(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년03월06일
(11) 등록번호 10-1500118
(24) 등록일자 2015년03월02일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2013-0094406
(22) 출원일자 2013년08월08일
심사청구일자 2013년08월08일
(65) 공개번호 10-2015-0018024
(43) 공개일자 2015년02월23일
(56) 선행기술조사문헌
KR1020040028086 A*
KR1020130027930 A*
KR1020030012764 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 에스원
서울특별시 중구 세종대로7길 25(순화동)
(72) 발명자
윤희정
서울 용산구 새창로 70, 104동 903호 (도원동, 삼성래미안아파트)
오광철
경기 용인시 기흥구 흥덕중앙로105번길 41, 1110동 101호 (영덕동, 흥덕마을11단지경남아너스빌)
(뒷면에 계속)
(74) 대리인
서만규, 서경민

전체 청구항 수 : 총 10 항 심사관 : 홍기완

(54) 발명의 명칭 **데이터 공유 방법 및 이를 이용한 데이터 공유 시스템**

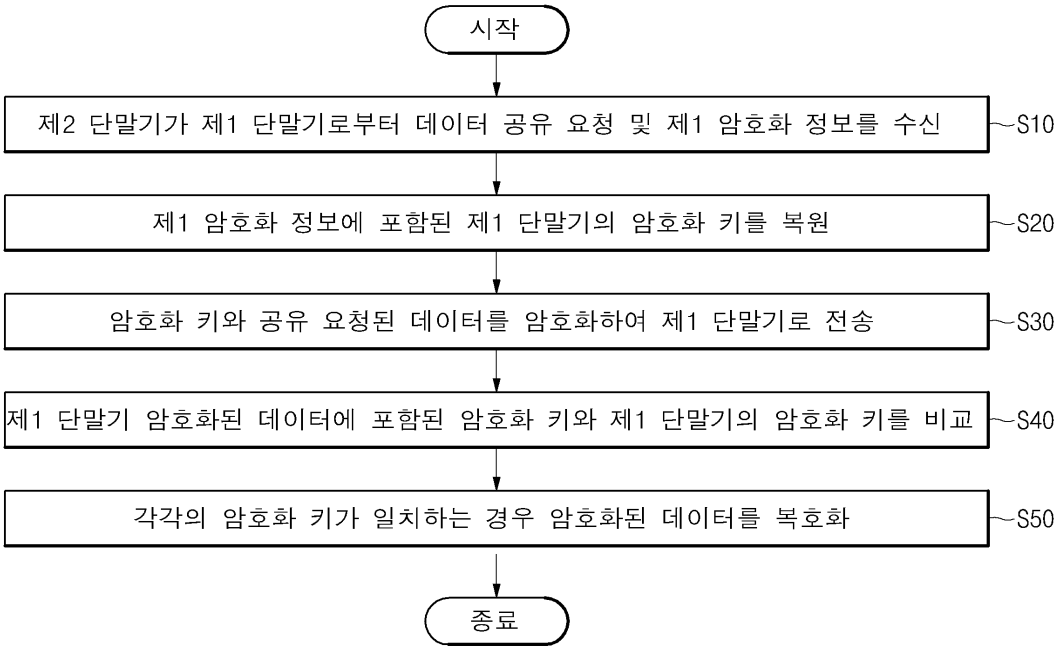
(57) 요 약

본 발명의 일 실시예는 데이터 공유 방법 및 이를 이용한 데이터 공유 시스템에 관한 것으로, 해결하고자 하는 기술적 과제는 수 있게 하는데 있다.

이를 위해 본 발명의 일 실시예는 정보 요청자의 제1 단말기와 정보 제공자의 제2 단말기 간에 암호화된 데이터

(뒷면에 계속)

대 표 도 - 도4



를 공유하는 데이터 공유 방법에 있어서, 상기 제2 단말기가 상기 제1 단말기로부터 원하는 데이터의 공유 요청과 함께 제1 암호화 정보를 수신하는 제1 단계; 상기 수신된 제1 암호화 정보에 포함된 제1 단말기의 암호화 키를 복원하는 제2 단계; 상기 복원된 암호화 키와 상기 제1 단말기로부터 공유 요청된 데이터를 암호화하여 상기 제1 단말기로 전송하는 제3 단계; 상기 제1 단말기가 상기 제2 단말기로부터 전송된 암호화된 데이터에 포함된 암호화 키와 상기 제1 단말기의 암호화 키를 비교하는 제4 단계; 및 각각의 암호화 키가 일치하는 경우 상기 암호화된 데이터를 복호화하는 제5 단계를 포함하는 데이터 공유 방법을 개시한다.

(72) 발명자

김진규

경기 수원시 영통구 권광로260번길 36, 110동 2303호 (매탄동, 매탄현대힐스테이트)

김우재

서울 양천구 목동동로 50, 1208동 301호 (신정동, 목동12단지아파트)

이동성

경기 성남시 분당구 느티로 70, 312동 1101호 (정자동, 느티마을아파트)

특허청구의 범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

각각 데이터 공유 어플리케이션이 탑재되어 있는 정보 요청자의 제1 단말기와 정보 제공자의 제2 단말기를 포함하며, 상기 데이터 공유 어플리케이션의 실행에 의하여 상기 제1 단말기와 제2 단말기 간에 암호화된 데이터를 공유하는 데이터 공유 시스템이고,

상기 제2 단말기가 상기 제1 단말기로부터 원하는 데이터의 공유 요청과 함께 제1 암호화 정보를 수신하여 상기 제1 암호화 정보에 포함된 제1 단말기의 암호화 키를 복원한 후, 상기 복원된 암호화 키와 상기 제1 단말기로부터 공유 요청된 데이터를 암호화하여 상기 제1 단말기로 전송하며,

상기 제1 단말기가 상기 제2 단말기로부터 전송된 암호화된 데이터에 포함된 암호화 키와 상기 제1 단말기의 암호화 키를 비교한 후, 각각의 암호화 키가 일치하는 경우 상기 암호화된 데이터를 복호화하고,

