



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년06월10일
(11) 등록번호 10-1987579
(24) 등록일자 2019년06월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) H04L 12/58 (2006.01)
H04L 29/08 (2006.01) H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/0618 (2013.01)
H04L 51/18 (2013.01)
(21) 출원번호 10-2018-0014373
(22) 출원일자 2018년02월06일
심사청구일자 2018년02월06일
(56) 선행기술조사문헌
JP2000031957 A*
JP2002190796 A*
KR1020160131744 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
양효식
서울특별시 광진구 군자로12길 46, 제101동 208호(군자동, 일성파크아파트)
박명주
서울특별시 강동구 풍성로52길 6-4(성내동)
(74) 대리인
양정보

전체 청구항 수 : 총 9 항

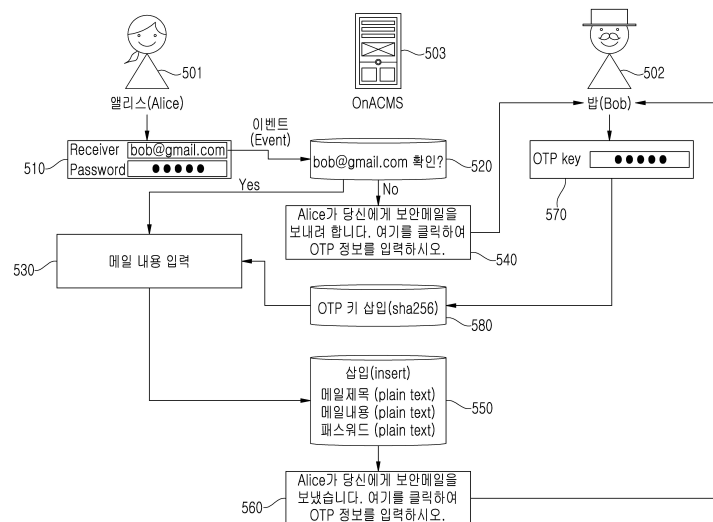
심사관 : 박보미

(54) 발명의 명칭 웹 메일과 OTP 및 디피 헬만 키교환을 이용한 보안메일의 송수신 방법 및 시스템

(57) 요약

웹 메일과 OTP 및 디피 헬만 키교환을 이용한 보안메일의 송수신 방법 및 시스템이 제시된다. 일 실시예에 따른 보안메일의 송수신 방법은 인증 시스템에 사용자를 등록하는 단계; 및 등록된 상기 사용자의 로그인 요청에 응답하여 사용자를 인증하는 단계를 포함하고, 상기 사용자의 로그인 요청에 응답하여 사용자를 인증하는 단계는, 인증 시스템에서 상기 사용자로부터 로그인을 위한 OTP 키 및 OTP에서 생성된 코드를 입력 받아 기 저장된 인증 데이터베이스와 비교하여 일치하는 경우, 사용자로부터 입력 받은 상기 OTP 키를 이용하여 OTP 코드를 생성하고, 생성된 상기 OTP 코드가 사용자로부터 입력 받은 OTP 코드와 일치하는지 여부를 확인하여, 이중 정보 인증 절차를 통해 사용자의 로그인을 허용할 수 있다.

대표도



(52) CPC특허분류

H04L 67/02 (2013.01)

H04L 9/0822 (2013.01)

H04L 9/0844 (2013.01)

H04L 9/0863 (2013.01)

H04L 9/3228 (2013.01)

H04L 9/3242 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711055194 (세부과제번호 2015-0-00938)

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 SW전문인력역량강화

연구과제명 SW중심대학(세종대)

기 여 율 1/1

주관기관 세종대학교 산학협력단

연구기간 2015.10.01 ~ 2024.02.29

명세서

청구범위

청구항 1

인증 시스템에 사용자를 등록하는 단계;

등록된 상기 사용자의 로그인 요청에 응답하여 사용자를 인증하는 단계; 및

상기 사용자의 로그인 완료 후, 상기 사용자로부터 메일 메시지를 입력 받아 다른 사용자에게 전달하는 단계를 포함하고,

상기 사용자의 로그인 요청에 응답하여 사용자를 인증하는 단계는,

인증 시스템에서 상기 사용자로부터 로그인을 위한 OTP 키 및 OTP에서 생성된 코드를 입력 받아 기 저장된 인증 데이터베이스와 비교하여 일치하는 경우, 사용자로부터 입력 받은 상기 OTP 키를 이용하여 OTP 코드를 생성하고, 생성된 상기 OTP 코드가 사용자로부터 입력 받은 OTP 코드와 일치하는지 여부를 확인하여, 이중 정보 인증 절차를 통해 사용자의 로그인을 허용하며,

상기 사용자의 로그인 완료 후, 상기 사용자로부터 메일 메시지를 입력 받아 다른 사용자에게 전달하는 단계는,

상기 다른 사용자에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달하여, 상기 사용자로부터 입력 받은 메일 메시지를 상기 뷰어 페이지를 통해 상기 다른 사용자에게 전달하고, 상기 하이퍼링크의 URL(uniform resource locator)에는 유니크(unique)한 메시지 ID와 메시지가 저장된 데이터베이스의 순서 번호(sequence number)가 포함되며,

상기 사용자의 메시지를 웹 서버에서 전달 받을 때 상기 메시지에 대한 암호와 함께 메시지를 입력 받고, 사용자로부터 입력 받은 암호와 서버에서 생성한 난수(random number) 간의 디피 헬만(Diffie-Hellman) 키교환(key exchange)을 통하여 대칭키(symmetric key)를 생성하며, 생성된 상기 대칭키를 이용하여 메일 제목 및 메시지를 암호화하고,

상기 사용자로부터 입력 받은 암호는 최초에만 저장되고 1회 열람 후 어디에도 저장되지 않도록 하여 대칭키(symmetric key)를 유추할 수 없도록 하며, 암호화된 메시지는 메일 서버의 데이터베이스에 저장되고, 저장된 후 사용자가 작성한 메시지 원문은 제거되는 것

을 특징으로 하는 보안메일의 송수신 방법.

청구항 2

제1항에 있어서,

상기 인증 시스템에 사용자를 등록하는 단계는,

인증 시스템에서 상기 사용자로부터 ID, 패스워드 및 OTP 키의 정보를 전송 받는 단계; 및

상기 인증 시스템으로 전송된 사용자 정보 중 패스워드와 OTP 키를 해시(Hash)하여 인증 데이터베이스에 저장하는 단계

를 포함하는 보안메일의 송수신 방법.

청구항 3

제1항에 있어서,

상기 사용자의 로그인 요청에 응답하여 사용자를 인증하는 단계는,

인증 시스템에서 상기 사용자로부터 로그인을 위한 ID, 패스워드, OTP 키 및 OTP에서 생성된 코드(code)를 입력 받는 단계;

상기 사용자로부터 입력 받은 ID, 입력 받은 패스워드를 해시(Hash)한 값 및 입력 받은 OTP 키를 해시(Hash)한

값으로 변환하는 단계;

상기 사용자로부터 입력 받은 ID, 입력 받은 패스워드를 해시(Hash)한 값 및 입력 받은 OTP 키를 해시(Hash)한 값을 기 저장된 인증 데이터베이스와 비교하는 단계;

상기 사용자로부터 입력 받은 정보들과 상기 인증 데이터베이스 사이에 일치하는 데이터가 발견되는 경우, 인증 시스템에서 사용자로부터 입력 받은 OTP 키를 이용하여 OTP 코드를 생성하는 단계;

생성된 상기 OTP 코드가 사용자로부터 입력 받은 OTP 코드와 일치하는지 여부를 확인하는 단계; 및

상기 OTP 코드가 사용자가 입력한 OTP 코드와 일치하는 경우, 사용자의 로그인을 허용하는 단계

를 포함하는 보안메일의 송수신 방법.

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

제1항에 있어서,

상기 사용자의 로그인 완료 후, 상기 사용자로부터 메일 메시지를 입력 받아 다른 사용자에게 전달하는 단계는,

상기 사용자로부터 상기 다른 사용자의 이메일 주소 작성 이벤트(event)를 감지하여, 상기 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있는지 여부를 확인하는 단계;

상기 다른 사용자의 이메일 주소가 상기 데이터베이스에 저장되어 있을 경우, 상기 사용자로부터 이메일 제목, 이메일 메시지 및 메시지 암호를 입력 받아, 상기 데이터베이스에 일반 텍스트(plain text) 형태로 저장하는 단계; 및

상기 다른 사용자에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달하는 단계

를 포함하는 보안메일의 송수신 방법.

