



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0053206
(43) 공개일자 2015년05월15일

(51) 국제특허분류(Int. Cl.)
H04N 21/266 (2011.01) H04N 21/6334 (2011.01)
(21) 출원번호 10-2013-0156232
(22) 출원일자 2013년12월16일
심사청구일자 2013년12월16일
(30) 우선권주장
1020130135039 2013년11월07일 대한민국(KR)

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
홍충선
경기 용인시 수지구 상현로 30-10, 233동 101호 (상현동, 성원3차상떼빌아파트)
조용준
경기 수원시 영통구 청명로59번길 54, 103호 (영통동)
(74) 대리인
서재승

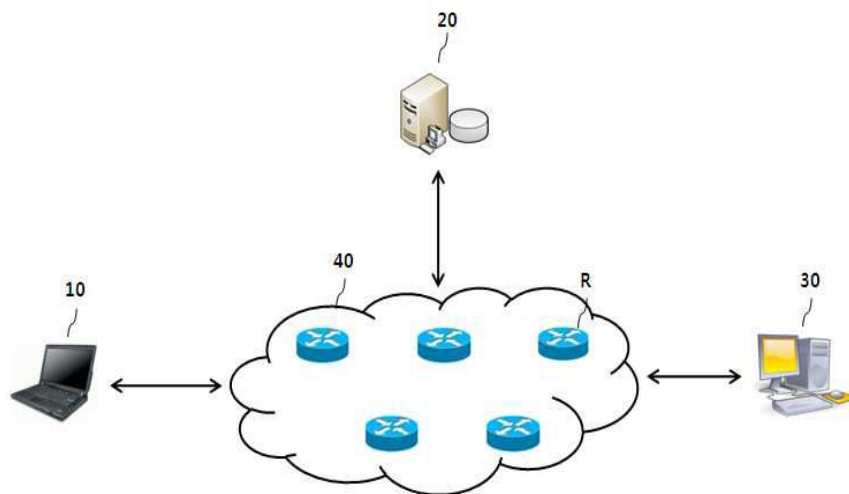
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 콘텐츠 기반 네트워크의 콘텐츠 송신 방법

(57) 요약

본 발명은 콘텐츠 기반 네트워크(content centric network, CCN)에서 사용자에게 요청 콘텐츠를 제공하는 방법에 관한 것으로, 보다 구체적으로 사용자 단말기로부터 수신한 콘텐츠 요청 메시지에 기초하여 사용자 인증 및 요청 콘텐츠에 대한 사용자 접속 권한을 판단하며 요청 콘텐츠에 대한 사용자 접속 권한이 존재하는 사용자에게만 요청 콘텐츠를 제공할 수 있는 콘텐츠 기반의 데이터 송신 방법에 관한 것이다.

대표도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호 1415128860

부처명 미래창조과학부

연구관리전문기관 정보통신산업진흥원

연구사업명 정보통신기술인력양성사업

연구과제명 스마트그리드 기술연구

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2013.01.01 ~ 2013.12.31

명세서

청구범위

청구항 1

사용자 단말기로부터 사용자 개인키(UK_{pri})로 암호화된 사용자 공개키(UK_{pub})와 난수($nonce$), 암호화되지 않은 사용자 공개키, 요청 콘텐츠 식별자를 구비하는 콘텐츠 요청 메시지를 수신하는 단계;

상기 암호화되지 않은 사용자 공개키를 이용하여 상기 콘텐츠 요청 메시지를 복호화하여 사용자를 인증하는 사용자 인증 단계;

상기 사용자 공개키, 난수 및 요청 콘텐츠 식별자를 구비하는 접속 권한 요청 메시지를 생성하고, 상기 접속 권한 요청 메시지를 인증 서버로 송신하는 접속 권한 요청 메시지의 송신 단계;

상기 접속 권한 요청 메시지에 응답하여 인증 서버로부터 수신한 접속 권한 응답 메시지에 기초하여 요청 콘텐츠에 대한 사용자의 접속 권한을 인증하는 인증 단계; 및

상기 요청 콘텐츠에 대한 사용자 접속 권한의 인증 결과에 기초하여, 상기 요청 콘텐츠 식별자에 해당하는 콘텐츠를 상기 사용자 단말기로 송신하는 콘텐츠 송신 단계를 포함하는 것을 특징으로 하는 콘텐츠 기반 네트워크의 콘텐츠 송신 방법.

청구항 2

제 1 항에 있어서, 상기 콘텐츠 기반 네트워크의 콘텐츠 송신 방법은

상기 요청 콘텐츠 식별자에 해당하는 요청 콘텐츠가 라우터의 캐시에 저장되어 있는지 판단하는 판단 단계를 더 포함하며,

상기 요청 콘텐츠 식별자에 해당하는 요청 콘텐츠가 상기 라우터의 캐시에 저장되어 있는 경우, 상기 사용자 인증 단계, 상기 접속 권한 요청 메시지의 송신 단계 및 상기 콘텐츠 송신 단계를 수행하는 것을 특징으로 하는 콘텐츠 기반 네트워크의 콘텐츠 송신 방법.

청구항 3

제 2 항에 있어서, 상기 콘텐츠 기반 네트워크의 콘텐츠 송신 방법은

상기 요청 콘텐츠 식별자에 해당하는 요청 콘텐츠가 상기 라우터의 캐시에 저장되어 있지 않은 경우 인접 라우터로 상기 콘텐츠 요청 메시지를 송신하는 것을 특징으로 하는 콘텐츠 기반 네트워크의 콘텐츠 송신 방법.

청구항 4

제 2 항 또는 제 3 항에 있어서, 상기 접속 권한 요청 메시지의 송신 단계는

상기 콘텐츠 요청 메시지의 요청 콘텐츠 식별자 및 사용자 공개키를 구비하는 접속 권한 요청 메시지를 생성하는 단계;

요청 콘텐츠 식별자에 매핑되어 있는 인증 서버 주소를 저장하고 있는 매핑 테이블에서 상기 요청 콘텐츠 식별자에 매핑되어 있는 인증 서버 주소를 검색하는 단계; 및

상기 생성한 접속 권한 요청 메시지를 상기 검색한 인증 서버 주소로 송신하는 단계를 포함하는 것을 특징으로 하는 콘텐츠 기반 네트워크의 콘텐츠 송신 방법.

청구항 5

제 4 항에 있어서,

상기 사용자 개인키(UK_{pri})로 암호화된 사용자 공개키(UK_{pub})와 난수($nonce$), 암호화되지 않은 사용자 공개키는 상기 콘텐츠 요청 메시지의 인증 필드에 구비되어 있는 것을 특징으로 하는 콘텐츠 기반 네트워크의 콘텐츠 송

신 방법.

청구항 6

제 4 항에 있어서,

상기 사용자 개인키와 상기 사용자 공개키는 사용자가 상기 인증 서버에 등록시 상기 인증 서버에서 상기 사용자
자로 제공하는 것을 특징으로 하는 콘텐츠 기반네트워크의 콘텐츠 송신 방법.

