(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년09월10일
(11) 등록번호 10-2301407
(24) 등록일자 2021년09월07일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *G06F 21/55* (2013.01)
G06F 21/86 (2013.01) *H04L 12/26* (2006.01)
H04L 29/08 (2006.01) *H04W 12/00* (2021.01)
H04W 4/70 (2018.01) *H04W 68/12* (2009.01)
(52) CPC특허분류
H04L 63/20 (2013.01)
G06F 21/55 (2013.01)
(21) 출원번호 10-2019-7012815
(22) 출원일자(국제) 2017년10월30일
심사청구일자 2020년10월05일
(85) 번역문제출일자 2019년05월02일
(65) 공개번호 10-2019-0073409
(43) 공개일자 2019년06월26일
(86) 국제출원번호 PCT/US2017/058926
(87) 국제공개번호 WO 2018/085166
국제공개일자 2018년05월11일
(30) 우선권주장
15/344,461 2016년11월04일 미국(US)
(56) 선행기술조사문헌
US20160212099 A1
US20150163121 A1
US09478132 B1

(73) 특허권자
마이크로소프트 테크놀로지 라이센싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
사무엘 아즈맨드
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 마이크로소프트 테크놀로지 라이센싱, 엘엘씨
(74) 대리인
제일특허법인(유)

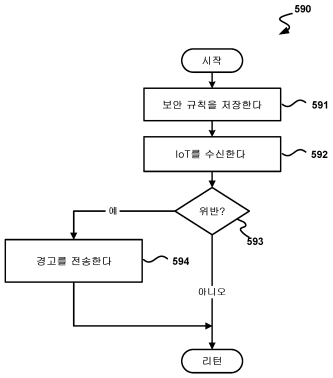
전체 청구항 수 : 총 20 항 심사관 : 홍기완

(54) 발명의 명칭 **IOT 보안 서비스**

(57) 요 약

본 개시된 기술은 일반적으로 IoT 환경에서의 디바이스 보안에 관한 것이다. 예를 들어, 그러한 기술은 IoT 보안에서 사용 가능하다. 이 기술의 일 예에서, 적어도 하나의 IoT 디바이스의 예상된 조건과 관련된 보안 규칙들의 세트가 저장된다. 적어도 하나의 IoT 디바이스와 관련된 IoT 데이터가 수신된다. IoT 데이터는 적어도 두 개의 상이한 타입의 데이터를 포함하는 집계 데이터일 수 있다. IoT 데이터에 기초하여, 보안 규칙들의 세트가 위반되었는지의 여부에 대한 결정이 행해진다. 경고는 이러한 결정에 기초하여 선택적으로 전송된다.

대 표 도 - 도5



(52) CPC특허분류
G06F 21/86 (2013.01)
H04L 43/08 (2013.01)
H04L 63/14 (2013.01)
H04L 63/1425 (2013.01)
H04L 67/12 (2013.01)
H04W 12/65 (2021.01)
H04W 4/70 (2018.02)
H04W 68/12 (2013.01)
G06F 2221/2111 (2013.01)

명 세 서

청구범위

청구항 1

사물 인터넷(Internet of Things)(IoT) 보안을 위한 장치로서,

하나 이상의 디바이스를 포함한 IoT 허브를 포함하되,

상기 디바이스는 상기 디바이스를 위한 런타임 데이터를 저장하도록 구성된 적어도 하나의 메모리와, 프로세서 실행 가능 코드를 실행하도록 구성된 적어도 하나의 프로세서를 포함하며,

상기 프로세서 실행 가능 코드는 실행에 응답하여 상기 IoT 허브로 하여금 아래의 액션을 수행하게 하며, 상기 액션은,

적어도 하나의 IoT 디바이스의 예상된 조건과 관련된 보안 규칙들의 세트를 저장하는 것 - 상기 보안 규칙들의 세트는 복수의 IoT 디바이스의 각각으로부터 수신된 운영 정보(operating information)에 기초함 - 과,

상기 적어도 하나의 IoT 디바이스와 관련된 IoT 데이터를 수신하는 것 - 상기 IoT 데이터는 적어도 두 개의 상이한 타입의 데이터를 포함하는 집계 데이터(aggregated data)임 - 과,

상기 IoT 데이터에 기초하여, 상기 적어도 하나의 IoT 디바이스의 각각의 IoT 디바이스에 대해, 상기 복수의 IoT 디바이스의 각각으로부터 수신된 운영 정보에 기초하여 상기 IoT 디바이스에 대한 상기 보안 규칙들의 세트가 위반되었는지의 여부에 대한 결정을 행하는 것 - 상기 결정은 함께 고려되는 상기 복수의 IoT 디바이스 중 적어도 두 개로부터의 적어도 두 개의 상이한 타입의 데이터의 결합에 기초함 - 과,

상기 결정에 기초하여 경고를 선택적으로 전송하는 것을 포함하는

장치.

청구항 2

제 1 항에 있어서,

상기 액션은,

구성 요청을 수신하는 것과,

상기 구성 요청에 기초하여 상기 보안 규칙들의 세트를 조정하는 것을 더 포함하는

장치.

청구항 3

제 1 항에 있어서,

상기 IoT 데이터는 상기 적어도 하나의 IoT 디바이스 상에 배치된 데이터 수집 에이전트로부터 수신되는

장치.

청구항 4

제 1 항에 있어서,

상기 적어도 하나의 IoT 디바이스는 복수의 IoT 디바이스를 포함하고, 상기 IoT 데이터는 상기 복수의 IoT 디바

이스 상에 배치된 데이터 수집 에이전트로부터 수신되는

장치.

청구항 5

제 1 항에 있어서,

상기 보안 규칙들의 세트는 화이트리스트의 프로세스 또는 블랙리스트의 프로세스 중 적어도 하나를 포함하는

장치.

청구항 6

제 1 항에 있어서,

상기 IoT 데이터는 상기 적어도 하나의 IoT 디바이스 상의 변조 스위치(tampering switch)의 상태를 포함하는

장치.

청구항 7

제 1 항에 있어서,

상기 IoT 데이터는 상기 적어도 하나의 IoT 디바이스를 포함하는 다수의 IoT 디바이스로부터 집계되는

장치.

청구항 8

제 1 항에 있어서,

상기 IoT 데이터의 집계 데이터는 환경 데이터 및 내부 상태 데이터를 포함하는

장치.

청구항 9

제 8 항에 있어서,

상기 환경 데이터는 온도, 습도, 감지된 위치, 또는 위치 정보(geolocation) 중 적어도 하나를 포함하는

장치.

청구항 10

제 8 항에 있어서,

상기 내부 상태 데이터는 운영 체제 버전, 활성 프로세스의 현재 상태, 개방 포트, 또는 상기 적어도 하나의 IoT 디바이스에 접속된 디바이스들과 관련된 정보 중 적어도 하나를 포함하는

장치.

청구항 11

제 1 항에 있어서,

상기 보안 규칙들의 세트는 상기 보안 규칙들의 세트의 위반이 적어도 공격의 가능성을 나타내도록 구성되며, 상기 공격은 상기 적어도 하나의 IoT 디바이스에 대한 물리적 공격 또는 사이버 공격 중 적어도 하나인

장치.

청구항 12

제 11 항에 있어서,

상기 결정에 기초하여 경고를 선택적으로 전송하는 것은, 상기 경고와 함께 상기 공격에 관한 정보를 선택적으로 전송하는 것을 더 포함하는

장치.

청구항 13

사물 인터넷(IoT) 보안을 위한 방법으로서,

복수의 IoT 디바이스의 각각으로부터 수신된 운영 정보에 기초하여, 구성 가능한 IoT 디바이스 모델을 생성하는 단계와,

적어도 하나의 IoT 디바이스로부터 집계된 IoT 디바이스 데이터를 수신하는 단계 - 상기 집계된 IoT 디바이스 데이터는 상기 복수의 IoT 디바이스로부터의 적어도 두 개의 상이한 타입의 데이터를 포함함 - 와,

상기 집계된 IoT 디바이스 데이터를 상기 구성 가능한 IoT 디바이스 모델과 비교하기 위해 적어도 하나의 프로세서를 이용하는 단계 - 상기 비교는 함께 고려되는 상기 복수의 IoT 디바이스 중 적어도 두 개로부터의 적어도 두 개의 상이한 타입의 데이터의 결합에 기초하여 판정됨(adjudicated) - 와,

상기 비교에 기초하여 경고를 선택적으로 전송하는 단계를 포함하는

방법.

청구항 14

제 13 항에 있어서,

상기 적어도 하나의 IoT 디바이스는 복수의 IoT 디바이스를 포함하고, 상기 집계된 IoT 디바이스 데이터는 상기 복수의 IoT 디바이스 상에 배치된 데이터 수집 에이전트로부터 수신되는

방법.

청구항 15

제 13 항에 있어서,

상기 집계된 IoT 디바이스 데이터는 환경 데이터 및 내부 상태 데이터를 포함하는

방법.

청구항 16

제 13 항에 있어서,

구성 요청을 수신하는 단계와,

상기 구성 요청에 기초하여 상기 구성 가능한 IoT 디바이스 모델을 조정하는 단계를 더 포함하는

방법.

청구항 17

사물 인터넷(IoT) 보안을 위한 방법으로서,

구성 요청을 생성하기 위해 적어도 하나의 프로세서를 이용하는 단계 - 상기 구성 요청은 보안 규칙들의 세트를 조정된 보안 규칙들의 세트로 변경하기 위한 요청이며, 상기 조정된 보안 규칙들의 세트는 적어도 하나의 IoT 디바이스의 예상된 조건과 관련되며, 상기 조정된 보안 규칙들의 세트는 복수의 IoT 디바이스의 각각과 관련된 IoT 데이터의 평가에 기초하고, 상기 IoT 데이터는 상기 복수의 IoT 디바이스로부터의 적어도 두 개의 상이한 타입의 데이터를 포함하는 집계 데이터이고, 상기 조정된 보안 규칙들의 세트는 함께 고려되는 상기 복수의 IoT 디바이스 중 적어도 두 개로부터의 적어도 두 개의 상이한 타입의 데이터의 결합에 기초하여 적용됨 - 와,

상기 구성 요청을 IoT 허브에 전송하는 단계와,

상기 IoT 허브가 상기 조정된 보안 규칙들의 세트가 위반되었다는 결정을 행할 때 상기 IoT 허브로부터 경고를 수신하는 단계를 포함하는

방법.

