(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0076668
(43) 공개일자 2010년07월06일

(51) Int. Cl.
G06F 21/00 (2006.01) *G06F 15/16* (2006.01)
G06F 9/06 (2006.01)
(21) 출원번호 10-2008-0134793
(22) 출원일자 2008년12월26일
심사청구일자 2008년12월26일

(71) 출원인
이화여자대학교 산학협력단
서울 서대문구 대현동 11-1 이화여자대학교내
(72) 발명자
조동섭
서울특별시 송파구 문정동 패밀리아파트 223동 506호
서대희
서울특별시 영등포구 도림동 대우미래사랑아파트 101동 909호
(뒷면에 계속)
(74) 대리인
강경찬, 변창규

전체 청구항 수 : 총 5 항

(54) 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법

(57) 요 약

본 발명은 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법에 관한 것으로서, 더욱 상세하게는 웹 서버가 웹 페이지의 내용을 안전하게 보호하기 위해 하이퍼 링크를 암호화하여 클라이언트에게 전송하고 클라이언트는 사전에 공유한 키를 사용해 복호화를 수행하여 본래의 요청 페이지를 획득함으로써, 키를 공유하지 못한 사용자로 하여금 해당 웹 페이지에 하이퍼 링크로 연결된 다른 웹 페이지와 멀티미디어 데이터들로의 접근을 방지하여 웹 컨텐츠를 보호할 수 있도록 하는 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법에 관한 것이다.

본 발명인 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법은,

웹 서버/클라이언트 환경의 웹 콘텐츠 보호 방법에 있어서,

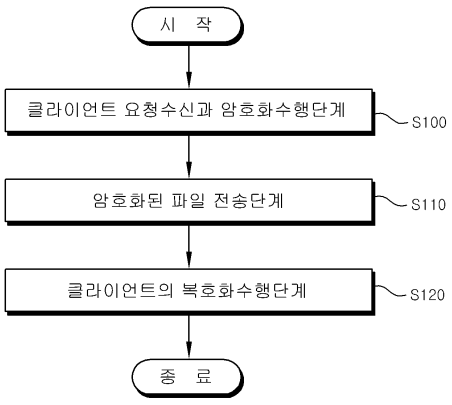
클라이언트의 웹 페이지 요청에 대해 일반 html 파일의 하이퍼링크에 대칭키 암호화 알고리즘을 이용하여 암호화를 수행하는 클라이언트요청수신과암호화수행단계(S100)와;

클라이언트에서 웹 서버로부터 암호화된 파일을 전송받는 암호화된파일전송단계(S110)와;

클라이언트에서 암호화된 파일에 복호화를 적용하여 본래의 html 파일을 획득하는 클라이언트의복호화수행단계(S120);를 포함하여 이루어지는 것을 특징으로 한다.

본 발명을 통해 클라이언트에게 사전에 암호화에 사용되는 대칭키를 분배함으로써 복호화에 동일한 대칭키를 사용하여 선별된 사용자들만이 웹 페이지에 링크되어있는 다른 문서들을 열람할 수 있고 이로 인해 인증과 기밀성을 유지할 수 있게 된다.

대 표 도 - 도2



(72) 발명자

문일형

서울특별시 중랑구 중화동 296-44 세광하나타운 다-208

한소희

서울특별시 영등포구 당산동5가 30번지 102호

특허청구의 범위

청구항 1

웹 서버/클라이언트 환경의 웹 콘텐츠 보호 방법에 있어서,

클라이언트의 웹 페이지 요청에 대해 일반 html 파일의 하이퍼링크에 대칭키 암호화 알고리즘을 이용하여 암호화를 수행하는 클라이언트요청수신과암호화수행단계(S100)와;

클라이언트에서 웹 서버로부터 암호화된 파일을 전송받는 암호화된파일전송단계(S110)와;

클라이언트에서 암호화된 파일에 복호화를 적용하여 본래의 html 파일을 획득하는 클라이언트의복호화수행단계(S120);를 포함하여 이루어지는 것을 특징으로 하는 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법.

청구항 2

제 1항에 있어서,

상기 클라이언트요청수신과암호화수행단계(S100)는,

웹 서버가 클라이언트로부터 HTTP 요청을 수신하는 단계(S101)와,

웹 서버 내의 특정 디렉토리로부터 요청 문서를 검색하는 단계(S102)와,

대칭키 암호화 모듈을 호출하는 단계(S103)와,

대칭키 암호화 모듈에서 하이퍼링크 검색 알고리즘을 호출하는 단계(S104)와,

하이퍼링크 검색 알고리즘에서 하이퍼링크 부분 만을 암호화하는 단계(S105)와,

암호화된 결과를 웹 서버에게 전달하는 단계(S106)를 포함하여 이루어지는 것을 특징으로 하는 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법.