청구항 7

제 6 항에 있어서,

상기 인증 서버는 콘텐츠 제공 서버로부터 상기 요청 콘텐츠에 사용자 접속 권한에 대한 정보를 수신하여 저장
하고 있으며, 상기 사용자 접속 권한에 대한 정보를 이용하여 상기 접속 권한 응답 메시지를 생성하는 것을 특
징으로 하는 콘텐츠 기반 네트워크의 콘텐츠 송신 방법.

청구항 8

송수신부;

상기 송수신부를 통해 사용자 단말기로부터 수신한 콘텐츠 요청 메시지의 인증 필드를 복호화하여 사용자를 인
증하는 사용자 인증부;

상기 콘텐츠 요청 메시지의 요청 콘텐츠 식별자 및 사용자 공개키를 구비하는 접속 권한 요청 메시지를 생성하
고, 상기 접속 권한 요청 메시지에 응답하여 인증 서버로부터 수신한 접속 권한 응답 메시지에 기초하여 요청
콘텐츠에 대한 사용자의 접속 권한을 인증하는 콘텐츠 인증부; 및

상기 콘텐츠 인증부의 인증 결과에 기초하여 상기 요청 콘텐츠 식별자에 해당하는 요청 콘텐츠를 상기 사용자
단말기로 제공하는 콘텐츠 제공부를 포함하는 것을 특징으로 하는 콘텐츠 기반 네트워크의 라우터.

청구항 9

제 8 항에 있어서, 상기 콘텐츠 기반 네트워크의 라우터는

상기 요청 콘텐츠 식별자에 해당하는 요청 콘텐츠가 상기 라우터 캐시에 저장되어 있는지 판단하는 판단부를 더
포함하는 것을 특징으로 하는 콘텐츠 기반 네트워크의 라우터.

청구항 10

제 9 항에 있어서,

상기 판단부는 상기 요청 콘텐츠 식별자에 해당하는 요청 콘텐츠가 상기 라우터의 캐시에 저장되어 있지 않은
경우 상기 송수신부를 통해 인접 라우터로 상기 콘텐츠 요청 메시지를 송신하는 것을 특징으로 하는 콘텐츠 기
반 네트워크의 라우터.

청구항 11

제 9 항에 있어서, 상기 콘텐츠 인증부는

상기 콘텐츠 요청 메시지의 요청 콘텐츠 식별자 및 사용자 공개키를 구비하는 접속 권한 요청 메시지를 생성하
는 메시지 생성부;

상기 요청 콘텐츠 식별자에 매핑되어 있는 인증 서버 주소를 저장하고 있는 매핑 테이블;

상기 요청 콘텐츠 식별자에 매핑되어 있는 인증 서버 주소를 상기 매핑 테이블에서 검색하는 인증 서버 검색부;
및

상기 생성한 접속 권한 요청 메시지를 상기 검색한 인증 서버 주소로 송신하며, 상기 인증 서버로부터 수신한
접속 권한 응답 메시지에 기초하여 요청 콘텐츠에 대한 사용자 접속 권한을 인증하는 인증부를 포함하는 것을
특징으로 콘텐츠 기반 네트워크의 라우터.

청구항 12

제 8 항 내지 제 11 항 중 어느 한 항에 있어서,

상기 인증 필드에는 사용자 개인키(UK_{pri})로 암호화된 사용자 공개키(UK_{pub})와 난수(nonce), 암호화되지 않은 사용자 공개키가 구비되어 있는 것을 특징으로 하는 콘텐츠 기반 네트워크의 라우터.

청구항 13

제 12 항에 있어서, 상기 사용자 인증부는

상기 암호화되지 않은 사용자 공개키를 이용하여 상기 사용자 개인키(UK_{pri})로 암호화된 사용자 공개키(UK_{pub})와 난수(nonce)를 복호화하고, 복호화한 사용자 공개키와 난수가 각각 상기 암호화되지 않은 사용자 공개키 및 상기 라우터가 공유하는 난수와 일치하는지 여부로 사용자를 인증하는 것을 특징으로 하는 콘텐츠 기반 네트워크의 라우터.

청구항 14

제 12 항에 있어서,

상기 접속 권한 요청 메시지는 상기 사용자 공개키, 상기 요청 콘텐츠 식별자 및 상기 난수를 구비하도록 생성되는 것을 특징으로 하는 콘텐츠 기반 네트워크의 라우터.

발명의 설명

기술 분야

[0001]

본 발명은 콘텐츠 기반 네트워크(content centric network, CCN)에서 사용자에게 요청 콘텐츠를 제공하는 방법과 관련한 것으로, 보다 구체적으로 사용자 단말기로부터 수신한 콘텐츠 요청 메시지에 기초하여 사용자 인증 및 요청 콘텐츠에 대한 사용자 접속 권한을 판단하며 요청 콘텐츠에 대한 사용자 접속 권한이 존재하는 사용자에게만 요청 콘텐츠를 제공할 수 있는 콘텐츠 기반의 데이터 송신 방법에 관한 것이다.

배경 기술

[0002]

지금까지 널리 사용되고 있는 인터넷은 IP 주소를 이용하여 송신자와 수신자 사이의 1:1 구조로 서비스를 요청하고 제공받는 구조이다. 그러나 인터넷 고화질 TV, 인터넷 음성/화성 통신, 인터넷 원격 제어, 사물통신(Internet of Things:IoT) 등 인터넷을 이용한 다양한 분야와 용도가 계속되어 개발되어 사용되고 있는 현실에서 1:1구조의 인터넷은 주소체계 고갈로 인한 확장성, 보안성, 서비스 품질 보장성 등에서 한계점을 가진다.

[0003]

인터넷의 한계를 극복하기 위해 미래 인터넷에 관한 연구가 진행되고 있는데, 미래 인터넷에 관한 연구는 크게 점진적 접근(evolutionary approach)과 혁신적 접근(revolutionary approach)이 있을 수 있다. 점진적 접근이란 현재 인터넷의 기본 특성은 그대로 견지하는 한편 서비스의 연속성을 보장하면서 개선 방향을 모색하는 것이다. 반면에 혁신적 접근이란 현재 인터넷 기술에 속박되거나 구속되지 않으며 미래사회의 요구 사항을 완전하게 만족시킬 수 있는 네트워크 기술을 창조하는 것이다.

[0004]

혁신적 접근 방식 중 콘텐츠 중심 네트워크(Content Centric Network, CCN)는 종래 IP 주소를 이용하여 1:1 구조로 서비스를 요청하고 제공하는 구조 대신 콘텐츠 이름에 기반하여 서비스를 요청하고 제공하는 구조이다.

[0005]

콘텐츠 중심 네트워크는 다수의 라우터를 구비하는 네트워크와 네트워크에 접속되어 있는 사용자 단말기 및 콘텐츠 제공 서버를 구비하여 구성되어 있다. 사용자 단말기는 네트워크에 구비되어 있는 다수의 라우터 중 어느 하나의 라우터에 접속하며, 라우터로 콘텐츠 요청 메시지를 송신한다. 라우터는 콘텐츠 요청 메시지에서 요청 콘텐츠 식별자를 추출하고, 요청 콘텐츠 식별자에 기초하여 요청 콘텐츠가 라우터에 저장 등록되어 있는지 판단한다. 라우터에 요청 콘텐츠가 존재하지 않는 경우, 라우터는 네트워크의 인접 라우터로 콘텐츠 요청 메시지를 플러딩(flooding) 방식으로 전송하며 인접 라우터 중 요청 콘텐츠를 저장 등록하고 있는 주변 라우터 또는 요청 콘텐츠를 제공하는 콘텐츠 서버에 접속되어 있는 소스 라우터는 콘텐츠 요청 메시지를 전송받은 순서의 역순으로 요청 콘텐츠를 이동 단말기로 제공한다.