청구항 18

제 17 항에 있어서,

상기 조정된 보안 규칙들의 세트는 상기 적어도 하나의 IoT 디바이스와 관련된 IoT 데이터의 평가에 기초하고, 상기 적어도 하나의 IoT 디바이스는 복수의 IoT 디바이스인

방법.

청구항 19

제 17 항에 있어서,

상기 IoT 데이터의 집계 데이터는 환경 데이터 및 내부 데이터를 포함하는

방법.

청구항 20

제 19 항에 있어서,

상기 환경 데이터는 온도, 습도, 감지된 위치, 또는 위치 정보 중 적어도 하나를 포함하고, 상기 내부 데이터는 운영 체제 버전, 활성 프로세스의 현재 상태, 개방 포트, 또는 상기 적어도 하나의 IoT 디바이스에 접속된 디바이스들과 관련된 정보 중 적어도 하나를 포함하는

방법.

발명의 설명

기 술 분 야

배 경 기 술

[0001] 사물 인터넷(Internet of Things)("IoT")은 일반적으로 네트워크를 통해 통신할 수 있는 디바이스들의 시스템을 지칭한다. 이들 디바이스는 토스터, 커피 머신, 온도 조절 시스템, 세탁기, 건조기, 램프, 자동차, 및 기타 등과 같은 일상적인 물체를 포함할 수 있다. 네트워크 통신은 디바이스 자동화, 데이터 캡처, 경고 제공, 설정 개인화 및 다양한 다른 용도에 사용될 수 있다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0002] 본 개요는 개념의 선택을 단순화된 형태로 소개하기 위해 제공되며, 그 개념은 아래의 상세한 설명에서 추가로 설명된다. 이 개요는 청구된 발명의 요지의 핵심 특징 또는 필수 특징을 식별하기 위한 것도 아니고 청구된 발명의 요지의 범위를 제한하도록 사용되는 것도 아니다.

[0003] 간단히 말해서, 본 개시된 기술은 일반적으로 IoT 환경에서의 디바이스 보안에 관한 것이다. 예를 들어, 그러한 기술은 IoT 보안에서 사용 가능하다. 이 기술의 일 예에서, 적어도 하나의 IoT 디바이스의 예상된 조건과 관련된 보안 규칙들의 세트가 저장된다. 적어도 하나의 IoT 디바이스와 관련된 IoT 데이터가 수신된다. IoT 데이터는 적어도 두 개의 상이한 타입의 데이터를 포함하는 집계 데이터(aggregated data)일 수 있다. IoT 데이터에 기초하여 보안 규칙들의 세트가 위반되었는지의 여부에 대한 결정이 행해진다. 경고는 이러한 결정에 기초하여 선택적으로 전송된다.

[0004] 본 개시 내용의 일부 예는 IoT 디바이스 보안 상태에 관한 원격 측정(telemetry)을 사용하고 그리고 다른 IoT 디바이스로부터의 다른 환경 데이터를 사용하여 IoT 디바이스에 대한 보안 위협을 모니터링, 검출 및 완화하는 시스템을 포함한다. 일부 예에서, 이러한 환경 내의 다수의 IoT 디바이스로부터의 원격 측정 데이터가 사용되고, 그 환경의 모델이 형성된다. 일부 예에서, 결과적인 모델은 침입(intrusions) 및 변조(tampering)와 같은 보안 위협을 검출하는 데 사용된다.

[0005] 본 개시된 기술의 다른 양태 및 응용은 첨부된 도면 및 설명을 읽고 파악하게 되면 이해될 것이다.

도면의 간단한 설명

[0006] 본 개시 내용의 비 제한적 및 비 절대적인 예가 다음의 도면을 참조하여 설명된다. 도면에서, 달리 명시되지 않는 한, 유사한 참조 번호는 다양한 도면들 전반에 걸쳐 유사한 부분을 나타낸다. 이들 도면은 반드시 축척대로 도시되는 것은 아니다.

본 개시 내용의 더 나은 이해를 위해, 첨부된 도면과 관련하여 읽혀질 다음의 상세한 설명이 참조될 것이다:

도 1은 본 기술의 양태가 이용될 수 있는 적절한 환경의 일 예를 나타내는 블록도이다.

도 2는 본 개시된 기술의 양태에 따른 적절한 컴퓨팅 디바이스의 일 예를 나타내는 블록도이다.

도 3은 IOT 보안을 위한 시스템의 일 예를 나타내는 블록도이다.

도 4는 IoT 보안을 위한 프로세스의 일 예시적인 데이터 흐름을 나타내는 도면이다.

도 5는 본 개시 내용의 양태에 따라, IoT 보안을 위한 프로세스의 일 예를 나타내는 논리 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0007] 아래의 설명은 본 기술의 다양한 예를 완전하게 이해하고 그에 대한 설명을 가능하게 하기 위한 특정 세부 사항을 제공한다. 본 기술 분야의 통상의 기술자는 이러한 기술이 많은 세부 사항 없이도 실시될 수 있음을 이해할 것이다. 경우에 따라, 잘 알려진 구조 및 기능은 본 기술의 예의 설명을 불필요하게 모호하게 하는 것을 피하기 위해 상세하게 표시하거나 설명하지 않았다. 본 개시 내용에 사용된 용어는 본 기술의 특정 예에 대한 상세한 설명과 함께 사용되더라도 가장 광범위하게 합리적인 방식으로 해석되어야 한다는 것이다. 아래에서 특정 용어가 강조될 수 있지만, 임의의 제한된 방식으로 해석되도록 의도된 임의의 용어는 이 상세한 설명 섹션에서와 같이 명백하고 구체적으로 정의될 것이다. 본 명세서 및 청구범위 전체에서, 다음의 용어들은 문맥이 달리

지시하지 않는 한, 본원에서 명백히 관련된 의미를 적어도 갖는다. 아래에 명시된 의미는 용어를 반드시 제한하는 것이 아니고, 그 용어에 대한 예시적인 예만을 제공할 뿐이다. 예를 들어, "기초하는(based on)" 및 "기반하는(based upon)"이라는 용어는 모두 배타적인 것이 아니고, "적어도 부분적으로 기초하는"이란 용어와 동등하며, 추가 요인에 기초하는 옵션을 포함하며, 그 요인의 일부는 여기에 기술되지 않을 수 있다. 다른 예로서, "통해(via)"라는 용어는 배타적인 것이 아니며, "적어도 부분적으로 통해"라는 용어와 동일하며, 추가 요인을 통하는 옵션을 포함하며, 그 요인의 일부는 여기에 기술되지 않을 수 있다. "내(in)"의 의미는 "내(in)" 및 "상(on)"을 포함한다. 본원에서 사용되는 "일 실시예에서" 또는 "일 예에서"라는 문구는 반드시 동일한 실시예 또는 예를 지칭하지는 않지만, 그러한 것을 지칭할 수도 있다. 특정 텍스트 숫자 지정자의 사용은 값이 보다 작은 숫자 지정자의 존재를 의미하는 것은 아니다. 예를 들어, "제 3의 foo와 제 4의 bar로 구성된 그룹에서 선택된 위젯"이라고 열거하는 것 그 자체로 적어도 3 개의 foo가 있다는 것을 의미하는 것도 아니고, 적어도 4 개의 bar 요소가 있다는 것을 의미하는 것도 아닐 것이다. 단수 형태의 참조물은 단지 판독의 명확성을 위해 이루어진 것이며 복수의 참조물이 구체적으로 배제되지 않는 한 복수의 참조물을 포함한다. "또는"이라는 용어는 달리 명시하지 않는 한 포괄적인 "또는" 연산자이다. 예를 들어, "A 또는 B"는 "A, B 또는 A 및 B"를 의미한다. 본원에 사용되는 바와 같이, "컴포넌트" 및 "시스템"이라는 용어는 하드웨어, 소프트웨어, 또는 하드웨어 및 소프트웨어의 다양한 조합을 포함하도록 의도된다. 따라서, 예를 들어, 시스템 또는 컴포넌트는 프로세스, 컴퓨팅 디바이스 상에서 실행중인 프로세스, 컴퓨팅 디바이스, 또는 그 일부일 수 있다. "IoT 허브"라는 용어는 하나의 특정 타입의 IoT 서비스에 한정되지 않고, IoT 디바이스가 프로비저닝 후에, 적어도 하나의 IoT 솔루션 또는 임의의 타입의 IoT 서비스를 위해 통신하는 디바이스를 지칭한다. 즉, 본 명세서 및 청구범위 전반에 걸쳐 사용되는 "IoT 허브"라는 용어는 모든 IoT 솔루션에 대한 일반적인 용어이다.

[0008] 간단히 말해서, 본 개시된 기술은 일반적으로 IoT 환경에서의 디바이스 보안에 관한 것이다. 예를 들어, 그러한 기술은 IoT 보안에서 사용 가능하다. 이 기술의 일 예에서, 적어도 하나의 IoT 디바이스의 예상된 조건과 관련된 보안 규칙들의 세트가 저장된다. 적어도 하나의 IoT 디바이스와 관련된 IoT 데이터가 수신된다. IoT 데이터는 적어도 두 개의 상이한 타입의 데이터를 포함하는 집계 데이터일 수 있다. IoT 데이터에 기초하여 보안 규칙들의 세트가 위반되었는지의 여부에 대한 결정이 행해진다. 경고는 이러한 결정에 기초하여 선택적으로 전송된다.

