(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0062085
(43) 공개일자 2016년06월01일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *G06F 21/62* (2013.01)
(52) CPC특허분류
H04L 63/0281 (2013.01)
G06F 21/6245 (2013.01)
(21) 출원번호 10-2016-7010764
(22) 출원일자(국제) 2013년11월25일
심사청구일자 2016년04월22일
(85) 번역문제출일자 2016년04월22일
(86) 국제출원번호 PCT/US2013/071718
(87) 국제공개번호 WO 2015/076846
국제공개일자 2015년05월28일

(71) 출원인
맥아피 인코퍼레이티드
미국 95054 캘리포니아 산타클라라 미션컬리지 블러바드 2821
(72) 발명자
머틱 이고르
영국 에이치피4 3비에스 버크햄스티드 허트포드셔 킹스데일 로드 우드랜즈
(74) 대리인
제일특허법인

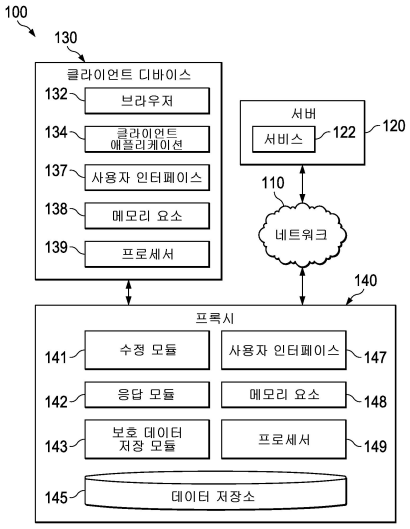
전체 청구항 수 : 총 25 항

(54) 발명의 명칭 **비공개 데이터를 보호하는 보안 프록시**

(57) 요 약

실시예에서 비공개 데이터를 보호하는 기술이 제공된다. 실시예는 서버에서 클라이언트 디바이스로 전달되는 도중의 네트워크 흐름을 가로채고, 네트워크 흐름의 객체 내에서 비공개 데이터 항목의 요청을 식별하고, 데이터 저장소에서 비공개 데이터 항목을 식별하고, 승인 요청을 포함하는 수정된 객체를 클라이언트 디바이스로 제공하고, 유효한 승인 정보가 수신될 때 비공개 데이터 항목을 서버로 전송하도록 구성된다. 실시예는 또한 클라이언트 디바이스로부터 승인 정보를 수신하고, 승인 정보가 유효한지를 결정하고, 승인 정보가 유효한 것으로 결정되면 비공개 데이터 항목을 취득하도록 구성된다. 실시예는 또한 비공개 데이터 항목의 잠금 해제 메커니즘을 결정하고, 잠금 해제 메커니즘에 적어도 일부 기초하여, 승인 요청을 포함하는 수정된 객체를 생성하도록 구성된다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/08 (2013.01)
H04L 63/168 (2013.01)

명 세 서

청구범위

청구항 1

비공개 데이터를 보호하기 위한 명령어가 저장된 적어도 하나의 머신 판독 가능한 저장 매체로서,

상기 명령어는 적어도 하나의 프로세서에 의해 실행될 때, 상기 적어도 하나의 프로세서로 하여금,

서버에서 클라이언트 디바이스로 전달되는 도중의 네트워크 흐름을 가로채도록 하고,

상기 네트워크 흐름의 객체 내에서 비공개 데이터 항목의 요청을 식별하도록 하고,

데이터 저장소에서 상기 비공개 데이터 항목을 식별하도록 하고,

승인 요청을 포함하는 수정된 객체를 상기 클라이언트 디바이스로 제공하도록 하고,

유효한 승인 정보가 수신될 때 상기 비공개 데이터 항목을 상기 서버로 전송하도록 하는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 2

제 1 항에 있어서,

상기 명령어는 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 적어도 하나의 프로세서로 하여금 또한,

상기 클라이언트 디바이스로부터 승인 정보를 수신하도록 하고,

상기 승인 정보가 유효한지 여부를 판정하도록 하고,

상기 승인 정보가 유효한 것으로 판정되면 상기 비공개 데이터 항목을 취득하도록 하는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 3

제 1 항에 있어서,

상기 명령어는 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 적어도 하나의 프로세서로 하여금 또한,

상기 비공개 데이터 항목의 잠금 해제 메커니즘을 결정하도록 하고,

상기 잠금 해제 메커니즘에 적어도 일부 기초하여, 상기 승인 요청을 포함하는 상기 수정된 객체를 생성하도록 하는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 4

제 3 항에 있어서,

상기 잠금 해제 메커니즘은, 일회용 비밀번호, 사용자의 생체 인식 식별, 및 다중요소 인증 프로세스(multi-factor authentication process)를 포함하는 일군의 잠금 해제 메커니즘 중에서 선택되는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 5

제 1 항에 있어서,

상기 명령어는 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 적어도 하나의 프로세서로 하여금 또한,

상기 비공개 데이터 항목의 요청에 의해 표시된 데이터의 형태를 결정하도록 하며,

상기 데이터 저장소 내 상기 비공개 데이터 항목은 상기 데이터의 형태 및 상기 서버에 의해 제공된 서비스와 연관되는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 6

제 1 항에 있어서,

상기 데이터 저장소 내 상기 비공개 데이터 항목은, 상기 클라이언트 디바이스, 상기 클라이언트 디바이스의 사용자, 및 상기 클라이언트 디바이스에서 실행되는 클라이언트 애플리케이션 중 적어도 하나와 연관되는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 7

제 1 항에 있어서,

상기 비공개 데이터 항목은 비밀번호인

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 8

제 1 항에 있어서,

상기 승인 정보가 유효하지 않을 때 상기 비공개 데이터 항목은 상기 서버에 제공되지 않는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 9

제 1 항에 있어서,

상기 객체는 하이퍼텍스트 마크업 언어(HyperText Markup Language, HTML) 웹 페이지인

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 10

제 9 항에 있어서,

상기 명령어는 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 적어도 하나의 프로세서로 하여금 또한,

상기 데이터 저장소로부터 상기 비공개 데이터 항목을 취득하도록 하고,

상기 유효한 승인 정보가 수신될 때 상기 비공개 데이터 항목을 상기 HTML 웹 페이지 내에 삽입함으로써 상기 HTML 웹 페이지를 완성하도록 하고,

상기 완성된 HTML 웹 페이지에 기초하여 상기 서버로 응답을 전송하도록 하는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 11

제 1 항 내지 제 10 항 중 어느 한 항에 있어서,

상기 데이터 저장소는 하나 이상의 비공개 데이터 항목의 복수 집합을 포함하고, 상기 복수의 집합은 각기 복수의 서비스와 연관되는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 12

제 1 항 내지 제 10 항 중 어느 한 항에 있어서,

프록시는 복수의 데이터 집합을 포함하고, 상기 복수의 데이터 집합의 각각의 집합은 적어도 하나의 네트워크 에이전트와 연관되며,

각각의 데이터 집합은 적어도 하나의 비공개 데이터 항목의 하나 이상의 집합을 포함하고,

특정 데이터 집합의 적어도 하나의 비공개 데이터 항목의 하나 이상의 집합은 상이한 서비스와 각기 연관되는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 13

제 1 항 내지 제 10 항 중 어느 한 항에 있어서,

상기 클라이언트 디바이스는,

사용자가 브라우저를 통해 상기 서버에 액세스할 수 있게 하도록 구성된 컴퓨팅 디바이스와,

상기 서버에 의해 제공된 서비스에 자동 인증하도록 구성된 클라이언트 애플리케이션을 포함하는 컴퓨팅 디바이스와,

상기 서버에 의해 제공된 상기 서비스에 자동 인증하도록 구성된 내장형 제어기

를 포함하는 일군의 클라이언트 디바이스 중에서 선택되는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 14

제 1 항 내지 제 10 항 중 어느 한 항에 있어서,

상기 명령어는 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 적어도 하나의 프로세서로 하여금 또한,

상기 서버에서 상기 클라이언트 디바이스로 전달되는 도중의 다른 네트워크 흐름을 가로채도록 하고,

상기 서버에 의해 제공된 특정 서비스와 연관된 하나 이상의 특정 비공개 데이터 항목에 대응하는 하나 이상의 크리덴셜을 변경하려는 요청을 식별하도록 하고,

상기 네트워크 흐름을 상기 클라이언트 디바이스로 포워딩하지 않고 하나 이상의 새로운 크리덴셜을 선택하도록 하고,

상기 데이터 저장소 내 상기 하나 이상의 특정 비공개 데이터 항목을 상기 하나 이상의 새로운 크리덴셜로 갱신하도록 하는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 15

제 1 항 내지 제 10 항 중 어느 한 항에 있어서,

상기 명령어는 상기 클라이언트 디바이스 상의 신뢰성 있는 실행 환경에서 실행되도록 구성되는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 16

제 1 항 내지 제 10 항 중 어느 한 항에 있어서,

상기 적어도 하나의 머신 판독 가능한 저장 매체는 상기 클라이언트 디바이스와 분리된 프록시에서 구현되는

적어도 하나의 머신 판독 가능한 저장 매체.

청구항 17

데이터 보호 장치로서,

적어도 하나의 메모리 요소와,

상기 적어도 하나의 메모리 요소에 연결된 적어도 하나의 프로세서와,

상기 적어도 하나의 프로세서에 의해 실행될 때,

네트워크 흐름이 서버에서 클라이언트 디바이스로 전달되는 도중일 때 상기 장치에 의해 가로채인 상기 네트워크 흐름의 객체 내에서 비공개 데이터 항목의 요청을 식별하고,

데이터 저장소에서 상기 비공개 데이터 항목을 식별하고,

승인 요청을 포함하는 수정된 객체를 상기 클라이언트 디바이스로 제공하도록 구성된 수정 모듈과,

적어도 하나의 프로세서에 의해 실행될 때, 유효한 승인 정보가 수신되면 상기 비공개 데이터 항목을 상기 서버로 전송하도록 구성된 응답 모듈을 포함하는

데이터 보호 장치.

청구항 18

제 17 항에 있어서,

상기 응답 모듈은 또한,

상기 클라이언트 디바이스로부터 승인 정보를 수신하고,

상기 승인 정보가 유효한지 여부를 판정하고,

상기 승인 정보가 유효한 것으로 판정되면 상기 비공개 데이터 항목을 취득하도록 구성되는

데이터 보호 장치.

청구항 19

제 17 항에 있어서,

상기 수정 모듈은 또한,

상기 비공개 데이터 항목의 잠금 해제 메커니즘을 결정하고,

상기 잠금 해제 메커니즘에 적어도 일부 기초하여, 상기 승인 요청을 포함하는 상기 수정된 객체를 생성하도록 구성되는

데이터 보호 장치.

청구항 20

제 17 항에 있어서,

상기 수정 모듈은 또한, 상기 비공개 데이터 항목의 요청에 의해 표시된 데이터의 형태를 결정하도록 구성되며,

상기 데이터 저장소 내 상기 비공개 데이터 항목은 상기 데이터의 형태 및 상기 서버에 의해 제공된 서비스와 연관되는

데이터 보호 장치.

청구항 21

제 17 항 내지 제 20 항 중 어느 한 항에 있어서,

클라이언트 디바이스를 더 포함하며,

상기 클라이언트 디바이스는 신뢰성 있는 실행 환경을 포함하고, 상기 수정 모듈 및 상기 응답 모듈은 상기 신뢰성 있는 실행 환경에서만 실행되는

데이터 보호 장치.

청구항 22

제 17 항 내지 제 20 항 중 어느 한 항에 있어서,

상기 장치는 상기 클라이언트 디바이스와 분리된 프록시인

데이터 보호 장치.

청구항 23

비공개 데이터를 보호하는 방법으로서,

프록시에 의해, 서버에서 클라이언트 디바이스로 전달되는 도중의 네트워크 흐름을 가로채는 단계와,

상기 네트워크 흐름의 객체 내에서 비공개 데이터 항목의 요청을 식별하는 단계와,

데이터 저장소에서 상기 비공개 데이터 항목을 식별하는 단계와,

승인 요청을 포함하는 수정된 객체를 상기 클라이언트 디바이스로 제공하는 단계와,

유효한 승인 정보가 수신될 때 상기 비공개 데이터 항목을 상기 서버로 전송하는 단계를 포함하는

비공개 데이터 보호 방법.

청구항 24

제 23 항에 있어서,

상기 데이터 저장소 내 상기 비공개 데이터 항목은, 상기 클라이언트 디바이스, 상기 클라이언트 디바이스의 사용자, 및 상기 클라이언트 디바이스 상에서 실행되는 클라이언트 애플리케이션 중 적어도 하나와 연관되는

비공개 데이터 보호 방법.

청구항 25

제 23 항 내지 제 24 항 중 어느 한 항에 있어서,

상기 데이터 저장소는 하나 이상의 비공개 데이터 항목의 복수의 집합을 포함하고, 상기 복수의 집합은 복수의 서비스와 각기 연관되는

비공개 데이터 보호 방법.

발명의 설명

기 술 분 야

[0001] 본 개시는 일반적으로 컴퓨터 네트워크 보안의 분야에 관한 것으로, 특히 비공개 데이터(privacy data)를 보호하는 보안 프록시를 제공하는 것에 관한 것이다.

배 경 기 술

[0002] 컴퓨터 보안 분야는 오늘날의 사회에서 점점 더 중요시되고 있다. 전세계의 사용자는 각종 형태의 클라이언트 디바이스를 작동하여 매일 인터넷을 검색하고 있다. 클라이언트 디바이스는 다양한 공중 및/또는 사유 네트워크를 통해 인터넷에 액세스하는 소프트웨어(예를 들면, 웹 브라우저)를 갖추어 구성될 수 있다. 클라이언트 디바이스에 의한 인터넷에 액세스를 제공하는 네트워크는 많으며, 예를 들면 사유 기업 네트워크, 홈 네트워크, 사업 시설에서 제공하는 공중 네트워크, 셀룰러 네트워크, 학교 또는 캠퍼스 네트워크 등을 포함할 수 있다.

[0003] 클라이언트 디바이스를 통해 인터넷을 검색할 때 정보의 프라이버시 및 보안을 유지하는 것은 중요한 관심사이다. 클라이언트 디바이스의 사용자는 인터넷을 통해 웹 서버 및 다른 시스템에 액세스할 때 클라이언트 디바이스의 사용자 인터페이스를 통해 종종 비공개 데이터를 제공하기도 한다. 어떤 악의의 소프트웨어("멀웨어(malware)")는 특히 인터넷에 액세스하는 브라우저를 통해 사용자에 의해 입력된 비공개 데이터를 표적으로 삼는다. 그러한 멀웨어는 브라우저에 있는 비공개 데이터를 가로채어 그 데이터를 훔쳐내도록 구성될 수 있다. 멀웨어는 또한 네트워크를 통해 제공된 서비스를 자동으로 인증하도록 임베디드 디바이스, 클라이언트 애플리케이션, 및 비밀번호 관리자에 의해 제공되는 인증 크리덴셜(authentication credential)과 같은 비공개 데이터를 가로채도록 구성될 수 있다. 훔쳐내온 특정 데이터에 따라, 권한이 없고, 심지어는 불법적인 활동이 몇 회라도 착수될 수도 있다. 그래서, 네트워크 보안 관리자 및 개인은 둘 다 클라이언트 디바이스로부터 비공개 데이터를 유용하려 시도하는 악의적인 사람으로부터 클라이언트 디바이스를 보호하는데 있어서 중대한 과제에 직면하게 된다.

도면의 간단한 설명

[0004] 본 개시 및 본 개시의 특징 및 장점의 더욱 완벽한 이해를 위해, 첨부 도면과 함께 설명되는 다음과 같은 설명이 참조되며, 도면에서 유사한 참조 부호는 유사한 부품을 나타낸다.

도 1은 본 개시의 실시예에 따라서 비공개 데이터가 보호되는 예시적인 네트워크 환경의 간략화된 블록도이다.

도 2는 본 개시의 다른 실시예에 따라서 비공개 데이터가 보호되는 다른 예시적인 네트워크 환경의 간략화된 블록도이다.

도 3은 본 개시의 실시예에 따라서 네트워크 환경의 실시예 중 적어도 하나의 실시예와 연관된 가능한 상호작용을 예시하는 상호작용 다이어그램이다.

도 4는 본 개시의 실시예에 따라서 네트워크 환경의 실시예 중 적어도 하나의 실시예와 연관된 잠재적인 행위를 예시하는 간략화된 플로우차트이다.

도 5는 실시예에 따라서 예시적인 프로세서에 연결된 메모리의 블록도이다.

도 6은 실시예에 따라서 포인트-투-포인트(point-to-point, PtP) 구성으로 배열된 예시적인 컴퓨팅 시스템의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0005] 도 1은 비공개 데이터를 보호하기 위한 시스템이 구현되는 예시적인 네트워크 환경(100)의 간략화된 블록도이다. 비공개 데이터는 이것으로 한정되지 않지만, 네트워크를 통해 제공된 서비스에 인증하는데 사용되는 크리덴셜(예를 들면, 인터넷을 검색할 때 사용자가 클라이언트 디바이스를 통해 입력되는 데이터)을 포함할 수 있다. 네트워크 환경(100)은 네트워크(110), 서버(120), 클라이언트 디바이스(130), 및 프록시(140)를 포함한다. 프록시(140)는 이것으로 한정되지 않지만, 메모리 요소(148) 및 프로세서(149)와 같은 적절한 하드웨어를 포함할 수 있다. 일부 실시예에서, 프록시(140)는 또한 사용자가 프록시(140)와 상호작용할 수 있는 사용자 인터페이스(147)를 포함할 수 있다. 데이터 저장소(145)는 비공개 데이터로 지정된 사용자 이름, 비밀번호 및 기타 정보와 같은 비공개 데이터를 저장하기 위해 프록시(140)와 통합될 수 있거나 프록시(140)의 외부에 있을 수 있다. 보호 데이터 저장 모듈(143)은 데이터 저장소(145)가 채워질 수 있도록 구성될 수 있다. 프록시(140)는 또한 데이터 저장소(145)에 저장된 비공개 데이터를 보호하도록 구성된 하나 이상의 모듈을 포함한다. 적어도 일 실시예에서, 이러한 모듈은 수정 모듈(141) 및 응답 모듈(142)을 포함할 수 있다. 클라이언트 디바이스(130)는 서버(120) 및 프록시(140)와 같은 다른 노드와 전자 통신을 개시할 수 있는 디바이스이다. 일부 실시예에서, 클라이언트 디바이스(130)는 브라우저(132), 사용자 인터페이스(137), 메모리 요소(138), 및 프로세서(139)를 포함한다. 일부 실시예에서, 클라이언트 디바이스(130)는 서버(120)와 같은 서버에 자동으로 인증하도록 구성된 클라이언트 애플리케이션(134)을 포함한다. 서버(120)는 자원을 클라이언트 디바이스(130)에 제공할 수 있는 서비스(122)를 포함하고 있다.

