(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년10월12일
(11) 등록번호 10-1784613
(24) 등록일자 2017년09월27일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *G01R 21/133* (2006.01)
G01R 22/06 (2006.01) *G06F 11/30* (2006.01)
G06F 17/30 (2006.01)
(52) CPC특허분류
G06F 21/602 (2013.01)
G01R 21/1333 (2013.01)
(21) 출원번호 10-2016-0075437
(22) 출원일자 2016년06월17일
심사청구일자 2016년06월17일
(56) 선행기술조사문헌
JP2013219775 A*
KR101548876 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
이문규
경기도 부천시 원미구 계남로 81, 2222동 702호(상동, 진달래마을)
(74) 대리인
양성보

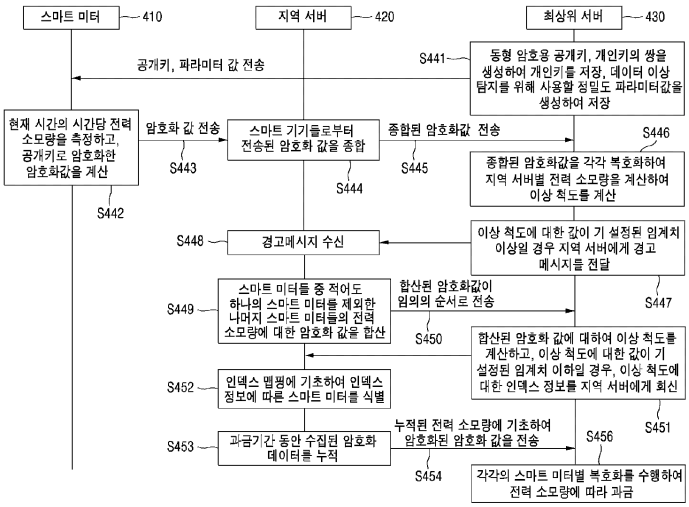
전체 청구항 수 : 총 5 항 심사관 : 구대성

(54) 발명의 명칭 **분산 데이터 이상 징후 탐지 방법 및 장치**

(57) 요 약

일 실시예에 따른 분산 데이터 이상 징후 탐지 방법은, 동형 암호용 공개키, 개인키의 쌍을 생성하여 상기 개인키를 저장하고, 이상 탐지를 위해 사용할 정밀도 파라미터 값을 생성하여 저장하는 단계; 각각의 노드에서 데이터를 측정하고, 상기 측정된 데이터를 상기 공개키로 암호화하여 지역 서버에게 전송하고, 상기 지역 서버에서 상기 각각의 노드로부터 전송된 상기 공개키로 암호화된 암호화 값을 합산하는 단계; 상기 지역 서버에서 상기 합산된 암호화 값이 전송됨에 따라 상기 합산된 암호화 값을 복호화하여 지역 서버별 취합 데이터를 계산하여 이상 척도를 판단하는 단계; 및 상기 이상 척도에 대한 값이 기 설정된 임계치 이상일 경우, 상기 취합 데이터와 연관된 지역 서버에게 경고 메시지를 전달하고, 상기 경고 메시지를 전달받은 지역 서버에서 상기 지역 서버가 관장하는 노드들 중 이상 징후가 발견된 노드를 식별하는 단계를 포함할 수 있다.

대 표 도



(52) CPC특허분류
G01R 22/066 (2013.01)
G06F 11/3006 (2013.01)
G06F 17/30144 (2013.01)
G06F 17/30194 (2013.01)
G06F 2211/008 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711035246
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신기술인력양성사업
연구과제명 클라우드 환경의 스마트 기기와 서비스 보안 기술개발 및 연구 인력양성
기 여 율 1/1
주관기관 숭실대학교 산학협력단
연구기간 2016.01.01 ~ 2016.12.31

명 세 서

청구범위

청구항 1

분산 데이터 이상 징후 탐지 방법에 있어서,

동형 암호용 공개키, 개인키의 쌍을 생성하여 상기 개인키를 저장하고, 이상 탐지를 위해 사용할 정밀도 파라미터 값을 생성하여 저장하는 단계;