상기 제2 단말기는

상기 제1 단말기와 데이터를 송수신하는 제2 통신부;

상기 제1 단말기로부터 요청된 데이터의 공유 여부를 결정하되, 상기 제1 단말기로부터 요청된 데이터의 공유를 원하지 않는 경우 상기 요청된 데이터를 일반 데이터를 암호화하는 방식으로 암호화하는 공유 여부 결정부;

상기 제1 단말기로부터 수신된 제1 암호화 정보를 분석하되, 제1 암호화 정보에 포함된 칩 일련번호 정보를 조회하고, 해당 위치 정보를 생성하는 암호화 정보 분석부;

상기 제1 암호화 정보의 분석 결과에 따라 암호화 명령을 생성하되, 제1 암호화 정보에 포함된 칩 일련번호가 조회되어 해당 위치 정보가 생성되는 경우에 암호화 명령을 생성하는 암호화 명령 생성부;

상기 제1 암호화 정보에 포함된 암호화키와 상기 제1 단말기로부터 공유 요청된 데이터를 암호화하여 데이터를 생성하는 암호화 데이터 생성부; 및

상기 데이터 공유 어플리케이션을 탑재하고, 상기 데이터 공유 어플리케이션의 실행에 의하여 상기 각각의 구성요소들의 동작을 제어하는 제2 제어부를 포함하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 12

삭제

청구항 13

제11항에 있어서,

상기 암호화 데이터 생성부는 상기 암호화된 데이터에 매번 다른 레퍼런스 데이터를 다른 위치에 패딩시키는 것을 특징으로 하는 데이터 공유 시스템.

청구항 14

제11항에 있어서,

상기 제2 통신부는 상기 암호화된 데이터를 NFC의 P2P(Peer-to-Peer)를 이용하여 전송하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 15

제11항에 있어서,

상기 제1 단말기는

상기 제2 단말기와 데이터를 송수신하는 제1 통신부;

상기 제2 단말기에 원하는 데이터에 대한 공유를 요청하는 데이터 공유 요청부;

상기 제2 단말기로부터 전송된 암호화된 데이터를 분석하는 암호화 데이터 분석부;

상기 암호화된 데이터의 분석 결과에 따라 복호화 명령을 생성하는 복호화 명령 생성부;

상기 암호화된 데이터에 포함된 암호화 키와 상기 제1 단말기의 암호화 키를 비교하는 일련번호 비교부;

상기 암호화된 데이터에 포함된 암호화 키와 상기 제1 단말기의 암호화 키가 일치하는 경우, 상기 암호화된 데이터를 복호화하는 데이터 복호화부; 및

상기 데이터 공유 어플리케이션을 탑재하고, 상기 데이터 공유 어플리케이션의 실행에 의하여 상기 각각의 구성요소들의 동작을 제어하는 제1 제어부를 포함하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 16

제15항에 있어서,

상기 데이터 공유 요청부는 상기 원하는 데이터의 공유 요청을 SMS로 전송하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 17

제15항에 있어서,

상기 데이터 공유 요청부는 상기 데이터 공유 어플리케이션에 의하여 자동으로 원하는 데이터의 공유 요청을

SMS로 전송하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 18

제15항에 있어서,

상기 암호화 키는 상기 제1 단말기에 포함된 칩 일련번호를 포함하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 19

제15항에 있어서,

상기 암호화된 데이터는 변형 키를 생성하는 레퍼런스 데이터를 포함하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 20

제15항에 있어서,

상기 암호화된 데이터는 아이디, 칩 일련번호, 위치정보, 및 상기 제1 단말기의 공유 요청 데이터를 포함하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 21

제11항에 있어서,

상기 암호화된 데이터를 수신하여 저장하는 클라우드 서버를 더 포함하고,

상기 제1 단말기는 상기 클라우드 서버와 데이터를 송수신하는 제3 통신부를 더 포함하며,

상기 제2 단말기는 상기 클라우드 서버와 데이터를 송수신하는 제4 통신부를 더 포함하는 것을 특징으로 하는 데이터 공유 시스템.

명 세 서

기 술 분 야

[0001] 본 발명의 일 실시예는 데이터 공유 방법 및 이를 이용한 데이터 공유 시스템에 관한 것이다.

배 경 기 술

[0002] 통신 중계 서버를 통해 발신 단말과 수신 단말을 연결하는 통신 시스템에서, 발신 단말과 수신 단말 사이의 데이터는 외부 침입자에 의해 통신 경로 상에서 데이터를 복제하거나 훔쳐가는 것에 의해 안전하지 못하다.

[0003] 이와 같은 문제를 해결하기 위하여, 발신 단말과 수신 단말 사이의 데이터 흐름에 암호를 추가하는 방법이 제안되었다.

[0004] 특히, 이동 통신망은 무선 통신을 위해 전파의 형태로 데이터가 송수신되기 때문에, 데이터가 외부에 노출되어 있다. 따라서, 이동통신망은 CAVE(Cellular Authentication and Voice Encryption) 알고리즘을 사용하여 Private long code를 암호화 키로 생성하여 사용한다. 이 알고리즘은 기본적으로 비밀키 방식의 알고리즘을 근간으로 하고 있으나, 현재 이 알고리즘은 상당히 많이 분석되어 이미 해독되었다고 알려져 있다. 비록, 이 암호화 키가 안전하다 할지라도, 이 암호화 키를 이용한 통신 암호화는 기지국과 단말들 사이에만 이루어지기 때문에, 사용자들 간의 완전한 비밀 통신을 통하여 원하는 데이터를 공유하는 것이 불가능한 문제가 있다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 공개특허 제10-2006-0093782호 '무선 통신망을 이용하여 데이터를 공유하는 휴대용 단말기와,

데이터 공유를 위한 무선 데이터 통신 서비스 시스템 및 그 방법'

(특허문헌 0002) 등록특허 제10-1040832호 '이동통신 단말기를 이용한 비밀 메시지 수신 시스템 및 이를 이용한 비밀 메시지 수신 방법'

발명의 내용

해결하려는 과제

[0006] 본 발명의 일 실시예는 정보를 요청하는 수신자와 정보를 제공하는 제공자간 개인 대 개인으로 암호화 데이터를 공유할 수 있는 데이터 공유 방법 및 이를 이용한 데이터 공유 시스템을 제공한다.