[0006] 도 1의 요소들은 네트워크 통신을 위한 실행 가능한 경로를 제공하는 임의의 적합한 (유선 또는 무선) 접속을 이용하는 하나 이상의 인터페이스를 통해 서로 연결될 수 있다. 또한 도 1의 이러한 요소 중 임의의 하나 이상의 요소는 특정한 구성의 필요성에 따라 조합되거나 아키텍처로부터 제거될 수 있다. 예로서, 클라이언트 디바이스(130)는 브라우저 없이 서버(120)와 통신하는 사용자 인터페이스 없는 내장된 제어기(embedded controller)일 수 있다. 네트워크 환경(100)은 네트워크에서 패킷을 송신 및/또는 수신하기 위한 전송 제어 프로토콜/인터넷 프로토콜(transmission control protocol/internet protocol, TCP/IP) 통신할 수 있는 구성을 포함할 수 있다. 네트워크 환경(100)은 또한 적절하다고 생각하는 어디에서든 특별한 필요성에 따라, 사용자 데이터그램 프로토콜/IP(user datagram protocol/IP, UDP/IP) 또는 임의의 다른 적합한 프로토콜과 함께 동작할 수 있다.

[0007] 비공개 데이터를 보호하기 위한 시스템의 특정한 예시적인 기술을 예시하기 위해, 네트워크 환경(100)에서 발생할 수 있는 행위를 이해하는 것이 중요하다. 다음의 기본적인 정보는 본 개시가 적절하게 설명될 수 있는 토대라고 생각될 수 있다.

[0008] 이동 전화, 랩톱, 데스크톱, 게이밍 시스템, 태블릿, 내장형 제어기, 스마트 센서, 차량 인포테인먼트 시스템 등과 같은 클라이언트 디바이스는 전형적으로 인터넷과 같은 네트워킹 기반 설비를 통해 네트워크 서버 및 다른 시스템과 통신하도록 구성된다. 브라우저는 인터넷을 통해 웹 페이지에 액세스하는데 사용되는 소프트웨어 애플리케이션이다. 브라우저는 웹 서버에 의해 제공된 정보 자원을 취득하고, 제시하며, 고찰하는데 사용될 수 있다. 브라우저는 전형적으로 데이터를 수신 및 송신하기 위해 하이퍼텍스트 전송 프로토콜(Hypertext Transfer Protocol, HTTP)을 이용하여 정보에 액세스하도록 구성된다. 물론, 임의의 애플리케이션은 브라우저를 이용하지 않고 직접 HTTP를 통해 통신할 수 있다. 인터넷을 통해 정보를 전파하는 다른 프로토콜, 예를 들면 SPDY 프로토콜, 파일 전송 프로토콜(file transfer protocol, FTP), 단순 메시지 전송 프로토콜(simple messaging transfer protocol, SMTP), 및 확장 가능한 마크업 언어(Extensible Markup Language, XML), 비동기 자바스크립트 및 XML(Asynchronous JavaScript and XML, AJAX), 단순 객체 액세스 프로토콜(Simple Object Access Protocol, SOAP), 자바스크립트 객체 표시(JavaScript Object Notation, JSON), RESTful 등과 같은 다양한 다른 프로토콜과 데이터 포맷이 사용될 수 있다.

[0009] 클라이언트 디바이스의 사용자는 종종 웹 서버 및 다른 시스템의 콘텐츠 및 서비스에 액세스하기 위해 자기의 클라이언트 디바이스를 통해 사용자 이름 및 비밀번호와 같은 크리덴셜을 비롯한 비공개 데이터(예를 들면, 사용자 인터페이스를 통한 사용자 입력, 저장된 데이터로부터 액세스된 입력)을 제공하기도 한다. 사용자는 또한 예를 들면 서비스를 제공하는 웹 서버 또는 다른 시스템에 의해 요청된 각종의 다른 비공개 데이터를 제공할 수

있다. 인간 사용자는 네트워크를 통해 자원 및 서비스에 액세스하는 클라이언트 디바이스와 상호작용하기 위해 몇 가지 형태의 소프트웨어(예를 들면, 브라우저, 네트워크 직면 애플리케이션(network facing application)를 구동하거나 동작할 수 있다. '서비스'는 서버로부터 클라이언트 디바이스에게 이용 가능해지는 프로그래밍 및 데이터의 임의의 조합을 포함하는 것으로 의도한다. 본 명세서에서 사용된 바와 같이, 용어 '비공개 데이터'는 사용자 또는 주체가 크리덴셜을 보존하기를 희망하는 임의의 데이터 또는 정보를 포함하는 것으로 의도한다. 비공개 데이터는 웹 서버나 다른 시스템의 콘텐츠 및 서비스에 대해 허가받은 액세스를 취득하기 위해 사용되는 비밀번호, 암호 구호(pass phrase), 사용자 이름, 개인 식별 번호(personal identification number, PIN), 및 임의의 다른 데이터를 포함할 수 있다. 비공개 데이터는 또한 이것으로 한정되지 않지만, 계정 번호(예를 들면, 금융, 건강, 학교 등), 신용 카드 번호, 개인 데이터(예를 들면, 성별, 체중 등), 사회 보장 번호, 집 주소, 특정 사진 등을 비롯하여, 사용자 또는 주체에 의해 지정된 임의의 다른 데이터 또는 정보를 포함할 수 있다.

[0010] 웹 서버 및 다른 시스템과 통신할 때 비공개 데이터의 프라이버시 및 보안을 유지하는 것은 중대한 과제를 제공한다. 하이퍼텍스트 마크업 언어(HTML) 프로토콜은 HTTP와 함께 사용되어 사용자에게 사용자 이름 및 비밀번호와 같은 비공개 데이터의 입력을 요청할 수 있는 웹 페이지를 제공하는 일반적인 프로토콜이다. 예를 들면, 암호화되지 않은 비공개 데이터가 클라이언트 디바이스의 브라우저를 통해 HTML 형태로 제공될 때, 이 데이터는 원시 형태이고 그 원시 형태로 서버에 전송될 수 있다. 원시 형태는 예를 들면 키 누름이나 버튼을 통해, 문자를 선택하는 톱다운 메뉴를 통해, 저장 장소로부터 자동 채워짐으로써 클라이언트 디바이스에 제공되는 데이터를 포함할 수 있다. 그러므로 비공개 데이터는 클라이언트 디바이스에서 볼 수 있다. 클라이언트 디바이스와 서버 사이에서 통신 신호가 (예를 들면, HTTPS 프로토콜을 통해) 암호화될지라도, 브라우저에 처음 제공된 비공개 데이터는 여전히 원시 형태이고, 따라서 클라이언트 디바이스에게 보일 수 있으며 멀웨어, 하드웨어 키 로거(hardware keylogger) 등에 의한 가로채기에 취약할 수 있다. 비공개 데이터는 브라우저가 통신 신호를 암호화하기 전에 보일 수 있고/있거나 액세스 가능하다.

[0011] 일부 사례에서, 소프트웨어는 요청된 정보에 따라 웹 서버에 의해 제공된 HTML 형태와 같은 형태로 자동으로 채워주기 위해 사용될 수 있다. 비밀번호를 요청하는 형태가 제시될 때마다 사용자에게 수작업으로 비밀번호를 입력할 것을 요구하지 않고, 비밀번호를 요청하는 HTML 형태로 비밀번호를 삽입하는 비밀번호 보관장소(비밀번호 컨센트레이터(password concentrator))가 또한 사용될 수 있다. 일부 브라우저는 또한 비밀번호를 '기억'하고, 동일한 비밀번호의 후속 요청을 인식하고, 요청될 때 그 비밀번호를 자동으로 제공하도록 구성된다. 또한, 일부의 외부 소프트웨어는 유사한 기능성을 갖는다. 그러나 이러한 해법에서, 최종 결과는 사용자를 대신하여 비공개 데이터를 어떤 형태로 삽입하는 몇 가지 형식의 소프트웨어이다. 이러한 비공개 데이터는 가로채이거나 유용되는 위험이 있다. 유사하게, 다른 프로토콜(예를 들면, SPDY, FTP, SMTP, TELNET 등)은 또한 클라이언트 디바이스와의 네트워크 통신 동안 비공개 데이터의 입력을 요청할 수 있다. 그러한 요청에 응답하여 수작업으로 또는 자동으로 제공된 비공개 데이터도 또한 가로채이거나 유용되는 위험이 있을 수 있다. 하이퍼텍스트 전송 프로토콜 보안(HyperText Transfer Protocol Secure, HTTPS), FTP 보안(FTP Secure, FTPS), 보안 셸(Secure Shell, SSH), 및 SSH 파일 전송 프로토콜(SSH File Transfer Protocol, SFTP)과 같은 암호화 프로토콜은 변환시에 데이터를 보호할 뿐이지 데이터가 암호화되기 전에는 보호하지 않는다.

[0012] 특정 멀웨어는 클라이언트 디바이스 및/또는 클라이언트 디바이스의 사용자로부터 정보를 훔쳐내기 위해 클라이언트 디바이스를 감염시키도록 설계된다. 예를 들면, 키 로거 멀웨어는 컴퓨터 내에서 구동하여 모든 키 누름을 기록하도록 구성된다. 다른 부류의 멀웨어는 맨-인-더-브라우저(man-in-the-browser)라고 지칭되며, 이는 사용자가 브라우저에 입력하는 데이터 또는 그렇지 않으면 (예를 들면, 소프트웨어에 의해) 브라우저에 삽입되는 데이터를 가로챌 수 있는 악의적인 브라우저 확장이다. 특히, 웹 양식(webform)을 채우는 비밀번호 보관소는 맨-인-더-브라우저 공격을 통해 비밀번호를 누출할 수 있다. 그러나 브라우저에 입력된 데이터를 보호하는 현재의 접근방법은 브라우저 변경(강화(hardening))에 의존하는데, 이는 비쌀 수 있다.

[0013] 도 1에서 개략적으로 개요 설명된 바와 같이, 네트워크 환경에서 비공개 데이터를 보호하는 시스템은 이러한 문제 및 다른 문제를 해결할 수 있다. 도 1의 네트워크 환경(100)에서, 프록시는 서버(예를 들면, 웹 서버)로부터 클라이언트 디바이스로 전송되어 비공개 데이터(예를 들면, 사용자 이름, 비밀번호 등)를 요청하는 객체(예를 들면, HTML 웹 페이지)를 그때그때 수정하도록 구성된다. 수정된 객체는 관련된 비공개 데이터를 잠금 해제(즉, 액세스/취득)하고 비공개 데이터를 요청 서버에게 제공하는 승인 요청을 포함한다. 프록시는 클라이언트 디바이스에게 승인 요청을 담은 수정된 객체를 제공한다. 적어도 일부 실시예에서, 관련된 비공개 데이터는 보안 환경에서 동작될 수 있는 프록시 내부에 저장될 수 있다. 일단 클라이언트 디바이스로부터 승인을 받으면, 프록시는 비공개 데이터를 취득하고 비공개 데이터를 담은 응답을 서버에게 전송한다. 일부 사례에서, 프록시는 비공개

데이터를 직접 원 객체에다 삽입하고, 데이터가 기입된 원 객체(예를 들면, HTTP POST 형태)를 서버에 업로딩할 수 있다.

[0014] 용이한 설명을 위해, 본 명세서에서 여러 실시예는 특정 형태의 객체에서 요청되어 제공된 비공개 데이터(또는 서버 전송신호), 즉 HTML 웹 페이지를 보호하는 시스템의 맥락에서 설명된다. HTML 형식을 포함할 수 있는 HTML 웹 페이지는 웹 서버로부터 클라이언트 디바이스로 제공된다. 일부 HTML 웹 페이지는 응답으로 제공될 비공개 데이터의 요청을 포함한다. 그러나 본 명세서에서 설명되는 비공개 데이터를 보호하는 시스템의 다양한 실시예의 넓은 가르침은 비공개 데이터를 송신하는 매체로서 사용되는 임의의 통신 프로토콜에서 적용될 수 있다. 그러므로, 객체라는 용어는 송신을 위해 형식화(예를 들면, HTML, XML, FTP, SMTP, SPDY, 웹 메일 등)될 수 있고 그리고 요청된 데이터를 입력하도록 구성될 수 있는 임의의 파일이나 데이터, 또는 요청 데이터를 가진 다른 응답을 포함하는 것으로 의도된다. 예를 들면, 객체는 사용자로 하여금 요청 데이터를 클라이언트 디바이스의 스크린을 통해 입력할 수 있게 할 수 있거나, 클라이언트 디바이스 또는 클라이언트 애플리케이션(예를 들면, 웹 서버에 자동으로 인증하는 클라이언트 디바이스 또는 클라이언트 애플리케이션)으로 하여금 그 요청 데이터를 가진 응답을 발생할 수 있게 할 수도 있다. 본 명세서에서 사용된 것으로 '클라이언트 애플리케이션'은 하나 이상의 프로세서에 의해 클라이언트 디바이스에서 실행되어 특정 작업을 수행할 수 있는 컴퓨터 프로그램 또는 컴퓨터 프로그램의 그룹을 의미하는 것으로 의도되며, 이는 소프트웨어, 코드, 로직, 명령어, 함수, 알고리즘 등을 포함할 수 있다. 이러한 작업은 서버에 자동 인증하는 것과 같이 비공개 데이터를 네트워크를 통해 서비스에 제공하는 것을 포함한다.

[0015] 이제 도 1을 참조하면, 네트워크 환경(100)은 클라이언트 디바이스와 웹 서버(또는 다른 시스템) 사이의 네트워크 통신 동안 비공개 데이터를 보호하기 위한 시스템을 제공한다. 도 1의 아키텍처와 연관된 잠재적인 흐름을 논의하기 전에, 네트워크 환경(100)과 연관될 수 있는 가능한 컴포넌트 및 기반 설비 중 일부에 관해 간략한 설명이 제공된다.

[0016] 일반적으로, 네트워크 환경(100)은 네트워크(110)로 표시된 임의의 형태 또는 토폴로지의 네트워크를 포함할 수 있다. 네트워크(110)는 네트워크 환경(100)을 통해 전파하는 네트워크 통신 신호를 수신하고 전송하기 위한 상호 접속된 통신 경로의 일련의 지점 또는 노드를 나타낸다. 네트워크(110)는 노드들 사이에서 통신 인터페이스를 제공하며, 무선(예를 들면, 3G/4G/5G/nG 네트워크, WiFi, IEEE(Institute of Electrical and Electronics Engineers, IEEE) 표준 802.11™-2012 (2012년 3월 29일 공개), WiMAX, IEEE 표준 802.16™-2012 (2012년 8월 17일 공개), 무선 주파수 식별(Radio-frequency Identification, RFID), 근접장 통신(Near Field Communication, NFC), Bluetooth™, 등) 및/또는 유선 (예를 들면, 이더넷 등) 통신을 비롯한 네트워크 환경에서 통신을 가능하게 해주는 임의의 근거리 네트워크(local area network, LAN), 가상 근거리 네트워크(virtual local area network, VLAN), 인터넷과 같은 광역 네트워크(wide area network, WAN), 무선 근거리 네트워크(wireless local area network, WLAN), 도시 지역 네트워크(metropolitan area network, MAN), 인트라넷, 엑스트라넷(Extranet), 가상 사설 네트워크(virtual private network, VPN), 및 임의의 다른 적절한 아키텍처나 시스템, 또는 이들의 임의의 적적한 조합일 수 있다. 일반적으로, 임의의 적절한 통신 수단, 즉 전기, 소리, 빛, 적외선, 무선(예를 들면, WiFi, 블루투스 또는 NFC)이 사용될 수 있다.

[0017] 패킷, 프레임, 신호, 데이터, 객체 등을 포함할 수 있는 네트워크 흐름(또한 '네트워크 통신신호' 및 '네트워크 전송신호'라고도 지칭함)은 임의의 적합한 통신 메시징 프로토콜에 따라서 전송되고 수신될 수 있다. 적합한 통신 메시징 프로토콜은 개방 시스템 상호접속(Open Systems Interconnection, OSI) 모델과 같은 다계층 체계, 또는 이것의 임의의 유도체나 변형체(예를 들면, 전송 제어 프로토콜/인터넷 프로토콜(Transmission Control Protocol/Internet Protocol, TCP/IP), 사용자 데이터그램 프로토콜/IP(user datagram protocol/IP, UDP/IP)를 포함할 수 있다. 접속은 동적 방식으로 소프트웨어 정의 네트워크(software defined network, SDN)를 통해 이루어질 수 있다. 본 명세서에서 사용된 바와 같은 용어 '데이터'는 컴퓨팅 디바이스(예를 들면, 클라이언트 디바이스, 서버, 프록시) 및/또는 네트워크에서 한 지점에서 다른 지점으로 전달될 수 있는 임의의 적당한 포맷으로 된 임의의 형태의 이진수, 숫자, 음성, 영상, 텍스트, 사진이나 스크립트 데이터, 또는 임의의 형태의 소스나 오브젝트 코드, 또는 임의의 다른 적합한 정보를 말한다. 또한, 메시지, 요청, 응답, 답변, 쿼리 등은 네트워크 흐름의 형태이다.

[0018] 클라이언트 디바이스(130)와 같은 클라이언트 디바이스는 네트워크 환경에서 네트워크 통신을 개시하는데 사용될 수 있고 비공개 데이터가 전달될 수 있는 임의의 형태의 컴퓨팅 디바이스를 나타내는 것으로 의도된다. 일부 실시예에서, 클라이언트 디바이스는 네트워크 환경(100)에서 일부 네트워크를 통해 네트워크 세션을 설정하기를 바라는 최종 사용자(end user)와 연관될 수 있다. 용어 '클라이언트 디바이스'는 또한 네트워크 환경에서 사용

자 상호작용 없이 서버와 통신하는 임의의 형태의 컴퓨팅 디바이스(예를 들면, 네트워크를 통해 서버에 자동으로 인증하는 내장형 제어기, 네트워크를 통해 서버에 자동으로 인증하는 클라이언트 애플리케이션을 갖춘 컴퓨팅 디바이스)를 포함하는 것으로 의도된다. 클라이언트 디바이스는 이것으로 한정되지 않지만, 네트워크 환경(100) 내에서 음성, 오디오, 비디오, 미디어, 또는 데이터의 교환을 개시할 수 있는 워크스테이션, 단말기, 랩톱, 데스크톱, 태블릿, 게이밍 시스템, 이동 디바이스, 스마트폰, 스마트 센서, 인포테인먼트 시스템, 내장형 제어기, 스마트 가전기기, 글로벌 포지셔닝 시스템(GPS), 또는 임의의 다른 디바이스, 컴포넌트나 요소를 포함할 수 있다. 일부 실시예에서, 클라이언트 디바이스(130)는 또한 디스플레이, 키보드, 터치패드, 리모콘, 또는 이들의 임의의 적합한 조합과 같은 사람 사용자와의 적합한 인터페이스를 포함할 수 있다.

