭키를 제공받아 상기 클라이언트와의 웹 서비스 메시지를 암호화하는 웹 서비스 서버;

로 구성됨을 특징으로 하는 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 시스템.

청구항 2

제 1 항에 있어서, 상기 랜덤 대칭키는

사용자 인증이 필요한 경우 상기 클라이언트에서 랜덤하게 생성되는 것을 특징으로 하는 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 시스템.

청구항 3

제 1 항에 있어서, 상기 개인키는

상기 보안 관리 웹 서비스 서버의 개인키인 것을 특징으로 하는 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 시스템.

청구항 4

제 1 항에 있어서, 상기 보안 관리 웹 서비스 서버는

사용자 인증 정보인 사용자 ID와 이에 대응되는 랜덤 대칭키가 쌍으로 저장되는 데이터베이스를 구비하는 것을 특징으로 하는 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 시스템.

청구항 5

제 4 항에 있어서, 상기 보안 관리 웹 서비스 서버는

상기 사용자 ID와 랜덤 대칭키 쌍의 동일한 시간에 중복 불가, 동일한 랜덤 대칭키의 사용 불가의 제약조건을 바탕으로 상기 제약조건을 어긴 클라이언트의 IP를 차단하는 것을 특징으로 하는 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 시스템.

청구항 6

클라이언트가 보안 관리 웹 서비스 서버로부터 제공되는 공개키를 바탕으로 사용자 인증 정보를 1차 암호화 한 후, 랜덤 대칭키로 상기 1차 암호화된 사용자 인증 정보를 2차 암호화하여 2차 암호화된 사용자 인증 정보를 상기 보안 관리 웹 서비스 서버로 제공하는 제1과정;

상기 클라이언트와 보안 관리 웹 서비스 서버간 랜덤 대칭키의 교환 후, 상기 보안 관리 웹 서비스 서버가 상기 랜덤 대칭키를 바탕으로 상기 클라이언트로부터 제공된 암호화된 사용자 인증 정보를 1차 복호화한 후, 보안 관리 웹 서비스 서버의 개인키로 2차 복호화하여 사용자를 인증하는 제2과정; 및

상기 사용자 인증 후, 사용자가 웹 서비스 서버에 웹 서비스 요청시 상기 웹 서비스 서버가 상기 보안 관리 웹 서비스 서버로부터 제공되는 랜덤 대칭키로 웹 서비스 메시지를 암호화하여 클라이언트와 교환하는 제3과정;

을 포함하는 것을 특징으로 하는 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 방법.

청구항 7

제 6 항에 있어서, 상기 제1과정에서 상기 2차 암호화된 사용자 인증 정보와 더불어 사용자 ID로 함께 상기 보안 관리 웹 서비스 서버로 제공되는 것을 특징으로 하는 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 방법.

청구항 8

제 6 항에 있어서, 상기 제2과정에서 상기 클라이언트와 보안 관리 웹 서비스 서버간 랜덤 대칭키의 교환시

상기 클라이언트는 상기 랜덤 대칭키를 사용자 ID와 함께 상기 보안 관리 웹 서비스 서버의 공개키로 암호화하여 상기 보안 관리 웹 서비스 서버로 제공하는 것을 특징으로 하는 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 방법.

청구항 9

제 8 항에 있어서, 상기 보안 관리 웹 서비스 서버는 상기 클라이언트로부터 제공받은 상기 공개키로 암호화된 정보를 자신의 개인키로 복호화하여 사용자 ID와 이에 대응되는 랜덤 대칭키 쌍을 데이터베이스에 저장하는 것을 특징으로 하는 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 방법.

청구항 10

제 9 항에 있어서, 상기 보안 관리 웹 서비스 서버는 상기 사용자 ID와 랜덤 대칭키 쌍의 동일한 시간에 중복 불가, 동일한 랜덤 대칭키의 사용 불가의 제약조건을 바탕으로 상기 제약조건을 어긴 클라이언트의 IP를 차단하는 것을 특징으로 하는 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<21> 본 발명은 웹 서비스 시스템 및 방법에 관한 것으로, 특히 통상의 웹 서비스와는 별도로 보안 관리 웹 서비스를 둠으로써 사용자 인증의 이중 강화 및 메시지 보안을 강화하고 이를 실제 웹 서비스와 분산처리 함으로써 그 부하를 줄여서 안전하고도 보다 효율적인 웹 서비스를 구현할 수 있도록 하는 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 시스템 및 방법에 관한 것이다.

<22> 최근 XML기반의 웹 서비스(Web Service)가 기업 내 또는 기업간 통합 서비스 문제를 해결해주는 차세대 e-비즈니스의 기반으로 급부상하고 있다. 과거 시스템들은 메인 프레임 서버가 모든 정보를 중앙에서 집중하여 처리하는 자립형(stand-alone) 방식을 사용하여 왔으며, 최근까지도 서버-클라이언트 방식이 주류를 이루고 있다. 이러한 과거 시스템은 대부분 폐쇄적 네트워크를 사용하고 있으며, 시스템 자체의 유연성이 없는 매우 고정적인 아키텍처를 채택하고 있어서 웹 브라우저를 통해 각종 데이터를 조회한다든가 다른 시스템의 데이터를 가져와 가공하거나 분석하는 등의 작업을 할 수가 없었다.

<23> 가트너그룹에 따르면 전세계 기업들의 중요 업무 시스템 가운데 네트워크에 연결된 시스템은 20%에 불과하며, 나머지 80%는 서버-클라이언트 개념의 폐쇄된 시스템을 사용하는 것으로 나타났다.

<24> 최근에는 기업의 IT투자 확대에 따라 기업 내에서도 다수의 이질적인 시스템을 도입하면서 기업의 시스템이 산재해 있으며, 이러한 분산 시스템을 통합하고자 많은 노력을 기울이고 있다. 이렇게 산재해 있는 개별적인 어플리케이션을 효율적으로 통합하는 대안으로 떠오르고 있는 것이 웹 서비스이다.

<25> 웹 서비스의 정의는 공급업체 및 관련 단체에 따라 다양한 정의를 제시하고 있으며, 이러한 정의들을 포괄하여 제시한 일반적인 정의는 다음과 같다.