[0009] 일부 애플리케이션에서, IoT 디바이스는 잠재적으로 불리한 환경에서 원격으로 배치되는 경향이 있다. 이러한 디바이스는 종종 디바이스의 운영자 또는 소유자가 물리적으로 액세스할 수 있는 것이 아닐 수 있다. 이러한 디바이스는 또한 물리적인 모니터링, 물리적인 감시, 또는 물리적인 보안 없이 방치되어 공중에게 물리적으로 이용가능하게 되는 "통제 불능(wild) 상태"에 있을 수 있으므로, 사람들은 그 디바이스를 물리적으로 조작할 수 있다. 누군가가 멀웨어를 그러한 디바이스에 전송하거나 그러한 디바이스로부터 인증서를 도용하는 등이 가능할 수 있다. 본 개시 내용의 예는 디바이스의 보안을 감시하고, 디바이스에 대한 침입 및/또는 위협을 검출하고, 및/또는 그러한 침입 및/또는 위협을 원격 당사자에게, 가령, 그러한 침입 및/또는 위협을 완화시킬 수도 있는 시스템 또는 운영자에게 통신한다.

[0010] 본 개시 내용의 일부 예는 IoT 디바이스 보안 상태에 관한 원격 측정 정보를 사용하고, 원격 측정 데이터를 사용하고, 그리고 다른 IoT 디바이스로부터의 다른 환경 데이터를 사용하여, IoT 디바이스에 대한 보안 위협을 모니터링, 검출 및 완화하는 시스템을 포함한다. 일부 예에서, 데이터 수집 에이전트는 IoT 디바이스들 상에 배치되고, 그러한 IoT 디바이스들에 의해 생성된 센서 데이터는 IoT 디바이스에 대한 보안 위협을 모델링하고 검출하는 데 사용된다. 이러한 데이터 수집 에이전트는 구성 데이터를 사용하여 원격으로 구성될 수 있다.

[0011] 일부 예에서, 다양한 IoT 디바이스 상의 다수의 에이전트는 다양한 타입의 데이터를 수집하는 데 사용될 수 있고, 그 후, 이 데이터는 디바이스 운영(device operation) 및 침입에 대한 보다 총체적인 모델을 형성하는 데 결합적으로 사용될 수 있다. 일부 예에서, IoT 디바이스 자체로부터의 에이전트 데이터는 IoT 디바이스의 보안 상태를 보고하는 데 사용된다. 일부 예에서, 디바이스들의 집단으로부터의 에이전트 데이터는 운영 환경의 모델을 형성하는 데 사용된다. 일부 예에서, 이러한 환경 내의 다수의 IoT 디바이스로부터의 원격 측정 데이터가 사용되고 그 환경의 모델이 형성된다.

[0012] 일부 예에서, 결과적인 모델은 침입 및 변조와 같은 보안 위협을 검출하는 데 사용된다.

[0013] 예시적인 디바이스/운영 환경

[0014] 도 1은 본 기술의 양태가 실시될 수 있는 환경(100)을 도면이다. 도시된 바와 같이, 환경(100)은 네트워크(130)를 통해 접속된 네트워크 노드(120)뿐만 아니라 컴퓨팅 디바이스(110)를 포함한다. 환경(100)의 특정 컴

포넌트가 도 1에 도시되어 있지만, 다른 예에서, 환경(100)은 또한 추가적 및/또는 상이한 컴포넌트르 포함할 수 있다. 예를 들어, 특정 예에서, 환경(100)은 또한 네트워크 저장 디바이스, 유지 보수 관리자, 및/또는 다른 적절한 컴포넌트(도시되지 않음)를 포함할 수 있다. 도 1에 도시된 컴퓨팅 디바이스(110)는 온 프레미스(on premise), 클라우드(cloud) 내에서, 또는 기타 등을 포함하는 다양한 위치에 있을 수 있다. 예를 들어, 컴퓨팅 디바이스(110)는 클라이언트 측, 서버 측, 또는 기타 등에 있을 수 있다.

[0015] 도 1에 도시된 바와 같이, 네트워크(130)는 다수의 컴퓨팅 디바이스(110)를 상호 접속하고 컴퓨팅 디바이스(110)를 외부 네트워크(140)에, 예를 들어, 인터넷 또는 인트라넷에 접속시키는 하나 이상의 네트워크 노드(120)를 포함할 수 있다. 예를 들어, 네트워크 노드(120)는 스위치, 라우터, 허브, 네트워크 컨트롤러, 또는 다른 네트워크 요소를 포함할 수 있다. 특정 예에서, 컴퓨팅 디바이스(110)는 랙(racks), 액션 존(action zones), 그룹, 세트, 또는 다른 적절한 분할로 조직화될 수 있다. 예를 들어, 도시된 예에서, 컴퓨팅 디바이스(110)는 제 1, 제 2, 및 제 3 호스트 세트(112a 내지 112c)로 개별적으로 식별되는 3 개의 호스트 세트로 그룹화된다. 도시된 예에서, 각각의 호스트 세트(112a 내지 112c)는 일반적으로 "탑 오브 랙(top-of-rack)", 즉 "TOR" 네트워크 노드로 지칭되는 해당 네트워크 노드(120a 내지 120c)에 각각 동작 가능하게 결합된다. 그 후, TOR 네트워크 노드(120a 내지 120c)는 추가 네트워크 노드(120)에 동작 가능하게 결합되어, 컴퓨팅 디바이스(110)와 외부 네트워크(140) 간의 통신을 가능하게 하는 계층적, 플랫, 메시, 또는 다른 적절한 타입의 토폴로지로 컴퓨터 네트워크를 형성할 수 있다. 다른 예에서, 다수의 호스트 세트들(112a 내지 112c)은 단일 네트워크 노드(120)를 공유할 수 있다. 컴퓨팅 디바이스(110)는 사실상 임의의 타입의 범용 또는 특수 목적 컴퓨팅 디바이스일 수 있다. 예를 들어, 이러한 컴퓨팅 디바이스는 사용자 디바이스, 가령, 데스크탑 컴퓨터, 랩탑 컴퓨터, 태블릿 컴퓨터, 디스플레이 디바이스, 카메라, 프린터, 또는 스마트폰일 수 있다. 그러나, 데이터 센터 환경에서, 이러한 컴퓨팅 디바이스는 서버 디바이스, 가령, 애플리케이션 서버 컴퓨터, 가상 컴퓨팅 호스트 컴퓨터, 또는 파일 서버 컴퓨터일 수 있다. 또한, 컴퓨팅 디바이스(110)는 개별적으로 구성되어, 컴퓨팅, 저장, 및/또는 다른 적절한 컴퓨팅 서비스를 제공할 수 있다.

[0016] 일부 예에서, 하나 이상의 컴퓨팅 디바이스(110)는 IoT 디바이스, 게이트웨이 디바이스, IoT 허브의 일부 또는 전부를 포함하는 디바이스, 디바이스 포털 서비스의 일부 또는 전부를 포함하는 디바이스, 또는 기타 등으로서, 이는 아래에서 보다 상세히 설명된다.

[0017] 예시적인 컴퓨팅 디바이스

[0018] 도 2은 본 기술의 양태가 실시될 수 있는 컴퓨팅 디바이스(200)의 일 예를 나타내는 도면이다. 컴퓨팅 디바이스(200)는 사실상 임의의 타입의 범용 또는 특수 목적 컴퓨팅 디바이스일 수 있다. 예를 들어, 컴퓨팅 디바이스(200)는 사용자 디바이스, 가령, 데스크탑 컴퓨터, 랩탑 컴퓨터, 태블릿 컴퓨터, 디스플레이 디바이스, 카메라, 프린터, 또는 스마트폰일 수 있다. 마찬가지로, 컴퓨팅 디바이스(200)는 또한 서버 디바이스, 가령, 애플리케이션 서버 컴퓨터, 가상 컴퓨팅 호스트 컴퓨터, 또는 파일 서버 컴퓨터일 수 있으며, 예를 들어, 컴퓨팅 디바이스(200)는 도 1의 컴퓨팅 디바이스(110) 또는 네트워크 노드(120)의 일 예일 수 있다. 컴퓨팅 디바이스(200)는 또한 IoT 서비스를 수신하기 위해 네트워크에 접속되는 IoT 디바이스일 수도 있다. 마찬가지로, 컴퓨팅 디바이스(200)는 도 3 내지 도 5에 도시되거나 도 3 내지 도 5에서 참조되는 디바이스들 중의 임의의 일 예일 수 있으며, 이는 아래에서 보다 상세하게 설명된다. 도 2에 도시된 바와 같이, 컴퓨팅 디바이스(200)는 프로세싱 회로(210), 운영 메모리(220), 메모리 컨트롤러(230), 데이터 저장 메모리(250), 입력 인터페이스(260), 출력 인터페이스(270), 및 네트워크 어댑터(280)를 포함한다. 컴퓨팅 디바이스(200)의 이들 각각의 앞서 리스트된 컴포넌트는 적어도 하나의 하드웨어 요소를 포함한다.

[0019] 컴퓨팅 디바이스(200)는 명령어, 가령, 본원에 설명된 작업 부하, 프로세스, 또는 기술을 구현하기 위한 명령어를 실행하도록 구성된 적어도 하나의 프로세싱 회로(210)를 포함한다. 프로세싱 회로(210)는 마이크로프로세서, 마이크로컨트롤러, 그래픽 프로세서, 코프로세서, 필드 프로그래머블 게이트 어레이, 프로그래머블 로직 디바이스, 신호 프로세서, 또는 데이터를 프로세싱하기에 적합한 임의의 다른 회로를 포함할 수 있다. 전술한 명령어는 다른 데이터(예를 들어, 데이터 세트, 메타 데이터, 운영 체제 명령어 등)와 함께 컴퓨팅 디바이스(200)의 런타임 동안 운영 메모리(220)에 저장될 수 있다. 운영 메모리(220)는 또한 휘발성 메모리, 반 휘발성 메모리, 랜덤 액세스 메모리, 정적 메모리, 캐시, 버퍼, 또는 런타임 정보를 저장하는 데 사용되는 다른 매체와 같은 다양한 데이터 저장 디바이스/컴포넌트 중 임의의 것을 포함할 수 있다. 일 예에서, 운영 메모리(220)는 컴퓨팅 디바이스(200)의 전원이 꺼질 때 정보를 유지하지 않는다. 오히려, 컴퓨팅 디바이스(200)는 부팅 또는 다른 로딩 프로세스의 일부로서 비 휘발성 데이터 저장 컴포넌트(예를 들어, 데이터 저장 컴포넌

트(250))로부터 운영 메모리(220)로 명령어를 전송하도록 구성될 수 있다.

