(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0058220
(43) 공개일자 2015년05월28일

(51) 국제특허분류(Int. Cl.)
H04L 29/08 (2006.01) *H04L 29/06* (2006.01)
H04L 29/12 (2006.01)
(52) CPC특허분류
H04L 67/02 (2013.01)
H04L 61/1511 (2013.01)
(21) 출원번호 10-2015-7006803
(22) 출원일자(국제) 2013년09월16일
심사청구일자 없음
(85) 번역문제출일자 2015년03월17일
(86) 국제출원번호 PCT/EP2013/069178
(87) 국제공개번호 WO 2014/044641
국제공개일자 2014년03월27일
(30) 우선권주장
12306126.9 2012년09월18일
유럽특허청(EPO)(EP)

(71) 출원인
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 루 잔다르크 1-5
(72) 발명자
르 스꾸아르네 니꼴라
프랑스 35 576 세송 세비네 아브뉘 데 샹 블랑 975 자끄 데 샹 블랑 씨에스 176 16 테크니컬러 알 앤드 디 프랑스
르 메레 에르완
프랑스 35 576 세송 세비네 아브뉘 데 샹 블랑 975 자끄 데 샹 블랑 씨에스 176 16 테크니컬러 알 앤드 디 프랑스
스트롭 질
프랑스 35 576 세송 세비네 아브뉘 데 샹 블랑 975 자끄 데 샹 블랑 씨에스 176 16 테크니컬러 알 앤드 디 프랑스
(74) 대리인
특허법인코리아나

전체 청구항 수 : 총 12 항

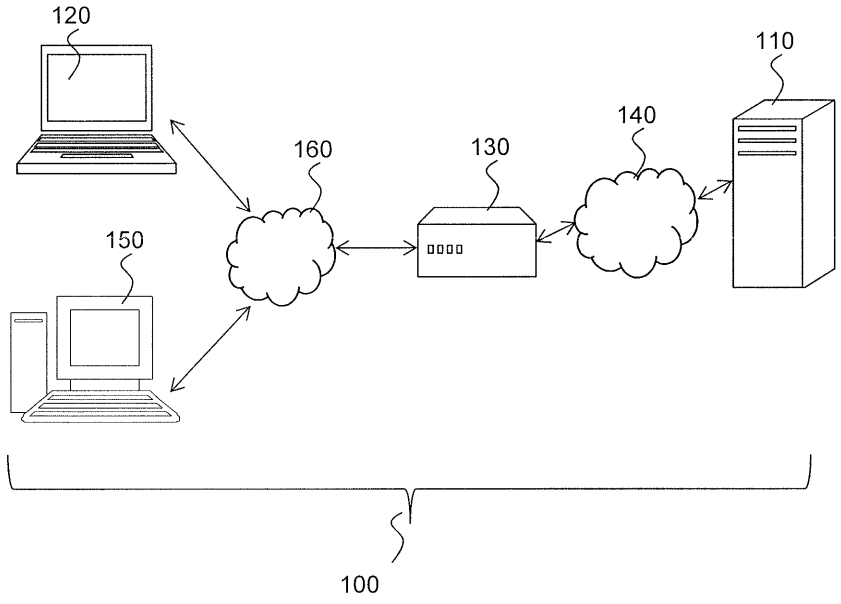
(54) 발명의 명칭 **웹 서비스를 안전하게 액세스하기 위한 방법 및 디바이스**

(57) 요 약

본 발명은 네트워크를 통해 사용자 디바이스 상에서 웹 애플리케이션을 실행하는 브라우저에 의해 웹 서비스를 안전하게 액세스하는 방법에 관한 것이다. 웹 서비스는 적어도 하나의 디바이스에 의해 호스팅되고, 그 적어도 하나의 디바이스 중에서 로컬 디바이스가 사용자 디바이스에 의해 액세스되고 있다. 로컬 디바이스는, 로

(뒷면에 계속)

대 표 도 - 도1



컬 디바이스를 고유하게 식별하는 글로벌 명칭 및 글로벌 명칭에 연관된 인증서를 포함한다. 방법은, 웹 서비스를 호스팅하는 임의의 디바이스를 식별하는 일반 명칭을 어드레싱함으로써 웹 서비스를 액세스하기 위한 요청을 네트워크에 웹 애플리케이션에 의해 전송하는 단계; 웹 서비스를 호스팅하는 로컬 디바이스를 식별하는 글로벌 명칭을 포함하는 요청에 대한 응답을 웹 애플리케이션에 의해 네트워크로부터 수신하는 단계; 수신된 글로벌 명칭이 리스트에 포함된 것을 웹 애플리케이션에 의해 검증하는 단계; 및 검증이 성공적인 경우에, 글로벌 명칭을 어드레싱함으로써 로컬 디바이스에 연결하는 단계; 로컬 디바이스로부터 인증서를 수신하는 단계; 브라우저에 의해 글로벌 명칭에 연관된 인증서를 검증하는 단계 및 웹 서비스를 안전하게 액세스하는 단계를 더 포함한다. 일반 명칭은, 웹 서비스들을 호스팅하는 모든 디바이스들에 대해 공통인, 그 명칭 하에 임의의 로컬 디바이스가 액세스가능한 명칭이다. 리스트는 웹 서비스를 호스팅기 위해 신뢰되고 있는 디바이스들의 글로벌 명칭들을 포함한다.

(52) CPC특허분류
H04L 61/305 (2013.01)
H04L 63/0823 (2013.01)
H04L 67/2814 (2013.01)

명 세 서

청구범위

청구항 1

네트워크 (160) 를 통해 사용자 디바이스 (120) 상에서 웹 애플리케이션을 실행하는 브라우저에 의해 웹 서비스를 안전하게 (securely) 액세스하는 방법으로서,

상기 웹 서비스는 적어도 하나의 디바이스에 의해 호스팅되고, 상기 적어도 하나의 디바이스 중에서 로컬 디바이스 (150, 130) 가 상기 사용자 디바이스에 의해 액세스되고 있으며,

상기 방법은, 상기 로컬 디바이스 (150, 130) 가, 상기 로컬 디바이스를 고유하게 식별하는 글로벌 명칭 (301) 및 상기 글로벌 명칭에 연관된 인증서를 포함하는 것을 특징으로 하고,

상기 방법은,

· 상기 웹 서비스를 호스팅하는 임의의 디바이스를 식별하는 일반 명칭 (300) 을 어드레싱함으로써 상기 웹 서비스를 액세스하기 위한 요청을 상기 네트워크 (160) 에 상기 웹 애플리케이션에 의해 전송하는 단계;

