(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년09월12일
(11) 등록번호 10-1777698
(24) 등록일자 2017년09월06일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 12/58* (2006.01)
H04L 9/06 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 9/0861 (2013.01)
H04L 51/08 (2013.01)
(21) 출원번호 10-2015-0149491
(22) 출원일자 2015년10월27일
심사청구일자 2015년10월27일
(65) 공개번호 10-2017-0048864
(43) 공개일자 2017년05월10일
(56) 선행기술조사문헌
JP2007053569 A*
JP2009026014 A*
KR1020150083650 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
라인 가부시키가이샤
일본국 도쿄도 신주쿠쿠 신주쿠 4-1-6
(72) 발명자
신기빈
경기도 성남시 분당구 황새울로360번길 42 AK플라자 11F
원종일
경기도 성남시 분당구 황새울로360번길 42 AK플라자 11F
(74) 대리인
리앤목특허법인

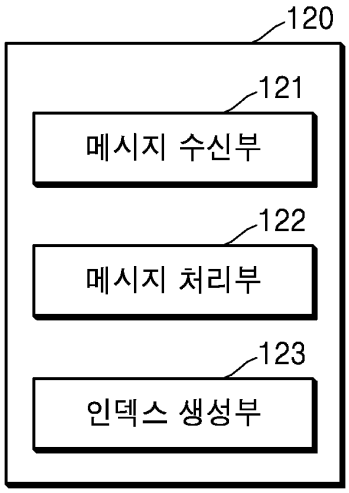
전체 청구항 수 : 총 14 항 심사관 : 윤태섭

(54) 발명의 명칭 **사용자 단말, 메시지를 송수신하는 방법 및 컴퓨터 프로그램**

(57) 요 약

본 실시예는 컴퓨터를 이용하여, 제1 첨부 파일을 포함하는 제1 메시지를 입력 받도록 제어하는 단계; 상기 제1 첨부 파일의 종류를 고려하여, 상기 제1 메시지를 암호화하는 암호화 키를 생성하는 단계; 상기 암호화 키를 이용하여 상기 제1 메시지의 제1 첨부 파일을 암호화하는 단계; 상기 제1 메시지에 상기 제1 메시지의 발신자 정보를 포함 시켜 메시지 서버로 전송하는 단계;를 포함하는 방법을 실행시키기 위하여 매체에 저장된 컴퓨터 프로그램을 개시한다.

대 표 도 - 도3



(52) CPC특허분류
H04L 9/0643 (2013.01)
H04L 9/3242 (2013.01)

명 세 서

청구범위

청구항 1

컴퓨터를 이용하여,

제1 첨부 파일을 포함하는 제1 메시지를 입력 받도록 제어하는 단계;

상기 제1 첨부 파일의 종류를 고려하여, 상기 제1 메시지를 암호화하는 암호화 키를 생성하는 단계;

상기 암호화 키를 이용하여 상기 제1 메시지의 제1 첨부 파일을 암호화하는 단계;

상기 제1 메시지에 상기 제1 메시지의 발신자 정보를 포함 시켜 메시지 서버로 전송하는 단계;를 포함하고,

복수의 사용자들에게 전송되도록 설정된 메시지의 경우,

상기 암호화 키를 생성하는 단계는

상기 메시지의 수신자 정보에 따라 상기 메시지의 암호화 키를 복수 개만큼 생성하고,

상기 암호화하는 단계는

상기 메시지를 수신자 별로 생성된 암호화 키를 이용하여 각각 암호화하는 점을 특징으로 하는, 방법을 실행시키기 위하여 매체에 저장된 컴퓨터 프로그램.

청구항 2

제1항에 있어서,

상기 암호화 키를 생성하는 단계는,

상기 제1 첨부 파일의 크기가 기 설정된 임계 값 이상인 경우, 상기 제1 첨부 파일의 해쉬값을 상기 제1 첨부 파일의 암호화 키로 생성하는, 방법을 실행시키기 위하여 매체에 저장된 컴퓨터 프로그램.

청구항 3

제1항에 있어서,

상기 암호화 키를 생성하는 단계는

상기 제1 첨부 파일의 종류가 동영상인 경우, 상기 제1 첨부 파일의 해쉬값을 상기 제1 첨부 파일의 암호화 키로 생성하는, 방법을 실행시키기 위하여 매체에 저장된 컴퓨터 프로그램.

청구항 4

삭제

청구항 5

제1항에 있어서,

상기 컴퓨터 프로그램은

상기 메시지 서버로부터 제2 사용자 단말기로부터의 제2 첨부 파일을 포함하는 제2 메시지를 수신하는 단계;

상기 제2 첨부 파일에 대한 인덱스를 추출하고, 상기 인덱스와 대응되는 데이터를 호출하는 단계;

상기 제2 사용자 단말기로부터 수신한 복호화 키를 이용하여, 상기 데이터를 복호화하는 단계;를 더 포함하는

방법을 실행시키기 위하여 매체에 저장된 컴퓨터 프로그램.

청구항 6

제5항에 있어서,

상기 컴퓨터 프로그램은

제3 사용자 단말기를 통해 상기 메시지를 확인할 수 있도록 상기 제3 사용자 단말기에 의해 출력된 인증 키를 입력 받도록 제어하는 단계;를 더 포함하는 방법을 실행시키기 위하여 매체에 저장된 컴퓨터 프로그램.

청구항 7

제6항에 있어서,

상기 인증 키를 입력 받도록 제어하는 단계는

상기 인증 키를 상기 메시지 서버로 전송하고,

상기 인증 키에 대한 응답으로, 상기 인증 키의 유효성을 수신하고, 상기 인증 키의 유효성에 따라 상기 제3 사용자 단말기로 상기 제1 메시지 및 상기 제2 메시지를 전송하도록 제어하는, 방법을 실행시키기 위하여 매체에 저장된 컴퓨터 프로그램.

청구항 8

제6항에 있어서,

상기 인증 키를 입력 받도록 제어하는 단계는

상기 인증 키를 이용하여 상기 암호화 키를 암호화하고, 상기 암호화된 암호화 키를 상기 제3 사용자 단말기로 전송하는, 방법을 실행시키기 위하여 매체에 저장된 컴퓨터 프로그램.

청구항 9

제어부, 통신부 및 메모리를 포함하는 사용자 단말에 있어서,

제1 첨부 파일을 포함하는 제1 메시지를 입력 받도록 제어하는 입력 제어부;

상기 제1 첨부 파일의 종류를 고려하여, 상기 제1 메시지를 암호화하는 암호화 키를 생성하는 키 생성부;

상기 암호화 키를 이용하여 상기 제1 메시지의 제1 첨부 파일을 암호화하는 암호화부;

상기 제1 메시지에 상기 제1 메시지의 발신자 정보를 포함 시켜 메시지 서버로 전송하는 메시지 전송부;를 포함하고,

복수의 사용자들에게 전송되도록 설정된 메시지의 경우,

상기 키 생성부는

상기 메시지의 수신자 정보에 따라 상기 메시지의 암호화 키를 복수 개만큼 생성하고,

상기 암호화부는

상기 메시지를 수신자 별로 생성된 암호화 키를 이용하여 각각 암호화하는 점을 특징으로 하는, 사용자 단말.

청구항 10

제9항에 있어서,

상기 키 생성부는

상기 제1 첨부 파일의 크기가 기 설정된 임계 값 이상인 경우, 상기 제1 첨부 파일의 해쉬값을 상기 제1 첨부 파일의 암호화 키로 생성하는, 사용자 단말.

청구항 11

제9항에 있어서,

상기 키 생성부는

상기 제1 첨부 파일의 종류가 동영상인 경우, 상기 제1 첨부 파일의 해쉬값을 상기 제1 첨부 파일의 암호화 키로 생성하는, 사용자 단말.

청구항 12

삭제

청구항 13

제9항에 있어서,

상기 메시지 서버로부터 제2 사용자 단말기로부터의 제2 첨부 파일을 포함하는 제2 메시지를 수신하는 메시지 수신부;

상기 제2 첨부 파일에 대한 인덱스를 추출하고, 상기 인덱스와 대응되는 데이터를 호출하는 데이터 호출부;

상기 제2 사용자 단말기로부터 수신한 복호화 키를 이용하여, 상기 데이터를 복호화하는 복호화부;를 포함하는, 사용자 단말.

청구항 14

제13항에 있어서,

제3 사용자 단말기를 통해 상기 메시지를 확인할 수 있도록 상기 제3 사용자 단말기에 의해 출력된 인증 키를 입력 받도록 제어하는 인증 관리부;를 더 포함하는, 사용자 단말.

청구항 15

제14항에 있어서,

상기 인증 관리부는

상기 인증 키를 상기 메시지 서버로 전송하고,

상기 인증 키에 대한 응답으로, 상기 인증 키의 유효성을 수신하고, 상기 인증 키의 유효성에 따라 상기 제3 사용자 단말기로 상기 제1 메시지 및 상기 제2 메시지를 전송하도록 제어하는, 사용자 단말.

청구항 16

제14항에 있어서,

상기 인증 관리부는

상기 인증 키를 이용하여 상기 암호화 키를 암호화하고, 상기 암호화된 암호화 키를 상기 제3 사용자 단말기로 전송하는, 사용자 단말.

발명의 설명

기 술 분 야

[0001] 본 발명은 사용자 단말, 메시지를 송수신하는 방법 및 컴퓨터 프로그램에 관한 것으로 보다 구체적으로는 메시지를 암호화하거나 복호화하는데 이용되는 키 정보를 메시지 서버와 공유하지 않도록 제어하는 사용자 단말, 방법 및 컴퓨터 프로그램에 관한 것이다.

배 경 기 술

[0002] 메신저를 통한 커뮤니케이션은 단말기, 서버, 단말기의 형태로 메시지의 수발신이 진행된다. 제1 사용자가 단말기에 탑재된 메시지 애플리케이션에 글을 입력하면, 해당 메신저 서비스 업체의 서버를 거쳐 제2 사용자의 단말기에 탑재된 메시지 애플리케이션으로 전달된다. 대부분의 메시지 애플리케이션은 스마트폰과 서버 사이에 암호화 장치를 적용해 주는데, 서버에 도착한 메시지는 서버에 의해 복호화 즉 암호가 풀리게 되는 것이 일반적이였다.

[0003] 종래의 방식에 따르면, 서버에 의해 복호화가 가능하게 되며, 이는 서버를 해킹하게 되면 사용자들 간의 메시지들이 공개될 수 있는 위험이 있음을 의미한다.

[0004] 이러한 종래 기술의 문제점을 해결하기 위해서, 사용자의 단말기들에서만 복호화되도록 하는 종단간 암호화(End to End Encryption) 기술을 적용하기 시작 했다.

[0005] 그러나, 종단간 암호화 기술을 적용하게 되는 경우, 수신자 또는 발신자에 따라서 동일한 메시지를 다르게 암호화 해야 하고, 서버는 사용자들 간의 메시지를 모두 개별적으로 관리해야 하는 문제점이 있었다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 실시예들은 암호화 키를 이용하여 제1 메시지를 암호화하여 발신자인 제2 사용자 단말기로 전송하고 제2 사용자 단말기로부터 수신한 제2 메시지를 상기 암호화 키와 짝을 이루는 복호화 키를 이용하여 복호화하는 사용자 단말기, 방법 및 컴퓨터 프로그램을 제공할 수 있다.

[0007] 또한, 본 발명의 실시예들은 사용자가 보유한 또 다른 단말기인 제3 사용자 단말기에 대한 인증을 수행하고, 인증이 완료되면 상기 제3 사용자 단말기와도 메시지를 공유하도록 제어하는 사용자 단말기, 방법 및 컴퓨터 프로그램을 제공할 수 있다.

[0008] 또한, 본 발명의 실시예들은 하나 이상의 사용자 단말기들 사이의 메시지를 송수신하도록 제어하는 메시지 서버에서는 해독할 수 없도록 암호화 또는 복호화된 정보를 메시지 서버와 공유하지 않는 사용자 단말, 방법 및 컴퓨터 프로그램을 제공할 수 있다.