<26> 웹 서비스란 인터넷을 이용한 오픈 네트워크를 통해 단일한 비즈니스 또는 다수의 비즈니스 업체간의

기존 컴퓨터 시스템 프로그램을 결합시키는 표준화된 소프트웨어 기술로서 이러한 표준 기술을 이용해 모든 비즈니스를 가능케 하는 활동을 일컫는다. 웹 서비스는 PC, PDA, 핸드폰 등 다양한 디바이스를 통해서 접근할 수 있으며, 주문관리 소프트웨어 신용정보 서비스 등 다양한 어플리케이션 프로그램과 연동해 사용할 수 있다. 웹 서비스는 기존의 다른 소프트웨어처럼 완벽한 정의를 지정하여 구성하는 것이 아니라 서로 주고받는 데이터 표준에 대한 정의를 규정함으로써 매우 유연하다. 인터넷상에서 웹 서비스는 거래업체간의 이질적인 운영시스템, 이질적인 프로그램언어간의 커뮤니케이션 차이를 극복해주는 연결고리 역할을 해준다.

<27> 웹 서비스의 특징을 살펴보면 다음과 같다.

<28> 첫째, 시스템 구조의 유연성이다. 과거의 메인 프레임 또는 기존 서버-클라이언트 방식은 폐쇄적이면서도 소프트웨어 구조가 단단히 묶어져 있는(tightly coupled) 고정적 시스템이었으나, 웹 서비스는 유연한(loosely coupled) 소프트웨어 구조를 통해 이질적인 데이터 표준을 유연하게 통합하여 운영해준다.

<29> 둘째, 사용의 편리성이다. 웹 서비스는 사용자가 소프트웨어를 설치한 후에는 사용자가 느끼지 못할 정도로 자연스럽게 서비스를 제공받으며 인터넷을 연결할 수 있는 유.무선 단말기를 통해 시간과 장소에 관계없이 웹 서비스에 접근하여 다양한 서비스를 제공받을 수 있다.

<30> 셋째, 기존 시스템의 통합 환경을 제공한다는 것이다. 기존에 자사가 보유하고 있는 내부 또는 외부 이질적인 어플리케이션간의 통합 서비스를 제공받을 수 있으며, 새로운 비즈니스 파트너간의 시스템과의 통합도 자동적으로 이루어지게 된다. 특히, 웹 서비스는 새로운 시스템을 구축하는 것이 아니라 기존에 존재하고 있는 시스템을 통합하여 운영해 줌으로써 기업에게 다양한 이점을 제공해줄 것이다.

<31> 넷째, 비용 효율적이라는 것이다. 웹 서비스는 분산 시스템의 소프트웨어간의 통합을 자동화적으로 이행해줌으로서 개별 기업마다 투입해야하는 IT 개발 및 운영비용을 절감해주고, 상호 연결된 작업을 기존에 비해 훨씬 빠르고, 유연하며 효율적으로 제공해주면서 기업의 비즈니스 프로세스를 효율적으로 개선해줄 것이다.

<32> 현재 W3C가 추진 중인 웹 서비스 표준 규약에서 웹 서비스의 아키텍처를 구성하고 있는 기본적인 표준들은 HTTP(Hypertext transfer protocol), XML(eXtensible Markup Language), SOAP(Simple Object Access Protocol), WSDL(Web Service Description Language), UDDI(Universal Discovery Description and Integration) 등이 있다.

<33> 웹 서비스를 만들 때 사용되는 표준 프로토콜로 구성된 몇 가지 스펙이 있으며, 도 1은 현재 존재하는 웹 서비스 스펙을 나타낸 것이다.

<34> 현재 웹 사이트는 웹 브라우져를 통해 사람에 의해서 접근되지만, 웹 서비스는 컴퓨터 프로그램을 통해서 접근되며, 웹 서비스는 어떠한 응용프로그램 로직이나 코드를 공개한다. 웹 서비스는 하나의 프로그램을 통해서 접근된다. 그 프로그램은 웹 응용프로그램, 윈도우 응용프로그램 등 도 1에 표시된 모든 유형의 응용프로그램이 될 수 있다. 응용프로그램은 조직의 내부 웹 서비스나 제휴업체들로부터 제공된 외부 웹 서비스, 또는 일반적인 빌딩 블록 서비스를 사용할 수 있다. 웹 서비스는 다른 웹 서비스에 의해서 사용될 수도 있다. 도 2는 웹 서비스의 일반적인 프로그램 접근도를 나타낸 것이다.

<35> 한편, 웹 서비스 메시지 보안(WS-Security)의 목표는 안전한 SOAP 메시지 교환을 하도록 하는 것이다. 이것은 보안 프로토콜의 범위를 세우는데 사용할 수 있는 다양한 메커니즘을 제공하지만 특정하게 고정된 보안 프로토콜을 설명하진 않는다. 다시 말해 웹 서비스 메시지 보안의 초점은 세션 성립, 보안 context 및 정책 동의 가정 하에서 메시지 보안을 제공하는 단일 메시지 보안 언어를 설명한다.

<36> 신뢰성, 무결성과 관련된 메시지 보호는 보안에서의 주관심사이다. 이 메시지 보안 모델은 SOAP 메시지의 헤더, 바디 또는 헤더와 바디를 조합하여 암호화 하거나 서명함으로써 메시지를 보호하는 수단을 제공한다. 메시지의 무결성은 메시지의 변형 탐지를 보장하는 보안 토큰과 결합된 XML Signature에 의해 보장 받을 수 있으며, 메시지의 신뢰성은 SOAP 메시지의 신뢰를 유지하기 위해 보안 토큰과 결합된 XML Encryption에 의해 보장받을 수 있다.

<37> SOAP 메시지의 Encryption은 바디 블록, 헤더 블록, 이들의 어느 하부 구조의 조합들을 보내는 자와 받는 자에 의해 공유된 대칭키를 이용하여 암호화 하거나 대칭키를 암호화된 양식에 의해 전달하기 위한 명세이다.

<38> 암호화된 SOAP 메시지를 생성하는 일반적인 단계는 다음과 같다.

<39> (1) 새로운 SOAP 엔벨로프(envelope)를 만든다.

<40> (2) <wsse:Security> 헤더를 만든다.

<41> (3) 암호화할 아이템을 위치시킨다.

<42> (4) 아이템들을 암호화하고 암호화한 데이터를<xenc:EncryptedData>로 대체시킨다.

<43> (5) 생성된 <xenc:EncryptedData> 엘리먼트를 참조하는 <xenc: DataReference> 엘리먼트를 만든다.

<44> (6) 암호화 되지 않은 나머지 데이터를 복사한다.

<45> 암호화된 SOAP 메시지를 복호화 하는 일반적인 단계는 다음과 같다.

<46> (1) 메시지를 받은자가 소유하고 있는 복호화 키를 확인하고 복호하 해야 할 메시지의 엘리먼트를 확인한다.

<47> (2) <xenc:EncryptedData>를 찾는다.