청구항 8

제7항에 있어서,

상기 사용자의 로그인 완료 후, 상기 사용자로부터 메일 메시지를 입력 받아 다른 사용자에게 전달하는 단계는,

상기 사용자로부터 상기 다른 사용자의 이메일 주소 작성 이벤트(event)를 감지하여, 상기 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있는지 여부를 확인한 다음, 상기 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있지 않을 경우, 상기 다른 사용자에게 OTP 정보를 입력 받기 위한 메시지를 보내는 단계;

상기 다른 사용자로부터 메시지 내의 하이퍼링크를 통해 이동한 페이지에서 OTP 정보를 입력 받는 단계; 및

입력 받은 상기 OTP 정보를 데이터베이스에 저장 후, 상기 사용자에게 상기 다른 사용자에게 이메일을 보내도 좋다는 메시지 전달하는 단계

를 더 포함하고,

상기 사용자에게 상기 다른 사용자에게 이메일을 보내도 좋다는 메시지 전달한 다음, 상기 사용자로부터 이메일 제목, 이메일 메시지 및 메시지 암호를 입력 받아, 상기 데이터베이스에 일반 텍스트(plain text) 형태로 저장하고, 상기 다른 사용자에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달하는 것

을 특징으로 하는 보안메일의 송수신 방법.

청구항 9

사용자를 등록하는 등록부;

등록된 상기 사용자의 로그인 요청에 응답하여 사용자를 인증하는 인증부; 및

상기 사용자의 로그인 완료 후, 상기 사용자로부터 메일 메시지를 입력 받아 다른 사용자에게 전달하는 메시지 전송부

를 포함하고,

상기 인증부는,

상기 사용자로부터 로그인을 위한 OTP 키 및 OTP에서 생성된 코드를 입력 받아 기 저장된 인증 데이터베이스와 비교하여 일치하는 경우, 사용자로부터 입력 받은 상기 OTP 키를 이용하여 OTP 코드를 생성하고, 생성된 상기 OTP 코드가 사용자로부터 입력 받은 OTP 코드와 일치하는지 여부를 확인하여, 이중 정보 인증 절차를 통해 사용자의 로그인을 허용하며,

상기 메시지 전송부는,

상기 다른 사용자에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달하여, 상기 사용자로부터 입력 받은 메일 메시지를 상기 뷰어 페이지를 통해 상기 다른 사용자에게 전달하고, 상기 하이퍼링크의 URL(uniform resource locator)에는 유니크(unique)한 메시지 ID와 메시지가 저장된 데이터베이스의 순서 번호(sequence number)가 포함되며,

상기 사용자의 메시지를 웹 서버에서 전달 받을 때 상기 메시지에 대한 암호와 함께 메시지를 입력 받고, 사용자로부터 입력 받은 암호와 서버에서 생성한 난수(random number) 간의 디피 헬만(Diffie-Hellman) 키교환(key exchange)을 통하여 대칭키(symmetrical key)를 생성하며, 생성된 상기 대칭키를 이용하여 메일 제목 및 메시지를 암호화하고,

상기 사용자로부터 입력 받은 암호는 최초에만 저장되고 1회 열람 후 어디에도 저장되지 않도록 하여 대칭키(symmetrical key)를 유추할 수 없도록 하며, 암호화된 메시지는 메일 서버의 데이터베이스에 저장되고, 저장된 후 사용자가 작성한 메시지 원문은 제거되는 것

을 특징으로 하는 보안메일의 송수신 시스템.

청구항 10

제9항에 있어서,

상기 등록부는,

상기 사용자로부터 ID, 패스워드 및 OTP 키의 정보를 전송 받아, 전송된 사용자 정보 중 패스워드와 OTP 키를 해시(Hash)하여 인증 데이터베이스에 저장하고,

상기 인증부는,

상기 사용자로부터 로그인을 위한 ID, 패스워드, OTP 키 및 OTP에서 생성된 코드(code)를 입력 받아 입력 받은 ID, 입력 받은 패스워드를 해시(Hash)한 값 및 입력 받은 OTP 키를 해시(Hash)한 값으로 변환하고 기 저장된 인증 데이터베이스와 비교하여, 상기 사용자로부터 입력 받은 정보들과 상기 인증 데이터베이스 사이에 일치하는 데이터가 발견되는 경우, 인증 시스템에서 사용자로부터 입력 받은 OTP 키를 이용하여 OTP 코드를 생성하고, 생성된 상기 OTP 코드가 사용자로부터 입력 받은 OTP 코드와 일치하는지 여부를 확인하며, 상기 OTP 코드가 사용자가 입력한 OTP 코드와 일치하는 경우, 사용자의 로그인을 허용하는 것

을 특징으로 하는 보안메일의 송수신 시스템.

청구항 11

삭제

청구항 12

제9항에 있어서,

상기 메시지 전송부는,

상기 사용자로부터 상기 다른 사용자의 이메일 주소 작성 이벤트(event)를 감지하여, 상기 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있는지 여부를 확인하는 감지부;

상기 다른 사용자의 이메일 주소가 상기 데이터베이스에 저장되어 있을 경우, 상기 사용자로부터 이메일 제목, 이메일 메시지 및 메시지 암호를 입력 받아, 상기 데이터베이스에 일반 텍스트(plain text) 형태로 저장하는 저장부; 및

상기 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있지 않을 경우, 상기 다른 사용자에게 OTP 정보를 입력 받기 위한 메시지를 보내고, 상기 다른 사용자로부터 메시지 내의 하이퍼링크를 통해 이동한 페이지에서 OTP 정보를 입력 받아, 입력 받은 상기 OTP 정보를 데이터베이스에 저장 후, 상기 사용자에게 상기 다른 사용자에게 이메일을 보내도 좋다는 메시지를 전달하며, 사용자로부터 전송 받은 메시지 전송을 위해 상기 다른 사용자에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달하는 메시지부

를 포함하는 보안메일의 송수신 시스템.

청구항 13

제9항에 있어서,

최초 열람 시, 데이터베이스에 저장된 일반 텍스트(plain text)에 대하여 암호화(encrypt)가 진행되며, 암호화는 서로 다른 두 개의 대칭키(symmetric key)를 생성하여 하나는 상기 사용자가 열람할 데이터베이스에 사용하고 나머지 하나는 상기 다른 사용자가 열람할 데이터베이스에 사용하는 것

을 특징으로 하는 보안메일의 송수신 시스템.

청구항 14

삭제

청구항 15

삭제

발명의 설명

기술 분야

[0001] 아래의 실시예들은 웹 메일과 OTP 및 디피 헬만 키교환을 이용한 보안메일의 송수신 방법 및 시스템에 관한 것으로, 더욱 상세하게는, OTP 및 AES 암호화 메일 시스템의 웹 메일과 OTP 및 디피 헬만 키교환을 이용한 보안메일의 송수신 방법 및 시스템에 관한 것이다.

[0002]본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학사업의 연구결과로 수행되었음(2015-0-00938).

배경 기술

[0003]일반적으로 웹 메일(web mail) 시스템은 인터넷 망에 접속된 단말기를 이용하는 사용자가 전하고 싶은 내용을 담은 텍스트나 단말기에 저장된 텍스트파일 및 멀티미디어파일 등의 첨부파일을 포함한 메시지를 인터넷 망에 접속된 단말기를 이용하는 다른 사용자와 서로 주고 받을 수 있도록 한 시스템이다.

[0004]상기의 웹 메일 시스템은 인터넷 망과, 인터넷 망에 연결되고 메일작성을 위한 메일작성 인터페이스가 구비된 단말기와, 웹 메일 주소를 제공하는 웹 메일 서버로 구성되고, 인터넷 망과 단말기와 웹 메일 서버 간에 HTTP 프로토콜과 SMTP 프로토콜과 POP3 프로토콜과 IMAP4 프로토콜이 적용된다.

[0005]따라서 발신자가 단말기의 메일작성 인터페이스를 통해 웹 메일을 작성하여 수신자에게 발신하게 되면, 상기한 HTTP 프로토콜과 SMTP 프로토콜과 POP3 프로토콜과 IMAP4 프로토콜에 의하여 발신자의 웹 메일 서버와 수신자의 웹 메일 서버를 거쳐 수신자는 자신의 단말기를 통해 웹 메일을 수신하게 되는 것이다.

[0006] 그러나 이러한 종래의 웹 메일 시스템은 상기 SMTP 프로토콜, POP3 프로토콜, IMAP4 프로토콜, HTTP 프로토콜이 강력한 보안 메커니즘이 추가 구성되지 않으므로, 웹 메일의 메시지 내용을 알려고 하는 공격자의 공격으로부터 안전하지 못하다.

[0007] 이에 따라 Secure/MIME(Secure/Multipurpose Internet Mail Extension; 이하, S/MIME라 함) 형식의 메일 포맷을 사용하여 웹 메일 메시지를 작성하고, 그 작성된 웹 메일 메시지에 대해 암호화 및 전자서명을 추가한 보안 메일이 생겨났다. 이러한 S/MIME은 전자서명과 메시지 암호화의 두 가지 보안 서비스를 제공한다. 공개키 기반의 암호화 프레임워크가 S/MIME을 사용하여 메시지 내용을 보호하기에는 훌륭하지만 공개키를 통합 관리하는 데에는 높은 비용 따르며, PC의 해킹 또는 멀웨어(malicious software; malware)나 랜섬웨어(ransomware)로부터 메시지를 안전하게 보호할 수 없다.