과제의 해결 수단

[0009] 본 발명의 실시예들에 따른 기록 매체에 저장된 컴퓨터 프로그램은 컴퓨터를 이용하여,

[0010] 제1 첨부 파일을 포함하는 제1 메시지를 입력 받도록 제어하는 단계; 상기 제1 첨부 파일의 종류를 고려하여, 상기 제1 메시지를 암호화하는 암호화 키를 생성하는 단계; 상기 암호화 키를 이용하여 상기 제1 메시지의 제1 첨부 파일을 암호화하는 단계; 상기 제1 메시지에 상기 제1 메시지의 발신자 정보를 포함 시켜 메시지 서버로 전송하는 단계;를 포함하는 방법을 실행시킬 수 있다.

[0011] 상기 암호화 키를 생성하는 단계는, 상기 제1첨부 파일의 크기가 기 설정된 임계 값 이상인 경우, 상기 제1 첨부 파일의 해쉬값을 상기 제1 첨부 파일의 암호화 키로 생성하는, 방법을 실행시킬 수 있다.

[0012] 상기 암호화 키를 생성하는 단계는 상기 제1 첨부 파일의 종류가 동영상인 경우, 상기 제1 첨부 파일의 해쉬값

을 상기 제1 첨부 파일의 암호화 키로 생성하는, 방법을 실행시킬 수 있다.

[0013] 상기 암호화 키를 생성하는 단계는 복수의 사용자에게 전송되도록 설정된 메시지의 경우, 상기 메시지의 수신자 정보에 따라 상기 메시지의 암호화 키를 복수 개 생성하는, 방법을 실행시킬 수 있다.

[0014] 상기 컴퓨터 프로그램은 상기 메시지 서버로부터 제2 사용자 단말기로부터의 제2 첨부 파일을 포함하는 제2 메시지를 수신하는 단계; 상기 제2 첨부 파일에 대한 인덱스를 추출하고, 상기 인덱스와 대응되는 데이터를 호출하는 단계; 상기 제2 사용자 단말기로부터 수신한 복호화 키를 이용하여, 상기 데이터를 복호화하는 단계;를 더 포함하는 방법을 실행 시킬 수 있다.

[0015] 상기 컴퓨터 프로그램은 제3 사용자 단말기를 통해 상기 메시지를 확인할 수 있도록 상기 제3 사용자 단말기에 의해 출력된 인증 키를 입력 받도록 제어하는 단계;를 더 포함하는 방법을 실행시킬 수 있다.

[0016] 상기 인증 키를 입력 받도록 제어하는 단계는 상기 인증 키를 상기 메시지 서버로 전송하고, 상기 인증 키에 대한 응답으로, 상기 인증 키의 유효성을 수신하고, 상기 인증 키의 유효성에 따라 상기 제3 사용자 단말기로 상기 제1 메시지 및 상기 제2 메시지를 전송하도록 제어하는, 방법을 실행시킬 수 있다.

[0017] 상기 인증 키를 입력 받도록 제어하는 단계는 상기 인증 키를 이용하여 상기 암호화 키를 암호화하고, 상기 암호화된 암호화 키를 상기 제3 사용자 단말기로 전송하는, 방법을 실행시킬 수 있다.

[0018] 본 발명의 실시예들에 따른 사용자 단말은 제어부, 통신부 및 메모리를 포함하고, 제1 첨부 파일을 포함하는 제1 메시지를 입력 받도록 제어하는 입력 제어부; 상기 제1 첨부 파일의 종류를 고려하여, 상기 제1 메시지를 암호화하는 암호화 키를 생성하는 키 생성부; 상기 암호화 키를 이용하여 상기 제1 메시지의 제1 첨부 파일을 암호화하는 암호화부; 상기 제1 메시지에 상기 제1 메시지의 발신자 정보를 포함 시켜 메시지 서버로 전송하는 메시지 전송부;를 포함할 수 있다.

[0019] 상기 키 생성부는 상기 제1첨부 파일의 크기가 기 설정된 임계 값 이상인 경우, 상기 제1 첨부 파일의 해쉬값을 상기 제1 첨부 파일의 암호화 키로 생성할 수 있다.

[0020] 상기 키 생성부는 상기 제1 첨부 파일의 종류가 동영상인 경우, 상기 제1 첨부 파일의 해쉬값을 상기 제1 첨부 파일의 암호화 키로 생성할 수 있다.

[0021] 상기 키 생성부는 복수의 사용자에게 전송되도록 설정된 메시지의 경우, 상기 메시지의 수신자 정보에 따라 상기 메시지의 암호화 키를 복수 개 생성할 수 있다.

[0022] 본 발명의 실시예들에 따른 사용자 단말은 상기 메시지 서버로부터 제2 사용자 단말기로부터의 제2 첨부 파일을 포함하는 제2 메시지를 수신하는 메시지 수신부; 상기 제2 첨부 파일에 대한 인덱스를 추출하고, 상기 인덱스와 대응되는 데이터를 호출하는 데이터 호출부; 상기 제2 사용자 단말기로부터 수신한 상기 복호화 키를 이용하여, 상기 데이터를 복호화하는 복호화부;를 더 포함할 수 있다.

[0023] 본 실시예에 따르면, 사용자 단말은 제3 사용자 단말기를 통해 상기 메시지를 확인할 수 있도록 상기 제3 사용자 단말기에 의해 출력된 인증 키를 입력 받도록 제어하는 인증 관리부;를 더 포함할 수 있다.

[0024] 상기 인증 관리부는 상기 인증 키를 상기 메시지 서버로 전송하고, 상기 인증 키에 대한 응답으로, 상기 인증 키의 유효성을 수신하고, 상기 인증 키의 유효성에 따라 상기 제3 사용자 단말기로 상기 제1 메시지 및 상기 제2 메시지를 전송하도록 제어할 수 있다.

[0025] 상기 인증 관리부는 상기 인증 키를 이용하여 상기 암호화 키를 암호화하고, 상기 암호화된 암호화 키를 상기 제3 사용자 단말기로 전송할 수 있다.

[0026] 이 외에도, 본 발명을 구현하기 위한 다른 방법, 다른 시스템 및 상기 방법을 실행하기 위한 컴퓨터 프로그램을 기록하는 컴퓨터 판독 가능한 기록 매체가 더 제공된다.

[0027] 전술한 것 외의 다른 측면, 특징, 이점이 이하의 도면, 특허청구범위 및 발명의 상세한 설명으로부터 명확해 질 것이다.

발명의 효과

[0028] 본 발명은 암호화 키를 이용하여 제1 메시지를 암호화하여 발신자인 제2 사용자 단말기로 전송하고 제2 사용자 단말기로부터 수신한 제2 메시지를 상기 암호화 키와 짝을 이루는 복호화 키를 이용하여 복호화 할 수 있다.

[0029] 또한, 본 발명은 사용자가 보유한 또 다른 단말기인 제3 사용자 단말기에 대한 인증을 수행하고, 인증이 완료되면 상기 제3 사용자 단말기와도 메시지를 공유하도록 제어할 수 있다.

[0030] 또한, 본 발명은 하나 이상의 사용자 단말기들 사이의 메시지를 송수신하도록 제어하는 메시지 서버에서는 해독할 수 없도록 암호화 또는 복호화된 정보를 메시지 서버와 공유하지 않을 수 있다.

도면의 간단한 설명

[0031] 도 1은 본 발명의 실시예들에 따른 메시지 송수신 시스템을 나타내는 블록도이다.

도 2는 본 발명의 실시예들에 따른 메시지 서버의 구조를 나타내는 블록도이다.

도 3은 메시지 서버의 제어부(120)의 구조를 나타내는 블록도이다.

도 4는 본 발명의 실시예들에 따른 사용자 단말기의 구조를 나타내는 블록도이다.

도 5는 사용자 단말기의 제어부(250)의 구조를 나타내는 블록도이다.

도 6은 사용자 단말기의 인증 관리부(257)의 구조를 나타내는 블록도이다.

도 7 내지 도 8은 본 발명의 실시예들에 따른 메시지 송수신 방법을 나타내는 흐름도이다.

도 9 내지 도 10은 사용자 단말기들 및 메시지 서버 사이의 데이터 송수신을 나타내는 흐름도이다.

도 11 내지 도 14는 본 발명의 실시예들에 따라 제공되는 사용자 인터페이스의 일 예를 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0032] 본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시예를 가질 수 있는바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 본 발명의 효과 및 특징, 그리고 그것들을 달성하는 방법은 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 다양한 형태로 구현될 수 있다.

[0033] 이하, 첨부된 도면을 참조하여 본 발명의 실시예들을 상세히 설명하기로 하며, 도면을 참조하여 설명할 때 동일하거나 대응하는 구성 요소는 동일한 도면부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

[0034] 이하의 실시예에서, 제1, 제2 등의 용어는 한정적인 의미가 아니라 하나의 구성 요소를 다른 구성 요소와 구별하는 목적으로 사용되었다.

[0035] 이하의 실시예에서, 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는한, 복수의 표현을 포함한다.

[0036] 이하의 실시예에서, 포함하다 또는 가지다 등의 용어는 명세서 상에 기재된 특징, 또는 구성요소가 존재함을 의미하는 것이고, 하나 이상의 다른 특징을 또는 구성요소가 부가될 가능성을 미리 배제하는 것은 아니다.

[0037] 어떤 실시예가 달리 구현 가능한 경우에 특정한 공정 순서는 설명되는 순서와 다르게 수행될 수도 있다. 예를 들어, 연속하여 설명되는 두 공정이 실질적으로 동시에 수행될 수도 있고, 설명되는 순서와 반대의 순서로 진행될 수 있다.

[0038] 이하의 실시예에서, "회로"는, 예를 들어, 프로그램가능한 회로에 의해 실행되는 인스트럭션을 저장하는 하드와이어드 회로, 프로그램가능한 회로, 상태 머신 회로, 및/또는 펌웨어를 단독으로 또는 임의의 조합으로 포함할 수 있다. 애플리케이션은 호스트 프로세서 또는 다른 프로그램가능한 회로와 같은 프로그램가능한 회로 상에서 실행될 수 있는 코드 또는 인스트럭션으로서 구현될 수 있다. 본원의 임의의 실시예에서 사용되는 바와 같은, 모듈은,회로로서 구현될 수 있다. 회로는 집적 회로 칩과 같은 집적 회로로서 구현될 수 있다.

[0039] 이하의 실시예에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "…부", "…기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0040] 도 1은 본 발명의 실시예에 따른 메시지 송수신 시스템(10)을 나타내는 도면이다.

[0041] 도 1을 참조하면, 본 발명의 실시예에 따른 메시지 송수신 시스템(10)은 메시지 서버(100), 사용자 단말기(200,

300), 통신망(400)을 포함할 수 있다.

[0042] 메시지 서버(100)는 사용자 단말기(200, 300)로부터 수신된 메시지를 다른 사용자 단말기(200, 300)로 전송함으로써, 복수의 사용자 단말기 사이의 메시지를 송수신하는 기능을 수행한다. 메시지 서버(100)는 회원 가입, 로그인 등의 절차를 거친 복수의 사용자 단말기(200, 300)들 사이의 메시지를 수발신하는 기능을 제공할 수 있다. 메시지 서버(100)는 복수의 사용자 단말기(200, 300)들 사이의 대화를 가능하게 하는 대화방을 제공하는 기능을 제공할 수 있다. 메시지 서버(100)는 대화방에 입장한 각 사용자에 의해 입력된 또는 수신된 대화가 대화방을 통해, 대화방에 있는 복수의 사용자들과 공유될 수 있도록 제어할 수 있다.

[0043] 메시지 서버(100)는 회원 가입, 로그인 등의 절차를 거치지 않은 사용자 단말기(200, 300)에게 대화방 초대 메시지를 전송할 수도 있다.

[0044] 메시지 서버(100)는 사용자 단말기(200, 300)들 사이의 메시지 또는 대화(chatting, talk)를 암호 또는 복호할 수 있도록 제어할 수 있다. 특히, 메시지 서버(100)는 종단 간 암호화 기술을 활용하여 메시지를 수발신하거나 대화방의 대화를 처리하는 기능을 제공할 수 있다. 좀더 구체적으로, 메시지 서버(100)는 암호화된 메시지를 각 발신자의 사용자 단말기로 그대로 전달할 뿐이고, 각 암호화된 메시지를 해독 또는 복호화와 관련된 정보를 저장 관리하지 않는다.