· 상기 요청에 대한 응답을 상기 웹 애플리케이션에 의해 상기 네트워크 (160) 로부터 수신하는 단계로서, 상기 응답은 상기 웹 서비스를 호스팅하는 상기 로컬 디바이스 (130, 150) 를 식별하는 상기 글로벌 명칭 (301) 을 포함하는, 상기 요청에 대한 응답을 상기 웹 애플리케이션에 의해 상기 네트워크 (160) 로부터 수신하는 단계;

· 수신된 상기 글로벌 명칭이 리스트에 포함된 것을 상기 웹 애플리케이션에 의해 검증하는 단계; 및

· 상기 검증이 성공적인 경우에, 상기 글로벌 명칭 (301) 을 어드레싱함으로써 상기 로컬 디바이스 (150, 130) 에 연결하고; 상기 로컬 디바이스로부터 상기 인증서를 수신하며; 상기 브라우저에 의해 상기 글로벌 명칭에 연관된 상기 인증서를 검증하고, 상기 웹 서비스를 안전하게 액세스하는 단계를 더 포함하는, 웹 서비스를 안전하게 액세스하는 방법.

청구항 2

제 1 항에 있어서,

상기 리스트는 상기 웹 서비스를 호스팅하기 위해 신뢰되고 있는 디바이스들의 글로벌 명칭들을 포함하는, 웹 서비스를 안전하게 액세스하는 방법.

청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 로컬 디바이스는 신뢰된 오퍼레이터에 의해 상기 글로벌 명칭 및 상기 글로벌 명칭에 연관된 상기 인증서를 전달받는, 웹 서비스를 안전하게 액세스하는 방법.

청구항 4

제 3 항에 있어서,

상기 리스트는 상기 브라우저에서 실행되는 상기 웹 애플리케이션에 의해 상기 신뢰된 오퍼레이터로부터 동적으로 획득되는, 웹 서비스를 안전하게 액세스하는 방법.

청구항 5

제 3 항에 있어서,

상기 리스트는 상기 브라우저에서 실행되는 상기 웹 애플리케이션에서 하드 코딩되는, 웹 서비스를 안전하게 액세스하는 방법.

청구항 6

제 1 항 내지 제 5 항 중 어느 한 항에 있어서,

상기 글로벌 명칭 (301) 을 어드레싱함으로써 상기 로컬 디바이스 (150, 130) 에 연결하는 것은, 글로벌 명칭 (301) 을 어드레싱함으로써 상기 웹 서비스를 액세스하기 위한 제 2 요청을 외부 네트워크 (140) 에 전송하고; 상기 제 2 요청에 대한 응답을 상기 네트워크 (140) 로부터 수신하는 것을 더 포함하고,

상기 응답은 상기 로컬 디바이스 (130, 150) 의 로컬 IP 어드레스를 포함하는, 웹 서비스를 안전하게 액세스하는 방법.

청구항 7

제 6 항에 있어서,

신뢰된 오퍼레이터에 대해 상기 글로벌 명칭에 연관된 상기 로컬 디바이스의 상기 로컬 IP 어드레스를 발행하는 예비 단계를 더 포함하는, 웹 서비스를 안전하게 액세스하는 방법.

청구항 8

제 6 항 또는 제 7 항에 있어서,

상기 로컬 디바이스의 상기 로컬 IP 어드레스와 상기 글로벌 명칭 사이의 맵핑이 상기 신뢰된 오퍼레이터에 의해 실행되는 DNS 서비스에 의해 유지되는, 웹 서비스를 안전하게 액세스하는 방법.

청구항 9

제 1 항 내지 제 8 항 중 어느 한 항에 있어서,

상기 일반 명칭을 어드레싱함으로써 상기 웹 서비스를 액세스하기 위한 상기 요청은, HTTP 요청인, 웹 서비스를 안전하게 액세스하는 방법.

청구항 10

제 1 항 내지 제 9 항 중 어느 한 항에 있어서,

상기 글로벌 명칭을 어드레싱함으로써 상기 웹 서비스를 안전하게 액세스하기 위한 요청은, HTTPS 요청인, 웹 서비스를 안전하게 액세스하는 방법.

청구항 11

제 1 항 내지 제 10 항 중 어느 한 항에 있어서,

상기 로컬 디바이스는 게이트웨이인, 웹 서비스를 안전하게 액세스하는 방법.

청구항 12

네트워크를 통해 웹 애플리케이션을 실행하는 브라우저에 의해 웹 서비스를 안전하게 (securely) 액세스하기 위한 사용자 디바이스 (120, 400) 로서,

상기 웹 서비스는 적어도 하나의 디바이스에 의해 호스팅되고, 상기 적어도 하나의 디바이스 중에서 로컬 디바이스가 상기 사용자 디바이스에 의해 액세스되고 있으며,

상기 디바이스는,

· 상기 웹 서비스를 호스팅하는 임의의 디바이스를 식별하는 일반 명칭을 어드레싱함으로써 상기 웹 서비스를 액세스하기 위한 요청을 상기 네트워크에 상기 웹 애플리케이션에 의해 전송하는 수단;

· 상기 웹 서비스를 호스팅하는 상기 로컬 디바이스를 고유하게 식별하는 글로벌 명칭을 포함하는 상기 요청에 대한 응답을 상기 웹 애플리케이션에 의해 상기 네트워크로부터 수신하는 수단;

· 수신된 상기 글로벌 명칭이 리스트에 포함된 것을 상기 웹 애플리케이션에 의해 검증하는 수단으로서, 상기 리스트는 상기 웹 서비스를 호스팅하기 위해 신뢰되고 있는 디바이스들의 글로벌 명칭들을 포함하는, 상기 검증하는 수단;

· 상기 글로벌 명칭을 어드레싱함으로써 상기 로컬 디바이스에 상기 웹 애플리케이션에 의해 연결하는 수단, 상기 로컬 디바이스로부터 수신된 인증서를 수신하는 수단, 및 상기 브라우저에 의해 상기 글로벌 명칭에 연관된 상기 인증서를 검증하는 수단 및 상기 웹 서비스를 안전하게 액세스하는 수단을 포함하는, 사용자 디바이스.

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 웹 서비스에 대한 보안 액세스 (secure access) 의 분야에 관한 것이다. 보다 정확하게는, 본 발명은, 네트워크를 통해 사용자 디바이스 상에서 웹 애플리케이션을 실행하는 브라우저에 의해 웹 서비스를 안전하게 액세스하는 방법에 관한 것이고, 여기서, 웹 서비스는 로컬 디바이스에 의해 호스팅된다.

