(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년02월01일
(11) 등록번호 10-1701625
(24) 등록일자 2017년01월24일

(51) 국제특허분류(Int. Cl.)
H04N 21/4385 (2011.01)
(52) CPC특허분류
H04N 21/43853 (2013.01)
H04L 9/30 (2013.01)
(21) 출원번호 10-2015-0099800
(22) 출원일자 2015년07월14일
심사청구일자 2015년07월14일
(65) 공개번호 10-2017-0008514
(43) 공개일자 2017년01월24일
(56) 선행기술조사문헌
JP2003229843 A
JP2003235012 A
KR100446336 B1
JP5908296 B2

(73) 특허권자
라인 가부시키가이샤
일본국 도쿄토 시부야쿠 시부야 2-21-1
(72) 발명자
정재헌
경기도 성남시 분당구 황새울로360번길 42,11층(서현동,에이케이플라자분당점)
정구현
경기도 성남시 분당구 황새울로360번길 42,11층(서현동,에이케이플라자분당점)
(뒷면에 계속)
(74) 대리인
양성보

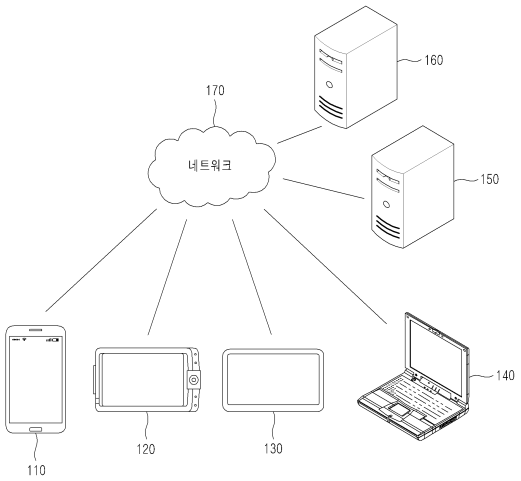
전체 청구항 수 : 총 16 항 심사관 : 김창원

(54) 발명의 명칭 **암호화된 컨텐츠의 복호화 키를 안전하게 획득하여 컨텐츠를 재생하기 위한 방법 및 시스템**

(57) 요 약

암호화된 컨텐츠의 복호화 키를 안전하게 획득하여 컨텐츠를 재생하기 위한 방법 및 시스템이 개시된다. 컨텐츠 재생 방법은, 클라이언트에서, 암호화된 컨텐츠의 수신 또는 상기 암호화된 컨텐츠에 대한 사용자의 재생요청에 대한 응답으로 상기 암호화된 컨텐츠의 복호화 키를 암호화하기 위한 암호키를 생성하는 단계, 상기 클라이언트에서, 상기 암호화된 컨텐츠의 복호화 키를 서버로 요청하기 위해, 상기 생성된 암호키를 상기 서버의 공개키로 암호화하여 상기 서버로 전송하는 단계 및 상기 클라이언트에서, 상기 서버로부터 상기 암호키로 암호화된 복호화 키를 수신하고, 상기 암호화된 복호화 키를 상기 암호키로 복호화하여 상기 암호화된 컨텐츠의 복호화 키를 획득하고, 상기 획득한 복호화 키로 상기 암호화된 컨텐츠를 복호화하여 컨텐츠를 획득 및 재생하는 단계를 포함할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04N 21/4353 (2013.01)
(72) 발명자
최재영
경기도 성남시 분당구 황새울로360번길 42,11층(서현동,에이케이플라자분당점)
정상민
경기도 성남시 분당구 황새울로360번길 42,11층(서현동,에이케이플라자분당점)
류대원
경기도 성남시 분당구 황새울로360번길 42,11층(서현동,에이케이플라자분당점)
권영재
경기도 성남시 분당구 황새울로360번길 42,11층(서현동,에이케이플라자분당점)

명 세 서

청구범위

청구항 1

컨텐츠 재생 방법에 있어서,

클라이언트에서, 암호화된 컨텐츠의 수신 또는 상기 암호화된 컨텐츠에 대한 사용자의 재생요청에 대한 응답으로 상기 암호화된 컨텐츠의 복호화 키를 암호화하기 위한 암호키를 생성하는 단계;

상기 클라이언트에서, 상기 암호화된 컨텐츠의 복호화 키를 서버로 요청하기 위해, 상기 생성된 암호키를 상기 서버의 공개키로 암호화하여 상기 서버로 전송하는 단계; 및

상기 클라이언트에서, 상기 서버로부터 상기 암호키로 암호화된 복호화 키를 수신하고, 상기 암호화된 복호화 키를 상기 암호키로 복호화하여 상기 암호화된 컨텐츠의 복호화 키를 획득하고, 상기 획득한 복호화 키로 상기 암호화된 컨텐츠를 복호화하여 컨텐츠를 획득 및 재생하는 단계

를 포함하고,

상기 서버에서, 상기 서버의 공개키로 암호화된 상기 암호키가 상기 서버의 비밀키로 복호화되어 상기 서버가 상기 암호키를 획득하고, 상기 획득한 암호키로 상기 복호화 키를 암호화하여 상기 암호키로 암호화된 복호화 키를 상기 클라이언트로 전송하는 것을 특징으로 하는 컨텐츠 재생 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 암호화된 컨텐츠는 상기 클라이언트와 상기 서버간에 설정된 통신 세션을 통해 상기 서버에서 상기 클라이언트로 전송되는 하나의 암호화된 파일 또는 복수의 암호화된 파일들을 포함하고,

상기 암호키를 생성하는 단계는,

상기 통신 세션마다 또는 상기 암호화된 파일마다 서로 다른 암호키를 생성하는 것을 특징으로 하는 컨텐츠 재생 방법.

청구항 4

제1항에 있어서,

상기 암호화된 컨텐츠는 상기 클라이언트와 상기 서버간에 설정된 통신 세션 동안 스트리밍 서비스를 통해 상기 서버에서 상기 클라이언트로 제공되는 복수의 암호화된 파일들을 포함하고,

상기 획득한 복호화 키로 상기 암호화된 컨텐츠를 복호화하여 컨텐츠를 획득 및 재생하는 단계는,

상기 스트리밍 서비스에 따라 순차적으로 수신되는 상기 복수의 암호화된 파일들을 상기 획득한 복호화 키로 복호화하여 순차적으로 재생하는 것을 특징으로 하는 컨텐츠 재생 방법.

청구항 5

제1항에 있어서,

상기 암호키는 상기 클라이언트의 공개키 및 비밀키를 포함하고,

상기 서버의 공개키로 암호화된 암호키는 상기 서버의 공개키로 암호화된 상기 클라이언트의 공개키를 포함하고,

상기 서버로부터 수신된 상기 암호키로 암호화된 복호화 키는 상기 클라이언트의 공개키로 암호화된 복호화 키

를 포함하고,

상기 클라이언트의 공개키로 암호화된 복호화 키는 상기 클라이언트의 비밀키로 복호화되는 것을 특징으로 하는 컨텐츠 재생 방법.