[0045] 또한, 메시지 서버(100)는 제1 사용자 단말기(201)로 전송되도록 설정된 메시지를 제1 사용자 단말기와 연계된 제2 사용자 단말기(202)로 전송하도록 제어할 수 있다. 메시지 서버(100)는 제1 사용자 단말기(201) 및 제2 사용자 단말기(202) 사이의 동일성을 확인하기 위해서 인증 과정을 수행하도록 제어할 수 있다. 또한, 메시지 서버(100)는 제1 사용자 단말기(201)가 메시지를 송수신하는데 이용하는 암호 키를 제1 사용자 단말기(201)와 연결된 제2 사용자 단말기(202)로 전송하도록 제어할 수 있다. 이때, 암호 키는 제1 사용자 단말기(201) 및 제2 사용자 단말기(202) 사이를 인증하는데 이용된 인증 키를 이용하여 암호화된 상태로 송수신될 수 있다.

[0046] 또한, 메시지 서버(100)는 메시지 송수신을 할 수 있도록 구현된 애플리케이션을 사용자 단말기(200, 300)로 배포하는 기능을 수행할 수 있다.

[0047] 사용자는 사용자 단말기(200, 300)를 통해, 메시지 서버(100)에 접속할 수 있다. 사용자 단말기(200, 300)는 메시지 송수신에 대한 애플리케이션(또는 컴퓨터 프로그램)을 탑재하고, 상기 애플리케이션을 이용하여, 다른 사용자 단말기(200, 300)로 메시지를 전송하게 되고, 다른 사용자 단말기(200, 300)로부터 메시지를 수신하게 된다.

[0048] 또한, 사용자 단말기(200, 300)는 공개하고 싶지 않은 메시지를 암호화하여 전송할 수 있으며, 암호화 관련 정보를 메시지 서버(100)와 공유하지 않게 된다.

[0049] 복수 개의 사용자 단말기(200, 300)들은 유무선 통신 환경에서 웹 서비스를 이용할 수 있는 통신 단말기를 의미한다. 여기서, 사용자 단말기(200, 300)는 사용자의 퍼스널 컴퓨터(201, 301)일 수도 있고, 또는 사용자의 휴대용 단말(202)일 수도 있다. 도 1에서는 휴대용 단말기(202, 302)가 스마트폰으로 도시되었지만, 본 발명의 사상은 이에 제한되지 아니하며, 상술한 바와 같이 웹 브라우징이 가능한 애플리케이션을 탑재한 단말은 제한 없이 차용될 수 있다.

[0050] 이를 더욱 상세히 설명하면, 사용자 단말기(200)는 컴퓨터(예를 들면, 데스크톱, 랩톱, 태블릿 등), 미디어 컴퓨팅 플랫폼(예를 들면, 케이블, 위성 셋톱박스, 디지털 비디오 레코더), 핸드헬드 컴퓨팅 디바이스(예를 들면, PDA, 이메일 클라이언트 등), 핸드폰의 임의의 형태, 또는 다른 종류의 컴퓨팅 또는 커뮤니케이션 플랫폼의 임의의 형태를 포함할 수 있으나, 본 발명이 이에 한정되는 것은 아니다.

[0051] 한편, 통신망(400)은 복수 개의 사용자 단말기(200, 300)들과 메시지 서버(100)를 연결하는 역할을 수행한다. 즉, 통신망(400)은 사용자 단말기(200, 300)들이 메시지 서버(100)에 접속한 후 데이터를 송수신할 수 있도록 접속 경로를 제공하는 통신망을 의미한다. 통신망(400)은 예컨대 LANs(Local Area Networks), WANs(Wide Area Networks), MANs(Metropolitan Area Networks), ISDNs(Integrated Service Digital Networks) 등의 유선 네트워크나, 무선 LANs, CDMA, 블루투스, 위성 통신 등의 무선 네트워크를 망라할 수 있으나, 본 발명의 범위가 이에 한정되는 것은 아니다.

[0052] 도 2는 본 발명의 실시예들에 따른 메시지 서버의 구조를 나타내는 블록도이다.

[0053] 도 2를 참조하면, 본 발명의 실시예들에 따른 메시지 서버(100)는 통신부(110), 제어부(120), 데이터베이스

(130)를 포함할 수 있다.

[0054] 통신부(110)는 메시지 서버(100)와 적어도 하나의 사용자 단말기(200, 300) 간의 통신을 가능하게 하는 하나 이상의 구성요소를 포함할 수 있다.

[0055] 여기서, 통신부(110)는 다른 네트워크 장치와 유무선 연결을 통해 제어 신호 또는 데이터 신호와 같은 신호를 송수신하기 위해 필요한 하드웨어 및 소프트웨어를 포함하는 장치일 수 있다.

[0056] 제어부(120)는, 통상적으로 메시지 서버(100)의 전반적인 동작을 제어한다. 예를 들어, 제어부(120)는, 데이터베이스(130)에 저장된 프로그램들을 실행함으로써, 통신부(110), 데이터베이스(130) 등을 전반적으로 제어할 수 있다.

[0057] 여기서, 제어부(120)는 프로세서(processor)와 같이 데이터를 처리할 수 있는 모든 종류의 장치를 포함할 수 있다. 여기서, '프로세서(processor)'는, 예를 들어 프로그램 내에 포함된 코드 또는 명령으로 표현된 기능을 수행하기 위해 물리적으로 구조화된 회로를 갖는, 하드웨어에 내장된 데이터 처리 장치를 의미할 수 있다. 이와 같이 하드웨어에 내장된 데이터 처리 장치의 일 예로써, 마이크로프로세서(microprocessor), 중앙처리장치(central processing unit: CPU), 프로세서 코어(processor core), 멀티프로세서(multiprocessor), ASIC(application-specific integrated circuit), FPGA(field programmable gate array) 등의 처리 장치를 망라할 수 있으나, 본 발명의 범위가 이에 한정되는 것은 아니다.

[0058] 데이터베이스(130)는, 제어부(120)의 처리 및 제어를 위한 프로그램을 저장할 수도 있고, 입/출력되는 데이터들(예컨대, 복수의 메뉴, 복수의 메뉴 각각에 대응하는 복수의 제 1 계층 서브 메뉴, 복수의 제 1 계층 서브 메뉴 각각에 대응하는 복수의 제 2 계층 서브 메뉴 등)을 저장할 수도 있다.

[0059] 데이터베이스(130)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(RAM, Random Access Memory) SRAM(Static Random Access Memory), 롬(ROM, Read-Only Memory), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다. 또한, 지식 공유 서비스 제공 장치(100)는 인터넷(internet)상에서 데이터베이스(130)의 저장 기능을 수행하는 웹 스토리지(web storage) 또는 클라우드 서버를 운영할 수도 있다.

[0060] 데이터베이스(130)에 저장된 프로그램들은 그 기능에 따라 복수 개의 모듈들로 분류할 수 있는데, 예를 들어, UI 모듈, 터치 스크린 모듈, 알림 모듈 등으로 분류될 수 있다.

[0061] 메시지 서버(100)는 단문 메시지, 인스턴트 메시지, 이메일 등의 메시지를 사용자 단말기(200, 300)로 전송하는 기능을 수행할 수 있다. 메시지 서버(100)가 송수신하는 메시지의 종류는 다양하며, 하나의 종류에 한정되지 않는다.

[0062] 도 3은 메시지 서버(100)의 제어부(120)의 구조를 나타내는 블록도이다.

[0063] 도 3을 참조하면, 메시지 서버(100)의 제어부(120)는 메시지 수신부(121), 메시지 처리부(122), 인덱스 생성부(123)를 포함할 수 있다.

[0064] 메시지 수신부(121)는 사용자 단말기(200, 300)로부터 메시지를 수신하도록 제어한다. 여기서, 메시지는 메시지의 제목, 내용, 발신자 정보, 수신자 정보, 첨부 파일을 포함할 수 있다. 상기 메시지의 발신자 및 수신자 관련 정보는 사용자의 아이디 정보, 이메일 주소, 전화 번호 등을 포함할 수 있다. 첨부 파일은 이미지, 동영상, 음성 파일, 링크 정보 등을 포함할 수 있다. 메시지 서버(100)는 소정의 회원가입 과정을 거쳐 회원으로 등록된 사용자의 사용자 단말기(200, 300) 사이의 메시지를 송수신하도록 제어할 수 있다.

[0065] 메시지 처리부(122)는 사용자 단말기(200, 300)로부터 수신한 하나 이상의 메시지를 각 메시지의 발신자의 사용자 단말기(200, 300)로 전송하도록 제어할 수 있다. 이때, 첨부 파일을 포함하고 있는 메시지의 경우, 메시지 처리부(122)는 첨부 파일을 전송하지 않고, 첨부 파일의 인덱스 만을 사용자 단말기(200, 300)로 전송할 수 있다. 특히, 하나의 첨부 파일이 많은 사용자에 의해 전송 또는 공유되는 경우, 메시지 처리부(122)는 전송되거나 공유되는 수만큼 첨부 파일 또는 첨부 파일의 인덱스를 저장 관리 하지 않고, 하나의 인덱스로 첨부 파일이 전송 또는 공유되도록 처리할 수 있다. 예를 들어, 사람들에게 인기가 있는 동영상의 경우, 동일한 동영상을 매우 많은 사용자 사이에 주고 받는 이벤트가 발생하게 되는데 이런 경우, 메시지 서버(100)가 사용자에 의해 생성된 이벤트(메시지 송수신 등)마다 동영상 또는 동영상과 대응되는 인덱스를 생성하는 것은 리소스를 매우 낭비할

수 있다. 이런 경우, 메시지 처리부(122)는 수신된 메시지의 첨부 파일이 기존에 전송된 이력(history)이 있는지를 판단하여 첨부 파일에 대한 메타 데이터를 새롭게 생성할지 여부를 판단할 수 있다.

[0066] 또한, 메시지 처리부(122)는 메시지의 수신자 정보에 따라 메시지를 수신하는 다른 서버로 전송하거나, 직접 사용자 단말기(200, 300)로 메시지를 전송할 수 있다.

[0067] 인덱스 생성부(123)는 메시지가 첨부 파일을 포함하고 있는 경우, 첨부 파일을 식별할 수 있는 인덱스를 생성하고, 상기 인덱스와 상기 첨부 파일이 서로 대응될 수 있도록 테이블을 생성할 수 있다. 인덱스 생성부(123)는 첨부 파일 또는 메시지와 대응되는 인덱스를 각각 생성할 수도 있다.

[0068] 도 4는 본 발명의 실시예들에 따른 사용자 단말기(200, 300)의 구조를 나타내는 블록도이다.

[0069] 도 4를 참조하면, 본 발명의 일 실시예에 따른 사용자 단말기(200, 300)는, 크게 통신부(210), 제어부(250) 및 메모리(260)를 포함하며, 선택적으로 출력부(230), 사용자 입력부(240)를 더 포함할 수 있다.

[0070] 통신부(210)는 사용자 단말기(200, 300) 간의 통신 또는 사용자 단말기(200, 300)와 메시지 서버(100) 간의 통신을 가능하게 하는 하나 이상의 구성요소를 포함할 수 있다. 예를 들어, 통신부(210)는, 근거리 통신부(211), 이동 통신부(212)를 포함할 수 있다.

[0071] 근거리 통신부(short-range wireless communication unit)(211)는, 블루투스 통신부, BLE(Bluetooth Low Energy) 통신부, 근거리 무선 통신부(Near Field Communication unit), WLAN(와이파이) 통신부, 지그비(Zigbee) 통신부, 적외선(IrDA, infrared Data Association) 통신부, WFD(Wi-Fi Direct) 통신부, UWB(ultra wideband) 통신부, Ant+ 통신부 등을 포함할 수 있으나, 이에 한정되는 것은 아니다.

[0072] 이동 통신부(212)는, 이동 통신망 상에서 기지국, 외부의 단말, 서버 중 적어도 하나와 무선 신호를 송수신한다. 여기에서, 무선 신호는, 음성 호 신호, 화상 통화 호 신호 또는 문자/멀티미디어 메시지 송수신에 따른 다양한 형태의 데이터를 포함할 수 있다.