배 경 기 술

[0002] 이 섹션은 이하 설명되고 및/또는 청구되는 본 발명의 다양한 양태들에 관련될 수도 있는 기술분야의 다양한 양태들에 독자를 소개하도록 의도된다. 이 논의는, 독자에게 본 발명의 다양한 양태들의 더 나은 이해를 용이하게 하기 위해 배경 정보를 제공하는 것에 도움이 될 것으로 믿는다. 따라서, 이들 진술들은 이러한 견지에서 읽혀져야 하고 종래 기술의 인정들로서 읽혀져서는 아니된다는 것을 이해하여야 한다.

[0003] 디지털 데이터 (예를 들어, 사진들, 비디오들) 는 모바일 디바이스들 (예를 들어, 스마트폰들, 태블릿들, 랩톱들) 상에서 점점 더 많이 생산되고 관리된다. 이 데이터는 또한 종종 인터넷을 통해 공유되거나, 백업되거나, 또는 프로세싱된다. 실제로, 광범위한 "클라우드 (cloud)" 서비스들은 사용자들의 콘텐츠를 그들이 사진 처리 서비스들, 소셜 네트워크들 또는 온라인 스토리지 (storage) 에 있도록 다룬다. 이들 클라우드 서비스들의 대부분은 웹 기술들에 전적으로 의존한다. 그 결과로서, 사용자들은 대량의 콘텐츠를 HTTP 를 통해 웹 애플리케이션들에 업로드할 필요가 있다. 하지만, 업로드들의 속도는 이용가능한 대역폭에 의해 제한된다. 실제로, 인터넷에 대한 연결 속도는 레거시 (legacy) 인프라스트럭처들 (xDSL) 의, 또는 공유된 매체 (셀룰러) 의 사용으로 인해 제한된 채로 유지된다.

[0004] 긴 업로드 시간들은 사용자들이 그들의 독립형 디바이스들을 대기시키거나 전원을 끄는 것을 방해하고, 이들 사용자들이 그들의 디바이스들을 인터넷을 통한 전송을 처리하도록 연결된 채로 유지하는 것을 필요로 한다. 이들 이슈들을 경감시키기 위해, 가정용 게이트웨이와 같은, 네트워크에 영구적으로 연결되는 제 3 자 디바이스에 HTTP 를 통해 업로드들을 오프로드 (offload) 하기 위한 메커니즘이 제안된다. 오프로딩 웹 서비스를 제공하는 제 3 자 디바이스를 로케이팅하는 방법이 따라서 제안된다.

[0005] 하지만, 제 3 자에 태스크 (task) 를 오프로딩하는 것은 이 제 3 자를 신뢰할 것을 필요로 한다, 즉, 오프로드 서비스를 제공하는 제 3 자 디바이스는 사용자 독립형 디바이스에 의해 인증될 필요가 있다. 디바이스 또는 웹 서비스를 인증하기 위한 알려진 솔루션 (solution) 은 인증 기관 (trust authority) 에 의한 인증 (certification) 에 기초한다. 인증서들 (certificates) 은 인증 기관에 의해 웹 서비스를 소유하는 신뢰된 오퍼레이터 (trusted operator) 에 또는 아니면 사용자의 물리적인 디바이스에 전달된다. 하지만, 이들 솔루션들은 웹 브라우저와 같은 레거시 소프트웨어, 및 프로세싱 환경이 제한되는 표준 웹 프로토콜들과 양립가능하지 않다. 다시 말해서, 브라우저는 입력들 및 출력들의 면에서 제한되고, 예를 들어, 브라우저는 그것이 실행되는 디바이스의 (하드 디스크 드라이브와 같은) 저장 매체에 액세스할 수 없고, 네트워크에 직접 액세스할 수 없다.

[0006] 로컬 디바이스에 의해 웹 서비스가 호스팅되는 경우에, 네트워크를 통해 사용자 디바이스 상에서 웹 애플리케이션을 실행하는 브라우저에 의해 웹 서비스를 안전하게 액세스하기 위한 솔루션이 따라서 필요하다. 방법은 구현 및 이용이 쉽도록 신중하게 간단하여야 하고, 레거시 소프트웨어와 양립가능하여야 하며, JavaScript 에서 구현되도록 그리고 브라우저에서 실행되도록 적응되어야 한다.

[0007] 본 발명은 이러한 솔루션을 제공한다.

발명의 내용

과제의 해결 수단

[0008] 일 양태에서, 본 발명은 네트워크를 통해 사용자 디바이스 상에서 웹 애플리케이션을 실행하는 브라우저에 의해

웹 서비스를 안전하게 액세스하는 방법에 지향된다. 웹 서비스는 적어도 하나의 디바이스에 의해 호스팅되고, 그 적어도 하나의 디바이스 중에서 로컬 디바이스가 사용자 디바이스에 의해 액세스되고 있다. 유리하게, 로컬 디바이스는 웹 서비스를 호스팅하고 사용자 디바이스에 가장 가까운 디바이스이다. 로컬 디바이스는, 로컬 디바이스를 고유하게 식별하는 글로벌 명칭 (global name) 및 글로벌 명칭에 연관된 인증서 (certificate) 를 포함한다. 방법은, 웹 서비스를 호스팅하는 임의의 디바이스를 식별하는 일반 명칭 (generic name) 을 어드레싱 (addressing) 함으로써 웹 서비스를 액세스하기 위한 요청을 네트워크에 웹 애플리케이션에 의해 전송하는 단계; 웹 서비스를 호스팅하는 로컬 디바이스를 식별하는 상기 글로벌 명칭을 포함하는, 요청에 대한 응답을 웹 애플리케이션에 의해 네트워크로부터 수신하는 단계; 수신된 글로벌 명칭이 리스트에 포함된 것을 웹 애플리케이션에 의해 검증하는 단계; 및 검증 (verification) 이 성공적인 경우에, 글로벌 명칭을 어드레싱함으로써 로컬 디바이스에 연결하는 단계; 로컬 디바이스로부터 인증서를 수신하는 단계; 브라우저에 의해 글로벌 명칭에 연관된 인증서를 검증하는 단계 및 웹 서비스를 안전하게 액세스하는 단계를 더 포함한다. 유리하게, 일반 명칭은 그 명칭 하에 임의의 로컬 디바이스가 액세스가능한 명칭, 즉, 웹 서비스들을 호스팅하는 모든 디바이스들에 공통인 명칭이다. 유리하게, 리스트는 또한, 웹 서비스를 호스팅하기 위해 신뢰되고 있는 디바이스들의 글로벌 명칭들을 포함한다. 유리하게, 글로벌 명칭들의 수는 방대할 수 있을 것이기 때문에, 리스트는, 웹 서비스를 호스팅하기 위해 신뢰되고 있는 로컬 디바이스들의 글로벌 명칭들의 망라적인 리스트를 포함하지 않고, 로컬 디바이스들의 글로벌 명칭들에 매칭 (matching) 하기 위한 패턴들을 포함한다.