청구항 6

컨텐츠 재생 방법에 있어서,

서버에서, 클라이언트로부터 암호화된 컨텐츠의 복호화 키에 대한 요청으로서 상기 서버의 공개키로 암호화된 상기 클라이언트의 암호키를 수신하는 단계;

상기 서버의 공개키로 암호화된 상기 클라이언트의 암호키를 상기 서버의 비밀키로 복호화하여 상기 클라이언트의 암호키를 획득하는 단계;

상기 복호화 키를 상기 암호키로 암호화하여 상기 암호키로 암호화된 복호화 키를 생성하는 단계; 및

상기 암호키로 암호화된 복호화 키를 상기 클라이언트로 전송하는 단계

를 포함하고,

상기 클라이언트에서 상기 암호키로 암호화된 복호화 키가 상기 클라이언트의 암호키로 복호화되어 재생되는 것을 특징으로 하는 컨텐츠 재생 방법.

청구항 7

제6항에 있어서,

상기 클라이언트에서, 상기 암호화된 컨텐츠의 수신 또는 상기 암호화된 컨텐츠에 대한 사용자의 재생요청에 대한 응답으로 상기 암호화된 컨텐츠의 복호화 키를 암호화하기 위한 상기 클라이언트의 암호키가 생성되는 것을 특징으로 하는 컨텐츠 재생 방법.

청구항 8

제6항에 있어서,

상기 암호화된 컨텐츠는 상기 클라이언트와 상기 서버간에 설정된 통신 세션을 통해 상기 서버에서 상기 클라이언트로 전송되는 하나의 암호화된 파일 또는 복수의 암호화된 파일들을 포함하고,

상기 통신 세션마다 또는 상기 암호화된 파일마다 서로 다른 암호키가 생성되는 것을 특징으로 하는 컨텐츠 재생 방법.

청구항 9

제6항에 있어서,

상기 클라이언트와 상기 서버간에 설정된 통신 세션 동안 스트리밍 서비스를 통해 상기 클라이언트로 상기 암호화된 컨텐츠가 포함하는 복수의 파일들을 순차적으로 전송하는 단계

를 더 포함하고,

상기 스트리밍 서비스에 따라 상기 서버에서 상기 클라이언트로 순차적으로 전송되는 상기 복수의 암호화된 파일들이 상기 클라이언트에서 상기 복호화 키로 복호화되어 순차적으로 재생되는 것을 특징으로 하는 컨텐츠 재생 방법.

청구항 10

제6항에 있어서,

상기 클라이언트의 암호키는 상기 클라이언트의 공개키 및 비밀키를 포함하고,

상기 서버의 공개키로 암호화된 암호키는 상기 서버의 공개키로 암호화된 상기 클라이언트의 공개키를 포함하고,

상기 암호키로 암호화된 복호화 키는 상기 클라이언트의 공개키로 암호화된 복호화 키를 포함하고,

상기 클라이언트의 공개키로 암호화된 복호화 키는 상기 클라이언트의 비밀키로 복호화되는 것을 특징으로 하는 컨텐츠 재생 방법.

청구항 11

제1항 또는 제3항 내지 제10항 중 어느 한 항의 방법을 실행하기 위한 프로그램이 기록되어 있는 것을 특징으로 하는 컴퓨터에서 판독 가능한 기록 매체.

청구항 12

하나 이상의 프로세서들을 포함하는 클라이언트의 시스템에 있어서,

상기 하나 이상의 프로세서들은,

암호화된 컨텐츠의 수신 또는 상기 암호화된 컨텐츠에 대한 사용자의 재생요청에 대한 응답으로 상기 암호화된 컨텐츠의 복호화 키를 암호화하기 위한 암호키를 생성하는 암호키 생성부;

상기 암호화된 컨텐츠의 복호화 키를 서버로 요청하기 위해, 상기 생성된 암호키를 상기 서버의 공개키로 암호화하여 상기 서버로 전송하도록 상기 클라이언트를 제어하는 암호키 전송 제어부; 및

상기 서버로부터 수신된 상기 암호키로 암호화된 복호화 키를 상기 암호키로 복호화하여 상기 암호화된 컨텐츠의 복호화 키를 획득하고, 상기 획득한 복호화 키로 상기 암호화된 컨텐츠를 복호화하여 컨텐츠를 획득 및 재생하는 컨텐츠 재생부

를 포함하는 것을 특징으로 하는 시스템.

청구항 13

제12항에 있어서,

상기 서버에서, 상기 서버의 공개키로 암호화된 상기 암호키가 상기 서버의 비밀키로 복호화되어 상기 서버가 상기 암호키를 획득하고, 상기 획득한 암호키로 상기 복호화 키를 암호화하여 상기 암호키로 암호화된 복호화 키를 상기 클라이언트로 전송하는 것을 특징으로 하는 시스템.

청구항 14

제12항에 있어서,

상기 암호화된 컨텐츠는 상기 클라이언트와 상기 서버간에 설정된 통신 세션을 통해 상기 서버에서 상기 클라이언트로 전송되는 하나의 암호화된 파일 또는 복수의 암호화된 파일들을 포함하고,

상기 암호키 생성부는,

상기 통신 세션마다 또는 상기 암호화된 파일마다 서로 다른 암호키를 생성하는 것을 특징으로 하는 시스템.

청구항 15

하나 이상의 프로세서들을 포함하는 서버의 시스템에 있어서,

상기 하나 이상의 프로세서들은,

클라이언트로부터 암호화된 컨텐츠의 복호화 키에 대한 요청으로서 상기 서버의 공개키로 암호화된 상기 클라이언트의 암호키를 수신하도록 상기 서버를 제어하는 암호키 수신 제어부;

상기 서버의 공개키로 암호화된 상기 클라이언트의 암호키를 상기 서버의 비밀키로 복호화하여 상기 클라이언트의 암호키를 획득하는 암호키 복호화부;

상기 복호화 키를 상기 암호키로 암호화하여 상기 암호키로 암호화된 복호화 키를 생성하는 복호화 키 암호화부; 및

상기 암호키로 암호화된 복호화 키를 상기 클라이언트로 전송하도록 상기 서버를 제어하는 복호화 키 전송 제어

부

를 포함하고,

상기 클라이언트에서 상기 암호키로 암호화된 복호화 키가 상기 클라이언트의 암호키로 복호화되어 재생되는 것을 특징으로 하는 시스템.

청구항 16

제15항에 있어서,

상기 암호화된 컨텐츠는 상기 클라이언트와 상기 서버간에 설정된 통신 세션을 통해 상기 서버에서 상기 클라이언트로 전송되는 하나의 암호화된 파일 또는 복수의 암호화된 파일들을 포함하고,

상기 통신 세션마다 또는 상기 암호화된 파일마다 서로 다른 암호키가 생성되는 것을 특징으로 하는 시스템.

청구항 17

제15항에 있어서,

상기 하나 이상의 프로세서들은,

상기 클라이언트와 상기 서버간에 설정된 통신 세션 동안 스트리밍 서비스를 통해 상기 클라이언트로 상기 암호화된 컨텐츠가 포함하는 복수의 파일들을 순차적으로 전송하도록 상기 서버를 제어하는 파일 전송부

를 더 포함하고,

상기 스트리밍 서비스에 따라 상기 서버에서 상기 클라이언트로 순차적으로 전송되는 상기 복수의 암호화된 파일들이 상기 클라이언트에서 상기 복호화 키로 복호화되어 순차적으로 재생되는 것을 특징으로 하는 시스템.

발명의 설명

기 술 분 야

[0001] 아래의 설명은 암호화된 컨텐츠의 복호화 키를 안전하게 획득하여 컨텐츠를 재생하기 위한 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] HTTPS(Hypertext Transfer Protocol over Secure Sockets Layer, HTTP over SSL)는 월드 와이드 웹 통신 프로토콜인 HTTP의 보안이 강화된 버전으로 통신의 인증과 암호화를 위해 개발되었다. HTTPS는 소켓 통신에서 일반 텍스트를 이용하는 대신에, SSL이나 TLS 프로토콜을 통해 세션 데이터를 암호화한다.