청구항 3

제 2항에 있어서,

상기 암호화된 결과를 웹 서버에게 전달하는 단계(S106)에서,

암호화가 완료된 웹 페이지는 .des 의 확장자로 명시되는 것을 특징으로 하는 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법.

청구항 4

제 1항에 있어서,

상기 암호화된파일전송단계(S110)는,

웹 서버로부터 클라이언트에게 HTTP 프로토콜을 통해 암호화된 파일이 전송되는 것을 특징으로 하는 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법.

청구항 5

제 1항에 있어서,

상기 클라이언트의복호화수행단계(S120)는,

클라이언트가 웹 서버에게 HTTP 요청을 시도하는 단계(S121)와,

웹 서버로부터 암호화된 웹 페이지를 수신하는 단계(S122)와,

수신한 웹 페이지에 대해 대칭키 암호화 모듈을 호출하는 단계(S123)와,

대칭키 암호화 모듈에서 하이퍼링크 검색 알고리즘을 호출하는 단계(S124)와,

하이퍼링크 검색 알고리즘에서 하이퍼링크 부분만을 복호화하는 단계(S125)와,

복호화된 결과를 웹 브라우저에 전달하여 정상적인 HTML 문서를 출력하는 단계(S126)를 포함하여 이루어지는 것을 특징으로 하는 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법에 관한 것으로서, 더욱 상세하게는 웹 서버가 웹 페이지의 내용을 안전하게 보호하기 위해 하이퍼 링크를 암호화하여 클라이언트에게 전송하고 클라이언트는 사전에 공유한 키를 사용해 복호화를 수행하여 본래의 요청 페이지를 획득함으로써, 키를 공유하지 못한 사용자로 하여금 해당 웹 페이지에 하이퍼 링크로 연결된 다른 웹 페이지와 멀티미디어 데이터들로의 접근을 방지하여 웹 컨텐츠를 보호할 수 있도록 하는 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법에 관한 것이다.

배 경 기 술

[0002] 종래의 웹 컨텐츠 보호 방식은 아래와 같이 크게 메시지 기반 방식의 SHTTP(Secure-HTTP)와 채널 기반 방식의 SSL(Secure Socket Layter) 2가지로 요약할 수 있다.

[0003] 첫 번째로 메시지 기반 방식의 SHTTP는 다른 응용프로토콜(예, HTTP)에 의해 생성되는 메시지를 트랜잭션 단위로 암호화하는 방식으로 1994년 EIT(Enterprise Integration Technology)사에 의해 개발되었다.

[0004] HTTP와 같이 독립적으로 개발된 프로토콜이 아니라 기존의 HTTP 프로토콜에 보안기능을 추가하면서 HTTP의 서버/클라이언트 모델의 구조를 그대로 사용하는 것이다.

[0005] 따라서 요청 형식은 "Secure Secure-HTTP/1.1" 과 같고 기존의 GET/PUT 메쏘드와 구분하여 SHTTP를 수행하기 위해 Secure 메쏘드를 새롭게 정의하였다.

[0006] 프로토콜 지시자로 shttp를 사용하기 때문에 URL 형식은 “shttp:// "로 시작한다.

[0007] Request 전달시 헤더에 암호화와 관련된 정보가 포함되어 전송된다.

[0008] 전송 문서 형태는 확장된 HTML로 새로운 앵커 요소들이 추가되었다.

[0009] 링크 태그에 식별명(DN)과 암호 옵션(CRYPTOPS)을 지정할 수 있고 CERTS 태그를 통해 인증서를 지정할 수도 있다.

[0010] SHTTP는 SSL(Secure Socket Layer)이 암호화된 채널을 통해 서비스 단위로 암호화와 인증을 수행하는 것과 달리 전달되는 메시지 혹은 트랜잭션 단위로 암호화와 인증을 수행한다.

[0011] 지원하는 암호화 기법으로는 키 교환 알고리즘을 위해 RSA(Rivest Shamir Adleman), Diffie-Hellan, Kerberos를 사용하고 인증서 양식은 X.509, 캡슐화 형식은 PKCS-6을 사용한다.