[0019] 프록시(140)와 같은 프록시는 클라이언트 디바이스와 웹 서버(또는 다른 컴퓨팅 디바이스 또는 시스템) 사이에서 통신을 위한 중재자로서 역할을 하는 네트워크 요소이다. 본 명세서에서 사용된 바와 같은, 용어 '네트워크 요소'는 네트워크 환경에서 정보를 교환하도록 동작할 수 있는 라우터, 스위치, 게이트웨이, 브릿지, 로드밸런서, 방화벽, 인라인 서비스 노드, 프록시, 서버, 프로세서, 모듈, SDN 제어기/스위치, 또는 임의의 다른 적합한 디바이스, 컴포넌트, 요소 또는 전용 가전기기를 포함하는 의미를 갖는다. 이러한 네트워크 요소는 이들의 동작을 가능하게 해주는 임의의 적합한 하드웨어, 소프트웨어, 펌웨어, 컴포넌트, 모듈, 인터페이스 또는 객체를 포함할 수 있다. 네트워크 요소는 데이터나 정보의 효과적인 교환을 가능하게 해주는 적절한 알고리즘 및 통신 프로토콜을 포함할 수 있다. 프록시(140)는 임의의 네트워크 요소 내에 포함될 수 있다.

[0020] 일부 실시예에서, 프록시(140)는 도 1에서 예시된 바와 같이 클라이언트 디바이스(130)로부터 분리될 수 있으며, 클라이언트 디바이스(130)와 서버(120) 사이의 적절하다고 생각하는 어디에서든 특별한 필요성에 따라 구현될 수 있다. 만일 프록시(140)가 클라이언트 디바이스(130)와는 별개의 디바이스에서 구현되면, 프록시(140)의 코드는 비공개 데이터의 요청에 응답하여 서버(120)로부터 제공된 비공개 데이터를 보호하는 보안 환경에서 동작할 수 있다.

[0021] 예시적인 구현예에서, 프록시(140)는 보호받는 기업 네트워크에서 보안 라우터 또는 게이트웨이일 수도 있다. 프록시(140)는 서버와 보호받는 기업 네트워크에 속한 복수의 클라이언트 디바이스 사이에서 전달되는 도중의 네트워크 흐름을 가로채도록 구성될 수 있다. 프록시(140)는 예를 들면 인터넷을 통해 서버(120)에 접속하도록 구성될 수 있다. 다른 예에서, 프록시(140)는 홈 네트워크의 보안 라우터에서 구현될 수 있다. 프록시(140)는 인터넷과 같은 네트워크를 통해 액세스 가능한 홈 네트워크 내 클라이언트 디바이스(예를 들면, 클라이언트 디바이스(130))와 서버(예를 들면, 서버(120)) 사이에서 전달되는 도중의 네트워크 흐름을 가로채도록 구성될 수 있다. 또 다른 구현예에서, 프록시(140)는 신뢰성 있는 클라우드에서 구현될 수 있다. 서버(120)와의 접속을 시작하는 클라이언트 디바이스는 인터넷을 통해 먼저 프록시(140)에 접속할 수 있다. 따라서, 프록시(140)는 각종 네트워크(예를 들면, 기업 네트워크, 가정 네트워크, 학교 네트워크 등) 및 스탠드 얼론 클라이언트 디바이스(예를 들면, 셀룰러 기술을 이용하는 이동 디바이스, 무선 기술을 이용하는 이동 디바이스 등)로부터 복수의 클라이언트 디바이스의 비공개 데이터를 보호할 수 있다. 본 명세서에서 제공된 예는 그저 프록시(140)의 가능한 구현의 예시일 뿐이지 본 개시 및 본 명세서에서 개시된 실시예의 잠재적인 애플리케이션과 다른 구현예의 넓은 가르침을 한정하려 의도하지 않는다.

[0022] 적어도 일 예에서, 프록시(140)는 본 명세서에서 개요 설명한 바와 같이, 비공개 데이터 보호를 달성하는(또는 조성하는) 소프트웨어를 포함한다. 이러한 요소는 각기 본 명세서에서 설명된 동작의 일부를 가능하게 하는 내부 구조체(예를 들면, 프로세서, 메모리 요소 등)를 가질 수 있다. 다른 실시예에서, 이러한 비공개 데이터 보호는 이러한 요소의 외부에서 실행될 수 있거나, 이렇게 의도된 기능성을 달성하는 몇몇 다른 네트워크 요소에 포함될 수 있다. 대안으로, 프록시(140)는 본 명세서에서 개요 설명한 바와 같이, 그 동작을 달성하기 위해 다른 네트워크 요소와 협력할 수 있는 이러한 소프트웨어(또는 왕복 소프트웨어(reciprocating software))를 포함할 수 있다. 또 다른 실시예에서, 하나 또는 여러 디바이스는 그의 동작을 가능하게 해주는 임의의 적합한 알고리즘, 하드웨어, 소프트웨어, 펌웨어, 컴포넌트, 모듈, 인터페이스 또는 객체를 포함할 수 있다.

[0023] 도 1에서 서버(120)와 같은 서버는 네트워크(110)와 같은 하나 이상의 네트워크를 통해 클라이언트 디바이스 또는 다른 컴퓨팅 디바이스에게 서비스를 제공하는 네트워크 요소이다. 서버(120)에 의해 제공된 서비스(122)는 그 서비스에 인증하는데 필요한 크리덴셜과 같은 비공개 데이터를 요청하도록 구성될 수 있다. 서비스(122)는 예를 들면 각종 자원이나 계정(예를 들면, 금융, 의료, 소매, 조직, 기업 등), 파일 전송, 이메일, 웹 콘텐츠 등으로의 액세스를 포함할 수 있다. 적어도 일부 실시예에서, 서버(120)는 이것으로 한정되지 않지만, 웹 콘텐츠를 전달하는 웹 서버, 파일을 요청 시 클라이언트 디바이스에 전달하는 파일 전송 서버, 전자 메일 메시지를 클라이언트 디바이스에서 목적지로 전달하는 이메일 서버, 뉴스그룹에 액세스하기 위한 뉴스 서버, 상호작용 게

임을 제공하는 게이밍 서버, 애플리케이션 및/또는 데이터베이스로의 액세스를 제공하는 애플리케이션 서버, 또는 이들의 임의의 조합을 포함할 수 있다.

[0024] 프록시(140)는 비공개라고 지정된 데이터를 보호하도록 구성된 하나 이상의 모듈을 포함하는 보안 프록시이다. 데이터 저장소는 하나 이상의 네트워크 에이전트와 연관된 비공개 데이터의 저장소로서 구성될 수 있다. 본 명세서에서 사용된 바와 같은, 용어 '네트워크 에이전트'는 사용자, 클라이언트 애플리케이션, 및 클라이언트 디바이스를 포함하는 것으로 의도된다. 데이터가 데이터 저장소(145)에 저장될 때 이 데이터는 비공개로서 지정된다. 적어도 일부 실시예에서, 비공개 데이터는 적어도 하나의 네트워크 에이전트 이외에도, 적어도 하나의 서비스(및 그의 대응하는 서버)와 '연관'될 수 있다. 데이터 저장소(145) 내 비공개 데이터 항목(또는 비공개 데이터 항목의 집합)은 특정 서비스의 하나 이상의 식별자에 맵핑되어 서비스와의 연관성을 표시할 수 있다. 이러한 식별자는 이것으로 한정되지 않지만, 서버의 도메인 이름, 서비스의 균일 자원 위치 표시자(uniform resource locator, URL)(예를 들면, HTML 웹 페이지의 URL), 서버의 네트워크 어드레스 등을 포함할 수도 있다. 비공개 데이터 항목(또는 비공개 데이터 항목의 집합)은 또한 하나 이상의 네트워크 에이전트와의 연관성을 표시하기 위해 하나 이상의 네트워크 에이전트의 식별자에 맵핑될 수 있다. 이러한 식별자는 이것으로 한정되지 않지만, 매체 접근 제어(Media Access Control, MAC) 어드레스, 보안 식별자(Security Identifier, SID)와 같은 사용자 식별자, 파일명과 같은 클라이언트 애플리케이션 식별자 등을 포함할 수도 있다. 비공개 데이터 항목의 집합의 일 예는 특정 사용자가 하나 이상의 특정 클라이언트 디바이스를 통해 특정 서비스에 액세스하기 위한 사용자 이름 및 비밀번호일 수도 있다. 비공개 데이터 항목의 여러 집합은 비공개 데이터 항목의 각 집합이 상이한 서비스와 연관되는 동일 네트워크 에이전트(또는 에이전트들)와 연관될 수 있다. 개개의 비공개 데이터 항목은 또한 항목이 표현하는 비공개 데이터의 형태(예를 들면, 사용자 이름, 비밀번호, 계좌번호, 개인 식별 번호(personal identification number, PIN), 보안 질문 답변 등)가 무엇인지를 표시하는 임의의 적합한 서술자 또는 태그와 연관될 수 있다.

[0025] 적어도 일부 실시예에서, 서비스 및/또는 네트워크 에이전트의 식별자는 비공개 데이터 항목과 식별자 사이의 관계, 연결, 또는 링크를 나타내는 임의의 적합한 맵핑, 마킹, 또는 링킹 기술(예를 들면, 리스트, 테이블, 연관 배열(associative array), 포인터, 색인, 그래프, 링크된 리스트, 파일명, 관계형 데이터베이스, 해시 테이블 등) 또는 임의의 다른 기술이나 메커니즘을 이용하여 데이터 항목(또는 비공개 데이터 항목의 집합)에 맵핑될 수 있다. 예를 들면, 일반적으로 전자 정보를 조직화하기 위해 사용되는 데이터 구조인 간단한 테이블 구성은 이전에 설명한 것처럼 데이터 저장소(145)를 구현하는 한 가지 가능한 방법이다. 그러나, 데이터 저장소(145)는 다양한 다른 방법으로 모델링될 수도 있으며, 이렇게 다른 구성은 특정 구현의 특별한 선호도 및 필요성에 근거할 수 있다. 비공개 데이터 항목은 또한 그 형태를 표시하는 태그 또는 서술자에 맵핑될 수 있다.

[0026] 적어도 일부 실시예에서, 프록시가 동일한 비공개 데이터와 연관된 하나 이상의 네트워크 에이전트(예를 들면, 하나 이상의 클라이언트 디바이스를 사용하는 단일의 사용자, 단일 클라이언트 애플리케이션을 갖춘 단일의 클라이언트 디바이스 등)의 비공개 데이터를 다루도록 구성되었을 때, 비공개 데이터 항목은 (비록 이 데이터 항목이 그럴 필요가 있을지라도) 연관된 네트워크 에이전트의 임의의 식별자에 반드시 맵핑될 필요가 없을 수 있다. 그러나 만일 프록시가 여러 비공개 데이터와 연관된 복수의 네트워크 에이전트의 비공개 데이터를 다루도록 구성되면, 특정 네트워크 에이전트와 연관된 비공개 데이터 항목(또는 비공개 데이터 항목의 집합)은 그 네트워크 에이전트의 식별자에 맵핑될 수 있다. 또한, 일부 사례에서, 복수의 네트워크 에이전트는 비공개 데이터 항목(또는 비공개 데이터 항목의 집합)과 연관될 수 있다. 예를 들면, 사용자에 의해 클라이언트 디바이스를 통해 서비스에 (예를 들어, 수작업으로 또는 자동으로) 제공된 비공개 데이터 항목은 사용자 및 클라이언트 디바이스와 연관된다. 만일 사용자가 복수의 클라이언트 디바이스를 통해 비공개 데이터 항목을 서비스에 공급하면, 비공개 데이터 항목은 사용자 및 그 사용자에 의해 사용된 모든 클라이언트 디바이스에 연관될 수 있다. 이러한 사례에서, 데이터 저장소(145) 내 비공개 데이터 항목은 사용자에 의해 사용된 하나 이상의 클라이언트 디바이스 각각의 식별자, 아니면 사용자의 식별자 또는 이들의 임의의 조합에 맵핑될 수 있다. 다른 예로, 만일 비공개 데이터 항목이 클라이언트 애플리케이션에 의해 클라이언트 디바이스를 통해 서비스에 제공되면, 비공개 데이터 항목은 클라이언트 애플리케이션 및 클라이언트 디바이스와 연관된다. 이러한 사례에서, 데이터 저장소(145) 내 비공개 데이터 항목은 클라이언트 애플리케이션의 식별자, 아니면 클라이언트 디바이스의 식별자, 또는 그 조합에 맵핑될 수도 있다. 또 다른 예로, 만일 비공개 데이터 항목이 내장형 제어기인 클라이언트 디바이스에 의해 서비스에 제공되면, 비공개 데이터 항목은 내장형 제어기와 연관되며 내장형 제어기의 식별자에 맵핑될 수 있다.

[0027] 예로써, 금융 기관과 같은 특정 주체가 기관의 웹 서버를 통해 계정에 액세스하기를 허가받기 전에 등록된 사용

자 이름과 비밀번호를 제공할 것을 요구할 때, 사용자-1이 소유한 계정의 사용자 이름 및 비밀번호는 프록시(140)의 데이터 저장소(145) 내의 금융 기관과 연관될 수 있다. 적어도 일 실시예에서, 사용자 이름 및 비밀번호는 사용자 이름 및 비밀번호를 요청하는 금융 기관의 도메인 이름 또는 금융 기관의 웹 페이지의 균일 자원 위치 표시기(URL)에 맵핑될 수도 있다. 만일 프록시가 복수의 사용자의 비공개 데이터를 포함하고 있으면, 사용자 이름 및 비밀번호는 또한 사용자-1의 식별자, 아니면 사용자-1에 의해 사용된 하나 이상의 클라이언트 디바이스의 식별자, 또는 그 조합에 맵핑될 수 있다.

[0028] 일부 실시예에서, 특정 비공개 데이터는 반드시 특정 서비스 및 대응하는 서버와 직접 연관될 필요 없을 수 있다. 예를 들면, 특성상 더 일반적이면서 많은 서비스에 의해 요청된 비공개 데이터는 항목이 나타내는 비공개 데이터가 무슨 형태인지를 표시하는 적합한 서술자 또는 태그와 함께 데이터 저장소(145) 내에 저장될 수 있다. 예를 들면, 집 주소, 전화번호, 성별, 혼인 여부 등이 임의의 적절한 서술자, 태그 등과 함께 데이터 저장소(145) 내에 저장될 수 있다. 서비스(122)가 이렇게 일반적인 비공개 데이터의 요청을 클라이언트 디바이스(130)로 전송할 때, 프록시(140)는 요청되는 비공개 데이터의 특정 형태를 해석하도록 구성될 수 있다. 프록시(140)는 또한 서버로부터의 요청에 대응하는 클라이언트 디바이스 및 다른 네트워크 에이전트(예를 들면, 사용자, 클라이언트 애플리케이션)와 연관된 비공개 데이터를 찾아 데이터 저장소(145)를 검색할 수 있다. 프록시(140)는 또한 프록시(140) 내 어느 비공개 데이터 항목이 서버(120)에 의해 요청된 특정 형태의 데이터를 나타내는 서술자 또는 태그와 연관되는지를 식별할 수 있다.

[0029] 적어도 일부 실시예에서, 데이터 저장소(145)는 프록시(140) 내에 통합되어 보호되는 비공개 데이터의 보안 저장소이다. 다른 실시예에서, 데이터 저장소(145)는 프록시(140)에 의해 액세스 가능한 별개의 저장 디바이스에서 보호될 수 있다. 임의의 적합한 기술은 데이터 저장소(145)에다 저장하도록 구성될 수 있다. 일 예로, 비공개 데이터 항목 및 이들의 연관된 서비스의 리스트를 승인된 사람이나 주체(예를 들면, 서비스 공급자, 네트워크 관리자 등)에 제공하도록 임의의 하나 이상의 통신 채널(예를 들면, 작성된 메일, 암호화된 파일 전송, 구두 연락 등)이 활용될 수 있다. 이후 데이터 저장소(145)에는 비공개 데이터 항목이 저장되어 있을 수 있다. 예를 들면, 기업 네트워크 환경에서, 사용자는 비공개 데이터 항목 및 관련된 서비스의 식별자를 데이터 저장소(145)에 입력하기 위해 네트워크 관리자에게 제공할 수도 있다. 각각의 사용자는 또한 기업 네트워크 환경에 속한 그 사용자에 의해 사용된 모든 클라이언트 디바이스의 리스트를 제공할 수도 있다. 클라이언트 디바이스의 식별자는 데이터 저장소(145)에 입력되어 사용자의 비공개 데이터 항목에 맵핑될 수도 있다. 적어도 일부 실시예에서, 보호 데이터 저장 모듈(143)은 비공개 데이터 항목을 (예를 들면, 비공개 데이터 항목의 수작업 입력을 위한 사용자 인터페이스를 통해, 특정 형태의 파일을 판독하고 그 파일로부터 데이터 항목을 저장하는 소프트웨어를 통해, 등등) 데이터 저장소(145)에 채워질 수 있도록 구성될 수도 있다. 다른 예로, 특정 비공개 데이터 항목은 제조자에 의해 데이터 저장소(145)에 채워질 수 있다. 예를 들면, 내장형 제어기의 제조자는 내장형 제어기가 제조자의 서비스를 인증하도록 할 수 있는 비밀번호 및 사용자/디바이스 식별자를 데이터 저장소에 채워질 수 있다.

[0030] 일부 실시예에서, 데이터 저장소(145)에다 채우고/채우거나 데이터 저장소(145)를 갱신하는 점진적인 접근법이 사용될 수 있다. 프록시(140)는 서버에 의해 요청된 비공개 데이터가 사용 가능하지 않다는 것을 자동으로 검출하도록 구성될 수 있다. 이러한 시나리오에서, 프록시(140)는 요청된 비공개 데이터의 엔트리를 생성하라는 요청을 클라이언트 디바이스(130)에게 전송할 수 있다. 서버로부터 비공개 데이터의 요청에 대응하는 임의의 네트워크 에이전트(즉, 사용자, 클라이언트 애플리케이션, 또는 클라이언트 디바이스)는 요청된 비공개 데이터를 생성할 수 있다. 일 예로, 프록시(140)는 사용자로 하여금 사용자가 어느 웹 요소를 비공개로 간주하는지를 프록시(140)에게 표시하게 하도록 구성될 수 있다. 예를 들면, 사용자는 어느 데이터 항목이 비공개로 취급되어야 할지를 표시하기 위해 프록시(140)와 대역외 통신(out-of-band communication)할 수 있다. 다른 예로, 수정되지 않은 HTML 웹 페이지와 같은 수정되지 않은 정보 요청이 클라이언트 디바이스(130)에 제공될 수 있으며 사용자는 요청된 데이터 항목에 필요한 입력을 제공할 수 있다. 프록시(140)는 후속 네트워크 흐름에서 이와 같은 새로운 요소를 인식하고 처리하도록 구성될 수 있다. 적어도 일부 실시예에서, 프록시(140)는 또한 데이터 저장소(145)를 사용자에 의해 표시된 이러한 새로운 비공개 데이터로 채워지게 할 수 있다.

[0031] 프록시(140)는 또한 클라이언트 디바이스가 사용자와의 연계를 학습하도록 구성될 수 있다. 이러한 연계는 구성 시간 때 학습되어 동일 사용자에 의해 사용되는 모든 클라이언트 디바이스를 그룹화한 일련의 MAC 어드레스로서 저장될 수 있다. 이러한 연계는 또한 자동으로 학습될 수 있다. 예를 들면, 만일 특정 서비스에 대해 비밀번호가 없으면, 사용자는 비밀번호 요청을 담은 변경되지 않은 객체를 얻을 수 있다. 사용자는 비밀번호를 공급할 수 있다. 만일 복수의 클라이언트 디바이스로부터 동일한 비밀번호가 입력되면, 클라이언트 디바이스는 향후 자

동으로 동일한 사용자와 연관될 수 있다.