[0003] 그러나 암호화된 컨텐츠와 암호화된 컨텐츠를 복호화하기 위한 복호화 키를 HTTPS를 이용하여 전달(일례로 서버에서 클라이언트로 암호화된 컨텐츠와 복호화 키를 전달)함에 있어서, 통신구간을 암호화(상술한 세션 데이터의 암호화를 통한 송수신 구간의 암호화)한다 하더라도 MITM(Man In The Middle attack)과 같은 공격을 통해 중간자가 해당 통신을 감청하여 복호화 키를 획득할 수 있고, 획득한 복호화 키를 이용하여 암호화된 컨텐츠를 무단으로 취득할 수 있다는 문제점이 있다.

[0004] 참고자료: <PCT/KR/2014/010167, US20140019540A1, US20130332543A1, US20130260893>

발명의 내용

해결하려는 과제

[0005] 클라이언트에서 재생하고자 하는 암호화된 컨텐츠에 대한 복호화 키를 서버에서 안전하게 클라이언트로 전달함으로써 클라이언트에서 안전하게 컨텐츠를 재생할 수 있는 컨텐츠 재생 방법 및 시스템을 제공한다.

과제의 해결 수단

[0006] 컨텐츠 재생 방법에 있어서, 클라이언트에서, 암호화된 컨텐츠의 수신 또는 상기 암호화된 컨텐츠에 대한 사용자의 재생요청에 대한 응답으로 상기 암호화된 컨텐츠의 복호화 키를 암호화하기 위한 암호키를 생성하는 단계;

상기 클라이언트에서, 상기 암호화된 컨텐츠의 복호화 키를 서버로 요청하기 위해, 상기 생성된 암호키를 상기 서버의 공개키로 암호화하여 상기 서버로 전송하는 단계; 및 상기 클라이언트에서, 상기 서버로부터 상기 암호키로 암호화된 복호화 키를 수신하고, 상기 암호화된 복호화 키를 상기 암호키로 복호화하여 상기 암호화된 컨텐츠의 복호화 키를 획득하고, 상기 획득한 복호화 키로 상기 암호화된 컨텐츠를 복호화하여 컨텐츠를 획득 및 재생하는 단계를 포함하는 것을 특징으로 하는 컨텐츠 재생 방법을 제공한다.

[0007] 일측에 따르면, 상기 서버에서, 상기 서버의 공개키로 암호화된 상기 암호키가 상기 서버의 비밀키로 복호화되어 상기 서버가 상기 암호키를 획득하고, 상기 획득한 암호키로 상기 복호화 키를 암호화하여 상기 암호키로 암호화된 복호화 키를 상기 클라이언트로 전송하는 것을 특징으로 할 수 있다.

[0008] 다른 측면에 따르면, 상기 암호화된 컨텐츠는 상기 클라이언트와 상기 서버간에 설정된 통신 세션을 통해 상기 서버에서 상기 클라이언트로 전송되는 하나의 암호화된 파일 또는 복수의 암호화된 파일들을 포함하고, 상기 암호키를 생성하는 단계는, 상기 통신 세션마다 또는 상기 암호화된 파일마다 서로 다른 암호키를 생성하는 것을 특징으로 할 수 있다.

[0009] 또 다른 측면에 따르면, 상기 암호화된 컨텐츠는 상기 클라이언트와 상기 서버간에 설정된 통신 세션 동안 스트리밍 서비스를 통해 상기 서버에서 상기 클라이언트로 제공되는 복수의 암호화된 파일들을 포함하고, 상기 획득한 복호화 키로 상기 암호화된 컨텐츠를 복호화하여 컨텐츠를 획득 및 재생하는 단계는, 상기 스트리밍 서비스에 따라 순차적으로 수신되는 상기 복수의 암호화된 파일들을 상기 획득한 복호화 키로 복호화하여 순차적으로 재생하는 것을 특징으로 할 수 있다.

[0010] 또 다른 측면에 따르면, 상기 암호키는 상기 클라이언트의 공개키 및 비밀키를 포함하고, 상기 서버의 공개키로 암호화된 암호키는 상기 서버의 공개키로 암호화된 상기 클라이언트의 공개키를 포함하고, 상기 서버로부터 수신된 상기 암호키로 암호화된 복호화 키는 상기 클라이언트의 공개키로 암호화된 복호화 키를 포함하고, 상기 클라이언트의 공개키로 암호화된 복호화 키는 상기 클라이언트의 비밀키로 복호화되는 것을 특징으로 할 수 있다.

[0011] 컨텐츠 재생 방법에 있어서, 서버에서, 클라이언트로부터 암호화된 컨텐츠의 복호화 키에 대한 요청으로서 상기 서버의 공개키로 암호화된 상기 클라이언트의 암호키를 수신하는 단계; 상기 서버의 공개키로 암호화된 상기 클라이언트의 암호키를 상기 서버의 비밀키로 복호화하여 상기 클라이언트의 암호키를 획득하는 단계; 상기 복호화 키를 상기 암호키로 암호화하여 상기 암호키로 암호화된 복호화 키를 생성하는 단계; 및 상기 암호키로 암호화된 복호화 키를 상기 클라이언트로 전송하는 단계를 포함하고, 상기 클라이언트에서 상기 암호키로 암호화된 복호화 키가 상기 클라이언트의 암호키로 복호화되어 재생되는 것을 특징으로 하는 컨텐츠 재생 방법을 제공한다.

[0012] 하나 이상의 프로세서들을 포함하는 클라이언트의 시스템에 있어서, 상기 하나 이상의 프로세서들은, 암호화된 컨텐츠의 수신 또는 상기 암호화된 컨텐츠에 대한 사용자의 재생요청에 대한 응답으로 상기 암호화된 컨텐츠의 복호화 키를 암호화하기 위한 암호키를 생성하는 암호키 생성부; 상기 암호화된 컨텐츠의 복호화 키를 서버로 요청하기 위해, 상기 생성된 암호키를 상기 서버의 공개키로 암호화하여 상기 서버로 전송하도록 상기 클라이언트를 제어하는 암호키 전송부; 및 상기 서버로부터 수신된 상기 암호키로 암호화된 복호화 키를 상기 암호키로 복호화하여 상기 암호화된 컨텐츠의 복호화 키를 획득하고, 상기 획득한 복호화 키로 상기 암호화된 컨텐츠를 복호화하여 컨텐츠를 획득 및 재생하는 컨텐츠 재생부를 포함하는 것을 특징으로 하는 시스템을 제공한다.

[0013] 하나 이상의 프로세서들을 포함하는 서버의 시스템에 있어서, 상기 하나 이상의 프로세서들은, 클라이언트로부터 암호화된 컨텐츠의 복호화 키에 대한 요청으로서 상기 서버의 공개키로 암호화된 상기 클라이언트의 암호키를 수신하도록 상기 서버를 제어하는 암호키 수신 제어부; 상기 서버의 공개키로 암호화된 상기 클라이언트의 암호키를 상기 서버의 비밀키로 복호화하여 상기 클라이언트의 암호키를 획득하는 암호키 복호화부; 상기 복호화 키를 상기 암호키로 암호화하여 상기 암호키로 암호화된 복호화 키를 생성하는 복호화 키 암호화부; 및 상기 암호키로 암호화된 복호화 키를 상기 클라이언트로 전송하도록 상기 서버를 제어하는 복호화 키 전송 제어부를 포함하고, 상기 클라이언트에서 상기 암호키로 암호화된 복호화 키가 상기 클라이언트의 암호키로 복호화되어 재생되는 것을 특징으로 하는 시스템을 제공한다.