[0012] 디지털 서명 알고리즘으로 RSA, DSA(Digital Signature Algorithm)와 메시지 다이제스트 알고리즘으로 MD2, MD5, SHA를 사용한다.

[0013] 그리고 전송 메시지 혹은 데이터 암호를 위해 DES, RC2 알고리즘을 사용한다.

[0014] 정상적인 HTTP 메시지는 위에서 언급한 암호화 기법을 통해 암호화 되거나 서명되고 난 뒤 PKCS-7 형식에 따라

캡슐화 된 후 전달계층인 TCP/IP 계층을 통해 SHTTP 헤더와 함께 전송된다.

[0015] 이때 SSL과의 중요한 차이점은 HTTP가 주고받는 메시지가 암호화 및 서명된 후 TCP/IP를 통해 전달된다는 것이다.

[0016] 이러한 SHTTP의 동작구조는 암호 옵션 태그를 사용함으로써 다양한 암호화 메커니즘을 적용할 수 있고, 메시지 기반 방식으로서 모든 TCP/IP 패킷이 암호화되어 전송되므로 강력한 암호화를 제공하며 클라이언트로 하여금 공개키를 유지하지 않아도 되도록 한다.

[0017] 그러나, SHTTP의 단점은 본래 SHTTP가 HTTP에 기반 해서 개발되었기 때문에 WWW에만 적용 가능하며 또한 SHTTP용 웹 서버와 웹 브라우저의 개발을 요구한다는 것이다.

[0018] 두 번째로 채널 기반 방식의 SSL(Secure Socket Layter)는 HTTP와 TCP/IP 사이에 보안계층을 삽입하여 채널 전체를 암호화하는 방식으로 SHTTP와 같이 특정 용용을 위한 보안 프로토콜이 아닌 일반적인 웹 보안 프로토콜로써 HTTP외에 다른 응용에도 적용 할 수 있다.

[0019] 네스케이프사에 의해 탄생한 SSL은 TCP/IP와 HTTP, SMTP와 같은 응용 프로토콜 사이에 존재하는 독립적인 레이어 기반의 프로토콜로 전송 혹은 서비스 수준의 암호화 프로토콜이다.

[0020] 네트워크레이어의 암호화 방식이므로 HTTP를 포함한 다른 응용 프로토콜에도 적용가능하다는 큰 장점을 지니고 있다.

[0021] SSL을 사용하기 위한 URL 표기 방식은 “https:// "이며 포트번호는 http의 80과 구분되는 별도의 443포트를 사용한다.

[0022] 따라서 하나의 브라우저로 https의 보안 웹 서버와 http의 보안기능이 없는 일반 웹 서버의 동시 사용이 가능하다.

[0023] 또한 SHTTP보다 하위계층에 있는 프로토콜이므로 SSL위에 SHTTP를 실행하는 것이 가능하여 SHTTP 보안의 안정성을 보완할 수 있다.

[0024] SSL의 동작은 Handshake Protocol(SSLHP) 단계에서 네트워크계층 사이에 공개키 암호화 기술을 이용한 소켓 루틴을 사용하여 안전한 암호화된 채널을 형성한 후 이 채널을 통해 웹 서버와 클라이언트의 인증과 세션 키 교환 과정을 수행하며 이 과정이 끝나면 Record Protocol(SSLRP) 단계에서 웹 서버와 클라이언트 간에 공유된 세션 키를 통해 대칭키 암호 알고리즘을 이용한 메시지 혹은 데이터의 암호화가 이루어진다.

[0025] 메시지 혹은 데이터 암호의 과정은 먼저 메시지가 block으로 나뉜 후 block이 압축되면 메시지 인증 코드(MAC-Message Authentication Code)가 추가되는 형식으로 진행된다.

[0026] 암호화된 메시지를 전송받으면 먼저 복호화를 실시하고 MAC을 확인한 후에 압축을 해제하고 block을 재배열하여 상위 프로토콜로 전달한다.

[0027] SSL이 지원하는 보안 서비스는 먼저 웹 서버와 클라이언트 사이의 인증 서비스로 RSA 비 대칭키 암호화 알고리즘을 사용한다.

[0028] 또한 웹 서버와 클라이언트 간의 신뢰성 있는 전송을 보장하기 위해 DES 대칭키 암호화 알고리즘을 이용해 데이터를 암호화하며 이때 사용되는 비밀 키(세션 키)는 미국 외에서 사용할 수 없다는 암호화 소프트웨어에 대한 법적 제한 때문에 현재 우리나라에서는 40bit 사이즈로 제한되어 사용되고 있다.