- [0006] 도 1과 도 2는 종래 콘텐츠 중심 네트워크에서 콘텐츠가 송수신되는 과정을 설명하기 위한 도면이다.
- [0007] 도 1을 참고로 보다 구체적으로 살펴보면, 사용자 단말기(1)는 요청 콘텐츠가 존재하는 경우, 요청 콘텐츠에 대한 정보를 구비하는 콘텐츠 요청 메시지(CR)를 접속 라우터(A)로 전송한다. 접속 라우터(A)는 요청 콘텐츠 식별자와 접속 라우터(A)에 저장 등록되어 있는 등록 콘텐츠 리스트를 비교하여 접속 라우터(A)에 요청 콘텐츠가 존재하는지 판단한다. 접속 라우터(A)에 요청 콘텐츠가 존재하지 않는 경우, 접속 라우터(A)는 인접 라우터(B)로 콘텐츠 요청 메시지를 전송하며, 인접 라우터(B)에서도 접속 라우터(A)와 동일하게 주변 라우터(B)에 요청 콘텐츠가 존재하는지 판단하여, 인접 라우터(B)에 요청 콘텐츠가 존재하지 않는 경우 인접 라우터(B)의 인접 라우터(C)로 콘텐츠 요청 메시지를 전송하며, 요청 콘텐츠가 인접 라우터(C)에 등록 저장되어 있지 않은 경우 인접 라우터(C)는 다시 인접 라우터(C)의 인접 라우터(D)로 콘텐츠 요청 메시지를 전송한다. 인접 라우터(D)는 요청 콘텐츠를 제공하는 콘텐츠 서버(30)가 접속되어 있는 소스 라우터로, 소스 라우터(D)는 콘텐츠 요청 메시지(CR)에 응답하여 요청 콘텐츠를 구비하는 콘텐츠 응답 메시지(CP)를 콘텐츠 요청 메시지(CR)의 수신 경로의 역경로로 전송한다. 즉, 콘텐츠 응답 메시지는 소스 라우터(D)로부터 주변 라우터(C), 주변 라우터(B) 및 접속 라우터(A)로 전송된다. 이때 콘텐츠 응답 메시지(CP)의 전송 경로에 위치하는 라우터들(B, C, D)는 콘텐츠 응답 메시지에 저장되어 있는 요청 콘텐츠를 각각 자신의 라우터에 등록 저장한다.
- [0008] 도 2에 도시되어 있는 바와 같이, 다른 사용자 단말기(4)로부터 동일한 콘텐츠에 대한 요청이 있는 경우, 요청 콘텐츠를 저장하고 있는 서버(3)로부터 요청 콘텐츠를 제공받는 것이 아니라, 요청 콘텐츠를 저장하고 있는 인접 라우터(C)로부터 직접 요청 콘텐츠를 제공받음으로써, 빠르게 요청 콘텐츠를 제공받을 수 있다.
- [0009] 위에서 설명한 종래 콘텐츠 기반 네트워크에서 요청 콘텐츠를 저장하고 있는 라우터는 사용자 단말기로부터 요청 콘텐츠 메시지를 수신하는 경우, 요청 콘텐츠에 대한 사용자의 접속 권한이 존재하는지를 판단하지 못하며, 모든 사용자에게 저장되어 있는 요청 콘텐츠를 제공한다.
- [0010] 그러나 IPTV와 같이 다양한 콘텐츠 중 불특정 사용자에게 제공되는 콘텐츠와 별도로 요청 콘텐츠에 대한 접속 권한을 가지는 사용자에게만 제공되는 콘텐츠를 구분하여 서비스하는 경우도 존재한다. 따라서 IPTV와 같이 콘텐츠 접속 권한으로 구분하여 사용자에게 콘텐츠를 제공하는 서비스에서 종래 콘텐츠 기반 네트워크를 적용하기 곤란하다는 문제점을 가진다.

발명의 내용

해결하려는 과제

- [0011] 본 발명은 위에서 언급한 종래 콘텐츠 기반 네트워크가 가지는 문제점을 해결하기 위한 것으로, 본 발명이 이루고자 하는 목적은 콘텐츠에 대한 사용자 접속 권한을 판단할 수 있는 콘텐츠 기반 네트워크의 콘텐츠 송신 방법을 제공하는 것이다.
- [0012] 본 발명이 이루고자 하는 다른 목적은 사용자가 요청 콘텐츠에 대한 사용자 접속 권한을 인증하는 인증 서버 주소를 라우터의 매핑 테이블에 설정하며, 설정한 인증 서버를 통해 요청 콘텐츠에 대한 사용자 접속 권한을 인증할 수 있는 콘텐츠 기반 네트워크의 콘텐츠 송신 방법을 제공하는 것이다.
- [0013] 본 발명이 이루고자 하는 또 다른 목적은 불특정 다수인에게 제공하는 콘텐츠와, 비용을 지불한 사용자 또는 권한이 있는 사용자에게만 제공하는 콘텐츠로 구분하여 콘텐츠를 제공하는 다양한 서비스에서 적용 가능한, 콘텐츠 기반 네트워크의 콘텐츠 송신 방법을 제공하는 것이다.

과제의 해결 수단

- [0014] 본 발명의 목적을 달성하기 위하여, 본 발명에 따른 콘텐츠 기반 네트워크에서의 콘텐츠 송신 방법은 사용자 단말기로부터 사용자 개인키(UK_{pri})로 암호화된 사용자 공개키(UK_{pub})와 난수(nonce), 암호화되지 않은 사용자 공개키, 요청 콘텐츠 식별자를 구비하는 콘텐츠 요청 메시지를 수신하는 단계와, 암호화되지 않은 사용자 공개키를 이용하여 콘텐츠 요청 메시지를 복호화하여 사용자를 인증하는 사용자 인증 단계와, 사용자 공개키, 난수 및 요청 콘텐츠 식별자를 구비하는 접속 권한 요청 메시지를 생성하고 접속 권한 요청 메시지를 인증 서버로 송신하는 접속 권한 요청 메시지의 송신 단계와, 접속 권한 요청 메시지에 응답하여 인증 서버로부터 접속 권한 응답 메시지를 수신하는 경우 접속 권한 응답 메시지에 응답하여 요청 콘텐츠 식별자에 해당하는 콘텐츠를 사용자 단

말기로 송신하는 콘텐츠 송신 단계를 포함하는 것을 특징으로 한다.