각각의 노드에서 데이터를 측정하고, 상기 측정된 데이터를 상기 공개키로 암호화하여 지역 서버에게 전송하고, 상기 지역 서버에서 상기 각각의 노드로부터 전송된 상기 공개키로 암호화된 암호화 값을 합산하는 단계;

상기 지역 서버에서 상기 합산된 암호화 값이 전송됨에 따라 상기 합산된 암호화 값을 복호화하여 지역 서버별 취합 데이터를 계산하여 이상 척도를 판단하는 단계; 및

상기 이상 척도에 대한 값이 기 설정된 임계치 이상일 경우, 상기 취합 데이터와 연관된 지역 서버에게 경고 메시지를 전달하고, 상기 경고 메시지를 전달받은 지역 서버에서 상기 지역 서버가 관장하는 노드들 중 이상 징후가 발견된 노드를 식별하는 단계

를 포함하고,

상기 경고 메시지를 전달받은 지역 서버에서 상기 지역 서버가 관장하는 노드들 중 이상 징후가 발견된 노드를 식별하는 단계는,

순차적으로 전송받은 상기 지역 서버에 연결된 노드들 중 적어도 하나의 노드를 제외한 나머지 노드들의 데이터에 대한 암호화 값을 합산함에 따른 암호화 값에 대하여 상기 이상 척도를 계산하고, 상기 이상 척도에 대한 값이 기 설정된 임계치를 이하임에 따라 상기 이상 척도에 대한 값의 인덱스 정보를 지역 서버에게 회신하고, 상기 지역 서버에서 인덱스 맵핑에 기초하여 상기 인덱스 정보에 따른 노드를 식별하는 단계

를 포함하는 분산 데이터 이상 징후 탐지 방법.

청구항 2

제1항에 있어서,

상기 지역 서버에서 관리하는 노드들에 대하여 과금기간 동안 누적된 데이터에 기초하여 상기 각각의 노드별로 상기 암호화된 암호화값을 복호화함으로써 사용량에 따라 과금하는 단계

를 더 포함하는 분산 데이터 이상 징후 탐지 방법.

청구항 3

제1항에 있어서,

상기 경고 메시지를 전달받은 지역 서버에서 상기 지역 서버가 관장하는 노드 중 이상 징후가 발견된 노드를 식별하는 단계는,

상기 지역 서버에 연결된 노드들 중 적어도 하나의 노드를 제외한 나머지 노드들의 데이터에 대한 암호화 값을 합산하고, 상기 합산된 암호화 값이 임의의 순서로 전송되는 단계

를 포함하는 분산 데이터 이상 징후 탐지 방법.

청구항 4

삭제

청구항 5

삭제

청구항 6

제1항에 있어서,

상기 동형 암호용 공개키, 개인키의 쌍을 생성하여 상기 개인키를 저장하고, 이상 탐지를 위해 사용할 정밀도 파라미터 값을 생성하여 저장하는 단계는,

상기 파라미터 값이 동형 암호에 의해 가능한 곱셈 누적 횟수를 의미하고, 상기 각각의 노드가 최상위 서버의 공개키 및 상기 파라미터 값을 탑재한 상태로 각 가정에 설치되고, 상기 각각의 노드가 데이터를 전송할 지역 서버의 정보를 보유하는 단계

를 포함하는 분산 데이터 이상 징후 탐지 방법.

청구항 7

적어도 하나의 프로그램이 로딩된 메모리; 및

적어도 하나의 프로세서

를 포함하고,

상기 적어도 하나의 프로세서는, 상기 프로그램의 제어에 따라,

동형 암호용 공개키, 개인키의 쌍을 생성하여 상기 개인키를 저장하고, 이상 탐지를 위해 사용할 정밀도 파라미터 값을 생성하여 저장하는 과정;

각각의 노드에서 데이터를 측정하고, 상기 측정된 데이터를 상기 공개키로 암호화하여 지역 서버에게 전송하고, 상기 지역 서버에서 상기 각각의 노드로부터 전송된 상기 공개키로 암호화된 암호화 값을 합산하는 과정;