[0029] 마지막으로 메시지의 무결성을 위해 MAC을 MD5나 SHA와 같은 해쉬 함수로 검사한다.

[0030] SSL은 다른 기술에 비해 구축이 용이하고 모든 응용 프로토콜들에 적용되어 사용될 수 있다는 장점을 지닌 반면 IP Spoofing등의 해킹에 취약하고 인증서나 대칭키가 PC에 저장되어 있어야 하므로 클라이언트의 이동성에 제약을 두고 있다.

[0031] 또한 현재 대부분의 전자 상거래와 인터넷 뱅킹에 사용되고 있으나 온라인 쇼핑몰이나 각종 정보보호 사이트의 인증방식이 서로 상이하기 때문에 데이터 처리 속도가 매우 늦어 사용자들이 불편을 겪게 된다.

발명의 내용

해결 하고자하는 과제

[0032] 따라서, 본 발명은 상기 종래의 문제점을 해소하기 위해 안출된 것으로,

[0033] 본 발명의 목적은 웹 서버/클라이언트 환경에서 웹 페이지 내의 웹 링크들을 암호화함으로써 웹 콘텐츠를 보호하는 방법을 제공함에 목적이 있다.

[0034] 본 발명의 다른 목적은 웹 서버/클라이언트 환경에서 웹 페이지에 연결되어 있는 수많은 웹 문서들과 멀티미디어 데이터들에 대하여 불법으로 탈취, 배포하는 행위를 방지 할 수 있는 방법을 제공함에 있다.

과제 해결수단

[0035] 본 발명이 해결하고자 하는 과제를 달성하기 위하여,

[0036] 본 발명인 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법은,

[0037] 웹 서버/클라이언트 환경의 웹 콘텐츠 보호 방법에 있어서,

[0038] 클라이언트의 웹 페이지 요청에 대해 일반 html 파일의 하이퍼링크에 대칭키 암호화 알고리즘을 이용하여 암호화를 수행하는 클라이언트요청수신과암호화수행단계(S100)와;

[0039] 클라이언트에서 웹 서버로부터 암호화된 파일을 전송받는 암호화된파일전송단계(S110)와;

[0040] 클라이언트에서 암호화된 파일에 복호화를 적용하여 본래의 html 파일을 획득하는 클라이언트의복호화수행단계(S120);를 포함하여 이루어지는 것을 특징으로 한다.

효 과

[0041] 본 발명에 따른 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법은,

[0042] 웹 서버/클라이언트 환경에서 선별적인 사용자들에게 웹 컨텐츠를 제공할 수 있는 효과가 있다.

[0043] 즉, 클라이언트에게 사전에 암호화에 사용되는 대칭키를 분배함으로써 복호화에 동일한 대칭키를 사용하여 선별된 사용자들만이 웹 페이지에 링크되어있는 다른 문서들을 열람할 수 있고 이로 인해 인증과 기밀성을 유지할 수 있다.

[0044] 더불어 암호화된 하이퍼링크는 웹 링크를 보호하고 웹 링크에 의해 연결되어 있는 수많은 다른 문서들과 멀티미디어 데이터로의 접근을 방지하여 불법 복사나 배포를 방지할 수 있게 된다.

[0045] 또한, 일반 html 파일의 웹 링크 암호화를 통해 웹 링크에 연결된 문서들의 컨텐츠들을 보호 관리할 수 있는 효과가 있다.

발명의 실시를 위한 구체적인 내용

[0046] 상기 과제를 달성하기 위한 본 발명의 일실시예에 따른 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법은,

[0047] 웹 서버/클라이언트 환경의 웹 콘텐츠 보호 방법에 있어서,

[0048] 클라이언트의 웹 페이지 요청에 대해 일반 html 파일의 하이퍼링크에 대칭키 암호화 알고리즘을 이용하여 암호화를 수행하는 클라이언트요청수신과암호화수행단계(S100)와;

[0049] 클라이언트에서 웹 서버로부터 암호화된 파일을 전송받는 암호화된파일전송단계(S110)와;

[0050] 클라이언트에서 암호화된 파일에 복호화를 적용하여 본래의 html 파일을 획득하는
클라이언트의복호화수행단계(S120);를 포함하여 이루어지는 것을 특징으로한다.