[0009] 일 유리한 특징에 따르면, 로컬 디바이스는 신뢰된 오퍼레이터 (trusted operator) 에 의해 글로벌 명칭 및 글로벌 명칭에 연관된 인증서를 전달받는다.

[0010] 다른 유리한 특징에 따르면, 화이트 리스트 (white list) 는 브라우저에서 실행되는 웹 애플리케이션에 의해 신뢰된 오퍼레이터로부터 동적으로 획득된다. 변형 형태에서, 화이트 리스트는 브라우저에서 실행되는 웹 애플리케이션에서 하드 코딩된다 (hard coded).

[0011] 제 1 바람직한 실시형태에서, 일반 명칭을 어드레싱함으로써 웹 서비스를 액세스하기 위한 요청은 HTTP 요청이고, 글로벌 명칭을 어드레싱함으로써 웹 서비스를 안전하게 액세스하기 위한 요청은 SSL 요청을 포함하는 HTTPS 요청이다.

[0012] 변형 형태에 따르면, 로컬 디바이스는 게이트웨이 디바이스, 셋톱 박스, 네트워크 부착 스토리지 (Network Attached Storage; NAS) 이다.

[0013] 제 2 양태에서, 본 발명은 네트워크를 통해 웹 애플리케이션을 실행하는 브라우저에 의해 웹 서비스를 안전하게 액세스하기 위한 사용자 디바이스에 지향된다. 웹 서비스는 적어도 하나의 디바이스에 의해 호스팅되고, 그 적어도 하나의 디바이스 중에서 로컬 디바이스가 사용자 디바이스에 의해 액세스되고 있다. 유리하게, 로컬 디바이스는 웹 서비스를 호스팅하고 사용자 디바이스에 가장 가까운 디바이스이다. 디바이스는, 웹 서비스를 호스팅하는 임의의 디바이스를 식별하는 일반 명칭을 어드레싱함으로써 웹 서비스를 액세스하기 위한 요청을 네트워크에 웹 애플리케이션에 의해 전송하는 수단; 웹 서비스를 호스팅하는 로컬 디바이스를 고유하게 식별하는 글로벌 명칭을 포함하는 요청에 대한 응답을 웹 애플리케이션에 의해 네트워크로부터 수신하는 수단; 수신된 글로벌 명칭이 화이트 리스트로도 불리는 리스트에 포함된 것을 웹 애플리케이션에 의해 검증하는 수단으로서, 리스트는 웹 서비스를 호스팅하기 위해 신뢰되고 있는 로컬 디바이스들의 글로벌 명칭들을 포함하는, 상기 검증하는 수단; 글로벌 명칭을 어드레싱함으로써 로컬 디바이스에 웹 애플리케이션에 의해 연결하는 수단; 로컬 디바이스로부터 인증서를 수신하는 수단, 및 글로벌 명칭에 연관된 인증서를 검증하는 수단 및 웹 서비스를 안전하게 액세스하는 수단을 포함한다.

[0014] 웹 서비스가 로컬 디바이스에 의해 호스팅되는 경우에, 사용자 디바이스 상에서 웹 애플리케이션을 실행하는 브라우저에 의해 네트워크를 통해 웹 서비스를 안전하게 액세스하는 방법에 대해 기술된 임의의 특징 또는 실시형태는, 개시된 방법을 구현하도록 적응된 사용자 디바이스 또는 로컬 디바이스와 양립가능하다.

[0015] 제 1 실시형태에 따른 방법은 현재의 소프트웨어 및 표준 웹 프로토콜들과 유리하게 양립가능하다. 따라서, 그것은 사용자의 브라우저들에 대해 또는 사용되는 프로토콜들에 대해 변경들을 필요로 함이 없이 알맞게 사용될 수 있다.

도면의 간단한 설명

[0016] 이제 본 발명의 바람직한 특징들이 첨부 도면들을 참조하여 비제한적인 예의 방식으로 설명될 것이다.

도 1 은 본 발명이 이용될 수도 있는 예시적인 네트워크를 나타낸다.

도 2 는 본 발명의 제 1 실시형태에 따른 보안 액세스 방법의 단계들을 나타낸다.

도 3 은 본 발명의 바람직한 실시형태에 따른 보안 액세스 방법의 단계들을 나타낸다.

도 4 는 본 발명의 바람직한 실시형태에 따른 보안 액세스 방법을 구현하는 로컬 디바이스를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0017] 도 1 은 본 발명이 이용될 수도 있는 예시적인 네트워크 (100) 를 나타낸다. 네트워크 (100) 는 사진 공유 애플리케이션과 같은 웹 애플리케이션을 호스팅하는 서버 디바이스 (110) 를 포함한다. 사용자는, 웹 브라우저가 이용가능한 배터리 전원공급된 디바이스들 (태블릿, 랩톱 컴퓨터, 모바일 폰) 또는 컴퓨터들과 같은 퍼스널 디바이스들 (120) 을 소유한다. 웹 애플리케이션의 클라이언트 부분 (client part), 예컨대 사진 공유 애플리케이션이 사용자 디바이스 (120) 의 브라우저 상에서 실행되고, 웹 애플리케이션은 웹 애플리케이션의 서버 부분 (server part) 에 액세스한다. 웹 애플리케이션의 클라이언트 부분은 또한 오프로딩 서비스와 같은 웹 서비스에 액세스할 수 있다. 사용자 디바이스는 로컬 영역 네트워크 (160) 에 의해 인터넷 라우터, 셋톱 박스, 다른 사용자 컴퓨터, 가정용 게이트웨이 (residential gateway), NAS (150) 와 같은 로컬 디바이스 상에서 실행되는 웹 서비스에 연결한다. 웹 애플리케이션의 클라이언트 부분, 및 웹 서비스는 무선 인터넷 라우터 또는 가정용 게이트웨이와 같은 네트워크 액세스 디바이스 (130) 를 통해 웹 애플리케이션의 서버 부분에 액세스할 수 있다. 따라서, 가정용 게이트웨이는, 웹 애플리케이션의 서버 부분에 데이터를 업로드하기 위해 느린 광대역 네트워크에 대한 액세스가 이슈인 경우에 상대적으로 느린 광대역 네트워크 (140) 와 고속 로컬 영역 네트워크 (160) 사이의 프론티어 (frontier) 에 있다. 바람직한 실시형태에서, 네트워크 액세스 디바이스 (130) 는, 네트워크 액세스 디바이스가 항상 전원이 켜져 있기 때문에 로컬 디바이스이다. 변형 형태에서, 예컨대 이러한 네트워크 액세스 디바이스 (130) 가 오프로딩 기능을 지원하지 않는 경우에, 로컬 디바이스는 상기 상세하게 설명된 바와 같이 바람직하게 올웨이즈-온 (always-on) 타입의 로컬 네트워크 (140) 의 임의의 유형의 디바이스, 예컨대 NAS (150) 이다. 본 발명은, 로컬 디바이스에서 임시로 천이하는 업로드된 데이터가 로컬 디바이스를 사칭하는 공격자들을 회피함으로써 공격자들로부터 보호되도록, 로컬 디바이스 (130, 150) 를, 또는 보다 정확하게는, 로컬 디바이스 (130, 150) 상에서 실행되는 웹 서비스를 인증하기 위한 솔루션을 제공한다.