[0020] 운영 메모리(220)는 제 4 세대 더블 데이터 레이트(DDR4) 메모리, 제 3 세대 더블 데이터 레이트(DDR3) 메모리, 다른 동적 랜덤 액세스 메모리(DRAM), 고 대역폭 메모리(High Bandwidth Memory)(HBM), 하이브리드 메모리 큐브 메모리(Hybrid Memory Cube memory), 3D-적층 메모리, 정적 랜덤 액세스 메모리(static random access memory)(SRAM), 또는 다른 메모리를 포함할 수 있으며, 이러한 메모리는 DIMM, SIMM, SODIMM, 또는 다른 패키징 상에 통합된 하나 이상의 메모리 회로를 포함할 수 있다. 이러한 운영 메모리 모듈 또는 디바이스는 채널, 랭크(rank) 및 뱅크(bank)에 따라 조직화될 수 있다. 예를 들어, 운영 메모리 디바이스는 채널의 메모리 컨트롤러(230)를 통해 프로세싱 회로(210)에 연결될 수 있다. 컴퓨팅 디바이스(200)의 일 예는 채널당 하나 또는 두개의 랭크와 함께, 채널당 하나 또는 두개의 DIMM을 포함할 수 있다. 랭크 내의 운영 메모리는 공유 클록 및 공유 어드레스 및 커맨드 버스로 동작할 수 있다. 또한, 운영 메모리 디바이스는, 뱅크가 행 및 열에 의해 어드레싱되는 어레이로 간주될 수 있는 수 개의 뱅크로 조직화될 수 있다. 이러한 운영 메모리의 조직화(organization)에 기초하여, 운영 메모리 내의 물리적 어드레스는 채널, 랭크, 뱅크, 행, 및 열의 투플(tuple)에 의해 참조될 수 있다.

[0021] 전술한 설명에도 불구하고, 운영 메모리(220)는 특히 통신 매체, 임의의 통신 매체 또는 임의의 신호 그 자체를 포함하거나 포괄하지는 않는다.

[0022] 메모리 컨트롤러(230)는 프로세싱 회로(210)를 운영 메모리(220)에 인터페이스하도록 구성된다. 예를 들어, 메모리 컨트롤러(230)는 운영 메모리(220)와 프로세싱 회로(210) 사이에서 커맨드, 어드레스 및 데이터를 인터페이스하도록 구성될 수 있다. 메모리 컨트롤러(230)는 또한 프로세싱 회로(210)로부터 또는 프로세싱 회로(210)에 대한 메모리 관리의 특정 양태를 추출하거나 달리 관리하도록 구성될 수 있다. 메모리 컨트롤러(230)가 프로세싱 회로(210)와 분리된 단일 메모리 컨트롤러로 도시되고 있지만, 다른 예에서, 다수의 메모리 컨트롤러가 사용될 수 있고, 메모리 컨트롤러(들)는 운영 메모리(220) 등과 통합될 수 있다. 또한, 메모리 컨트롤러(들)는 프로세싱 회로(210)에 통합될 수 있다. 이러한 변형 및 다른 변형이 가능하다.

[0023] 컴퓨팅 디바이스(200)에서, 데이터 저장 메모리(250), 입력 인터페이스(260), 출력 인터페이스(270), 및 네트워크 어댑터(280)는 버스(240)에 의해 프로세싱 회로(210)에 인터페이스된다. 도 2는 버스(240)를 단일 수동 버스로서 도시하지만, 다른 구성들, 예를 들어, 버스들의 집단, 점대점 링크들의 집단, 입/출력 컨트롤러, 브릿지, 다른 인터페이스 회로, 또는 이들의 임의의 집단이 또한 데이터 저장 메모리(250), 입력 인터페이스(260), 출력 인터페이스(270), 또는 네트워크 어댑터(280)를 프로세싱 회로(210)에 인터페이스하기 위해 적절하게 사용될 수 있다.

[0024] 컴퓨팅 디바이스(200)에서, 데이터 저장 메모리(250)는 장기 비 휘발성 데이터 저장을 위해 사용된다. 데이터 저장 메모리(250)는 비 휘발성 메모리, 디스크, 디스크 드라이브, 하드 드라이브, 솔리드 스테이트 드라이브, 또는 비 휘발성 정보 저장을 위해 사용될 수 있는 임의의 다른 매체와 같은 다양한 비 휘발성 데이터 저장 디바이스/컴포넌트 중 임의의 것을 포함할 수 있다. 그러나, 데이터 저장 메모리(250)는 특히 통신 매체, 임의의 통신 매체 또는 임의의 신호 그 자체를 포함하거나 포괄하지는 않는다. 운영 메모리(220)와는 대조적으로, 데이터 저장 메모리(250)는 런타임 데이터 저장 대신에 비 휘발성 장기 데이터 저장을 위해 컴퓨팅 디바이스(200)에 의해 사용된다.

[0025] 또한, 컴퓨팅 디바이스(200)는 프로세서 판독가능 저장 매체(예를 들어, 운영 메모리(220) 및 데이터 저장 메모리(250)) 및 통신 매체(예를 들어, 통신 신호 및 무선파)와 같은 임의의 유형의 프로세서 판독가능 매체를 포함하거나 이에 연결될 수 있다. 프로세서 판독가능 저장 매체라는 용어는 운영 메모리(220) 및 데이터 저장 메모리(250)를 포함하지만, 본원 명세서 및 청구범위 전체에 걸쳐 단수 또는 복수로 사용되는 용어 "프로세서 판독가능 저장 매체"는 본원 명세서에서 특히 통신 매체, 임의의 통신 매체 또는 임의의 신호 그 자체를 배제하고 이를 포함하지 않는 것으로 정의된다. 그러나, "프로세서 판독가능 저장 매체"라는 용어는 프로세서 캐시, 랜덤 액세스 메모리(RAM), 레지스터 메모리, 및/또는 기타 등을 포함한다.

[0026] 컴퓨팅 디바이스(200)는 또한 컴퓨팅 디바이스(200)가 사용자 또는 다른 디바이스로부터 입력을 수신할 수 있게 구성될 수 있는 입력 인터페이스(260)를 포함한다. 또한, 컴퓨팅 디바이스(200)는 컴퓨팅 디바이스(200)로부터의 출력을 제공하도록 구성될 수 있는 출력 인터페이스(270)를 포함한다. 일 예에서, 출력 인터페이스(270)는 프레임 버퍼, 그래픽 프로세서, 그래픽 프로세서 또는 가속기를 포함하고, 별도의 시각 디스플레이 디스플레이(가령, 모니터, 프로젝터, 가상 컴퓨팅 클라이언트 컴퓨터 등) 상에 표시를 위한 디스플레이를 렌더링하도록 구성된다. 다른 예에서, 출력 인터페이스(270)는 시각 디스플레이 디바이스를 포함하고, 시청을 위한 디스플레이

를 렌더링하고 제공하도록 구성된다.

[0027] 도시된 예에서, 컴퓨팅 디바이스(200)는 네트워크 어댑터(280)를 통해 다른 컴퓨팅 디바이스 또는 엔티티와 통신하도록 구성된다. 네트워크 어댑터(280)는 유선 네트워크 어댑터, 예를 들어, 이더넷 어댑터, 토큰 링 어댑터, 또는 디지털 가입자 라인(DSL) 어댑터를 포함할 수 있다. 네트워크 어댑터(280)는 또한 무선 네트워크 어댑터, 예를 들어, Wi-Fi 어댑터, 블루투스 어댑터, 지그비 어댑터, LTE (Long Term Evolution) 어댑터, 또는 5G 어댑터를 포함할 수 있다.

[0028] 비록 컴퓨팅 디바이스(200)가 특정 배열로 구성된 특정 컴포넌트와 함께 도시되어 있지만, 이들 컴포넌트 및 배열은 본 기술이 사용될 수 있는 컴퓨팅 디바이스의 단순한 일 예에 불과하다. 다른 예에서, 데이터 저장 메모리(250), 입력 인터페이스(260), 출력 인터페이스(270), 또는 네트워크 어댑터(280)는 프로세싱 회로(210)에 직접 연결되거나, 입/출력 컨트롤러, 브릿지, 또는 다른 인터페이스 회로를 통해 프로세싱 회로(210)에 연결될 수 있다. 다른 변형의 기술도 가능하다.

[0029] 컴퓨팅 디바이스(200)의 일부 예는 런타임 데이터를 저장하도록 구성된 적어도 하나의 메모리(예를 들어, 운영 메모리(220)) 및 실행에 응답하여 컴퓨팅 디바이스(200)가 액션을 수행할 수 있게 하는 프로세서 실행 가능 코드를 실행하도록 제각기 구성되는 적어도 하나의 프로세서(가령, 프로세싱 유닛(210))를 포함한다. 일부 예에서, 컴퓨팅 디바이스(200)는 액션, 가령, 아래의 도 4 또는 도 5의 프로세스에서의 액션을 수행하거나, 또는 아래의 도 3의 하나 이상의 컴퓨팅 디바이스에 의해 수행되는 프로세스에서의 액션을 수행하도록 인에이블된다.

[0030] 예시적 시스템

[0031] 도 3은 IOT 통신을 위한 시스템(300)의 일 예를 나타내는 블록도이다. 시스템(300)은 네트워크(330), IoT 허브(351), IoT 디바이스(341-343), 게이트웨이 디바이스(311 및 312), 및 디바이스 포털 서비스(313)를 포함할 수 있으며, 이들 모두는 네트워크(330)에 접속된다. 전술한 바와 같이, "IoT 허브"라는 용어는 하나의 특정 타입의 IoT 서비스에 한정되지 않고, IoT 디바이스가 프로비저닝 후에, 적어도 하나의 IoT 솔루션 또는 임의의 타입의 IoT 서비스를 위해 통신하는 디바이스를 지칭한다. 즉, 본원 명세서 및 청구범위 전반에 걸쳐 사용되는 "IoT 허브"라는 용어는 모든 IoT 솔루션에 대한 일반적인 용어이다. "IoT 디바이스"라는 용어는 IoT 서비스를 이용하거나 이용하도록 의도된 디바이스를 지칭한다. IoT 디바이스는 원격 측정 수집 또는 임의의 다른 목적을 포함하여 IoT 서비스를 사용하기 위해 클라우드에 접속하는 거의 모든 디바이스를 포함할 수 있다. 디바이스 포털 서비스(313)는 디바이스 포털을 제공하는 하나 이상의 디바이스를 포함한다. "IoT 허브"라는 용어는 IoT 디바이스가 IoT 서비스를 위해 네트워크를 통해 접속하는 디바이스, 또는 분산 시스템과 같은 다수의 디바이스를 지칭한다.