과제의 해결 수단

[0007] 본 발명의 일 실시예에 의한 데이터 공유 방법은 정보 요청자의 제1 단말기와 정보 제공자의 제2 단말기 간에 암호화된 데이터를 공유하는 데이터 공유 방법에 있어서, 상기 제2 단말기가 상기 제1 단말기로부터 원하는 데이터의 공유 요청과 함께 제1 암호화 정보를 수신하는 제1 단계; 상기 수신된 제1 암호화 정보에 포함된 제1 단말기의 암호화 키를 복원하는 제2 단계; 상기 복원된 암호화 키와 상기 제1 단말기로부터 공유 요청된 데이터를 암호화하여 상기 제1 단말기로 전송하는 제3 단계; 상기 제1 단말기가 상기 제2 단말기로부터 전송된 암호화된 데이터에 포함된 암호화 키와 상기 제1 단말기의 암호화 키를 비교하는 제4 단계; 및 각각의 암호화 키가 일치하는 경우 상기 암호화된 데이터를 복호화하는 제5 단계를 포함할 수 있다.

[0008] 상기 제1 단말기와 제2 단말기는 각각 데이터 공유 어플리케이션이 탑재되어 있고, 상기 제1 단계 내지 제5 단계는 상기 데이터 공유 어플리케이션의 실행에 의하여 수행될 수 있다.

[0009] 상기 제1 단계에서 상기 제1 단말기로부터 원하는 데이터의 공유 요청을 SMS로 수신할 수 있다.

[0010] 상기 제1 단계에서 상기 제1 단말기는 상기 데이터 공유 어플리케이션에 의하여 자동으로 원하는 데이터의 공유 요청을 SMS로 전송할 수 있다.

[0011] 상기 암호화 키는 상기 제1 단말기에 포함된 칩 일련번호를 포함할 수 있다.

[0012] 상기 암호화된 데이터는 변형 키를 생성하는 레퍼런스 데이터를 포함할 수 있다.

[0013] 상기 암호화된 데이터는 아이디, 칩 일련번호, 위치정보, 및 상기 제1 단말기의 공유 요청 데이터를 포함할 수 있다.

[0014] 상기 제2 단말기는 상기 암호화된 데이터에 매번 다른 레퍼런스 데이터를 다른 위치에 패딩시킬 수 있다.

[0015] 상기 제2 단말기는 상기 암호화된 데이터를 NFC의 P2P(Peer-to-Peer)를 이용하여 전송할 수 있다.

[0016] 상기 제2 단말기는 상기 암호화된 데이터를 클라우드 서버에 저장할 수 있다.

[0017] 또한, 본 발명의 다른 실시예에 따른 데이터 공유 시스템은, 각각 데이터 공유 어플리케이션이 탑재되어 있는 정보 요청자의 제1 단말기와 정보 제공자의 제2 단말기를 포함하며, 상기 데이터 공유 어플리케이션의 실행에 의하여 상기 제1 단말기와 제2 단말기 간에 암호화된 데이터를 공유하는 데이터 공유 시스템이고, 상기 제2 단말기가 상기 제1 단말기로부터 원하는 데이터의 공유 요청과 함께 제1 암호화 정보를 수신하여 상기 제1 암호화 정보에 포함된 제1 단말기의 암호화 키를 복원한 후, 상기 복원된 암호화 키와 상기 제1 단말기로부터 공유 요청된 데이터를 암호화하여 상기 제1 단말기로 전송하며, 상기 제1 단말기가 상기 제2 단말기로부터 전송된 암호화된 데이터에 포함된 암호화 키와 상기 제1 단말기의 암호화 키를 비교한 후, 각각의 암호화 키가 일치하는 경우 상기 암호화된 데이터를 복호화할 수 있다.

[0018] 상기 제2 단말기는 상기 제1 단말기와 데이터를 송수신하는 제2 통신부; 상기 제1 단말기로부터 요청된 데이터의 공유 여부를 결정하는 공유 여부 결정부; 상기 제1 단말기로부터 수신된 제1 암호화 정보를 분석하는 암호화 정보 분석부; 상기 제1 암호화 정보의 분석 결과에 따라 암호화 명령을 생성하는 암호화 명령 생성부; 상기 제1 암호화 정보에 포함된 암호화키와 상기 제1 단말기로부터 공유 요청된 데이터를 암호화하여 데이터를 생성하는 암호화 데이터 생성부; 및 상기 데이터 공유 어플리케이션을 탑재하고, 상기 데이터 공유 어플리케이션의 실행

에 의하여 상기 각각의 구성요소들의 동작을 제어하는 제2 제어부를 포함할 수 있다.

[0019] 상기 암호화 데이터 생성부는 상기 암호화된 데이터에 매번 다른 레퍼런스 데이터를 다른 위치에 패딩시킬 수 있다.

[0020] 상기 제2 통신부는 상기 암호화된 데이터를 NFC의 P2P(Peer-to-Peer)를 이용하여 전송할 수 있다.