[0018] 본 발명의 핵심적인 창의적인 아이디어는 로컬 웹 서비스를 브라우저로부터 웹 애플리케이션 내에서 사용되도록 로케이팅시키고, 그리고 로컬 서비스를 인증하도록 하는 것이다. 방법은 오프로딩 서비스를 로케이팅시키도록 이용될 수 있지만, 그것은 유리하게, 웹을 DLNA/UPNP 릴레이에 로케이팅시키는 것과 같이 다른 애플리케이션과 양립가능하고, 여기서, 웹 애플리케이션은 DLNA/UPNP 릴레이에 대한 웹 서비스를 통해, 사용자의 디바이스들에 대해 제어하도록 허가된다.

[0019] 바람직한 실시형태에서, 방법은 JavaScript 언어에 의해 실행되도록 적응된다. 따라서, 방법은 유리하게는 웹 브라우저에 의해 제공된 제약된 실행 환경에 맞춰지도록 적응된다. 이들 제약들은 브라우저가 임의의 악성 코드가 매우 제한된 파워를 갖는 것을 보장하는데 도움이 된다.

[0020] 그 외에, 웹 서비스를 안전하게 액세스하는 방법은 서비스의 존재 및 그것의 어드레스 양자 모두를 동적으로 결정한다. 메커니즘은 또한 재-로케이팅된 (re-located) 서비스를 인증하는 것을 보살핀다. 메커니즘은 또한 서비스의 존재에 의존하여 웹 애플리케이션의 클라이언트 부분의 동적 적응을 구현하도록 허용한다.

[0021] 도 2 는 본 발명의 제 1 실시형태에 따른 보안 액세스 방법의 단계들을 나타낸다.

[0022] 브라우저는 소위 브라우저 네트워크 API 에서 구현되는 XMLHttpReq 를 이용하여 네트워크에 오직 액세스할 수 있다. 브라우저는 JavaScript 머신을 더 포함한다. 브라우저에 존재하는 허가/인증 메커니즘은 TLS/SSL 메커니즘이다.

[0023] 도 2 에 나타내지 않은 예비 단계에서, 신뢰된 오퍼레이터는 도메인 (offload.org), 및 그 도메인에 대한 SSL 인증서를 산다. 서비스를 실행하는 각각의 신뢰된 디바이스들은 고유 명칭 (예컨대 af34a), 및 그것의 명칭에 대응하는 인증서 (af34a.offload.org) 를 수신한다. 신뢰된 오퍼레이터는, 명칭 af34a.offload.org 가 항상 올바른 로컬 IP 어드레스에 맵핑하도록, 신뢰된 디바이스들이 업데이트할 수 있는, (인터넷 상에서 이용가

능한) DNS 서비스를 실행한다.

[0024] 로케이션(location)/인증(authentication) 절차의 제 1 단계 (210) 에서, 로컬로 (locally) 호스팅된 웹 서비스를 액세스하기를 시도하는 브라우저는 일반 명칭 (offload.local) 에 대한 요청을 네트워크에 전송한다. 보다 정확하게는, JavaScript 는, 브라우저 네트워크 API 를 통해, 임의의 로컬 네트워크 상에서 서비스를 실행하는 임의의 디바이스에 공통인 몇몇 정해진 어드레스 (offload.local) 에 대한 로컬 쿼리 (local query) 를 발행한다. 게이트웨이에 존재하는 DNS 는 로컬 IP 어드레스로 DNS 쿼리에 대해 응답할 것이고, 브라우저 네트워크 API 는 비보안 HTTP 프로토콜을 이용하여 이 IP 어드레스, 즉, 웹 서비스를 호스팅하는 로컬 디바이스의 IP 어드레스에 연결한다. 쟁점은, 이 명칭이 아무에게도 속하지 않고 어떤 인증 기관도 이러한 인증서를 전달하지 않을 것이기 때문에, "offload.local" 에 대한 인증서를 얻는 것이 가능하지 않을 수 있다는데 있다.

[0025] 따라서, 제 2 단계 (220) 에서, 브라우저는, 로컬 디바이스에 의해 호스팅되고 로컬 디바이스 IP 어드레스에 연관된 웹 서비스에 대해 글로벌 명칭이라고 불리는 충분히 자격이 있는 명칭 (af34a.offload.org) 을 획득한다. 하지만, 이미 설명된 바와 같이, 충분히 자격이 있는 명칭은 손상될 수도 있다.

[0026] 제 3 단계 (230) 에서, 브라우저는, 획득된 글로벌 명칭 (af34a.offload.org) 이 몇몇 신뢰된 오퍼레이터에 의해 관리되는 것을 체크한다. 실제로, 누군가는 hacker.org 에 대한 유효한 인증서를 가질 수도 있는 동안, 이것은 충분한 조건이 아니다. 추가적인 요건은 인증서의 소유자가 신뢰되는 것이다. 따라서, 브라우저는, 서브-인증서 (af34a.offload.org) 가 신뢰된 오퍼레이터 (offload.org) 로부터 나오는 것을 보장하도록, 화이트 리스트에 대해 획득된 글로벌 명칭을 검증한다. 당해 기술분야에서 통상의 지식을 가진 자 (이하, '통상의 기술자' 라 함) 는, 화이트 리스트가 각각의 신뢰된 디바이스들의 글로벌 명칭에 대한 망라적인 리스트를 포함하지 않을 수도 있지만 글로벌 명칭을 검증하기 위해 사용되는 스킴 (scheme) 에 매칭하는 패턴을 포함할 수도 있다는 것을 이해할 것이다.