[0032] IoT 디바이스(341 내지 343), 게이트웨이 디바이스(311 및 312), 및/또는 IoT 허브(351) 및/또는 디바이스 포털 서비스(313)를 포함하는 디바이스의 각각은 도 2의 컴퓨팅 디바이스(200)의 예를 포함할 수 있다. 도 3 및 본원 명세서 내에서의 도 3의 해당 설명은 본 개시 내용의 범위를 제한하지 않는 예시적인 목적의 예시 시스템을 나타내고 있다.

[0033] 네트워크(330)는 유선 및/또는 무선 네트워크를 포함하는 하나 이상의 컴퓨터 네트워크를 포함할 수 있으며, 여기서 각각의 네트워크는, 예를 들어, 무선 네트워크, 근거리 통신망(LAN), 광역 통신망(WAN), 및/또는 인터넷과 같은 글로벌 네트워크일 수 있다. 서로 다른 아키텍처 및 프로토콜을 기반으로 하는 LAN을 포함하여 상호 접속된 LAN들의 세트 상에서, 라우터는 LAN 간의 링크로서 기능하여 메시지가 서로 간에 전송될 수 있게 한다. 또한, LAN 내의 통신 링크는 일반적으로 연선 또는 동축 케이블을 포함하지만, 네트워크 간의 통신 링크는 아날로그 전화 회선, T1, T2, T3 및 T4를 포함한 전체 또는 부분 전용 디지털 회선, 통합 서비스 디지털 네트워크(Integrated Services Digital Networks)(ISDN), 디지털 가입자 회선(DSL), 위성 링크를 포함한 무선 링크, 또는 본 기술 분야의 통상의 기술자에게 알려진 다른 통신 링크를 이용할 수 있다. 또한 원격 컴퓨터 및 다른 관련 전자 디바이스는 모뎀 및 임시 전화 링크를 통해 LAN 또는 WAN에 원격으로 접속될 수 있다. 본질적으로, 네트워크(330)는 IoT 허브(351), IoT 디바이스(341 내지 343), 게이트웨이 디바이스(311 내지 312), 및 디바이스 포털 서비스(313) 사이에서 정보가 이동할 수 있는 임의의 통신 방법을 포함한다.

[0034] 일 예로서, IoT 디바이스(341 내지 343)는 IoT 허브(351)와 같은 하나 이상의 IoT 허브에 의해 제공되는 IoT 서비스를 이용하도록 의도된 디바이스이다. 디바이스 포털 서비스(313)는 IoT 디바이스의 사용자에게 디바이스 포털을 제공하는 액션을 수행하는 디바이스 또는 다수의 디바이스를 포함한다.

[0035] 선택적인 게이트웨이 디바이스(311 및 312)는 IoT 허브(351)에 액세스하기 위해 IoT 디바이스(341 내지 343) 중 일부에 의해 사용될 수 있는 디바이스이다. 일부 예에서, 프로비저닝 후에, IoT 디바이스(341 내지 343)의 일부 또는 전부는 중개자를 사용하지 않고 IoT 허브(351)와 통신한다. 다른 예에서, IoT 디바이스(341 내지 343)의 일부 또는 전부는 하나 이상의 게이트웨이 디바이스(311 및 312)와 같은 중개자 디바이스를 사용하여 IoT 허브(351)와 통신한다. 디바이스 포털 서비스(313)는 IoT 디바이스(341 내지 343)를 포함하여 IoT 디바이스에 대한 IoT 서비스를 관리하기 위해 IoT 디바이스의 사용자에 의해 사용될 수 있는 서비스이다.

[0036] 시스템(300)은 단지 예로서 도시한 도 3에 도시된 것보다 많거나 적은 디바이스를 포함할 수 있다.

[0037] 예시적 프로세스

[0038] 명료함을 위해, 본원에 설명된 프로세스는 시스템의 특정 디바이스 또는 컴포넌트에 의해 특정 시퀀스로 수행되는 동작으로 설명된다. 그러나, 주목할 것은 다른 프로세스가 명시된 시퀀스, 디바이스 또는 컴포넌트에 한정되지 않는다는 것이다. 예를 들어, 특정 행위들은 상이한 시퀀스로 수행될 수 있거나, 병렬로 수행될 수 있거나, 생략될 수 있거나, 또는 그러한 시퀀스, 병렬화, 행위, 또는 특징이 본원에 기술되는지의 여부와는 상관없이, 추가의 행위 또는 특징으로 보완될 수 있다. 마찬가지로, 본 개시 내용에서 설명된 임의의 기술은 그 기술이 프로세스와 관련하여 구체적으로 기술되는지의 여부와는 상관없이, 설명된 프로세스 또는 다른 프로세스에 통합될 수 있다. 본 개시된 프로세스는 또한 다른 디바이스, 컴포넌트 또는 시스템이 본원 명세서에 기술되는지의 여부와는 상관없이 그 다른 디바이스, 컴포넌트 또는 시스템 상에서 또는 그에 의해 수행될 수 있다. 이러한 프로세스는 또한 다양한 방식으로 구현될 수 있다. 예를 들어, 이들 프로세스는 제조 물품 상에서, 예를 들어, 프로세서 판독가능 저장 매체에 저장된 프로세서 판독가능 명령어로서 구현되거나 컴퓨터에 의해 구현되는 프로세스로서 수행될 수 있다. 다른 예로서, 이들 프로세스는 프로세서 실행가능 명령어로서 인코딩될 수 있고 통신 매체를 통해 전송될 수 있다.

[0039] 도 4는 IoT 인증을 위한 프로세스의 일 예시적인 데이터 흐름을 나타내는 도면이다. 도 4 및 본원 명세서 내에서의 도 4의 해당 설명은 본 개시 내용의 범위를 제한하지 않는 예시적인 목적의 예시 프로세스를 나타내고 있다.

[0040] 도시된 예에서, 먼저, 단계(421)가 발생한다. 단계(421)에서, IoT 허브(451)는 적어도 하나의 IoT 디바이스의 예상된 조건과 관련된 보안 규칙들의 세트를 저장한다. 일부 예에서, 보안 규칙들의 세트는 적어도 하나의 IoT 디바이스(예를 들어, IoT 디바이스(441))와 관련된 IoT 데이터의 평가에 기초한다. 저장된 보안 규칙들의 세트는, 예를 들어, IoT 디바이스의 타입, 특정 배치 컨텍스트, 및 다른 요인에 기초하여 다를 수 있다. 보안 규칙들의 세트는 (아래의 단계(424)에서 수집된 IoT 데이터의 설명 후에) 아래에서 보다 상세히 설명된다.

[0041] 도시된 바와 같이, 일부 예에서는 단계(422)가 다음에 발생한다. 단계(422)에서, 디바이스 포털 서비스(413)에 의해 구성 요청(configuration request)이 생성될 수 있고, 그 후, 구성 요청은 디바이스 포털 서비스(413)로부터 IoT 허브(451)로 전달될 수 있다. 구성 요청은 IoT 허브(451)에 저장된 보안 규칙들의 세트를 조정하는 것과 연관될 수 있다. 일부 예에서, 구성 요청은 보안 규칙들의 세트를 조정된 보안 규칙들의 세트로 변경하라는 요청이다. 구성 요청은 다른 예에서 상이한 방식으로 행해질 수 있다. 일부 예에서는, 디폴트 보안 규칙들의 세트가 사용되는 기본 모드가 존재하며, 또한 사용자가 디폴트 보안 규칙들의 세트를 변경하기 위한 구성 요청을 행할 수 있는 고급 설정이 존재한다. 도시된 바와 같이, 일부 예에서는 단계(423)가 다음에 발생한다. 단계(423)에서, IoT 허브(451)는 단계(422)에서 디바이스 포털 서비스(413)로부터 수신된 구성 요청에 기초하여 IoT 허브(451)에 저장된 보안 규칙들의 세트를 조정할 수 있다.

[0042] 도시된 바와 같이, 일부 예에서는 단계(424)가 다음에 발생한다. 단계(424)에서, IoT 디바이스(441)는 환경, 예를 들어, IoT 디바이스(441) 부근의 환경으로부터 환경 데이터를 수신 및 수집하고, IoT 디바이스(441)의 내부 보안 상태에 관한 데이터를 수집한다. 환경 데이터는 원격 측정 데이터, IoT 디바이스(441)가 물리적으로 변조되었는지의 여부를 나타내는 데이터, 및/또는 기타 등을 포함할 수 있다. 원격 측정 데이터는 온도, 습도, IoT 디바이스와 관련된 위치의 점유(occupancy of a location), 위치 정보(geolocation), 및/또는 기타 등을 포함할 수 있다. IoT 디바이스(441)의 내부 보안 상태에 관한 데이터는 운영 체제(OS) 버전, 활성 프로세스의 현재 상태, 개방 포트, 접속된 디바이스의 인터넷 프로토콜(IP) 어드레스, 및/또는 기타 등을 포함할 수 있다. 데이터는 소프트웨어 입력, 하드웨어 입력 또는 둘 다를 통해 수집될 수 있다.

[0043] 단계(424)에서 수집된 원격 측정 데이터는 일부 예에서 IoT 디바이스가 이미 수집한 원격 측정을 포함할 수 있다. 예를 들어, 온도 센서인 IoT 디바이스는 온도 데이터를 수집하도록 이미 구성되어 있을 수 있다.