[0008] 한국공개특허 특2002-0067372호는 이러한 에스/마임 표준을 준수하는 보안 웹 메일의 송수신 방법에 관한 것으로, 인증서버와의 연동을 통하여 자체적으로 인증서를 발급받는 에스/마임 표준을 준수하는 보안 웹 메일의 송수신 방법에 관한 기술을 기재하고 있다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 한국공개특허 특2002-0067372호

발명의 내용

해결하려는 과제

[0010] 실시예들은 웹 메일과 OTP 및 디피 헬만 키교환을 이용한 보안메일의 송수신 방법 및 시스템에 관하여 기술하며, 보다 구체적으로 메일 메시지의 암호화를 위해 메일 송신자와 서버, 서버와 수신자 간 디피-헬만 키교환(Diffie-Hellman key exchange)을 이용한 비밀키를 생성한 후 생성된 비밀키를 이용하여 메일 본문을 암호화하여 해당 메일의 열람을 제한하는 웹 메일과 OTP 및 디피 헬만 키교환을 이용한 보안메일의 송수신 방법 및 시스템을 제공하는데 있다.

과제의 해결 수단

[0011] 일 실시예에 따른 보안메일의 송수신 방법은, 인증 시스템에 사용자를 등록하는 단계; 및 등록된 상기 사용자의 로그인 요청에 응답하여 사용자를 인증하는 단계를 포함하고, 상기 사용자의 로그인 요청에 응답하여 사용자를 인증하는 단계는, 인증 시스템에서 상기 사용자로부터 로그인을 위한 OTP 키 및 OTP에서 생성된 코드를 입력 받아 기 저장된 인증 데이터베이스와 비교하여 일치하는 경우, 사용자로부터 입력 받은 상기 OTP 키를 이용하여 OTP 코드를 생성하고, 생성된 상기 OTP 코드가 사용자로부터 입력 받은 OTP 코드와 일치하는지 여부를 확인하여, 이중 정보 인증 절차를 통해 사용자의 로그인을 허용할 수 있다.

[0012] 상기 인증 시스템에 사용자를 등록하는 단계는, 인증 시스템에서 상기 사용자로부터 ID, 패스워드 및 OTP 키의 정보를 전송 받는 단계; 및 상기 인증 시스템으로 전송된 사용자 정보 중 패스워드와 OTP 키를 해시(Hash)하여 인증 데이터베이스에 저장하는 단계를 포함할 수 있다.

[0013] 상기 사용자의 로그인 요청에 응답하여 사용자를 인증하는 단계는, 인증 시스템에서 상기 사용자로부터 로그인을 위한 ID, 패스워드, OTP 키 및 OTP에서 생성된 코드(code)를 입력 받는 단계; 상기 사용자로부터 입력 받은 ID, 입력 받은 패스워드를 해시(Hash)한 값 및 입력 받은 OTP 키를 해시(Hash)한 값으로 변환하는 단계; 상기 사용자로부터 입력 받은 ID, 입력 받은 패스워드를 해시(Hash)한 값 및 입력 받은 OTP 키를 해시(Hash)한 값을 기 저장된 인증 데이터베이스와 비교하는 단계; 상기 사용자로부터 입력 받은 정보들과 상기 인증 데이터베이스 사이에 일치하는 데이터가 발견되는 경우, 인증 시스템에서 사용자로부터 입력 받은 OTP 키를 이용하여 OTP 코드를 생성하는 단계; 생성된 상기 OTP 코드가 사용자로부터 입력 받은 OTP 코드와 일치하는지 여부를 확인하는 단계; 및 상기 OTP 코드가 사용자가 입력한 OTP 코드와 일치하는 경우, 사용자의 로그인을 허용하는 단계를 포함할 수 있다.

[0014] 상기 사용자의 로그인 완료 후, 상기 사용자로부터 메일 메시지를 입력 받아 다른 사용자에게 전달하는 단계를

더 포함하고, 상기 다른 사용자에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달하여, 상기 사용자로부터 입력 받은 메일 메시지를 상기 뷰어 페이지를 통해 상기 다른 사용자에게 전달할 수 있다.

[0015] 상기 사용자의 메시지를 웹 서버에 전달 받을 때 상기 메시지에 대한 암호와 함께 메시지를 입력 받고, 상기 사용자로부터 입력 받은 암호와 서버에서 생성한 난수(random number) 간의 디피 헬만(Diffie-Hellman) 키교환(key exchange)을 통하여 대칭키(symmetric key)를 생성할 수 있다.

[0016] 상기 사용자로부터 입력 받은 암호는 최초에만 저장되고 1회 열람 후 어디에도 저장되지 않도록 하여 대칭키(symmetric key)를 유추할 수 없도록 하며, 암호화된 메시지는 메일 서버의 데이터베이스에 저장되고, 저장된 후 사용자가 작성한 메시지 원문은 제거될 수 있다.

[0017] 상기 사용자의 로그인 완료 후, 상기 사용자로부터 메일 메시지를 입력 받아 다른 사용자에게 전달하는 단계는, 상기 사용자로부터 상기 다른 사용자의 이메일 주소 작성 이벤트(event)를 감지하여, 상기 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있는지 여부를 확인하는 단계; 상기 다른 사용자의 이메일 주소가 상기 데이터베이스에 저장되어 있을 경우, 상기 사용자로부터 이메일 제목, 이메일 메시지 및 메시지 암호를 입력 받아, 상기 데이터베이스에 일반 텍스트(plain text) 형태로 저장하는 단계; 및 상기 다른 사용자에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달하는 단계를 포함할 수 있다.

[0018] 상기 사용자의 로그인 완료 후, 상기 사용자로부터 메일 메시지를 입력 받아 다른 사용자에게 전달하는 단계는, 상기 사용자로부터 상기 다른 사용자의 이메일 주소 작성 이벤트(event)를 감지하여, 상기 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있는지 여부를 확인한 다음, 상기 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있지 않을 경우, 상기 다른 사용자에게 OTP 정보를 입력 받기 위한 메시지를 보내는 단계; 상기 다른 사용자로부터 메시지 내의 하이퍼링크를 통해 이동한 페이지에서 OTP 정보를 입력 받는 단계; 및 입력 받은 상기 OTP 정보를 데이터베이스에 저장 후, 상기 사용자에게 상기 다른 사용자에게 이메일을 보내도 좋다는 메시지 전달하는 단계를 더 포함하고, 상기 사용자에게 상기 다른 사용자에게 이메일을 보내도 좋다는 메시지 전달한 다음, 상기 사용자로부터 이메일 제목, 이메일 메시지 및 메시지 암호를 입력 받아, 상기 데이터베이스에 일반 텍스트(plain text) 형태로 저장하고, 상기 다른 사용자에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달할 수 있다.

[0019] 다른 실시예에 따른 보안메일의 송수신 시스템은, 사용자를 등록하는 등록부; 및 등록된 상기 사용자의 로그인 요청에 응답하여 사용자를 인증하는 인증부를 포함하고, 상기 인증부는, 상기 사용자로부터 로그인을 위한 OTP 키 및 OTP에서 생성된 코드를 입력 받아 기 저장된 인증 데이터베이스와 비교하여 일치하는 경우, 사용자로부터 입력 받은 상기 OTP 키를 이용하여 OTP 코드를 생성하고, 생성된 상기 OTP 코드가 사용자로부터 입력 받은 OTP 코드와 일치하는지 여부를 확인하여, 이중 정보 인증 절차를 통해 사용자의 로그인을 허용할 수 있다.

[0020] 상기 등록부는, 상기 사용자로부터 ID, 패스워드 및 OTP 키의 정보를 전송 받아, 전송된 사용자 정보 중 패스워드와 OTP 키를 해시(Hash)하여 인증 데이터베이스에 저장하고, 상기 인증부는, 상기 사용자로부터 로그인을 위한 ID, 패스워드, OTP 키 및 OTP에서 생성된 코드(code)를 입력 받아 입력 받은 ID, 입력 받은 패스워드를 해시(Hash)한 값 및 입력 받은 OTP 키를 해시(Hash)한 값으로 변환하고 기 저장된 인증 데이터베이스와 비교하여, 상기 사용자로부터 입력 받은 정보들과 상기 인증 데이터베이스 사이에 일치하는 데이터가 발견되는 경우, 인증 시스템에서 사용자로부터 입력 받은 OTP 키를 이용하여 OTP 코드를 생성하고, 생성된 상기 OTP 코드가 사용자로부터 입력 받은 OTP 코드와 일치하는지 여부를 확인하며, 상기 OTP 코드가 사용자가 입력한 OTP 코드와 일치하는 경우, 사용자의 로그인을 허용할 수 있다.