[0027] 마지막 단계 (240) 에서, 검증이 성공하는 경우에, 브라우저는 글로벌 명칭에 안전하게 액세스하기 위한 요청을 전송한다. 보다 정확하게는, 브라우저 네트워크 API 는 충분히 자격이 주어진 명칭 (af34a.offload.org) 에 대한 새로운 쿼리를 수행한다. 신뢰된 오퍼레이터에 의해 동작되는 DNS 는 로컬 IP 어드레스로 답한다. 브라우저는 이 로컬 IP 어드레스에 HTTPS 에서 연결하고, 글로벌 명칭에 연관된 인증서가 그것이 연결하는 디바이스에 대응하는 것 및 브라우저의 인증서 컬렉션 (collection) 을 이용하여 인증서가 유효하고 폐지되지 않았다는 것을 체크한다. 단계 (240) 는 유리하게는 로컬 디바이스가 인증되는 것을 허용하고, 단계 (230) 는 유리하게는 로컬 디바이스가 신뢰된 오퍼레이터에 의해 승인된 것을 허용한다.

[0028] 따라서, https://af34a.offload.org 에서 이용가능한 웹 서비스는 안전하고 보안 가능하게 이용된다.

[0029] 임의의 단계에서의 임의의 실패는, 서비스가 이용가능하지 않거나 또는 아니면 어떤 인증 문제점들 때문에 그것이 신뢰될 수 없다는 것을 의미한다. 따라서, 그것은 사용되어서는 안된다.

[0030] 도 3 은 본 발명의 바람직한 실시형태에 따른 보안 액세싱의 단계들을 나타낸다. 이미 설명된 바와 같이, 바람직한 실시형태에서, 웹 서비스는 오프로딩 업로드들을 위한 웹 서비스이다.

[0031] 로케이션 서비스는 정해진 URL http://offload.local/test 에서 이용가능하다. 명확함을 위해, 우리는 전체 설명에서 포트 번호는 생략한다. 하지만, 기존의 서비스들과의 충돌들을 회피하기 위해, 우리는 비-표준 HTTP/HTTPS 포트들 (예를 들어, HTTP 에 대한 8787 및 HTTPS 에 대한 8788) 을 이용한다. 충분하게 자격이 주어진 명칭 및 포트들이 정해지고 모든 게이트웨이들에 대해 공통된다. 그 결과로서, 오직 XMLHttpRequest 만을 이용하여 네트워크에 액세스할 수 있는 브라우저에서 실행되는 웹 애플리케이션이 서비스를 액세스할 수 있다. 브라우저는 게이트웨이의 IP 어드레스에 대해 일반적인 충분히 자격이 주어진 명칭 (offload.local (300)) 을 분석하고, 그것에 연결한다. 임의의 연결 에러 (실패한 DNS 분석 (resolution), 연결 타임아웃, 404, 403...) 는 서비스가 이용가능하지 않은 것을 나타낸다. 오프로딩 서비스가 실행되고 있고 오프로드 요청들을 수용할 수 있는 경우, 브라우저는 답으로서 OK 를 수신할 것이다.

[0032] 로케이션 서비스는 LAN 상에서 서비스를 지원하는 디바이스의 IP 어드레스로 정해진 명칭을 분석하기 위해 DNS 에 강하게 의존한다. 대부분의 게이트웨이들은 그들 자신의 DNS 를 실행하고, 따라서 그들 스스로 offload.local 로서 등록할 수 있다. 오프로딩 서비스가 다른 디바이스에 의해 제공되는 경우에, 이 디바이스는 DHCP 프로토콜 덕분에 게이트웨이의 DNS 에서 명칭 offload.local 을 여전히 등록할 수 있다. DNS 분석이 DHCP 를 이용하여 offload.local 에 대해 등록하는 동일 LAN 상의 누군가에 의해 쉽게 영향을 받을 수도 있기 때문에, 웹 개발자는 분석이 (브라우저의 SSL 인증서들에 따라) 신뢰된 게이트웨이로 이끄는 것을 보장하

기를 기꺼이 원할 수도 있을 것이다. 솔루션은 HTTPS 인증 메커니즘에 의존하는 것이다. 이를 위해, 각 게이트웨이는 그 자신의 자체-서명된 (self-signed) 인증서를 가지고, 사용자는 그가 신뢰하는 게이트웨이들로부터의 인증서들을 그의 브라우저의 인증서 리스트에 수동으로 추가한다. 요청들은 http://offload.local/ 대신에 https://offload.local/ 로 전송된다. 게이트웨이가 신뢰되지 않는 경우, 로케이션 서비스에 대한 요청들은 연결 에러들로 귀결된다. 따라서, 오프로딩은 인에이블되지 않을 것이다. 하지만, 이 프로세스는, 사용자가 그의 브로우저에서 적절한 인증서를 추가함으로써 그가 사용하는 각각의 새로운 게이트웨이들을 수동으로 승인하는 것을 필요로 한다. 이 프로세스는 방심할 수 없을 수도 있고, 충분히 투명한 사용자의 경험을 방해할 수도 있다.

[0033] 프로세스가 매끄럽도록 하기 위해, 선호되는 실시형태에 따른 방법은, 유리하게는, 게이트웨이를 인증하는 것을 또한 보살피는 개선된 로케이션 방법을 제공한다. 방법은 신뢰된 소프트웨어를 실행하는 임베딩된 디바이스들과 함께 이용되는 것으로 의미되고 그것의 인증서는 복사될 수 없다. 도 3 은 전체 로케이션 및 인증 프로세스를 나타낸다. 이 프로세스는 전에 여기서 설명된 비-인증된 로케이션 서비스를 개선한다. 이 경우에, 각 게이트웨이는 고유 명칭 (예컨대, af34a.offload.org (301)) 과 연관되고, 신뢰된 인증 기관에 의해 사인된 대응하는 인증서를 갖는다. 각 게이트웨이는 신뢰된 도메인 offload.org 에 대해 실행되는 동적 DNS 서비스 상으로 그것의 로컬 IP 어드레스를 발행한다.