[0044] IoT 디바이스(441)는 물리적 변조를 검출하는 하나 이상의 변조 스위치(tampering switches)를 가질 수 있다. 일 예에서, IoT 디바이스(441)가 물리적으로 변조되어 있지 않다면, 변조 스위치는 오프(off)이고, IoT 디바이스(441)가 물리적으로 변조되었다면 변조 스위치는 온(on)이다. 환경 데이터는 변조 스위치가 온 또는 오프인지에 대한 표시를 포함할 수 있다. 예를 들어, 일부 실시예에서, IoT 디바이스(441)는 2 개의 변조 스위치에 연결된 커버를 갖는다. 커버가 개방되면, 두 변경 스위치는 모두 온으로 된다.

[0045] 일부 예에서, IoT 디바이스(441)는 IoT 디바이스(441)의 내부 보안에 관한 데이터 및 환경 데이터를 수집하는 소프트웨어 에이전트를 포함할 수 있다. 일부 예에서, IoT 디바이스(441)는 환경 및/또는 내부 상태 데이터를 수집하기 위해 IoT 디바이스(441) 상에 배치된 소프트웨어 데이터 수집 에이전트를 갖는다. 일부 예에서, 일부 또는 모든 IoT 디바이스는 IoT 디바이스로부터 환경 및/또는 내부 상태 데이터를 수집하기 위해 IoT 디바이스 상에 배치된 소프트웨어 데이터 수집 에이전트를 갖는다.

[0046] IoT 허브(451)에 저장된 보안 규칙들의 세트는 IoT 디바이스(예를 들어, 도 3의 441 및/또는 341 내지 434)의 정상 동작의 모델에 기초한다. 이 모델은 IoT 디바이스가 정상 조건에서 작동하는 동안 IoT 디바이스의 상태를 나타낼 수 있다. 일부 예에서, 보안 규칙들의 세트는 구성 가능한 IoT 디바이스 모델로서 작용한다. 규칙들의 세트는 공격 또는 기타 보안 침입 또는 보안 위협이 발생하면 위반되도록 정의될 수 있다.

[0047] 예를 들어, IoT 디바이스는 사이버 공격 및 물리적 공격의 두 가지 카테고리로 분류될 수 있는 다양한 타입의 보안 공격을 받을 수 있다. 사이버 공격은 디바이스의 사이버 특성에 대한 공격, 가령, 운영 체제, 네트워크 인프라 구조, 접속, 및 데이터에 대한 공격을 포함한다. 물리적 공격은 디바이스의 물리적 변조, 디바이스의 데이터 생성 요소의 조작, 재배치, 및 기타 등과 같은 공격을 포함한다. 일부 예에서, 보안 규칙들의 세트의 위반이 하나 이상의 IoT 디바이스에 대한 적어도 하나의 공격(예를 들어, 물리적 공격 또는 사이버 공격)의 가능성을 나타내도록 보안 규칙들의 세트가 생성되거나 조정된다. 따라서, 이러한 공격 중의 임의의 하나가 발생하면, 디바이스로부터 수집되는 데이터는 이후에 모델과는 달라지기 때문에 일 예에서는 규칙들의 세트의 위반이 발생해야 한다. 모델은 원격 측정 데이터에 대한 하나 이상의 패턴을 포함할 수 있다.

[0048] 따라서, 보안 규칙들의 세트는 충족되지 않으면 보안 위협의 가능성을 나타낼 수 있는 정상 동작 조건을 정의할 수 있다. 예를 들어, 하나 이상의 데이터 요소가 예상 범위를 벗어나면 보안 규칙들의 세트가 위반될 수 있다. 예를 들어, 보안 규칙들의 세트는, 온도가 특정 범위 내에 있고, 변조 스위치가 오프이고, 특정의 블랙리스트의 프로세스가 실행되고 있지 않다는 것을 요구할 수 있다. 예상 범위 또는 예상 불연속 값은 시각(time of day) 및 기타 요인에 따라 달라질 수 있다. 일부 예에서, 온도 등의 각 타입의 데이터를 예상 범위(또는 예상된 불연속 값)와 개별적으로 비교하기보다는, 보안 규칙들의 세트는 모델에 기초하여 함께 고려되는 여러 타입의 데이터에 기초한다. 예를 들어, 일부 예에서, 환경 내에서 예상 범위를 초과하는 온도는 그 환경에 점유가 또한 존재하지 않는 한 보안 규칙들의 위반을 생성하지 않을 수 있다.

[0049] 일부 예에서, 보안 규칙들의 세트는 IoT 디바이스에 의해 수집된 환경 및 내부 보안 데이터의 모델에 기초하고 있으며, 여기서 모델은 예상 데이터의 "골든" 이미지를 효과적으로 제공한다. 골든 이미지는 임의의 침입 또는 보안 위협이 없는 정상적인 작동 조건에서 IoT 디바이스의 정상적인 동작을 반영할 수 있다. 수신된 IoT 데이터에 기초하여, 일부 양태가 골든 이미지와 다른 경우, 다른 데이터에 따라 규칙들의 세트는 위반된 것으로 간주될 수 있다. 예를 들어, 쇼핑몰의 특정 방의 점유 센서에 대한 골든 이미지에 따라, 그 점유 센서는 어느 누구도 쇼핑몰에 있을 것으로 예상되지 않는 특정 시간 동안의 점유를 나타내면 안된다. 그러나, 규칙은, 예를 들어, 쇼핑몰 게이트가 열려 있고 경비가 쇼핑몰에 여전히 존재하는 경우, 예기치 않은 시간에서의 점유는 보안 규칙들의 세트의 위반을 트리거하는 것이 아니라는 것을 명시할 수 있다. 일부 예에서, 다수의 IoT 디바이스로부터의 데이터는 규칙들의 세트가 위반되었는지 여부를 결정하기 위해 보안 규칙들의 세트 및 모델에 포함될 수 있다. 디바이스 운영 및 운영 환경 및 침입에 대한 보다 총체적인 모델은 하나의 IoT 디바이스에 기반한 것보다 다수의 IoT 디바이스로부터의 데이터를 사용함으로써 사용될 수 있다.

[0050] 일부 예에서, 보안 규칙들의 세트는 화이트리스트의 프로세스 및 블랙리스트의 프로세스 중 하나 또는 둘 모두를 포함한다. 화이트리스트 및 블랙리스트의 프로세스는 IoT 디바이스가 멀웨어에 감염되었는지의 여부를 결정하는 데 유용할 수 있다. "화이트리스트"의 프로세스는 승인된 리스트의 프로세스를 지칭하며, "블랙리스트"의 프로세스는 금지된 리스트의 프로세스를 지칭한다.

[0051] 일부 예에서, 수집된 원격 측정 데이터를 포함하는 수집된 IoT 데이터는 보안 규칙들의 세트를 생성 또는 조정하기 위해 모델을 구성하는 것을 지원하는 데 사용될 수 있다.

[0052] 도시된 바와 같이, 일부 예에서는 단계(425)가 다음에 발생한다. 단계(425)에서, IoT 디바이스(441)는 IoT 허브(451)로 데이터를 전송할지의 여부에 관한 결정을 할 수 있다. 일부 예에서, 단계(425)에서, IoT 디바이스(441)는 단순히 모든 데이터를 IoT 허브(451)로 항상 전송할 것을 결정한다. 일부 예에서, 하나 이상의 타입의 데이터에 기초한 임계치를 초과하는 경우의 데이터만이 전송된다.

[0053] 예를 들어, 일부 예에서, IoT 디바이스(441)는 검출된 온도가 미리 결정된 범위, 예를 들어, 화씨 65 내지 75도의 범위를 벗어난 경우에만 온도 데이터를 전송하는 결정을 행한다. 일부 예에서, 온도가 화씨 65 내지 75도의 범위를 벗어난다는 사실 자체가 보안 규칙을 위반하는 것이 아니고, 따라서, IoT 디바이스(441)는 보안 규칙들의 세트가 이 예에서 위반되었는지의 여부에 관한 결정을 행하지 않지만, 단지 온도가 특정 범위를 벗어날 때만 온도 데이터를 전송하므로, 다른 요인에 따라 보안 규칙들의 세트의 위반이 있을 수도 있다.

[0054] 도시된 바와 같이, 일부 예에서, 단계(426)는 이후 단계(425)에서의 결정이 긍정인 경우에 발생한다. 단계(426)에서, IoT 데이터는 IoT 디바이스(441)로부터 IoT 허브(451)로 전달될 수 있다. 대조적으로, 단계(426)에서의 결정이 부정적이라면, 다른 프로세싱이 재개된다.

[0055] 도시된 바와 같이, 일부 예에서는 단계(427)가 단계(426) 이후에 발생한다. 단계(427)에서, IoT 허브(451)는, 단계(426)에서 수신된 IoT 데이터에 기초하여, IoT 허브(451)에 저장된 보안 규칙들의 세트가 위반되었는지의 여부에 대한 결정을 행한다. 일부 예에서, 단계(427)에서의 결정은 수집된 IoT 디바이스 데이터와 구성 가능한 IoT 디바이스 모델의 비교이다.

[0056] 도시된 바와 같이, 일부 예에서는 단계(428)가 다음에 발생한다. 단계(428)에서, IoT 허브(451)는 단계(427)에서의 결정에 기초하여 디바이스 포털 서비스(413)에 경고를 선택적으로 전송한다. 단계(427)에서 규칙들의 세트가 위반되었다고 결정되었다면, IoT 허브(451)는 디바이스 포털 서비스(413)에 경고를 전달한다. 대신에, 단계(427)에서, 규칙들의 세트가 위반되지 않았다고 결정되면, IoT 허브(451)는 경고를 발송하지 않는다.

[0057] IoT 디바이스(441)가 클라우드로부터 접속 해제되면, 데이터는 IoT 디바이스(441)로부터 수집될 수 없지만, IoT 디바이스(441)가 클라우드로부터 접속 해제된다는 사실 자체가 정보의 형태가 되고, 일부 예에서는 IoT 디바이스(441)가 클라우드로부터 접속 해제된다는 것으로부터 경고가 발생할 수 있다.

