(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0091758
(43) 공개일자 2020년07월31일

(51) 국제특허분류(Int. Cl.)
G06Q 50/00 (2018.01) *G06Q 50/10* (2012.01)
G06Q 50/30 (2012.01) *H04L 29/08* (2006.01)
H04L 29/12 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
G06Q 50/00 (2018.01)
G06Q 50/10 (2013.01)
(21) 출원번호 10-2019-0008946
(22) 출원일자 2019년01월23일
심사청구일자 2019년01월23일

(71) 출원인
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
(72) 발명자
엄태원
충청북도 청주시 흥덕구 오송읍 오송생명3로 87, 504동 802호(모아미래도아파트)
(74) 대리인
허용록

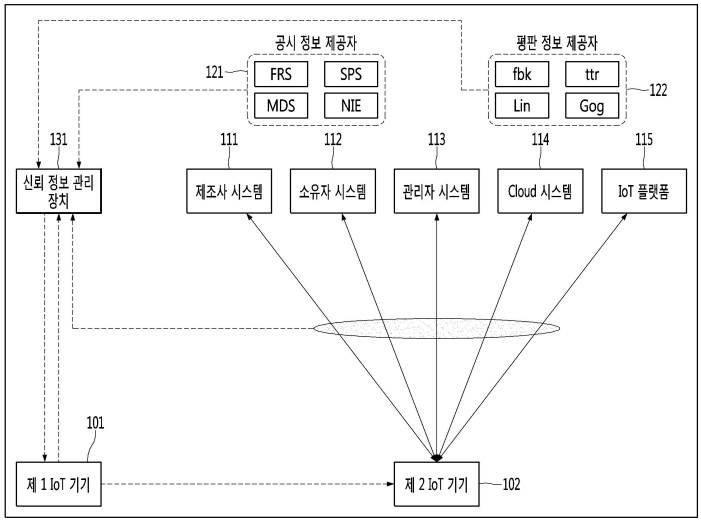
전체 청구항 수 : 총 33 항

(54) 발명의 명칭 **IoT 기기의 신뢰지수산출장치, IoT 기기의 신뢰지수산출방법, IoT 기기의 신뢰정보관리장치, IoT 기기의 신뢰정보관리방법, 신뢰기반하는 IoT 기기를 위한 협업시스템, 및 신뢰기반하는 IoT 기기의 협업방법**

(57) 요 약

본 발명에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템에는, 제 1 IoT 기기; 상기 제 1 IoT 기기가 연결하고자 하는 제 2 IoT 기기; 상기 제 2 IoT 기기를 관리하기 위하여 제공되는 적어도 하나의 관리를 위한 접속시스템; 상기 관리를 위한 접속시스템의 공시정보를 제공하는 공시정보제공자; 상기 관리를 위한 접속시스템 및 상기 제 2 IoT 기기 중의 적어도 하나의 평판정보를 제공하는 평판정보제공자; 및 상기 제 2 IoT 기기의 신뢰정도를 나타내는 신뢰지수를 산출하는 신뢰정보관리장치가 포함된다. 이에 따르면 네트워크의 각 노드의 신뢰성이 향상될 수 있다.

대 표 도



(52) CPC특허분류
G06Q 50/30 (2013.01)
H04L 61/1511 (2013.01)
H04L 67/12 (2013.01)
H04L 67/28 (2013.01)
H04L 9/08 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711076104
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 핵심기술개발
연구과제명 초소형 IoT 디바이스를 위한 자율적 상호협력기반 군집지능 기술개발
기 여 율 1/1
주관기관 조선대학교 산학협력단(과제참여기관)
연구기간 2018.07.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

IoT 기기와 상기 IoT 기기를 관리하는 관리를 위한 접속시스템이, 서로 간에 접속하는 양과 관련되는 정량정보를 처리하는 제 1 신뢰관련정보산출부;

상기 IoT 기기와 상기 관리를 위한 접속시스템 각각의 정성정보, 및 상기 IoT 기기와 상기 관리를 위한 접속시스템 각각의 정량정보, 중의 적어도 하나를 처리하는 제 2 신뢰관련정보산출부; 및

상기 제 1 신뢰관련정보산출부와 상기 제 2 신뢰관련정보산출부의 신뢰관련정보를 종합하여, 상기 IoT 기기의 신뢰지수를 산출하는 종합신뢰지수산출부가 포함되는 IoT 기기의 신뢰지수산출장치.

청구항 2

제 1 항에 있어서,

상기 제 1 신뢰관련정보산출부에서 처리되는 정량정보에는, 상기 IoT 기기와 상기 관리를 위한 접속시스템이 서로 접속하는 접속시간, 접속횟수, 및 접속빈도 중의 적어도 하나는 포함되는 IoT 기기의 신뢰지수산출장치.

청구항 3

제 1 항에 있어서,

상기 제 2 신뢰관련정보산출부로 신뢰관련정보를 제공하기 위하여,

공시정보를 처리하는 제 3 신뢰관련정보산출부; 및

평판정보를 처리하는 제 4 신뢰관련정보산출부가 더 포함되는 IoT 기기의 신뢰지수산출장치.

청구항 4

제 3 항에 있어서,

상기 공시정보에는, 상기 관리를 위한 접속시스템의 회사채등급과 신용등급 중의 적어도 하나는 포함되는 정성정보가 활용되는 IoT 기기의 신뢰지수산출장치.

청구항 5

제 3 항에 있어서,

상기 평판정보에는, 평판자의 진실성 및 평판자의 수 중의 적어도 하나는 포함되는, 정량정보 및 정성정보가 활용되는 IoT 기기의 신뢰지수산출장치.

청구항 6

제 1 항에 있어서,

상기 관리를 위한 접속시스템에는, 상기 제조사시스템, 소유자시스템, 관리자시스템, Cloud시스템, 및 IoT플랫폼 중의 적어도 하나는 포함되는 IoT 기기의 신뢰지수산출장치.

청구항 7

IoT 기기와 상기 IoT 기기를 관리하는 관리를 위한 접속시스템과의 접속상태정보를 입수하여 정량정보를 획득하는 것, 및

상기 관리를 위한 접속시스템의 공시정보와, 상기 IoT 기기와 상기 관리를 위한 접속시스템 중의 적어도 하나의 평판정보를 통하여 정량정보 및 정성정보를 획득하는 것을 포함하는 제 1 단계; 및

상기 제 1 단계에서 획득된 정량정보 및 정성정보를 종합하여 상기 IoT 기기의 신뢰지수를 산출하는 제 2 단계

가 포함되는 IoT 기기의 신뢰지수산출방법.

청구항 8

제 7 항에 있어서,

상기 공시정보에는, 상기 관리를 위한 접속시스템의 회사채등급과 신용등급 중의 적어도 하나는 포함되는 정성정보가 활용되는 IoT 기기의 신뢰지수산출방법.

청구항 9

제 7 항에 있어서,

상기 평판정보에는, 평판자의 진실성 및 평판자의 수 중의 적어도 하나는 포함되는 정량정보 및 정성정보가 활용되는 IoT 기기의 신뢰지수산출방법.

청구항 10

제 7 항에 있어서,

상기 관리를 위한 접속시스템에는, 상기 제조사시스템, 소유자시스템, 관리자시스템, Cloud시스템, 및 IoT플랫폼 중의 적어도 하나는 포함되는 IoT 기기의 신뢰지수산출방법.

청구항 11

외부의 정보를 이용하여 IoT 기기의 신뢰정도를 나타내는 신뢰지수를 산출하는 신뢰지수산출부;

상기 신뢰지수가 포함되는 정보를 저장하는 메모리;

외부의 노드들과의 입출력을 담당하는 통신부; 및

상기 신뢰지수를 메모리로부터 독출하여 통신부를 통하여 외부로 출력하는 제어부가 포함되는 IoT 기기의 신뢰정보관리장치.

청구항 12

제 11 항에 있어서,

상기 신뢰지수는,

-상기 IoT 기기와 상기 IoT 기기를 관리하는 관리를 위한 접속시스템이 서로 접속하는 정량정보,

-상기 관리를 위한 접속시스템의 공시정보, 및

-상기 IoT 기기와 상기 관리를 위한 접속시스템 중 적어도 하나의 평판정보

중의 적어도 하나에 근거하여 산출되는 IoT 기기의 신뢰정보관리장치.

청구항 13

제 11 항에 있어서,

상기 신뢰지수는 소정의 주기 및 외부의 요청 중 적어도 하나에 의해서 재산정되는 IoT 기기의 신뢰정보관리장치.

청구항 14

제 2 IoT 기기의 신뢰할 수 있는 정도를 나타내는 신뢰지수를 산출하여 메모리에 저장하는 단계; 및

제 1 IoT 기기로부터 요청이 있을 때, 상기 제 2 IoT 기기의 신뢰지수를 독출하여 출력하는 IoT 기기의 신뢰정보관리방법.

청구항 15

제 14 항에 있어서,

상기 신뢰지수는,

-상기 제 2 IoT 기기와 상기 제 2 IoT 기기를 관리하는 관리를 위한 접속시스템이 서로 접속하는 정량정보,

-상기 관리를 위한 접속시스템의 공시정보, 및

-상기 제 2 IoT 기기와 상기 관리를 위한 접속시스템 중 적어도 하나의 평판정보

중의 적어도 하나에 근거하여 산출되는 IoT 기기의 신뢰정보관리장치.