[0021] 상기 제1 단말기는 상기 제2 단말기와 데이터를 송수신하는 제1 통신부; 상기 제2 단말기에 원하는 데이터에 대한 공유를 요청하는 데이터 공유 요청부; 상기 제2 단말기로부터 전송된 암호화된 데이터를 분석하는 암호화 데이터 분석부; 상기 암호화된 데이터의 분석 결과에 따라 복호화 명령을 생성하는 복호화 명령 생성부; 상기 암호화된 데이터에 포함된 암호화 키와 상기 제1 단말기의 암호화 키를 비교하는 일련번호 비교부; 상기 암호화된 데이터에 포함된 암호화 키와 상기 제1 단말기의 암호화 키가 일치하는 경우, 상기 암호화된 데이터를 복호화하는 데이터 복호화부; 및 상기 데이터 공유 어플리케이션을 탑재하고, 상기 데이터 공유 어플리케이션의 실행에 의하여 상기 각각의 구성요소들의 동작을 제어하는 제1 제어부를 포함할 수 있다.

[0022] 상기 데이터 공유 요청부는 상기 원하는 데이터의 공유 요청을 SMS로 전송할 수 있다.

[0023] 상기 데이터 공유 요청부는 상기 데이터 공유 어플리케이션에 의하여 자동으로 원하는 데이터의 공유 요청을 SMS로 전송할 수 있다.

[0024] 상기 암호화 키는 상기 제1 단말기에 포함된 칩 일련번호를 포함할 수 있다.

[0025] 상기 암호화된 데이터는 변형 키를 생성하는 레퍼런스 데이터를 포함할 수 있다.

[0026] 상기 암호화된 데이터는 아이디, 칩 일련번호, 위치정보, 및 상기 제1 단말기의 공유 요청 데이터를 포함할 수 있다.

[0027] 상기 암호화된 데이터를 수신하여 저장하는 클라우드 서버를 더 포함하고, 상기 제1 단말기는 상기 클라우드 서버와 데이터를 송수신하는 제3 통신부를 더 포함하며, 상기 제2 단말기는 상기 클라우드 서버와 데이터를 송수신하는 제4 통신부를 더 포함할 수 있다.

발명의 효과

[0028] 본 발명의 일 실시예에 따른 데이터 공유 방법 및 이를 이용한 데이터 공유 시스템은 정보를 제공하는 제공자가 정보를 요청하는 수신자에게만 데이터를 전송함으로써, 서버를 통하지 않고도 개인 대 개인으로 암호화 데이터를 공유할 수 있다.

도면의 간단한 설명

[0029] 도 1은 본 발명의 일 실시예에 따른 데이터 공유 시스템을 개략적으로 나타내는 도면이다.

도 2는 도 1의 제1 단말기를 나타내는 블록도이다.

도 3은 도 1의 제2 단말기를 나타내는 블록도이다.

도 4는 본 발명의 다른 실시예에 따른 데이터 공유 방법을 나타내는 순서도이다.

도 5는 도 4의 제2 단말기의 동작을 구체적으로 나타내는 순서도이다.

도 6은 도 4의 제1 단말기의 동작을 구체적으로 나타내는 순서도이다.

도 7a 및 7b는 제2 단말기에 의하여 암호화된 데이터의 일 예를 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0030] 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있을 정도로 본 발명의 바람직한 일 실시예를 첨부된 도면을 참조하여 상세하게 설명하면 다음과 같다.

[0031] 도 1은 본 발명의 일 실시예에 따른 데이터 공유 시스템을 개략적으로 나타내는 도면이고, 도 2는 도 1의 제1 단말기를 나타내는 블록도이며, 도 3은 도 1의 제2 단말기를 나타내는 블록도이다.

[0032] 도 1 내지 도 3을 참조하면, 본 발명의 일 실시예에 따른 데이터 공유 시스템은 각각 데이터 공유 어플리케이션이 탑재되어 있는 정보 요청자의 제1 단말기(100)와 정보 제공자의 제2 단말기(200)를 포함하고, 데이터 공유 어플리케이션의 실행에 의하여 제1 단말기(100)와 제2 단말기(200) 간에 암호화된 데이터를 공유하는 시스템이다.

[0033] 본 발명에서의 제1 단말기(100) 및 제2 단말기(200)는 서로 유무선 통신망을 통하여 연결되도록 각각의 통신 인터페이스를 구비하는 통신 단말기이다. 상기 제1 단말기(100) 및 제2 단말기(200)는 PDA(personal digital assistant), 휴대폰, 스마트폰 등과 같이 무선 인터넷이 가능한 다양한 휴대용 단말기들(handheld terminal) 뿐만 아니라 데스크탑 컴퓨터, 노트북과 같은 퍼스널 컴퓨터가 사용될 수 있으나, 바람직하게는 어플리케이션 구동이 가능한 스마트폰일 수 있다. 또한, 상기 유무선 통신망은 이더넷(Ethernet) 모듈 또는 와이파이(Wi-Fi) 모듈일 수 있고, 또한 유선으로 접속할 수 있는 TCP/IP 프로토콜과 무선으로 접속할 수 있는 WAP 프로토콜 등을 사용한 인터넷망을 포함할 수 있으나, 본 발명에서는 유무선 통신망의 종류에 대하여 한정하는 것은 아니다.

[0034] 상기 제1 단말기(100) 및 제2 단말기(200)는 데이터 공유 서비스를 제공하는 데이터 공유 어플리케이션을 저장하고 있다. 즉, 상기 제1 단말기(100) 및 제2 단말기(200)는 데이터 공유 서비스 제공 업체 서버(미도시)로부터 데이터 공유 서비스를 수행할 수 있는 데이터 공유 어플리케이션을 다운로드받아 저장하고 있다.

[0035] 상기 제1 단말기(100)는 제2 단말기(200)에 원하는 데이터의 공유를 요청할 수 있다. 이때, 상기 제1 단말기(100)는 원하는 데이터의 공유 요청과 함께 제1 암호화 정보를 제2 단말기(200)에 전송한다. 상기 제1 암호화 정보는 제1 단말기(100)의 칩 일련번호일 수 있다.