<48> (3) XML Encryption 규칙에 따라서 SOAP 엔벨로프 내의 각 암호화 된 엘리먼트를 복호화 한다.

<49> 또한, 공개키 기반의 암호화 기법은 키 분배의 문제점을 잘 풀었지만 고비용이 드는 거대한 대수학적인 오퍼레이션을 사용해야 한다. 이와 상대적으로 대칭키 암호화 기법은 훨씬 효율적이다. 일반적으로 볼 때 공개키 기반의 암호화 기법은 대칭키 암호화 기법에 비해 훨씬 계산이 복잡하고 느리다.

<50> 하이브리드 암호화 기법은 큰 데이터를 공개키 기법으로 암호화 하는 대신에 수신자는 대칭 암호를 사용하여 큰 데이터를 암호화 하고, 대신에 대칭키를 공개키 기법으로 암호화 하는 것이다. 그 후, 두 데이터를 수신자에게 보낸다. 이것의 장점은 공개키 방식의 느린 계산시간을 줄여주며, 동시에 키 분배 문제를 해결해 준다는 것이다. 두 암호화 된 아이템을 받으면, 수신자는 먼저 대칭키를 자신의 개인키로 해독하고 나서 큰 데이터는 대칭키 기법을 이용하여 해독한다. 도 3은 하이브리드 암호화 기법을 이용한 암호화를 도식적으로 나타낸 것이다.

<51> 실제 하이브리드 암호화 기법이 많이 사용되고 있으며, 그 예로 전자 봉투(Digital envelope), SSL(Secure Sockets Layer) 프로토콜 등이 있다.

<52> 안전한 웹 서비스를 이용하기 위해 기존에 나와 있는 보안 표준 기술인 메시지 보안, 보안 정책, 프라이버시 보호, 신뢰 관리 등 여러 가지 기술이 나와 있으나, 이것을 모두 구현하기에는 많은 노력이 필요하며 복잡하다. 주로 이용되는 웹 서비스 보안 기술에는 웹 서비스 메시지에 SAML(Security Assertion Markup Language), Keberos 등의 보안 토큰을 내장하여 보안 토큰을 개별적으로 처리하는 방법 등이 실제로 쓰이고 있으나, 이 또한 XML을 이용하는 웹 서비스의 경우 스트링 처리 등 종래의 암호화 기법 그대로 쓰기에는 여전히 처리방법도 복잡하고 다른 부가 기술을 이용해야 하는 등 성능 저하의 우려도 있다.

<53> 사용자 인증 관점에서 볼 때 하이브리드 암호 기법 또한 문제가 발생 할 수 있다. 랜덤 대칭키로 사용자 인증 정보를 암호화 한다고 해도 그것을 가로챈다면 사용자 인증 정보를 복호화 할 가능성이 있으며, 이는 보안상의 문제를 야기할 수 있다.

발명이 이루고자 하는 기술적 과제

<54> 본 발명은 이러한 점을 감안한 것으로, 본 발명의 목적은 실제 웹 서비스와 별도로 보안을 위해 보안 관리 웹 서비스를 구성하여 사용자 인증을 이중으로 강화하고 이를 바탕으로 랜덤키를 교환하여 실제 웹 서비스 간에는 이를 이용하여 메시지 보안을 강화하고 실제 서비스를 제공하는 웹 서비스 서버의 부하를 분산시킬 수 있도록 한 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 시스템 및 방법을 제공함에 있다.

<55>

발명의 구성 및 작용

<56> 상기 목적을 달성하기 위한 본 발명에 따른 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 시스템은, 공개키로 사용자 인증 정보를 1차 암호화하며, 랜덤 대칭키로 상기 1차 암호화된 사용자 인증 정보를 2차 암호화하여 보안 관리 웹 서비스 서버로 제공하는 클라이언트; 상기 공개키를 클라이언트에 제공하며, 상기 클라이언트로부터 제공된 랜덤 대칭키를 바탕으로 상기 클라이언트로부터 제공된 암호화된 사용자 인증 정보를 1차 복호화한 후, 개인키로 2차 복호화하여 사용자를 인증하는 보안 관리 웹 서비스 서버; 및 사용자의 웹 서비

스 요청시 상기 보안 관리 웹 서비스 서버로부터 랜덤 대칭키를 제공받아 상기 클라이언트와의 웹 서비스 메시지를 암호화하는 실제 웹 서비스 서버;로 구성됨을 특징으로 한다.

<57> 상기 랜덤 대칭키는 사용자 인증이 필요한 경우 상기 클라이언트에서 랜덤하게 생성되며, 상기 개인키는 상기 보안 관리 웹 서비스 서버의 개인키이다.

<58> 상기 보안 관리 웹 서비스 서버는 사용자 인증 정보인 사용자 ID와 이에 대응되는 랜덤 대칭키가 쌍으로 저장되는 데이터베이스를 구비하며, 상기 보안 관리 웹 서비스 서버는 상기 사용자 ID와 랜덤 대칭키 쌍의 동일한 시간에 중복 불가, 동일한 랜덤 대칭키의 사용 불가의 제약조건을 바탕으로 상기 제약조건을 어긴 클라이언트의 IP를 차단한다.

<59> 상기 목적을 달성하기 위한 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 방법은, 클라이언트가 보안 관리 웹 서비스 서버로부터 제공되는 공개키를 바탕으로 사용자 인증 정보를 1차 암호화 한 후, 랜덤 대칭키로 상기 1차 암호화된 사용자 인증 정보를 2차 암호화하여 2차 암호화된 사용자 인증 정보를 상기 보안 관리 웹 서비스 서버로 제공하는 제1과정; 상기 클라이언트와 보안 관리 웹 서비스 서버간 랜덤 대칭키의 교환 후, 상기 보안 관리 웹 서비스 서버가 상기 랜덤 대칭키를 바탕으로 상기 클라이언트로부터 제공된 암호화된 사용자 인증 정보를 1차 복호화한 후, 보안 관리 웹 서비스 서버의 개인키로 2차 복호화하여 사용자를 인증하는 제2과정; 및 상기 사용자 인증 후, 사용자가 웹 서비스 서버에 웹 서비스 요청시 상기 웹 서비스 서버가 상기 보안 관리 웹 서비스 서버로부터 제공되는 랜덤 대칭키로 웹 서비스 메시지를 암호화하여 클라이언트와 교환하는 제3과정;을 포함하는 것을 특징으로 한다.