[0073] 통신부(210)는, 메시지 서버(100) 또는 다른 사용자 단말기(200, 300)로부터의 메시지를 획득한다.

[0074] 출력부(230)에는, 디스플레이부(231)와 음향 출력부(232), 진동 모터(233) 등이 포함될 수 있다.

[0075] 디스플레이부(231)는 사용자 단말기(200, 300)에서 처리되는 정보를 출력한다. 예를 들어, 디스플레이부(231)는, 메시지 송수신 애플리케이션 실행 시 제공되는 사용자 인터페이스를 출력할 수 있다. 디스플레이부(231)는 탑재된 메시지 송수신 애플리케이션에 따라 메시지 생성 또는 메시지 수신과 관련된 사용자 인터페이스를 표시할 수 있다. 디스플레이부(231)는 탑재된 메시지 송수신 애플리케이션의 버전에 따라 변경된 사용자 인터페이스를 표시할 수 있다. 디스플레이부(231)는 수신된 메시지가 암호화된 메시지인 경우, 사용자 인증 등의 과정이 필요하다는 화면을 표시할 수 있다. 디스플레이부(231)는 사용자로부터 입력된 사용자 입력에 따라 사용자 인터페이스를 변경하여 제공할 수 있다.

[0076] 한편, 디스플레이부(231)와 터치패드가 레이어 구조를 이루어 터치 스크린으로 구성되는 경우, 디스플레이부(231)는 출력 장치 이외에 입력 장치로도 사용될 수 있다. 디스플레이부(231)는 액정 디스플레이(liquid crystal display), 박막 트랜지스터 액정 디스플레이(thin film transistor-liquid crystal display), 유기 발광 다이오드(organic light-emitting diode), 플렉시블 디스플레이(flexible display), 3차원 디스플레이(3D display), 전기영동 디스플레이(electrophoretic display) 중에서 적어도 하나를 포함할 수 있다. 그리고 디바이스(100)의 구현 형태에 따라 디바이스(100)는 디스플레이부(231)를 2개 이상 포함할 수도 있다. 이때, 2개 이상의 디스플레이부(231)는 힌지(hinge)를 이용하여 마주보게 배치될 수 있다.

[0077] 음향 출력부(232)는 통신부(220)로부터 수신되거나 메모리(270)에 저장된 오디오 데이터를 출력한다. 또한, 음향 출력부(232)는 사용자 단말기(200, 300)에서 수행되는 기능(예를 들어, 메시지 애플리케이션 실행시 출력되는 배경음, 메시지 애플리케이션에서 동작을 수행할 때마다 발생되는 효과음)과 관련된 음향 신호를 출력한다. 이러한 음향 출력부(232)에는 스피커(speaker), 버저(Buzzer) 등이 포함될 수 있다.

[0078] 진동 모터(233)는 진동 신호를 출력할 수 있다. 예를 들어, 진동 모터(233)는 오디오 데이터 또는 이미지 데이터(예컨대, 게임 애플리케이션에서 동작을 수행할 때마다 발생되는 효과음, 게임 애플리케이션에서 동작을 수행한 결과 변경되는 이미지)의 출력에 대응하는 진동 신호를 출력할 수 있다. 또한, 진동 모터(233)는 터치스크린에 터치가 입력되는 경우 진동 신호를 출력할 수도 있다.

[0079] 제어부(250)는, 통상적으로 사용자 단말기(200, 300)의 전반적인 동작을 제어한다. 예를 들어, 제어부(250)는,

메모리(270)에 저장된 프로그램들을 실행함으로써, 센싱부(210), 통신부(220), 출력부(230), 사용자 입력부(240), A/V 입력부(260), 메모리(270) 등을 전반적으로 제어할 수 있다.

[0080] 제어부(250)는 메모리(270)에 미리 저장된 메시지 송수신 애플리케이션에 관한 메타데이터를 이용하여, 사용자 입력 및 사용자 단말기(200, 300)의 상태 정보에 대응되는 동작을 결정할 수 있다.

[0081] 사용자 입력부(240)는, 사용자가 사용자 단말기(200, 300)를 제어하기 위한 데이터를 입력하는 수단을 의미한다. 예를 들어, 사용자 입력부(240)에는 키 패드(key pad), 돔 스위치 (dome switch), 터치 패드(접촉식 정전 용량 방식, 압력식 저항막 방식, 적외선 감지 방식, 표면 초음파 전도 방식, 적분식 장력 측정 방식, 피에조 효과 방식 등), 조그 휠, 조그 스위치 등이 있을 수 있으나 이에 한정되는 것은 아니다.

[0082] 메모리(260)는, 제어부(250)의 처리 및 제어를 위한 프로그램을 저장할 수도 있고, 입/출력되는 데이터들(예컨대, 복수의 메뉴, 복수의 메뉴 각각에 대응하는 복수의 제 1 계층 서브 메뉴, 복수의 제 1 계층 서브 메뉴 각각에 대응하는 복수의 제 2 계층 서브 메뉴 등)을 저장할 수도 있다.

[0083] 메모리(260)는 메시지 송수신 애플리케이션에 관한 메타데이터를 미리 저장할 수 있다.

[0084] 메모리(260)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(RAM, Random Access Memory) SRAM(Static Random Access Memory), 롬(ROM, Read-Only Memory), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다. 또한, 사용자 단말기(200, 300)는 인터넷(internet)상에서 메모리(260)의 저장 기능을 수행하는 웹 스토리지(web storage) 또는 클라우드 서버를 운영할 수도 있다.

[0085] 도 5는 사용자 단말기(200, 300)의 제어부(250)의 구조를 나타내는 블록도이다.

[0086] 도 5를 참조하면, 사용자 단말기(200, 300)의 제어부(250)는 입력 제어부(251), 메시지 수신부(252), 메시지 전송부(253), 데이터 호출부(254), 암호화부(255), 복호화부(256), 키 생성부(257), 인증 관리부(258)를 포함할 수 있다. 먼저, 메시지 전송과 관련된 실시예들을 중심으로 사용자 단말기(200, 300)의 구조를 설명하겠다.

[0087] 입력 제어부(251)는 제1 메시지를 입력하도록 제어한다. 입력 제어부(251)는 사용자 입력부(240)에 의해 입력된 입력 신호에 따라 제1 메시지가 생성될 수 있도록 제어한다. 입력 제어부(251)는 사용자에 의해 입력된 입력 신호와 대응하여, 제1 메시지의 제목, 내용, 발신자 정보, 수신자 정보, 첨부 파일 등을 포함하는 제1 메시지를 생성할 수 있다.

[0088] 메시지 전송부(253)는 제1 메시지를 제1 메시지의 수신자의 제2 사용자 단말기(200, 300)로 전송하도록 제어한다. 메시지 전송부(253)는 제1 메시지와 관련된 프로토콜에 따라 제1 메시지의 포맷을 변경하는 기능을 수행할 수 있다. 예를 들어, 제1 메시지가 TCP/IP, 또는 NFC 등의 통신망을 통해 송수신 되는 경우, 메시지 전송부(253)는 각 통신 규약에 맞게 제1 메시지의 구조를 변경할 수 있다. 또한, 사용자의 설정에 따라, 메시지 전송부(253)는 제1 메시지의 각 파라미터를 암호화하는 과정을 더 수행하도록 제어할 수 있다. 즉, 사용자의 보안 관련 설정에 따라, 메시지 전송부(253)는 메시지를 암호화하거나 메시지를 그대로 전송할 수 있다.

[0089] 키 생성부(257)는 제1 메시지를 암호화하는 암호화 키를 생성할 수 있다. 키 생성부(257)는 제1 메시지를 암호화하는 암호화 키(private key) 및 상기 암호화 키와 대응되는 복호화 키(public key)를 생성할 수 있다. 여기서, 암호화 키 및 복호화 키의 관계는 대칭키 또는 비대칭키 중 하나 일 수 있다.

[0090] 키 생성부(257)는 메시지의 내용 및 첨부 파일을 암호화하는 키를 각각 생성할 수 있다. 먼저 첨부 파일의 암호화 키를 생성하는 과정을 설명하면, 키 생성부(257)는 메시지의 첨부 파일의 크기를 고려하여, 메시지의 첨부 파일의 암호화 키를 생성할 수 있다. 예를 들어, 메시지의 첨부 파일의 용량이 미리 설정된 임계 크기 보다 작은 경우, 키 생성부(257)는 첨부 파일과 관련 없이 랜덤한 값을 첨부 파일의 암호화 키로 생성할 수 있다.

[0091] 메시지의 첨부 파일의 용량이 상기 임계 크기 보다 큰 경우, 키 생성부(257)는 첨부 파일의 해쉬값을 첨부 파일의 암호화 키로 생성할 수 있다. 랜덤한 값을 첨부 파일의 암호화 키로 생성하는 경우, 사용자 단말기(200, 300)를 통해 메시지 수발신을 제공하는 메시지 서버(100)는 동일한 내용의 첨부 파일을 서로 다른 내용으로 암호화되고, 각 첨부 파일을 관리하기 위한 리소스를 많이 필요로 한다. 그에 반해, 해쉬 값을 첨부 파일의 암호

화 키로 생성하는 경우, 본 발명의 실시예들에 따른 사용자 단말기(200, 300)을 통해 메시지 수발신 하도록 제어하는 메시지 서버(100)는 동일한 파일에 대해서는 하나의 원본 만을 관리하면 된다.

[0092] 키 생성부(257)는 메시지의 첨부 파일의 종류를 고려하여, 메시지의 첨부 파일의 암호화 키를 생성할 수 있다. 예를 들어, 메시지의 첨부 파일이 동영상인 경우, 키 생성부(257)는 첨부 파일의 해쉬값을 첨부 파일의 암호화 키로 생성할 수 있다. 메시지의 첨부 파일이 음성 파일 또는 이미지인 경우, 키 생성부(257)는 첨부 파일과 관련 없이 랜덤한 값을 첨부 파일의 암호화 키로 생성할 수 있다.

[0093] 선택적 실시예에서, 키 생성부(257)는 메시지의 수신자의 수 또는 공유되는 수를 고려하여, 메시지의 첨부 파일의 암호화 키를 생성할 수 있다. 예를 들어, 하나의 메시지가 많은 사용자들에게 전송되도록 입력되는 경우, 즉, 메시지의 수신자의 수가 소정의 임계 수량 이상인 경우, 키 생성부(257)는 메시지의 수신자 정보에 따라 각각 첨부 파일을 암호화하는 키를 생성하기 보다는 첨부 파일의 해쉬값을 메시지의 수신자들을 위한 첨부 파일의 암호화 키로 생성할 수 있다. 또한, 하나의 메시지가 많은 사용자들에 의해 또 다른 사용자들에게 공유되도록 입력되는 경우, 메시지가 공유되는 수가 소정의 임계 수량 이상인 경우, 키 생성부(257)는 메시지의 발신자 또는 수신자와 무관하게, 첨부 파일의 해쉬값을 첨부 파일의 암호화 키로 생성할 수 있다. 다음으로 메시지의 내용을 암호화하는 암호화 키를 생성하는 과정을 설명하면, 키 생성부(257)는 메시지의 내용을 암호화하는 암호화 키를 랜덤하게 생성할 수 있다. 이때, 암호화 키는 수신자 정보, 발신자 정보, 발신 시간, 발신 날짜 등을 고려하여 랜덤하게 생성될 수 있다.

[0094] 다른 실시예에서, 키 생성부(257)는 복수의 수신자들의 사용자 단말기(200, 300)로 전송하도록 생성된 제1 메시지의 경우, 각 수신자 별로 다른 암호화 키를 생성할 수 있다. 제2 사용자 단말기(301) 및 제3 사용자 단말기(302)로 전송되어야 하는 제1 메시지의 경우, 키 생성부(257)는 제2 사용자 단말기(301)로 전송되는데 이용되는 제1 암호화 키 및 제3 사용자 단말기(302)로 전송되는데 이용되는 제2 암호화 키를 각각 생성할 수 있다.