- [0015] 바람직하게, 본 발명에 따른 콘텐츠 기반 네트워크의 콘텐츠 송신 방법은 요청 콘텐츠 식별자에 해당하는 요청 콘텐츠가 라우터의 캐시에 저장되어 있는지 판단하는 판단 단계를 더 포함하며, 요청 콘텐츠 식별자에 해당하는 요청 콘텐츠가 라우터의 캐시에 저장되어 있는 경우 사용자 인증 단계, 접속 권한 요청 메시지의 송신 단계 및 콘텐츠 송신 단계를 수행하는 것을 특징으로 한다.
- [0016] 여기서 요청 콘텐츠 식별자에 해당하는 요청 콘텐츠가 라우터의 캐시에 저장되어 있지 않은 경우 인접 라우터로 상기 콘텐츠 요청 메시지를 송신하는 것을 특징으로 한다.
- [0017] 바람직하게, 본 발명에 따른 접속 권한 요청 메시지의 송신 단계는 콘텐츠 요청 메시지의 요청 콘텐츠 식별자 및 사용자 공개키를 구비하는 접속 권한 요청 메시지를 생성하는 단계와, 요청 콘텐츠 식별자에 매핑되어 있는 인증 서버 주소를 저장하고 있는 매핑 테이블에서 요청 콘텐츠 식별자에 매핑되어 있는 인증 서버 주소를 검색하는 단계와, 생성한 접속 권한 요청 메시지를 검색한 인증 서버 주소로 송신하는 단계를 포함하는 것을 특징으로 한다.
- [0018] 여기서 사용자 개인키(UK_{pri})로 암호화된 사용자 공개키(UK_{pub})와 난수(nonce), 암호화되지 않은 사용자 공개키는 콘텐츠 요청 메시지의 인증 필드에 구비되어 있는 것을 특징으로 한다.
- [0019] 여기서 사용자 개인키와 사용자 공개키는 사용자가 상기 인증 서버에 등록시 인증 서버에서 사용자로 제공하는 것을 특징으로 한다.
- [0020] 여기서 인증 서버는 콘텐츠 제공 서버로부터 요청 콘텐츠에 사용자 접속 권한에 대한 정보를 수신하여 저장하고 있으며, 사용자 접속 권한에 대한 정보를 이용하여 접속 권한 응답 메시지를 생성하는 것을 특징으로 한다.
- [0021] 본 발명에 따른 콘텐츠 기반 네트워크의 라우터는 송수신부와, 송수신부를 통해 사용자 단말기로부터 수신한 콘텐츠 요청 메시지의 인증 필드를 복호화하여 사용자를 인증하는 사용자 인증부와, 콘텐츠 요청 메시지의 요청 콘텐츠 식별자 및 사용자 공개키를 구비하는 접속 권한 요청 메시지를 생성하고 접속 권한 요청 메시지를 송수신부를 통해 인증 서버로 송신 제어하는 콘텐츠 인증부와, 접속 권한 요청 메시지에 응답하여 인증 서버로부터 수신한 접속 권한 응답 메시지에 기초하여 요청 콘텐츠 식별자에 해당하는 요청 콘텐츠를 사용자 단말기로 제공하는 콘텐츠 제공부를 포함하는 것을 특징으로 한다.
- [0022] 바람직하게, 본 발명에 따른 콘텐츠 기반 네트워크의 라우터는 요청 콘텐츠 식별자에 해당하는 요청 콘텐츠가 상기 라우터 캐시에 저장되어 있는지 판단하는 판단부를 더 포함하는 것을 특징으로 한다.
- [0023] 여기서 판단부는 요청 콘텐츠 식별자에 해당하는 요청 콘텐츠가 라우터의 캐시에 저장되어 있지 않은 경우 송수신부를 통해 인접 라우터로 콘텐츠 요청 메시지를 송신하는 것을 특징으로 한다.
- [0024] 바람직하게, 본 발명에 따른 콘텐츠 인증부는 콘텐츠 요청 메시지의 요청 콘텐츠 식별자 및 사용자 공개키를 구비하는 접속 권한 요청 메시지를 생성하는 메시지 생성부와, 요청 콘텐츠 식별자에 매핑되어 있는 인증 서버 주소를 저장하고 있는 매핑 테이블과, 요청 콘텐츠 식별자에 매핑되어 있는 인증 서버 주소를 상기 매핑 테이블에서 검색하는 인증 서버 검색부와, 생성한 접속 권한 요청 메시지를 검색한 인증 서버 주소로 송신 제어하는 인증 요청부를 포함하는 것을 특징으로 한다.
- [0025] 여기서 인증 필드에는 사용자 개인키(UK_{pri})로 암호화된 사용자 공개키(UK_{pub})와 난수(nonce), 암호화되지 않은 사용자 공개키가 구비되어 있는 것을 특징으로 한다.
- [0026] 사용자 인증부는 암호화되지 않은 사용자 공개키를 이용하여 사용자 개인키(UK_{pri})로 암호화된 사용자 공개키(UK_{pub})와 난수(nonce)를 복호화하고, 복호화한 사용자 공개키와 난수가 각각 암호화되지 않은 사용자 공개키 및 라우터가 공유하는 난수와 일치하는지 여부로 사용자를 인증하는 것을 특징으로 한다.
- [0027] 여기서 접속 권한 요청 메시지는 사용자 공개키, 요청 콘텐츠 식별자 및 난수를 구비하도록 생성되는 것을 특징으로 한다.

발명의 효과

- [0028] 본 발명에 따른 콘텐츠 기반 네트워크의 콘텐츠 송신 방법은 다음과 같은 다양한 효과를 가진다.
- [0029] 첫째, 본 발명에 따른 콘텐츠 기반 네트워크의 콘텐츠 송신 방법은 콘텐츠에 대한 사용자 접속 권한을 판단함으

로써, 요청 콘텐츠에 대한 사용자 접속 권한을 가지는 사용자에게만 선택적으로 요청 콘텐츠를 제공할 수 있다.

[0030] 둘째, 본 발명에 따른 콘텐츠 기반 네트워크의 콘텐츠 송신 방법은 사용자 요청 콘텐츠에 대한 사용자 접속 권한을 인증하는 인증 서버 주소를 라우터의 매핑 테이블에 설정함으로써, 설정한 인증 서버를 통해 요청 콘텐츠에 대한 사용자 접속 권한을 정확하고 용이하게 인증할 수 있다.

[0031] 셋째, 본 발명에 따른 콘텐츠 기반 네트워크의 콘텐츠 송신 방법은 요청 콘텐츠에 대한 사용자 접속 권한을 판단하여 사용자 접속 권한을 가지는 사용자에게만 선택적으로 요청 콘텐츠를 제공함으로써, 불특정 다수인에게 제공하는 콘텐츠와, 비용을 지불한 사용자 또는 권한이 있는 사용자에게만 제공하는 콘텐츠로 구분하여 콘텐츠를 제공하는 다양한 서비스에서 적용 가능하다.

도면의 간단한 설명

[0032] 도 1과 도 2는 종래 콘텐츠 중심 네트워크에서 콘텐츠가 송수신되는 과정을 설명하기 위한 도면이다.

도 3은 본 발명에 따른 콘텐츠 기반 네트워크를 설명하기 위한 도면이다.

도 4는 본 발명에 따른 콘텐츠 기반 네트워크의 라우터를 설명하기 위한 기능 블록도이다.

도 5는 본 발명에 따른 콘텐츠 인증부(140)를 보다 구체적으로 설명하기 위한 기능 블록도이다.