[0036] 또한, 상기 제1 단말기(100)는 제2 단말기(200)로부터 전송된 암호화된 데이터에 포함된 암호화 키와 제1 단말기(100)의 암호화 키를 비교한 후, 각각의 암호화 키가 일치하는 경우 암호화된 데이터를 복호화할 수 있다.

[0037] 이러한 동작을 구현하기 위하여, 상기 제1 단말기(100)는 제1 통신부(110), 데이터 공유 요청부(120), 암호화 데이터 분석부(130), 복호화 명령 생성부(140), 일련번호 비교부(150), 데이터 복호화부(160) 및 제1 제어부(170)를 포함할 수 있다.

[0038] 상기 제1 통신부(110)는 제2 단말기(200)와 데이터를 송수신하는 통신 인터페이스이다. 상기 제1 통신부(110)는 제2 단말기(200)와 와이파이, 3G, 4G, LTE 등의 무선통신망을 통하여 연결될 수 있다.

[0039] 상기 데이터 공유 요청부(120)는 제2 단말기(200)에 원하는 데이터에 대한 공유를 요청한다. 이러한 데이터 공유 요청부(120)는 원하는 데이터의 공유 요청을 SMS로 전송할 수 있다. 또한, 상기 데이터 공유 요청부(120)는 데이터 공유 어플리케이션에 의하여 자동으로 원하는 데이터의 공유 요청을 SMS로 전송할 수 있다.

[0040] 상기 암호화 데이터 분석부(130)는 제2 단말기(200)로부터 전송된 암호화된 데이터를 분석한다. 즉, 상기 암호화 데이터 분석부(130)는 제2 단말기(200)에 의하여 칩 일련번호를 이용한 암호화 키와 정보 요청자가 원하는 데이터를 암호화된 데이터를 수신하여 데이터 헤더 등을 분석한다.

[0041] 상기 복호화 명령 생성부(140)는 암호화된 데이터의 분석 결과에 따라 복호화 명령을 생성한다. 즉, 상기 복호화 명령 생성부(140)는 암호화 데이터 분석부(130)에 의하여 데이터 헤더 등이 정상인 것으로 판단되는 경우 복호화 명령을 생성하게 된다.

[0042] 상기 일련번호 비교부(150)는 암호화된 데이터에 포함된 암호화 키와 제1 단말기(100)의 암호화 키를 비교한다. 즉, 상기 일련번호 비교부(150)는 제2 단말기(200)에 의하여 암호화된 데이터에 포함되어 있는 암호화 키에서의 칩 일련번호와 제1 단말기(100)에 저장되어 있는 칩 일련번호가 일치하는지 여부를 비교 판단한다. 상기 암호화 키는 제1 단말기(100)에 구비된 스마트 카드의 칩 일련번호일 수 있다.

[0043] 상기 데이터 복호화부(160)는 암호화된 데이터에 포함된 암호화 키와 제1 단말기(100)의 암호화 키가 일치하는 경우, 암호화된 데이터를 복호화한다.

[0044] 상기 제1 제어부(170)는 데이터 공유 어플리케이션을 탑재하고, 정보 요청자의 조작에 의한 데이터 공유 어플리케이션의 실행에 의하여 각각의 구성요소들(즉, 제1 통신부(110), 데이터 공유 요청부(120), 암호화 데이터 분석부(130), 복호화 명령 생성부(140), 일련번호 비교부(150), 데이터 복호화부(160))의 동작을 제어한다.

[0045] 상기 제2 단말기(200)는 제1 단말기(100)로부터 원하는 데이터의 공유 요청과 함께 제1 암호화 정보를

수신한다. 또한, 상기 제2 단말기(200)는 제1 암호화 정보에 포함된 제1 단말기(100)의 암호화 키를 복원한 후, 복원된 암호화 키와 제1 단말기(100)로부터 공유 요청된 데이터를 암호화하여 제1 단말기(100)로 전송한다.

[0046] 이러한 동작을 구현하기 위하여, 상기 제2 단말기(200)는 제2 통신부(210), 공유 여부 결정부(220), 암호화 정보 분석부(230), 암호화 명령 생성부(240), 암호화 데이터 생성부(250) 및 제2 제어부(260)를 포함할 수 있다.

[0047] 상기 제2 통신부(210)는 제1 단말기(100)와 데이터를 송수신하는 통신 인터페이스이다. 상기 제2 통신부(210)는 제1 단말기(100)와 와이파이, 3G, 4G, LTE 등의 무선통신망을 통하여 연결될 수 있다. 본 발명에서의 제2 통신부(210)는 암호화된 데이터를 NFC의 P2P(Peer-to-Peer)를 이용하여 제1 단말기(100)로 전송할 수 있다.

[0048] 상기 공유 여부 결정부(220)는 제1 단말기(100)로부터 요청된 데이터의 공유 여부를 결정한다. 상기 정보 제공자가 제1 단말기(100)로부터 요청된 데이터의 공유를 원하지 않는 경우에는 요청된 데이터를 일반 데이터를 암호화하는 방식으로 암호화하게 된다.

[0049] 상기 암호화 정보 분석부(230)는 제1 단말기(100)로부터 수신된 제1 암호화 정보를 분석한다. 즉, 상기 암호화 정보 분석부(230)는 제1 암호화 정보에 포함된 칩 일련번호 정보를 조회하고, 해당 위치 정보를 생성한다.

[0050] 상기 암호화 명령 생성부(240)는 제1 암호화 정보의 분석 결과에 따라 암호화 명령을 생성한다. 즉, 상기 암호화 명령 생성부(240)는 제1 암호화 정보에 포함된 칩 일련번호가 조회되어 해당 위치 정보가 생성되는 경우, 암호화 명령을 생성한다.