상기 지역 서버에서 상기 합산된 암호화 값이 전송됨에 따라 상기 합산된 암호화 값을 복호화하여 지역 서버별 취합 데이터를 계산하여 이상 척도를 판단하는 과정; 및

상기 이상 척도에 대한 값이 기 설정된 임계치 이상일 경우, 상기 취합 데이터와 연관된 지역 서버에게 경고 메시지를 전달하고, 상기 경고 메시지를 전달받은 지역 서버에서 상기 지역 서버가 관장하는 노드들 중 이상 징후가 발견된 노드를 식별하는 과정

을 포함하고,

상기 경고 메시지를 전달받은 지역 서버에서 상기 지역 서버가 관장하는 노드들 중 이상 징후가 발견된 노드를 식별하는 과정은,

순차적으로 전송받은 상기 지역 서버에 연결된 노드들 중 적어도 하나의 노드를 제외한 나머지 노드들의 데이터에 대한 암호화 값을 합산함에 따른 암호화 값에 대하여 상기 이상 척도를 계산하고, 상기 이상 척도에 대한 값이 기 설정된 임계치를 이하임에 따라 상기 이상 척도에 대한 값의 인덱스 정보를 지역 서버에게 회신하고, 상기 지역 서버에서 인덱스 맵핑에 기초하여 상기 인덱스 정보에 따른 노드를 식별하는 것

을 처리하는 분산 데이터 이상 징후 탐지 시스템.

발명의 설명

기 술 분 야

[0001] 아래의 설명은 동형 암호화 기술을 이용하여 데이터의 이상 징후를 탐지하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 완전 동형 또는 준동형 암호화 기술은 암호화된 상태에서 곱셈이나 덧셈이 가능하도록 하는 암호화 기술로서, 여러 분야에서 활용이 기대되고 있다. 예를 들면, 프라이버시를 보호할 필요가 있는 경우, 준동형 암호화 기술은 복호화를 할 필요없이 암호화된 상태에서 처리가 가능하므로, 유용할 수 있다.

[0003] 최근 기존의 전력시스템과 IT기술을 융합한 차세대 지능형 전력시스템인 스마트 그리드 개발이 활발하게 이루어지고 있다. 스마트 그리드의 핵심 구성요소인 스마트 미터는 실시간으로 사용되는 에너지를 측정하여 이를 사용자에게 제공함으로써 사용자가 에너지를 효율적으로 사용하도록 도와준다.

[0004] 구체적으로, 스마트 미터(smart meter)는 수용가 에너지 사용량을 실시간으로 계측하고 통신망을 통한 계측 정보 제공으로 전기사용요금 정보에 대응하여 수용가 에너지 사용을 적정하게 제어할 수 있는 기능을 갖는 디지털 전자식 계량기를 지칭하는 것으로, 스마트 미터의 도입은 수용가 측면에서는 스스로 사용 에너지 정보를 확인하고 이를 통해 자체적으로 에너지 사용 효율을 높일 수 있고, 전력회사 입장에서는 업무 효율화를 도모할 수 있으며, 나아가 사회 전체적으로 에너지 사용 정보를 활용한 새로운 서비스 창출 등을 통해 경제 활성화에 기여할 것으로 기대되고 있다.

[0005] 하지만, 스마트 미터의 경우, 수용가 측에 설치되어 외부에 노출되기 쉽기 때문에, 스마트 미터를 통한 데이터 노출 및 그에 따른 프라이버시 침해 가능성이 아주 높다. 예를 들어, 스마트 미터의 경우, 송수신되는 데이터의 보호를 위한 보안 키 정보가 저장되어 있기 때문에, 소자 분해 등의 공격에 의해 키 정보가 노출되거나, 키 정보의 갱신 및 관리의 문제가 있으며, 스마트 미터에 저장되는 정보의 왜곡이나 위변조가 가능하다는 문제점이 있다

발명의 내용

해결하려는 과제

[0006] 본 발명은 동형 암호(homomorphic encryption) 기술을 이용하여, 대규모 분산 시스템 환경에서 각 노드들이 생성하는 데이터의 기밀성을 유지한 상태로 각 데이터의 이상 여부를 개략적으로 판단하기 위한 방법을 제공할 수 있다.