발명의 효과

[0014] 클라이언트에서 재생하고자 하는 암호화된 컨텐츠에 대한 복호화 키를 안전하게 클라이언트로 전달함으로써 클

라이언트에서 안전하게 컨텐츠를 재생할 수 있다.

도면의 간단한 설명

[0015] 도 1은 본 발명의 일실시예에 따른 네트워크 환경의 예를 도시한 도면이다.

도 2는 본 발명의 일실시예에 있어서, 전자 기기 및 서버의 내부 구성을 설명하기 위한 블록도이다.

도 3은 본 발명의 일실시예에 있어서, 전자 기기와 서버의 프로세서가 포함할 수 있는 구성의 예를 도시한 도면이다.

도 4는 본 발명의 일실시예에 있어서, 컨텐츠 재생 방법의 예를 도시한 흐름도이다.

도 5는 본 발명의 일실시예에 있어서, 복수의 암호화된 파일을 포함하는 컨텐츠의 예를 나타낸 도면이다.

도 6은 본 발명의 일실시예에 있어서, 암호화 및 복호화를 위한 과정의 예를 보다 구체적으로 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0016] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0017] 도 1은 본 발명의 일실시예에 따른 네트워크 환경의 예를 도시한 도면이다. 도 1의 네트워크 환경은 복수의 전자 기기들(110, 120, 130, 140), 복수의 서버들(150, 160) 및 네트워크(170)를 포함하는 예를 나타내고 있다. 이러한 도 1은 발명의 설명을 위한 일례로 전자 기기의 수나 서버의 수가 도 1과 같이 한정되는 것은 아니다.

[0018] 복수의 전자 기기들(110, 120, 130, 140)은 컴퓨팅 시스템으로 구현되는 고정형 단말이거나 이동형 단말일 수 있다. 복수의 전자 기기들(110, 120, 130, 140)의 예를 들면, 스마트폰(smart phone), 휴대폰, 네비게이션, 컴퓨터, 노트북, 디지털방송용 단말, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 태블릿 PC 등이 있다. 일례로 전자 기기 1(110)은 무선 또는 유선 통신 방식을 이용하여 네트워크(170)를 통해 다른 전자 기기들(120, 130, 140) 및/또는 서버(150, 160)와 통신할 수 있다.

[0019] 통신 방식은 제한되지 않으며, 네트워크(170)가 포함할 수 있는 통신망(일례로, 이동통신망, 유선 인터넷, 무선 인터넷, 방송망)을 활용하는 통신 방식뿐만 아니라 기기들간의 근거리 무선 통신 역시 포함될 수 있다. 예를 들어, 네트워크(170)는, PAN(personal area network), LAN(local area network), CAN(campus area network), MAN(metropolitan area network), WAN(wide area network), BBN(broadband network), 인터넷 등의 네트워크 중 하나 이상의 임의의 네트워크를 포함할 수 있다. 또한, 네트워크(170)는 버스 네트워크, 스타 네트워크, 링 네트워크, 메쉬 네트워크, 스타-버스 네트워크, 트리 또는 계층적(hierarchical) 네트워크 등을 포함하는 네트워크 토폴로지 중 임의의 하나 이상을 포함할 수 있으나, 이에 제한되지 않는다.

[0020] 서버(150, 160) 각각은 복수의 전자 기기들(110, 120, 130, 140)과 네트워크(170)를 통해 통신하여 서비스를 위한 컨텐츠를 제공하는 장치 또는 복수의 장치들로 구현될 수 있다.

[0021] 일례로, 서버(150)는 전자 기기 1(110)을 통한 사용자의 요청 메시지에 따라 전자 기기 1(110)의 화면을 구성할 수 있는 코드를 전자 기기 1(110)로 제공할 수 있다. 이 경우 전자 기기 1(110)은 전자 기기 1(110)이 포함하는 운영체제(Operating System, OS) 및 적어도 하나의 프로그램(일례로 브라우저나 특정 어플리케이션)의 제어에 따라 제공된 코드를 이용하여 화면을 구성 및 표시함으로써 사용자에게 컨텐츠를 제공할 수 있다.

[0022] 다른 예로 서버(150)는 네트워크(170)를 통해 전자 기기 1(110)로 스트리밍 서비스를 위한 데이터를 전송할 수 있다. 이 경우 전자 기기 1(110)은 전자 기기 1(110)이 포함하는 운영체제 및 적어도 하나의 프로그램의 제어에 따라 스트리밍되는 데이터를 이용하여 컨텐츠를 재생하여 출력할 수 있다.

[0023] 또 다른 예로, 서버(150)는 서버(150)로 접속한 전자 기기 1(110) 및 전자 기기 2(120)간의 통신 세션을 설정할 수 있다. 이 경우 전자 기기들(110, 120)은 설정된 통신 세션을 이용하여 전자 기기들(110, 120)간의 채팅, 데이터 전송, 음성통화 또는 화상통화 등과 같은 서비스를 제공받을 수 있다.

[0024] 또 다른 실시예로, 서버(150, 160)의 개입 없이 전자 기기들(110, 120, 130, 140)간의 통신 역시 가능하다.

[0026] 도 2는 본 발명의 일실시예에 있어서, 전자 기기 및 서버의 내부 구성을 설명하기 위한 블록도이다. 도 2에서는 하나의 전자 기기에 대한 예로서 전자 기기 1(110), 그리고 하나의 서버에 대한 예로서 서버(150)의 내부 구

성을 설명한다.

[0027] 전자 기기 1(110)과 서버(150)는 메모리(211, 221), 프로세서(212, 222), 통신 모듈(213, 223) 그리고 입출력 인터페이스(214, 224)를 포함할 수 있다. 메모리(211, 221)는 컴퓨터에서 판독 가능한 기록 매체로서, RAM(random access memory), ROM(read only memory) 및 디스크 드라이브와 같은 비소멸성 대용량 기록장치(permanent mass storage device)를 포함할 수 있다. 또한, 메모리(211, 221)에는 운영체제와 적어도 하나의 프로그램 코드(일례로 전자 기기 1(110)에 설치되어 구동되는 브라우저나 특정 어플리케이션 등을 위한 코드)가 저장될 수 있다. 이러한 소프트웨어 구성요소들은 드라이브 메커니즘(drive mechanism)을 이용하여 메모리(211, 221)와는 별도의 컴퓨터에서 판독 가능한 기록 매체로부터 로딩될 수 있다. 이러한 별도의 컴퓨터에서 판독 가능한 기록 매체는 플로피 드라이브, 디스크, 테이프, DVD/CD-ROM 드라이브, 메모리 카드 등의 컴퓨터에서 판독 가능한 기록 매체를 포함할 수 있다. 다른 실시예에서 소프트웨어 구성요소들은 컴퓨터에서 판독 가능한 기록 매체가 아닌 통신 모듈(213, 223)을 통해 메모리(211, 221)에 로딩될 수도 있다. 예를 들어, 적어도 하나의 프로그램은 개발자들이 네트워크(170)를 통해 제공하는 파일들에 의해 설치되는 프로그램에 기반하여 메모리(211, 221)에 로딩될 수 있다.