도 6은 본 발명에 따른 콘텐츠 기반 네트워크에서 사용자 등록과 콘텐츠 등록 과정을 설명하기 위한 도면이다.

도 7은 본 발명에 따라, 요청 콘텐츠에 대한 사용자 접속 권한을 인증하기 위해 사용자 단말기, 라우터 및 인증 서버에서 송수신되는 메시지를 설명하기 위한 도면이다.

도 8은 본 발명에 따른 콘텐츠 기반 네트워크의 콘텐츠 송신 방법을 설명하기 위한 도면이다.

도 9는 접속 권한 요청 메시지를 생성하는 단계를 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0033] 이하 첨부한 도면을 참고로 본 발명에 따른 콘텐츠 기반 네트워크의 콘텐츠 송신 방법에 대해 보다 구체적으로 살펴본다.

[0034] 도 3은 본 발명에 따른 콘텐츠 기반 네트워크를 설명하기 위한 도면이다.

[0035] 도 3을 참고로 보다 구체적으로 살펴보면, 네트워크(40)에는 사용자 단말기(10), 인증 서버(20) 및 콘텐츠 제공 서버(30)가 접속되어 있다. 여기서 본 발명이 적용되는 분야에 따라 다수의 사용자 단말기가 네트워크(40)에 접속될 수 있거나, 다수의 인증 서버(20)가 네트워크(40)에 접속될 수 있거나 또는 다수의 콘텐츠 제공 서버(30)가 네트워크(40)에 접속될 수 있다.

[0036] 사용자 단말기(10)는 사용자가 사용하는 개인용 컴퓨터, 스마트폰 등과 같이 네트워크(40)에 접속하여 콘텐츠를 요청할 수 있는 단말기를 의미하며, 인증 서버(20)는 사용자를 인증하거나 사용자가 요청하는 콘텐츠에 대한 사용자 접속 권한을 판단하는 서버를 의미하며, 콘텐츠 제공 서버(30)는 요청 콘텐츠를 사용자 단말기(10)로 제공하는 단말을 의미한다.

[0037] 여기서 네트워크(40)는 유선/무선 인터넷일 수 있는데, 네트워크(40)에는 사용자 단말기(10)로부터 송신되는 콘텐츠 요청 메시지를 수신하며, 사용자가 요청한 콘텐츠를 저장하고 있는 경우 요청 콘텐츠에 대한 사용자 접속 권한을 판단하여 사용자 단말기(10)로 제공하는 다수의 라우터(100)를 구비하고 있다. 사용자가 요청한 콘텐츠를 저장하고 있지 않은 경우 라우터는 인접하고 있는 라우터로 콘텐츠 요청 메시지를 송신하며, 네트워크(40)의 라우터에 요청 콘텐츠가 저장되어 있지 않은 경우 콘텐츠 요청 메시지는 콘텐츠 제공 서버(30)로 송신된다. 콘텐츠 요청 콘텐츠를 수신한 콘텐츠 제공 서버(30)는 요청 콘텐츠를 네트워크(40)의 라우터(100)를 통해 사용자 단말기(10)로 제공하며, 요청 콘텐츠의 라우팅 경로에 위치하는 라우터들은 요청 콘텐츠를 라우터(100)의 캐시에 저장하여, 사후적으로 동일한 콘텐츠를 요청하는 콘텐츠 요청 메시지를 수신하는 경우 캐시에 저장되어 있는 요청 콘텐츠를 바로 사용자 단말기로 송신한다.

- [0038] 도 4는 본 발명에 따른 콘텐츠 기반 네트워크의 라우터를 설명하기 위한 기능 블록도이다.
- [0039] 도 4를 참고로 보다 구체적으로 살펴보면, 송수신부(110)는 사용자 단말기(10)로부터 콘텐츠 요청 메시지를 수신하며, 수신한 요청 메시지를 판단부(120)로 제공한다. 판단부(120)는 콘텐츠 요청 메시지에 구비되어 있는 요청 콘텐츠 식별자에 기초하여 캐시부(160)에 요청 콘텐츠가 저장되어 있는지 판단한다. 요청 콘텐츠가 캐시부(160)에 저장되어 있지 않은 경우, 판단부(120)는 수신한 콘텐츠 요청 메시지를 인접 라우터로 송신한다.
- [0040] 그러나 요청 콘텐츠가 캐시부(160)에 저장되어 있는 경우 판단부(120)는 텐츠 요청 메시지의 인증 필드에 저장되어 있는 사용자 인증 정보를 사용자 인증부(130)로 제공한다. 사용자 인증부(130)는 인증 필드에 저장되어 있는 사용자 개인키로 암호화된 난수와 사용자 공개키, 암호화되지 않은 사용자 공개키를 이용하여 콘텐츠 요청 메시지를 송신한 사용자를 인증한다.
- [0041] 콘텐츠 인증부(140)는 사용자 인증이 완료되는 경우, 콘텐츠 요청 메시지의 요청 콘텐츠 식별자 및 사용자 공개키를 구비하는 접속 권한 요청 메시지를 생성하고, 접속 권한 요청 메시지를 송수신부(110)를 통해 인증 서버로 송신 제어한다. 한편, 콘텐츠 인증부(140)는 접속 권한 요청 메시지에 응답하여 인증 서버로부터 수신한 접속 권한 응답 메시지에 기초하여 요청 콘텐츠에 대한 사용자 접속 권한을 인증한다.
- [0042] 콘텐츠 제공부(150)는 콘텐츠 인증부(140)의 인증 결과에 기초하여 사용자가 요청 콘텐츠에 대한 접속 권한을 가지는 경우, 캐시부(160)에 저장되어 있는 요청 콘텐츠를 송수신부(110)를 통해 사용자 단말기(10)로 송신한다.
- [0043] 도 5는 본 발명에 따른 콘텐츠 인증부(140)를 보다 구체적으로 설명하기 위한 기능 블록도이다.
- [0044] 도 5를 참고로 보다 구체적으로 살펴보면, 메시지 생성부(141)는 요청 콘텐츠에 대한 사용자 접속 권한을 인증하기 위하여 요청 콘텐츠 식별자 및 사용자 공개키를 구비하는 접속 권한 요청 메시지를 생성한다.
- [0045] 인증 서버 검색부(145)는 요청 콘텐츠 식별자에 매핑되어 있는 인증 서버 주소를 매핑 테이블(147)에서 검색하는데, 매핑 테이블(147)에는 요청 콘텐츠 식별자에 해당하는 요청 콘텐츠의 사용자 접속 권한을 관리하는 인증 서버 주소가 매핑되어 저장되어 있다.
- [0046] 인증 요청부(143)는 생성한 접속 권한 요청 메시지를 검색한 인증 서버 주소로 송신하며, 인증 서버로부터 접속 권한 요청 메시지에 응답하여 접속 권한 응답 메시지를 수신하는 경우 접속 권한 응답 메시지에 기초하여 요청 콘텐츠에 대한 사용자 접속 권한을 인증한다. 인증 요청부(143)는 요청 콘텐츠에 대한 사용자 접속 권한의 인증 결과를 콘텐츠 제공부(150)로 제공한다.
- [0047] 도 6은 본 발명에 따른 콘텐츠 기반 네트워크에서 사용자 등록과 콘텐츠 등록 과정을 설명하기 위한 도면이다.
- [0048] 도 6을 참고로 보다 구체적으로 살펴보면, 사용자는 사용자 정보를 인증 서버로 송신하여 인증 서버에 사용자를 등록 요청한다(S1). 여기서 사용자 정보는 사용자가 콘텐츠 제공 서버에 등록시 사용한 사용자 이름, 사용자 주민등록번호, 아이디 또는 비밀번호일수 있다.
- [0049] 한편, 콘텐츠 제공 서버는 제공하는 콘텐츠 정보를 인증 서버로 송신하여 인증 서버에 콘텐츠를 등록한다(S3). 여기서 콘텐츠 정보는 해당 콘텐츠의 식별자인 것을 특징으로 한다.
- [0050] 인증 서버는 사용자 등록이 완료되는 경우, 사용자 단말기로 사용자가 사용할 사용자 공개키(UK_{pub})와 사용자 개인키(UK_{pri})를 송신하며(S5), 콘텐츠 제공 서버는 콘텐츠에 대한 사용자 접속 권한에 대한 정보를 인증 서버로 송신한다.
- [0051] 인증 서버는 라우터로부터 요청 콘텐츠에 대한 사용자 접속 권한의 인증을 요청받는 경우, 사용자 공개키 또는 사용자 개인키에 매핑되는 사용자 접속 권한 정보에 기초하여 요청 콘텐츠에 대한 사용자 접속 권한을 인증한다.
- [0052] 도 7은 본 발명에 따라, 요청 콘텐츠에 대한 사용자 접속 권한을 인증하기 위해 사용자 단말기, 라우터 및 인증 서버에서 송수신되는 메시지를 설명하기 위한 도면이다.