[0095] 여기서, 해쉬 값에 대해서 좀더 구체적으로 설명하면, 파일의 해쉬 값은 파일의 데이터를 해쉬 함수(hash function) 또는 해쉬 알고리즘(hash algorithm)을 통해 계산하여 산출된 값으로, 해당 파일의 고유한 값이다. 해쉬 값은 파일의 고유한 값이기 때문에 서로 다른 두 파일의 해쉬 값이 같다는 것은 두 파일이 거의 일치하는 동일한 파일임을 의미한다. 해쉬 함수의 종류로는 CRC32, md5, SHA-1, RIPEMD-128, Tiger 등이 있다.

[0096] 암호화 방법에 대해서 좀더 구체적으로 설명하면, 본 발명의 실시예들에 따른 사용자 단말기(200, 300)는 메시지를 송수신하는데 송신자 및 수신자 이외의 제3자에 의해 해독되는 것을 방지 하기 위해서, 비대칭키를 활용한 암호화 방법을 이용할 수 있다. 즉, 본 발명의 실시예들에 따른 사용자 단말기(200, 300)는 메시지를 전송하는 제1 사용자 단말기(200) 또는 메시지를 수신하는 제2 사용자 단말기(300)에 의해 메시지를 암호화하는 개인 키 또는 메시지를 복호화하는 공개 키를 생성할 수 있다. 제1 개인 키로 암호화된 메시지는 제1 개인 키와 대응되는 제1 공개 키를 이용하여 복호화되고, 제1 공개 키로 암호화된 메시지는 제1 개인 키를 이용하여 복호화될 수도 있다. 즉, 개인 키 및 상기 개인 키와 대응되는 공개 키는 서로 대응되는 관계를 가지며, 복호화 또는 암호화의 기능을 각각 수행하게 된다. 대칭 키 암호 알고리즘(symmetric cryptography)의 경우, 암호화하거나 복호하는데 있어서 동일한 암호 키(개인 키)를 사용하는데 반해서, 비 대칭 키 암호 알고리즘(asymmetric cryptography)은 암호화의 개인 키 및 복호화의 공개 키가 서로 열쇠(key) 및 자물쇠(lock)의 관계 있으면서, 개인 키로부터 공개 키를 해독할 수 없는 장점이 있다. 대칭 키 암호 알고리즘의 예로는 DES, 2중 DES, 3중 DES, AES, IDEA, SEED, Blowfish, ARIA 등이 있을 수 있으며, 비 대칭 키 암호 알고리즘의 예로는 RSA, DSA, ECC, EIGamal, Rabin 등이 있을 수 있다. 또한, 본 발명의 실시예들에 따른 사용자 단말기(200, 300)는 메시지를 대칭키 알고리즘을 이용하여 암호화할 수 있다.

[0097] 암호화부(255)는 키 생성부(257)에 의해 생성된 암호화 키들을 이용하여 제1 메시지의 내용 및 첨부 파일을 각각 암호화하는 기능을 수행한다. 암호화부(255)는 하나 이상의 암호화 키를 이용하여, 제1 메시지의 내용 및 첨부 파일을 암호화할 수 있다. 암호화부(255)는 복수의 수신인에게 전송되도록 설정된 제1 메시지를 수신인 별로 생성된 암호화 키를 이용하여 각각 암호화할 수 있다.

[0098] 본 발명의 실시예들에 따른 사용자 단말기(200, 300)는 메시지의 내용이 공개되지 않도록 하기 위해서, 메시지의 내용을 랜덤하게 생성된 암호화 키를 이용하여 암호화하여 전송하도록 제어할 수 있고, 메시지의 첨부 파일의 종류 또는 크기를 고려하여 생성된 암호화 키를 이용하여 암호화하여 전송하도록 제어할 수 있다.

[0099] 다음으로, 메시지 수신과 관련된 실시예들을 중심으로 사용자 단말기(200, 300)의 구조를 설명하겠다.

[0100] 메시지 수신부(252)는 메시지 서버(100)로부터 제2 사용자 단말기(200, 300)로부터의 제2 메시지 또는 제2 메시

지와 대응되는 인덱스를 수신하도록 제어한다. 메시지 수신부(252)는 제2 메시지 또는 제2 메시지와 대응되는 인덱스와 함께, 제2 메시지의 복호화를 위한 복호화 키를 수신하도록 제어할 수 있다. 본 발명의 실시예들에 따른 사용자 단말기(200, 300)는 제2 메시지에 대한 응답 메시지를 전송하는데 있어서, 상기 복호화 키를 활용할 수 있다. 여기서, 인덱스는 본 발명의 실시예들에 따른 메시지 서버(200)에 의해 생성되어 관리되는 정보로서, 메시지를 송수신하는 것보다는 인덱스를 송수신하는 것이 좀더 적은 리소스를 이용하여 가능할 수 있기 때문에 메시지 자체를 송수신하지 않고 메시지와 대응되는 인덱스를 전송할 수 있다.

[0101] 메시지 자체를 송수신하는 경우에는 데이터 호출이 필요 없을 수 있으나, 그렇지 않고 메시지, 및 첨부 파일과 대응되는 인덱스들을 송수신하는 경우에는 데이터 호출부(254)는 제2 메시지에 포함된 첨부 파일과 대응되는 인덱스를 이용하여, 상기 첨부 파일을 호출할 수 있다. 데이터 호출부(254)는 메시지의 내용과 관련하여서도, 바로 메시지의 내용을 전달 받지 못하는 경우, 메시지와 대응되는 인덱스를 이용하여, 메시지의 내용을 호출할 수 있다. 데이터 호출부(254)는 메시지에 포함된 하나 이상의 항목을 인덱스를 이용하여 호출할 수 있다.

[0102] 복호화부(256)는 수신한 인덱스, 메시지의 내용 및 첨부 파일 등을 복호화 키를 이용하여 복호화할 수 있다.

[0103] 마지막으로 동일한 사용자가 보유 또는 사용하는 복수의 단말기, 즉 제1 사용자 단말기(201) 및 제3 사용자 단말기(202)를 이용하여, 메시지 송수신 서비스를 이용하는 방법과 관련된 구성을 설명하겠다.

[0104] 인증 관리부(258)는 제1 사용자 단말기(201)를 통한 메시지 송수신을 하는 사용자가 제1 사용자 단말기(201)을 통한 송수신 내역을 제3 사용자 단말기(202)를 통해 공유할 수 있도록 제3 사용자 단말기(202)에 대한 인증 과정을 수행할 수 있다.

[0105] 인증 관리부(258)는 도 5에 도시된 바와 같이, 인증 키 수신부(2581), 인증 키 처리부(2582), 암호화부(2583), 키 전송부(2584)를 포함할 수 있다.

[0106] 우선, 사용자가 제3 사용자 단말기(202)를 이용하여, 메시지 송수신을 하기 위해서는 메시지 송수신 애플리케이션을 통해 로그인 과정을 거쳐야 한다. 로그인 과정을 통해, 사용자 아이디 및 패스워드가 제1 사용자 단말기(201)를 통한 사용자 정보와 일치하는 경우, 메시지 서버(100)는 제1 사용자 단말기 및 제3 사용자 단말기를 통해 메시지 송수신을 할 수 있도록 제어할 수 있다.

[0107] 제1 사용자 단말기(201)를 통해 메시지 송수신을 하는 경우, 상기 제1 사용자 단말기와 다른 제3 사용자 단말기(202)의 인증 키 수신부(2581)는 메시지 공유 및 송수신을 위한 제1 인증 키를 메시지 서버(100)로부터 수신한다.

[0108] 제3 사용자 단말기(202)는, 수신한 인증 키를 입력하도록 제어되는 인증 키 처리부(2582)를 포함할 수 있다. 인증 키 처리부(2582)는 제1 사용자 단말기(201)를 통해 수신된 인증 키를 입력받도록 제어한다. 인증 키 처리부(2582)는 입력된 제2 인증 키를 메시지 서버(100)로 전송하는 기능을 수행한다. 인증 키 처리부(2582)는 인증 키 전송의 응답으로, 제2 인증 키의 유효성 판단 결과를 수신받을 수 있다. 즉, 제1 인증 키 및 제2 인증 키가 동일한 경우, 인증 키 처리부(2582)는 인증이 완료되었다는 메시지를 수신하고, 이에 따라 제1 사용자 단말기(201)를 통해 송수신된 하나 이상의 메시지를 공유하게 된다.

[0109] 또한, 인증 키 처리부(2582)는 인증 키를 이용하여, 암호화 키 또는 복호화 키를 제1 사용자 단말기(201)로부터 수신하도록 제어한다. 인증 과정을 통해 메시지 송수신이 가능하게 되었다면, 인증 키 처리부(2582)는 암호화 키 또는 복호화 키를 공유하도록 제어함으로써, 메시지의 해독 및 암호화가 가능하도록 한다. 이때, 암호화 키 또는 복호화 키는 인증 키를 이용하여 암호화되어 제1 사용자 단말기(201)로부터 제3 사용자 단말기(202)로 송수신된다.

[0110] 암호화부(2583)는 인증 키 처리부(2582)를 통해 수신한 암호화 키를 이용하여 메시지를 암호화한다.

[0111] 이를 통해, 사용자는 제1 사용자 단말기(201) 뿐만 아니라 제3 사용자 단말기(202)를 이용하여 메시지를 송수신할 수 있고, 제1 사용자 단말기(201)를 통해 송수신된 메시지를 제3 사용자 단말기(202)를 통해 확인할 수 있다.

[0112] 도 7 내지 도 8은 본 발명의 실시예들에 따른 메시지 송수신 방법을 나타내는 흐름도이다.

[0113] 도 7에 도시된 바와 같이, 본 발명의 실시예들에 따른 메시지 송수신 방법은 메시지 입력 단계(S110), 키 생성 단계(S120), 암호화 단계(S130), 전송 단계(S140)를 포함할 수 있다.

[0114] S110에서는 제1 사용자 단말기(201)는 제1 메시지를 입력하도록 제어한다. 제1 사용자 단말기(201)는 사용자 입

력부(240)에 의해 입력된 입력 신호에 따라 제1 메시지가 생성될 수 있도록 제어한다. 제1 사용자 단말기(201)는 사용자에 의해 입력된 입력 신호와 대응하여, 제1 메시지의 제목, 내용, 발신자 정보, 수신자 정보, 첨부 파일 등을 포함하는 제1 메시지를 생성할 수 있다.

[0115] S120에서는 제1 사용자 단말기(201)는 제1 메시지를 암호화하는 암호화 키를 생성할 수 있다. 제1 사용자 단말기(201)는 제1 메시지를 암호화하는 암호화 키(private key) 및 상기 암호화 키와 대응되는 복호화 키(public key)를 생성할 수 있다.

[0116] 제1 사용자 단말기(201)는 메시지의 내용 및 첨부 파일을 암호화하는 키를 각각 생성할 수 있다. 먼저 첨부 파일의 암호화 키를 생성하는 과정을 설명하면, 제1 사용자 단말기(201)는 메시지의 첨부 파일의 크기를 고려하여, 메시지의 첨부 파일의 암호화 키를 생성할 수 있다. 예를 들어, 메시지의 첨부 파일의 용량이 미리 설정된 임계 크기 보다 작은 경우, 제1 사용자 단말기(201)는 첨부 파일과 관련 없이 랜덤한 값을 첨부 파일의 암호화 키로 생성할 수 있다. 메시지의 첨부 파일의 용량이 상기 임계 크기 보다 큰 경우, 제1 사용자 단말기(201)는 첨부 파일의 해쉬값을 첨부 파일의 암호화 키로 생성할 수 있다.

[0117] 제1 사용자 단말기(201)는 메시지의 첨부 파일의 종류를 고려하여, 메시지의 첨부 파일의 암호화 키를 생성할 수 있다. 예를 들어, 메시지의 첨부 파일이 동영상인 경우, 제1 사용자 단말기(201)는 첨부 파일의 해쉬값을 첨부 파일의 암호화 키로 생성할 수 있다. 메시지의 첨부 파일이 음성 파일 또는 이미지인 경우, 제1 사용자 단말기(201)는 첨부 파일과 관련 없이 랜덤한 값을 첨부 파일의 암호화 키로 생성할 수 있다.]