청구항 16

제 1 IoT 기기;

상기 제 1 IoT 기기가 연결하고자 하는 제 2 IoT 기기;

상기 제 2 IoT 기기를 관리하기 위하여 제공되는 적어도 하나의 관리를 위한 접속시스템;

상기 관리를 위한 접속시스템의 공시정보를 제공하는 공시정보제공자;

상기 관리를 위한 접속시스템 및 상기 제 2 IoT 기기 중의 적어도 하나의 평판정보를 제공하는 평판정보제공자; 및

상기 제 2 IoT 기기의 신뢰정도를 나타내는 신뢰지수를 산출하는 신뢰정보관리장치가 포함되는 신뢰에 기반하는 IoT 기기를 위한 협업시스템.

청구항 17

제 16 항에 있어서,

상기 신뢰지수는,

상기 제 2 IoT 기기와 상기 관리를 위한 접속시스템이 서로 접속하는 정량정보,

상기 관리를 위한 접속시스템의 공시정보,

상기 제 2 IoT 기기의 평판정보, 및

상기 관리를 위한 접속시스템의 평판정보

중의 적어도 하나에 근거하여 산출되는 신뢰에 기반하는 IoT 기기를 위한 협업시스템.

청구항 18

제 16 항에 있어서,

상기 신뢰정보관리장치로부터 상기 신뢰지수를 전달받아, 상기 제 1 IoT 기기의 제 2 IoT 기기에 대한 IP 주소 요청 시에, IP 주소와 함께 상기 신뢰지수를 제공하는 DNS 서버가 더 포함되는 신뢰에 기반하는 IoT 기기를 위한 협업시스템.

청구항 19

제 16 항에 있어서,

상기 신뢰정보관리장치로부터 상기 신뢰지수를 전달받아, 상기 제 1 IoT 기기의 제 2 IoT 기기에 대한 공개키 요청 시에, 상기 공개키와 함께 신뢰지수를 제공하는 인증시스템이 더 포함되는 신뢰에 기반하는 IoT 기기를 위한 협업시스템.

청구항 20

제 16 항에 있어서,

신뢰 프락시 노드가 더 포함되고,

상기 신뢰 프락시 노드는,

-상기 제 1 IoT 기기로부터 상기 제 2 IoT 기기로 전송되는 시그널링 메시지 및 데이터 패킷을 중간에서 가로채

고,

-상기 신뢰지수에 근거하여, 상기 제 2 IoT 기기와의 연결을 허가 또는 차단하는 것을 결정하는

작업을 수행하는 신뢰에 기반하는 IoT 기기를 위한 협업시스템.

청구항 21

제 16 항에 있어서,

상기 제 1 IoT 기기로부터의 요청과 무관하게, 상기 신뢰지수는 상기 신뢰정보관리장치로부터 주기적으로 업데이트 되어 상기 신뢰 프락시 노드에 보관될 수 있는 신뢰에 기반하는 IoT 기기를 위한 협업시스템.

청구항 22

제 16 항에 있어서,

상기 신뢰지수는 상기 제 1 IoT 기기로부터의 요청이 있을 때 상기 신뢰정보관리장치로부터 획득하는 신뢰에 기반하는 IoT 기기를 위한 협업시스템.

청구항 23

제 2 IoT 기기의 신뢰지수를 산출하기 위하여

-상기 제 2 IoT 기기와 상기 제 2 IoT 기기를 관리하는 적어도하나의 관리를 위한 접속시스템과의 접속정보를 획득하는 것,

-공시정보제공자로부터 상기 적어도 하나의 관리를 위한 접속시스템의 공시정보를 획득하는 것, 및

-평판정보제공자로부터, 상기 제 2 IoT 기기 및 상기 적어도 하나의 관리를 위한 접속시스템 중의 적어도 하나의 평판정보를 획득하는 것,

중의 적어도 하는 수행하는 제 1 단계;

상기 제 1 단계에서 획득된 정보를 이용하여 상기 제 2 IoT 기기의 신뢰지수를 얻는 제 2 단계; 및

상기 제 2 IoT 기기에 연결하고자 하는 제 1 IoT 기기의 요청에 응하여, 상기 신뢰지수를 제공하는 제 3 단계가 포함되는 신뢰에 기반하는 IoT 기기를 위한 협업방법.

청구항 24

제 23 항에 있어서,

상기 신뢰지수는, 상기 제 1 IoT 기기에 제공되는 신뢰에 기반하는 IoT 기기를 위한 협업방법.

청구항 25

제 23 항에 있어서,

상기 신뢰지수는, 상기 제 1 IoT 기기와 접속되는 DNS 서버에 제공되는 신뢰에 기반하는 IoT 기기를 위한 협업방법.

청구항 26

제 23 항에 있어서,

상기 신뢰지수는, 상기 제 1 IoT 기기와 접속되는 인증시스템에 제공되는 신뢰에 기반하는 IoT 기기를 위한 협업방법.

청구항 27

제 23 항에 있어서,

상기 신뢰지수는, 상기 제 1 IoT 기기와 접속되고, 상기 제 2 IoT 기기와 접속되는 신뢰 프락시 노드에 제공되는 신뢰에 기반하는 IoT 기기를 위한 협업방법.

청구항 28

제 1 IoT 기기;

상기 제 1 IoT 기기가 연결하고자 하는 제 2 IoT 기기;

상기 제 2 IoT 기기의 신뢰정도를 나타내는 신뢰지수를 산출하는 신뢰정보관리장치; 및

상기 신뢰정보관리장치로부터 제공되는 신뢰지수를 제공하는 DNS 서버가 포함되는 신뢰에 기반하는 IoT 기기를 위한 협업시스템.

청구항 29

제 2 IoT 기기의 신뢰지수를 산출하여 DNS 서버에 저장하는 것;

상기 제 2 IoT 기기에 연결하고자 하는 제 1 IoT 기기가 상기 제 2 IoT 기기의 IP 정보를 상기 DNS 서버에 요청하는 것; 및

상기 DNS 서버가, 상기 제 1 IoT 기기의 요청에 응하여, 상기 신뢰지수와 상기 제 2 IoT 기기의 IP 정보를 제공하는 것이 포함되는 신뢰에 기반하는 IoT 기기를 위한 협업방법.

청구항 30

제 1 IoT 기기;

상기 제 1 IoT 기기가 연결하고자 하는 제 2 IoT 기기;

상기 제 2 IoT 기기의 신뢰정도를 나타내는 신뢰지수를 산출하는 신뢰정보관리장치; 및

상기 신뢰정보관리장치로부터 제공되는 신뢰지수를 제공하는 인증시스템이 포함되는 신뢰에 기반하는 IoT 기기를 위한 협업시스템.

청구항 31

제 2 IoT 기기의 신뢰지수를 산출하여 인증시스템에 저장하는 것;

상기 제 2 IoT 기기에 연결하고자 하는 제 1 IoT 기기가 상기 제 2 IoT 기기의 공개키를 상기 인증시스템에 요청하는 것; 및

상기 인증시스팀에, 상기 제 1 IoT 기기의 요청에 응하여, 상기 신뢰지수와 상기 제 2 IoT 기기의 공개키를 제공하는 것이 포함되는 신뢰에 기반하는 IoT 기기를 위한 협업방법.

청구항 32

제 1 IoT 기기;

상기 제 1 IoT 기기가 연결하고자 하는 제 2 IoT 기기;

상기 제 2 IoT 기기의 신뢰정도를 나타내는 신뢰지수를 산출하는 신뢰정보관리장치; 및

상기 제 1 IoT 기기에 접속되는 신뢰 프락시 서버가 포함되고,

상기 신뢰 프락시 서버는,

-상기 제 1 IoT 기기로부터 상기 제 2 IoT 기기로 전송되는 시그널링 메시지 또는 데이터 패킷을 중간에서 가로채고,

-상기 신뢰지수에 근거하여 상기 제 2 IoT 기기와의 연결을 허가 또는 차단하는 것을 결정하는, 신뢰에 기반하는 IoT 기기를 위한 협업시스템.

청구항 33

신뢰정보관리장치가 제 2 IoT 기기의 신뢰지수를 산출하는 것;

제 1 IoT 기기가 상기 제 2 IoT 기기로 연결을 요청하는 것;

상기 제 1 IoT 기기로부터 상기 제 2 IoT 기기로 전송되는 시그널링 메시지 및 데이터 패킷을, 신뢰 프락시 노드가 중간에서 가로채는 것; 및

상기 신뢰 프락시 노드가 상기 신뢰지수에 근거하여 상기 제 2 IoT 기기와의 연결을 허가 또는 차단하는 것을 결정하는 것이 포함되는 신뢰에 기반하는 IoT 기기를 위한 협업방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 IoT 기기의 신뢰정보를 이용하는 협업장치 및 협업방법으로서, 더 구체적으로는 IoT 기기의 신뢰지수 산출장치, IoT 기기의 신뢰지수산출방법, IoT 기기의 신뢰정보관리장치, IoT 기기의 신뢰정보관리방법, 신뢰에 기반하는 IoT 기기를 위한 협업시스템, 및 신뢰에 기반하는 IoT 기기의 협업방법에 관한 것이다.