<60> 상기 제1과정에서 상기 2차 암호화된 사용자 인증 정보와 더불어 사용자 ID로 함께 상기 보안 관리 웹 서비스 서버로 제공되며, 상기 제2과정에서 상기 클라이언트와 보안 관리 웹 서비스 서버간 랜덤 대칭키의 교환시 상기 클라이언트는 상기 랜덤 대칭키를 사용자 ID와 함께 상기 보안 관리 웹 서비스 서버의 공개키로 암호화하여 상기 보안 관리 웹 서비스 서버로 제공한다.

<61> 상기 보안 관리 웹 서비스 서버는 상기 클라이언트로부터 제공받은 상기 공개키로 암호화된 정보를 자신의 개인키로 복호화하여 사용자 ID와 이에 대응되는 랜덤 대칭키 쌍을 데이터베이스에 저장한다.

<62> 이하, 본 발명의 바람직한 실시 예를 첨부된 도면을 참조하여 보다 상세하게 설명한다. 단, 하기 실시 예는 본 발명을 예시하는 것일 뿐 본 발명의 내용이 하기 실시 예에 한정되는 것은 아니다.

<63> 도 4는 본 발명에 따른 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 시스템과 이의 처리 과정을 나타낸 도로, 본 발명은 크게 클라이언트(100), 보안 관리 웹 서비스 서버(200), 웹 서비스 서버(300)로 구성된다.

<64> 상기 클라이언트(100)는 보안 관리 웹 서비스 서버(200)에서 배포한 공개키(210)로 사용자 인증 정보(120)인 사용자 ID와 패스워드를 암호화하며, 암호화된 사용자 인증 정보(130)를 클라이언트(100)에서 랜덤하게 생성된 랜덤 대칭키(110)로 다시 한번 암호화하여 이중으로 암호화된 사용자 인증 정보(140)와 사용자 ID를 상기 보안 관리 웹 서비스 서버(200)로 제공한다.

<65> 상기 보안 관리 웹 서비스 서버(200)는 상기 클라이언트(100)로부터 제공받은 이중으로 암호화된 사용자 인증 정보(140)를 랜덤 대칭키(110)를 바탕으로 복호화하고, 복호화된 데이터를 보안 관리 웹 서비스 서버(200)의 개인키(220)로 복호화하여 사용자를 인증한다.

<66> 상기 웹 서비스 서버(300)는 클라이언트(100)가 상기 보안 관리 웹 서비스 서버(200)에 의한 사용자 인증 후, 웹 서비스 서버(300)의 웹 서비스를 요청하면 보안 관리 웹 서비스 서버(200)로부터 전달받게 되는 상기 랜덤 대칭키(110)로 클라이언트(100)와 웹 서비스 서버(300) 간의 메시지를 암호화하여 교환할 수 있도록 한다.

<67> 이와 같이 구성되는 본 발명은 도 5의 본 발명의 전체적인 흐름도에 도시한 바와 같이, 보안 관리 웹 서비스 서버(200)의 인증 및 공개키(210) 배포, 사용자 인증 정보(120)의 암호화에 의한 사용자 인증 정보(120)의 암호화 과정(S100), 클라이언트(100)와 보안 관리 웹 서비스 서버(200) 간의 랜덤 대칭키(110) 교환, 사용자 인증 등을 거치게 되는 사용자 인증 과정(S200), 사용자의 웹 서비스 요청에 따른 키 전달 및 서비스 개시 과정(S300)으로 이루어진다.

<68> 먼저, 상기 사용자 인증 정보(120)의 암호화 과정(S100)은 도 6에 도시한 바와 같이, 보안 관리 웹 서비스 서버(200)가 공격자가 가장한 서비스가 아닌 유효한 서비스인지를 확인하기 위해 공인된 인증기관을 통하여 이 보안 관리 웹 서비스 서버(200)가 실제 웹 서비스(300)를 이용할 곳의 보안 관리기 인지를 확신하고, 보

안 관리 웹 서비스 서버(200)로부터 공개키(210)를 부여 받는다(S110).

<69> 이후, 클라이언트(100)는 사용자로부터 사용자 ID와 패스워드로 구성된 사용자 인증 정보(120)를 입력받아 상기 보안 관리 웹 서비스 서버(200)에서 배포한 공개키(210)를 이용하여 사용자 인증 정보(120)를 암호화 한다(S120).

<70> 상기 암호화 된 사용자 인증 정보(130)는 클라이언트(100)에서 랜덤하게 생성된 랜덤 대칭키(110)를 이용하여 다시 한번 암호화 된다(S130). 상기 공개키(210)에 의해 1차 암호화된 후, 랜덤 대칭키(110)에 의해 2차 암호화된 사용자 인증 정보(140)는 사용자 ID와 함께 인터넷을 통해 보안 관리 웹 서비스 서버(200)로 보내진다(S140). 상기 랜덤 대칭키(110)는 클라이언트(100)의 사용자 인증이 필요한 경우 클라이언트(100)에서 랜덤하게 생성되는 대칭키이다. 도 7은 사용자 인증 정보(120)의 암호화 과정의 모식도이다.

<71> 상기 사용자 인증 과정(S200)은 도 8에 도시한 바와 같다.

<72> 먼저, 상기 클라이언트(100)와 보안 관리 웹 서비스 서버(200) 간의 랜덤 대칭키(110)의 교환이 이루어진다.

<73> 즉, 클라이언트(100)에 의해 랜덤하게 생성된 랜덤 대칭키(110)는 사용자 ID와 함께 보안 관리 웹 서비스 서버(200)의 공개키(210)로 암호화 되어 인터넷을 통해 보안 관리 웹 서비스 서버(200)에 전달된다(S210).

<74> 그리고 상기 단계(S210)에서 보안 관리 웹 서비스 서버(200)에 전달된 정보는 보안 관리 웹 서비스 서버(200)의 개인키(220)를 이용하여 복호화 되고, 사용자 ID를 판별하여 보안 관리 웹 서비스 서버(200)의 데이터베이스(230)에 사용자 ID 및 이에 대응되는 랜덤 대칭키(110)가 쌍으로 저장된다. 도 9는 이의 모식도이다.

<75> 제약조건은 사용자 ID : 랜덤 대칭키(110) 쌍은 동일한 시간에 중복될 수 없으며, 똑같은 랜덤 대칭키(110)의 사용은 불가이며, 이를 위해, 사용자 ID : 랜덤 대칭키(110) 쌍에 대한 기록을 남긴다. 몇 차례 이상 제약 조건을 어긴다면 수신된 IP정보를 바탕으로 차단한다. 사용자 ID : 랜덤 대칭키(110) 쌍은 클라이언트(100)에서 보내온 암호화된 사용자 인증 정보(140)를 복호화 하는데 사용한다.