[0034] 프로세스는 이제 게이트웨이를 로케이팅 (locating) 하고 그 다음 그것을 인증하는 것에 있다. 이를 위해, http://offload.local/auth 에 대한 요청이 발행된다. 이 요청은 게이트웨이에 대해 고유한 충분히 자격이 주어진 명칭 (예컨대, af34a.offload.org (301)) 를 리턴한다. 이 충분히 자격이 주어진 명칭은, 인증서가 신뢰된 게이트웨이들에 대한 적절한 인증 기관: 모든 유효한 SSL 도메인이 아니라 (즉, 브라우저 인증 리스트에 따라 승인된) 맵에 의해 발행된 것을 보장하기 위해 도메인들의 화이트-리스트와 매칭된다. 이 목적을 위해 오직 몇몇 도메인들 (예컨대, offload.org) 만이 신뢰되고, 그러한 것들이 화이트-리스트에 리스트된다. 이 지점까지, 게이트웨이는 신뢰되지 않고, 획득된 정보는 조작되었을 수도 있다. 하지만, 충분히 자격이 주어진 명칭은 게이트웨이들의 신뢰된 셋트에 맵핑된다. 다음으로, https://af34a.offload.org/test 에 대한 요청들이 발행된다. 브라우저는 게이트웨이의 인증서를 체크하고 따라서 임의의 하이잭킹 (hijacking) 을 방지한다. 인증서가 정당한 것일 경우, 오프로딩 메커니즘이 인에이블될 수 있고, 요청들은 https://af34a.offload.org/upload/ 에 포스팅될 수 있다.

[0035] 다시, 기본적인 로케이션 프로세스에서와 같이, 임의의 에러는 오프로딩 메커니즘이 인에이블될 수 없는 것을 의미한다. 각각의 디바이스는 그 자신의 인증서를 가지기 때문에, 그들이 도난당한 경우, 또는, 디바이스들의 서브셋트에서 보안 이슈가 발견되는 경우에, 개별 인증서들을 폐지하는 것이 가능하다. 기껏해야, 공격자는 DNS 엔트리들을 조작함으로써 로케이션 서비스를 방해하는데 성공하는 경우, 웹 애플리케이션은 오프로딩 능력 없이 정규 서비스로 간단하게 고장 대체할 것이고, 따라서, 비활성인 오프로딩을 제외하고는 사용자에 대해 다른 어떤 서비스 지장도 초래하지 않는다.

[0036] 통상의 기술자라면, 본 방법은 특별한 장비에 대한 필요성 없이 아주 쉽게 구현될 수 있으므로, 그것은 PC 들, 모바일 폰들, 홈 네트워크들에서의 게이트웨이들 등과 같은 '보통의 (normal)' 사용자 디바이스들에 의해 구현될 수도 있다는 것을 또한 이해할 것이다. 본 발명은 802.11 통신 (Wi-Fi), 또는 Bluetooth 또는 UWB 와 같은 임의의 유선 또는 무선 액세스와 추가로 양립가능하다. 본 발명은 유리하게는, 무선 네트워크의 핫스팟 (hotspot) 에 로케이팅된 웹 서비스와 양립가능하다.

[0037] 도 4 는 본 발명의 선호되는 실시형태에 따른 예시적인 사용자 디바이스를 나타낸다. 사용자 디바이스 (400) 는 브라우저 또는 웹 브라우저로 불리는 소프트웨어 모듈을 포함한다. 브라우저는 네트워크를 통해 웹 서비스를 안전하게 액세스하기를 시도하는 웹 애플리케이션을 실행한다. 다른 변형 형태들에 따르면, 사용자 디바이스는 컴퓨터, 모바일 디바이스, 태블릿에서 구현될 수도 있다.

[0038] 사용자 디바이스 (400) 는 802.11 무선 카드와 같은 네트워크 인터페이스 (410), 적어도 하나의 프로세서 (420) (이하, "프로세서"), 및 메모리 (430) 를 포함한다. 네트워크 인터페이스 (410) 는 사용자 디바이스를 네트워크에 연결하도록, 따라서, 사용자 디바이스를 로컬 디바이스에 연결하도록 적응된다. 네트워크 인터페이스 (410) 는 예를 들어 원격 웹 서비스에 액세스하기 위한 요청들을 물리적으로 송신하고 그 요청에 대한 응답을 물리적으로 수신한다. 변형 형태에서, 네트워크 인터페이스 (410) 는 이더넷과 같은 유선 인터페이스이다. 프로세서 (420) 는 웹 브라우저라고 불리는 소프트웨어 모듈을 구현하는 명령들을 실행하도록 적응된다. 웹 브라우저는 웹 애플리케이션을 실행하도록 적응된다. 본 발명의 이해를 위해 필요한 특징

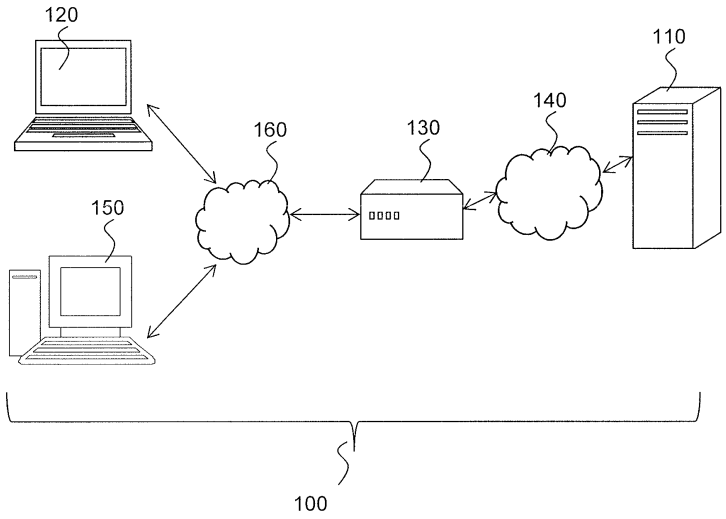
들만이 이하 상세히 설명된다. 웹 애플리케이션은, 웹 서비스를 호스팅하는 임의의 디바이스를 식별하는 일반 명칭을 어드레싱함으로써 웹 서비스에 액세스하기 위해 네트워크 인터페이스 (410) 를 통해 요청을 전송한다. 웹 애플리케이션은, 네트워크 인터페이스 (410) 를 통해, 웹 서비스를 호스팅하고 사용자 디바이스가 안전하게 액세스할 수 있는 로컬 디바이스를 고유하게 식별하는 글로벌 명칭을 포함하는 요청에 대한 응답을 수신한다. 웹 애플리케이션은, 수신된 글로벌 명칭이, 웹 서비스를 호스팅하기 위해 신뢰되고 있는 디바이스들의 글로벌 명칭들을 포함하는 리스트에 포함되는 것을 검증한다. 유리하게는, 리스트는 메모리 (430) 에 저장된다. 웹 애플리케이션은, 글로벌 명칭을 어드레싱함으로써 로컬 디바이스에, 네트워크 인터페이스 (410) 를 통해, 연결을 확립하고, 브라우저는 로컬 디바이스의 글로벌 명칭에 연관된 수신된 인증서를 검증한다. 따라서, 웹 애플리케이션은 웹 서비스에 안전하게 액세스한다. 변형 형태에서, 보안 기능들은 보안 프로세서와 같은 하드웨어의 피스 (piece) 에서 구현된다.