배 경 기 술

[0002] 스마트홈, 스마트빌딩, 스마트시티, 및 커넥티트카 등 수 많은 IoT(Internet of Things) 및 CPS(Cyber-Physical-System) 응용 서비스들이 상용화 단계에 이르고 있다. 상기 IoT 및 상기 CPS 환경에서, 사람, 사물, 및 서비스/응용 간의 원활한 상호 작용 및 협력을 위해서는 각 개체들 간의 신뢰(trust)가 전제되어야 한다. IoT 및 CPS의 본질은 연결에 있기 때문에, 연결 대상에 대한 신뢰는, 이러한 IoT 기반 산업 및 서비스들의 활성화를 위한 필수 조건이라 할 수 있다.

[0003] IoT 시스템에서 제공되는 응용 서비스와 연결 대상에 대한 신뢰 측정, 분석, 검증 방안이 존재하지 않는다면, IoT 서비스 확산은 요원한 일이 될 것이다. 그럼에도 불구하고, IoT를 구성하는 다양한 사물의 신뢰, 이들이 형성하고 있는 관계에 대한 신뢰에 대한 연구개발은 아직 초기단계이다. 예를 들어, 본 발명의 발명자가 개시한 특허등록번호 10-1883397호, '신뢰 기반 콘텐츠 공유 장치 및 방법'에는 콘텐츠의 공유시에 콘텐츠의 신뢰수준을 활용하는 것을 제안하고 있다.

[0004] 한편, 소셜 네트워크 및 소셜 미디어는 급격히 성장하고 있으며, 사용자가 가지는 생각을, 문자(예 : Twitter), 멀티미디어(예 : YouTube), 개인 활동, 정보(예 : Facebook), 문서, 및 캘린더(예 : Google+)로 공유할 수 있도록 하는 다양한 서비스들이 제공되고 있다.

[0005] 이들 소셜 네트워크 서비스는 사용자들이 쉽게 상호 통신하고 관심있는 콘텐츠를 용이하게 공유할 수 있는 환경을 제공함으로써, 사용자의 웹 참여를 크게 높여 주었으며, 사람들의 행동, 태도, 상호 작용 및 관계를 변화시키고 있다. 이러한, 소셜 네트워크는 일반적으로 사용자 프로필과 사용자 관계의 다양한 속성, 즉 사람과 사람 사이 및 사람과 콘텐츠 사이의 다양한 속성을 그안에 포함한다.

[0006] 나아가서, SIoT(Social Internet of Things)는 사람과 비슷한 모습으로 기기들 간에 소통하고 정보를 제공할 수 있는 형태를 띤다. 전통적인 소셜 네트워크에서의 소셜 분석 기술은 중요한 요소 기술 중 하나였고 많은 연구가 이루어졌으나, 사람 기반 소셜 네트워크 분석을 사물 기반 소셜 네트워크에 그대로 적용하는 데는 한계가 있다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 특허등록번호 10-1883397호, '신뢰 기반 콘텐츠 공유 장치 및 방법'

발명의 내용

해결하려는 과제

[0008] 본 개시는 IoT기기 간의 연결에 있어서 신뢰정보를 활용하는 장치 및 방법을 제공한다.

과제의 해결 수단

[0009] 본 발명에 따른 IoT 기기의 신뢰지수산출장치에는, IoT 기기와 상기 IoT 기기를 관리하는 관리를 위한 접속시스템이, 서로 간에 접속하는 양과 관련되는 정량정보를 처리하는 제 1 신뢰관련정보산출부; 상기 IoT 기기와 상기

관리를 위한 접속시스템 각각의 정성정보, 및 상기 IoT 기기와 상기 관리를 위한 접속시스템 각각의 정량정보, 중의 적어도 하나를 처리하는 제 2 신뢰관련정보산출부; 및 상기 제 1 신뢰관련정보산출부와 상기 제 2 신뢰관련정보산출부의 신뢰관련정보를 종합하여, 상기 IoT 기기의 신뢰지수를 산출하는 종합신뢰지수산출부가 포함된다. 본 발명에 따르면, IoT 기기의 신뢰지수를 보다 정확하게 얻어낼 수 있다.

[0010] 상기 제 1 신뢰관련정보산출부에서 처리되는 정량정보에는, 상기 IoT 기기와 상기 관리를 위한 접속시스템이 서로 접속하는 접속시간, 접속횟수, 및 접속빈도 중의 적어도 하나는 포함될 수 있고, 이 외에도 많은 정보가 더 포함될 수 있다.

[0011] 상기 제 2 신뢰관련정보산출부로 신뢰관련정보를 제공하기 위하여, 공시정보를 처리하는 제 3 신뢰관련정보산출부; 및 평판정보를 처리하는 제 4 신뢰관련정보산출부가 더 포함될 수 있다.

[0012] 상기 공시정보에는, 상기 관리를 위한 접속시스템의 회사채등급과 신용등급 중의 적어도 하나는 포함되는 정성정보가 활용될 수 있다.

[0013] 상기 평판정보에는, 평판자의 진실성 및 평판자의 수 중의 적어도 하나는 포함되는, 정량정보 및 정성정보가 활용될 수 있다.

[0014] 상기 관리를 위한 접속시스템에는, 상기 제조사시스템, 소유자시스템, 관리자시스템, Cloud시스템, 및 IoT플랫폼 중의 적어도 하나는 포함될 수 있다.

[0015] 본 발명에 따른 IoT 기기의 신뢰지수산출방법에는, IoT 기기와 상기 IoT 기기를 관리하는 관리를 위한 접속시스템과의 접속상태정보를 입수하여 정량정보를 획득하는 것, 및 상기 관리를 위한 접속시스템의 공시정보와, 상기 IoT 기기와 상기 관리를 위한 접속시스템 중의 적어도 하나의 평판정보를 통하여 정량정보 및 정성정보를 획득하는 것을 포함하는 제 1 단계; 및 상기 제 1 단계에서 획득된 정량정보 및 정성정보를 종합하여 상기 IoT 기기의 신뢰지수를 산출하는 제 2 단계가 포함될 수 있다.

[0016] 여기서, 상기 공시정보에는, 상기 관리를 위한 접속시스템의 회사채등급과 신용등급 중의 적어도 하나는 포함되는 정성정보가 활용될 수 있고, 상기 평판정보에는, 평판자의 진실성 및 평판자의 수 중의 적어도 하나는 포함되는 정량정보 및 정성정보가 활용될 수 있고, 상기 관리를 위한 접속시스템에는, 상기 제조사시스템, 소유자시스템, 관리자시스템, Cloud시스템, 및 IoT플랫폼 중의 적어도 하나는 포함될 수 있다.

[0017] 본 발명에 따른 IoT 기기의 신뢰정보관리장치에는, 외부의 정보를 이용하여 IoT 기기의 신뢰정도를 나타내는 신뢰지수를 산출하는 신뢰지수산출부; 상기 신뢰지수가 포함되는 정보를 저장하는 메모리; 외부의 노드들과의 입출력을 담당하는 통신부; 및 상기 신뢰지수를 메모리로부터 독출하여 통신부를 통하여 외부로 출력하는 제어부가 포함되어, 필요한 곳으로 신속하게 신뢰지수관련 정보를 알려줄 수 있다.

[0018] 본 발명에 따른 IoT 기기의 신뢰정보관리방법에는, 제 2 IoT 기기의 신뢰할 수 있는 정도를 나타내는 신뢰지수를 산출하여 메모리에 저장하는 단계; 및 제 1 IoT 기기로부터 요청이 있을 때, 상기 제 2 IoT 기기의 신뢰지수를 독출하여 출력하는 단계가 포함되어, 네트워크 상의 필요한 장소에 신속히 신뢰지수관련 정보를 제공할 수 있다.

[0019] 본 발명에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템에는, 제 1 IoT 기기; 상기 제 1 IoT 기기가 연결하고자 하는 제 2 IoT 기기; 상기 제 2 IoT 기기를 관리하기 위하여 제공되는 적어도 하나의 관리를 위한 접속시스템; 상기 관리를 위한 접속시스템의 공시정보를 제공하는 공시정보제공자; 상기 관리를 위한 접속시스템 및 상기 제 2 IoT 기기 중의 적어도 하나의 평판정보를 제공하는 평판정보제공자; 및 상기 제 2 IoT 기기의 신뢰정도를 나타내는 신뢰지수를 산출하는 신뢰정보관리장치가 포함될 수 있다.

[0020] 본 발명에 따른 신뢰에 기반하는 IoT 기기를 위한 협업방법에는, 제 2 IoT 기기의 신뢰지수를 산출하기 위하여 -상기 제 2 IoT 기기와 상기 제 2 IoT 기기를 관리하는 적어도하나의 관리를 위한 접속시스템과의 접속정보를 획득하는 것, -공시정보제공자로부터 상기 적어도 하나의 관리를 위한 접속시스템의 공시정보를 획득하는 것, 및 -평판정보제공자로부터, 상기 제 2 IoT 기기 및 상기 적어도 하나의 관리를 위한 접속시스템 중의 적어도 하나의 평판정보를 획득하는 것, 중의 적어도 하는 수행하는 제 1 단계; 상기 제 1 단계에서 획득된 정보를 이용하여 상기 제 2 IoT 기기의 신뢰지수를 얻는 제 2 단계; 및 상기 제 2 IoT 기기에 연결하고자 하는 제 1 IoT 기기의 요청에 응하여, 상기 신뢰지수를 제공하는 제 3 단계가 포함될 수 있다.

[0021] 본 발명에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템에는, 제 1 IoT 기기; 상기 제 1 IoT 기기가 연결하고자 하는 제 2 IoT 기기; 상기 제 2 IoT 기기의 신뢰정도를 나타내는 신뢰지수를 산출하는

신뢰정보관리장치; 및 상기 신뢰정보관리장치로부터 제공되는 신뢰지수를 제공하는 DNS 서버가 포함될 수 있다.