[0032] 초기에 데이터 저장소(145)에 채워질 때, 네트워크 에이전트로 하여금 프록시(140)가 데이터 저장소(145)로부터의 관련된 비공개 데이터를 사용하도록 인증할 수 있게 하는 잠금 해제 메커니즘이 시작될 수 있다. 적어도 일부 실시예에서, 비공개 데이터의 사용을 승인하기 위해 반복되지 않는 비밀번호의 시퀀스가 사용되는 일회용 비밀번호(one-time-password, OTP) 기술이 사용될 수 있다. 일회용 비밀번호는 알고리즘에 의해 미리 발생(또는 랜덤하게 발생)될 수 있고, 임의의 적절한 통신 채널(예를 들면, 이동 전화와 같은 개별 디바이스에서 구동하는 단문 메시지 서비스(short message service, SMS) 메시지, 보안 토큰, 소프트웨어 등과 같은 대역외 채널)을 이용하여 네트워크 에이전트와 공유될 수 있다. 다른 실시예에서, 프록시(140)와의 하나 이상의 보안 통신 채널이 인증(예를 들면, 다중 인증(multi-factor authentication), 인간 존재(human presence) 등)을 제공하기 위해 채용될 수 있다. 일부 실시예에서 생체 인식 데이터(예를 들면, 지문, 망막 및 홍채, 음성 인식 등)가 또한 비공개 데이터를 잠금 해제하는데 사용될 수 있다. 일부 실시예에서, 비공개 데이터의 자동 잠금 해제는 특정 시나리오(예를 들면, 검증된 사용자 존재, 이전 인증의 이력, 특정 HTML 형식의 인증을 요구하지 않는 사용자의 프록시(140) 요청 이력 등) 하에서 허용될 수 있다. HTTPS 프로토콜을 사용하는 네트워크 흐름의 경우, 프록시(140)는 또한 보안 경고를 발생하지 않고 HTTPS 네트워크 흐름을 처리하기 위해 보안 소켓 계층(secure socket layer, SSL) 중간자 공격(man-in-the-middle, MitM)로서 동작할 수 있다. 적어도 일부 실시예에서, 데이터 저장소(145)는 (예를 들면, 프록시(140)의 공개키로 암호화된) 암호화된 통신을 통해 채워질 수 있으며, 및 대응하는 비밀 키를 가진 프록시(140) 내부에서 유일하게 해독 가능할 수 있다. 이러한 접근방법은 임의의 개수의 다른 잠금 해제 메커니즘이 본 명세서에서 기술된 비공개 데이터를 보호하는 시스템의 실시예에서 구현될 수 있다는 것으로서 예시되는 것이지 한정하려는 의도는 아니다. 더욱이, 이러한 잠금 해제 메커니즘 중 하나 이상은 또한 이것으로 한정되지 않지만, HTTP, SPDY, FTP, SMTP, 포스트 오피스 프로토콜(Post Office Protocol, POP), 인터넷 메시지 액세스 프로토콜(Internet Message Access Protocol, IMAP) 등을 비롯한 임의의 프로토콜과 함께 동작할 수 있다.

[0033] 적어도 일부 실시예에서, 잠금 해제 메커니즘은 별개의 보안 프로토콜이나 통신 링크를 통해 수행될 수 있다. 승인 요청은 상이한 매체, 채널 또는 프로토콜을 사용하여 클라이언트 디바이스로 제공될 수 있다. 예를 들면, 프록시는 클라이언트를 조작하는 인간 사용자의 생체를 검증하기 위해 UDP 프로토콜을 통해 클라이언트 디바이스 내부의 신뢰성 있는 실행 환경(trusted execution environment, TEE)을 요청할 수 있다. TEE는 이것을 사용자에게 보이지 않게 행할 수 있고(예를 들면, 얼굴 인식), 그래서 사용자 친화적 방식으로 비공개 데이터의 잠금 해제를 승인하고 허용할 수 있다. 다른 예로, 프록시는 로그인하기 위해 크리덴셜을 요청하는 웹 페이지의 상황 외의 지문 스캔을 요청할 수 있다. 그러면 서버 전송신호의 프록시의 수정은 로그인-요청 페이지를 완전히 제거할 수 있고, 이 경우 생체 인식은 프록시가 사용자에게 투명하게 로그인을 수행하게 할 수 있다.

[0034] 동작 측면에서, 프록시(140)는 서버(120)에서 클라이언트 디바이스(130)로 전송된 비공개 데이터 요청을 담은 객체를 그때그때 수정하는 수정 모듈(141)로 구성될 수 있다. 수정 모듈(141)은 네트워크 통신의 임의의 레벨에서 구현될 수 있다. 예를 들면, 수정 모듈은 애플리케이션 계층 전송에서 동작할 수 있거나 수정 모듈은 전송(예를 들면, TCP/IP 패킷) 레벨에서 동작할 수 있다. 임의의 다른 적합한 수정 방법이 또한 채용될 수 있다. 요청된 비공개 데이터는 서버로부터의 네트워크 흐름에 대응하는 클라이언트 디바이스(130)의 사용자 또는 다른 네트워크 에이전트와 연관된 하나 이상의 비공개 데이터 항목(예를 들면, 사용자 이름, 비밀번호, 계정 번호, 암호 구호, 집 주소, 개인 데이터, 종교, 특정 사진 등)을 포함할 수 있다. 수정 모듈(141)은 어느 서비스가 요청과 연관되는지, 그리고 무슨 형태의 비공개 데이터 항목이 객체에서 요청되었는지를 결정하도록 구성될 수 있다. 수정 모듈(141)은 또한 데이터 저장소(145)가 요청된 비공개 데이터 항목과 동일한 형태를 갖고 그리고 그 특정 서비스(예를 들면, 서비스(122))와 연관된 클라이언트 디바이스(130)(및/또는 서버로부터 네트워크 흐름에 대응하는 다른 네트워크 에이전트)와 연관된 비공개 데이터 항목을 포함하고 있는지를 결정할 수 있다. 데이터 저장소(145)에 저장된 비공개 데이터 항목은 모두 잠재적으로 단일의 사용자, 단일의 클라이언트 애플리케이션, 또는 단일의 내장형 제어기와 연관될 수 있다. 이러한 시나리오에서, 수정 모듈(141)은 네트워크 에이전트(들)와 저장된 비공개 데이터 항목 사이의 연계를 결정하지 않아도 될 수 있다.

[0035] 서버에 의해 요청된 비공개 데이터 항목이 데이터 저장소(145) 내에서 발견될 때, 수정 모듈(141)은 요청된 비공개 데이터를 잠금 해제하는 승인 요청을 가진 수정된 객체를 생성할 수 있다. 수정된 객체는 원 객체의 사본을 수정함으로써, 새로운 객체를 만듦으로써, 또는 원 객체를 수정함으로써 생성될 수 있다. 일부 시나리오에서, 원 객체의 사본은 요청된 비공개 데이터를 요청 서버에게 제공하는 향후 사용을 위해 저장되지 않아도 될 수 있다. 비공개 데이터 요청을 가진 원 객체를 대신하여, 승인 요청을 가진 수정된 객체가 목적하는

클라이언트 디바이스로 제공될 수 있다. 적어도 일부 실시예에서, 승인 요청은 클라이언트 디바이스의 스크린 상에 디스플레이될 수 있고 요구된 승인을 입력하는 사용자에게 프롬프트를 제공할 수 있다. 사용자는 프록시(140)가 요청 서버와 연관된 사용자의 비공개 데이터를 잠금 해제하도록 승인하는 적절한 인증(예를 들면, 미리 공유된 일회용 비밀번호, 생체 인식 데이터, 다중 인증 등)을 제공할 수 있다.

[0036] 프록시(140)는 인증 요청에 응답하는 클라이언트 디바이스로부터의 통신 신호를 처리하는 응답 모듈(142)을 포함할 수 있다. 응답 모듈(142)은 클라이언트 디바이스(130)로부터 응답을 수신하고 그 응답에 담긴 임의의 인증 정보를 검증하도록 구성될 수 있다. 만일 인증 정보의 검증 결과 인증 정보가 유효하다고 표시되면, 프록시(140)는 관련된 비공개 데이터 항목을 데이터 저장소(145)로부터 구할 수 있다. 응답 모듈(142)은 비공개 데이터 항목을 요청 서비스(예를 들면, 서버(120)의 서비스(122))로 제공할 수 있다.

[0037] 예시적인 시나리오에서, 서비스(122)에 의해 클라이언트 디바이스(130)로 전송된 객체가 사용자 이름 및 비밀번호를 요청하는 HTML 웹 페이지라고 가정한다. 프록시(140)는 HTML 웹 페이지가 사용자의 사용자 이름 및 비밀번호의 입력을 받아 들이도록 구성된 필드를 포함하고 있다고 인식한다. 프록시(140)는 사용자 이름 및 비밀번호가 목적지 클라이언트 디바이스(및/또는 사용자)와 연관된 것인지 그리고 서버(120)와도 연관된 것인지를 결정하기 위해 데이터 저장소(145)를 검색할 수 있다. 사용자 이름 및 비밀번호가 발견되면, 프록시(140)는 승인 요청을 가진 수정된 HTML 웹 페이지를 생성할 수 있다. 인증 요청은 사용자 이름 및 비밀번호를 잠금 해제하기 위한 인증 메커니즘을 포함한다. 프록시(140)는 수정된 HTML 웹 페이지를 클라이언트 디바이스(130)로 전송할 수 있고 클라이언트 디바이스(130)로부터 응답을 수신할 수 있다. 만일 응답에서 인증 정보가 유효하면, 프록시(140)는 관련 사용자 이름 및 비밀번호 데이터 항목을 데이터 저장소(145)로부터 구할 수 있다. 프록시는 또한 원 HTML 웹 페이지의 사용자 이름 및 비밀번호 필드를 데이터 저장소(145)로부터 구한 사용자 이름 및 비밀번호 데이터 항목으로 채울 수 있다. 이후 응답(예를 들면, HTML POST 요청)은 완성된 HTML 웹 페이지에 기초하여 서버(120)로 전송될 수 있다.

[0038] 도 2는 시스템이 비공개 데이터를 보호하기 위해 구성된 네트워크 환경(200)을 제공하는 대안의 실시예를 예시한다. 네트워크 환경(200)은 네트워크(210) 및 서비스(222)를 가진 서버(220)를 포함할 수 있는데, 이는 도 1을 참조하여 앞에서 도시되고 설명된 네트워크(110) 및 서비스(122)를 가진 서버(120)와 유사하다. 네트워크 환경(200)은 또한 도 1의 클라이언트 디바이스(130)와 유사한 몇몇 컴포넌트를 가질 수 있는 클라이언트 디바이스(230)를 포함할 수 있다. 예를 들면, 클라이언트 디바이스(230)는 브라우저(232), 사용자 인터페이스(237), 메모리 요소(238) 및 프로세서(239)를 포함할 수 있다. 일부 실시예에서, 클라이언트 디바이스(230)는 또한 서버(220)와 같은 서버에 자동 인증하도록 구성된 클라이언트 애플리케이션(234)을 포함할 수 있다. 그러나, 클라이언트 디바이스(130)와 달리, 클라이언트 디바이스(230)는 프록시(240) 및 데이터 저장소(245)가 클라이언트 디바이스(230)의 신뢰성 있는 실행 환경(235) 내에 있는 것으로 구성된다. 신뢰성 있는 실행 환경의 적어도 일부 구성에 대해, 프록시(240)는 프록시(240)의 코드가 악의적인 소프트웨어에 의해 손상 받지 않도록 보장하기 위해 디바이스의 제조자에 의해 서명된 소프트웨어를 통해 클라이언트 디바이스(예를 들면, 이동 전화) 내에서 구현될 수 있다. 프록시(240)는 신뢰성 있는 실행 환경(235) 내부에서만 구동하도록 구성될 수 있다.

[0039] 적어도 일 실시예에서, 프록시(240)는 도 1을 참조하여 설명된 모듈(예를 들면, 수정 모듈(141), 응답 모듈(142), 보호 데이터 저장 모듈(143))과 유사한 모듈로 구성될 수 있다. 특히, 프록시(240)는 프록시(140)가 클라이언트 디바이스(130)와 서버(120) 사이에서 중재자로서 역할을 하는 것과 실질적으로 동일한 방법으로, 클라이언트 디바이스(230)와 서버(220) 사이에서 중재자로서 역할을 수행할 수 있다. 프록시(240)의 모듈은 비공개 데이터를 요청하고, 해당 비공개 데이터에 액세스하려는 승인을 요청하는 수정된 객체를 생성하고, 유효한 승인 정보를 수신하면 서버(220)에게 요청된 비공개 데이터를 제공하는 객체를 가진, 서버(220)로부터 클라이언트 디바이스(230)로 전달되는 도중의 네트워크 흐름을 가로채는 코드를 포함할 수 있다.

[0040] 신뢰성 있는 실행 환경(235)은 프록시(240)의 코드를 클라이언트 디바이스(230) 내부의 보안 환경에서 동작하게 함으로써, 프록시(240) 및 데이터 저장소(245)를 (예를 들면, 멀웨어에 의한) 악의적인 공격으로부터 보호한다. 신뢰성 있는 실행 환경(235)의 적어도 일부 실시예에서, 신뢰성 있는 코드만이 실행된다. 신뢰성 있는 실행 환경(235)은 프록시(240) 및 데이터 저장소(245)를 클라이언트 디바이스(230)의 다른 소프트웨어로부터 효과적으로 격리시킬 수 있다. 그래서, 데이터 저장소(245) 내의 비공개 데이터는 보호되고 보안된 채로 남아 있을 수 있다. 신뢰성 있는 실행 환경의 예는 이것으로 한정되지 않지만, 캘리포니아 싼타 클라라 소재의 인텔® 코포레이션에서 제안된 Intel® vPro™ 기술과, 인텔 코포레이션에 의해 제안된 Intel® Software Guard Extensions ™과, 이동 디바이스 상의 보안 요소 또는 신뢰 구역, 보안 엔클레이브(secure enclave), 자바 환경을 운영하는 스마트 카드 등을 포함한다. 신뢰성 있는 실행 환경(235) 내의 프록시(240)와 같은 보안 프록시는 비공개 데이

터가 보안 프록시를 통해서만 전송되는 것을 보장한다. 결과적으로, 보안 프록시가 네트워크 환경을 제어할 때, 프록시(240)에 의해 서버(220)로 전달된 비공개 데이터는 커널 레벨에서, 슈퍼바이저 레벨에서, 또는 심지어 펌웨어 또는 하드웨어(예를 들면, 루트킷(rootkit) 및 부트킷(bootkit))로부터 동작하는 멀웨어를 비롯한 멀웨어에 액세스될 수 없다.

[0041] 본 명세서에서 기술된 실시예는 여러 장점으로 비공개 데이터의 보호를 제공한다. 첫 째, 프록시(140, 240)는 클라이언트 디바이스의 어느 브라우저도 수정하지 않고 클라이언트 디바이스와 함께 사용하기 위해 구현될 수 있는데, 이것은 종종 비용이 많이 들 수 있다. 다른 통신 프로토콜에 의해 사용되는 소프트웨어에 대한 변경이 또한 회피될 수 있다. 또한, 프록시(140240)의 구현은 마찬가지로 서버 측(예를 들면, 120 또는 220)의 변경을 필요로 하지 않으며 프록시(140240)의 동작은 서버에 완전히 투명하다. 비공개 데이터가 요청될 때 적절한 승인을 제공하기 위해 사용자 행동(예를 들면, 클라이언트 애플리케이션 또는 내장형 제어기 작동)의 간단한 변경이 필요하다. 적어도 일부 실시예에서, 클라이언트 디바이스에 제공되는 수정된 HTML 웹 페이지는 클라이언트 디바이스 상에서 디스플레이될 수 있다. 수정된 HTML 웹 페이지에 포함된 승인 요청은 사용자에게 사용자의 비공개 데이터로의 액세스를 승인하는데 (예를 들면, 사용자가 "로그인 및 비밀번호를 잠금 해제하려면 OTP 번호를 입력하세요"를 볼 수 있는 "로그인(Login):" 및 "비밀번호(Password):" 요청 대신) 무엇이 필요한지에 관한 명령어를 제공할 수 있다. 그 밖에, 승인 요청은 또한 만일 프록시에 의해 수신된 비공개 데이터의 원 요청을 전송하는 서버와 연관된 비공개 데이터 항목이 없으면 데이터 저장소에 채우는 절차에 관련한 명령어를 사용자에게 제공할 수 있다.

[0042] 다른 장점은 인증 크리덴셜 이외에, 모든 형태의 비공개 데이터를 보호하는 융통성을 포함한다. 데이터를 간단히 비공개로 지정하는 것은 데이터 저장소를 비공개 데이터로 채우고, 저장된 비공개 데이터와의 적절한 연계(예를 들면, 서버, 클라이언트 디바이스, 사용자, 클라이언트 애플리케이션, 내장형 제어기에 의해 제공된 서비스)를 생성하고, 저장된 비공개 데이터를 그 형태를 표시하는데 적절한 태그나 서술자와 연계시키는 과정을 포함한다. 필요하면, 프록시는 서버로부터의 네트워크 환경에서 그 형태의 비공개 데이터의 요청을 인식하도록 용이하게 구성될 수 있다.

[0043] 본 명세서에서 개시된 적어도 일부 실시예의 다른 장점은 비밀번호 변경을 위한 주기적인 서버의 요청이 프록시에서 내부적으로 사용자에게 투명하게 처리될 수 있다는 것이다. 프록시는 서버에 의해 제공된 특정 서비스와 연관된 하나 이상의 비공개 데이터 항목에 대응하는 하나 이상의 크리덴셜(예를 들면, 만료된 비밀번호)을 변경하려는 서버로부터의 요청을 식별할 수 있다. 프록시는 만료된 비밀번호의 변경을 시작하고, 사용자가 연루되지 않고 이러한 트랜잭션을 처리하고, 데이터 저장소(145)에다 새로운 크리덴셜을 반영할 수 있다. 이러한 시나리오에서, 사용자는 뇌물, 갈취 또는 고문에 기초한 공격에 대비하여 심지어 부가적인 보안을 제공하는 비밀번호를 알지 않아도 될 것이다.