- [0053] 도 7을 참고로 보다 구체적으로 살펴보면, 사용자 단말기는 요청 콘텐츠가 존재하는 경우 콘텐츠 요청 메시지(interest packet)를 생성하여 라우터로 송신한다(S11). 콘텐츠 요청 메시지는 사용자가 요청하는 콘텐츠를 식별하기 위한 요청 콘텐츠 식별자, 임의로 생성된 난수 및 사용자를 인증하기 위한 인증 정보를 구비하고 있다. 바람직하게, 사용자를 인증하기 위한 인증 정보는 별도의 인증 필드에 저장되어 있는데 인증 필드에는 사용자 개인키(UK_{pri})로 암호화된 사용자 공개키(UK_{pub})와 난수(nonce), 암호화되지 않은 사용자 공개키(UK_{pub})가 구비되어 있다.
- [0054] 라우터는 요청 콘텐츠 식별자에 기초하여 요청 콘텐츠가 캐시에 저장되어 있는 경우, 콘텐츠 요청 메시지를 수신한 사용자를 인증하고 요청 콘텐츠에 대한 사용자 접속 권한을 인증하기 위하여 접속 권한 요청 메시지를 인증 서버로 송신한다(S13). 여기서 접속 권한 요청 메시지에는 콘텐츠 서명 비트, 사용자 공개키 및 난수가 구비되어 있다. 바람직하게, 콘텐츠 서명 비트로 요청 콘텐츠 식별자가 사용될 수 있다.
- [0055] 인증 서버는 콘텐츠 서명 비트, 사용자 공개키, 콘텐츠 제공자 서버로부터 기수신한 사용자 접속 권한 정보에 기초하여 사용자가 요청 콘텐츠에 대한 접속 권한이 있는지를 판단하여 접속 권한 응답 메시지를 생성하여 라우터로 송신한다(S15). 접속 권한 응답 메시지에 기초하여 사용자가 요청 콘텐츠에 대한 접속 권한이 존재하는 경우 캐시부에 저장되어 있는 요청 콘텐츠를 사용자 단말기로 송신한다(S17).
- [0056] 도 8은 본 발명에 따른 콘텐츠 기반 네트워크의 콘텐츠 송신 방법을 설명하기 위한 도면이다.
- [0057] 도 8을 참고로 라우터에서 사용자 요청 콘텐츠를 제공하는 방법을 보다 구체적으로 살펴보면, 사용자 단말기로부터 콘텐츠 요청 메시지를 수신하는 경우(S110), 콘텐츠 요청 메시지에 구비되어 있는 요청 콘텐츠 식별자에 기초하여 라우터의 캐시에 요청 콘텐츠가 저장되어 있는지 판단한다(S120). 라우터의 캐시에 요청 콘텐츠가 저장되어 있지 않은 경우 콘텐츠 요청 메시지를 인접 라우터로 라우팅한다(S130).
- [0058] 한편, 라우터의 캐시에 요청 콘텐츠가 저장되어 있는 경우 콘텐츠 요청 메시지의 인증 필드에 구비되어 있는 사용자 인증 정보에 기초하여 사용자를 인증한다(S140). 즉, 인증 필드에는 사용자 개인키(UK_{pri})로 암호화된 사용자 공개키(UK_{pub})와 난수(nonce) 및 암호화되지 않은 사용자 공개키가 저장되어 있는데, 사용자 개인키(UK_{pri})로 암호화된 사용자 공개키(UK_{pub})와 난수(nonce)를 암호화되지 않은 사용자 공개키로 복호화하여, 복호화한 사용자 공개키와 암호화되지 않은 사용자 공개키가 일치하는지와, 복호화한 난수와 암호화되지 않고 콘텐츠 요청 메시지에 구비되어 있는 난수가 일치하는지 여부로 사용자를 인증한다.
- [0059] 사용자 인증이 완료되는 경우 접속 권한 요청 메시지를 생성하고 생성한 접속 권한 요청 메시지를 인증 서버로 송신한다(S150). 인증 서버로부터 접속 권한 요청 메시지에 응답하여 접속 권한 응답 메시지를 수신하는 경우 요청 콘텐츠에 대한 사용자의 접속 권한이 있는지 인증하며(S160), 판단 결과 요청 콘텐츠에 대한 사용자 접속 권한을 인증하는 경우 요청 콘텐츠를 캐시부에서 추출하여 사용자 단말기로 송신한다(S170).
- [0060] 도 9는 접속 권한 요청 메시지를 생성하는 단계를 설명하기 위한 흐름도이다.
- [0061] 도 9를 참고로 보다 구체적으로 살펴보면, 요청 콘텐츠를 요청하는 사용자의 사용자 공개키, 콘텐츠 서명 비트 및 난수를 구비하는 접속 권한 요청 메시지를 생성한다(S151). 한편, 요청 콘텐츠의 사용자 접속 권한을 관리 인증하는 인증 서버의 주소를 매핑 테이블에서 검색하고(S153), 검색한 인증 서버 주소로 접속 권한 요청 메시지를 송신한다(S155).
- [0062] 본 발명에서 라우터는 각 콘텐츠별로 사용자 접속 권한을 관리 인증하는 인증 서버의 주소를 매핑 테이블에 저장하고 있으며, 해당 인증 서버를 통해 요청 콘텐츠에 대한 사용자 접속 권한을 요청함으로써, 접속 권한 요청 메시지를 멀티캐스팅하지 않아 메시지의 오버헤드를 방지하며 허락받지 않은 제3자가 불법으로 요청 콘텐츠에 대한 사용자 접속 권한을 인증하는 것을 방지할 수 있다.
- [0063] 한편, 상술한 본 발명의 실시 예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터로 읽을 수 있는 기록 매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.
- [0064] 상기 컴퓨터로 읽을 수 있는 기록 매체는 전기 또는 자기식 저장 매체(예를 들어, 롬, 플로피 디스크, 하드디스크

크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장 매체를 포함한다.