[0022] 본 발명에 따른 신뢰에 기반하는 IoT 기기를 위한 협업방법에는, 제 2 IoT 기기의 신뢰지수를 산출하여 DNS 서버에 저장하는 것; 상기 제 2 IoT 기기에 연결하고자 하는 제 1 IoT 기기가 상기 제 2 IoT 기기의 IP 정보를 상기 DNS 서버에 요청하는 것; 및 상기 DNS 서버가, 상기 제 1 IoT 기기의 요청에 응하여, 상기 신뢰지수와 상기 제 2 IoT 기기의 IP 정보를 제공하는 것이 포함될 수 있다.

[0023] 본 발명에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템에는, 제 1 IoT 기기; 상기 제 1 IoT 기기가 연결하고자 하는 제 2 IoT 기기; 상기 제 2 IoT 기기의 신뢰정도를 나타내는 신뢰지수를 산출하는 신뢰정보관리장치; 및 상기 신뢰정보관리장치로부터 제공되는 신뢰지수를 제공하는 인증시스템이 포함될 수 있다.

[0024] 본 발명에 따른 신뢰에 기반하는 IoT 기기를 위한 협업방법에는, 제 2 IoT 기기의 신뢰지수를 산출하여 인증시스템에 저장하는 것; 상기 제 2 IoT 기기에 연결하고자 하는 제 1 IoT 기기가 상기 제 2 IoT 기기의 공개키를 상기 인증시스템에 요청하는 것; 및 상기 인증시스팀에, 상기 제 1 IoT 기기의 요청에 응하여, 상기 신뢰지수와 상기 제 2 IoT 기기의 공개키를 제공하는 것이 포함될 수 있다.

[0025] 본 발명에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템에는, 제 1 IoT 기기; 상기 제 1 IoT 기기가 연결하고자 하는 제 2 IoT 기기; 상기 제 2 IoT 기기의 신뢰정도를 나타내는 신뢰지수를 산출하는 신뢰정보관리장치; 및 상기 제 1 IoT 기기에 접속되는 신뢰 프락시 서버가 포함되고, 상기 신뢰 프락시 서버는, -상기 제 1 IoT 기기로부터 상기 제 2 IoT 기기로 전송되는 시그널링 메시지 및 데이터 패킷을 중간에서 가로채고, -상기 신뢰정보관리장치로부터 상기 신뢰지수를 획득하고, -상기 제 2 IoT 기기와의 연결을 허가 또는 차단하는 것을 결정한다.

[0026] 본 발명에 따른 신뢰에 기반하는 IoT 기기를 위한 협업방법에는, 신뢰정보관리장치가 제 2 IoT 기기의 신뢰지수를 산출하는 것; 제 1 IoT 기기가 상기 제 2 IoT 기기로 연결을 요청하는 것; 상기 제 1 IoT 기기로부터 상기 제 2 IoT 기기로 전송되는 시그널링 메시지 및 데이터 패킷을, 신뢰 프락시 노드가 중간에서 가로채는 것; 상기 신뢰 프락시 노드가 상기 신뢰정보관리장치로부터 상기 신뢰지수를 획득하는 것; 및 상기 신뢰 프락시 노드가 상기 제 2 IoT 기기와의 연결을 허가 또는 차단하는 것을 결정하는 것이 포함될 수 있다.

발명의 효과

[0027] 본 발명에 따르면, IoT기기의 정확한 신뢰지수를 얻어낼 수 있고, 상기 신뢰지수를 정확히 관리하여, 신뢰지수가 필요한 곳에 제공할 수 있고, 신뢰지수가 필요한 다양한 곳에 편리하게 제공할 수 있다.

[0028] 본 발명에 따르면, 신뢰에 바탕하여 IoT기기가 연결될 수 있기 때문에, 원활한 네트워크 연결을 유도하여 정보의 신속한 흐름을 촉진시킬 수 있다.

도면의 간단한 설명

[0029] 도 1은 제 1 실시예에 따른 신뢰에 기반하는 IoT 기기를 위한 협업 시스템의 구성도.

도 2는 신뢰정보관리장치의 구성도.

도 3은 신뢰지수산출장치의 상세구성도.

도 4는 제 2 실시예에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템의 구성도.

도 5는 제 3 실시예에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템의 구성도.

도 6은 제 4 실시예에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템의 구성도.

발명을 실시하기 위한 구체적인 내용

[0030] 이하에서는 도면을 참조하여 본 발명의 구체적인 실시예를 상세하게 설명한다. 본 발명의 사상은 이하의 실시예에 제한되지 아니하고 본 발명의 사상을 이해하는 당업자는 동일한 사상의 범위내에 포함되는 다른 실시예를 구성요소의 부가, 변경, 삭제, 및 추가 등에 의해서 용이하게 제안할 수 있을 것이나 이 또한 본 발명 사상의 범위 내에 포함된다.

[0031] 이하의 실시예에 포함되는 개시 내용에 있어서, IoT 기기는 물리 IoT(Internet Of things) 및 소프트웨어로 구

성되는 가상 IoT를 포함하는 개념으로서, 네트워크 상의 연결되어 상호 작용이 수행될 수 있는 모든 노드를 말할 수 있다.

[0033] <제 1 실시예>

[0034] 도 1은 신뢰에 기반하는 IoT 기기를 위한 협업 시스템의 구성도를 나타낸다.

[0035] 도 1을 참조하면, 제 1 IoT 기기(101)과 제 2 IoT 기기(102)는 하드웨어를 갖는 물리적인 IoT 기기이거나 소프트웨어로만 구성된 가상의 IoT 기능일 수 있다. 도 1에서는, 상기 제 1 IoT 기기(101)가 자기의 필요에 의해서 제 2 IoT 기기(102)에 접속하는 상황을 예시적으로 보인다.

[0036] 상기 IoT 기기(101)(102)는, 각각의 제조사, 소유자가 존재하고, 별도의 장치 관리자가 존재할 수 있다. 상기 제조사, 소유자, 장치 관리자는, 자기와 연관되는 IoT 기기(도 1에서는 제 2 IoT 기기(102)를 예시한다)에 접속하여 상호 작용을 수행한다. 이를 위하여 IoT 기기 소프트웨어 업그레이드 등을 위한 제조사 시스템(111), IoT 기기를 제어 및 관리하는 스마트폰, 및 PC 등의 소유자시스템(112), 경우에 따라 소유자와는 별도의 장치 관리자가 운영하는 관리자시스템(113)이 포함될 수 있다. 뿐만 아니라, 상기 IoT 기기(101)(102)를 운영 관리하는 IoT플랫폼(115)에 연결되어, 상기 IoT 기기로부터 수집된 데이터를 IoT플랫폼으로 전송할 수도 있고, Cloud 시스템(114)으로 전달할 수도 있다.

[0037] 상기 제 2 IoT 기기(102)는 자기가 관리되기 위하여, 관리를 위한 접속시스템에 포함되는 각 시스템 및 플랫폼(111)(112)(113)(114)(115)에 접속하여 필요한 관리를 받을 수 있다.

[0038] 한편, 인터넷 상에는 기업들의 규모 및 매출 등의 공시정보사이트가 존재하며, 기업들의 신용정보를 제공하는 신용정보사이트가 공시정보제공자(121)로서 존재한다. 뿐만 아니라, 페이스북, 트위터, 및 링크드인 등의 소셜 네트워크서비스가 평판정보제공자(122)로서 존재하고, 이들은 기업, IoT 기기, 및 서비스에 대한 많은 평판 정보들을 보유하고 가시화한다.

[0039] 상기 공시정보제공자(121) 및 상기 평판정보제공자(122)는, 상기 관리를 위한 접속시스템(111)(112)(113)(114)(115)의 기업, 당 기업의 서비스, 및 당 기업의 IoT 기기 등의 공시정보와 평판정보를 제공한다.

[0040] 제 1 실시예에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템에는 신뢰정보관리장치(131)가 포함된다. 상기 신뢰정보관리장치(131)는 IoT 기기의 신뢰와 관련되는 다양한 정보를 관리하는 신뢰정보관리장치로 작동할 수 있고, 이후에는 약언하여 신뢰정보관리장치(131)로 기술한다.

[0041] 상기 신뢰정보관리장치(131)는 상기 제 2 IoT 기기(102)와 상기 관리를 위한 접속시스템과의 통신 시간 및 횟수 등의 정보를 획득할 수 있다. 상기 관리를 위한 접속시스템에는, 제조사시스템(111), 소유자시스템(112), 관리자시스템(113), Cloud시스템(114), 및 IoT플랫폼(115)등이 포함되는 것을 설명한 바가 있다.

[0042] 상기 제 2 IoT 기기(102)가 상기 관리를 위한 접속시스템에 자주 그리고 오랜 시간 동안 접속하면, 상기 제 2 IoT 기기(102)는 충실히 관리되는 기기로서, 외부로부터의 침입이 없고 악성정보가 포함되지 않은 등 신뢰가 높을 수 있다. 따라서, 이 경우에 상기 신뢰정보관리장치는 상기 제 2 IoT 기기(102)의 신뢰도가 높은 것으로 판단할 수 있다. 반대의 경우는 반대로 판단할 수 있다.