<76> 이후, 키 전달이 올바르게 이루어졌으면 클라이언트(100)와 보안 관리 웹 서비스 서버(200)간 교환된 랜덤 대칭키(110)를 바탕으로 클라이언트(100)에서 보내온 암호화된 사용자 인증 정보(140)를 복호화 한다(S220).

<77> 복호화된 데이터를 바탕으로 이것이 올바른 클라이언트(100)에서 보내졌는지 판단한다. 복호화된 데이터는 보안 관리 웹 서비스 서버(200)의 공개키(210)로 암호화 시킨 것이므로 이것의 개인키(220)를 이용하여 복호화 한다(S230). 랜덤 대칭키(110) 사용자와 동일 유무, 사용자의 페스워드에 따라 사용자 인증 여부를 판단한다(S240). 도 10은 이러한 사용자 인증과정의 모식도이다.

<78>

<79> 다음, 상기 사용자의 웹 서비스 요청에 따른 키 전달 및 서비스 개시 과정(S300)을 도 11과 함께 살펴본다.

<80> 상기 보안 관리 웹 서비스 서버(200)에 의한 사용자의 인증 후, 실제 사용자가 사용하고자하는 웹 서비스를 이용하기 위해 서비스를 요청하면 상기 보안 관리 웹 서비스 서버(200)는 상기 과정(S200)에서 전달받은 랜덤 대칭키(110)를 웹 서비스 서버(300)에 넘겨 준다(S310).

<81> 클라이언트(100)와 실제 웹 서비스 서버(300)의 웹 서비스간 메시지는 주어진 랜덤 대칭키(110)를 바탕으로 웹 서비스 메시지 보안 명세를 이용하여 메시지 일부분 또는 전체를 암호화 하여 교환하게 된다(S320).

<82>

<83> 도 12는 랜덤 대칭키(110)를 이용 triple-DES 암호화 기법으로 SOAP 메시지를 암호화 한 예이다. 메시지에는 추가적으로 타임 스템프와 키에 대한 사용자 정보가 들어간다.

<84> 상기와 같이 본 발명은 보안 관리 웹 서비스 서버(200)에서 배포한 공개키(210) 및 클라이언트(100)에서 생성된 랜덤 대칭키(110)를 복합 이용하는 하이브리드 암호 기법을 변형하여 웹 서비스 사용자 인증을 이중으로 강화하고 이와 동시에 클라이언트(100)에서 생성된 랜덤 대칭키(110)를 교환하여, 인증된 후에는 교환된 키를 바탕으로 계층에 따라 사용자에게 인가된 서비스를 암호화 하여 소통하도록 하는 보안 관리 웹 서비스 모델을 제시한 것이다.

<85> 상술한 바와 같이, 본 발명의 바람직한 실시 예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게

수정 또는 변형하여 실시할 수 있다.

발명의 효과

<86> 이상에서 살펴본 바와 같이, 본 발명은 실제 서비스를 제공하는 웹 서비스와 별도로 보안 관리 웹 서비스를 둠으로써 실제 웹 서비스에 대한 부하를 분산시키고, 별도의 키 전달 정책 없이 사용자 인증 동시에 키 교환이 이루어지며, 사용자 ID 및 패스워드와 관계없이 프로그램적인 측면에서 랜덤 대칭키가 생성되고, 이것이 암호화되어 웹 서비스에 전달되기 때문에 실제 사용자 패스워드가 더 안전하게 관리될 수 있게 된다. 또한, 사용자에 대한 서비스의 관리도 실제 서비스와 별도로 처리할 수 있어 관리가 더 수월해진다. 즉, 본 발명은 사용자 인증을 이중으로 강화하고 이를 바탕으로 전달된 랜덤 대칭키를 이용하여 메시지 보안을 강화하고 이것을 분산처리 함으로써 그 부하를 줄여서 안전하고도 보다 효율적인 웹 서비스를 이용할 수 있게 된다.

도면의 간단한 설명

<1> 도 1은 일반적인 웹 서비스 스펙 구성도.

<2> 도 2는 웹 서비스의 일반적인 프로그램 접근도.

<3> 도 3은 일반적인 하이브리드 암호화 기법을 이용한 암호화 방법을 나타낸 도.

<4> 도 4는 본 발명에 따른 사용자 인증의 이중 강화를 위한 보안 관리 웹 서비스 시스템의 구성도.

<5> 도 5는 본 발명의 전반적인 동작 흐름도.

<6> 도 6은 본 발명의 사용자 인증 정보의 암호화 과정의 상세 흐름도.

<7> 도 7은 본 발명의 사용자 인증 정보의 암호화 과정의 모식도.

<8> 도 8은 본 발명의 사용자 인증 과정의 상세 흐름도.

<9> 도 9는 본 발명의 랜덤 대칭키 교환의 모식도.

<10> 도 10은 본 발명의 사용자 인증 과정의 모식도.

<11> 도 11은 본 발명의 사용자의 웹 서비스 요청에 따른 키 전달 및 서비스 개시 과정의 상세 흐름도.

<12> 도 12는 SOAP 메시지 암호화 전달 예를 나타낸 도.