[0044] 시스템의 구현은 또한 기업 환경이나 다른 다중 사용자 환경에서도 장점을 제공한다. 보안 프록시(예를 들면, 프록시(140))는 주변 디바이스에서 구현될 수 있는데, 이는 엔드포인트(예를 들면, 클라이언트 디바이스(130))가 비공개 데이터를 잃어 버리는 위험성을 줄여준다. 기업에서 시스템의 구현은 지극히 비용 효과적일 수 있고, 기존의 브라우저를 복수의 엔드포인트에 수용할 수 있으며, BYOD(bring-your-own-device) 시나리오를 수용할 수 있다. 시스템을 시작하기 위해, 안전한 저장 보관소(예를 들면, 데이터 저장소(145))는 보안 방법으로 따로 존재될 수 있다. 안전한 저장 보관소에 채우는데 사용되는 데이터 항목은 사용자가 사용하는 모든 클라이언트 디바이스의 각각의 사용자마다 제공될 수 있다. 일단 안전 저장 보관소에 채워지면, 시스템은 식별된 클라이언트 디바이스가 사용될 때 비공개 데이터의 보호를 제공하기 시작할 수 있다. 기업 환경에서, 본 명세서에서 개시된 실시예는 외부 서비스(예를 들면, 122, 222)에 액세스의 중앙집중적이고 투명한 관리를 가능하게 해줄 수 있다. 크리덴셜은 모든 종업인이 즉각적인 액세스를 향유하도록 보이지 않게 공급될 수 있다. 요구된 크리덴셜은 관리자에 의해 사용자에게 완전히 투명하게 생성되어 관리될 수 있다. 액세스를 잠금 해제하기 위해 클라이언트 디바이스/사용자 식별/인증을 위한 임의의 외부 수단(예를 들면, 입장 로그, 도메인 로그인, 동적 호스트 구성 프로토콜(Dynamic Host Configuration Protocol, DHCP)을 통해 IP 어드레스를 할당하기, 생체 인식, 다중 인증 등)이 채용될 수 있다.

[0045] 클라이언트 디바이스(130, 230), 프록시(140) 및 서버(120, 220)와 연관된 내부 구조에 관해, 이들 디바이스는 본 명세서에서 개요 설명된 동작에서 사용되는 명령어, 로직 및/또는 코드를 비롯한 데이터 및 정보를 저장하기 위한 휘발성 및/또는 비휘발성 메모리 요소(예를 들면, 메모리 요소(138, 148, 238)를 포함할 수 있다. 클라이언트 디바이스(130, 230), 프록시(140) 및 서버(120, 220)는 데이터 및 정보를 임의의 적합한 메모리 요소(예를 들면, 데이터 및 정보를 저장할 수 있는 랜덤 액세스 메모리(random access memory, RAM), 판독 전용 메모리

(read-only memory, ROM), 프로그램가능 ROM(programmable ROM, PROM), 소거 가능한 PROM(erasable PROM, EPROM), 전기적 EPROM(electrically EPROM, EEPROM), 디스크 드라이브, 플로피 디스크, 콤팩트 디스크 ROM(compact disk ROM, CD-ROM), 디지털 다기능 디스크(digital versatile disk, DVD), 플래시 메모리, 자기-광 디스크, 주문형 집적회로(application specific integrated circuit, ASIC), 또는 다른 형태의 비휘발성 머신 판독 가능한 매체), 소프트웨어, 하드웨어, 펌웨어 내에서, 또는 적절하다고 생각하는 어디든 특별한 필요성에 따라 임의의 다른 적합한 컴포넌트, 디바이스 요소, 또는 객체 내에서 보존할 수 있다. 본 명세서에서 논의된 임의의 메모리 항목(예를 들면, 메모리 요소(138, 148, 238)는 넓은 용어인 '메모리 요소' 내에 포함되는 것으로 해석되어야 한다. 더욱이, 클라이언트 디바이스(130, 230), 프록시(140), 및 서버(120, 220)에서 사용되고, 저장되고, 추적되고, 전송되고, 또는 수신되는 정보는 이것으로 한정되지 않지만, 이들 모두 임의의 적합한 타임프레임에서 참조될 수 있는 저장소, 데이터베이스, 레지스터, 큐, 테이블 또는 캐시를 비롯한 임의의 저장 구조체에서 제공될 수 있다. 임의의 저장 구조체(예를 들면, 데이터 저장소(145, 245))는 또한 본 명세서에서 사용된 넓은 용어인 '메모리 요소' 내에 포함될 수 있다.

[0046] 예시적인 구현에서, 프록시(140, 240)는 본 명세서에서 개요 설명된 것과 같은 동작을 달성하거나 조성하는 소프트웨어 모듈(예를 들면, 수정 모듈(141), 응답 모듈(142), 보호 데이터 저장 모듈(143))을 포함할 수 있다. 이러한 모듈은 특정 구성 및/또는 프로비저닝 필요성에 기초할 수 있는 임의의 적절한 방식으로 적합하게 조합되거나 분할될 수 있다. 일부 실시예에서, 그러한 동작 중 하나 이상의 동작은 하드웨어 및/또는 펌웨어에 의해 실행될 수 있거나, 이들 요소의 외부에서 구현될 수 있거나, 아니면 의도된 기능성을 달성하는 일부 다른 컴퓨팅 디바이스에 포함될 수 있다. 이들 요소는 또한 본 명세서에서 개요 설명된 동작을 달성하기 위해 다른 컴퓨팅 디바이스와 협동할 수 있는 소프트웨어(또는 왕복 소프트웨어)를 포함할 수 있다.

[0047] 특정한 예시적인 구현예에서, 본 명세서에서 개요 설명된 기능은 비일시적 머신 판독 가능한 저장 매체를 포함할 수 있는 하나 이상의 유형의 매체에서 인코딩된 로직(예를 들면, 하나 이상의 프로세서 또는 다른 유사한 머신 등에 의해 실행되는 ASIC에서 제공된 임베디드 로직, 디지털 신호 프로세서(digital signal processor, DSP) 명령어, 소프트웨어(잠재적으로는 오브젝트 코드 및 소스 코드를 포함함)에 포함된 임베디드 로직)으로 구현될 수 있다. 클라이언트 디바이스(130, 230), 프록시(140), 및 서버(120, 220)는 본 명세서에서 논의된 바와 같은 행위를 수행하는 로직 또는 알고리즘을 실행할 수 있는 하나 이상의 프로세서(예를 들면, 프로세서(139, 149, 239)를 포함할 수 있다. 프로세서는 데이터와 연관된 임의의 형태의 명령어를 실행하여 본 명세서에서 상세히 설명된 동작을 성취할 수 있다. 일 예로, 프로세서는 요소 또는 물품(예를 들면, 데이터)을 하나의 상태 또는 어떤 것에서 다른 상태 또는 어떤 것으로 변환할 수 있다. 다른 예로, 본 명세서에서 개요 설명된 행위는 고정된 로직 또는 프로그래머블 로직(예를 들면, 프로세서에 의해 실행된 소프트웨어/컴퓨터 명령어)으로 구현될 수 있으며 본 명세서에서 식별된 요소는 디지털 로직, 소프트웨어, 코드, 전자 명령어 또는 이들의 임의의 적합한 조합을 포함하는 프로그래머블 프로세서, 프로그래머블 디지털 로직(예를 들면, 필드 프로그래머블 게이트 어레이(field programmable gate array, FPGA), EPROM, EEPROM) 또는 ASIC 중 몇몇 종류일 수 있다. 본 명세서에서 설명된 임의의 잠재적인 처리 요소, 모듈, 및 머신은 넓은 용어인 '프로세서'에 속하는 것으로 해석되어야 한다.

[0048] 도 3을 참조하면, 간략화된 상호작용 다이어그램은 적어도 일 실시예에 따라서, 네트워크 환경(100)의 클라이언트 디바이스(130), 프록시(140), 및 서버(120) 사이에서 일어날 수 있는 가능한 상호작용을 예시한다. 적어도 일부 실시예에서, 프록시(140)의 수정 모듈(141) 및 응답 모듈(142)은 프록시(140)와 연관된 하나 이상의 상호작용 및 행위를 수행할 수 있다. 브라우저(132)는 클라이언트 디바이스(130)와 연관된 하나 이상의 상호작용 및 행위를 수행할 수 있다. 서비스(122)는 객체에게 비공개 데이터의 요청을 제공할 수 있다. 일반적으로, 도 3을 참조하여 도시되고 설명되는 상호작용 및 행위는 또한 프록시(240)가 클라이언트 디바이스(230)의 신뢰성 있는 실행 환경(235)에서 통합되어 있는 실시예를 예시하는 도 2의 네트워크 환경(200)의 상호작용 및 행위에도 적용 가능하다. 도 3의 예는 그저 잠재적인 상호작용의 예일뿐이며 청구범위의 범위를 한정하지는 않는다. 예를 들면, 모듈의 개수는 변할 수 있고, 컴포넌트의 개수는 변할 수 있고, 특정 상호작용은 변할 수 있고, 상호작용의 순서는 변할 수 있다.

[0049] 도 3은 사용자가 클라이언트 디바이스(130)의 브라우저(132)를 사용하여 인터넷을 검색하는 예시적인 시나리오를 도시한다. 이러한 예시적인 시나리오에서, 서버(120)는 웹 서버이며 네트워크 통신에는 HTML 웹 페이지가 연루된다. 또한, 데이터 저장소(145)는 클라이언트 디바이스(130)의 사용자의 비공개 데이터로 이미 채워져 있다고 가정한다.

[0050] 초기에, 클라이언트 디바이스(130)의 브라우저(132)를 통해, 사용자는 액세스할 특정 웹 서버를 (예를 들면, 특

정 도메인 이름, 네트워크 어드레스, URL을 통해) 선택할 수 있다. (302)에서, 클라이언트 디바이스(130)는 하이퍼텍스트 전송 프로토콜(Hypertext Transfer Protocol, HTTP) 요청 메시지와 같은 네트워크 통신 신호를 선택된 웹 서버로 전송한다. 프록시(140)는 네트워크 통신 신호를 가로챈다. 통신 신호는 비공개 데이터를 잠금 해제하려는 승인 요청에 대한 응답이 아니기 때문에, (304)에서 프록시(140)는 이것을 목적지 웹 서버인 서버(120)로 포워딩한다.

[0051] 이러한 예시적인 시나리오에서, 서버(120)는 웹사이트에서 계정을 만들었던 사용자에 의한 자기의 서비스(예를 들면, 서비스(122))로의 액세스를 허용할 뿐이다. (306)에서, 서버(120)는 사용자의 비공개 데이터 항목 요청을 포함하는 HTML 웹 페이지, 예를 들면 서비스와 함께 등록된 계정의 사용자 이름 및 비밀번호를 전송함으로써 클라이언트 디바이스(130)에 응답한다. 만일 HTML 웹 페이지가 브라우저에 의해 디스플레이된다면, 이는 특정 서비스에 필요한 사용자의 이름 및 비밀번호를 입력하라는 명령어로서 사용자에 의해 인식될 수 있는, 예를 들면 "사용자 이름(Username):" 및 "비밀번호(Password):"가 앞에 나오는 두 개의 공백 박스를 포함할 수 있다. HTML 웹 페이지 자체는 또한 HTML 웹 페이지와 연관된 서비스의 식별자를 포함할 수 있는데, 예를 들면 식별자는 금융 기관의 도메인 이름일 수 있다.

[0052] 프록시(140)는 서버(120)로부터 제공된 HTML 웹 페이지의 네트워크 흐름을 가로챈다. 프록시(140)는 HTML 웹 페이지를 평가하고 무슨 비공개 데이터 항목이 요청되었는지를 결정한다. 이후 프록시(140)는 데이터 저장소(145)를 검색하여 클라이언트 디바이스(130)(및/또는 사용자)가 또한 서버(120)의 서비스에도 연관된 사용자 이름 및 비밀번호와 연관되어 있는지를 (예를 들면, 도메인 이름, 웹 페이지의 URL을 통해) 결정한다. 만일 사용자 이름 및 비밀번호가 발견되면, (308)에서, 프록시(140)는 서버(120)에 의해 요청된 비공개 데이터 항목에 액세스하려는 승인 요청을 담은 수정된 HTML 웹 페이지를 생성할 수 있다. (310)에서, 프록시(140)는 승인 요청을 담은 수정된 HTML 웹 페이지를 클라이언트 디바이스(130)에 전송할 수 있다.

[0053] 클라이언트 디바이스(130)의 브라우저(132)는 프록시(140)로부터 수신된 수정된 HTML 웹 페이지를 디스플레이할 수 있다. 웹 페이지는 서버(120)에 의해 요청된 비공개 데이터 항목에 프록시(140)가 액세스하는 것을 승인하고 그 항목을 서버(120)에 제공하라는 명령어를 사용자에게 제공할 수 있다. 일 실시예에서, 사용자는 사용자가 대역외 통신에서 수신하는 일회용 비밀번호를 제공할 것을 지시받을 수 있다. (312)에서, 클라이언트 디바이스(130)는 사용자에 의해 제공된 승인 정보를 담은 응답을 전송할 수 있다. 프록시(140)는 그 응답을 가로채고 승인 정보가 유효한지를 결정한다. 만일 승인 정보가 유효한 것으로 결정되면, 프록시(140)는 데이터 저장소(145)로부터 요청된 비공개 데이터 항목을 취득할 수 있다. (314)에서, 프록시(140)는 비공개 데이터 항목을 서버(120)로부터 제공된 원 HTML 웹 페이지에다 직접 삽입할 수 있다. (316)에서, 프록시(140)는 완성된 HTML 웹 페이지를 서버(120)에 업로딩할 수 있다. 그래서, 서버(120)에 의해 요청된 비공개 데이터를 보호하는 프록시(140)의 동작은 서버(120)에게 투명하다.

[0054] 도 4는 본 명세서에서 설명된 실시예와 연관될 수 있는 동작의 가능한 흐름(400)의 플로우차트이다. 적어도 일부 실시예에서, 하나 이상의 동작 집합은 도 4의 행위에 대응한다. 프록시(140, 240) 또는 그의 일부분은 하나 이상의 동작 집합을 활용할 수 있다. 프록시(140, 240)는 그 동작을 수행하기 위한 프로세서(149239)와 같은 수단을 포함할 수 있다. 실시예에서, 흐름(400)의 적어도 일부 동작은 수정 모듈(예를 들면, 141)에 의해 수행될 수 있으며 흐름(400)의 적어도 일부 다른 동작은 응답 모듈(예를 들면, 142)에 의해 수행될 수 있다. 도 4의 흐름(400)은 데이터 저장소(145, 245)가 하나 이상의 서비스 및 네트워크 에이전트(즉, 사용자, 클라이언트 디바이스, 클라이언트 애플리케이션, 내장형 제어기)와 연관된 비공개 데이터로 채워져 있을 때 네트워크 환경(100200)에서 일어날 수 있다.

[0055] 흐름(400)은 프록시가 클라이언트 디바이스로부터 네트워크 통신 신호(예를 들면, HTTP 요청, FTP 요청 등)를 수신하는 (402)에서 시작할 수 있다. 네트워크 통신 신호는 예를 들면 인터넷상의 특정 서버로 어드레스 지정될 수 있으며, 프록시는 그 통신 신호를 가로챌 수 있다. (404)에서, 프록시는 네트워크 통신신호를 적절한 목적지 서버(예를 들면, 웹 서버, FTP 서버 등)로 포워딩할 수 있다. (406)에서, 프록시는 서버에서 클라이언트 디바이스로 전달되는 네트워크 흐름을 가로챌 수 있다. 서버의 네트워크 흐름은 클라이언트 디바이스에 의해 전송되고 프록시에 의해 포워딩된 네트워크 통신 신호에 대한 응답일 수 있다.

[0056] (408)에서, 프록시는 서버로부터의 네트워크 흐름의 객체 내에서 하나 이상의 비공개 데이터 항목이 요청되었는지를 결정할 수 있다. 이러한 결정은 객체의 실제 내용을 평가함으로써(예를 들면, "사용자 이름:", "비밀번호:", "계정 번호:" 등과 같이 비공개 데이터 설명 앞에 나오는 공백 박스와 같은 비공개 데이터 요청의 표시를 찾아 HTML 웹 페이지를 검색함으로써) 이루어질 수 있다. 만일 응답이 비공개 데이터 요청을 포함하고 있지 않

으면, (409)에서, 프록시는 수정되지 않은 객체를 가진 네트워크 흐름을 클라이언트 디바이스로 포워딩할 수 있고, 흐름(400)은 끝난다.

[0057] 만일 (408)에서 객체가 비공개 데이터 항목의 요청을 포함하고 있으면, (410)에서, 프록시는 대응하는 비공개 데이터 항목이 데이터 저장소에 저장되어 있는지를 결정할 수 있다. 프록시는 요청되는 비공개 데이터의 형태(예를 들면, 사용자 이름, 비밀번호 등) 및 객체와 연관된 서비스의 식별자(예를 들면, 도메인 이름, 서비스의 URL 등)를 결정할 수 있다. 만일 프록시가 여러 사용자의 비공개 데이터를 처리하면, 프록시는 또한 서버로부터의 네트워크 흐름과 연관된 목적지 클라이언트 디바이스의 식별자를 결정할 수 있다. 일부 실시예에서, 프록시는 네트워크 흐름과 연관된 사용자 또는 클라이언트 애플리케이션의 식별자를 결정할 수 있다. 따라서, 프록시는 데이터 저장소를 검색하고, 서비스, 비공개 데이터의 형태, 및 어쩌면 클라이언트 디바이스와의 연계성에 적어도 일부 기초하여 대응하는 비공개 데이터 항목을 식별할 수 있다. 일부 실시예에서, 프록시는 또한 특정 사용자 또는 클라이언트 애플리케이션과의 연계에 기초하여 대응하는 비공개 데이터 항목을 식별할 수 있다.

[0058] 만일 대응하는 비공개 데이터 항목이 아무것도 발견되지 않으면, (412)에서 프록시는 적절한 조치를 취할 수 있다. 프록시는 데이터 저장소를 빠져 있는 비공개 데이터 항목으로 채우라는 절차에 관한 명령어를 사용자에게 제공할 수 있다. 한 가지 가능한 실시예에서, 객체가 클라이언트 디바이스의 사용자에 의해 요청된 HTML 웹 페이지일 때, 프록시는 클라이언트 디바이스의 브라우저에 의해 디스플레이될 HTML 문서를 사용자에게 데이터 저장소를 빠져 있는 비공개 데이터 항목으로 채우라고 안내하는 명령어와 함께 전송할 수 있다. 다른 실시예에서, 프록시는 적절한 오류 메시지를 클라이언트 디바이스로 전송할 수 있다. 다른 실시예에서, 프록시는 객체에 대해 아무런 수정 없이, 간단하게 비공개 데이터 항목의 요청을 비롯한, 응답을 클라이언트 디바이스로 포워딩할 수 있다. 흐름(400)은 (412)에서 표시된 바와 같이 프록시가 조치를 취한 후 끝날 수 있다.

[0059] (410)에서, 만일 대응하는 비공개 데이터 항목이 데이터 저장소에서 발견되면, (414)에서 프록시는 요청된 비공개 데이터 항목에 액세스하려는 승인 요청을 가진 수정된 객체를 생성하고 항목을 서버에 제공할 수 있다. 승인 요청은 임의의 개수의 잠금 해제 메커니즘(예를 들면, 일회용 비밀번호, 생체 인식 승인, 다중 인증 등)으로 구성될 수 있다. 비공개 데이터 항목에 대해 사용되는 특정 잠금 해제 메커니즘은 프록시에 의해 결정될 수 있고 비공개 데이터 항목과 연관된 특정 네트워크 에이전트에 기초할 수 있다. (416)에서, 수정된 객체는 클라이언트 디바이스로 제공될 수 있다. 도 1에서 도시된 바와 같은 구현 예에서, 수정된 객체는 네트워크 흐름으로 클라이언트 디바이스로 전송될 수 있다. 도 2 에서 도시된 바와 같은 구현 예에서, 수정된 객체는 신뢰성 있는 실행 환경에서 클라이언트 디바이스로 (예를 들면, 브라우저를 통해, 클라이언트 애플리케이션을 통해) 전송될 수 있다.