[0043] 상기 신뢰정보관리장치(131)는 기업 공시정보 및 기업신용정보 웹사이트(공시정보제공자라고 할 수 있다)로부터 제 2 IoT 기기(102)에 대한 제조사, 소유자, 관리자, IoT플랫폼, 및 Cloud시스템 등에 관련된 기업 규모, 매출, 부채 등에 대한 공시정보를 획득할 수 있다. 상기 신뢰정보관리장치(131)는 페이스북, 트위터, 링크드인 등의 소셜네트워크서비스(SNS)를 통해서 제조사, 소유자, 관리자, 사용자, 및 Cloud 시스템(평판정보제공자라고 할 수 있다) 등에 대한 평판정보를 획득할 수 있다.

[0044] 상기 공시정보 및 상기 평판정보를 바탕으로 상기 제 2 IoT 기기(102)의 신뢰를 좋거나 나쁘게 판단할 수 있다. 예를 들어 상기 공시정보를 통하여 기업의 부채가 높으면 관련하는 IoT 기기의 신뢰를 낮게 판단할 수 있고, 상기 평탄정보를 통하여 평판이 낮으면 관련하는 IoT 기기의 신뢰를 낮게 판단할 수 있다. 상기 공시정보 및 상기 평판정보와 신뢰도의 관계는 협업방법의 설명에서 더 구체적으로 설명된다.

[0045] 상기 신뢰정보관리장치(131)는, 제 2 IoT 기기(102)와 관리를 위한 접속시스템(111~115 등)과의 접속정보와, 상기 공시정보, 및 상기 평판정보들을 바탕으로, 상기 제 2 IoT 기기(102)에 대한 신뢰지수(trust index)를 분석

및 관리할 수 있다. 상기 신뢰정보관리장치(131)는 주기적으로 신뢰지수(trust index)를 분석 및 관리할 수 있다.

[0046] 상기 제 1 IoT 기기(101)의 요청이 있을 때 상기 제 2 IoT 기기(102)의 신뢰정보를 알려줄 수 있고, 상기 제 1 IoT 기기(101)는 신뢰정보를 근거로 하여 접속할지 말지를 결정할 수 있다. 예를 들어 상기 신뢰지수가 일정의 임계치 이상일 때에만 접속하는 것으로 결정할 수 있다.

[0047] 도 2는 상기 신뢰정보관리장치의 구성을 보이는 도면이다.

[0048] 상기 신뢰정보관리장치(131)에는, 외부정보를 이용하여 신뢰지수를 산출하는 신뢰지수산출부(1312), 산출된 신뢰지수 등의 필요정보를 저장하는 메모리(1313)와, 외부의 노드들과의 입출력을 담당하는 통신부(1314), 및 각 구성요소들을 제어하는 제어부(1311)가 포함될 수 있다.

[0049] 상기 제어부(1311)는 신뢰지수의 재산정 주기를 결정할 수 있고, 현재 신뢰지수를 메모리로부터 독출하여 통신부(1314)를 통하여 외부로 알릴 수 있다. 그외에, 신뢰정보관리장치(131)의 동작에 필요한 다수의 작용을 수행할 수 있다.

[0050] 상기 신뢰지수산출부(1312)는, 상기 제 2 IoT 기기(102)와 상기 관리를 위한 접속시스템과의 접속정보가 포함되는 제 1 입력과, 상기 공시정보와 상기 평판정보가 포함되는 제 2 입력을 받아들여 신뢰지수를 산출할 수 있다.

[0051] 상기 제 1 입력은 정량적인 정보로서 상기 제 2 IoT 기기(102)와 상기 관리를 위한 접속시스템이 많이 접속하느냐 적게 접속하느냐에 따라서 신뢰정보가 영향을 받을 수 있다. 상기 제 2 입력은 주로 정성적인 정보로서 공시정보 및 평판정보로서 주어질 수 있다.

[0052] 도 2를 참조하여 신뢰정보관리방법을 설명한다.

[0053] 상기 신뢰지수산출부(1312)는, 상기 제 2 IoT 기기(102)와 상기 관리를 위한 접속시스템과의 접속정보가 포함되는 제 1 입력과, 상기 공시정보와 상기 평판정보가 포함되는 제 2 입력을 받아들여 신뢰지수를 산출할 수 있다. 산출된 신뢰지수는 상기 메모리(1313)에 저장될 수 있다.

[0054] 상기 제어부(1311)는 상기 신뢰지수의 재산정 주기를 결정할 수 있고, 상기 신뢰지수산출부(1312)에 지시하여 신뢰지수를 재산정하도록 지시할 수 있다. 상기 신뢰지수는 외부의 요청에 의해서 재산정될 수도 있다.

[0055] 상기 통신부(1314)를 통하여 요청이 있을 때, 상기 메모리(1313)에 저장된 정보는, 제어부(1311)의 호출에 의해서 통신부(1314)를 통하여 외부로 출력될 수 있다.

[0056] 상기 제 1 입력은 정량적인 정보로서 상기 제 2 IoT 기기(102)와 상기 관리를 위한 접속시스템이 많이 접속하느냐 적게 접속하느냐에 따라서 신뢰정보가 영향을 받을 수 있다. 상기 제 2 입력은 주로 정성적인 정보로서 공시정보 및 평판정보로서 주어질 수 있다.

[0057] 이를 위하여 상기 신뢰지수산출부(1312)는 도 3에 제시되는 바와 같은 상세구성을 가질 수 있다. 상기 신뢰지수산출부는 IoT 기기의 신뢰지수산출장치로 작동할 수 있다.

[0058] 도 3을 참조하면, 상기 IoT 기기의 신뢰지수산출장치에는, 접속시간 및 접속량 등의 정량적인 정보를 처리하는 제 1 신뢰관련정보산출부(1315), 정성적인 정보와 정량적인 정보를 처리하는 제 2 신뢰관련정보산출부(1316), 상기 제 1 신뢰관련정보산출부(1315)와 상기 제 2 신뢰관련정보산출부(1316)의 신뢰정보를 종합하여 신뢰지수를 산출하여 출력하는 종합신뢰지수산출부(1319)가 포함될 수 있다.

[0059] 또한, 상기 제 2 신뢰관련정보산출부(1316)로 입력되는 서로 다른 성격의 정보로서, 공시정보를 처리하는 제 3 신뢰관련정보산출부(1317)와, 평판정보를 처리하는 제 4 신뢰관련정보산출부(1318)가 포함될 수 있다. 상기 공시정보는 정성정보이고, 상기 평판정보는 정성정보 및 정량정보의 성격을 함께 가질 수 있다. 각 정보는 상기 제 2 신뢰관련정보산출부(1316)로 입력되어 정성정보 및 정량정보의 성격을 함께 가질 수 있다.

[0060] 상기 IoT 기기의 신뢰지수산출장치에 근거하는 IoT 기기의 신뢰지수산출방법에 대하여 설명한다.

[0061] 상기 제 1 신뢰관련정보산출부(1315)는 상기 제 1 입력의 정량적인 정보가 입력될 수 있다. 상기 제 1 신뢰관련정보산출부(1315)는 다수의 상기 관리를 위한 접속시스템과 제 2 IoT 기기(102)의 접속상태로부터 정보를 입수하여 정량적인 처리(예를 들어, 합산)를 통하여 신뢰관련정보를 산출할 수 있다. 예를 들어, 상기 제 2 IoT 기기(102)가, 상기 제조사시스템(111), 소유자시스템(112), 관리자시스템(113), Cloud시스템(114), 및 IoT플랫폼(115) 등에 자주 오랜 시간 접속하면, 그 접속시간을 합산하여 상기 제 2 IoT 기기(102)가 신뢰가 높은 것으로

판단할 수 있다. 물론, 반대는 반대의 경우로 판단할 수 있다.

[0062] 상기 제 3 신뢰관련정보산출부(1317)는 공시정보로서 매출과 부채와 회사채등급과 신용등급 등의 정성정보를 활용할 수 있고, 상기 제 4 신뢰관련정보산출부(1318)는 평판정보로서 평판자의 진실성, 및 평판자의 수 등과 같은 정량 및 정성정보를 함께 활용할 수 있다.

[0063] 상기 제 3 신뢰관련정보산출부(1317)와 상기 제 4 신뢰관련정보산출부(1318)의 출력정보는 상기 제 2 신뢰관련정보산출부(1316)로 제공되어 정량/정성적인 정보로 가공된다.

[0064] 상기 종합신뢰지수산출부(1319)는 상기 제 1 신뢰관련정보산출부(1315)와 상기 제 2 신뢰관련정보산출부(1316)의 신뢰정보를 종합하여 신뢰지수를 산출하여 출력할 수 있다.

[0065] 한편, 도 3에 있어서 정성정보 및 정량정보는 각 처리부에서의 주된 처리방식이 바람직하게 예시되는 것으로서, 어느 하나의 처리방법이 수행되고 다른 처리방법이 수행되지 않는 것을 완전히 배제하지는 않는다.

[0066] 다시 도 1을 참조하여, 제 1 실시예에 따른 신뢰에 기반하는 IoT 기기의 협업방법을 설명한다. 도 1에서 괄호안의 번호는 본 협업방법의 각 스텝을 설명한다.