과제의 해결 수단

[0007] 일 실시예에 따르면, 분산 데이터 이상 징후 탐지 방법은, 동형 암호용 공개키, 개인키의 쌍을 생성하여 상기 개인키를 저장하고, 이상 탐지를 위해 사용할 정밀도 파라미터 값을 생성하여 저장하는 단계; 각각의 노드에서 데이터를 측정하고, 상기 측정된 데이터를 상기 공개키로 암호화하여 지역 서버에게 전송하고, 상기 지역 서버에서 상기 각각의 노드로부터 전송된 상기 공개키로 암호화된 암호화 값을 합산하는 단계; 상기 지역 서버에서 상기 합산된 암호화 값이 전송됨에 따라 상기 합산된 암호화 값을 복호화하여 지역 서버별 취합 데이터를 계산하여 이상 척도를 판단하는 단계; 및 상기 이상 척도에 대한 값이 기 설정된 임계치 이상일 경우, 상기 취합 데이터와 연관된 지역 서버에게 경고 메시지를 전달하고, 상기 경고 메시지를 전달받은 지역 서버에서 상기 지역 서버가 관장하는 노드들 중 이상 징후가 발견된 노드를 식별하는 단계를 포함할 수 있다.

[0008] 일측에 따르면, 상기 이상 징후 탐지 방법은, 상기 지역 서버에서 관리하는 노드들에 대하여 과금기간 동안 누적된 데이터에 기초하여 상기 각각의 노드별로 상기 암호화된 암호화값을 복호화함으로써 사용량에 따라 과금하는 단계를 더 포함할 수 있다.

[0009] 또 다른 일측에 따르면, 상기 경고 메시지를 전달받은 지역 서버에서 상기 지역 서버가 관장하는 노드들 중 이상 징후가 발견된 노드를 식별하는 단계는, 상기 지역 서버에 연결된 노드들 중 적어도 하나의 노드를 제외한 나머지 노드들의 데이터에 대한 암호화 값을 합산하고, 상기 합산된 암호화 값이 임의의 순서로 전송되는 단계를 포함할 수 있다.

[0010] 또 다른 일측에 따르면, 상기 경고 메시지를 전달받은 지역 서버에서 상기 지역 서버가 관장하는 노드들 중 이상 징후가 발견된 노드를 식별하는 단계는, 순차적으로 전송받은 상기 지역 서버에 연결된 노드들 중 적어도 하나의 노드를 제외한 나머지 노드들의 데이터에 대한 암호화 값을 합산함에 따른 암호화 값에 대하여 상기 이상 척도를 계산하고, 상기 이상 척도에 대한 값이 기 설정된 임계치를 이하임에 따라 상기 이상 척도에 대한 값의 인덱스 정보를 지역 서버에게 회신하는 단계를 포함할 수 있다.

[0011] 또 다른 일측에 따르면, 상기 경고 메시지를 전달받은 지역 서버에서 상기 지역 서버가 관장하는 노드들 중 이상 징후가 발견된 노드를 식별하는 단계는, 상기 지역 서버에서 인덱스 맵핑에 기초하여 상기 인덱스 정보에 따

른 노드를 식별하는 단계를 포함할 수 있다.

[0012] 또 다른 일측에 따르면, 상기 동형 암호용 공개키, 개인키의 쌍을 생성하여 상기 개인키를 저장하고, 이상 탐지를 위해 사용할 정밀도 파라미터 값을 생성하여 저장하는 단계는, 상기 파라미터 값이 동형 암호에 의해 가능한 곱셈 누적 횟수를 의미하고, 상기 각각의 노드가 최상위 서버의 공개키 및 상기 파라미터 값을 탑재한 상태로 각 가정에 설치되고, 상기 각각의 노드가 데이터를 전송할 지역 서버의 정보를 보유하는 단계를 포함할 수 있다.