[0021] 상기 사용자의 로그인 완료 후, 상기 사용자로부터 메일 메시지를 입력 받아 다른 사용자에게 전달하는 메시지 전송부를 더 포함하고, 상기 메시지 전송부는, 상기 다른 사용자에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달하여, 상기 사용자로부터 입력 받은 메일 메시지를 상기 뷰어 페이지를 통해 상기 다른 사용자에게 전달할 수 있다.

[0022] 상기 메시지 전송부는, 상기 사용자로부터 상기 다른 사용자의 이메일 주소 작성 이벤트(event)를 감지하여, 상기 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있는지 여부를 확인하는 감지부; 상기 다른 사용자의 이메일 주소가 상기 데이터베이스에 저장되어 있을 경우, 상기 사용자로부터 이메일 제목, 이메일 메시지 및 메시지 암호를 입력 받아, 상기 데이터베이스에 일반 텍스트(plain text) 형태로 저장하는 저장부; 및 상기 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있지 않을 경우, 상기 다른 사용자에게 OTP 정보를 입력 받기 위한 메시지를 보내고, 상기 다른 사용자로부터 메시지 내의 하이퍼링크를 통해 이동한 페이지에서 OTP 정보를

입력 받아, 입력 받은 상기 OTP 정보를 데이터베이스에 저장 후, 상기 사용자에게 상기 다른 사용자에게 이메일을 보내도 좋다는 메시지를 전달하며, 사용자로부터 전송 받은 메시지 전송을 위해 상기 다른 사용자에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달하는 메시지부를 포함할 수 있다.

[0023] 최초 열람 시, 데이터베이스에 저장된 일반 텍스트(plain text)에 대하여 암호화(encrypt)가 진행되며, 암호화는 서로 다른 두 개의 대칭키(symmetrical key)를 생성하여 하나는 상기 사용자가 열람할 데이터베이스에 사용하고 나머지 하나는 상기 다른 사용자가 열람할 데이터베이스에 사용할 수 있다.

[0024] 상기 사용자의 메시지를 웹 서버에 전달 받을 때 상기 메시지에 대한 암호와 함께 메시지를 입력 받고, 상기 사용자로부터 입력 받은 암호와 서버에서 생성한 난수(random number) 간의 디피 헬만(Diffie-Hellman) 키교환(key exchange)을 통하여 대칭키(symmetrical key)를 생성할 수 있다.

[0025] 상기 사용자로부터 입력 받은 암호는 최초에만 저장되고 1회 열람 후 어디에도 저장되지 않도록 하여 대칭키(symmetrical key)를 유추할 수 없도록 하며, 암호화된 메시지는 메일 서버의 데이터베이스에 저장되고, 저장된 후 사용자가 작성한 메시지 원문은 제거될 수 있다.

발명의 효과

[0026] 실시예들에 따르면 메일 메시지의 암호화를 위해 메일 송신자와 서버, 서버와 수신자 간 디피-헬만 키교환(Diffie-Hellman key exchange)을 이용한 비밀키를 생성한 후 생성된 비밀키를 이용하여 메일 본문을 암호화하여 해당 메일의 열람을 제한하는 웹 메일과 OTP 및 디피 헬만 키교환을 이용한 보안메일의 송수신 방법 및 시스템을 제공할 수 있다.

[0027] 실시예들에 따르면 사용되는 웹 메일 기반의 HTTP 통신은 HTTP를 사용하여 사용자가 작성한 메시지가 웹 서버로 전달될 때 암호화되도록 함으로써, 호스트 파일의 변조에 의한 웹 서버 스푸핑(spoofing) 또는 DNS 스푸핑과 같은 A Host 변조 공격을 제외한 모든 상황에서 메시지를 보호할 수 있다.

[0028] 실시예들에 따르면 사용자가 메시지를 웹 서버에 전달 시 해당 메시지에 대한 암호를 입력하고 입력된 암호가 메시지와 함께 전달되며, 이 때 사용자가 입력한 암호와 서버에서 생성한 난수(random number) 간의 디피 헬만(Diffie-Hellman) 키교환을 통하여 대칭키를 생성하고, 사용자가 입력한 암호는 최초에만 저장되고 1회 열람 후 어디에도 저장되지 않도록 하여 대칭키를 유추할 수 없도록 할 수 있다.

도면의 간단한 설명

- [0029] 도 1은 일 실시예에 따른 보안메일의 송수신 방법을 설명하기 위한 흐름도이다.
 도 2는 일 실시예에 따른 보안메일의 송수신 시스템을 설명하기 위한 블록도이다.
 도 3은 일 실시예에 따른 사용자 등록 방법을 설명하기 위한 도면이다.
 도 4는 일 실시예에 따른 사용자 인증 방법을 설명하기 위한 도면이다.
 도 5는 일 실시예에 따른 이메일 메시지 전송 방법을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0030] 이하, 첨부된 도면을 참조하여 실시예들을 설명한다. 그러나, 기술되는 실시예들은 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 이하 설명되는 실시예들에 의하여 한정되는 것은 아니다. 또한, 여러 실시예들은 당해 기술분야에서 평균적인 지식을 가진 자에게 본 발명을 더욱 완전하게 설명하기 위해서 제공되는 것이다. 도면에서 요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있다.

[0031] 아래의 실시예들은 웹 메일과 OTP 및 디피 헬만 키교환을 이용한 보안메일의 송수신 방법 및 시스템에 관한 것으로, 이메일(e-mail) 메시지를 아무나 열람할 수 없도록 S/MIME을 사용하지 않으면서 메일 서버(server)에 메시지를 저장하며, 개인 메일 메시지의 암호화를 위해 메일 송신자와 서버, 서버와 수신자 간의 디피-헬만 키교환(Diffie-Hellman key exchange)을 이용한 비밀키를 생성한 후 생성된 비밀키를 이용하여 메일 본문을 암호화하고, 해당 메일의 열람을 제한하여 이메일 서버가 노출되거나 개인 컴퓨터의 로그인 권한이 탈취되었을 상황에도 메일 내용을 보호할 수 있다. 또한, 부인방지 및 인증을 위해 OTP(One Time Password)를 활용할 수 있다.