<13> <도면의 주요부분에 대한 부호의 설명>

<14> 100 : 클라이언트 110 : 랜덤 대칭키

<15> 120 : 사용자 인증 정보 130 : 1차 암호화된 사용자 인증 정보

<16> 140 : 2차 암호화된 사용자 인증 정보

<17> 200 : 보안 관리 웹 서비스 서버 210 : 공개키

<18> 220 : 개인키

<19> 230 : 보안 관리 웹 서비스 서버의 데이터베이스

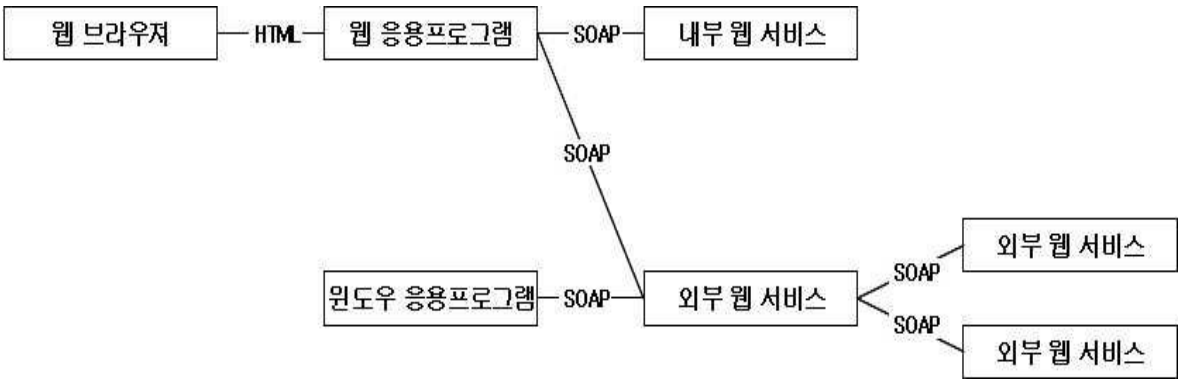
<20> 300 : 웹 서비스 서버

도면

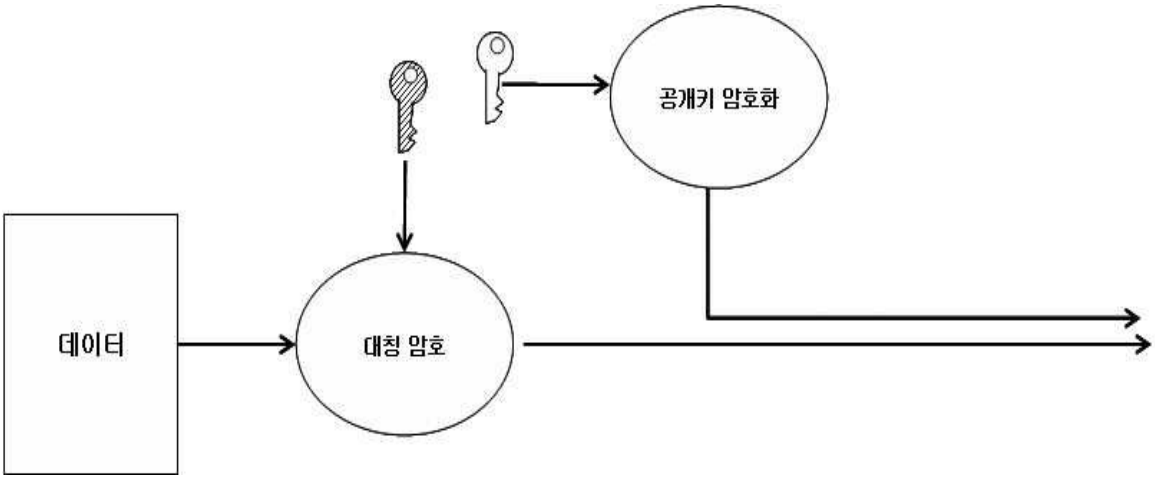
도면1

웹 서비스 찾기 UDDI(Universal Description, Discovery and Integration)
웹 서비스 설명하기 WSDL(Web Service Description Language)
웹 서비스 호출하기 SOAP(Simple Object Access Protocol)
데이터 인코딩 XML, XML 스키마
전 송 HTTP, SMTP