[0028] 프로세서(212, 222)는 기본적인 산술, 로직 및 입출력 연산을 수행함으로써, 컴퓨터 프로그램의 명령을 처리하도록 구성될 수 있다. 명령은 메모리(211, 221) 또는 통신 모듈(213, 223)에 의해 프로세서(212, 222)로 제공될 수 있다. 예를 들어 프로세서(212, 222)는 메모리(211, 221)와 같은 기록 장치에 저장된 프로그램 코드에 따라 수신되는 명령을 실행하도록 구성될 수 있다.

[0029] 통신 모듈(213, 223)은 네트워크(170)를 통해 전자 기기 1(110)과 서버(150)가 서로 통신하기 위한 기능을 제공할 수 있으며, 다른 전자 기기(일례로 전자 기기 2(120)) 또는 다른 서버(일례로 서버(160))와 통신하기 위한 기능을 제공할 수 있다. 일례로, 전자 기기 1(110)의 프로세서(212)가 메모리(211)와 같은 기록 장치에 저장된 프로그램 코드에 따라 생성한 요청(일례로 컨텐츠에 대한 스트리밍 서비스 요청)이 통신 모듈(213)의 제어에 따라 네트워크(170)를 통해 서버(150)로 전달될 수 있다. 역으로, 서버(150)의 프로세서(222)의 제어에 따라 제공될 제어 신호나 명령, 컨텐츠, 파일 등이 통신 모듈(223)과 네트워크(170)를 거쳐 전자 기기 1(110)의 통신 모듈(213)을 통해 전자 기기 1(110)로 수신될 수 있다. 예를 들어 통신 모듈(213)을 통해 수신된 서버(150)의 제어 신호나 명령 등은 프로세서(212)나 메모리(211)로 전달될 수 있고, 컨텐츠나 파일 등은 전자 기기 1(110)가 더 포함할 수 있는 저장 매체로 저장될 수 있다.

[0030] 입출력 인터페이스(214, 224)는 입출력 장치(215)와의 인터페이스를 위한 수단일 수 있다. 예를 들어, 입력 장치는 키보드 또는 마우스 등의 장치를, 그리고 출력 장치는 어플리케이션의 통신 세션을 표시하기 위한 디스플레이와 같은 장치를 포함할 수 있다. 다른 예로 입출력 인터페이스(214)는 터치스크린과 같이 입력과 출력을 위한 기능이 하나로 통합된 장치와의 인터페이스를 위한 수단일 수도 있다. 보다 구체적인 예로, 전자 기기 1(110)의 프로세서(212)는 메모리(211)에 로딩된 컴퓨터 프로그램의 명령을 처리함에 있어서 서버(150)나 전자 기기 2(120)가 제공하는 데이터를 이용하여 구성되는 서비스 화면이나 컨텐츠가 입출력 인터페이스(214)를 통해 디스플레이에 표시될 수 있다.

[0031] 또한, 다른 실시예들에서 전자 기기 1(110) 및 서버(150)는 도 2의 구성요소들보다 더 많은 구성요소들을 포함할 수도 있다. 그러나, 대부분의 종래기술적 구성요소들을 명확하게 도시할 필요성은 없다. 예를 들어, 전자 기기 1(110)은 상술한 입출력 장치(250) 중 적어도 일부를 포함하도록 구현되거나 또는 트랜시버(transceiver), GPS(Global Positioning System) 모듈, 카메라, 각종 센서 등과 같은 다른 구성요소들을 더 포함할 수도 있다.

[0032] 도 3은 본 발명의 일실시예에 있어서, 전자 기기와 서버의 프로세서가 포함할 수 있는 구성의 예를 도시한 도면이고, 도 4는 본 발명의 일실시예에 있어서, 컨텐츠 재생 방법을 도시한 흐름도이다. 도 3에 도시된 바와 같이, 전자 기기 1(110)의 프로세서(212)는 암호키 생성부(311), 암호키 전송 제어부(312) 및 컨텐츠 재생부(313)를 포함할 수 있고, 서버(150)의 프로세서(222)는 암호키 수신 제어부(321), 암호키 복호화부(322), 복호화 키 암호화부(323) 및 복호화 키 전송 제어부(324)를 포함할 수 있다. 이러한 프로세서(212, 222)의 구성요소들은 도 4의 컨텐츠 재생 방법이 포함하는 단계들(410 내지 480)이 전자 기기 1(110)과 서버(150)를 통해 실행될 수 있도록 하기 위해 메모리(211, 221)가 포함하는 운영체제와 적어도 하나의 프로그램 코드를 통해 동작하도록 구현될 수 있다.

[0033] 단계(410)에서 전자 기기 1(110)은 암호키를 생성할 수 있다. 보다 구체적으로 전자 기기 1(110)의 암호키 생성부(311)는 단계(410)에서 암호화된 컨텐츠의 수신 또는 암호화된 컨텐츠에 대한 사용자의 재생요청에 대한 응답으로 암호화된 컨텐츠의 복호화 키를 암호화하기 위한 암호키를 생성할 수 있다. 예를 들어, 전자 기기

1(110)과 서버(150)간에는 컨텐츠의 제공을 위한 통신 세션이 설정될 수 있다. 이를 위해 전자 기기 1(110)과 서버(150)간의 통신 세션을 설정하는 과정이 포함될 수 있으나, 이미 잘 알려진 부분에 대해서는 자세한 설명을 생략한다. 서버(150)는 이러한 통신 세션을 통해 전자 기기 1(110)로 암호화된 컨텐츠를 제공할 수 있으며, 전자 기기 1(110)은 이러한 암호화된 컨텐츠의 수신에 따라, 또는 이러한 암호화된 컨텐츠에 대한 사용자의 재생 요청에 따라 암호화된 컨텐츠를 복호화하기 위한 복호화 키를 서버(150)가 다시 암호화하여 전달할 수 있도록 암호키를 생성할 수 있다.

[0034] 단계(420)에서 전자 기기 1(110)은 암호키를 서버(150)로 전송할 수 있다. 보다 구체적으로 전자 기기 1(110)의 암호키 전송 제어부(312)는 암호화된 컨텐츠의 복호화 키를 서버(150)로 요청하기 위해, 생성된 암호키를 서버(150)의 공개키로 암호화하여 서버(150)로 전송하도록 전자 기기 1(110)을 제어할 수 있다. 이를 위해 전자 기기 1(110)은 서버(150)의 공개키를 미리 수신하여 보관(저장)하고 있을 수 있고, 저장된 공개키를 이용하여 생성된 암호키를 암호화하여 서버(150)로 전송함으로 중간자가 암호키를 알 수 없도록 할 수 있다.

[0035] 단계(430)에서 서버(150)는 암호키를 수신할 수 있다. 보다 구체적으로 서버(150)의 암호키 수신 제어부(321)는 암호화된 컨텐츠의 복호화 키에 대한 요청으로서 서버(150)의 공개키로 암호화된 암호키를 수신하도록 서버(150)를 제어할 수 있다. 다시 말해, 단계(420)에서 전자 기기 1(110)은 암호화된 컨텐츠의 복호화 키를 요청하면서 암호키를 서버(150)의 공개키로 암호화하여 서버(150)로 전송할 수 있고, 단계(430)에서 서버(150)는 이처럼 암호화된 암호키를 전자 기기 1(110)로부터 수신할 수 있다.