[0058] 일부 예에서, 보안 규칙들의 세트는 시간 경과에 따라 추가 조정될 수 있어서, 위양성(false positive)을 감소시키고, 다른 방식으로는 검출되지 않을 수도 있을 공격을 성공적으로 검출할 수 있다. 일부 예에서, IoT 허브(451)는 비정상으로부터 학습하고, 시간 경과에 따라 보안 규칙들의 세트를 변경하고 시간 경과에 따라 학습함으로써 적응되는 학습 계층(learning layer)을 포함한다.

[0059] 일부 예에서, IoT 데이터를 IoT 허브(451)에 직접 전송하는 대신에, IoT 디바이스(441)는 그 데이터를 게이트웨이 디바이스(예를 들어, 도 3의 게이트웨이 디바이스(311 또는 312))에 전송한다. 일부 예에서, IoT 디바이스(441)보다는 게이트웨이 디바이스는 IoT 데이터를 IoT 허브(451)로 전송할지의 여부에 관한 결정을 행한다. 일부 예에서, 다수의 상이한 IoT 디바이스(예를 들어, 도 3의 341 내지 343)는 하나의 게이트웨이 디바이스에 IoT 데이터를 전송하며, 이 게이트웨이 디바이스는 IoT 데이터를 수집한 후, IoT 데이터를 IoT 허브(451)에 전송할지의 여부 및 어떠한 IoT 데이터를 IoT 허브(451)에 전송할지를 결정한다.

[0060] 일부 예에서, 단계(428)에서, 단순하게 경고를 발송하기 보다는, 결정될 수 있는 한, 예를 들어, 공격 또는 위협의 속성에 관한 정보를 포함하는 다른 세부 사항이 또한 경고와 함께 IoT 허브(451)로부터 디바이스 포털 서비스(413)에 전달된다. 예를 들어, IoT 허브(451)가 GPS를 통해 디바이스가 이동되었다는 것을 그리고 다른 IoT 데이터로부터 멀웨어가 설치되었다는 것을 결정하면, 이 공격의 속성은 IoT 허브(451)로부터 디바이스 포털 서비스(413)로 전달될 수 있으며, 이는 이러한 두 개의 이벤트 중 하나만이 발생했을 때와는 잠재적으로 상이한 시나리오이다. IoT 허브(451)에서 디바이스 포털 서비스(413)로의 통신에서 보안 위협의 속성을 자세히 설명하기 위해 다수의 IoT 디바이스로부터 수집된 데이터가 적용 가능할 경우에 또한 사용될 수 있다.

[0061] 도 5는 IOT 인증을 위한 프로세스(590)의 일 예를 나타내는 논리 흐름도이다. 일 예에서, 프로세스(590)는 도 1의 IoT 허브(351)와 같은 IoT 허브에 의해 수행된다. 시작 블록 후에, 프로세스는 블록(591)으로 진행한다. 블록(591)에서, 적어도 하나의 IoT 디바이스의 예상된 조건과 관련된 보안 규칙들의 세트가 저장된다. 그 후, 프로세스는 블록(592)으로 이동한다. 블록(592)에서, 적어도 하나의 IoT 디바이스와 관련된 IoT 데이터가 수신된다. IoT 데이터는 적어도 두 개의 상이한 타입의 데이터를 포함하는 집계 데이터일 수 있다. 프로세스는 그 후 판정 블록(593)으로 진행한다.

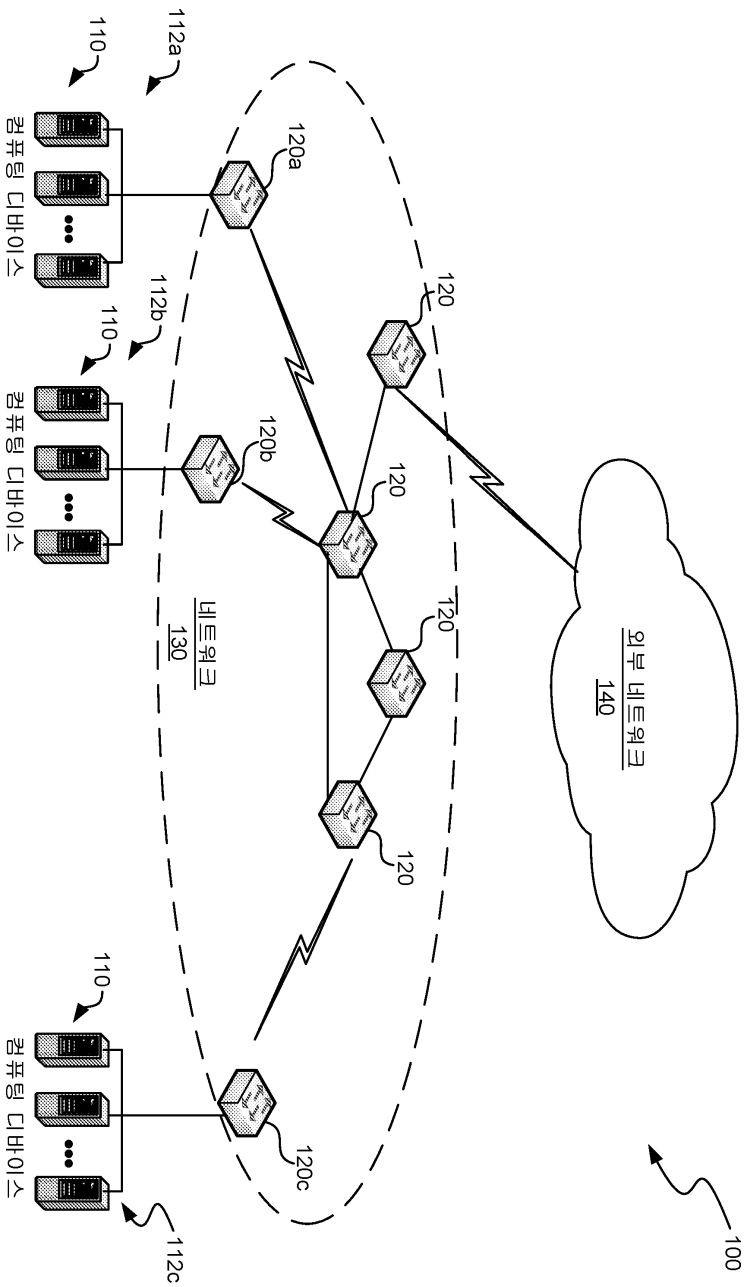
[0062] 판정 블록(593)에서, IoT 데이터에 기초하여 보안 규칙들의 세트가 위반되었는지의 여부에 대한 결정이 행해진다. 판정 블록(593)에서의 판정이 부정적이면, 프로세스는 리턴 블록을 진행하여 다른 프로세싱을 재개한다. 판정 블록(593)에서의 판정이 긍정적이라면, 프로세스는 블록(594)으로 진행하여 경고가 전송된다. 예를 들어, 일부 예에서, 경고는 디바이스 포털 서비스에 전송된다. 그런 다음, 프로세스는 리턴 블록으로 진행하여 다른 프로세싱을 재개한다. 이러한 방식으로, 판정 블록(593)에서의 결정에 기초하여 경고가 선택적으로 전송된다.

[0063] 결론

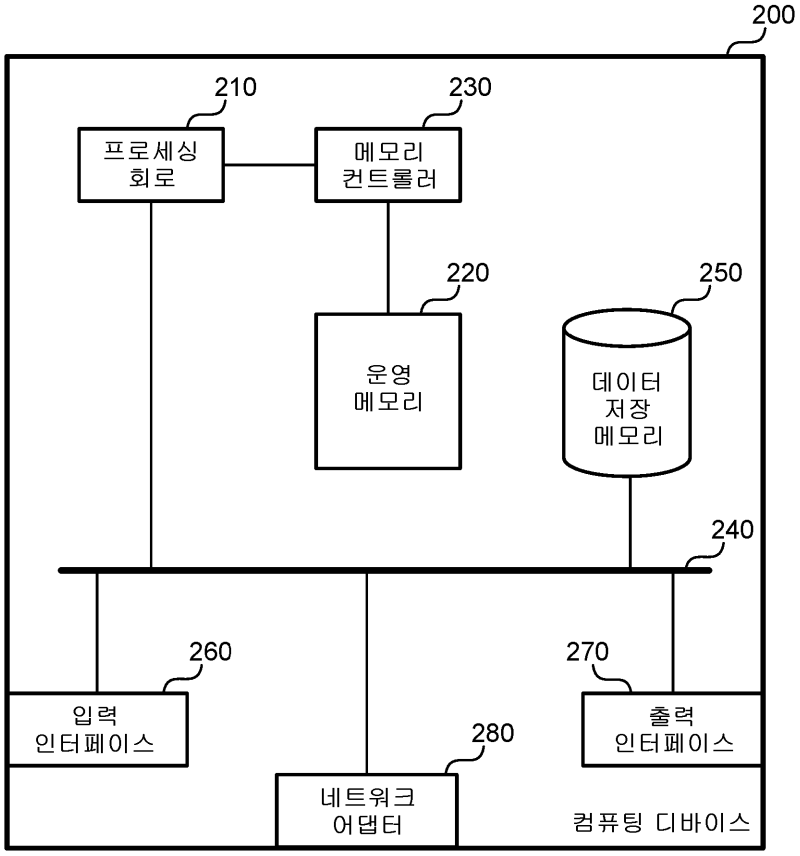
[0064] 전술한 상세한 설명은 본 기술의 특정 예를 설명하고, 고려된 최상의 모드를 설명하지만, 위의 내용이 텍스트에 제 아무리 상세하게 나타나 있더라도 본 기술은 여러 가지 방식으로 실행될 수 있다. 세부 사항이 구현시에 변할 수 있지만, 이는 본원에 설명된 기술에 여전히 포함된다. 전술한 바와 같이, 본 기술의 특정 특징 또는 양태를 설명할 때 사용된 특정 용어는 이 용어가 관련되는 임의의 특정 특성, 특징 또는 양태로 제한되도록 재 정의된다는 것을 의미하는 것으로 간주되어서는 안된다. 일반적으로, 아래의 청구범위에서 사용된 용어는 상세한 설명이 그러한 용어를 명시적으로 정의하지 않는 한, 그러한 용어를 본원에 개시된 특정 예로 제한하는 것으로 해석되어서는 안된다. 따라서, 본 기술의 실제 범위는 개시된 예뿐만 아니라 본 기술을 실시하거나 구현하는 모든 동등한 방식을 포함한다.