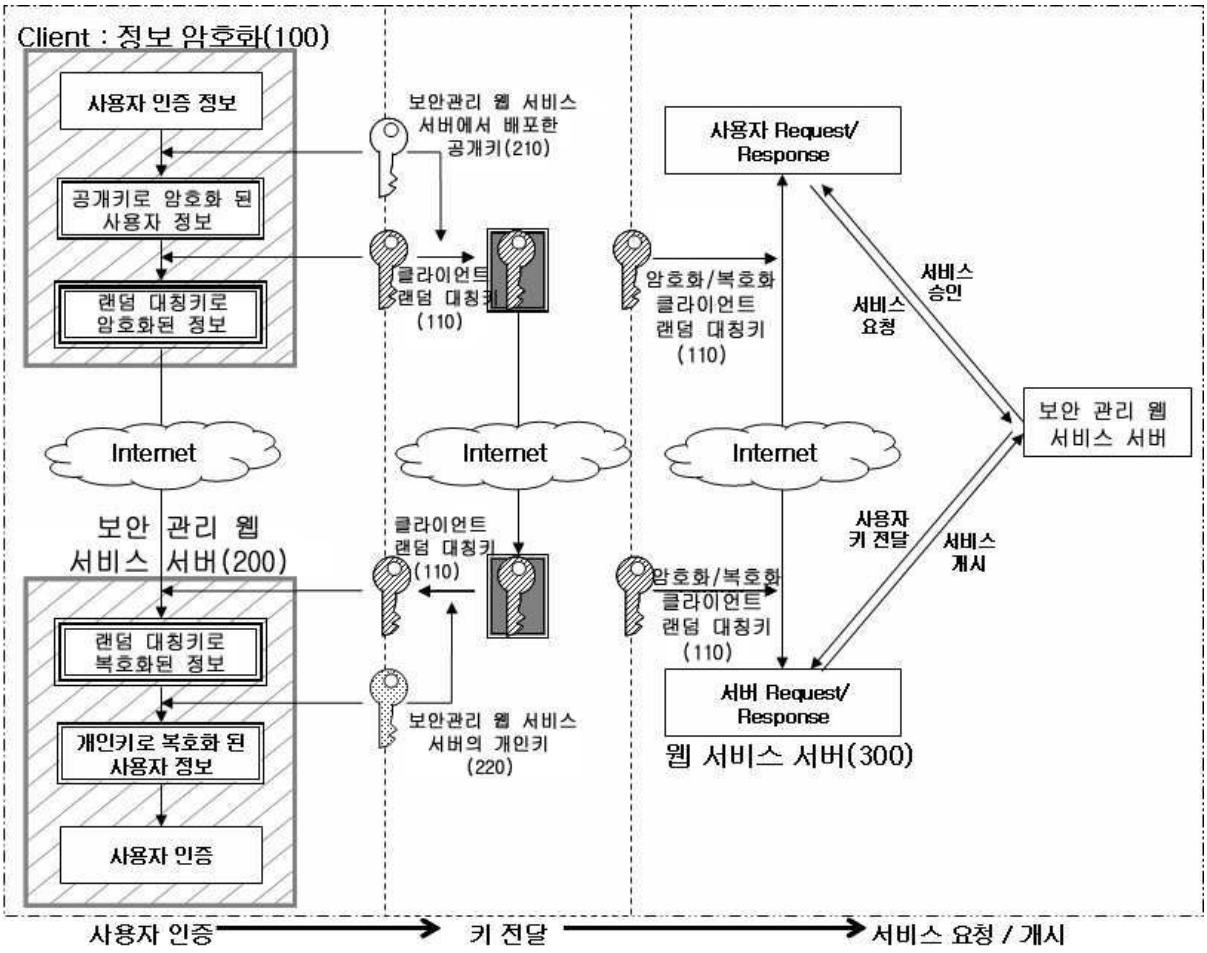
도면2



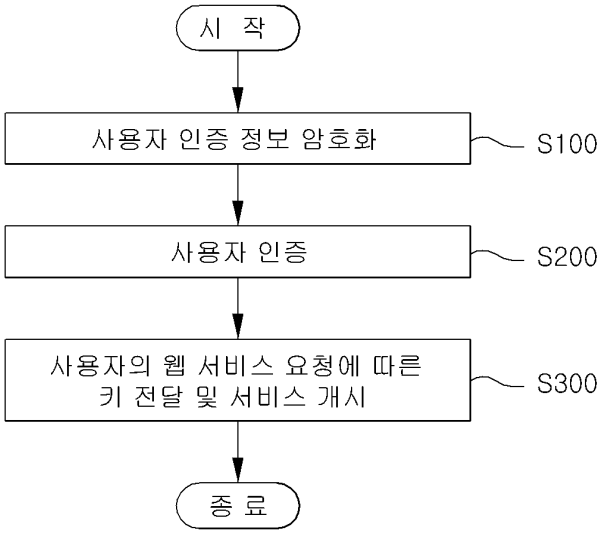
도면3



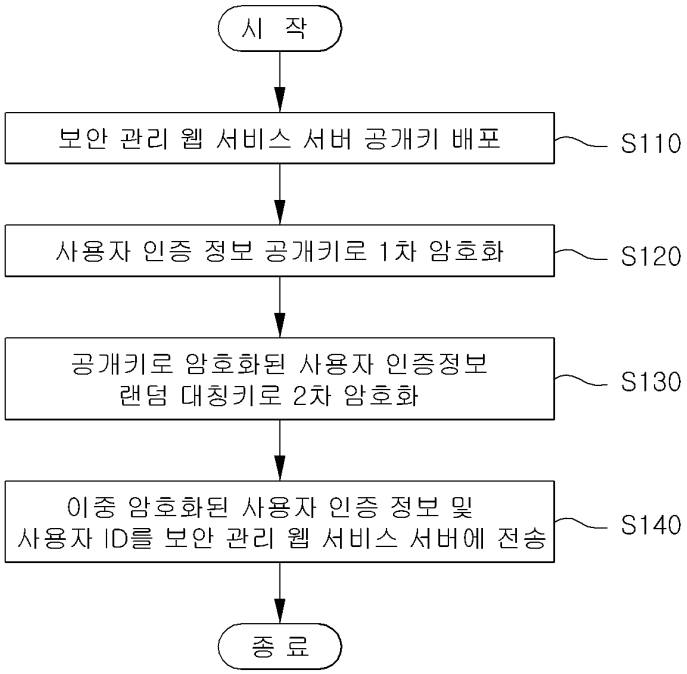
도면4


Client : 정보 암호화(100)
사용자 인증 정보
공개키로 암호화 된 사용자 정보
랜덤 대칭키로 암호화된 정보
보안관리 웹 서비스 서버에서 배포한 공개키(210)
클라이언트 랜덤 대칭키 (110)
Internet
보안 관리 웹 서비스 서버(200)
랜덤 대칭키로 복호화된 정보
개인키로 복호화 된 사용자 정보
사용자 인증
클라이언트 랜덤 대칭키 (110)
보안관리 웹 서비스 서버의 개인키 (220)
Internet
사용자 Request/ Response
암호화/복호화 클라이언트 랜덤 대칭키 (110)
서비스 승인
서비스 요청
보안 관리 웹 서비스 서버
Internet
사용자 키 전달
서비스 게시
암호화/복호화 클라이언트 랜덤 대칭키 (110)
서버 Request/ Response
웹 서비스 서버(300)
사용자 인증
키 전달
서비스 요청 / 개시

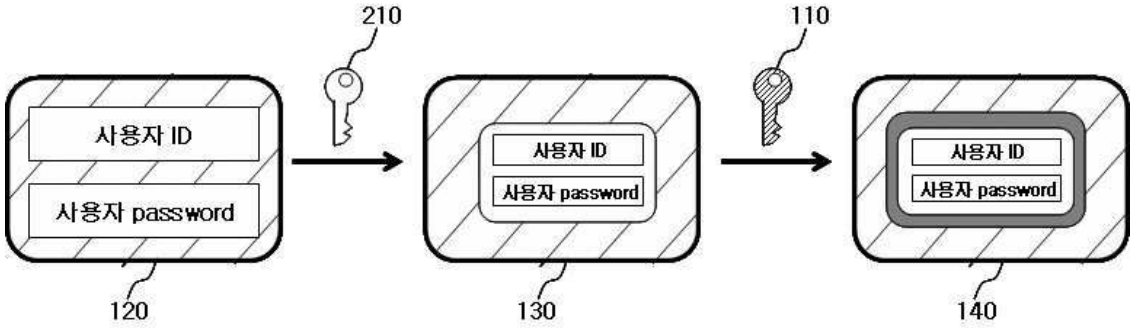
도면5


시 작
사용자 인증 정보 암호화
S100
사용자 인증
S200
사용자의 웹 서비스 요청에 따른 키 전달 및 서비스 개시
S300
종 료

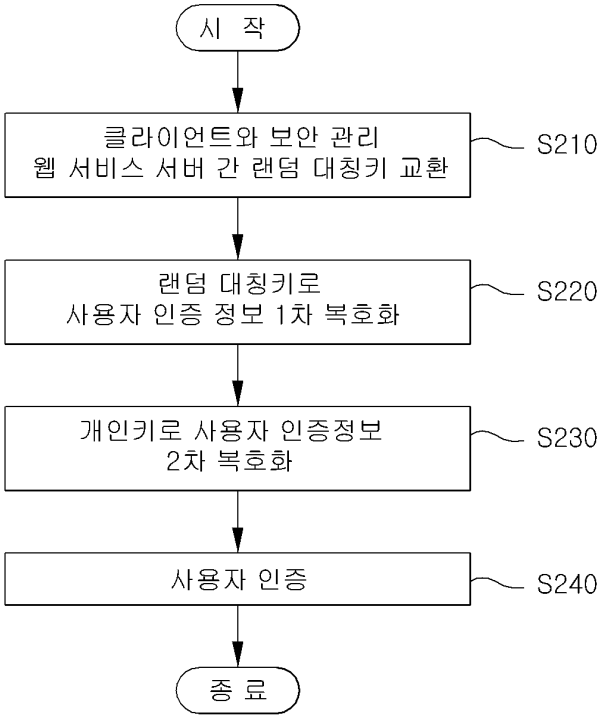
도면6


시 작
보안 관리 웹 서비스 서버 공개키 배포
S110
사용자 인증 정보 공개키로 1차 암호화
S120
공개키로 암호화된 사용자 인증정보
랜덤 대칭키로 2차 암호화
S130
이중 암호화된 사용자 인증 정보 및
사용자 ID를 보안 관리 웹 서비스 서버에 전송
S140
종 료