[0036] 단계(440)에서 서버(150)는 암호화된 암호키를 복호화할 수 있다. 보다 구체적으로 서버(150)의 암호키 복호화부(322)는 서버(150)의 공개키로 암호화된 암호키를 서버(150)의 비밀키로 복호화하여 암호키를 획득할 수 있다. 앞서 설명한 바와 같이 암호키는 서버(150)의 공개키로 암호화되어 전자 기기 1(110)에서 서버(150)로 전송되기 때문에 이러한 암호키를 안전하게 전달할 수 있다.

[0037] 단계(450)에서 서버(150)는 암호키로 복호화 키를 암호화할 수 있다. 보다 구체적으로 서버(150)의 복호화 키 암호화부(323)는 복호화 키를 암호키로 암호화하여 암호키로 암호화된 복호화 키를 생성할 수 있다.

[0038] 단계(460)에서 서버(150)는 암호키로 암호화된 복호화 키를 전자 기기 1(110)로 전송할 수 있다. 보다 구체적으로 서버(150)의 복호화 키 전송 제어부(324)는 암호키로 암호화된 복호화 키를 클라이언트로 전송하도록 서버(150)를 제어할 수 있다.

[0039] 단계(470)에서 전자 기기 1(110)은 암호화된 복호화 키를 수신하여 복호화할 수 있다. 보다 구체적으로 전자 기기 1(110)의 컨텐츠 재생부(313)는 서버(150)로부터 수신된 암호키로 암호화된 복호화 키를 암호키로 복호화하여 암호화된 컨텐츠의 복호화 키를 획득할 수 있다.

[0040] 단계(480)에서 전자 기기 1(110)은 복호화 키로 암호화된 컨텐츠를 복호화 및 재생할 수 있다. 보다 구체적으로 전자 기기 1(110)의 컨텐츠 재생부(313)는 복호화 키로 암호화된 컨텐츠를 복호화하여 컨텐츠를 획득 및 재생할 수 있다.

[0041] 앞서 설명한 바와 같이 종래기술에서는 HTTPS(Hypertext Transfer Protocol over Secure Sockets Layer, HTTP over SSL)와 같이 보안을 위해 통신 구간(세션 데이터)을 암호화하는 기술을 이용하여 복호화 키를 전달한다 하더라도 MITM(Man In The Middle attack)과 같은 공격을 통해 중간자가 해당 통신을 감청하여 복호화 키를 획득할 수 있다는 문제점이 있었다. 본 발명의 실시예들에서는 클라이언트(일례로 전자 기기 1(110))가 생성하는 암호키를 서버(150)의 공개키를 이용하여 서버(150)가 안전하게 획득하고, 서버(150)에서 클라이언트의 암호키로 복호화 키를 암호화하여 클라이언트로 전달함으로써 중간자가 이러한 암호키로 암호화된 복호화 키를 획득하더라도 복호화 키를 얻지 못하도록(중간자는 클라이언트의 암호키를 알 수 없기 때문에) 할 수 있다.

[0042] 또한 앞서 설명한 바와 같이 암호화된 컨텐츠는 전자 기기 1(110)과 서버(150)간에 설정된 통신 세션을 통해 서버(150)에서 전자 기기 1(110)로 전송될 수 있으며, 이때 암호화된 컨텐츠는 하나의 암호화된 파일로 구성될 수도 있으나 복수의 암호화된 파일들로 구성될 수도 있다. 이 경우, 전자 기기 1(110)은 통신 세션마다 서로 다른 암호키를 생성할 수도 있고, 암호화된 파일마다 서로 다른 암호키를 생성할 수도 있다. 예를 들어 동일한 암호화된 컨텐츠를 수신하는 경우에도 통신 세션이 다르다면, 통신 세션마다 서로 다른 암호키를 이용하여 해당 암호화된 컨텐츠의 복호화 키를 요청할 수 있다. 다른 예로, 하나의 암호화된 컨텐츠가 복수의 암호화된 파일들로 구성된 경우, 하나의 암호키로 복수의 암호화된 파일들에 대한 복호화 키를 요청할 수도 있으나, 파일마다 서로 다른 암호키를 생성하여 복호화 키를 요청할 수도 있다. 후자의 경우에는 파일마다 서로 다른 복호화 키가 존재하는 경우일 수 있다. 구체적인 예로, 하나의 컨텐츠가 복수의 파일을 포함하고, 복수의 파일이 서로

다른 키로 암호화되어 서로 다른 복수의 복호화 키가 존재한다면, 전자 기기 1(110)은 파일마다 암호키를 서로 다르게 생성하여 복호화 키를 각각 요청할 수 있다.

[0043] 또한 암호화된 컨텐츠는 전자 기기 1(110)과 서버(150)간에 설정된 통신 세션 동안 스트리밍 서비스를 통해 서버(150)에서 전자 기기 1(110)로 제공되는 복수의 암호화된 파일들을 포함할 수도 있다.

[0044] 도 5는 본 발명의 일실시예에 있어서, 복수의 암호화된 파일을 포함하는 컨텐츠의 예를 나타낸 도면이다. 화면(500)은 전자 기기 1(110)의 화면의 일부로서 하나의 음원 컨텐츠가 스트리밍 서비스를 통해 전송된 확장자 'ts'의 복수의 파일들을 나타내고 있다. 만약 확장자 'ts'의 복수의 파일들이 하나의 키로 암호화되어 하나의 복호화 키를 통해 복호화될 수 있다면, 전자 기기 1(110)은 해당 통신 세션을 위한 하나의 암호키를 생성할 수 있다. 반면, 확장자 'ts'의 복수의 파일들이 서로 다른 키로 암호화되어 복수의 복호화 키가 요구된다면, 전자 기기 1(110)은 파일마다 서로 다른 암호키를 생성하여 복호화 키를 요청할 수도 있다.

[0045] 도 6은 본 발명의 일실시예에 있어서, 복호화 키를 획득하는 과정의 예를 보다 구체적으로 설명하기 위한 도면이다. 도 6에서는 컨텐츠가 하나의 파일로 구성된 예로서 전자 기기 1(110)의 관점에서 복호화 키를 획득하는 과정을 설명한다.

[0046] 과정(610)에서 전자 기기 1(110)은 서버(150)로부터 서버(150)의 공개키 c를 수신할 수 있다. 수신된 서버(150)의 공개키 c는 전자 기기 1(110)이 포함할 수 있는 저장 매체에 저장될 수 있다. 다른 예로, 서버(150)의 공개키 c는 메모리(211)에 저장될 수도 있다.

[0047] 과정(620)에서 전자 기기 1(110)은 서버(150)로부터 컨텐츠용 암호화 키 a로 암호화된 컨텐츠 a(A)를 수신할 수 있다. 컨텐츠 A는 서버(150)에서 컨텐츠용 암호화 키 a로 암호화될 수도 있으나, 컨텐츠 A를 위한 별도의 시스템에서 암호화되어 컨텐츠용 복호화 키 b와 함께 서버(150)로 제공될 수도 있다. 다른 실시예로, 암호화된 컨텐츠 a(A)는 별도의 시스템을 통해 전자 기기 1(110)로 제공될 수도 있다. 이 경우 서버(150)는 별도의 시스템으로부터 컨텐츠용 복호화 키 b를 수신하여 보관하고 있을 수 있다. 이때, 전자 기기 1(110)은 암호화된 컨텐츠 a(A)의 수신에 따라 또는 암호화된 컨텐츠 a(A)에 대한 사용자의 재생 요청에 따라 암호키 e를 생성할 수 있고, 서버(150)의 공개키 c로 암호키 e를 암호화하여 암호화된 암호키 c(e)를 생성할 수 있다.