[0051] 이때, 상기 클라이언트요청수신과암호화수행단계(S100)는,

[0052] 웹 서버가 클라이언트로부터 HTTP 요청을 수신하는 단계(S101)와,

[0053] 웹 서버 내의 특정 디렉토리로부터 요청 문서를 검색하는 단계(S102)와,

[0054] 대칭키 암호화 모듈을 호출하는 단계(S103)와,

[0055] 대칭키 암호화 모듈에서 하이퍼링크 검색 알고리즘을 호출하는 단계(S104)와,

[0056] 하이퍼링크 검색 알고리즘에서 하이퍼링크 부분 만을 암호화하는 단계(S105)와,

[0057] 암호화된 결과를 웹 서버에게 전달하는 단계(S106)를 포함하여 이루어지는 것을 특징으로 한다.

[0058] 이때, 상기 암호화된 결과를 웹 서버에게 전달하는 단계(S106)에서,

[0059] 암호화가 완료된 웹 페이지는 .des 의 확장자로 명시되는 것을 특징으로 한다.

[0060] 이때, 상기 암호화된파일전송단계(S110)는,

[0061] 웹 서버로부터 클라이언트에게 HTTP 프로토콜을 통해 암호화된 파일이 전송되는 것을 특징으로 한다.

[0062] 이때, 상기 클라이언트의복호화수행단계(S120)는,

[0063] 클라이언트가 웹 서버에게 HTTP 요청을 시도하는 단계(S121)와,

[0064] 웹 서버로부터 암호화된 웹 페이지를 수신하는 단계(S122)와,

[0065] 수신한 웹 페이지에 대해 대칭키 암호화 모듈을 호출하는 단계(S123)와,

[0066] 대칭키 암호화 모듈에서 하이퍼링크 검색 알고리즘을 호출하는 단계(S124)와,

[0067] 하이퍼링크 검색 알고리즘에서 하이퍼링크 부분만을 복호화하는 단계(S125)와,

[0068] 복호화된 결과를 웹 브라우저에 전달하여 정상적인 HTML 문서를 출력하는 단계(S126)를 포함하여 이루어지는 것을 특징으로 한다.

[0069] 이하, 첨부된 도면을 참조하여 본 발명인 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법의 바람직한 실시예를 상세하게 설명한다.

[0070] 도 1은 본 발명의 일실시예에 따른 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법을 나타내는 시스템 구성도이다.

[0071] 도 2는 본 발명의 일실시예에 따른 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법의 흐름도이다.

[0072] 도 1을 참조하여 설명하자면, 본 발명의 방법을 수행하기 위한 시스템은,

[0073] 대칭키 암호화 모듈(300)과 하이퍼링크 검색 알고리즘을 통해 웹 링크들을 암호화하는 웹 서버(100)와;

[0074] 요청한 웹 페이지에 대해 암호화가 수행된 파일을 받아 복호화를 수행하기 위하여 복호화모듈(400)을 포함하여 구성되는 클라이언트(200)로 구성된다.

[0075] 먼저, 안전한 웹 컨텐츠 보호 방법을 위한 가정 사항은 다음과 같다.

[0076] ① 본 발명에서 웹 컨텐츠는 웹 서버/클라이언트 환경에서 웹 페이지 내의 웹 링크를 통해 연결되는 다른 웹 페이지나 데이터를 의미하는 것으로 정의한다.

[0077] ② 암호화에 사용된 키는 RSA 키 교환 알고리즘을 통해 웹 서버와 클라이언트 사이에 사전에 안전하게 주고받았다.

[0078] ③ RSA 비 대칭키 알고리즘에 사용되는 공개키와 개인키는 웹 서버와 클라이언트 각각이 공인된 인증기관으로부터 인증받아 생성한 것이다.

[0079] 이어, 웹 서버/클라이언트 환경에서 웹 서버와 클라이언트가 동일한 대칭키를 소유하고 이 대칭키를 이용해 웹 서버에서는 암호화를, 클라이언트에서는 복호화를 수행하여 안전하게 컨텐츠를 보호할 수 있는 방식이며, 다음과 같은 흐름을 갖는다.