[0065]

본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

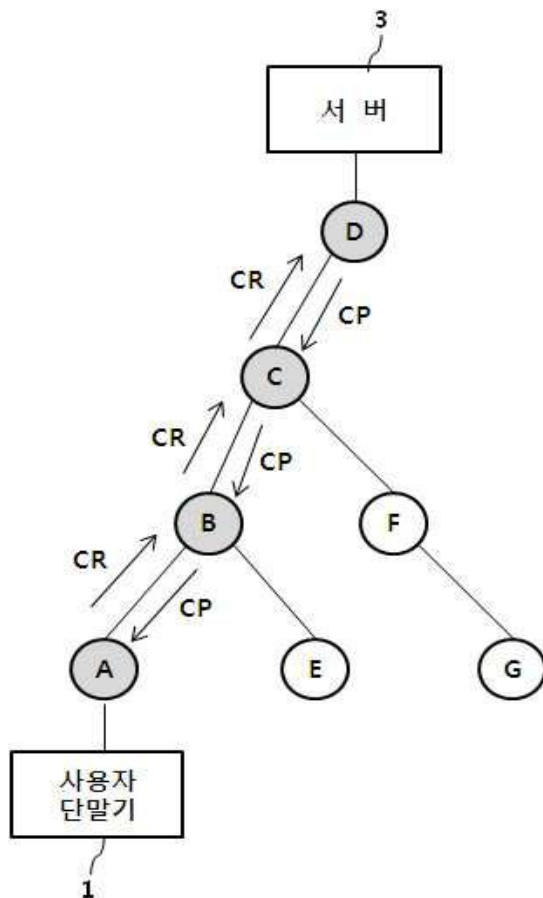
부호의 설명

[0066]

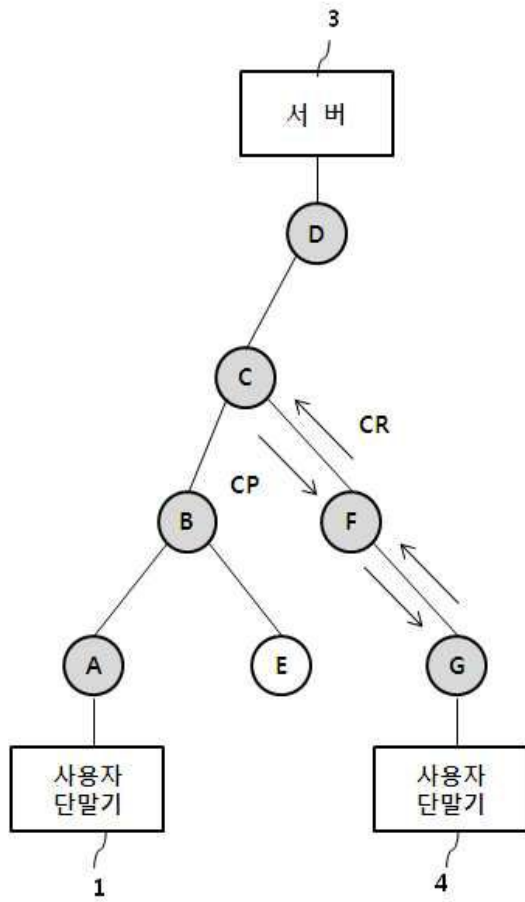
10: 사용자 단말기 20: 인증 서버
30: 콘텐츠 제공 서버 40: 네트워크
100: 라우터 110: 송수신부
120: 판단부 130: 사용자 인증부
140: 콘텐츠 인증부 150: 콘텐츠 제공부
160: 캐시부
141: 메시지 생성부 143: 인증부
145: 인증 서버 검색부 147: 매핑 테이블