[0067] 도 1을 참조하면, 제 2 IoT 기기(102)는 소프트웨어 업그레이드 등을 위해 제조사시스템(111)에 주기적으로 접속할 수 있다. 상기 제 2 IoT 기기(102)의 소유자는 자신의 스마트폰 또는 PC 등의 소유자시스템(112)을 통해서 제 2 IoT 기기(102)에 접속해서 이용하거나 제 2 IoT 기기(102)로부터 전달되는 데이터를 획득할 수 있다. 소유자와는 별도로 제 2 IoT 기기(102)에 대한 관리자가 존재할 수 있으며, 이 경우 관리자는 자신의 PC 및 서버 등의 관리자시스템(113)을 통해 제 2 IoT 기기(102)에 접속하여 상태 확인 등 운영관리를 수행할 수 있다. 제 2 IoT 기기(102)로부터 수집되는 데이터 등은 Cloud시스템(114) 또는 IoT플랫폼(115)등으로 전달될 수 있으며, 상기 Cloud시스템 및 상기 IoT플랫폼은 제 2 IoT 기기(102)에 대한 상태 관리 등을 수행할 수 있다.

[0068] 상기 신뢰정보관리장치(131)는 제 2 IoT 기기(102)와 상기 관리를 위한 접속시스템과의 통신 시간 및 횟수 등의 정보를 획득할 수 있다(Step 1).

[0069] 상기 관리를 위한 접속시스템에는, 제조사시스템(111), 소유자시스템(112), 관리자시스템(113), Cloud시스템(114), 및 IoT플랫폼(115)등이 포함될 수 있다.

[0070] 상기 신뢰정보관리장치(131)는 기업 공시정보 및 기업신용정보 웹사이트로부터 제 2 IoT 기기(102)에 대한 제조사, 관리자, IoT플랫폼, 및 Cloud시스템 등에 관련된 기업 규모, 매출, 부채 등에 대한 정보를 획득할 수 있다. 또한 페이스북, 트위터, 링크드인 등의 소셜네트워크서비스(SNS)를 통해서 제조사, 관리자, 사용자 및 Cloud 시스템 등에 대한 평판 정보를 획득할 수 있다(Step 2).

[0071] 상기 신뢰정보관리장치(131)는 상기 Step 1과 Step 2를 통하여 획득한 정보로부터, 평판이 좋고, 매출이 많고, 기업신용도가 높은 제조사이면 제 2 IoT 기기(102)의 신뢰지수를 증가시킬 수 있다(예, 1~5단계 중 5단계). 만약 반대의 경우이면 신뢰지수를 감소시킬 수 있다(예, 1~5단계 중 1단계).

[0072] 마찬가지 방식으로 소유자, 관리자, Cloud시스템, 및 IoT플랫폼에 대한 평판, 매출, 및 기업신용도 등을 바탕으로 제 2 IoT 기기(102)의 신뢰지수를 설정할 수 있다. 상기 신뢰지수는 고정된 것이 아니며, 제조사, 관리자 등의 상기 공시정보의 변경 및 상기 평판정보의 변경 등과 연계하여 업데이트될 수 있다. 바람직하게는 정하여진 소정의 주기로 업데이트되는 것이 바람직하다.

[0073] 또한, 상기 신뢰정보관리장치(131)는 제 2 IoT 기기와 제조사시스템(111), 소유자시스템(112), 관리자시스템(113), Cloud시스템(114), 및 IoT플랫폼(115) 간의 통신 빈도를 파악하여, 통신 빈도가 높으면, 제 2 IoT 기기가 제대로 관리되고 있는 것으로 판단하여 제 2 IoT 기기(102)에 대한 신뢰지수를 증가시킬 수 있다. 반대로 통신 빈도가 기준치 이하로 낮아지면 해당 제 2 IoT 기기(102)가 제대로 보안업데이트되거나 관리되지 않는 것으로 판단하여 신뢰지수를 낮출 수 있다.

[0074] 상기 신뢰정보관리장치(131)는 상기 과정을 통해서 도출되는 제 2 IoT 기기(102)에 대한 신뢰지수를 유지 및 관리할 수 있다. 상기 제 2 IoT 기기와 상기 관리를 위한 접속시스템과의 접속은, 접속빈도, 접속시간, 및 접속횟수 외에, 다른 방식에 의해서 평가될 수도 있을 것이다.

[0075] 상기 신뢰정보관리장치(131)에 의해서 IoT 기기의 신뢰지수가 관리되는 중에, 상기 제 1 IoT 기기(101)로부터 제 2 IoT 기기(102)에 대한 신뢰지수요청이 전달되면, 유지 관리하고 있는 제 2 IoT 기기(102)에 대한 신뢰지수를 제 1 IoT 기기(101)에게 제공한다(Step 3).

[0076] 상기 제 1 IoT 기기(101)는 신뢰정보관리장치(131)로부터 전달받은 신뢰지수를 참조하여 제 2 IoT 기기(102)로의 접속과 협력 수행 여부를 결정할 수 있다. 예를 들어, 상기 제 1 IoT 기기(101)는 자체 내에 설정되어 있는 신뢰기준치와 제 2 IoT 기기(102)의 신뢰지수를 비교한 후에, 적합한 수치 범위 내에 있을 때에만 상기 제 2 IoT 기기(102)로의 접속 및 협력을 수행할 수 있다.

[0077] 제 1 실시예에 개시되는, IoT 기기의 신뢰지수산출장치, IoT 기기의 신뢰지수산출방법, IoT 기기의 신뢰정보관리장치, IoT 기기의 신뢰정보관리방법, 신뢰에 기반하는 IoT 기기를 위한 협업시스템, 및 신뢰에 기반하는 IoT 기기의 협업방법은 개별 IoT 기기가 직접 IoT 기기의 신뢰정보관리장치에 접속하여 정보를 획득하는 것으로 설명한다.

[0078] 본 개시는 상기 IoT 기기가 상기 IoT 기기의 신뢰정보관리장치에 직접 접속하는 경우로 제한되지 아니하고, 구체적인 구현예에 따라서 다양한 다른 실시예를 가질 수 있다. 이하의 모든 실시예는 상기 IoT 기기와 상기 IoT 기기의 신뢰정보관리장치와의 접속관점이 제 1 실시예와 달라지는 것이고, 그 외에 구체적인 설명이 없는 부분은 제 1 실시예의 구성이 그대로 적용될 수 있다.

[0079] 예를 들어, IoT 기기의 신뢰지수산출장치, IoT 기기의 신뢰지수산출방법, IoT 기기의 신뢰정보관리장치, 및 IoT 기기의 신뢰정보관리방법은 도시 및 설명이 없더라도 제 1 실시예의 관련 내용이 그대로 적용되는 것으로 하고, 신뢰에 기반하는 IoT 기기를 위한 협업시스템, 및 신뢰에 기반하는 IoT 기기의 협업방법은 이하의 실시예에서 달라지는 것으로 한다.

[0081] <제 2 실시예>

[0082] 제 2 실시예에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템에는 DNS 서버(201)가 포함되고, 상기 DNS 서버(201)는 상기 제 2 IoT 기기(102)의 신뢰지수를 가지고 있다. 이미 설명한 바와 같이, IoT 기기의 신뢰지수산출장치와 IoT 기기의 신뢰정보관리장치, 및 그 외에 이들 장치의 동작을 위하여 필요한 구성은 도 1과 마찬가지로 포함되어 있을 수 있다.

[0083] 도 4는 제 2 실시예에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템의 구성도이다.

[0084] 도 4를 참조하면, 신뢰정보를 제공하는 DNS(Domain Name System) 서버(201)가 제공되어 상기 신뢰정보관리장치(131)과 접속된다. 상기 DNS 서버(201)는 상기 신뢰정보관리장치(131)로부터 제 2 IoT 기기(102)에 대한 신뢰지수를 전달받고, 제 1 IoT 기기(101)의 제 2 IoT 기기에 대한 IP 주소 요청 시에, IP 주소와 더불어서 신뢰 지수를 제공할 수 있다.

[0085] 제 2 실시예에 따른 신뢰에 기반하는 IoT 기기의 협업방법을 설명한다.

[0086] 도 4를 참조하면, 상기 DNS서버(201)는 상기 신뢰정보관리장치(131)로부터 제 2 IoT 기기(102)에 대한 신뢰지수를 전달받고 이를 유지 관리한다.(Step 1) 제 1 IoT 기기(101)의 제 2 IoT 기기(102)에 대한 DNS(Domain Name System) 질의 시에(Step 2), 상기 DNS서버(201)는 요청한 제 2 IoT 기기(102)에 대한 도메인네임에 매핑되는 IP주소와 더불어서, 제 2 IoT 기기(102)의 신뢰지수를 제 1 IoT 기기(101)에 응답한다.(Step 3) 상기 제 1 IoT 기기(101)는 DNS서버(201)로부터 전달받은 제 2 IoT 기기(102)에 대한 신뢰지수를 자체 설정되어 있는 신뢰기준치와 비교한 후에, 제 2 IoT 기기(102)로의 접속과 협력 수행 여부를 결정하고(Step 4), 연결하는 것으로 결정한 경우에는 제 2 IoT 기기(102)와 접속할 수 있다.(Step 5)

[0087] 제 2 실시예에 따르면, IoT 기기(제 1 IoT 기기를 예시)는 상대편 IoT 기기(제 2 IoT 기기를 예시)에 접속 및 통신하기 전에 DNS서버를 통해 상대편 IoT 기기에 대한 신뢰지수를 획득할 수 있다. 그 신뢰지수를 바탕으로하여 상대편 IoT 기기로의 접속 및 통신 여부를 판단할 수 있다. 이로써 상대편 IoT 기기와의 협업에서 발생하는 문제들을 예방할 수 있다. 구체적으로는 데이터 손실, 바이러스 감염, 차별적인 데이터 처리, 및 개인정보 탈취 등의 문제를 미연에 방지할 수 있다.