- [0032] 본 실시예에서 제안하는 암호화 시스템은 OTP 및 AES 암호화 메일 시스템(OTP & AES Cryptography Mail System; OnACMS)이다. 편의상 본 실시예에서 제안하는 시스템을 사용하는 사용자는 앨리스(Alice)(즉, 송신자)라 하고 다른 메일 시스템을 사용하는 사용자를 밥(Bob)(즉, 수신자)이라 하기로 한다.
- [0033] OTP는 그 기반이 되는 방식에 따라 해시(Hash)와 타임(Time)의 두 가지로 나뉜다. 해시(Hash)를 이용하는 방식을 해시 기반 메시지 인증 코드(Hash-based Message Authentication Code), 즉, HMAC 기반 OTP(HMAC-based One-Time Password)라고 하여 HOTP라 명명하고 RFC4226에 기술되어 있다. 또한, 타임(Time)을 이용하는 방식을 타임 기반 OTP(Time-based One-Time Password)라 하여 TOTP라 명명하고 RFC6328에 기술되어 있다. 아래에서는 하나의 예로써 구글(google.com)에서 진행 중인 구글 인증(google-authenticator) 프로젝트의 오픈 소스를 이용하여 OTP 인증을 구현하여 보다 구체적으로 설명한다.
- [0034] 본 실시예에 사용되는 웹 메일 기반의 HTTP 통신(communication)은 HTTPS(Hypertext Transfer Protocol over Secure Socket Layer)를 사용하여 앨리스(Alice)가 작성한 메시지가 웹 서버로 전달될 때 암호화되도록 한다. 이를 통하여 호스트(hosts) 파일의 변조에 의한 웹 서버 스푸핑(spoofing)(리눅스(Linux) 기반의 OS의 /etc/hosts 와 윈도우즈(Windows) 기반 OS의 C:\Windows\System32\drivers\etc\hosts 파일을 수정하면 공인된 도메인을 입력해도 해커가 제작한 페이크 웹 사이트(fake web site)로 이동하게 된다.) 또는 DNS 스푸핑(spoofing)과 같은 A Host 변조 공격을 제외한 모든 상황에서 메시지를 보호할 수 있다.
- [0035] 또한, 본 실시예에서 사용되는 암호화 방식은 대칭키(symetric key) AES (Advanced Encryption Standard) 암호화인데, 암호화 키(encrypt key)의 경우 앨리스(Alice)가 메시지를 웹 서버에 전달 시 해당 메시지에 대한 암호>Password)를 입력하고 입력된 암호가 메시지와 함께 전달되는데, 이 때 앨리스(Alice)가 입력한 암호와 서버에서 생성한 난수(random number) 간의 디피 헬만(Diffie-Hellman) 키교환(key exchange)을 통하여 생성하게 된다. 앨리스(Alice)가 입력한 암호는 최초에만 저장되고 1회 열람 후 어디에도 저장되지 않도록 하여 대칭키(symetric key)를 유추할 수 없도록 한다.
- [0036] 암호화된 메시지는 메일서버의 데이터베이스(Database)에 저장되고, 저장된 후 앨리스(Alice)가 작성한 메시지 원문은 제거된다. 메일 서버는 이메일 수신자인 밥(Bob)에게 보낼 새로운 메시지를 생성하고, 생성된 메시지에는 암호화된 메시지를 확인할 수 있는 뷰어 페이지(viewer page)에 대한 하이퍼링크(hyper link)가 포함된다. 밥(Bob)이 이메일을 수신한 후 메시지를 열람하면 특정 뷰어 페이지에 대한 하이퍼링크를 확인할 수 있다. 밥(Bob)은 본인의 이메일 주소와 OTP 정보를 미리 등록해둔 상태에서 앨리스(Alice)가 전달한 메시지를 보기 위해 특정 뷰어 페이지에서 OTP를 이용한 패스워드(이하, OTP code)를 입력해야 한다.
- [0037] 도 1은 일 실시예에 따른 보안메일의 송수신 방법을 설명하기 위한 흐름도이다.
- [0038] 도 1을 참조하면, 일 실시예에 따른 보안메일의 송수신 방법은 인증 시스템에 사용자를 등록하는 단계(110) 및 등록된 사용자의 로그인 요청에 응답하여 사용자를 인증하는 단계(120)를 포함할 수 있다. 실시예에 따라 일 실시예에 따른 보안메일의 송수신 방법은 사용자의 로그인 완료 후, 사용자로부터 메일 메시지를 입력 받아 다른 사용자에게 전달하는 단계(130)을 더 포함할 수 있다.
- [0039] 여기에서 사용자의 로그인 요청에 응답하여 사용자를 인증하는 단계는, 인증 시스템에서 사용자로부터 로그인을 위한 OTP 키 및 OTP에서 생성된 코드를 입력 받아 기 저장된 인증 데이터베이스와 비교하여 일치하는 경우, 사용자로부터 입력 받은 OTP 키를 이용하여 OTP 코드를 생성하고, 생성된 OTP 코드가 사용자로부터 입력 받은 OTP 코드와 일치하는지 여부를 확인하여, 이중 정보 인증 절차를 통해 사용자의 로그인을 허용할 수 있다.
- [0040] 아래에서는 일 실시예에 따른 보안메일의 송수신 방법을 보다 구체적으로 설명하기 위해 도 2에서 설명하는 일 실시예에 따른 보안메일의 송수신 시스템을 하나의 예로써 설명한다.
- [0041] 도 2는 일 실시예에 따른 보안메일의 송수신 시스템을 설명하기 위한 블록도이다.
- [0042] 도 2를 참조하면, 일 실시예에 따른 보안메일의 송수신 시스템은 등록부(210), 인증부(220) 및 메시지 전송부(230)를 포함하여 이루어질 수 있다. 또한, 메시지 전송부(230)는 감지부(231), 저장부(232) 및 메시지부(233)를 포함하여 이루어질 수 있다. 여기에서 도시되지는 않았지만 인터넷 망을 통해 메시지를 송신하는 사용자로부터 메시지를 전달 받고 전달 받은 메시지를 수신자에게 전달하기 위해 무선 통신부를 더 포함할 수 있다.
- [0043] 여기서, 사용자의 메시지를 웹 서버에 전달 받을 때 메시지에 대한 암호와 함께 메시지를 입력 받고, 사용자로부터 입력 받은 암호와 서버에서 생성한 난수(random number) 간의 디피 헬만(Diffie-Hellman) 키교환(key

exchange)을 통하여 대칭키(symmetric key)를 생성할 수 있다.

- [0044] 또한, 사용자로부터 입력 받은 암호는 최초에만 저장되고 1회 열람 후 어디에도 저장되지 않도록 하여 대칭키(symmetric key)를 유추할 수 없도록 하며, 암호화된 메시지는 메일 서버의 데이터베이스에 저장되고, 저장된 후 사용자가 작성한 메시지 원문은 제거될 수 있다.
- [0045] 단계(110)에서, 등록부(210)는 인증 시스템에 사용자를 등록할 수 있다.
- [0046] 등록부(210)는 인증 시스템에서 사용자로부터 ID, 패스워드 및 OTP 키의 정보를 전송 받고, 이후, 인증 시스템으로 전송된 사용자 정보 중 패스워드와 OTP 키를 해시(Hash)하여 인증 데이터베이스에 저장할 수 있다.
- [0047] 인증부(220)는 등록된 사용자의 로그인 요청에 응답하여 사용자를 인증할 수 있다. 이러한 인증부(220)는 인증 시스템에서 사용자로부터 로그인을 위한 OTP 키 및 OTP에서 생성된 코드를 입력 받아 기 저장된 인증 데이터베이스와 비교하여 일치하는 경우, 사용자로부터 입력 받은 OTP 키를 이용하여 OTP 코드를 생성하고, 생성된 OTP 코드가 사용자로부터 입력 받은 OTP 코드와 일치하는지 여부를 확인하여, 이중 정보 인증 절차를 통해 사용자의 로그인을 허용할 수 있다.
- [0048] 보다 구체적으로, 인증부(220)는 인증 시스템에서 사용자로부터 로그인을 위한 ID, 패스워드, OTP 키 및 OTP에서 생성된 코드(code)를 입력 받고, 사용자로부터 입력 받은 ID, 입력 받은 패스워드를 해시(Hash)한 값 및 입력 받은 OTP 키를 해시(Hash)한 값으로 변환한 후, 사용자로부터 입력 받은 ID, 입력 받은 패스워드를 해시(Hash)한 값 및 입력 받은 OTP 키를 해시(Hash)한 값을 기 저장된 인증 데이터베이스와 비교할 수 있다. 여기서, 인증부(220)는 사용자로부터 입력 받은 정보들과 인증 데이터베이스 사이에 일치하는 데이터가 발견되는 경우, 인증 시스템에서 사용자로부터 입력 받은 OTP 키를 이용하여 OTP 코드를 생성하고, 생성된 OTP 코드가 사용자로부터 입력 받은 OTP 코드와 일치하는지 여부를 확인할 수 있다. 그리고 인증부(220)는 OTP 코드가 사용자가 입력한 OTP 코드와 일치하는 경우, 사용자의 로그인을 허용할 수 있다.
- [0049] 메시지 전송부(230)는 사용자의 로그인 완료 후, 사용자로부터 메일 메시지를 입력 받아 다른 사용자에게 전달할 수 있다. 이러한 메시지 전송부(230)는 다른 사용자에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달하여, 사용자로부터 입력 받은 메일 메시지를 뷰어 페이지를 통해 다른 사용자에게 전달할 수 있다.
- [0050] 또한, 메시지 전송부(230)는 사용자의 메시지를 웹 서버에 전달 받을 때 메시지에 대한 암호와 함께 메시지를 입력 받고, 사용자로부터 입력 받은 암호와 서버에서 생성한 난수(random number) 간의 디피 헬만(Diffie-Hellman) 키교환(key exchange)을 통하여 대칭키(symmetric key)를 생성할 수 있다.
- [0051] 그리고, 메시지 전송부(230)는 사용자로부터 입력 받은 암호는 최초에만 저장되고 1회 열람 후 어디에도 저장되지 않도록 하여 대칭키(symmetric key)를 유추할 수 없도록 하며, 암호화된 메시지는 메일 서버의 데이터베이스에 저장되고, 저장된 후 사용자가 작성한 메시지 원문은 제거될 수 있다.
- [0052] 보다 구체적으로, 메시지 전송부(230)는 감지부(231), 저장부(232) 및 메시지부(233)를 포함하여 이루어질 수 있다.
- [0053] 먼저, 감지부(231)는 사용자로부터 다른 사용자의 이메일 주소 작성 이벤트(event)를 감지하여, 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있는지 여부를 확인할 수 있다.
- [0054] 저장부(232)는 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있을 경우, 사용자로부터 이메일 제목, 이메일 메시지 및 메시지 암호를 입력 받아, 데이터베이스에 일반 텍스트(plain text) 형태로 저장할 수 있다. 여기에서, 저장부(232)는 적어도 하나 이상의 데이터베이스로 이루어질 수 있으며, 예컨대 이메일 주소가 저장되는 데이터 베이스, OTP 정보가 저장되는 데이터 베이스 및 사용자로부터 전달 받은 메일 메시지가 저장되는 데이터 베이스 등으로 구분될 수도 있다.
- [0055] 메시지부(233)는 다른 사용자에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달할 수 있다.
- [0056] 한편, 사용자로부터 다른 사용자의 이메일 주소 작성 이벤트(event)를 감지하여, 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있는지 여부를 확인한 다음, 다른 사용자의 이메일 주소가 데이터베이스에 저장되어 있지 않을 경우, 메시지부(233)는 다른 사용자에게 OTP 정보를 입력 받기 위한 메시지를 보낼 수 있다. 그리고 메시지부(233)는 다른 사용자로부터 메시지 내의 하이퍼링크를 통해 이동한 페이지에서 OTP 정보를 입력 받을 수 있다.