도면

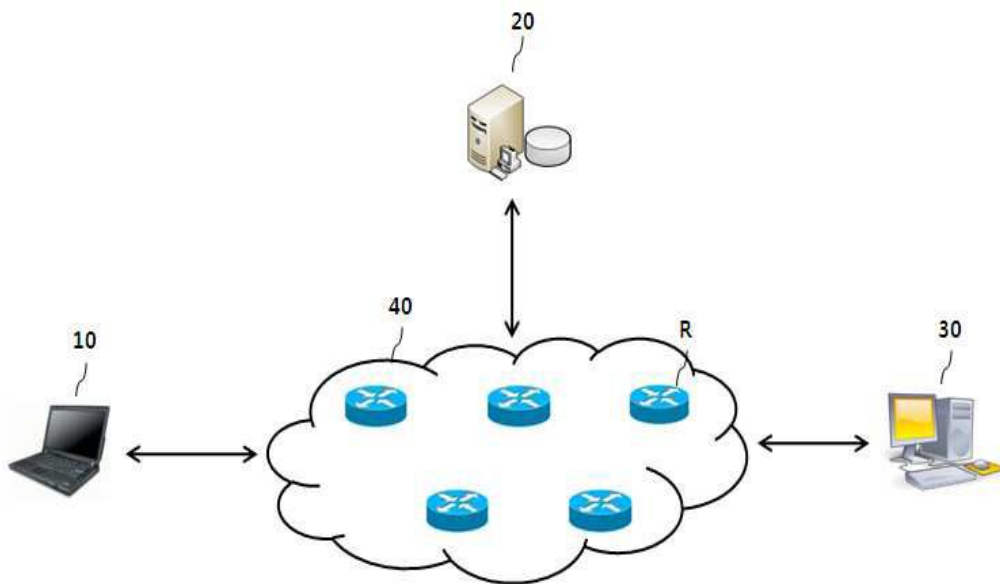
도면1



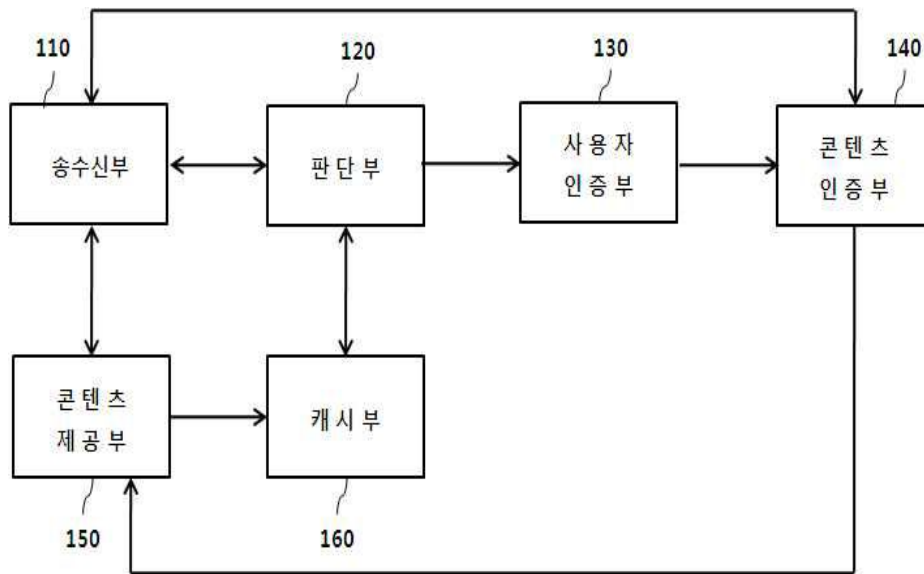
도면2



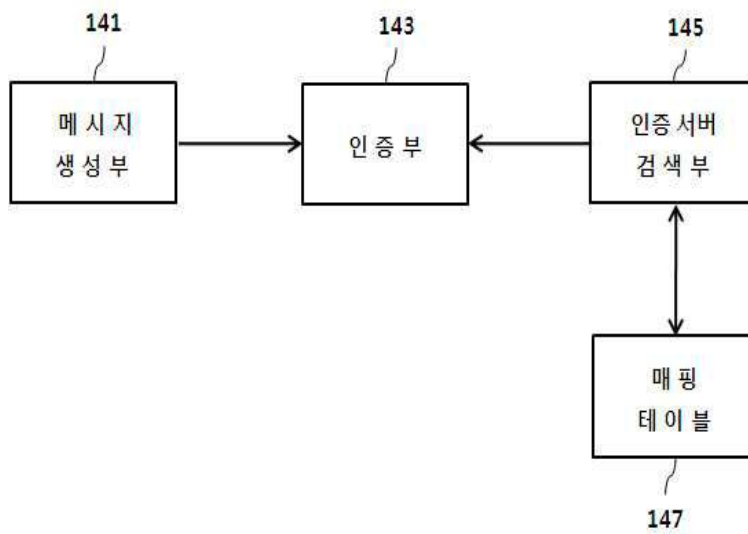
도면3



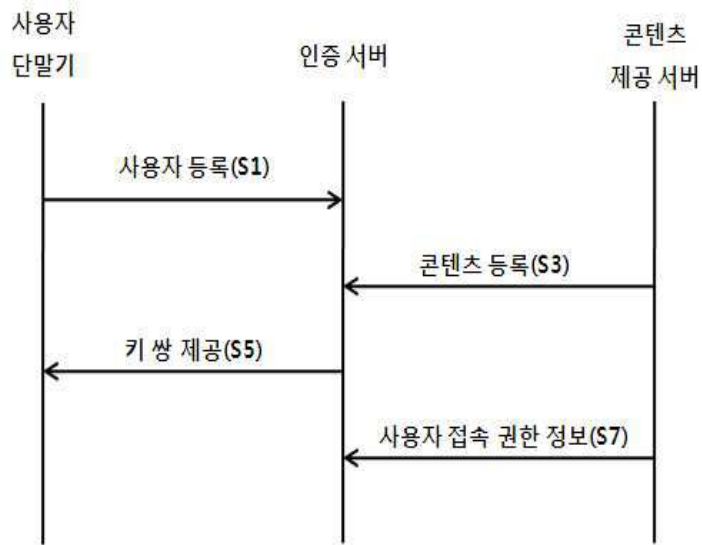
도면4



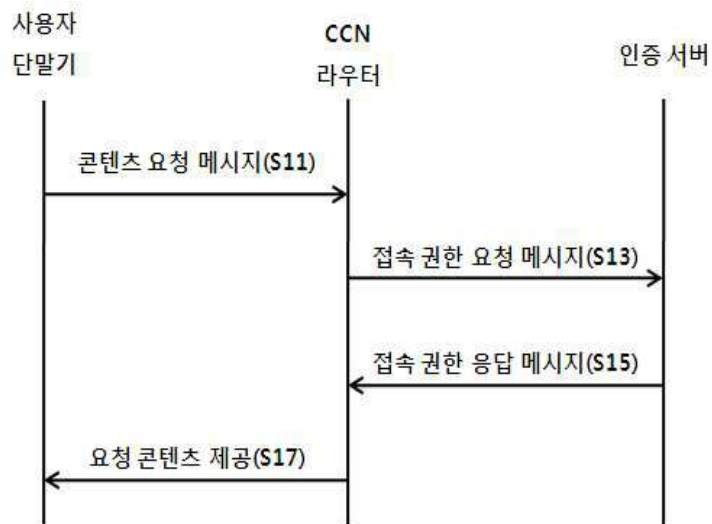
도면5



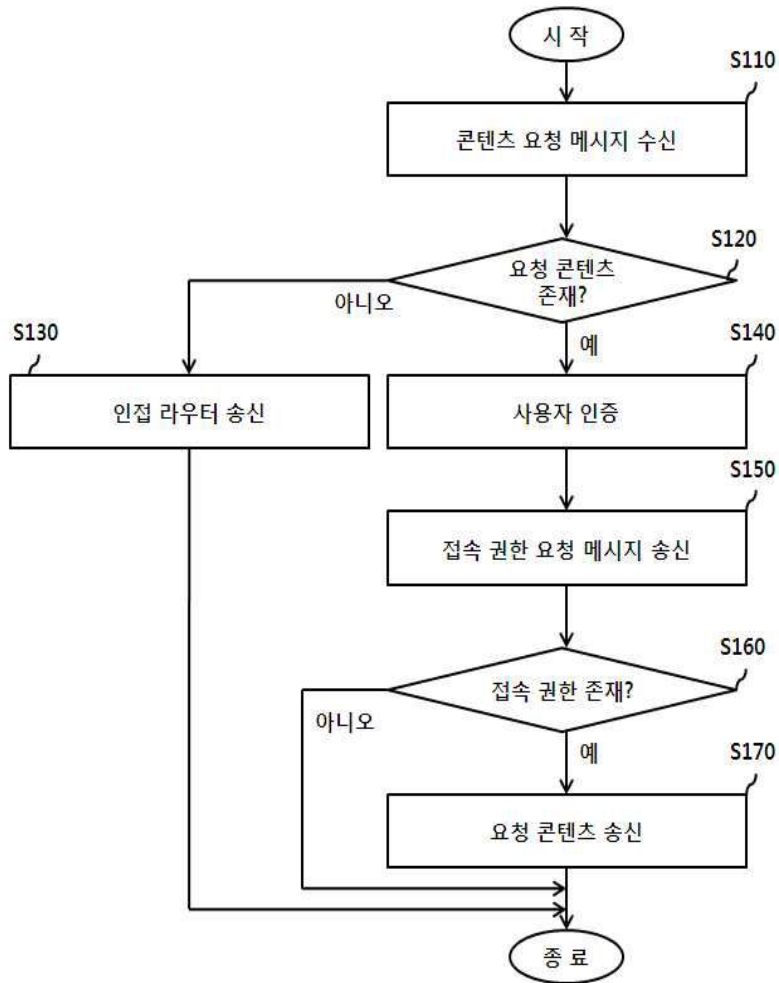
도면6



도면7



도면8



도면9