[0088] 상기 DNS 서버(201)는 주기적으로 상기 신뢰지수를 업데이트할 수 있다.

[0090] <제 3 실시예>

[0091] 제 3 실시예에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템에는 인증시스템(301)이 포함되고, 상기 인증

시스템(301)은 상기 제 2 IoT 기기(102)의 신뢰지수를 가지고 있다. 이미 설명한 바와 같이, IoT 기기의 신뢰지수산출장치와 IoT 기기의 신뢰정보관리장치, 및 그 외에 이들 장치의 동작을 위하여 필요한 구성은 도 1과 마찬가지로 포함되어 있을 수 있다.

[0092] 도 5는 제 3 실시예에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템의 구성도이다.

[0093] 도 5는 신뢰지수를 제공하는 인증시스템(301)이 제공되어 상기 신뢰정보관리장치(131)과 접속된다. 상기 인증시스템(301)은 상기 신뢰정보관리장치(131)로부터 제 2 IoT 기기(102)에 대한 신뢰 지수를 전달받는다. 제 1 IoT 기기(101)의 제 2 IoT 기기에 대한 공개키(public key) 요청 시에, 상기 인증시스템(301)은 상기 공개키와 더불어서 신뢰지수를 제공할 수 있다.

[0094] 제 3 실시예에 따른 신뢰에 기반하는 IoT 기기를 위한 협업방법을 설명한다.

[0095] 도 5를 참조하면, 상기 인증시스템(301)은 상기 신뢰정보관리장치(131)로부터 제 2 IoT 기기(102)에 대한 신뢰지수를 전달받고 이를 유지 관리한다.(Step 1) 제 1 IoT 기기(101)의 제 2 IoT 기기(102)에 대한 공개키(Public Key) 질의 시에(Step 2), 상기 인증시스템(301)은 요청한 제 2 IoT 기기(102)에 대한 공개키와 더불어서 제 2 IoT 기기(102)의 신뢰지수를 제 1 IoT 기기(101)에 응답한다.(Step 3) 상기 제 1 IoT 기기(101)는 인증시스템(301)로부터 전달받은 제 2 IoT 기기(102)에 대한 신뢰지수를 자체 설정되어 있는 신뢰기준치와 비교한 후에, 제 2 IoT 기기(102)로의 접속과 협력 수행 여부를 결정하고(Step 4), 연결하는 것으로 결정한 경우에는 제 2 IoT 기기(102)와 접속할 수 있다.(Step 5)

[0096] 본 실시예에 따르면, IoT 기기(제 1 IoT 기기를 예시)는 상대편 IoT 기기(제 2 IoT 기기를 예시)와의 현금 및 카드 결재 등을 처리하기에 앞서서 인증시스템을 통해 상대편 IoT 기기에 대한 신뢰지수를 얻을 수 있다. 상기 신뢰지수를 바탕으로 상대편 IoT 기기와의 거래 여부를 판단할 수 있으므로, 상대편 IoT 기기와의 거래에서 발생하는 문제들을 예방할 수 있다. 구체적으로는 결재 오류, 결재 사기 등의 문제를 미연에 방지할 수 있다.

[0097] 상기 인증시스템(301)은 주기적으로 상기 신뢰지수를 업데이트할 수 있다.

[0099] <제 4 실시예>

[0100] 제 4 실시예에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템에는 신뢰 프락시 노드(trust proxy node)(401)가 포함되고, 상기 신뢰 프락시 노드(401)는 상기 제 2 IoT 기기(102)의 신뢰지수를 가지고 있을 수 있다. 이미 설명한 바와 같이, IoT 기기의 신뢰지수산출장치와 IoT 기기의 신뢰정보관리장치, 및 그 외에 이들 장치의 동작을 위하여 필요한 구성은 도 1과 마찬가지로 포함되어 있을 수 있다.

[0101] 도 6은 제 4 실시예에 따른 신뢰에 기반하는 IoT 기기를 위한 협업시스템의 구성도이다.

[0102] 도 6을 참조하면, 신뢰 프락시 노드(401)가 제공되어, 상기 신뢰정보관리장치(131), 제 1 IoT 기기(101), 및 제 2 IoT 기기(102)에 직접 접속된다.

[0103] 상기 신뢰 프락시 노드(401)는 신뢰 정보질의 및 판단 능력이 없는 제 1 IoT 기기(101)로부터 제 2 IoT 기기(102)로 전송되는 시그널링 메시지 및 데이터 패킷을 중간에서 가로챌 수 있다. 상기 신뢰 프락시 노드(401)는 상기 신뢰정보관리장치(131)을 통해 제 1 IoT 기기(101)가 접속 및 통신하고자 하는 제 2 IoT 기기(102)의 신뢰지수를 획득할 수 있다. 상기 신뢰 프락시 노드(401)는 상기 제 2 IoT 기기(102)와의 통신을 허가 또는 차단하는 것을 결정할 수 있다. 신뢰 프락시 노드(401)가 통신을 허락하는 경우에 제 1 IoT기기(101)가 제 2 IoT 기기(102)에 접속 및 연결할 수 있다.

[0104] 제 4 실시예에 따른 신뢰에 기반하는 IoT 기기를 위한 협업방법을 설명한다.

[0105] 도 6을 참조하면, 상기 신뢰 프락시 노드(401)는, 신뢰 정보질의 및 판단 능력이 없는 제 1 IoT 기기(101)로부터 제 2 IoT 기기(102)로 전송되는 시그널링 패킷 및 데이터 패킷을 중간에서 가로챈다(Step 1). 상기 신뢰 프락시 노드(401)는 신뢰정보관리장치(131)에게 요청하여(Step 2), 제 1 IoT 기기(101)가 접속 및 통신하고자 하는 제 2 IoT 기기(102)의 신뢰지수를 획득한다(Step 3). 상기 신뢰 프락시 노드(401)는 획득한 신뢰지수를 바탕으로 상기 제 2 IoT 기기(102)와의 통신을 허가 또는 차단한다(Step 4). 통신이 허가된 경우에 제 1 IoT기기(101)가 제 2 IoT 기기(102)에 접속할 수 있다(Step 5).

[0106] 다른 방식으로, 상기 신뢰 프락시 노드(401)는 상기 제 1 IoT 기기(101)의 부터의 요청과는 무관하게 상기 신뢰

정보관리장치(131)로부터 주기적으로 신뢰지수를 획득하여 보관할 수 있다. 이 경우에는 요청이 있을 때, 상기 신뢰정보관리장치(131)에게 신뢰지수를 요청하여 획득하는 단계가 생략된 상태에서 신속하게 접속을 허가 또는 차단할 수도 있다.

[0107] 상기 신뢰 프락시 노드(401)는 물리적으로 네트워크 게이트웨이, IoT 게이트웨이, 무선통신 기지국, 라우터, 및 스위치 등에 탑재될 수 있다.

[0108] 본 실시예에 따르면, 신뢰지수 정보 획득, 신뢰지수 판단 기능과 성능이 없는 IoT 기기들도, 신뢰기반 접속 및 통신 여부를 검증받을 수 있으므로 신뢰 검증 서비스가 쉽게 적용되어 확산될 수 있다.

산업상 이용가능성

[0109] 본 발명에 따른 IoT 기기들이 서로 신뢰할 수 있게 되므로, IoT 기기 들 간의 협력이 증진될 수 있다.

[0110] 그에 따른 효과로서, 네트워크 노드 들 간의 커넥티버티(connectivity: 연결성)가 향상될 수 있고, 네트워크 정보교류가 증진될 수 있다. 정보보안이 향상됨으로써, 더욱 안정되는 상태에서 네트워크를 사용할 수 있다.