- [0057] 또한, 메시지부(233)는 입력 받은 OTP 정보를 저장부(232)의 데이터베이스에 저장 후, 사용자에게 다른 사용자에게 이메일을 보내도 좋다는 메시지 전달할 수 있다.
- [0058] 이에, 저장부(232)는 사용자로부터 이메일 제목, 이메일 메시지 및 메시지 암호를 입력 받아, 데이터베이스에 일반 텍스트(plain text) 형태로 저장하고, 메시지부(233)는 다른 사용자에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달할 수 있다.
- [0059] 도 3은 일 실시예에 따른 사용자 등록 방법을 설명하기 위한 도면이다.
- [0060] 도 3을 참조하면, 시스템에 사용자 등록을 하는 방법을 나타내며, 여기에서는 일 실시예에 따른 시스템을 사용하는 사용자인 앨리스(Alice)를 통해 사용자 등록 방법을 예를 들어 보다 구체적으로 설명한다. 여기서, 시스템은 앞에서 설명한 일 실시예에 따른 시스템을 의미하는 것으로, 이메일을 송신할 수 있는 시스템 또는 적어도 하나 이상의 서버가 될 수 있다.
- [0061] 앨리스(Alice)는 본 시스템에 사용자 등록(sign up)을 할 때, 단계(310)에서 본인의 계정정보와 OTP 키를 인증 시스템(Authentication System)으로 전송할 수 있다. 예를 들어, 앨리스(Alice)는 등록을 위해 자신의 ID와 패스워드 및 OTP 키를 인증 시스템으로 전송할 수 있다.
- [0062] 이에 따라 단계(320)에서 인증 시스템으로 전송된 앨리스(Alice)의 정보 중 패스워드와 OTP 키는 sha256 알고리즘(algorithm)으로 해시(Hash)하여 데이터베이스에 저장함으로써, 등록이 완료될 수 있다.
- [0063] 도 4는 일 실시예에 따른 사용자 인증 방법을 설명하기 위한 도면이다.
- [0064] 도 4를 참조하면, 시스템에 사용자 인증을 하는 방법을 나타내며, 여기에서는 일 실시예에 따른 시스템을 사용하는 사용자인 앨리스(Alice)를 통해 사용자 인증 방법을 예를 들어 보다 구체적으로 설명한다.
- [0065] 앨리스(Alice)는 시스템에 사용자 등록(sign up)을 종료한 다음, 단계(410)에서 시스템에 로그인(login) 시 자신의 ID와 패스워드, OTP 키와 OTP에서 생성된 코드(code)를 입력할 수 있다.
- [0066] 한편, 단계(420)에서 인증 시스템에서는 앨리스(Alice)가 입력한 ID와 입력한 패스워드를 sha256 해시(Hash)한 값, 입력한 OTP 키를 sha256 해시(Hash)한 값으로 변환하고, 단계(430)에서 이 입력한 ID와 입력한 패스워드를 sha256 해시(Hash)한 값, 입력한 OTP 키를 sha256 해시(Hash)한 값을 기 저장된 인증 데이터베이스와 비교할 수 있다. 이 때, 기 저장된 인증 데이터베이스는 사용자 등록 시 데이터베이스에 저장된 정보가 될 수 있다.
- [0067] 앨리스(Alice)가 로그인을 위해 입력한 정보들과 인증 데이터베이스 사이에 일치하는 데이터가 발견되면, 단계(450)에서 인증 시스템은 앨리스(Alice)가 입력한 OTP 키를 이용하여 OTP 코드를 생성하고, 단계(460)에서 이 값이 앨리스(Alice)가 입력한 OTP 코드와 일치하는지 여부를 확인하여 로그인 여부를 결정할 수 있다.
- [0068] 한편, 앨리스(Alice)가 로그인을 위해 입력한 정보들과 인증 데이터베이스 사이에 데이터가 일치하지 않으면, 인증 시스템은 로그인을 허용하지 않는다(440).
- [0069] 예를 들어, 앨리스(Alice)가 로그인을 위해 입력한 정보들과 인증 데이터베이스 사이에 일치하는 데이터가 발견되면, 인증 시스템은 앨리스(Alice)가 입력한 OTP 키를 이용하여 OTP 코드를 생성하고 이 값이 앨리스(Alice)가 입력한 OTP 코드와 일치하는지 여부를 확인하여 일치하는 경우, 로그인을 완료할 수 있다.
- [0070] 다른 예로, 앨리스(Alice)가 로그인을 위해 입력한 정보들과 인증 데이터베이스 사이에 일치하는 데이터가 발견되면, 인증 시스템은 앨리스(Alice)가 입력한 OTP 키를 이용하여 OTP 코드를 생성하고 이 값이 앨리스(Alice)가 입력한 OTP 코드와 일치하는지 여부를 확인하여 일치하지 않는 경우, 로그인을 허용하지 않는다.
- [0071] 이와 같은 이중 정보 인증 절차는 앨리스(Alice)에 대한 인증(authentication) 및 식별(identification)을 보장할 수 있다.
- [0072] 먼저, OnACMS를 통한 이메일 메시지 전송(transfer) 방법을 하나의 예를 들어 설명한다.
- [0073] 도 5는 일 실시예에 따른 이메일 메시지 전송 방법을 설명하기 위한 도면이다.

- [0074] 도 5를 참조하면, 시스템에 로그인 이후 이메일 메시지 전송 방법을 나타내는 것으로, 여기에서는 일 실시예에 따른 시스템을 사용하는 사용자인 앨리스(Alice)와 다른 메일 시스템을 사용하는 사용자를 밥(Bob)을 통해 이메일 메시지 전송 방법을 예를 들어 보다 구체적으로 설명한다.
- [0075] 앨리스(Alice)가 본 시스템의 로그인에 성공한 후, 밥(Bob)에게 이메일 메시지를 전송할 때 앨리스(Alice)와 시스템은 다음의 절차를 수행할 수 있다.
- [0076] 단계(510)에서, 앨리스(Alice)는 밥(Bob)의 이메일 주소를 작성할 수 있다.
- [0077] 단계(520)에서, 시스템(System)은 이메일 주소 작성 이벤트(event)를 감지하여 밥(Bob)의 이메일 주소가 데이터베이스에 저장되어 있는지 확인할 수 있다.
- [0078] 여기에서, 밥(Bob)의 이메일 주소가 데이터베이스에 저장되어 있을 경우, 단계(530)에서 앨리스(Alice)는 이메일 제목, 이메일 메시지 및 메시지 암호 작성 후 시스템에 제출할 수 있다.
- [0079] 이에, 단계(540)에서 시스템(System)은 이메일 제목, 이메일 메시지, 메시지 암호를 데이터베이스에 일반 텍스트(plain text) 형태로 저장 후, 밥(Bob)에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달할 수 있다.
- [0080] 한편, 밥(Bob)의 이메일 주소가 데이터베이스에 저장되어 있지 않을 경우, 단계(540)에서 시스템(System)은 밥(Bob)에게 OTP 정보 입력을 요구하는 이메일을 전달할 수 있다.
- [0081] 단계(570)에서, 밥(Bob)은 시스템으로부터 전달받은 메시지 내의 하이퍼링크를 클릭하여 이동한 페이지에서 자신의 OTP 정보 입력 후 시스템에 제출(submit)할 수 있다.
- [0082] 단계(580)에서, 시스템(System)은 제출된 정보를 데이터베이스에 저장 후, 앨리스(Alice)에게 밥(Bob)에게 이메일을 보내도 좋다는 메시지 전달할 수 있다.
- [0083] 단계(530)에서, 앨리스(Alice)는 이메일 제목, 이메일 메시지 및 메시지 암호 작성 후 시스템에 제출할 수 있다.
- [0084] 단계(540)에서, 시스템(System)은 이메일 제목, 이메일 메시지, 메시지 암호를 데이터베이스에 일반 텍스트(plain text) 형태로 저장 후, 밥(Bob)에게 뷰어 페이지로 이동이 가능한 하이퍼링크가 포함된 메시지를 전달할 수 있다.
- [0085] 한편, 아직까지는 암호화가 이루어지지 않은 상태를 나타낼 수 있다.
- [0086] 아래에서는 OnACMS를 통한 이메일 메시지 확인(viewing) 방법을 하나의 예를 들어 설명한다.
- [0087] 메일을 수신한 밥(Bob)은 내용을 열람하든지 아니면 열람하지 않든지 둘 중에 하나의 행동을 반드시 취하게 된다.
- [0088] 이 때, 앨리스(Alice)는 밥(Bob)이 메일을 열람하기 전에는 언제든지 메일 발송을 취소할 수 있다. 앨리스(Alice)가 메일 발송을 취소하면 OnACMS는 데이터베이스에 저장되어 있는 메시지를 삭제(delete)하고, 밥(Bob)은 앨리스(Alice)가 보낸 메시지를 영구히 열람할 수 없다.
- [0089] 만약, 앨리스(Alice)가 메일 발송을 취소하기 전에 밥(Bob)이 메시지를 열람했다면 앨리스(Alice)는 발송 취소를 할 수 없다. 일반적인 메일 시스템에서 MTA 간의 통신이 완료된 후에는 앨리스(Alice)가 메일 발송을 취소할 수 없는 것과 같은 원리이다.
- [0090] 밥(Bob)이 메시지를 열람하기 위해서는 OnACMS가 보낸 메시지의 하이퍼링크를 클릭하여 뷰어 페이지로 이동해야 하며, 밥(Bob)이 클릭하게 될 하이퍼링크의 URL(uniform resource locator)에는 유니크(unique)한 메시지 ID와 메시지가 저장된 데이터베이스의 순서 번호(sequence number)가 포함될 수 있다.
- [0091] 뷰어 페이지에서는 밥(Bob)의 OTP 키와 OTP에서 생성된 코드를 요구하며, OnACMS는 밥(Bob)이 입력한 OTP 키와 OTP에서 생성한 코드의 검증 확인(validation check)을 진행할 수 있다.
- [0092] 최초 열람 시, OnACMS는 앞서 3-3-2에서 데이터베이스에 저장된 일반 텍스트(plain text)에 대하여 암호화(encrypt)가 진행되며, 암호화는 서로 다른 두 개의 대칭키(symmetric key)를 생성하여 하나는 앨리스(Alice)가