[0051] 상기 암호화 데이터 생성부(250)는 제1 암호화 정보에 포함된 암호화키와 제1 단말기(100)로부터 공유 요청된 데이터를 암호화하여 데이터를 생성한다. 상기 암호화된 데이터는 변형 키를 생성하는 레퍼런스 데이터를 포함할 수 있다. 상기 암호화된 데이터는 아이디, 칩 일련번호, 위치정보, 및 상기 제1 단말기(100)의 공유 요청 데이터를 포함할 수 있다. 또한, 상기 암호화 데이터 생성부(250)는 상기 암호화된 데이터에 매번 다른 레퍼런스 데이터를 다른 위치에 패딩시켜 세션 키 사용효과를 가질 수 있다. 이와 같이, 상기 암호화 데이터 생성부(250)에 의하여 암호화가 정상적으로 동작되면 암호화된 데이터에 헤더를 구성하고, 제2 통신부(210)를 통하여 헤더가 부가된 암호화 데이터를 제1 단말기(100)로 전송하게 된다.

[0052] 예를 들어, 상기 암호화 데이터 생성부(250)는 아래 표 1과 같이 암호화 키를 직접 노출시키지 않고, 2단계의 과정을 거쳐 암호화된 공유 데이터를 생성할 수 있다.

표 1

[0053]

ID(2바이트)	칩 일련번호(4바이트)	위치정보(1바이트)	데이터 n바이트
데이터 구분자 0xFFFF	정보 요청자의 스마트카드 일련번호	칩 일련번호 하위 2바이트가 패딩될 위치 지정	암호화된 데이터

[0054] 즉, 도 7b에 도시된 바와 같이, 도 7a의 마스터 키 배열에 위치정보 0x08의 위치에 레퍼런스 데이터로 칩 일련번호 2바이트 0x1122를 패딩시킬 수 있다.

[0055] 상기 제2 제어부(260)는 데이터 공유 어플리케이션을 탑재하고, 정보 제공자의 조작에 의하여 데이터 공유 어플리케이션의 실행에 의하여 각각의 구성요소들(즉, 제2 통신부(210), 공유 여부 결정부(220), 암호화 정보 분석부(230), 암호화 명령 생성부(240), 암호화 데이터 생성부(250))의 동작을 제어한다.

[0056] 한편, 본 데이터 공유 시스템은 제2 단말기(200)에 의하여 암호화된 데이터를 수신하여 저장하는 클라우드 서버를 더 포함할 수 있다.

[0057] 이러한 경우에, 상기 제1 단말기(100)는 클라우드 서버와 데이터를 송수신하는 제3 통신부를 더 포함할 수 있고, 상기 제2 단말기(200) 또한 클라우드 서버와 데이터를 송수신하는 제4 통신부를 더 포함할 수 있다.

[0058] 도 4는 본 발명의 다른 실시예에 따른 데이터 공유 방법을 나타내는 순서도이고, 도 5는 도 4의 제2 단말기(200)의 동작을 구체적으로 나타내는 순서도이며, 도 6은 도 4의 제1 단말기(100)의 동작을 구체적으로 나타내는 순서도이다.

[0059] 도 4를 참조하면, 본 발명의 다른 실시예에 따른 데이터 공유 방법은 도 1 내지 도 3의 데이터 공유 시스템을 이용하여 정보 요청자의 제1 단말기(100)와 정보 제공자의 제2 단말기(200) 간에 암호화된 데이터를 공유하는

방법이다.

[0060] 보다 구체적으로는, 본 발명의 다른 실시예에 따른 데이터 공유 방법은 제2 단말기(200)가 제1 단말기(100)로부터 원하는 데이터의 공유 요청과 함께 제1 암호화 정보를 수신하는 제1 단계(S10)와, 제1 단계(S10)에서 수신된 제1 암호화 정보에 포함된 제1 단말기(100)의 암호화 키를 복원하는 제2 단계(S20)와, 제2 단계(S20)에서 복원된 암호화 키와 제1 단말기(100)로부터 공유 요청된 데이터를 암호화하여 제1 단말기(100)로 전송하는 제3 단계(S30)와, 제1 단말기(100)가 제2 단말기(200)로부터 전송된 암호화된 데이터에 포함된 암호화 키와 제1 단말기(100)의 암호화 키를 비교하는 제4 단계(S40)와, 각각의 암호화 키가 일치하는 경우 암호화된 데이터를 복호화하는 제5 단계(S50)를 포함할 수 있다.

[0061] 상기 제1 단말기(100)와 제2 단말기(200)는 각각 데이터 공유 어플리케이션이 탑재되어 있고, 제1 단계(S10) 내지 제5 단계(S50)는 데이터 공유 어플리케이션의 실행에 의하여 수행될 수 있다.

[0062] 본 데이터 공유 방법을 각각의 단말기별로 구분하여 설명하자면, 우선 상기 제2 단말기(200)는 도 5에 도시된 바와 같이, 제1 단말기(100)로부터 데이터 공유 요청을 받아 데이터 공유 전송 여부를 결정(S100, S101)하고, 데이터 공유 전송이 결정된 경우 제1 암호화 정보에 포함된 칩의 일련번호를 조회(S110)한 후 암호화 데이터에 레퍼런스 데이터가 패딩될 위치 정보를 생성(S120)하게 된다. 그런 다음, 상기 제2 단말기(200)는 암호화 명령을 생성(S130)하고, 암호화가 성공(S140)되면 암호화된 데이터의 헤더를 구성(S150)하여 제1 단말기(100)로 전송(S160)하게 된다.

[0063] 상기 제1 단말기(100)는 제2 단말기(200)로부터 암호화된 데이터를 다운로드(S200)하여 그 데이터에 포함된 데이터의 헤더를 분석(S210)하고, 분석 결과 헤더가 정상(S220)이면 복호화 명령을 생성(S230)하게 된다. 그런 다음, 상기 제1 단말기(100)는 암호화된 데이터에 포함된 칩 일련번호와 제1 단말기(100)에 저장된 칩 일련번호를 비교(S240)하여 일치하는 경우 데이터 복호화를 수행(S250)하게 된다.