[0048] 과정(630)에서 전자 기기 1(110)은 서버(150)의 공개키 c로 암호화된 암호키 c(e)를 서버(150)로 전송할 수 있다. 일례로 c(e)는 컨텐츠용 복호화 키 b를 서버(150)로 요청하기 위한 메시지에 포함되어 전송될 수 있다. 이때 서버(150)는 서버(150)의 비밀키 d로 c(e)를 복호화하여 암호키 e를 얻을 수 있다. 또한 서버(150)는 암호키 e로 컨텐츠용 복호화 키 b를 암호화하여 암호화된 복호화 키 e(b)를 생성할 수 있다.

[0049] 과정(640)에서 전자 기기 1(110)은 서버(150)로부터 암호화된 복호화 키 e(b)를 수신할 수 있다. 이때, 전자 기기 1(110)는 암호키 e로 암호화된 복호화 키 e(b)를 복호화하여 복호화 키 b를 획득할 수 있다. 또한 전자 기기 1(110)은 복호화 키 b를 이용하여 암호화된 컨텐츠 a(A)를 복호화하여 컨텐츠 A를 획득 및 재생할 수 있게 된다.

[0050] 이상의 실시예들에서는 클라이언트(일례로 전자 기기 1(110))가 생성하는 암호키가 대칭키인 경우를 설명하였으나, 암호키로서 공개키와 비밀키를 포함하는 비대칭키가 이용될 수도 있다. 예를 들어, 클라이언트는 클라이언트의 공개키를 서버(일례로 서버(150))의 공개키로 암호화하여 서버로 전송할 수 있다. 이때, 서버는 서버의 비밀키로, 암호화된 클라이언트의 공개키를 복호화하여 클라이언트의 공개키를 획득할 수 있고, 복호화 키를 클라이언트의 공개키로 암호화하여 클라이언트로 전송할 수 있다. 이 경우 클라이언트는 자신의 비밀키로, 암호화된 복호화 키를 복호화하여 복호화 키를 얻을 수 있다.

[0052] 이처럼 본 발명의 실시예들에 따르면, 클라이언트에서 재생하고자 하는 암호화된 컨텐츠에 대한 복호화 키를 안전하게 클라이언트로 전달함으로써 클라이언트에서 안전하게 컨텐츠를 재생할 수 있다.

[0053] 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, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate 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 어플리케이션을 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 설

명된 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 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0054] 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, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)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.

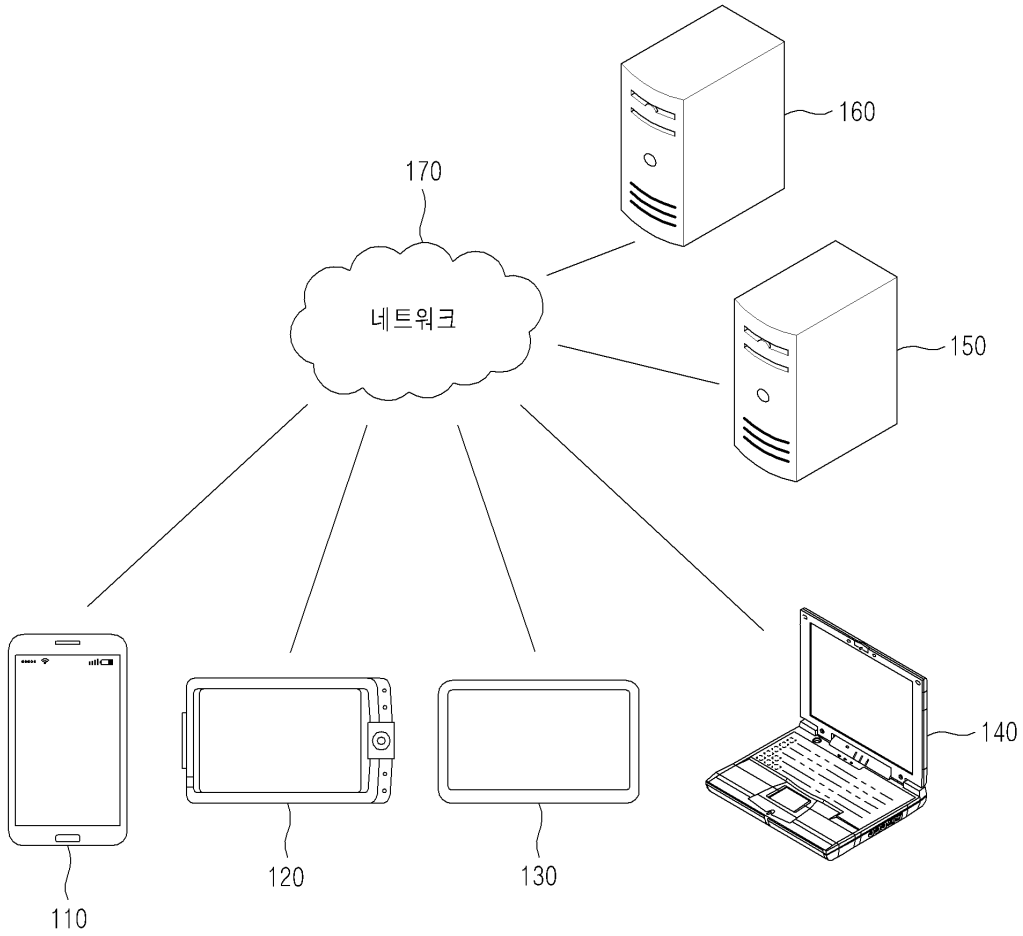
[0055] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic 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. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0056] 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.

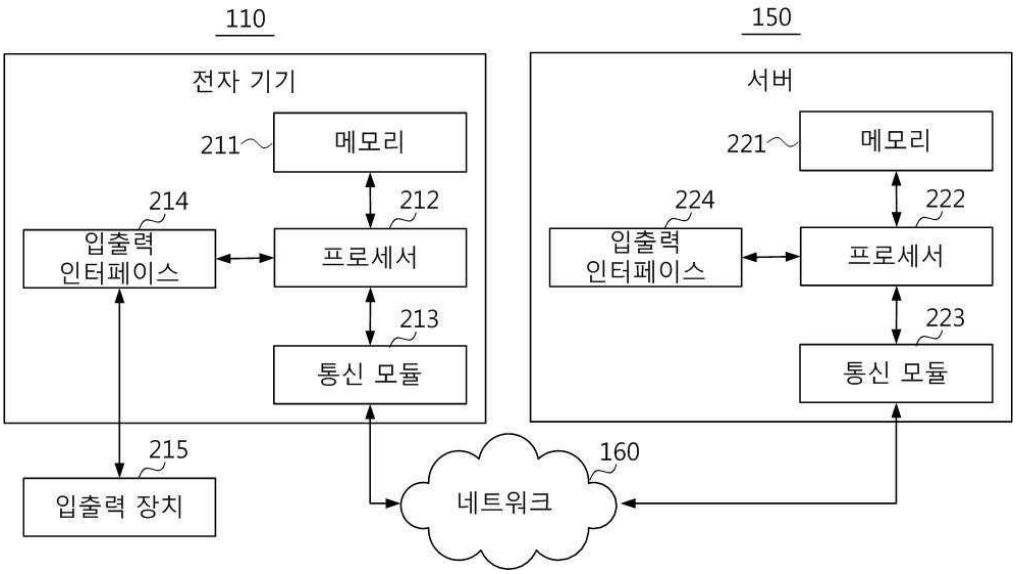
[0057] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