[0039] 설명은 웹 애플리케이션에 대한 업로드에 초점이 맞춰지지만, 본 발명은 웹 서비스가 로컬로 서빙되는 메커니즘들과 양립가능하다.

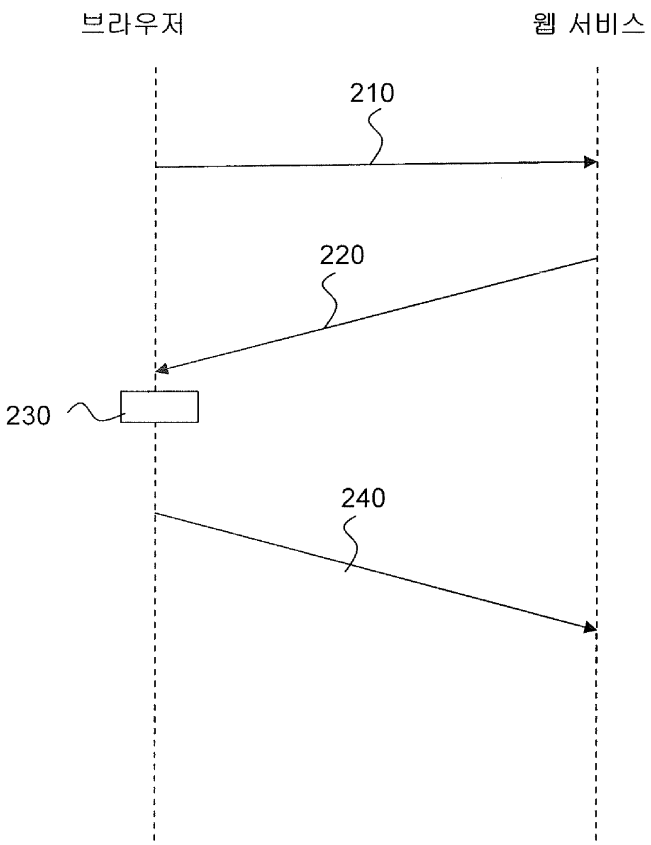
[0040] 상세한 설명 및 (적절한 경우에) 청구항들 및 도면들에서 개시된 각 특징은 독립적으로 또는 임의의 적절한 조합으로 제공될 수도 있다. 소프트웨어에서 구현되는 바와 같이 설명된 특징들은 또한 하드웨어로 구현될 수도 있고, 그 역도 가능하다. 청구항들에 나타나는 참조 부호들은 오직 예시적인 것이고, 청구항들의 범위에 대한 어떤 제한하는 효과도 갖지 않는다.

도면

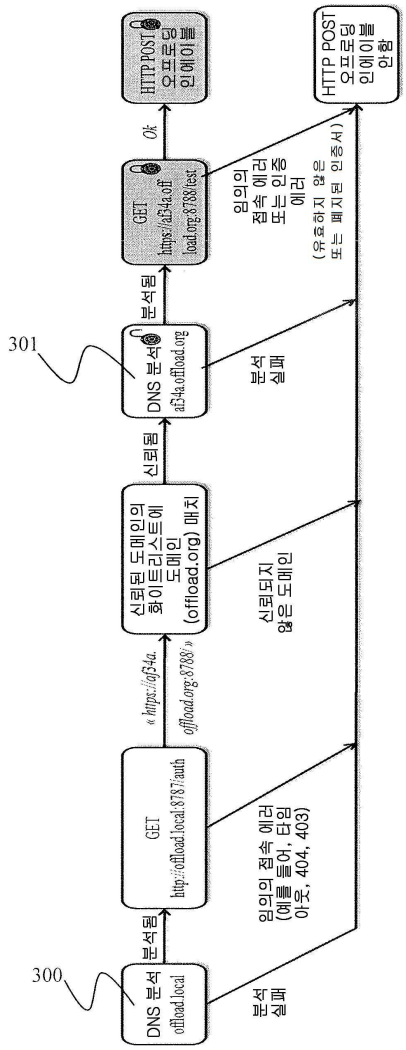
도면1



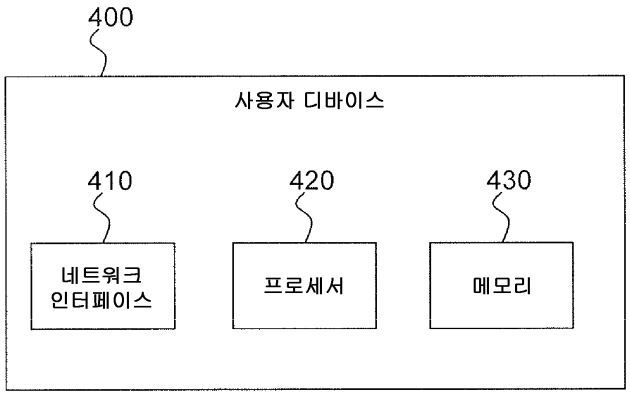
도면2



도면3


HTTP POST 오프로딩 인에이블
Ok
GET https://a234.off load.org:8788/test
분석됨
DNS 분석 a234.offload.org
신뢰됨
신뢰된 도메인의 화이트리스트에 도메인 (offload.org) 매치
« https://a234. offload.org:8788/ »
GET http://offload.local:8787/auth
분석됨
DNS 분석 offload.local
301
300
분석 실패
임의의 접속 에러 (에를들어, 타임 아웃, 404, 403)
신뢰되지 않은 도메인
분석 실패
임의의 접속 에러 또는 인증 에러 (유효하지 않은 또는 폐지된 인증서)
HTTP POST 오프로딩 인에이블 안됨

도면4


400
사용자 디바이스
410
420
430
네트워크 인터페이스
프로세서
메모리