[0118] 다음으로 메시지의 내용을 암호화하는 암호화 키를 생성하는 과정을 설명하면, 제1 사용자 단말기(201)는 메시지의 내용을 암호화하는 암호화 키를 랜덤하게 생성할 수 있다. 이때, 암호화 키는 수신자 정보, 발신자 정보, 발신 시간, 발신 날짜 등을 고려하여 랜덤하게 생성될 수 있다.

[0119] 다른 실시예에서, 제1 사용자 단말기(201)는 복수의 수신자들의 사용자 단말기(200, 300)로 전송하도록 생성된 제1 메시지의 경우, 각 수신자 별로 다른 암호화 키를 생성할 수 있다. 제2 사용자 단말기(301) 및 제3 사용자 단말기(302)로 전송되어야 하는 제1 메시지의 경우, 제1 사용자 단말기(201)는 제2 사용자 단말기(301)로 전송되는데 이용되는 제1 암호화 키 및 제3 사용자 단말기(302)로 전송되는데 이용되는 제2 암호화 키를 각각 생성할 수 있다.

[0120] S130에서는 제1 사용자 단말기(201)는 키 생성부(257)에 의해 생성된 암호화 키들을 이용하여 제1 메시지의 내용 및 첨부 파일을 각각 암호화하는 기능을 수행한다. 제1 사용자 단말기(201)는 하나 이상의 암호 키(또는 암호화 키)를 이용하여, 제1 메시지의 내용 및 첨부 파일을 암호화할 수 있다. 제1 사용자 단말기(201)는 복수의 사용자에게 전송되도록 설정된 제1 메시지를 사용자 별로 생성된 암호화 키를 이용하여 각각 암호화할 수 있다.

[0121] S140에서는 제1 사용자 단말기(201)는 암호화된 제1 메시지를 제1 메시지의 수신자인 제2 사용자 단말기로 전송하도록 메시지 서버(100)로 전송한다.

[0122] 도 8에 도시된 바와 같이, 본 발명의 실시예들에 따른 메시지 송수신 방법은 메시지 수신 단계(S210), 데이터 호출 단계(S220), 데이터 복호화 단계(S230)를 포함할 수 있다.

[0123] S210에서는 제1 사용자 단말기(201)는 메시지 서버(100)로부터 제2 사용자 단말기(200, 300)로부터의 제2 메시지 또는 제2 메시지와 대응되는 인덱스를 수신하도록 제어한다. 제1 사용자 단말기(201)는 제2 메시지 또는 제2 메시지와 대응되는 인덱스와 함께, 제2 메시지의 복호화를 위한 복호화 키를 수신하도록 제어할 수 있다.

[0124] S220에서는 메시지 자체를 송수신하는 경우에는 데이터 호출이 필요 없을 수 있으나, 그렇지 않고 메시지, 및 첨부 파일과 대응되는 인덱스들을 송수신하는 경우에는 제1 사용자 단말기(201)는 제2 메시지에 포함된 첨부 파일과 대응되는 인덱스를 이용하여, 상기 첨부 파일을 호출할 수 있다. 제1 사용자 단말기(201)는 메시지의 내용과 관련하여서도, 바로 메시지의 내용을 전달 받지 못하는 경우, 메시지와 대응되는 인덱스를 이용하여, 메시지의 내용을 호출할 수 있다. 제1 사용자 단말기(201)는 메시지에 포함된 하나 이상의 항목을 인덱스를 이용하여 호출할 수 있다.

[0125] S230에서는 제1 사용자 단말기(201)는 수신한 인덱스, 메시지의 내용 및 첨부 파일 등을 복호화 키를 이용하여 복호화할 수 있다. 제1 사용자 단말기(201)는 복호화가 실패한 경우, 해당 메시지에 대한 보안을 요청하는 내용을 포함하는 화면을 표시하도록 제어할 수 있다.

[0126] 도 9는 제1 사용자 단말기 및 제2 사용자 단말기 사이의 메시지 송수신 과정을 설명하기 위한 흐름도이다.

[0127] 제1 사용자 단말기(201)는 입력한 메시지를 암호화하기 위한 암호화 키를 생성하고, 상기 암호화 키와 대응되는 복호화 키를 생성할 수 있다. 암호화 키 및 복호화 키 사이의 관계는 상술하였으므로, 자세한 설명을 생략한다(S901). 여기서, 암호화 키는 메시지의 내용 및 메시지의 첨부 파일을 암호화하기 위해서 각각 생성될 수 있다.

[0128] 제1 사용자 단말기(201)는 첨부 파일을 포함하는 메시지를 생성하는 사용자 입력을 입력 받는다(S902). 제1 사용자 단말기(201)는 상기 첨부 파일 및 메시지의 내용을 상기 암호화 키를 이용하여 암호화한다(S903). 제1 사용자 단말기(201)는 복호화 키 및 암호화된 파일 및 메시지를 메시지 서버로 전송한다(S904, S905). 여기서, 복호화 키는 메시지 및 메시지에 포함된 첨부 파일 각각을 위해서 복수 개가 생성될 수 있다. 메시지에 포함된 수신자의 제2 사용자 단말기(300)로 전송하도록 생성된 메시지는 제2 사용자 단말기(300)로 전송된다(S905, S906). 복호화 키 및 암호화된 파일 및 메시지를 수신한 제2 사용자 단말기(300)는 메시지 및 메시지에 포함된 파일을 복호화 키로 복호화 한다(S908).

[0129] 도 10은 제1 사용자 단말기 및 제3 사용자 단말기 사이의 메시지 공유 과정을 설명하기 위한 흐름도이다.

[0130] 제1 사용자 단말기(201) 및 제3 사용자 단말기(202)를 모두 보유 또는 소유하고 있는 사용자는 제3 사용자 단말기(202)를 통해 메시지 송수신을 위한 로그인 정보를 입력 할 수 있다(S1001). 제3 사용자 단말기(202)는 로그인 정보를 메시지 서버(100)로 전송한다(S1002). 메시지 서버(100)는 로그인 정보의 유효성을 판단한다(S1003). 즉, 메시지 서버(100)는 로그인 정보에 포함되는 아이디 정보 및 패스워드 정보가 서로 대응되는지 여부를 판단한다. 메시지 서버(100)는 제1 사용자 아이디 및 제1 사용자의 패스워드가 포함되어 있는지 여부를 판단한다. 로그인 정보가 유효한 경우, 메시지 서버(100)는 랜덤하게 생성된 제1 인증 번호를 제3 사용자 단말기(202)로 전송한다(S1004). 이후, 사용자가 보유 또는 소유하고 있는 제1 사용자 단말기(201)로 인증 번호를 입력하도록 하는 신호를 전송한다. 상기 신호와 대응하여, 제1 사용자 단말기(201)은 인증 번호를 입력하도록 하는 사용자 인터페이스를 표시한다(S1005). 상기 사용자 인터페이스에 따라 제1 사용자 단말기(201)은 제2 인증 번호를 입력 받는다(S1006). 제1 사용자 단말기(201)는 입력된 제2 인증 번호를 메시지 서버(100)로 전송한다(S1007). 메시지 서버(100)는 제1 인증 번호 및 제2 인증 번호 사이의 일치 여부를 판단하고(S1008), 일치한 경우, 제3 사용자 단말기에 대한 인증 과정, 처리를 완료한다(S1009). S1001 내지 S1009 단계를 수행한 다음 부터는 메시지 서버(100)는 제1 사용자 단말기(201)에 의해 수신되거나 송신된 메시지를 제3 사용자 단말기(202)로 전달하고, 반대로 제3 사용자 단말기(202)에 의해 수신되거나 송신된 메시지를 제1 사용자 단말기(201)로 전달하게 된다. 즉, 제1 사용자 단말기(201) 및 제3 사용자 단말기(202)는 동일한 메시지 송수신 이력을 공유하게 된다.

[0131] 선택적 실시예에서, 각 메시지에 대한 확인 정보는 제1 사용자 단말기(201) 및 제3 사용자 단말기(202) 간에 차이가 있을 수 있다. 예를 들어, 제1 사용자 단말기(201)를 통해 확인된 메시지는 제3 사용자 단말기(202)에서는 미확인 메시지로 표시될 수 있다.

[0132] 도 11 내지 도 14는 본 발명의 실시예들에 따른 사용자 단말기에 제공되는 사용자 인터페이스의 예시들을 설명하기 위한 도면이다.

[0133] 도 11에 도시된 1101은 제1 사용자 단말기(201)에 표시되는 사용자 인터페이스로서, 제3 사용자 단말기(202)로 전송된 인증 번호를 입력 받도록 하는 화면이다. 사용자는 도 11에 도시된 바와 같이 6자리의 인증 번호를 입력하고, 본인 확인 버튼(1102)를 클릭함으로써, 제1 사용자 단말기(201)는 인증 처리를 수행할 수 있다.

[0134] 도 12에 도시된 1201은 사용자 단말기(200, 300)에 메시지를 표시하는 사용자 인터페이스이다. 본인 인증을 거치지 않은 사용자 단말기(200, 300)은 메시지를 암호화된 상태로 보여주게 되며(1202), 본인 확인을 위한 버튼(1203)을 클릭함으로써, 별도의 본인 확인을 수행해야 한다.

[0135] 도 13에 도시된 바와 같이, 1301은 사용자에 의해 생성된 하나 이상의 대화방을 리스트로 표시하는 화면과 각 대화방에서 이루어진 대화를 표시하는 화면을 함께 표시할 수 있다(1301). 상대방이 추가적인 보안 과정을 필요로 하는 메시지(1302)를 전송한 경우, 이미 본인 확인을 한 사용자라 하더라도 상기 메시지를 표시하지 않고, 사용자는 상기 메시지의 내용을 확인하기 위해서 별도의 인증 과정을 거치도록 제어할 수 있다(S1303).

[0136] 도 14에 도시된 바와 같이, 1401은 대화방 리스트를 표시할 수 있고, 대화방 리스트에서 암호화된 메시지가 표시되지 않도록 한다(1402).

[0137] 이상 설명된 본 발명에 따른 실시예는 컴퓨터 상에서 다양한 구성요소를 통하여 실행될 수 있는 컴퓨터 프로그램의 형태로 구현될 수 있으며, 이와 같은 컴퓨터 프로그램은 컴퓨터로 판독 가능한 매체에 기록될 수 있다. 이

때, 매체는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM 및 DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical medium), 및 ROM, RAM, 플래시 메모리 등과 같은, 프로그램 명령어를 저장하고 실행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다.

[0138] 한편, 상기 컴퓨터 프로그램은 본 발명을 위하여 특별히 설계되고 구성된 것이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수 있다. 컴퓨터 프로그램의 예에는, 컴파일러에 의하여 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용하여 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함될 수 있다.

[0139] 본 발명에서 설명하는 특정 실행들은 일 실시 예들로서, 어떠한 방법으로도 본 발명의 범위를 한정하는 것은 아니다. 명세서의 간결함을 위하여, 종래 전자적인 구성들, 제어 시스템들, 소프트웨어, 상기 시스템들의 다른 기능적인 측면들의 기재는 생략될 수 있다. 또한, 도면에 도시된 구성 요소들 간의 선들의 연결 또는 연결 부재들은 기능적인 연결 및/또는 물리적 또는 회로적 연결들을 예시적으로 나타낸 것으로서, 실제 장치에서는 대체 가능하거나 추가의 다양한 기능적인 연결, 물리적인 연결, 또는 회로 연결들로서 나타내어질 수 있다. 또한, “필수적인”, “중요하게” 등과 같이 구체적인 언급이 없다면 본 발명의 적용을 위하여 반드시 필요한 구성 요소가 아닐 수 있다.