[0060] (418)에서, 프록시는 클라이언트 디바이스로부터 승인 정보(예를 들면, 일회용 비밀번호, 생체 인식 데이터 등)를 포함하는 응답을 수신할 수 있다. 특정 구현예에 따라서, 이러한 승인 정보는 사용자에 의해 또는 클라이언트 디바이스나 클라이언트 애플리케이션(예를 들면, 특정 서비스에 자동 인증하는 클라이언트 디바이스 또는 클라이언트 애플리케이션)에 의해 (예를 들면, 클라이언트 디바이스의 스크린을 통해) 제공될 수 있다. (420)에서, 프록시는 승인 정보를 검증하려 (예를 들면, 일회용 비밀번호가 유효한지를 결정하고, 생체 인식 데이터가 예상된 생체 인식 데이터와 일치하는지를 결정하려) 시도한다. 승인 정보를 검증하는 것은 승인 정보가 유효한지를 결정하는 것을 포함한다. (420)에서 만일 승인 정보가 유효하지 않은 것으로 결정되면, (422)에서 프록시는 오류 메시지를 클라이언트 디바이스로 전송할 수 있으며, 흐름은 일단 새로운 승인 정보를 수신하는 (418)로 되돌아 갈 수 있다. 만일 미리 결정된 횟수로(예를 들면, 1회 이상) 무효의 승인 정보가 수신되면, 프록시는 승인된 사용자(또는 클라이언트 디바이스 또는 클라이언트 애플리케이션)가 해당 비공개 데이터로의 액세스를 승인해달라고 시도하는 것을 보장하는 부가적인 메커니즘을 불러올 수 있다.

[0061] (420)에서 만일 승인 정보가 유효한 것으로 결정되면, (424)에서 프록시는 서버로부터 수신한 원 객체 내에서 하나 이상의 요청된 비공개 데이터 항목에 대응하는 하나 이상의 비공개 데이터 항목을 데이터 저장소로부터 취득할 수 있다. (426)에서, 프록시는 하나 이상의 비공개 데이터 항목을 담은 응답을 서버에게 주려고 준비할 수 있다. 예를 들면, 만일 비공개 데이터 요청이 HTML 웹 페이지를 통해 전송되면, 프록시는 비공개 데이터 항목을 직접 HTML 웹 페이지의 적절한 위치(예를 들면, 데이터 입력 박스)에 삽입할 수 있다. (428)에서, 비공개 데이터 항목을 담은 응답은 서버로 (예를 들면, HTTP POST 형태로서) 전송될 수 있으며, 흐름(400)은 종료된다.

[0062] 도 5는 실시예에 따른 프로세서의 예시도이다. 프로세서(500)는 클라이언트 디바이스(130 및 230)의 프로세서(139 및 239) 및 프록시(140)의 프로세서(149) 중 하나 이상의 프로세서에 관한 하나의 가능한 실시예이다. 프로세서(500)는 코드를 실행하는 마이크로프로세서, 내장형 프로세서, 디지털 신호 프로세서(digital signal

processor, DSP), 네트워크 프로세서, 다중 코어 프로세서, 단일 코어 프로세서, 또는 다른 디바이스와 같은 임의의 형태의 프로세서일 수 있다. 비록 하나의 프로세서(500)만이 도 5에서 예시되어 있지만, 프로세싱 요소는 대안으로 도 5에서 예시된 하나의 프로세서(500)보다 많은 프로세서를 포함할 수 있다. 프로세서(500)는 단일 스레드 코어(single-threaded core)일 수 있거나, 적어도 일부 실시예의 경우 프로세서(500)는 코어 당 하나보다 많은 하드웨어 스레드 콘텍스트(또는 "논리 프로세서")를 포함할 수 있다는 점에서 멀티 스레드일 수 있다.

[0063] 도 5는 또한 실시예에 따라서 프로세서(500)에 연결된 메모리(502)를 예시한다. 메모리(502)는 클라이언트 디바이스 플랫폼(100)의 메모리 요소(114)의 일 실시예이다. 메모리(502)는 본 기술에서 통상의 지식을 가진 자에게 알려졌거나 그렇지 않으면 통상의 지식을 가진 자에게 사용 가능한 (다양한 계층의 메모리 계층구조를 비롯한) 각종의 메모리 중 임의의 메모리일 수 있다. 그러한 메모리 요소는 이것으로 한정되지 않지만, 랜덤 액세스 메모리(random access memory, RAM), 판독 전용 메모리(read only memory, ROM), 필드 프로그래머블 게이트 어레이(field programmable gate array, FPGA)의 로직 블록, 소거 가능한 프로그래머블 판독 전용 메모리(erasable programmable read only memory, EPROM), 및 전기적으로 소거 가능한 프로그래머블 ROM(electrically erasable programmable ROM, EEPROM)을 포함할 수 있다.

[0064] 프로세서(500)에 의해 실행되는 하나 이상의 명령어일 수 있는 코드(504)는 메모리(502)에 저장될 수 있다. 코드(504)는 적절하다고 생각하는 어디에서든 특별한 필요성에 따라 소프트웨어, 하드웨어, 펌웨어나 이들의 임의의 적합한 조합에서 저장될 수 있거나, 또는 임의의 다른 내부나 외부 컴포넌트, 디바이스, 요소 또는 객체에 저장될 수 있는 각종 모듈(예를 들면, 수정 모듈(141), 응답 모듈, 보호 데이터 저장 모듈(143) 등)의 명령어를 포함할 수 있다. 일 예로, 프로세서(500)는 코드(504)에 의해 표시된 명령어들의 프로그램 시퀀스를 추종할 수 있다. 각각의 명령어는 프론트-엔드 로직(506)에 입력되고 하나 이상의 디코더(508)에 의해 처리된다. 디코더는 그의 출력으로서 미리 정의된 포맷으로 된 고정 폭의 마이크로 동작과 같은 마이크로 동작을 발생할 수 있거나 또는 원 코드 명령어를 반영하는 다른 명령어, 마이크로명령어, 또는 제어 신호를 발생할 수 있다. 프론트-엔드 로직(506)은 또한 레지스터 리네임 로직(510) 및 스케줄링 로직(512)을 포함하는데, 이들은 일반적으로 자원을 할당하고 실행을 위한 명령어에 대응하는 동작을 대기 행렬로 대기시킨다.

[0065] 프로세서(500)는 또한 일련의 실행 유닛(516-1 내지 516-M)을 갖는 실행 로직(514)을 포함할 수 있다. 일부 실시예는 특정 기능이나 일련의 기능에 전용되는 복수의 실행 유닛을 포함할 수 있다. 다른 실시예는 특정 기능을 수행할 수 있는 단 하나의 실행 유닛 또는 하나의 실행 유닛을 포함할 수 있다. 실행 로직(514)은 코드 명령어에 의해 명시된 동작을 수행할 수 있다.

[0066] 코드 명령어에 의해 명시된 동작의 실행을 완료한 후, 백-엔드 로직(518)은 코드(504)의 명령어를 퇴거시킬 수 있다. 일 실시예에서, 프로세서(500)는 순서를 벗어나는 명령어의 실행을 허용하지만 명령어의 퇴거를 순서대로 요구한다. 퇴거 로직(520)은 각종의 공지된 형태(예를 들면, 재배열 버퍼 또는 유사한 것)를 취할 수 있다. 이러한 방식으로, 레지스터 리네임 로직(510)에 의해 활용된 디코더, 하드웨어 레지스터 및 테이블에 의해 발생된 그리고 실행 로직(514)에 의해 수정된 임의의 레지스터(도시되지 않음)의 출력의 최소한의 관점에서, 프로세서(500)는 코드(504)의 실행 중에 변환된다.

[0067] 도 5에서는 도시되지 않았지만, 프로세싱 요소는 프로세서(500)를 가진 칩 상에서 다른 요소를 포함할 수 있다. 예를 들면, 프로세싱 요소는 프로세서(500)와 함께 메모리 제어 로직을 포함할 수 있다. 프로세싱 요소는 I/O 제어 로직을 포함할 수 있고/있거나 메모리 제어 로직과 함께 통합된 I/O 제어 로직을 포함할 수 있다. 프로세싱 요소는 또한 하나 이상의 캐시를 포함할 수 있다. 일부 실시예에서, (플래시 메모리 또는 퓨즈와 같은) 비휘발성 메모리는 또한 프로세서(500)를 가진 칩상에 포함될 수 있다. 도 2를 참조하여 도시되고 설명될 실시예에서, 메모리(502)의 부분은 신뢰성 있는 실행 환경(235)을 제공하고 데이터 저장소(245)를 보호하기 위해 암호화될 수 있으며 프록시 코드(240)와 다른 임의의 코드에는 액세스 가능하지 않다. (예를 들면, 디지털로 서명된) 특별히 조작된 코드만이 환경(235) 내부에서 구동하도록 구성될 수 있다.

[0068] 도 6은 실시예에 따라서 포인트-투-포인트(point-to-point, PtP) 구성으로 배열된 컴퓨팅 디바이스의 한 가지 가능한 예이다. 특히, 도 6은 프로세서, 메모리 및 입력/출력 디바이스가 복수의 포인트-투-포인트 인터페이스에 의해 상호 접속된 시스템을 도시한다. 적어도 일 실시예에서, 본 명세서에서 도시되고 설명된 클라이언트 디바이스(130, 230), 프록시(140) 및 서버(120, 220) 중 하나 이상은 예시적인 컴퓨팅 시스템(600)과 동일하거나 유사한 방식으로 구성될 수 있다.

[0069] 프로세서(670 및 680)는 또한 메모리 요소(632 및 634)와 통신하는 통합된 메모리 제어기 로직(memory controller logic, MC)(672 및 682)을 포함할 수 있다. 대안의 실시예에서, 메모리 제어기 로직(672 및 682)은

프로세서(670 및 680)와 분리된 이산적인 로직일 수 있다. 메모리 요소(632 및/또는 634)는 본 명세서에서 개요 설명된 바와 같이 비공개 데이터의 보호와 연관된 동작을 달성하는데 있어서 프로세서(670 및 680)에 의해 사용되는 각종 데이터를 저장할 수 있다.

[0070] 프로세서(670 및 680)는 도 5의 프로세서(500), 도 1의 프로세서(139, 149) 및 도 2의 프로세서(239)를 참조하여 논의된 프로세서와 같은 임의의 형태의 프로세서일 수 있다. 프로세서(670 및 680)는 각기 포인트-투-포인트 인터페이스 회로(678 및 688)를 이용하여 데이터를 포인트-투-포인트(PtP) 인터페이스(650)를 통해 교환할 수 있다. 프로세서(670 및 680)는 각기 포인트-투-포인트 인터페이스 회로(676, 688, 694 및 698)를 이용하여 개개의 포인트-투-포인트 인터페이스(652 및 654)를 통해 데이터를 제어 로직(690)과 교환할 수 있다. 본 명세서에서 도시된 바와 같이, 제어 로직은 프로세싱 요소(670 및 680)와 분리될 수 있다. 그러나, 실시예에서, 제어 로직(690)은 프로세싱 요소(670 및 680)와 동일한 칩 상에서 통합된다. 또한, 제어 로직(690)은 상이하게 더 적거나 더 많이 통합된 회로로 분할될 수 있다. 그 밖에, 제어 로직(690)은 또한 인터페이스 회로(692)를 이용하여, PtP 인터페이스 회로일 수 있는 고성능 그래픽 인터페이스(639)를 통해 고성능 그래픽 회로(638)와 데이터를 교환할 수 있다. 대안의 실시예에서, 도 6에서 예시된 임의의 또는 모든 PtP 링크는 PtP 링크 대신 멀티-드롭 버스로서 구현될 수 있다.

[0071] 제어 로직(690)은 인터페이스 회로(696)를 통해 버스(620)와 통신할 수 있다. 버스(620)는 버스 브릿지(618) 및 I/O 디바이스(616)와 같이 버스를 통해 통신하는 하나 이상의 디바이스를 가질 수 있다. 버스 브릿지(618)는 버스(610)를 통해, 키보드/마우스(612)(또는 터치 스크린, 트랙볼, 조이스틱 등과 같은 다른 입력 디바이스), (컴퓨터 네트워크(660)를 통해 통신할 수 있는 모뎀, 네트워크 인터페이스 디바이스, 또는 다른 형태의 통신 디바이스와 같은) 통신 디바이스(626), 오디오 I/O 디바이스(614), 및/또는 데이터 저장 디바이스(628)와 같은 다른 디바이스와 통신할 수 있다. 데이터 저장 디바이스(628)는 프로세서(670 및/또는 680)에 의해 실행될 수 있는 코드(630)를 저장할 수 있다. 대안의 실시예에서, 버스 아키텍처의 임의의 부분은 하나 이상의 PtP 링크로 구현될 수 있다.

[0072] 도 6에서 도시된 컴퓨터 시스템은 본 명세서에서 논의된 다양한 실시예를 구현하는데 활용될 수 있는 컴퓨팅 시스템의 실시예의 개략적인 예시이다. 도 6에서 도시된 시스템의 각종 컴포넌트는 본 명세서에서 제공된 다양한 실시예에 따라서, 비공개 데이터의 보호를 달성할 수 있는 시스템 온 칩(system-on-a-chip, SoC) 아키텍처에서 조합될 수 있거나 임의의 다른 적합한 구성에서 조합될 수 있다.

[0073] 본 명세서에서 제공된 예와 함께, 명령어는 둘, 셋 또는 그 이상의 컴퓨팅 디바이스와 관련하여 설명될 수 있다는 것을 주목하자. 그러나 이것은 명료하게 하기 위한 목적을 위해 그러한 것이며 단지 예일뿐이다. 특정 사례에서, 제한된 개수의 컴퓨팅 디바이스를 단지 참조함으로써 주어진 일련의 흐름의 하나 이상의 기능성을 설명하는 것이 더 쉬울 수 있다. 더욱이, 비공개 데이터 보호 시스템은 용이하게 확장 가능하고 다수의 컴포넌트 전체에 걸쳐 구현될 수 있을 뿐만 아니라, 더 복잡하고/정교한 배열 및 구성으로 구현될 수 있다. 따라서, 제공된 예들은 다수의 다른 구조에 잠재적으로 적용되는 비공개 데이터 보호 시스템의 광범위한 교시를 나타내거나 그 범위를 제한하는 것이 아니다.

[0074] 도 1-6을 참조하여 설명된 동작은 네트워크 환경(100 및 200)에 의해 또는 네트워크 환경 내에서 실행될 수 있는 가능한 비공개 데이터 보호 행위 중 일부의 행위만을 예시하고 있다는 것을 또한 주목하는 것이 중요하다. 이러한 동작 중 일부 동작은 적절하다고 생각하는 어디에서든 삭제되거나 제거될 수 있고, 또는 이러한 동작은 본 개시의 범위를 벗어나지 않고 상당히 수정되거나 변경될 수 있다. 또한, 이러한 동작의 타이밍은 상당하게 변경될 수 있다. 앞에서의 동작 흐름은 예시와 설명 목적으로 제공되었다. 임의의 적합한 배열, 연대, 구성, 및 타이밍 메커니즘이 본 개시의 가르침을 벗어나지 않고 제공될 수 있다는 점에서 본 명세서에서 설명된 실시예에 의해 상당한 융통성이 제공된다.

[0075] 본 개시가 특정 배열 및 구성을 참조하여 상세하게 설명되었지만, 이러한 예시적인 구성 및 배열은 본 개시의 범위를 벗어나지 않고 상당히 변경될 수 있다. 또한, 네트워크 환경(100 및 200)이 비공개 데이터 보호 행위를 가능하게 하는 특정한 요소 및 동작을 참조하여 예시되었지만, 이러한 요소 및 동작은 비공개 데이터 보호 시스템의 의도된 기능성을 달성하는 임의의 적합한 아키텍처, 프로토콜 및/또는 프로세스로 대체될 수 있다.

[0076] 다른 특징 및 예

[0077] 다음과 같은 예는 본 명세서에 따른 실시예에 관한 것이다. 앞에서 설명된 장치 및 시스템의 모든 선택사양의 특징은 또한 본 명세서에서 설명된 방법 또는 프로세스에 대해 구현될 수 있으며 예에 있는 특정한 사항은 하나

이상의 실시예의 어디에서든 사용될 수 있다.

[0078] 예 1은 비공개 데이터를 보호하기 위한 명령어가 저장된 적어도 하나의 머신 판독 가능한 저장 매체이며, 명령어는 적어도 하나의 프로세서에 의해 실행될 때 적어도 하나의 프로세서로 하여금, 서버에서 클라이언트 디바이스로 전달되는 도중의 네트워크 흐름을 가로채도록 하고, 네트워크 흐름의 객체 내에서 비공개 데이터 항목의 요청을 식별하도록 하고, 데이터 저장소에서 비공개 데이터 항목을 식별하도록 하고, 승인 요청을 포함하는 수정된 객체를 클라이언트 디바이스로 제공하도록 하고, 유효한 승인 정보가 수신될 때 비공개 데이터 항목을 서버로 전송하도록 한다.

[0079] 예 2에서, 예 1의 주제는 선택사양으로 명령어가 적어도 하나의 프로세서에 의해 실행될 때 적어도 하나의 프로세서로 하여금 또한 클라이언트 디바이스로부터 승인 정보를 수신하도록 하고, 승인 정보가 유효한지를 결정하도록 하고, 승인 정보가 유효한 것으로 결정되면 상기 비공개 데이터 항목을 취득하도록 하는 것을 포함할 수 있다.

[0080] 예 3에서, 예 1-2 중 어느 한 예의 주제는 선택사양으로 명령어가 적어도 하나의 프로세서에 의해 실행될 때 적어도 하나의 프로세서로 하여금 또한 비공개 데이터 항목의 잠금 해제 메커니즘을 결정하도록 하고, 잠금 해제 메커니즘에 적어도 일부 기초하여, 승인 요청을 포함하는 수정된 객체를 생성하도록 하는 것을 포함할 수 있다.

[0081] 예 4에서, 예 3의 주제는 선택사양으로 잠금 해제 메커니즘이 일회용 비밀번호, 사용자의 생체 인식 식별, 및 다중요소 인증 프로세스(multi-factor authentication process)를 포함하는 일군의 잠금 해제 메커니즘 중에서 선택되는 것을 포함할 수 있다.

[0082] 예 5에서, 예 1-4 중 어느 한 예의 주제는 선택사양으로 명령어가 적어도 하나의 프로세서에 의해 실행될 때 상기 적어도 하나의 프로세서로 하여금 또한 비공개 데이터 항목의 요청에 의해 표시된 데이터의 형태를 결정하도록 하는 것을 포함할 수 있으며, 데이터 저장소 내 상기 비공개 데이터 항목은 상기 데이터의 형태 및 상기 서버에 의해 제공된 서비스와 연관된다.