[0080] (Step 1) 클라이언트 요청 수신과 암호화 수행단계(S100)

[0081] ① 웹 서버(100)는 클라이언트(200)로부터 웹 페이지 요청을 수신하게 되며, 본 발명은 웹 페이지 내의 하이퍼링크들로 연결된 문서의 컨텐츠를 보호하는 것이 목적이기 때문에 클라이언트(200)의 웹 페이지에 대한 별도의 암호화 요구가 없어도 자동으로 웹 페이지를 암호화 한다.(S101)

[0082] ② 웹 서버(100)는 서버내의 해당 디렉토리로부터 요청된 페이지를 검색하며, 클라이언트(200)로부터 요청된 페이지는 웹 서버(100)의 특정 디렉토리로부터 검색되며 파일의 확장자를 달리한 암호화가 완료된 파일 역시 원본 파일과 같은 디렉토리에 저장된다.(S102)

[0083] ③ 페이지 검색이 완료되면 웹 서버(100)는 페이지의 암호화를 위해 대칭키 암호화 모듈(300)의 수행을 요청한다.(S103)

[0084] 이때 수행 명령어는,

[0085] ShellExecute(NULL, "open", "C:₩₩WebPages₩₩DES₩₩Debug₩₩des.exe", parameter, NULL, SW_SHOW); 이다.

[0086] ④ 대칭키 암호화 모듈(300)은 하이퍼링크 검색 알고리즘을 호출한다.(S104)

[0087] ⑤ 하이퍼링크 검색 알고리즘은 웹 페이지의 소스에서 하이퍼링크만을 검색하고 이를 암호화한다.(S105)

[0088] 이때 하이퍼링크 검색 알고리즘 흐름은,

[0089] while(hPosition<8 && textBuff[t] != 'h') { //'href'의 검사

[0090] //'href'단어가 있다면

[0091] if(textBuff[1]=='r' && textBuff[2]=='e' && textBuff[3]=='f')

[0092] DoEncryption(); //암호화

[0093] //'href'단어의 일부만 있다면

[0094] else if(textBuff[6]=='r' && textBuff[7]=='e')

[0095] if(next_textBuff[0]=='f') //다시 검사

[0096] DoEncryption();

[0097] //'href'가 없다면

[0098] else

[0099] copy to targetData

[0100] }

[0101] 이다.

[0102] 이때 암호화된 결과는,

[0103] href="/css/www.css?20081021" -> href="?c}V?a.css?20081021" 이다.

[0104] ⑥ 암호화 모듈(300)은 암호화 과정이 끝나면 웹 서버에게 암호화된 페이지를 전달한다.

[0105] 암호화가 완료된 웹 페이지는 '.des'의 확장자로 명시된다.(S106)

[0106] (Step 2) 암호화된 파일 전송단계(S110)

[0107] 웹 서버로부터 클라이언트에게 HTTP 프로토콜을 통해 암호화된 파일이 전송된다.

[0108] (Step 3) 클라이언트의 복호화 수행단계(S120)

[0109] 클라이언트에서 암호화된 파일에 복호화를 적용하여 본래의 html 파일을 획득하는 단계이다.

[0110] ① 클라이언트는 먼저 웹 서버에게 HTTP 요청을 시도한다.(S121)

[0111] ② 웹 서버로부터 암호화된 웹 페이지를 수신한다.(S122)

[0112] 요청한 웹 페이지는 '.html' 파일이지만 웹 서버로부터 전송받는 결과는 암호화가 수행된 '.des' 파일이다.

[0113] 따라서 클라이언트는 이미 소유하고 있는 대칭키를 통해 복호화를 수행하여 웹 서버에게 요청했던 본래의

'.html'파일을 얻을 수 있다.

[0114] 반면 대칭키를 소유하고 있지 않거나 다른 대칭키를 소유하고 있는 클라이언트는 '.des'파일 수신 후 복호화를 진행할 수 없으므로 정상적인 '.html'파일을 얻을 수 없다.

[0115] ③ 클라이언트는 대칭키 복호화 모듈(400)의 수행을 요청한다.(S123)

[0116] 이때 수행 명령어는,

[0117] ShellExecute(NULL,
"open","C:₩₩WebPages₩₩desFinal₩₩Debug₩₩des.exe", parameter, NULL, SW_SHOW); 이다.

[0118] ④ 대칭키 복호화 모듈은 하이퍼링크 검색 알고리즘을 호출한다.(S124)

[0119] ⑤ 하이퍼링크 검색 알고리즘은 웹 페이지 소스의 암호화된 하이퍼링크 부분을 복호화 한다.(S125)

[0120] 클라이언트 측에서 진행되는 복호화 과정 역시 웹 서버에서 웹 페이지 내의 'href'를 검색하여 'href' 문자열 다음 부분을 암호화 한 것과 마찬가지로 'href' 다음에 나타나는 복호화 부분을 textBuff로 읽어 들여 복호화 과정을 수행한다.