[0064] 따라서, 본 발명에서는 개인 대 개인으로 암호화 데이터를 공유할 수 있고, 지정된 사람만이 암호화된 데이터를 복호화할 수 있으며, 레퍼런스 데이터만을 이용하여 세션키를 생성함으로써, 효율적으로 데이터 공유를 수행할 수 있게 된다. 나아가, 본 발명에서는 암호화 키 관리를 위한 별도의 관리 서버가 필요없게 되어 사용자 및 관리자의 편의성을 향상시킬 수 있다.

[0065] 이상에서 설명한 것은 본 발명에 의한 데이터 공유 방법 및 이를 이용한 데이터 공유 시스템을 실시하기 위한 하나의 실시예에 불과한 것으로서, 본 발명은 상기 실시예에 한정되지 않고, 이하의 특허청구범위에서 청구하는 바와 같이 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변경 실시가 가능한 범위까지 본 발명의 기술적 정신이 있다고 할 것이다.

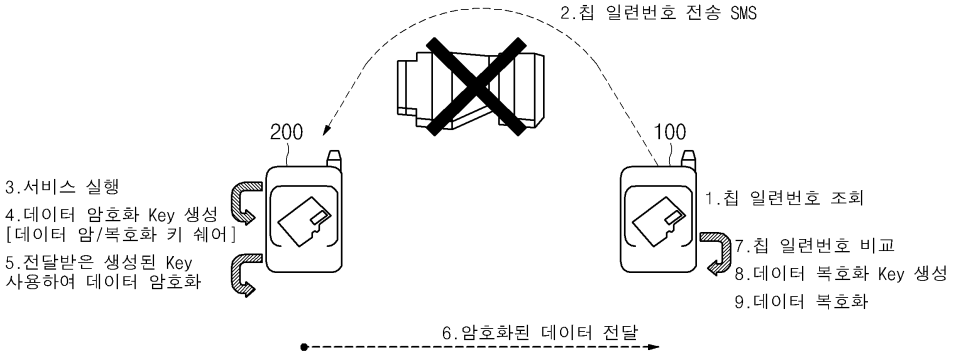
부호의 설명

[0066]

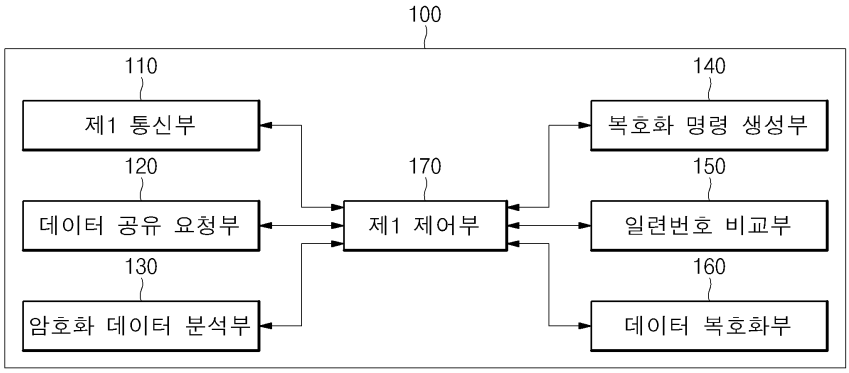
100: 제1 단말기	110: 제1 통신부
120: 데이터 공유 요청부	130: 암호화 데이터 분석부
140: 복호화 명령 생성부	150: 일련번호 비교부
160: 데이터 복호화부	170: 제1 제어부
200: 제2 단말기	210: 제2 통신부
220: 공유 여부 결정부	230: 암호화 정보 분석부
240: 암호화 명령 생성부	250: 암호화 데이터 생성부
260: 제2 제어부	