[0083] 예 6에서, 예 1-5 중 어느 한 예의 주제는 선택사양으로 상기 데이터 저장소 내 상기 비공개 데이터 항목이 클라이언트 디바이스, 클라이언트 디바이스의 사용자, 및 상기 클라이언트 디바이스에서 실행하는 클라이언트 애플리케이션 중 적어도 하나와 연관되는 것을 포함할 수 있다.

[0084] 예 7에서, 예 1-6 중 어느 한 예의 주제는 선택사양으로 상기 비공개 데이터 항목이 비밀번호인 것을 포함할 수 있다.

[0085] 예 8에서, 예 1-7 중 어느 한 예의 주제는 선택사양으로 상기 승인 정보가 유효하지 않을 때 상기 비공개 데이터 항목이 상기 서버에 제공되지 않는 것을 포함할 수 있다.

[0086] 예 9에서, 예 1-8 중 어느 한 예의 주제는 선택사양으로 객체가 하이퍼텍스트 마크업 언어(HyperText Markup Language, HTML) 웹 페이지인 것을 포함할 수 있다.

[0087] 예 10에서, 예 9의 주제는 선택사양으로 명령어가 적어도 하나의 프로세서에 의해 실행될 때 적어도 하나의 프로세서로 하여금 또한 상기 데이터 저장소로부터 상기 비공개 데이터 항목을 취득하도록 하고, 유효한 승인 정보가 수신될 때 비공개 데이터 항목을 상기 HTML 웹 페이지 내에 삽입함으로써 HTML 웹 페이지를 완성하도록 하고, 완성된 HTML 웹 페이지에 기초하여 상기 서버로 응답을 전송하도록 하는 것을 포함할 수 있다.

[0088] 예 11에서, 예 1-10 중 어느 한 예의 주제는 선택사양으로 상기 데이터 저장소가 하나 이상의 비공개 데이터 항목의 복수 집합을 포함하는 것을 포함할 수 있으며, 복수의 집합은 각기 복수의 서비스와 연관된다.

[0089] 예 12에서, 예 1-10 중 어느 한 예의 주제는 선택사양으로 프록시가 복수의 데이터 집합을 포함하는 것을 포함할 수 있으며, 데이터의 복수의 집합의 각각은 적어도 하나의 네트워크 에이전트와 연관되고, 각각의 데이터 집합은 적어도 하나의 비공개 데이터 항목의 하나 이상의 집합을 포함하며, 복수의 데이터 집합 중 적어도 하나의 비공개 데이터 항목의 하나 이상의 집합은 복수의 서비스와 각기 연관된다.

[0090] 예 13에서, 예 1-12 중 어느 한 예의 주제는 선택사양으로 클라이언트 디바이스가 사용자로 하여금 브라우저를 통해 상기 서버에 액세스할 수 있도록 구성된 컴퓨팅 디바이스와, 상기 서버에 의해 제공된 서비스에 자동 인증하도록 구성된 클라이언트 애플리케이션을 포함하는 컴퓨팅 디바이스와, 상기 서버에 의해 제공된 상기 서비스에 자동 인증하도록 구성된 내장형 제어기를 포함하는 일군의 클라이언트 디바이스 중에서 선택되는 것을 포함할 수 있다.

[0091] 예 14에서, 예 1-13 중 어느 한 예의 주제는 선택사양으로 상기 명령어가 상기 적어도 하나의 프로세서에 의해 실행될 때 상기 적어도 하나의 프로세서로 하여금 또한 상기 서버에서 상기 클라이언트 디바이스로 전달되는 도중의 다른 네트워크 흐름을 가로채도록 하고, 서버에 의해 제공된 특정 서비스와 연관된 하나 이상의 특정 비공개 데이터 항목에 대응하는 하나 이상의 크리덴셜을 변경하려는 요청을 식별하도록 하고, 네트워크 흐름을 상기 클라이언트 디바이스로 포워딩하지 않고 하나 이상의 새로운 크리덴셜을 선택하도록 하고, 데이터 저장소 내 상기 하나 이상의 특정 비공개 데이터 항목을 상기 하나 이상의 새로운 크리덴셜로 갱신하도록 하는 것을 포함할 수 있다.

[0092] 예 15에서, 예 1-14 중 어느 한 예의 주제는 선택사양으로 명령어가 클라이언트 디바이스 상의 신뢰성 있는 실행 환경에서 실행하도록 구성되는 것을 포함할 수 있다.

[0093] 예 16에서, 예 1-14 중 어느 한 예의 주제는 선택사양으로 상기 적어도 하나의 머신 판독 가능한 저장 매체가 상기 클라이언트 디바이스와 분리된 프록시에서 구현되는 것을 포함할 수 있다.

[0094] 예 17은 데이터를 보호하는 장치이며, 이 장치는, 적어도 하나의 메모리 요소와, 적어도 하나의 메모리 요소에 연결된 적어도 하나의 프로세서와, 적어도 하나의 프로세서에 의해 실행될 때, 네트워크 흐름이 서버에서 클라이언트 디바이스로 전달되는 도중일 때 장치에 의해 가로채인 상기 네트워크 흐름의 객체 내에서 비공개 데이터 항목의 요청을 식별하도록 하고, 데이터 저장소에서 상기 비공개 데이터 항목을 식별하도록 하고, 승인 요청을 포함하는 수정된 객체를 상기 클라이언트 디바이스로 제공하도록 구성된 수정 모듈과, 적어도 하나의 프로세서에 의해 실행될 때 유효한 승인 정보가 수신되면 상기 비공개 데이터 항목을 상기 서버로 전송하도록 구성된 응답 모듈을 포함한다.

[0095] 예 18에서, 예 17의 주제는 선택사양으로 상기 응답 모듈이 또한 클라이언트 디바이스로부터 승인 정보를 수신하고, 승인 정보가 유효한지를 결정하고, 승인 정보가 유효한 것으로 결정되면 상기 비공개 데이터 항목을 취득하도록 구성되는 것을 포함할 수 있다.

[0096] 예 19에서, 예 17-18 중 어느 한 예의 주제는 선택사양으로 상기 수정 모듈이 또한 비공개 데이터 항목의 잠금 해제 메커니즘을 결정하고, 상기 잠금 해제 메커니즘에 적어도 일부 기초하여, 상기 승인 요청을 포함하는 상기 수정된 객체를 생성하도록 구성되는 것을 포함할 수 있다.

[0097] 예 20에서, 예 19의 주제는 선택사양으로 상기 잠금 메커니즘이 또한 일회용 비밀번호, 사용자의 생체 인식 식별, 및 다중요소 인증 프로세스를 포함하는 일군의 잠금 해제 메커니즘 중에서 선택되는 것을 포함할 수 있다.

[0098] 예 21에서, 예 17-20 중 어느 한 예의 주제는 선택사양으로 인증 모듈이 또한 비공개 데이터 항목의 요청에 의해 표시된 데이터의 형태를 결정하도록 구성되는 것을 포함할 수 있으며, 데이터 저장소 내 상기 비공개 데이터 항목은 상기 데이터의 형태 및 상기 서버에 의해 제공된 서비스와 연관된다.

[0099] 예 22에서, 예 17-21 중 어느 한 예의 주제는 선택사양으로 상기 데이터 저장소 내 상기 비공개 데이터 항목이 클라이언트 디바이스, 클라이언트 디바이스의 사용자, 및 상기 클라이언트 디바이스에서 실행하는 클라이언트 애플리케이션 중 적어도 하나와 연관되는 것을 포함할 수 있다.

[0100] 예 23에서, 예 17-22 중 어느 한 예의 주제는 선택사양으로 상기 비공개 데이터 항목이 비밀번호인 것을 포함할 수 있다.

[0101] 예 24에서, 예 17-23 중 어느 한 예의 주제는 선택사양으로 상기 승인 정보가 유효하지 않을 때 상기 비공개 데이터 항목이 상기 서버에 제공되지 않는 것을 포함할 수 있다.

[0102] 예 25에서, 예 17-24 중 어느 한 예의 주제는 선택사양으로 객체가 하이퍼텍스트 마크업 언어(HyperText Markup Language, HTML) 웹 페이지인 것을 포함할 수 있다.

[0103] 예 26에서, 예 25의 주제는 선택사양으로 응답 모듈이 또한 유효한 승인 정보가 수신될 때 상기 데이터 저장소로부터 상기 비공개 데이터 항목을 취득하고, 유효한 승인 정보가 수신될 때 비공개 데이터 항목을 상기 HTML 웹 페이지 내에 삽입함으로써 HTML 웹 페이지를 완성하고, 완성된 HTML 웹 페이지에 기초하여 상기 서버로 응답을 전송하도록 구성되는 것을 포함할 수 있다.

[0104] 예 27에서, 예 17-26 중 어느 한 예의 주제는 선택사양으로 상기 데이터 저장소가 하나 이상의 비공개 데이터 항목의 복수 집합을 포함하는 것을 포함할 수 있으며, 복수의 집합은 각기 복수의 서비스와 연관된다.

[0105] 예 28에서, 예 17-26 중 어느 한 예의 주제는 선택사양으로 프록시가 복수의 데이터 집합을 포함하는 것을 포함

할 수 있으며, 데이터의 복수의 집합의 각각은 적어도 하나의 네트워크 에이전트와 연관되고, 각각의 데이터 집합은 적어도 하나의 비공개 데이터 항목의 하나 이상의 집합을 포함하며, 복수의 데이터 집합 중 적어도 하나의 비공개 데이터 항목의 하나 이상의 집합은 복수의 서비스와 각기 연관된다.

[0106] 예 29에서, 예 17-28 중 어느 한 예의 주제는 선택사양으로 클라이언트 디바이스가 사용자로 하여금 브라우저를 통해 상기 서버에 액세스할 수 있도록 구성된 컴퓨팅 디바이스와, 상기 서버에 의해 제공된 서비스에 자동 인증하도록 구성된 클라이언트 애플리케이션을 포함하는 컴퓨팅 디바이스와, 상기 서버에 의해 제공된 상기 서비스에 자동 인증하도록 구성된 내장형 제어기를 포함하는 일군의 클라이언트 디바이스 중에서 선택되는 것을 포함할 수 있다.

[0107] 예 30에서, 예 17-29 중 어느 한 예의 주제는 선택사양으로 수정 모듈이 또한 상기 서버에서 상기 클라이언트 디바이스로 전달되는 도중의 다른 네트워크 흐름을 가로채고, 서버에 의해 제공된 특정 서비스와 연관된 하나 이상의 특정 비공개 데이터 항목에 대응하는 하나 이상의 크리덴셜을 변경하려는 요청을 식별하고, 네트워크 흐름을 상기 클라이언트 디바이스로 포워딩하지 않고 하나 이상의 새로운 크리덴셜을 선택하고, 데이터 저장소 내 하나 이상의 특정 비공개 데이터 항목을 상기 하나 이상의 새로운 크리덴셜로 갱신하도록 구성되는 것을 포함할 수 있다.

[0108] 예 31에서, 예 17-30 중 어느 한 예의 주제는 선택사양으로 장치가 클라이언트 디바이스를 포함하는 것을 포함할 수 있으며, 클라이언트 디바이스는 신뢰성 있는 실행 환경을 포함하고, 수정 모듈 및 응답 모듈은 신뢰성 있는 실행 환경에서만 실행된다.

[0109] 예 32에서, 예 17-30 중 어느 한 예의 주제는 선택사양으로 장치가 클라이언트 디바이스와 분리된 프록시인 것을 포함할 수 있다.

[0110] 예 33은 비공개 데이터를 보호하는 방법으로, 이 방법은 프록시에 의해, 서버에서 클라이언트 디바이스로 전달되는 도중의 네트워크 흐름을 가로채는 단계와, 네트워크 흐름의 객체 내에서 비공개 데이터 항목의 요청을 식별하는 단계와, 데이터 저장소에서 상기 비공개 데이터 항목을 식별하는 단계와, 승인 요청을 포함하는 수정된 객체를 상기 클라이언트 디바이스로 제공하는 단계와, 유효한 승인 정보가 수신될 때 상기 비공개 데이터 항목을 상기 서버로 전송하는 단계를 포함한다.

[0111] 예 34에서, 예 33의 주제는 선택사양으로 클라이언트 디바이스로부터 승인 정보를 수신하는 단계와, 승인 정보가 유효한지를 결정하는 단계와, 승인 정보가 유효한 것으로 결정되면 비공개 데이터 항목을 취득하는 단계를 포함할 수 있다.

[0112] 예 35에서, 예 33-34 중 어느 한 예의 주제는 선택사양으로 비공개 데이터 항목의 잠금 해제 메커니즘을 결정하는 단계와, 잠금 해제 메커니즘에 적어도 일부 기초하여, 승인 요청을 포함하는 수정된 객체를 생성하는 단계를 포함할 수 있다.

[0113] 예 36에서, 예 35의 주제는 선택사양으로 잠금 해제 메커니즘이 일회용 비밀번호, 사용자의 생체 인식 식별, 및 다중요소 인증 프로세스를 포함하는 일군의 잠금 해제 메커니즘 중에서 선택되는 것을 포함할 수 있다.

[0114] 예 37에서, 예 33-36 중 어느 한 예의 주제는 선택사양으로 비공개 데이터 항목의 요청에 의해 표시된 데이터의 형태를 결정하는 단계를 포함할 수 있으며, 데이터 저장소 내 상기 비공개 데이터 항목은 상기 데이터의 형태 및 상기 서버에 의해 제공된 서비스와 연관된다.

[0115] 예 38에서, 예 33-37 중 어느 한 예의 주제는 선택사양으로 데이터 저장소 내 상기 비공개 데이터 항목이 클라이언트 디바이스, 클라이언트 디바이스의 사용자, 및 상기 클라이언트 디바이스에서 실행하는 클라이언트 애플리케이션 중 적어도 하나와 연관되는 것을 포함할 수 있다.

[0116] 예 39에서, 예 33-38 중 어느 한 예의 주제는 선택사양으로 상기 비공개 데이터 항목이 비밀번호인 것을 포함할 수 있다.

[0117] 예 40에서, 예 33-39 중 어느 한 예의 주제는 선택사양으로 상기 승인 정보가 유효하지 않을 때 비공개 데이터 항목이 상기 서버에 제공되지 않는 것을 포함할 수 있다.

[0118] 예 41에서, 예 33-40 중 어느 한 예의 주제는 선택사양으로 객체가 하이퍼텍스트 마크업 언어(HTML) 웹 페이지인 것을 포함할 수 있다.

[0119] 예 42에서, 예 41의 주제는 선택사양으로 유효한 승인 정보가 수신될 때 데이터 저장소로부터 상기 비공개 데이

터 항목을 취득하는 단계와, 유효한 승인 정보가 수신될 때 비공개 데이터 항목을 HTML 웹 페이지 내에 삽입함으로써 HTML 웹 페이지를 완성하는 단계와, 완성된 HTML 웹 페이지에 기초하여 상기 서버로 응답을 전송하는 단계를 포함할 수 있다.

[0120] 예 43에서, 예 33-42 중 어느 한 예의 주제는 선택사양으로 상기 데이터 저장소가 하나 이상의 비공개 데이터 항목의 복수 집합을 포함하는 것을 포함할 수 있으며, 복수의 집합은 각기 복수의 서비스와 연관된다.

[0121] 예 44에서, 예 33-42 중 어느 한 예의 주제는 선택사양으로 프록시가 복수의 데이터 집합을 포함하는 것을 포함할 수 있으며, 데이터의 복수의 집합의 각각은 적어도 하나의 네트워크 에이전트와 연관되고, 각각의 데이터 집합은 적어도 하나의 비공개 데이터 항목의 하나 이상의 집합을 포함하며, 복수의 데이터 집합 중 적어도 하나의 비공개 데이터 항목의 하나 이상의 집합은 복수의 서비스와 각기 연관된다.

[0122] 예 45에서, 예 33-44 중 어느 한 예의 주제는 선택사양으로 클라이언트 디바이스가 사용자로 하여금 브라우저를 통해 상기 서버에 액세스할 수 있도록 구성된 컴퓨팅 디바이스와, 상기 서버에 의해 제공된 서비스에 자동 인증하도록 구성된 클라이언트 애플리케이션을 포함하는 컴퓨팅 디바이스와, 상기 서버에 의해 제공된 상기 서비스에 자동 인증하도록 구성된 내장형 제어기를 포함하는 일군의 클라이언트 디바이스 중에서 선택되는 것을 포함할 수 있다.

[0123] 예 46에서, 예 33-45 중 어느 한 예의 주제는 선택사양으로 서버에서 상기 클라이언트 디바이스로 전달되는 도중의 다른 네트워크 흐름을 가로채는 단계와, 서버에 의해 제공된 특정 서비스와 연관된 하나 이상의 특정 비공개 데이터 항목에 대응하는 하나 이상의 크리덴셜을 변경하려는 요청을 식별하는 단계와, 네트워크 흐름을 상기 클라이언트 디바이스로 포워딩하지 않고 하나 이상의 새로운 크리덴셜을 선택하는 단계와, 데이터 저장소 내 상기 하나 이상의 특정 비공개 데이터 항목을 상기 하나 이상의 새로운 크리덴셜로 갱신하는 단계를 포함할 수 있다.

[0124] 예 47에서, 예 33-46 중 어느 한 예의 주제는 선택사양으로 비공개 데이터 항목의 요청을 식별하는 단계와, 데이터 저장소 내에서 비공개 데이터 항목을 식별하는 단계와, 클라이언트 디바이스 상의 신뢰성 있는 실행 환경에서 수행되는 수정된 객체를 클라이언트 디바이스로 제공하는 단계를 포함할 수 있다.

[0125] 예 48에서, 예 33-46 중 어느 한 예의 주제는 선택사양으로 프록시가 클라이언트 디바이스와 분리되어 있는 것을 포함할 수 있다.

[0126] 예 49는 비공개 데이터를 보호하는 장치이며, 이 장치는 예 33-48 중 어느 한 예의 방법을 수행하기 위한 수단을 포함한다.

[0127] 예 50에서, 예 49의 주제는 선택사양으로 방법을 수행하기 위한 적어도 하나의 프로세서와 적어도 하나의 메모리 요소를 포함하는 수단을 포함할 수 있다.

[0128] 예 51에서, 예 50의 주제는 선택사양으로 실행될 때 장치로 하여금 예 33-48 중 어느 한 예의 방법을 수행하도록 하는 머신 판독 가능한 명령어를 포함하는 적어도 하나의 메모리 요소를 포함할 수 있다.