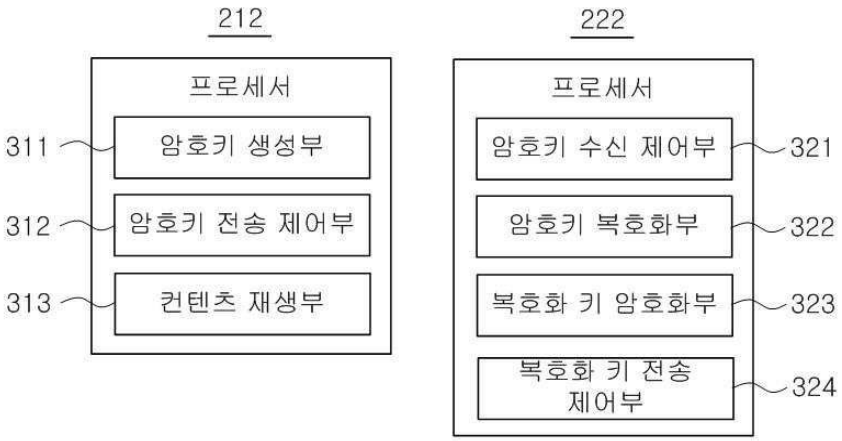
도면1



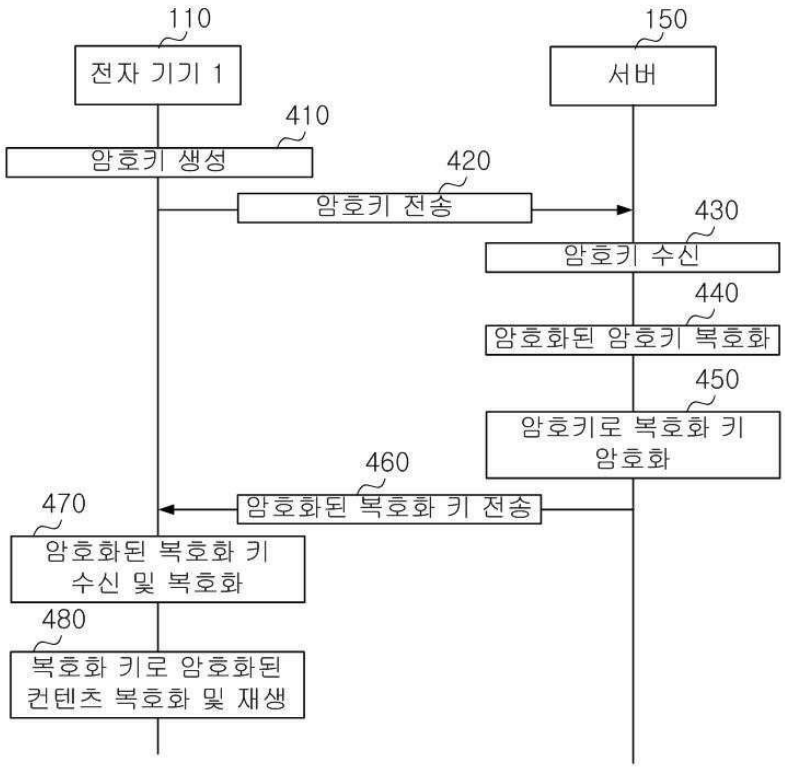
도면2


110
전자 기기
211
메모리
214
입출력 인터페이스
212
프로세서
213
통신 모듈
215
입출력 장치
150
서버
221
메모리
224
입출력 인터페이스
222
프로세서
223
통신 모듈
160
네트워크

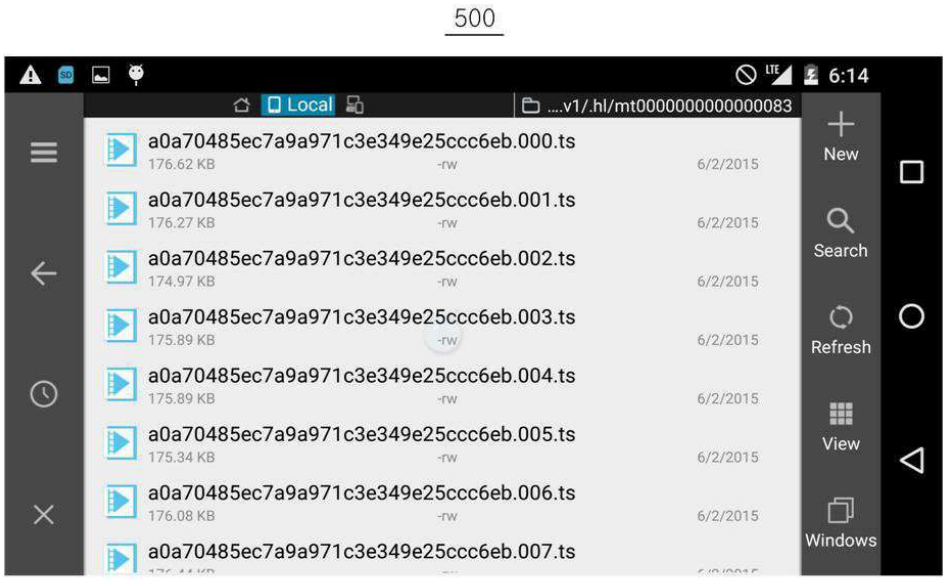
도면3


212
프로세서
311
암호키 생성부
312
암호키 전송 제어부
313
컨텐츠 재생부
222
프로세서
암호키 수신 제어부
321
암호키 복호화부
322
복호화 키 암호화부
323
복호화 키 전송 제어부
324

도면4


110
전자 기기 1
150
서버
410
암호키 생성
420
암호키 전송
430
암호키 수신
440
암호화된 암호키 복호화
450
암호키로 복호화 키 암호화
460
암호화된 복호화 키 전송
470
암호화된 복호화 키 수신 및 복호화
480
복호화 키로 암호화된 컨텐츠 복호화 및 재생

도면5


500
6:14
Local
....v1/.hl/mt0000000000000083
a0a70485ec7a9a971c3e349e25ccc6eb.000.ts
176.62 KB
-rw
6/2/2015
a0a70485ec7a9a971c3e349e25ccc6eb.001.ts
176.27 KB
-rw
6/2/2015
a0a70485ec7a9a971c3e349e25ccc6eb.002.ts
174.97 KB
-rw
6/2/2015
a0a70485ec7a9a971c3e349e25ccc6eb.003.ts
175.89 KB
-rw
6/2/2015
a0a70485ec7a9a971c3e349e25ccc6eb.004.ts
175.89 KB
-rw
6/2/2015
a0a70485ec7a9a971c3e349e25ccc6eb.005.ts
175.34 KB
-rw
6/2/2015
a0a70485ec7a9a971c3e349e25ccc6eb.006.ts
176.08 KB
-rw
6/2/2015
a0a70485ec7a9a971c3e349e25ccc6eb.007.ts
New
Search
Refresh
View
Windows

도면6

컨텐츠	➔ A
컨텐츠용 암호화 키	➔ a
컨텐츠용 복호화 키	➔ b
a로 암호화된 A	➔ a(A)
서버(150)의 공개키	➔ c
서버(150)의 비밀키	➔ d
전자 기기 1(110)의 암호키	➔ e