[0013] 일 실시예에 따르면, 적어도 하나의 프로그램이 로딩된 메모리; 및 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 상기 프로그램의 제어에 따라, 동형 암호용 공개키, 개인키의 쌍을 생성하여 상기 개인키를 저장하고, 이상 탐지를 위해 사용할 정밀도 파라미터 값을 생성하여 저장하는 과정; 각각의 노드에서 데이터를 측정하고, 상기 측정된 데이터를 상기 공개키로 암호화하여 지역 서버에게 전송하고, 상기 지역 서버에서 상기 각각의 노드로부터 전송된 상기 공개키로 암호화된 암호화 값을 합산하는 과정; 상기 지역 서버에서 상기 합산된 암호화 값이 전송됨에 따라 상기 합산된 암호화 값을 복호화하여 지역 서버별 취합 데이터를 계산하여 이상 척도를 판단하는 과정; 및 상기 이상 척도에 대한 값이 기 설정된 임계치 이상일 경우, 상기 취합 데이터와 연관된 지역 서버에게 경고 메시지를 전달하고, 상기 경고 메시지를 전달받은 지역 서버에서 상기 지역 서버가 관장하는 노드들 중 이상 징후가 발견된 노드를 식별하는 과정을 처리할 수 있다.

발명의 효과

[0014] 본 발명은 대규모 분산 시스템 환경에서 각 노드들이 생성하는 데이터의 기밀성을 유지한 상태로 대량의 데이터 분석을 통한 각 데이터의 이상 여부를 판단할 수 있다. 일 실시예에 따른 대규모 분산 시스템은 이상 데이터를 실시간으로 검출할 수 있고, 스마트 미터에 과금기간 동안 누적된 누척치에 기초하여 과금을 부여할 수 있다.

도면의 간단한 설명

[0015] 도 1은 일 실시예에 따른 네트워크 환경의 예를 도시한 도면이다.

도 2는 일 실시예에 따른 분산 데이터 이상 징후 탐지 시스템의 구성을 설명하기 위한 블록도이다.

도 3은 일 실시예에 따른 분산 데이터 이상 징후 탐지 시스템의 이상 징후를 탐지하는 방법을 설명하기 위한 흐름도이다.

도 4는 일 실시예에 따른 스마트 미터, 지역 서버 및 최상위 서버 사이에서 이상 징후를 탐지하는 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0016] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0017] 도 1은 일 실시예에 따른 네트워크 환경의 예를 도시한 도면이다.

[0018] 도 1의 네트워크 환경은 사용자 단말(110), 복수의 서버들(100, 101, 102) 및 네트워크(120)를 포함하는 예를 나타내고 있다. 이러한 도 1은 발명의 설명을 위한 일례로 사용자 단말의 수나 서버의 수가 도 1과 같이 한정되는 것은 아니다.

[0019] 사용자 단말(110)은 컴퓨터 장치로 구현되는 고정형 단말이거나 이동형 단말일 수 있다. 사용자 단말(110)의 예를 들면, 스마트폰(smart phone), 휴대폰, 네비게이션, 컴퓨터, 노트북, 디지털방송용 단말, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 태블릿 PC 등이 있다. 일례로 사용자 단말(110)은 무선 또는 유선 통신 방식을 이용하여 네트워크(120)를 통해 다른 사용자 단말들 및/또는 서버(100, 101, 102)와 통신할 수 있다. 사용자 단말(110)은 유권자로부터 투표가 실시될 수 있도록 제공할 수 있다.

[0020] 통신 방식은 제한되지 않으며, 네트워크(120)가 포함할 수 있는 통신망(일례로, 이동통신망, 유선 인터넷, 무선 인터넷, 방송망)을 활용하는 통신 방식뿐만 아니라 기기들간의 근거리 무선 통신 역시 포함될 수 있다. 예를

들어, 네트워크(170)는, PAN(personal area network), LAN(local area network), CAN(campus area network), MAN(metropolitan area network), WAN(wide area network), BBN(broadband network), 인터넷 등의 네트워크 중 하나 이상의 임의의 네트워크를 포함할 수 있다. 또한, 네트워크(120)는 버스 네트워크, 스타 네트워크, 링 네트워크, 메쉬 네트워크, 스타-버스 네트워크, 트리 또는 계층적(hierarchical) 네트워크 등을 포함하는 네트워크 토폴로지 중 임의의 하나 이상을 포함할 수 있으나, 이에 제한되지 않는다.