[0121] ⑥ 복호화 과정이 완료되면 웹 브라우저는 정상적인 HTML 문서를 출력한다.(S126)

[0122] 이때 복호화된 결과는,

[0123] href="?c}V?a.css?20081021" -> href="/css/www.css?20081021" 이다.

[0124] 상기와 같은 동작 과정을 통해 웹 서버/클라이언트 환경에서 HTTP와 HTML에 의한 노출이 불가피한 웹 페이지 내의 콘텐츠들을 웹 링크의 암호화를 통해 안전하게 보호할 수 있다.

[0125] 클라이언트에게 사전에 암호화에 사용되는 대칭키를 분배함으로써 복호화에 동일한 대칭키를 사용하여 선별된 사용자들만이 웹 페이지에 링크되어있는 다른 문서들을 열람할 수 있고 이로 인해 인증과 기밀성을 유지할 수 있다.

[0126] 더불어 암호화된 하이퍼링크는 웹 링크를 보호하고 웹 링크에 의해 연결되어 있는 수많은 다른 문서들과 멀티미디어 데이터로의 접근을 방지하여 불법 복사나 배포를 방지할 수 있게 된다.

[0127] 이상에서와 같은 내용의 본 발명이 속하는 기술분야의 당업자는 본 발명의 기술적 사상이나 필수적 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시 예들은 모든 면에서 예시된 것이며 한정적인 것이 아닌 것으로서 이해해야만 한다.

[0128] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구 범위의 의미 및 범위 그리고 그 등가 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

산업이용 가능성

[0129] 본 발명에 따른 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법은,

[0130] 웹 서버/클라이언트 환경에서 웹 링크에 의해 연결되어 있는 수많은 데이터들을 보호할 수 있는 효과를 지니며 웹을 기반 기술로 서비스가 확장되어가는 방송통신 융합 환경에서 사용가치가 높을 것이다.

도면의 간단한 설명

[0131] 도 1은 본 발명의 일실시예에 따른 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법을 나타내는 시스템 구성도이다.

[0132] 도 2는 본 발명의 일실시예에 따른 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법의 흐름도이다.

[0133] 도 3은 본 발명의 일실시예에 따른 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법의 클라이언트요청수신과암호화수행단계를 구체적으로 나타낸 흐름도이다.

[0134] 도 4는 본 발명의 일실시예에 따른 웹 링크의 암호화를 통한 웹 컨텐츠의 보호 방법의 클라이언트의복호화수행

단계를 구체적으로 나타낸 흐름도이다.