부호의 설명

[0111] 131: 신뢰정보관리장치

1312: 신뢰지수산출장치

1315: 제 1 신뢰관련정보산출부

1316: 제 2 신뢰관련정보산출부

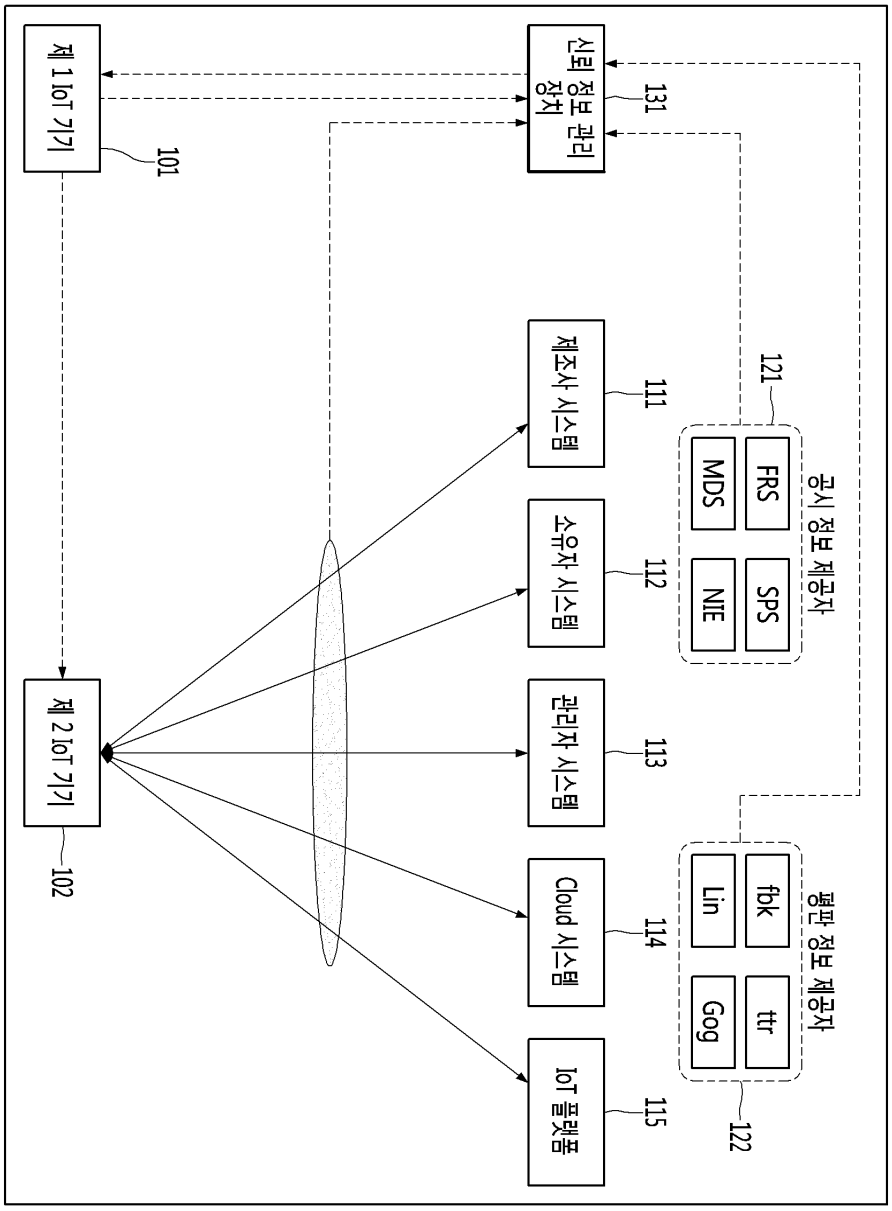
1317: 제 3 신뢰관련정보산출부

1318: 제 4 신뢰관련정보산출부

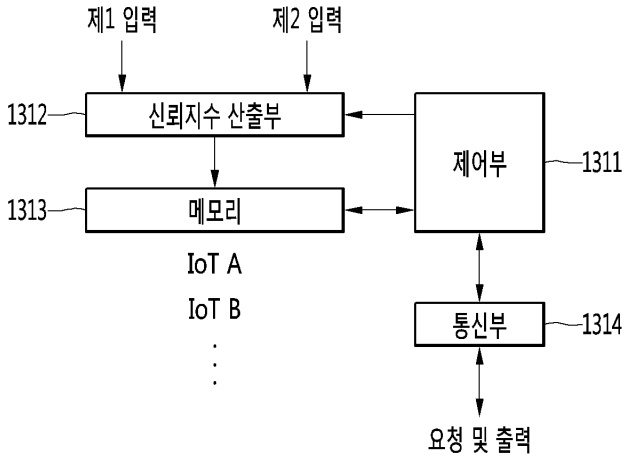
1319: 종합신뢰지수산출부

도면

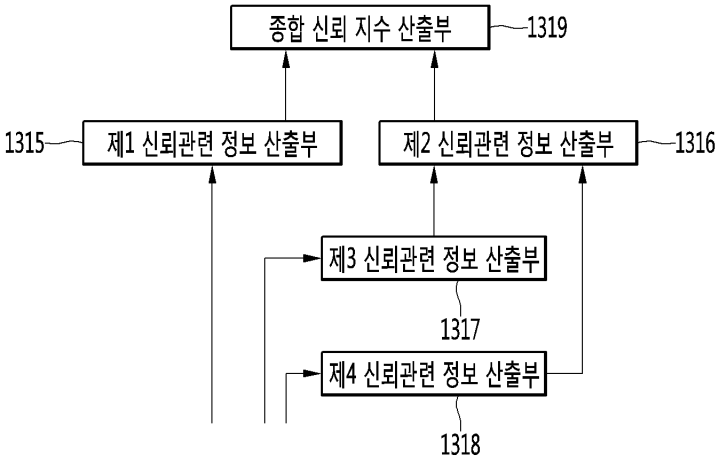
도면1


제 1 IoT 기기
101
신뢰 정보 관리 장치
131
제조사 시스템
111
소유자 시스템
112
관리자 시스템
113
Cloud 시스템
114
IoT 플랫폼
115
제 2 IoT 기기
102
121
공시 정보 제공자
FRS
SPS
MDS
NIE
122
평판 정보 제공자
fbk
ttr
Lin
Gog

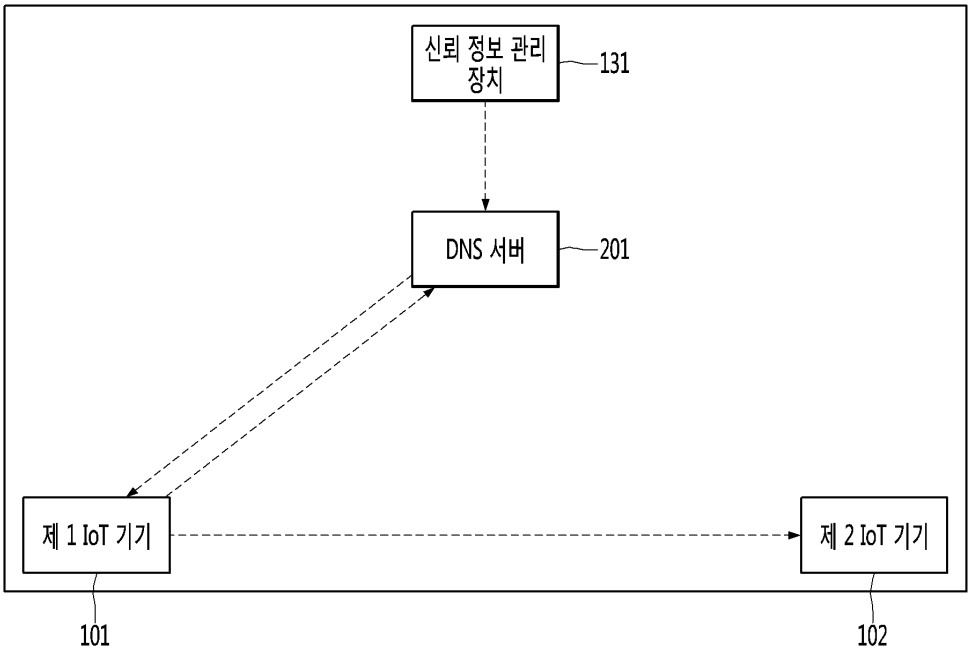
도면2


제1 입력
제2 입력
1312
신뢰지수 산출부
제어부
1311
1313
메모리
IoT A
IoT B
통신부
1314
요청 및 출력

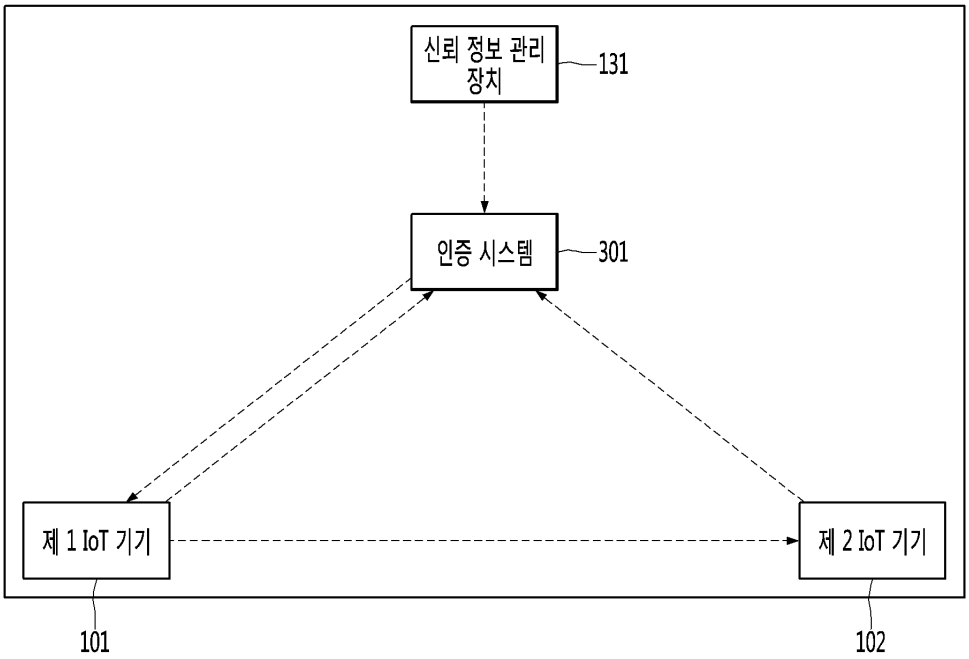
도면3


종합 신뢰 지수 산출부
1319
1315
제1 신뢰관련 정보 산출부
제2 신뢰관련 정보 산출부
1316
제3 신뢰관련 정보 산출부
1317
제4 신뢰관련 정보 산출부
1318

도면4


신뢰 정보 관리 장치
131
DNS 서버
201
제 1 IoT 기기
제 2 IoT 기기
101
102

도면5


신뢰 정보 관리 장치
131
인증 시스템
301
제 1 IoT 기기
제 2 IoT 기기
101
102

도면6