[0021] 서버(100, 101, 102) 각각은 사용자 단말(110)과 네트워크(120)를 통해 통신하여 명령, 코드, 파일, 컨텐츠, 서비스 등을 제공하는 컴퓨터 장치 또는 복수의 컴퓨터 장치들로 구현될 수 있다.

[0022] 일례로, 서버(100)는 네트워크(120)를 통해 접속한 사용자 단말(110)로 어플리케이션의 설치를 위한 파일을 제공할 수 있다. 이 경우 사용자 단말(110)은 서버(100)로부터 제공된 파일을 이용하여 어플리케이션을 설치할 수 있다. 또한 사용자 단말(110)이 포함하는 운영체제(Operating System, OS) 및 적어도 하나의 프로그램(일례로 브라우저나 상기 설치된 어플리케이션)의 제어에 따라 서버(100)에 접속하여 서버(100)가 제공하는 서비스나 컨텐츠를 제공받을 수 있다. 예를 들면, 사용자 단말(110)이 어플리케이션의 제어에 따라 네트워크(120)를 통해 서비스 요청 메시지를 서버(100)로 전송하면, 서버(100)는 서비스 요청 메시지에 대응하는 코드를 사용자 단말(110)로 전송할 수 있고, 사용자 단말(110)은 어플리케이션의 제어에 따라 코드에 따른 화면을 구성하여 표시함으로써 사용자에게 컨텐츠를 제공할 수 있다.

[0023] 도 2는 일 실시예에 따른 분산 데이터 이상 징후 탐지 시스템의 구성을 설명하기 위한 블록도이다.

[0024] 분산 데이터 이상 징후 탐지 시스템(200)은 프로세서(210), 버스(220), 네트워크 인터페이스(230), 메모리(240) 및 데이터베이스(250)를 포함할 수 있다. 메모리(240)는 운영체제(241) 및 서비스 제공 루틴(242)를 포함할 수 있다. 다른 실시예들에서 분산 데이터 이상 징후 시스템(200)은 도 2의 구성요소들보다 더 많은 구성요소들을 포함할 수도 있다. 그러나, 대부분의 종래기술적 구성요소들을 명확하게 도시할 필요성은 없다. 예를 들어, 분산 데이터 이상 징후 시스템(200)은 디스플레이나 트랜시버(transceiver)와 같은 다른 구성요소들을 포함할 수도 있다.

[0025] 메모리(240)는 컴퓨터에서 판독 가능한 기록 매체로서, RAM(random access memory), ROM(read only memory) 및 디스크 드라이브와 같은 비소멸성 대용량 기록장치(permanent mass storage device)를 포함할 수 있다. 또한, 메모리(240)에는 운영체제(241)와 서비스 제공 루틴(242)을 위한 프로그램 코드가 저장될 수 있다. 이러한 소프트웨어 구성요소들은 드라이브 메커니즘(drive mechanism, 미도시)을 이용하여 메모리(240)와는 별도의 컴퓨터에서 판독 가능한 기록 매체로부터 로딩될 수 있다. 이러한 별도의 컴퓨터에서 판독 가능한 기록 매체는 플로피 드라이브, 디스크, 테이프, DVD/CD-ROM 드라이브, 메모리 카드 등의 컴퓨터에서 판독 가능한 기록 매체(미도시)를 포함할 수 있다. 다른 실시예에서 소프트웨어 구성요소들은 컴퓨터에서 판독 가능한 기록 매체가 아닌 네트워크 인터페이스(230)를 통해 메모리(240)에 로딩될 수도 있다.

[0026] 버스(220)는 분산 데이터 이상 징후 탐지 시스템(200)의 구성요소들간의 통신 및 데이터 전송을 가능하게 할 수 있다. 버스(220)는 고속 시리얼 버스(high-speed serial bus), 병렬 버스(parallel bus), SAN(Storage Area Network) 및/또는 다른 적절한 통신 기술을 이용하여 구성될 수 있다.