[0140] 본 발명의 명세서(특히 특허청구범위에서)에서 “상기”의 용어 및 이와 유사한 지시 용어의 사용은 단수 및 복수 모두에 해당하는 것일 수 있다. 또한, 본 발명에서 범위(range)를 기재한 경우 상기 범위에 속하는 개별적인 값을 적용한 발명을 포함하는 것으로서(이에 반하는 기재가 없다면), 발명의 상세한 설명에 상기 범위를 구성하는 각 개별적인 값을 기재한 것과 같다. 마지막으로, 본 발명에 따른 방법을 구성하는 단계들에 대하여 명백하게 순서를 기재하거나 반하는 기재가 없다면, 상기 단계들은 적당한 순서로 행해질 수 있다. 반드시 상기 단계들의 기재 순서에 따라 본 발명이 한정되는 것은 아니다. 본 발명에서 모든 예들 또는 예시적인 용어(예들 들어, 등등)의 사용은 단순히 본 발명을 상세히 설명하기 위한 것으로서 특허청구범위에 의해 한정되지 않는 이상 상기 예들 또는 예시적인 용어로 인해 본 발명의 범위가 한정되는 것은 아니다. 또한, 당업자는 다양한 수정, 조합 및 변경이 부가된 특허청구범위 또는 그 균등물의 범주 내에서 설계 조건 및 팩터에 따라 구성될 수 있음을 알 수 있다.

부호의 설명

[0141] 10: 메시지 송수신 시스템

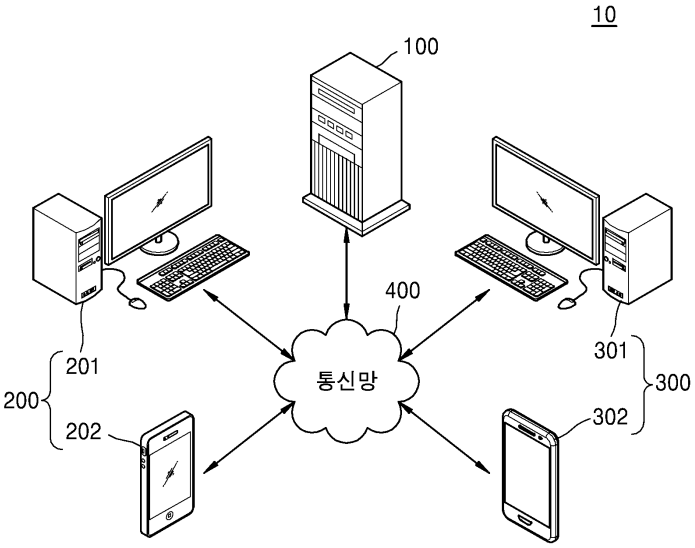
100: 메시지 서버

200, 300: 사용자 단말기

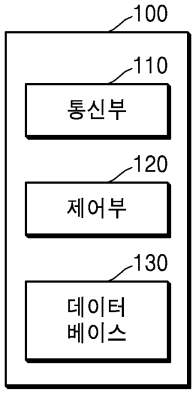
400: 통신망

도면

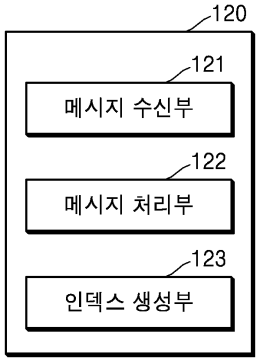
도면1



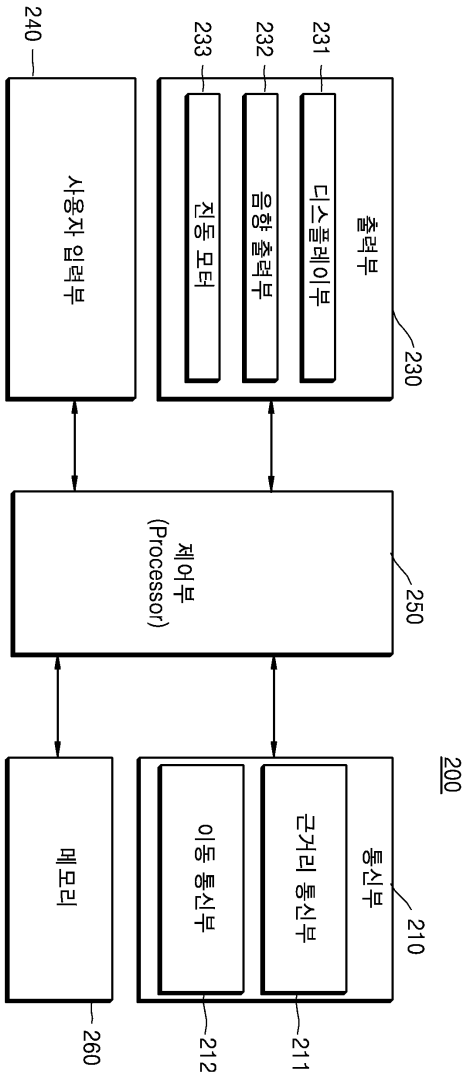
도면2



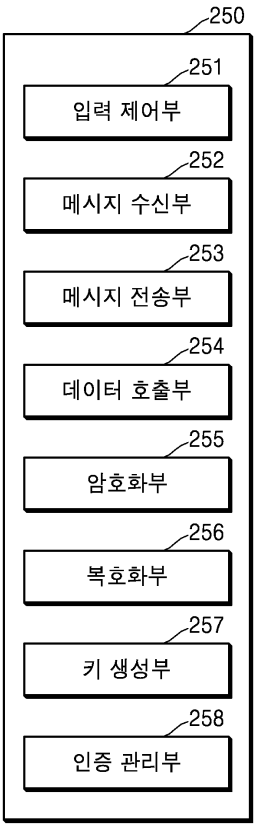
도면3



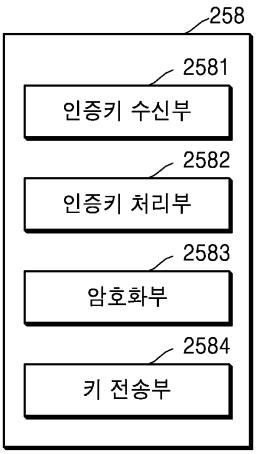
도면4


240
233
232
231
사용자 입력부
진동 모터
음향 출력부
디스플레이부
출력부
230
제어부
(Processor)
250
200
메모리
이동 통신부
근거리 통신부
통신부
210
260
212
211

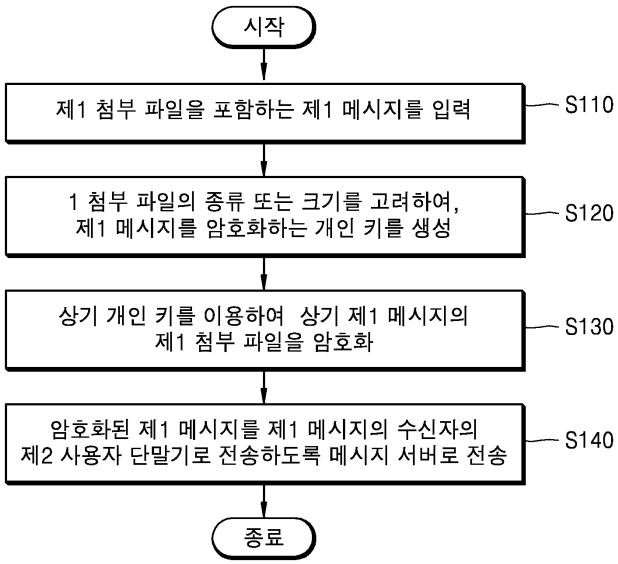
도면5


250
251
입력 제어부
252
메시지 수신부
253
메시지 전송부
254
데이터 호출부
255
암호화부
256
복호화부
257
키 생성부
258
인증 관리부

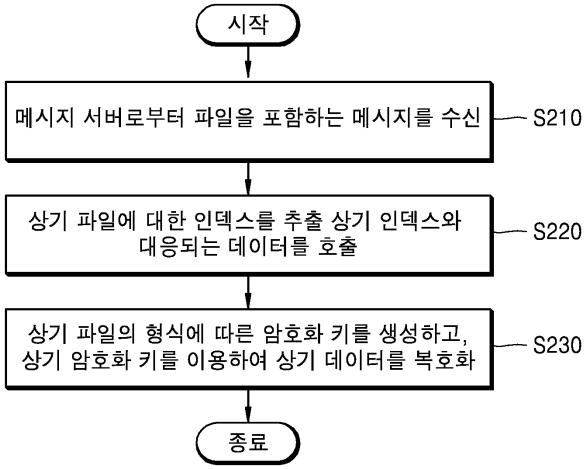
도면6


258
2581
인증키 수신부
2582
인증키 처리부
2583
암호화부
2584
키 전송부

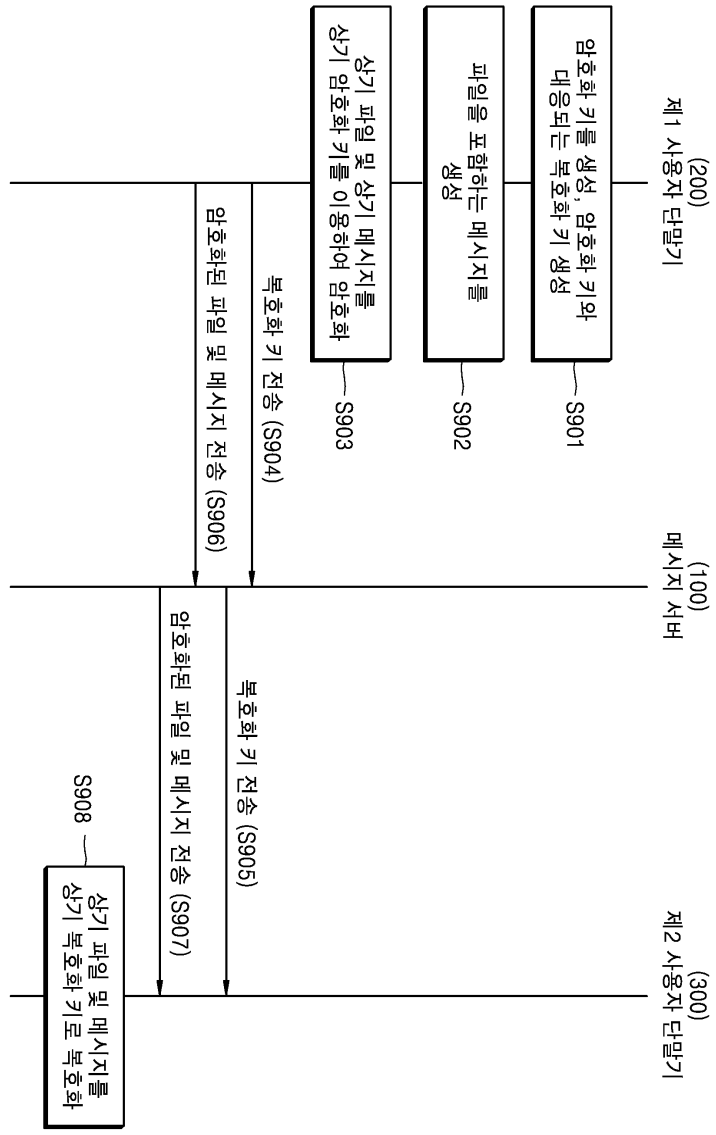
도면7


시작
제1 첨부 파일을 포함하는 제1 메시지를 입력
S110
1 첨부 파일의 종류 또는 크기를 고려하여,
제1 메시지를 암호화하는 개인 키를 생성
S120
상기 개인 키를 이용하여 상기 제1 메시지의
제1 첨부 파일을 암호화
S130
암호화된 제1 메시지를 제1 메시지의 수신자의
제2 사용자 단말기로 전송하도록 메시지 서버로 전송
S140
종료