도면

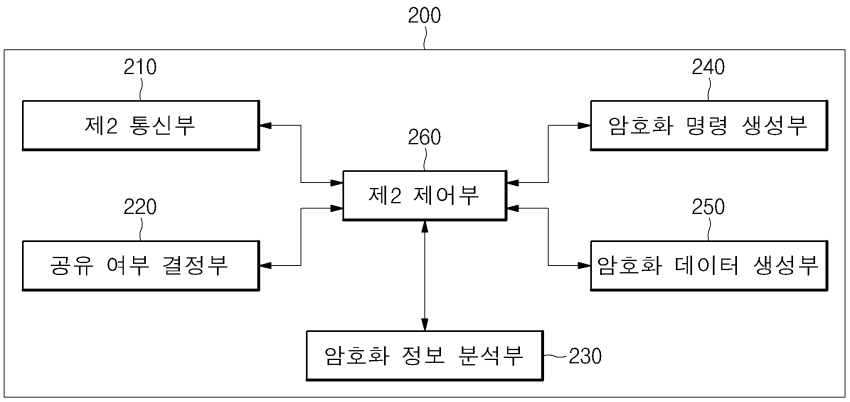
도면1



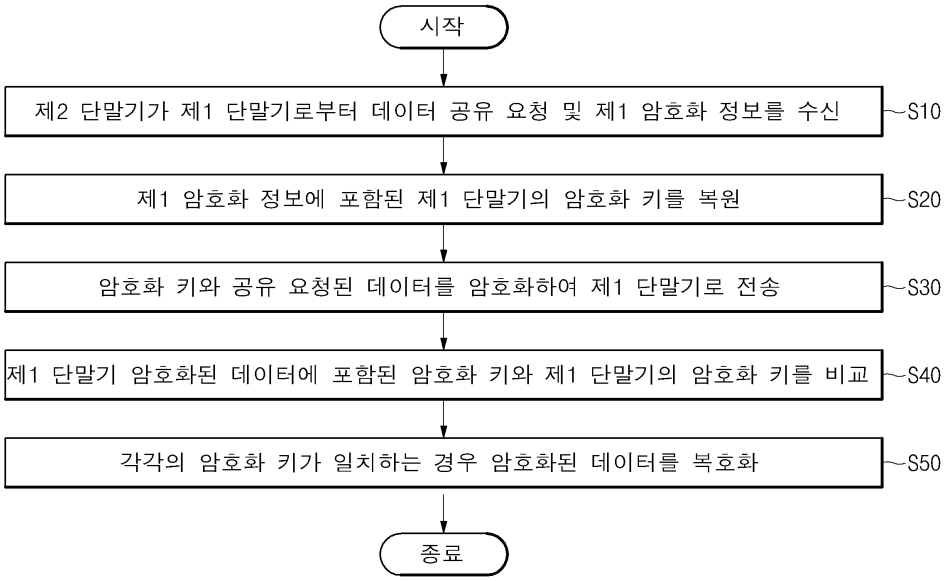
도면2



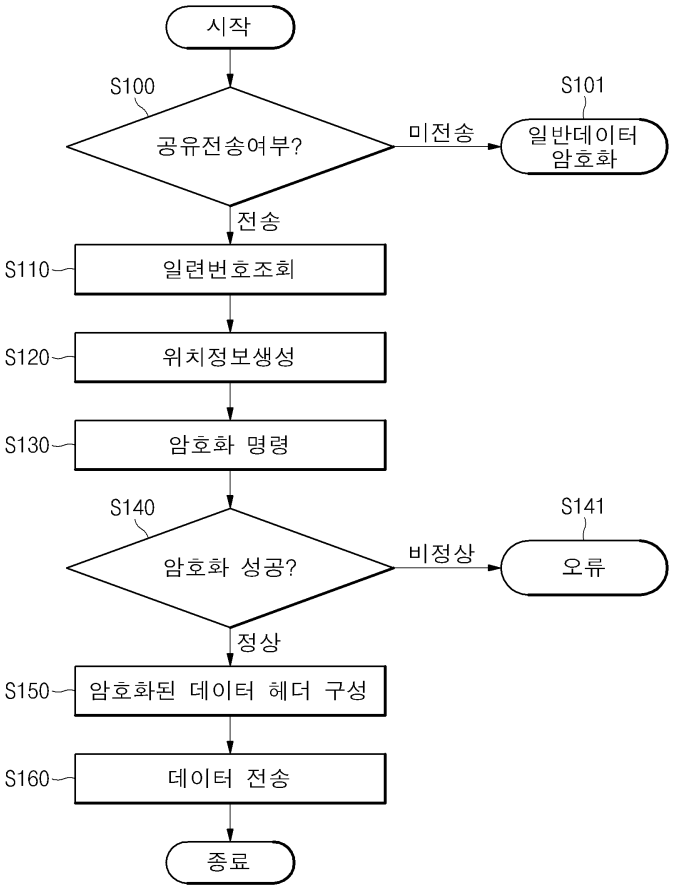
도면3



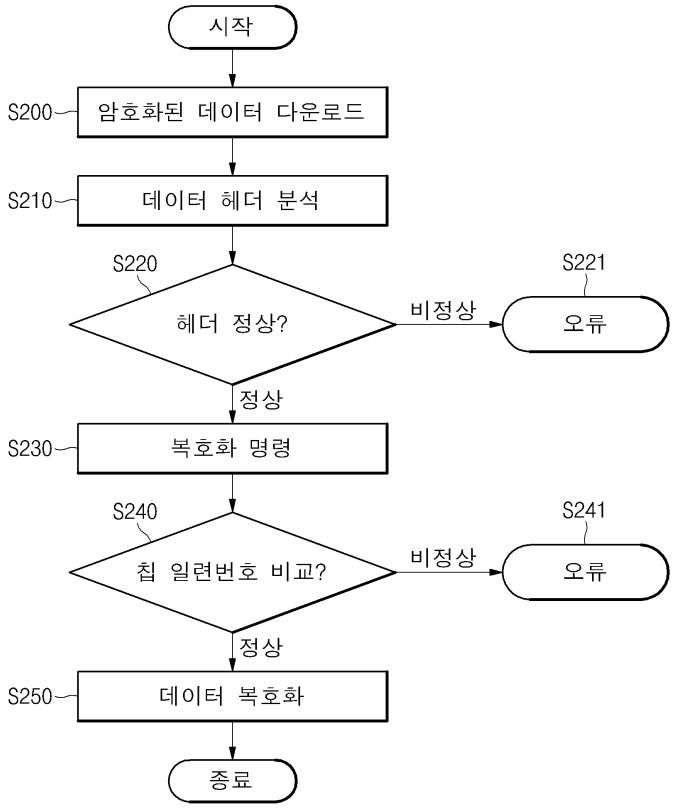
도면4


시작
제2 단말기가 제1 단말기로부터 데이터 공유 요청 및 제1 암호화 정보를 수신
S10
제1 암호화 정보에 포함된 제1 단말기의 암호화 키를 복원
S20
암호화 키와 공유 요청된 데이터를 암호화하여 제1 단말기로 전송
S30
제1 단말기 암호화된 데이터에 포함된 암호화 키와 제1 단말기의 암호화 키를 비교
S40
각각의 암호화 키가 일치하는 경우 암호화된 데이터를 복호화
S50
종료

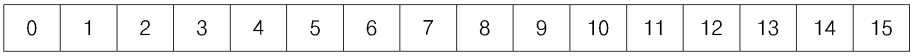
도면5


시작
S100
공유전송여부?
미전송
S101
일반데이터 암호화
전송
S110
일련번호조회
S120
위치정보생성
S130
암호화 명령
S140
암호화 성공?
비정상
S141
오류
정상
S150
암호화된 데이터 헤더 구성
S160
데이터 전송
종료

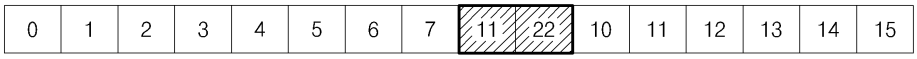
도면6



도면7a



도면7b



레퍼런스 데이터 패딩