[0027] 네트워크 인터페이스(230)는 분산 데이터 이상 징후 시스템(200)을 컴퓨터 네트워크에 연결하기 위한 컴퓨터 하드웨어 구성요소일 수 있다. 네트워크 인터페이스(230)는, 이더넷 카드와 같은 네트워크 인터페이스 카드, 광학 송수신기, 무선 주파수 송수신기, 혹은 정보를 송수신할 수 있는 임의의 다른 타입의 디바이스일 수 있다. 이러한 네트워크 인터페이스들의 다른 예들은 모바일 컴퓨팅 디바이스들 및 USB 내의 블루투스(Bluetooth), 3G 및 WiFi 등을 포함하는 무선기기일 수 있다. 일부 예들에서, 컴퓨팅 디바이스는, 서버, 모바일 폰, 혹은 다른 네트워크화된 컴퓨팅 디바이스와 같은 외부 디바이스와 무선으로 통신하기 위해 네트워크 인터페이스(230)를 사용할 수 있다. 네트워크 인터페이스(230)는 분산 데이터 이상 징후 시스템(200)을 무선 또는 유선 커넥션을 통해 컴퓨터 네트워크에 연결시킬 수 있다.

[0028] 데이터베이스(250)는 이상 징후를 탐지하기 위한 정보를 저장 및 유지하는 역할을 할 수 있다. 도 2에서 분산 데이터 이상 징후 시스템(200)의 내부에 데이터베이스(250)를 구축하여 포함하는 것으로 도시하고 있으나, 이에 한정되는 것은 아니며 시스템 구현 방식이나 환경 등에 따라 생략될 수 있고 혹은 전체 또는 일부의 데이터베이스가 별개의 다른 시스템 상에 구축된 외부 데이터베이스로서 존재하는 것 또한 가능하다.

[0029] 도 3은 일 실시예에 따른 분산 데이터 이상 징후 탐지 시스템의 이상 징후를 탐지하는 방법을 설명하기 위한 흐름도이다.

[0030] 분산 데이터 이상 징후 탐지 시스템을 구성하는 각 노드 N_i들은 지속적으로 데이터를 생성하며, 효과적인 시스템 관리를 위해 각 데이터들을 수집하여 분석하는 중간 단계의 서버(지역 서버) S_j들이 존재하고, 중간 단계 서버(지역 서버)가 전처리한 데이터를 종합하는 최상위 서버 C 가 존재한다. 최상위 서버 C는 각 노드들에서 발생한 개별 데이터에는 관여하지 않으며, 데이터 전체에 대한 통계적 경향, 예를 들면, 총합이나 평균 등을 분석함으로써 개별 데이터 중 이상 데이터가 있는지를 감지할 수 있다.

[0031] 아래의 실시예에서는 전력 데이터를 안전하게 관리하는 스마트 그리드를 고려할 수 있다. 하지만 본 발명은 스마트 미터 및 스마트 그리드에 한정되는 것은 아니며, 분산 데이터 이상 징후를 탐지하는 다양한 분야에 적용될 수 있다. 예를 들면, 계량기(스마트 미터)를 노드의 예로 하여 설명하기로 한다.

[0032] 각각의 가정의 계량기(스마트 미터) N_i는 실시간으로 시간당 전력 소모량 데이터를 측정하여 지역 서버(배전 서버) S_j에게 전송하며, 지역 서버는 각 계량기로부터 수집된 전력 소모량을 합계하여 해당 지역에서의 시간당 전력 소모량을 계산할 수 있다. 이 결과는 다시 발전소(전력 관리 회사)에 위치한 최상위 서버 C에게 전송되어, 최상위 서버는 복수의 지역 서버 S_j들로부터 수집된 데이터들을 분석하여 지역별 전력 소모량에 따라 지역별 배전량과 발전량을 조정함으로써 에너지를 효과적으로 관리할 수 있다. 단, 각 가정의 실시간 전력 소모량은 예를 들면, TV 시청 여부, 냉난방기 가동 여부, 이에 따른 댁내 체류 및 부재 여부 등 다양하고 민감한 개인 정보를 포함할 수 있으므로 암호화하여 전송하는 것이 안전하며, 이러한 개인 정보는 외부의 공격자뿐만 아니라 전력 관리 회사에도 노출되지 않는 것이 바람직하다.