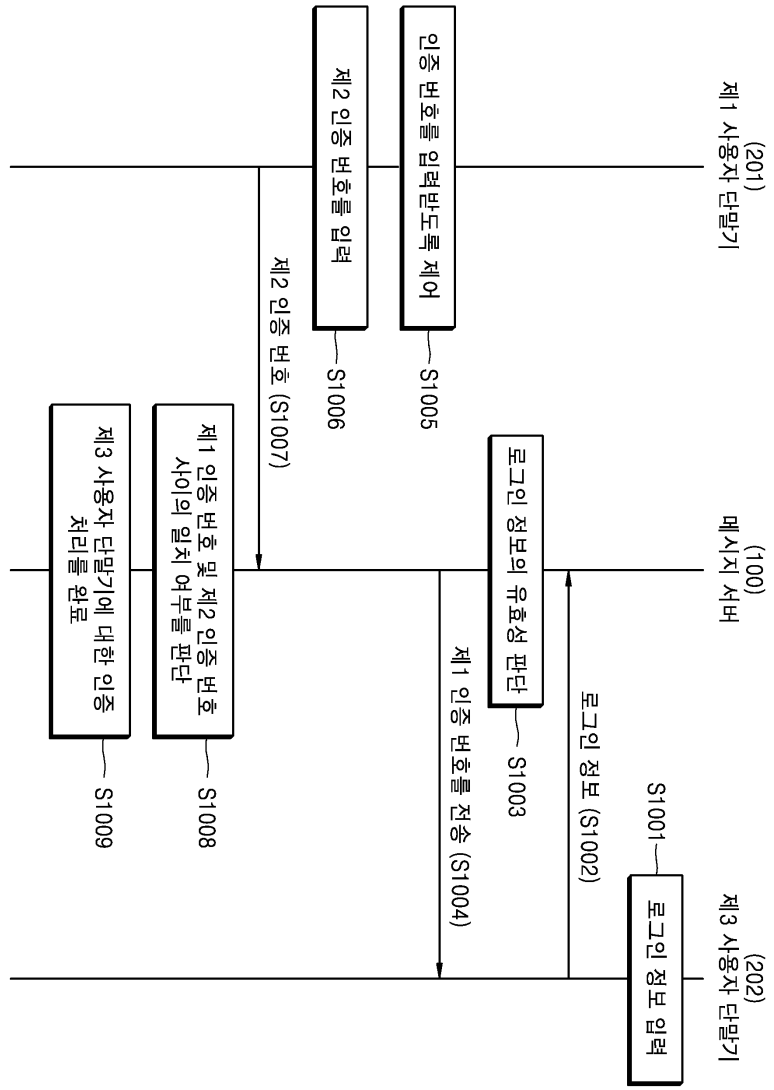
도면8


시작
메시지 서버로부터 파일을 포함하는 메시지를 수신
S210
상기 파일에 대한 인덱스를 추출 상기 인덱스와
대응되는 데이터를 호출
S220
상기 파일의 형식에 따른 암호화 키를 생성하고,
상기 암호화 키를 이용하여 상기 데이터를 복호화
S230
종료

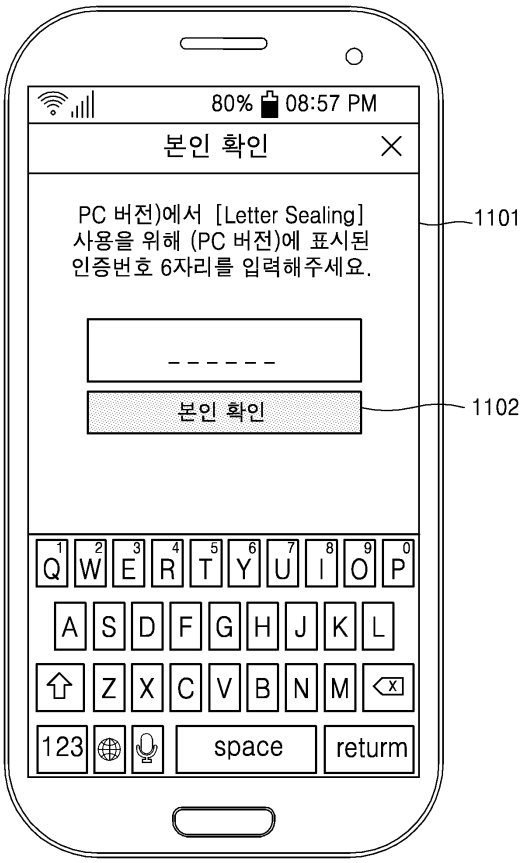
도면9


(200)
제1 사용자 단말기
(100)
메시지 서버
(300)
제2 사용자 단말기
암호화 키를 생성, 암호화 키와 대응되는 복호화 키 생성
S901
파일을 포함하는 메시지를 생성
S902
상기 파일 및 상기 메시지를 상기 암호화 키를 이용하여 암호화
S903
복호화 키 전송 (S904)
암호화된 파일 및 메시지 전송 (S906)
복호화 키 전송 (S905)
암호화된 파일 및 메시지 전송 (S907)
S908
상기 파일 및 메시지를 상기 복호화 키로 복호화

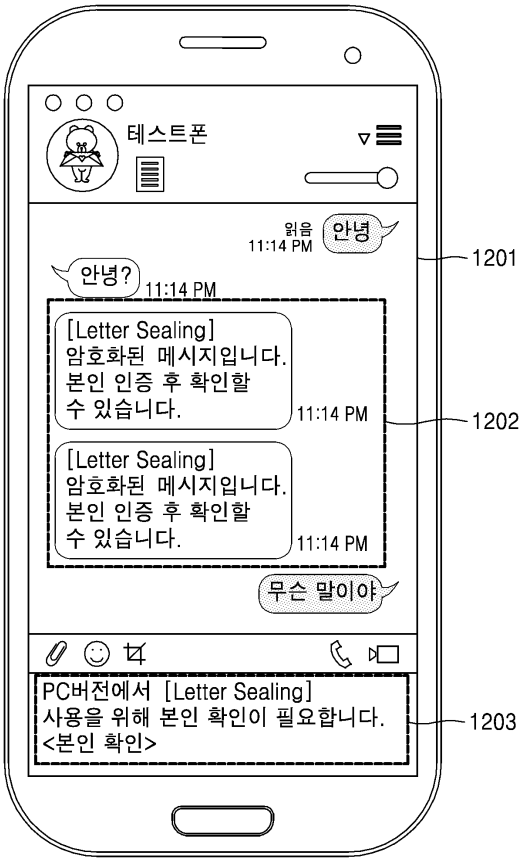
도면10


(201)
제1 사용자 단말기
(100)
메시지 서버
(202)
제3 사용자 단말기
인증 번호를 입력받도록 제어
S1005
제2 인증 번호를 입력
S1006
제2 인증 번호 (S1007)
로그인 정보의 유효성 판단
S1003
제1 인증 번호를 전송 (S1004)
로그인 정보 (S1002)
S1001
로그인 정보 입력
제1 인증 번호 및 제2 인증 번호 사이의 일치 여부를 판단
S1008
제3 사용자 단말기에 대한 인증 처리를 완료
S1009

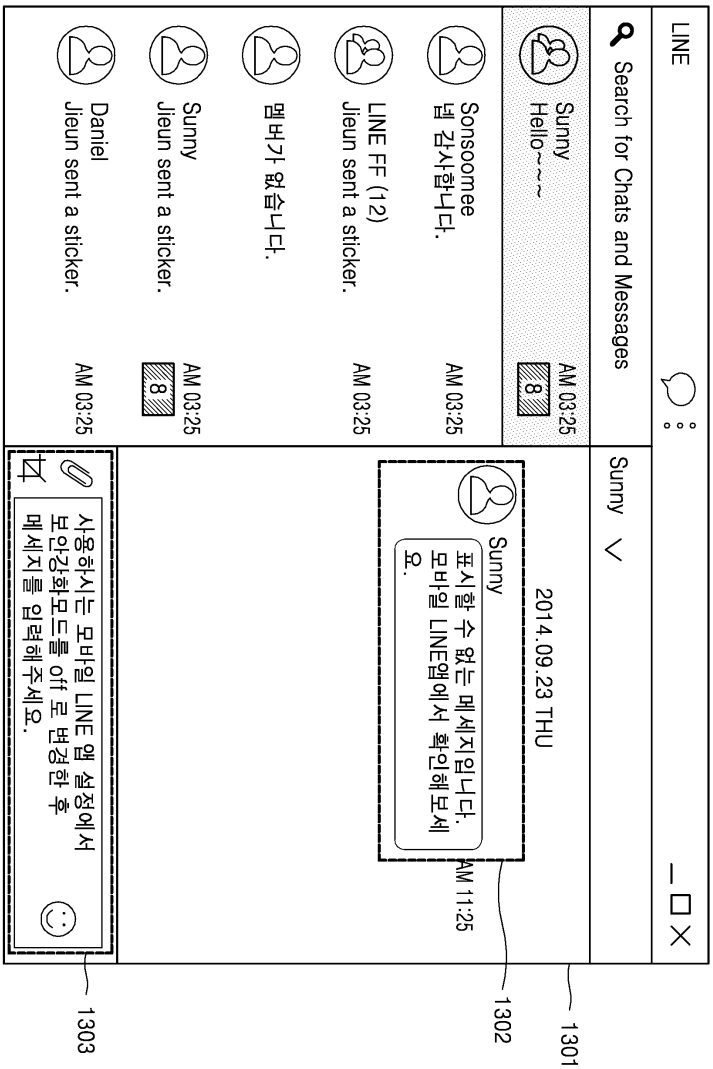
도면11


80% 08:57 PM
본인 확인
PC 버전)에서 [Letter Sealing]
사용을 위해 (PC 버전)에 표시된
인증번호 6자리를 입력해주세요.
1101
- - - - - -
본인 확인
1102
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return

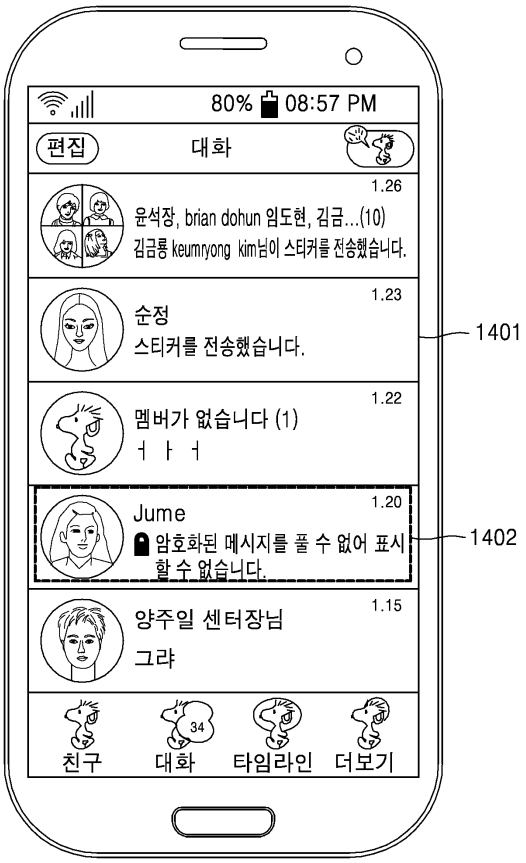
도면12


테스트폰
읽음
11:14 PM
안녕
안녕?
11:14 PM
[Letter Sealing]
암호화된 메시지입니다.
본인 인증 후 확인할
수 있습니다.
11:14 PM
[Letter Sealing]
암호화된 메시지입니다.
본인 인증 후 확인할
수 있습니다.
11:14 PM
무슨 말이야
PC버전에서 [Letter Sealing]
사용을 위해 본인 확인이 필요합니다.
<본인 확인>
1201
1202
1203

도면13


LINE
Search for Chats and Messages
Sunny
Hello~~~
AM 03:25
8
Sonsoomee
넵 감사합니다.
AM 03:25
LINE FF (12)
Jieun sent a sticker.
AM 03:25
멤버가 없습니다.
Sunny
Jieun sent a sticker.
AM 03:25
8
Daniel
Jieun sent a sticker.
AM 03:25
Sunny
2014.09.23 THU
Sunny
표시할 수 없는 메세지입니다.
모바일 LINE앱에서 확인해보세요.
AM 11:25
사용하시는 모바일 LINE 앱 설정에서
보안강화모드를 off 로 변경한 후
메세지를 입력해주세요.
1301
1302
1303

도면14


80% 08:57 PM
편집
대화
1.26
윤석장, brian dohun 임도현, 김금...(10)
김금룡 keumryong kim님이 스티커를 전송했습니다.
1.23
순정
스티커를 전송했습니다.
1401
1.22
멤버가 없습니다 (1)
ㅓ ㅏ ㅓ
1.20
Jume
암호화된 메시지를 풀 수 없어 표시할 수 없습니다.
1402
1.15
양주일 센터장님
그랴
34
친구
대화
타임라인
더보기