도면

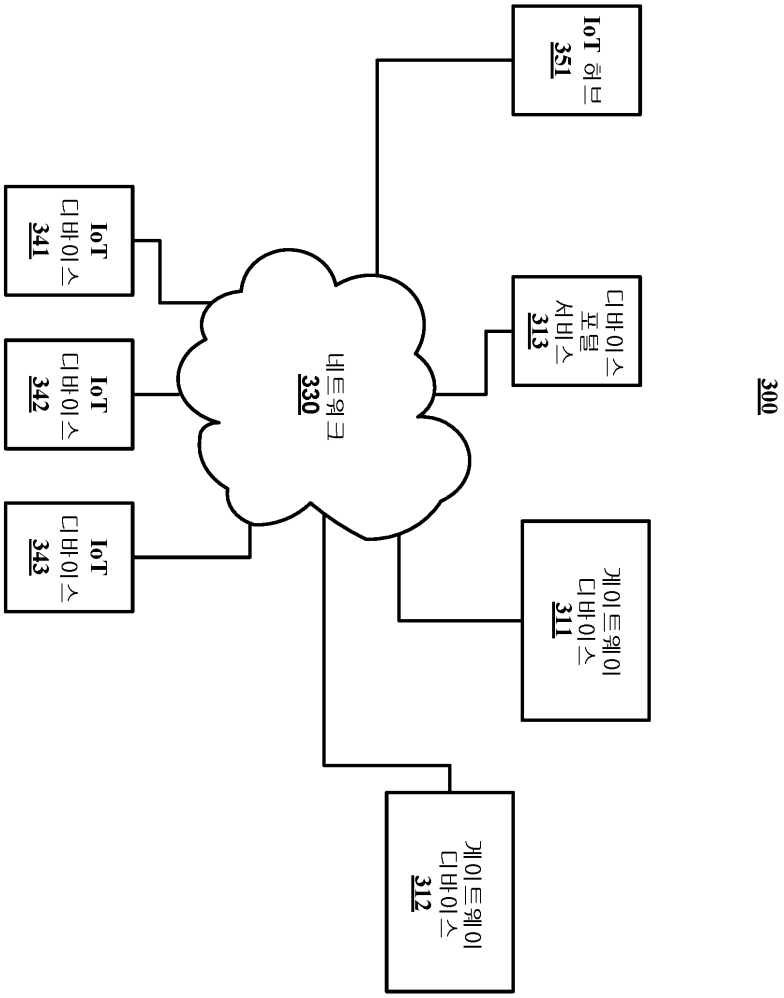
도면1


110
112a
120a
120
112b
110
120b
120
120
네트워크
130
외부 네트워크
140
110
120c
112c
100
컴퓨팅 디바이스
컴퓨팅 디바이스
컴퓨팅 디바이스

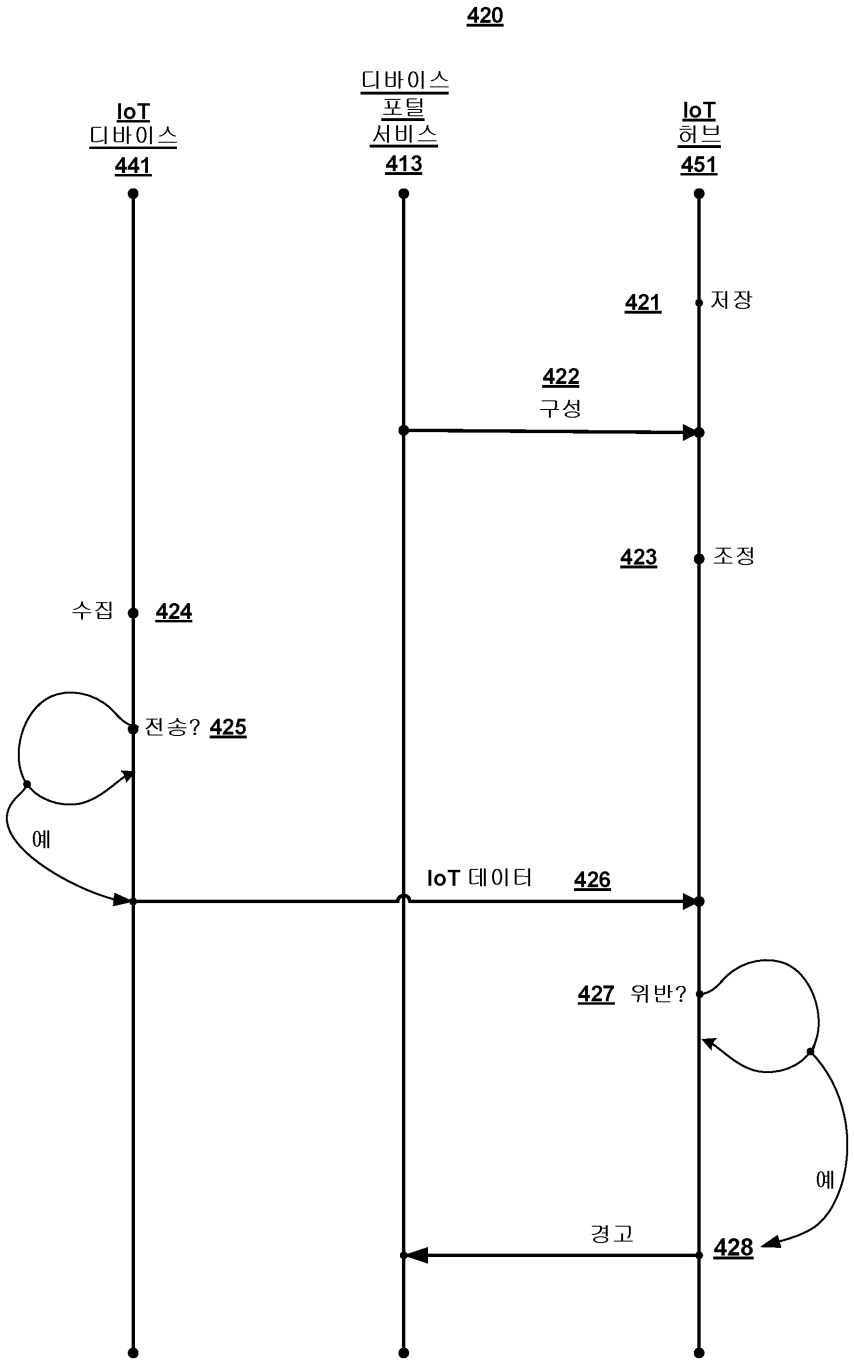
도면2


200
210
프로세싱
회로
230
메모리
컨트롤러
220
운영
메모리
250
데이터
저장
메모리
240
260
입력
인터페이스
270
출력
인터페이스
280
네트워크
어댑터
컴퓨팅 디바이스

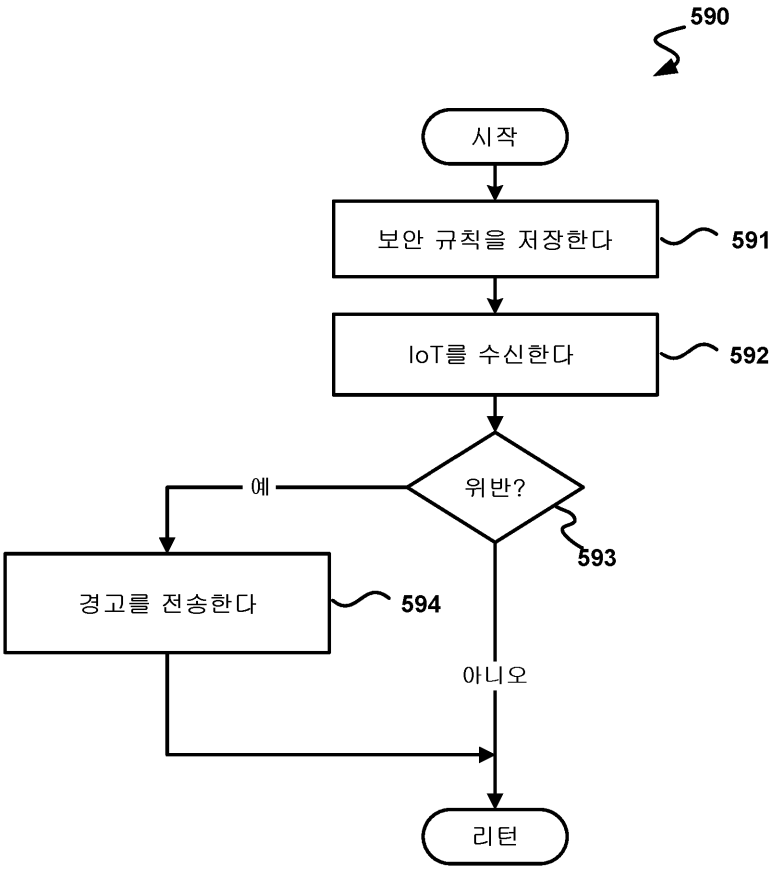
도면3


300
네트워크
330
IoT 허브
351
디바이스 포털 서비스
313
게이트웨이 디바이스
311
게이트웨이 디바이스
312
IoT 디바이스
341
IoT 디바이스
342
IoT 디바이스
343

도면4


420
IoT
디바이스
441
디바이스
포털
서비스
413
IoT
허브
451
421
저장
422
구성
423
조정
수집
424
전송? 425
예
IoT 데이터
426
427
위반?
예
경고
428

도면5



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 10

【변경전】

제 8 항에 있어서,

상기 내부 데이터는 운영 체제 버전, 활성 프로세스의 현재 상태, 개방 포트, 또는 상기 적어도 하나의 IoT 디바이스에 접속된 디바이스들과 관련된 정보 중 적어도 하나를 포함하는

장치.

【변경후】

제 8 항에 있어서,

상기 내부 상태 데이터는 운영 체제 버전, 활성 프로세스의 현재 상태, 개방 포트, 또는 상기 적어도 하나의 IoT 디바이스에 접속된 디바이스들과 관련된 정보 중 적어도 하나를 포함하는

장치.