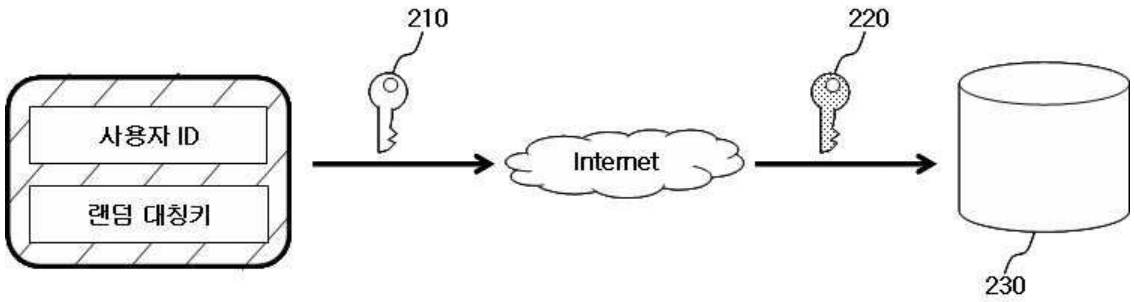
도면7


210
110
사용자 ID
사용자 password
120
사용자 ID
사용자 password
130
사용자 ID
사용자 password
140

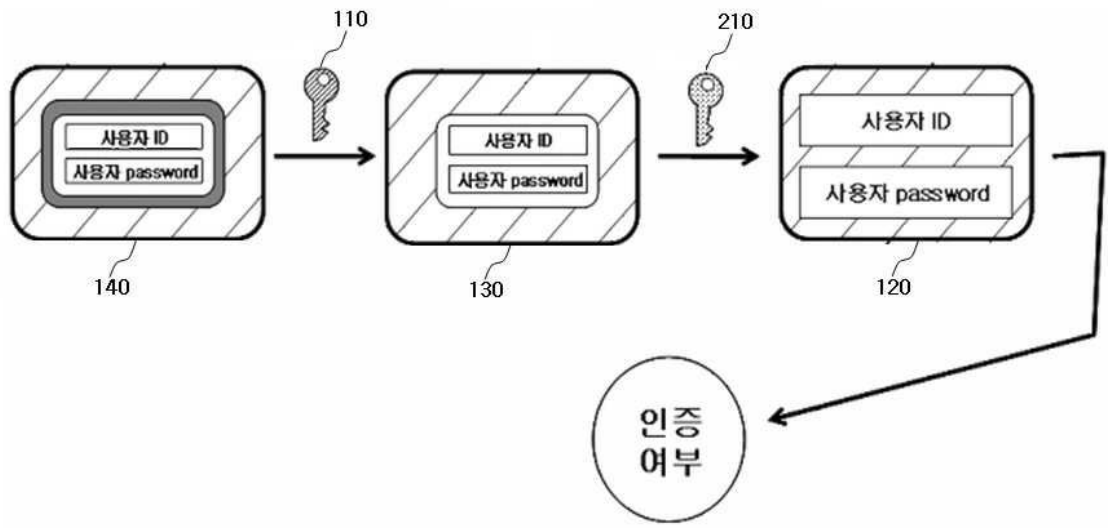
도면8


시 작
클라이언트와 보안 관리
웹 서비스 서버 간 랜덤 대칭키 교환
S210
랜덤 대칭키로
사용자 인증 정보 1차 복호화
S220
개인키로 사용자 인증정보
2차 복호화
S230
사용자 인증
S240
종 료

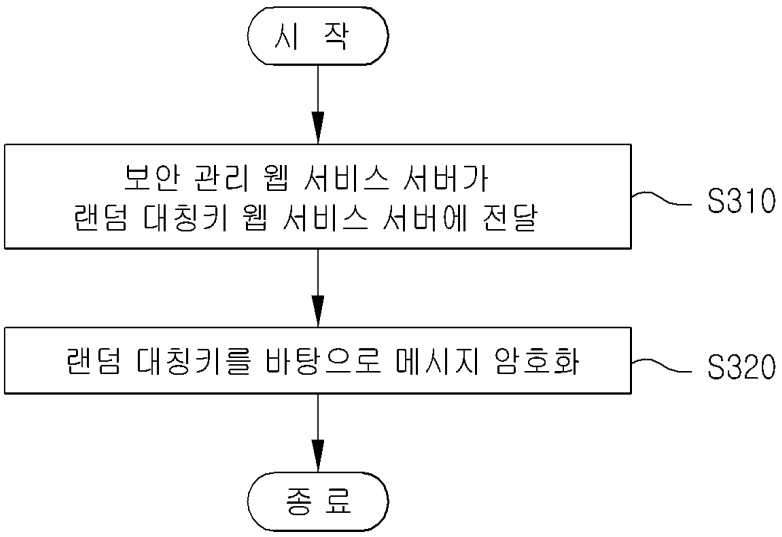
도면9


210
220
사용자 ID
랜덤 대칭키
Internet
230

도면10


110
210
사용자 ID
사용자 password
사용자 ID
사용자 password
사용자 ID
사용자 password
140
130
120
인증
여부

도면11


시 작
보안 관리 웹 서비스 서버가
랜덤 대칭키 웹 서비스 서버에 전달
S310
랜덤 대칭키를 바탕으로 메시지 암호화
S320
종 료

도면12

```
<?xml version="1.0" encoding="utf-8"?>
<S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu="..." xmlns:xenc="..." xmlns:ds="...">
  <S11:Header>
    <wsse:Security>
      <wsu:Timestamp wsu:Id="T0">
        <wsu:Created>2001-09-13T08:42:00Z</wsu:Created>
      </wsu:Timestamp>
      <xenc:ReferenceList>
        <xenc:DataReference URI="#enc1"/>
      </xenc:ReferenceList>
    </wsse:Security>
  </S11:Header>
  <S11:Body wsu:Id="body">
    <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element" wsu:Id="enc1">
      <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
      <ds:KeyInfo>
        <ds:KeyName>CN=Hiroshi Maruyama, C=JP</ds:KeyName>
      </ds:KeyInfo>
      <xenc:CipherData>
        <xenc:CipherValue>d2FpbmdvbGRfE0lm4byV0...</xenc:CipherValue>
      </xenc:CipherData>
    </xenc:EncryptedData>
  </S11:Body>
</S11:Envelope>
```