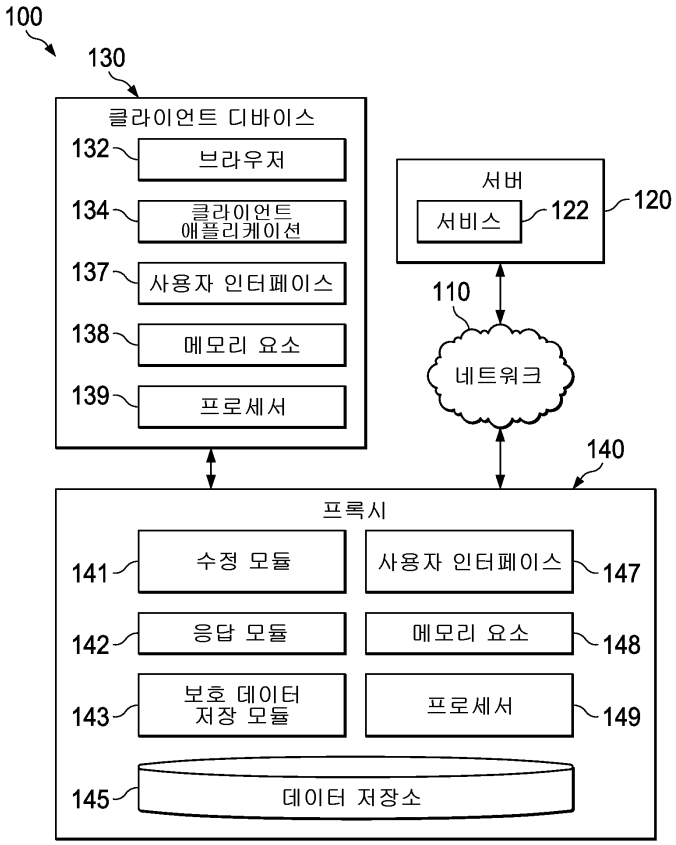
[0129] 예 52에서, 예 49-51 중 어느 하나의 주제는 선택사양으로 장치가 컴퓨팅 디바이스인 것을 포함할 수 있다.

[0130] 예 53은 명령어가 실행될 때 예 17-48 중 어느 한 예에서 인용된 바와 같은 방법을 구현하거나 장치를 실현하는 비공개 데이터를 보호하기 위한 명령어를 포함하는 적어도 하나의 머신 판독 가능한 저장 매체이다.

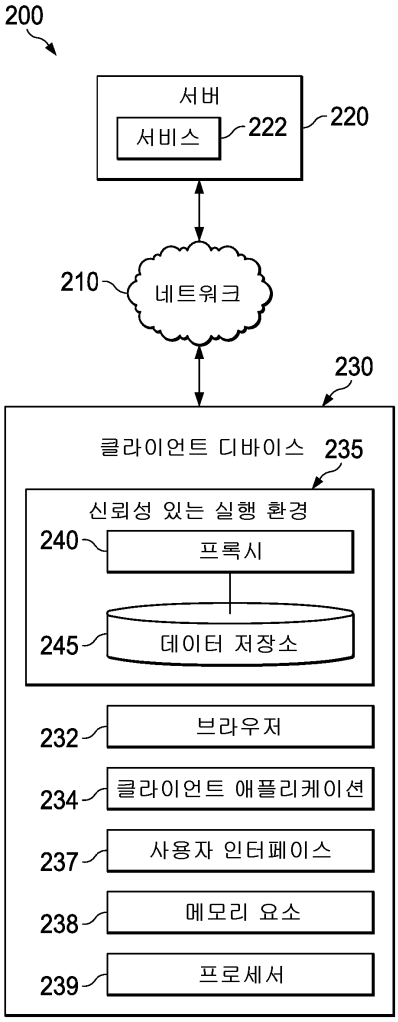
[0131] 예 54는 데이터를 보호하기 위한 장치이며, 이 장치는 프록시에 의해, 서버에서 클라이언트 디바이스로 전달되는 도중의 네트워크 흐름을 가로채는 수단과, 네트워크 흐름의 객체 내에서 비공개 데이터 항목의 요청을 식별하는 수단과, 데이터 저장소에서 비공개 데이터 항목을 식별하는 수단과, 승인 요청을 포함하는 수정된 객체를 클라이언트 디바이스로 제공하는 수단과, 유효한 승인 정보가 수신될 때 비공개 데이터 항목을 상기 서버로 전송하는 수단을 포함할 수 있다.

도면

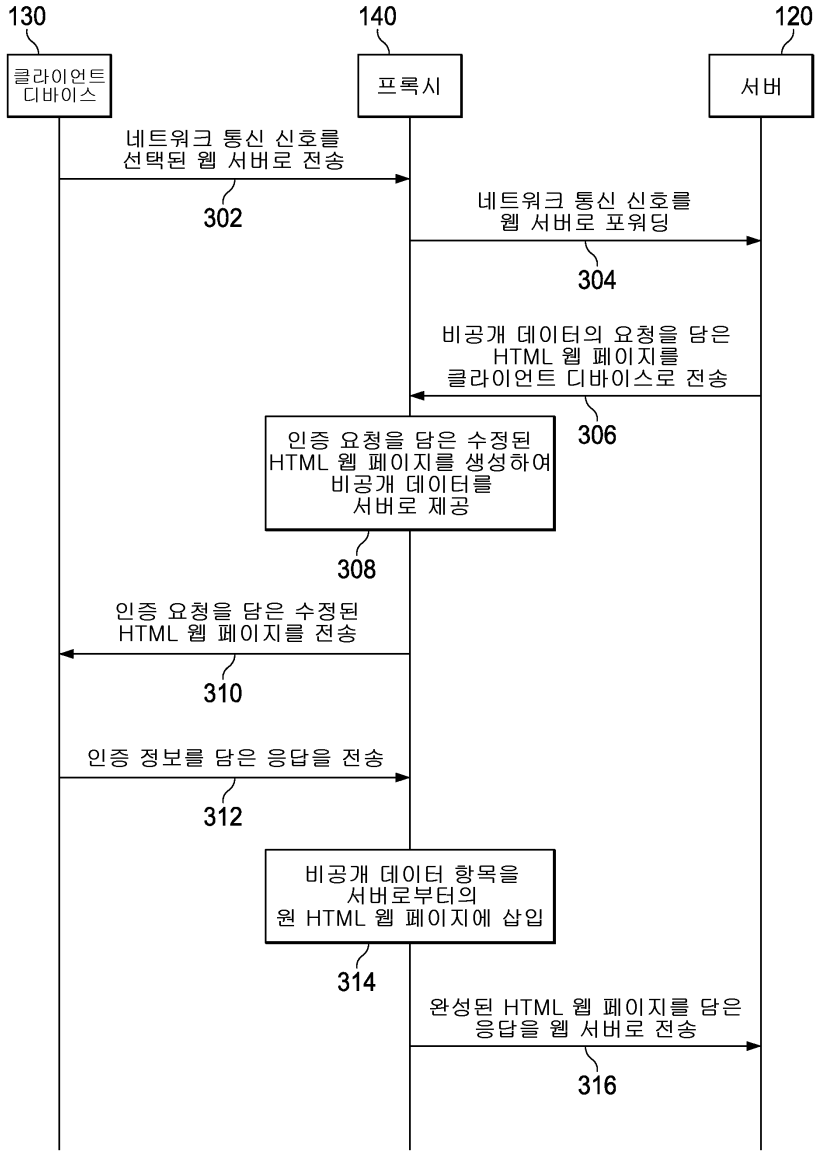
도면1


100
130
클라이언트 디바이스
132
브라우저
134
클라이언트
애플리케이션
137
사용자 인터페이스
138
메모리 요소
139
프로세서
서버
서비스
122
120
110
네트워크
140
프록시
141
수정 모듈
사용자 인터페이스
147
142
응답 모듈
메모리 요소
148
143
보호 데이터
저장 모듈
프로세서
149
145
데이터 저장소

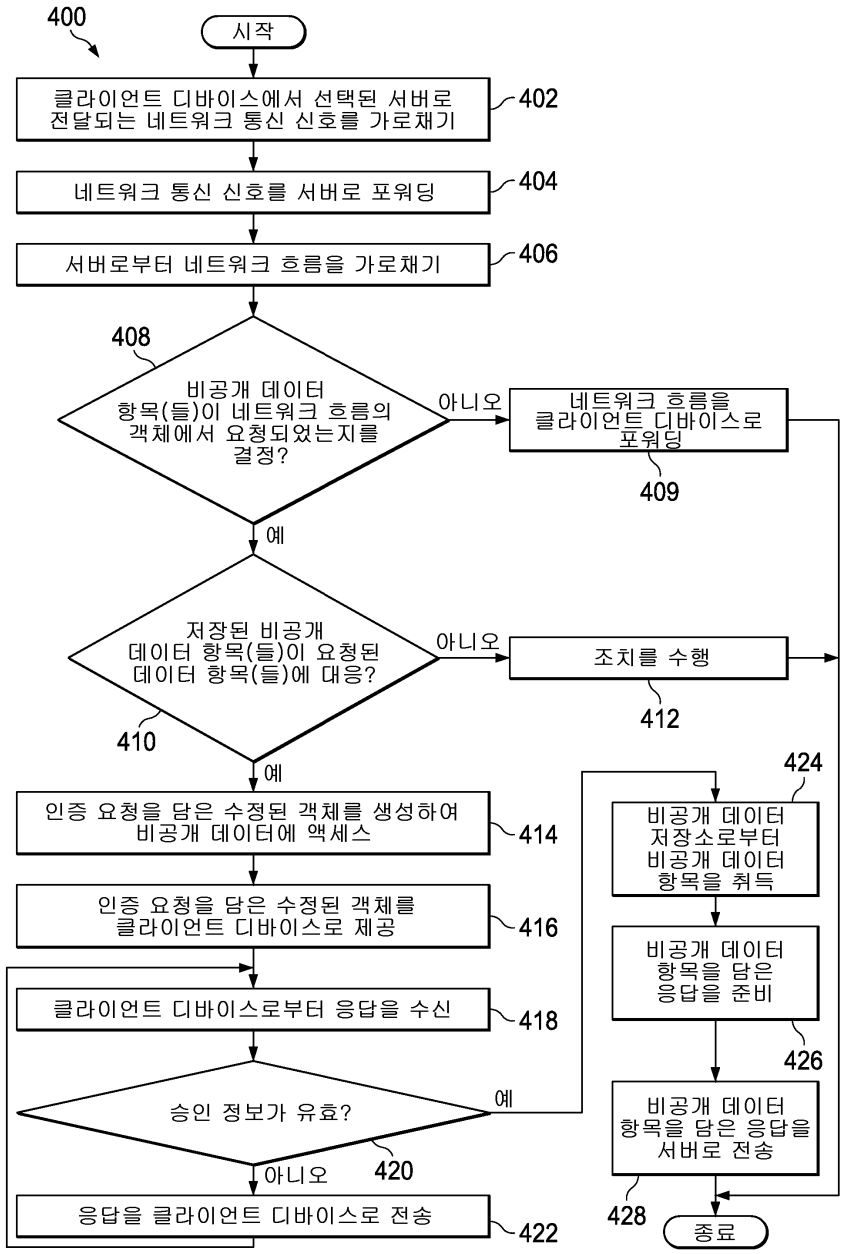
도면2


200
서버
서비스
222
220
210
네트워크
230
클라이언트 디바이스
235
신뢰성 있는 실행 환경
240
프록시
245
데이터 저장소
232
브라우저
234
클라이언트 애플리케이션
237
사용자 인터페이스
238
메모리 요소
239
프로세서

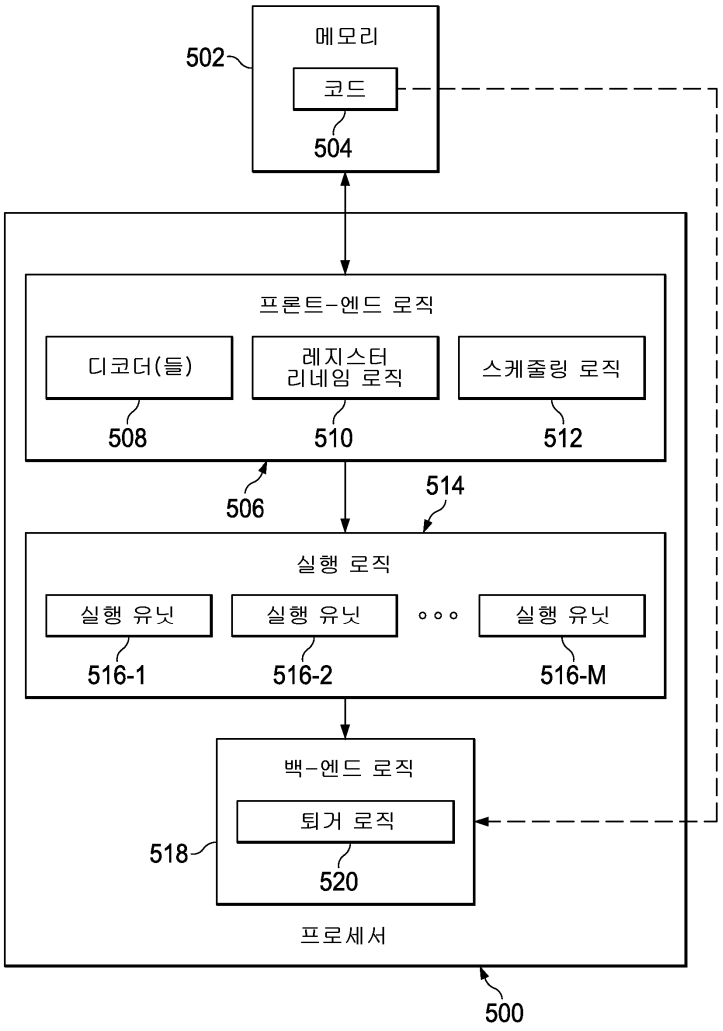
도면3


130
140
120
클라이언트 디바이스
프록시
서버
네트워크 통신 신호를 선택된 웹 서버로 전송
302
네트워크 통신 신호를 웹 서버로 포워딩
304
비공개 데이터의 요청을 담은 HTML 웹 페이지를 클라이언트 디바이스로 전송
306
인증 요청을 담은 수정된 HTML 웹 페이지를 생성하여 비공개 데이터를 서버로 제공
308
인증 요청을 담은 수정된 HTML 웹 페이지를 전송
310
인증 정보를 담은 응답을 전송
312
비공개 데이터 항목을 서버로부터의 원 HTML 웹 페이지에 삽입
314
완성된 HTML 웹 페이지를 담은 응답을 웹 서버로 전송
316

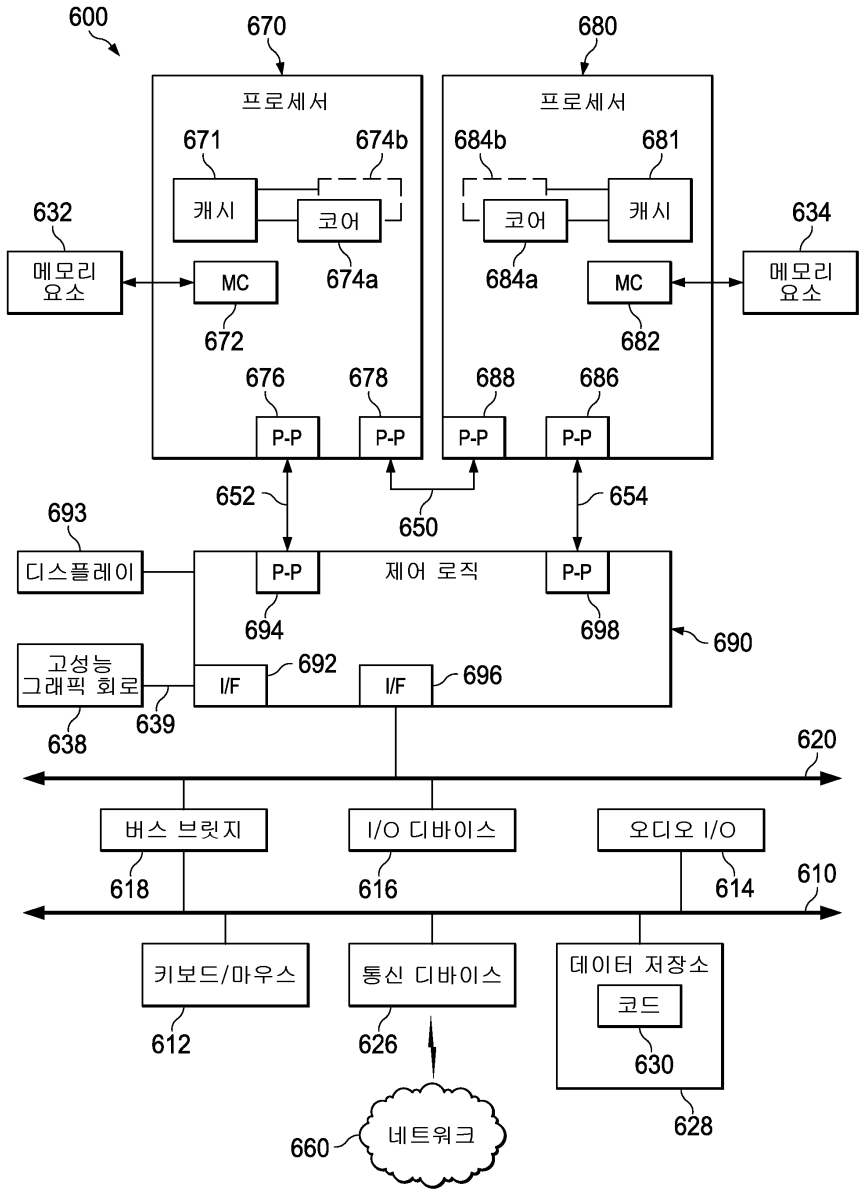
도면4


400
시작
클라이언트 디바이스에서 선택된 서버로 전달되는 네트워크 통신 신호를 가로채기
402
네트워크 통신 신호를 서버로 포워딩
404
서버로부터 네트워크 흐름을 가로채기
406
408
비공개 데이터 항목(들)이 네트워크 흐름의 객체에서 요청되었는지를 결정?
아니오
네트워크 흐름을 클라이언트 디바이스로 포워딩
409
예
저장된 비공개 데이터 항목(들)이 요청된 데이터 항목(들)에 대응?
아니오
조치를 수행
412
410
예
인증 요청을 담은 수정된 객체를 생성하여 비공개 데이터에 액세스
414
인증 요청을 담은 수정된 객체를 클라이언트 디바이스로 제공
416
클라이언트 디바이스로부터 응답을 수신
418
승인 정보가 유효?
예
420
아니오
응답을 클라이언트 디바이스로 전송
422
424
비공개 데이터 저장소로부터 비공개 데이터 항목을 취득
비공개 데이터 항목을 담은 응답을 준비
426
비공개 데이터 항목을 담은 응답을 서버로 전송
428
종료

도면5


메모리
502
코드
504
프론트-엔드 로직
디코더(들)
레지스터 리네임 로직
스케줄링 로직
508
510
512
506
514
실행 로직
실행 유닛
실행 유닛
실행 유닛
516-1
516-2
516-M
백-엔드 로직
퇴거 로직
518
520
프로세서
500

도면6


600
670
680
프로세서
프로세서
671
674b
684b
681
캐시
코어
코어
캐시
632
634
메모리 요소
MC
674a
684a
MC
메모리 요소
672
682
676
678
688
686
P-P
P-P
P-P
P-P
652
650
654
693
디스플레이
P-P
제어 로직
P-P
694
698
690
고성능 그래픽 회로
I/F
692
I/F
696
639
638
620
버스 브릿지
I/O 디바이스
오디오 I/O
618
616
614
610
키보드/마우스
통신 디바이스
데이터 저장소
코드
612
626
630
628
660
네트워크