[0135] * 도면의 주요 부분에 대한 부호의 설명 *

[0136] 100 : 웹서버

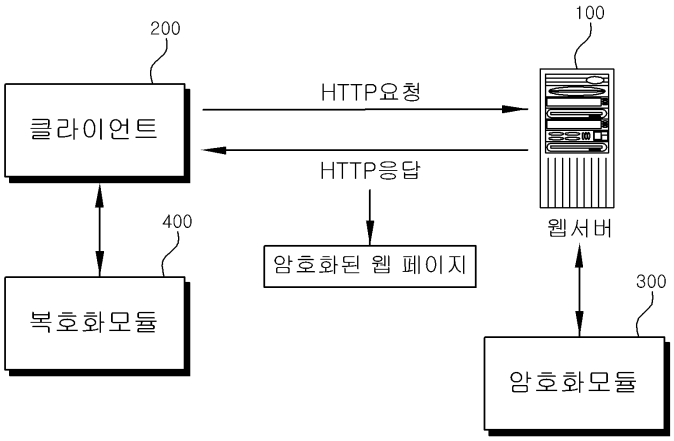
[0137] 200 : 클라이언트

[0138] 300 : 암호화모듈

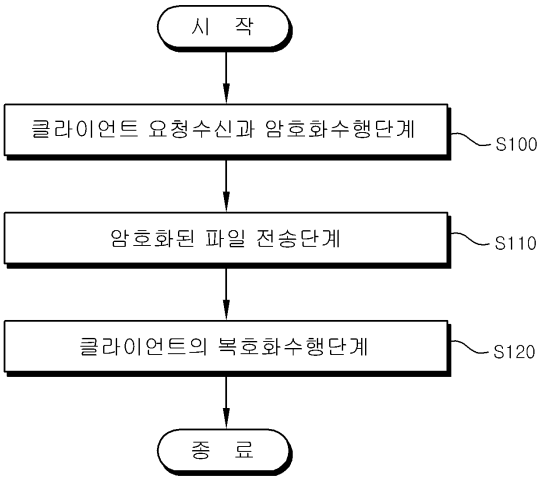
[0139] 400 : 복호화모듈

도면

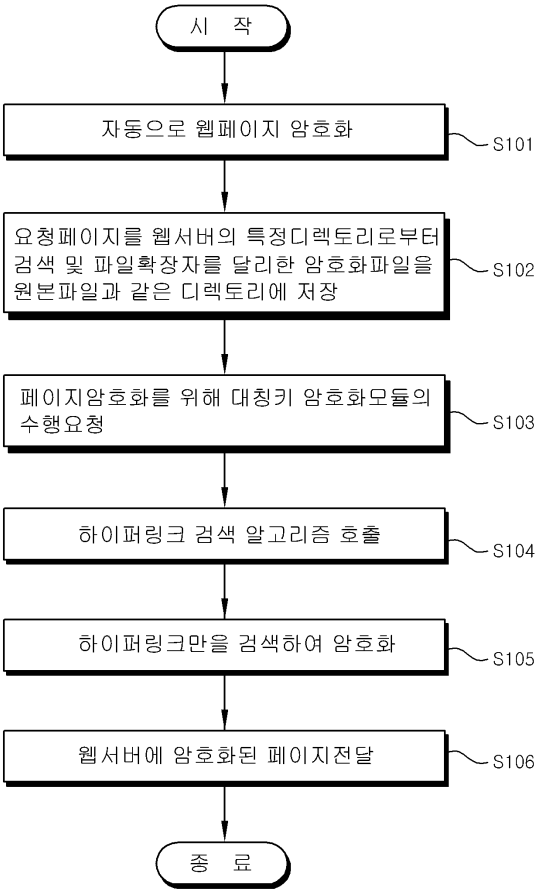
도면1



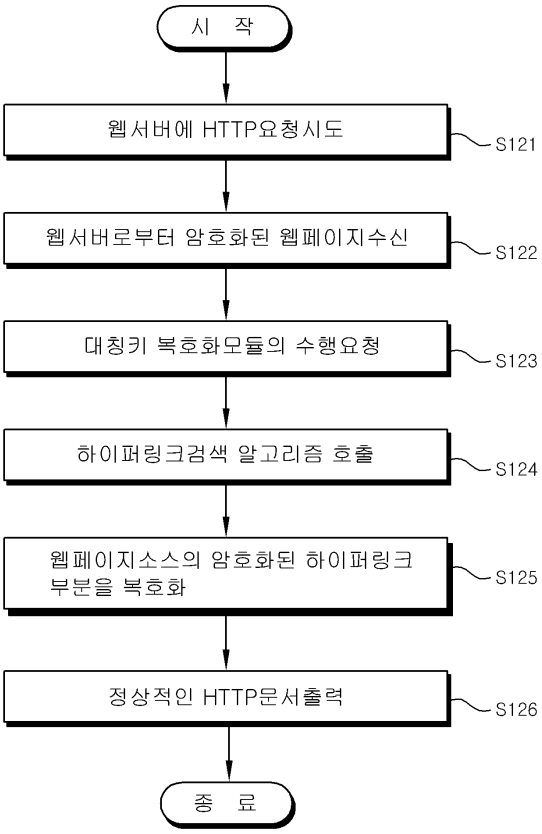
도면2



도면3


시 작
자동으로 웹페이지 암호화
S101
요청페이지를 웹서버의 특정디렉토리로부터 검색 및 파일확장자를 달리한 암호화파일을 원본파일과 같은 디렉토리에 저장
S102
페이지암호화를 위해 대칭키 암호화모듈의 수행요청
S103
하이퍼링크 검색 알고리즘 호출
S104
하이퍼링크만을 검색하여 암호화
S105
웹서버에 암호화된 페이지전달
S106
종 료

도면4


시 작
웹서버에 HTTP요청시도
S121
웹서버로부터 암호화된 웹페이지수신
S122
대칭키 복호화모듈의 수행요청
S123
하이퍼링크검색 알고리즘 호출
S124
웹페이지소스의 암호화된 하이퍼링크 부분을 복호화
S125
정상적인 HTTP문서출력
S126
종 료