열람할 데이터베이스에 사용하고 나머지 하나는 밥(Bob)이 열람할 데이터베이스에 사용하게 된다.

각각의 대칭키(symmetric key)의 생성과 암호화(encryption)는 다음 표와 같은 순서를 가지고 생성할 수 있다.

표 1은 밥(Bob)의 대칭키(symmetric key)의 생성과 암호화(encryption)를 설명하기 위한 알고리즘을 나타낸다.

[표 1]

밥 (Bob) 's 알고리즘
뷰어 페이지에서 입력한 OTP 키와 3-3-2에서 밥 (Bob)이 입력한 OTP 키의 일치 여부 확인
뷰어 페이지에서 입력한 OTP 코드와 OnACMS에서 생성한 OTP 코드의 일치 여부 확인
3 개의 난수 (random number)를 생성
3 개의 난수 (random number)와 OTP 키를 사용하여 대칭키 (symmetric key) 생성 (디피 헬만 키교환)
생성된 대칭키 (symmetric key)를 이용하여 3-3-2에서 앨리스 (Alice)가 입력한 메일제목, 메일내용을 AES 알고리즘으로 암호화하여 밥 (Bob)의 데이터베이스에 삽입 (insert)
앨리스 (Alice) 's 알고리즘으로 이동

표 2는 앨리스(Alice)의 대칭키(symmetric key)의 생성과 암호화(encryption)를 설명하기 위한 알고리즘을 나타낸다.

[0098] [표 2]

앨리스 (Alice) 's 알고리즘
3-3-2에서 앨리스 (Alice)가 입력하여 일반 텍스트 (plain text) 형태로 저장된 패스워드를 선택 (select)
패스워드를 숫자의 형태로 변환
3 개의 난수 (random number)를 생성
3 개의 난수 (random number)와 패스워드를 사용하여 대칭키 (symmetric key) 생성 (디피 헬만 키교환)
생성된 대칭키 (symmetric key)를 이용하여 3-3-2에서 앨리스 (Alice)가 입력한 메일제목, 메일내용을 AES 알고리즘으로 암호화하여 앨리스 (Alice)의 데이터베이스에 삽입 (insert)
3-3-2에서 앨리스 (Alice)가 입력한 일반 텍스트 (plain text) 형태의 데이터 제거

[0099]

[0100] 위의 표에서 OnACMS가 생성한 세 개의 난수(random number)는 각각 다음과 같은 용도로 사용될 수 있다.

[0101] 첫 번째 난수(random number)는 디피 헬만의 키교환 공식에서 a 로 사용될 수 있다.

[0102] 두 번째 난수(random number)는 디피 헬만의 키교환 공식에서 q 로 사용될 수 있다.

[0103] 그리고 세 번째 난수(random number)는 디피 헬만의 키교환 공식에서 OnACMS가 사용할 X_i 로 사용할 수 있다.

[0104] 여기서 중요한 것은 X_i 의 범위는 “ X_i chosen uniformly from the set of integers $\{1, 2, \dots, q-1\}$ ” 즉, OnACMS가 random수 q 를 생성한 다음 X_i 를 생성할 때 “1부터 $q-1$ 의 범위에 해당하는 난수(random number)로 생성해야만 한다.

[0105] OnACMS는 디피 헬만의 키교환 공식에 위의 난수(random number)를 대입하여 전달할 수(number)를 생성하고, 앨리스(Alice)의 패스워드와 밥(Bob)의 OTP 키로부터 생성한 숫자를 이용하여 AES 암호화에 이용될 대칭키 (symmetric key)를 생성할 수 있다. 여기에서, 디피 헬만의 키교환 공식은 $Y_i = a^{X_i} \bmod q$ 이 될 수 있다.

[0106] 이 부분을 간단한 수로 예를 들면,

[0107] OnACMS가 난수(random number)를 $a=3$, $q=5$, $X_i=4$ 로 생성했고,

[0108] 앨리스(Alice)의 패스워드를 숫자의 형태로 변환한 수가 2이며,

[0109] 밥(Bob)의 OTP 키를 숫자의 형태로 변환한 수가 3이라고 가정 할 때,

[0110] OnACMS가 전달할 수 Y_i 는 $3^4 \bmod 5$ 이므로 1이 된다.

[0111] 앨리스(Alice)가 전달할 수는 $3^2 \bmod 5$ 이므로 4가 된다.

- [0112] 밥(Bob)이 전달할 수는 $3^3 \bmod 5$ 이므로 2 가 된다.
- [0113] OnACMS와 앨리스(Alice)간의 키교환은 다음과 같이 이루어질 수 있다.
- [0114] 앨리스(Alice)가 전달한 수는 4 이고 OnACMS의 대칭키(symmetrix key)는 $4^4 \bmod 5$ 이므로 1이 된다.
- [0115] OnACMS가 전달한 수는 1 이고 앨리스(Alice)의 대칭키(symmetrix key)는 $1^2 \bmod 5$ 이므로 1이 된다.
- [0116] 따라서, OnACMS와 앨리스(Alice)간의 대칭키(symmetrix key)는 1이 된다.
- [0117] OnACMS와 밥(Bob)간의 키교환은 다음과 같이 이루어질 수 있다.
- [0118] 밥(Bob)이 전달한 수는 2 이고 OnACMS의 대칭키(symmetrix key)는 $2^4 \bmod 5$ 이므로 1이 된다.
- [0119] OnACMS가 전달한 수는 1 이고 밥(Bob)의 대칭키(symmetrix key)는 $1^3 \bmod 5$ 이므로 1이 된다.
- [0120] 따라서, OnACMS와 밥(Bob)간의 대칭키(symmetrix key)는 1이 된다.
- [0121] 이렇게 생성된 대칭키(symmetrix key)를 이용하여 메일 제목과 메일 메시지를 AES 암호화한 다음 각각 앨리스(Alice)와 밥(Bob)의 데이터베이스에 저장한 후, 3-3-2에서 저장한 일반 텍스트(plain text)를 제거할 수 있다.
- [0122] 키 생성을 위해 OnACMS가 생성한 난수(random number) a 와 q 와 X 는 별도의 데이터베이스에 저장하지만 앨리스(Alice)의 패스워드와 밥(Bob)의 OTP 키는 별도 저장하지 않는다.
- [0123] 만약, 앨리스(Alice)나 밥(Bob)이 추후에 해당 메시지의 열람을 시도할 경우 앨리스(Alice)가 패스워드를 모르거나 밥(Bob)이 자신의 OTP 키를 모르는 경우 메시지의 열람은 영원히 불가능하게 된다.
- [0124] 밥(Bob)이 다른 메일 서버를 이용하여 앨리스(Alice)에게 이메일을 전송할 때도 3-3-2와 마찬가지로 일반 텍스트(plain text) 형태로 저장해 두었다가 앨리스(Alice)가 메시지 열람을 시도할 때 3-3-3의 밥(Bob)과 같은 알고리즘을 앨리스(Alice)가 수행하여 메시지를 암호화하게 된다.
- [0125] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 컨트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPA(field programmable array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.
- [0126] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embodiment)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.
- [0127] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등

을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

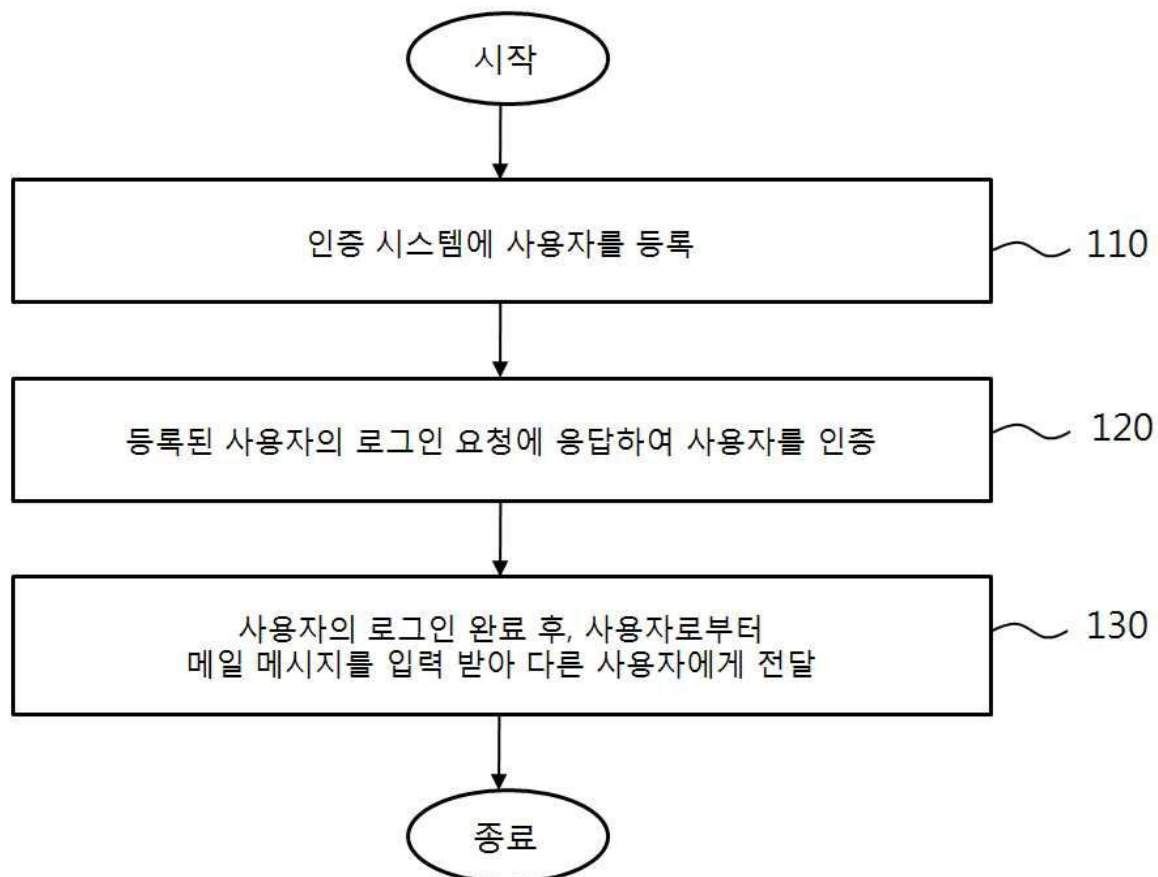
[0128] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0129] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

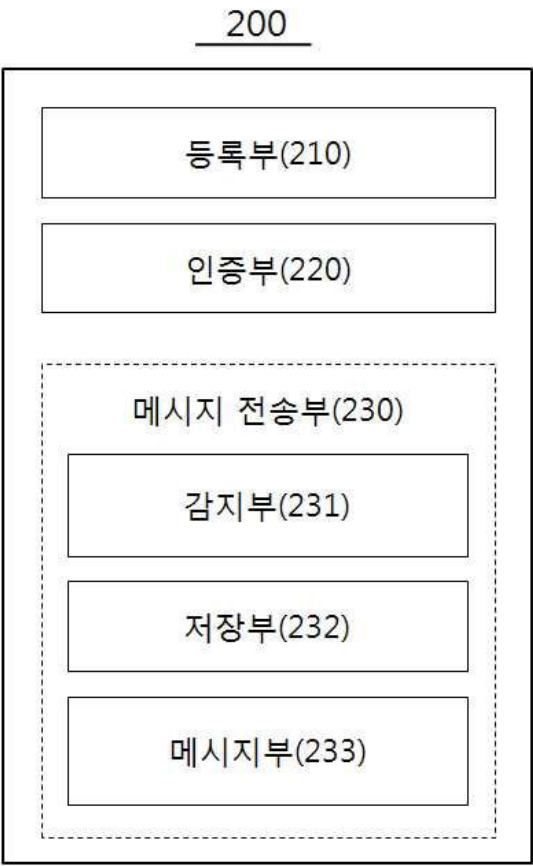
[0130]

도면

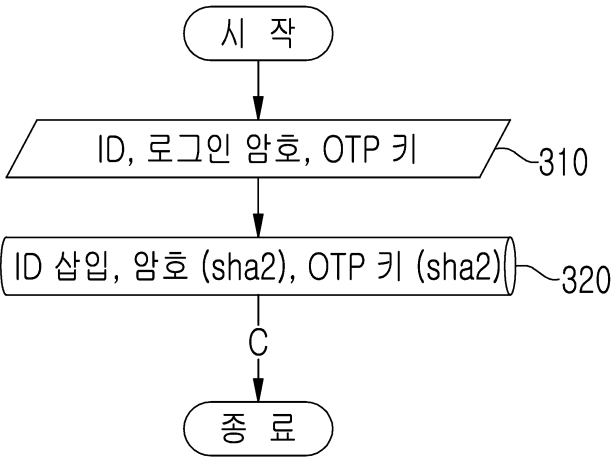
도면1



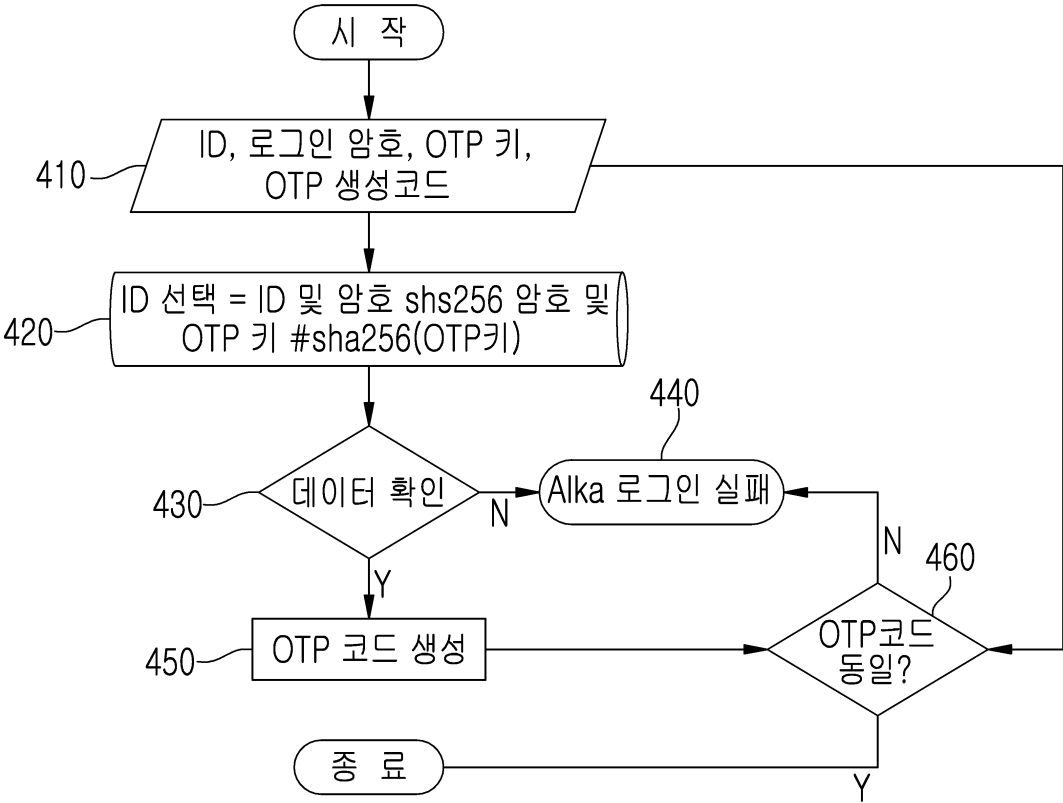
도면2



도면3



도면4



도면5