[0033] 이에 따라 지역 서버(배전 서버) S_j들은 개별 가정으로부터 전송된 전력 소모량 데이터를 그대로 최상위 서버 C에게 전송하는 것이 아니라, 각각의 전력 소모량 데이터를 합한 총량만을 전송하면 된다. 이와는 별도로, 지역 서버들은 스마트 미터별 시간당 전력 소모량을 누적한 총 전력 사용량을 월별로 계산하여 최상위 서버에게 전송함으로써 월별 과금이 가능하도록 한다. 시간당 전력 소모량을 누적한 총 전력 사용량 역시 암호화되어 전송되며, 실시간 데이터 대신 총량만을 전송하게 되므로 개인 정보가 최대한 보호될 수 있다.

[0034] 위와 같은 구성에서는 특정 가정에 누전 사고가 발생하거나 스마트 미터에 고장이 생기는 등과 같이 즉시 조치가 필요한 상황에 대한 대처가 어렵게 된다. 다시 말해서, 지역 서버들로부터 최상위 서버로 실시간으로 전송되는 데이터는 개별 가정 데이터가 아닌 지역 누계이므로 특정 가정에서 발생한 이상 데이터(전력 소모량의 급증 등)를 검출해내기 어려우며, 월별로 누적하여 전송되는 데이터는 월별 누계이므로 특정 시간에 발생하는 이상 데이터를 실시간으로 확인하기 어렵다. 이와 같은 문제는 동형 암호를 활용함으로써 해결 가능하다. 동형 암호(homomorphic encryption)란 평문(plaintext)에 특정 연산을 수행하여 암호화한 결과와, 평문에 바로 암호화를 한 후 같은 연산을 적용한 결과가 서로 같은 암호이다. 예를 들어, 덧셈에 대한 동형 암호는 평문 m_1, m_2의 암호화 연산 E 및 복호화 연산 D 에 대하여 $D(E(m_1+m_2)) = D(E(m_1)+E(m_2))$를 만족하는 암호이며, 곱셈에 대한 동형 암호는 $D(E(m_1 \times m_2)) = D(E(m_1) \times E(m_2))$를 만족하는 암호이다. 덧셈과 곱셈에 대해 모두 동형인 암호를 완전 동형 암호(fully homomorphic encryption)라 한다. 본 발명에서는 평문 m_1, m_2가 정수인 경우를 고려하며, 본 발명에서 목표로 하는 이상 징후 탐지 방법은 완전 동형 암호 이외에도 곱셈 소수, 덧셈 다수가 가능한 부분 동형 암호(somewhat homomorphic encryption)로도 구성 가능하다.

[0035] 분산 데이터 이상 징후 탐지 시스템은 단계(310) 내지 단계(330)을 수행할 수 있다.

[0036] 단계(310)에서 분산 데이터 이상 징후 탐지 시스템은 초기화 단계를 수행할 수 있다.

[0037] 최상위 서버 C는 동형 암호용 공개키, 개인키의 쌍을 생성하여 개인키 S_C를 저장할 수 있다. 최상위 서버는 데이터 이상 탐지를 위해 사용할 정밀도 파라미터 값 n(n은 2이상의 정수)을 생성하여 저장할 수 있다(S441). 이때, n-1은 동형 암호에 의해 가능한 곱셈 누적 횟수를 의미할 수 있다. 각 스마트 미터는 최상위 서버의 공

개키 P_C 및 파라미터 값 n을 탑재한 상태로 각 가정에 설치될 수 있다. 추가로 각 스마트 미터는 데이터를 전송할 지역 서버 S_j의 정보를 보유할 수 있다.

[0038] 단계(320)에서 분산 데이터 이상 징후 탐지 시스템은 데이터 중간 집계 단계를 수행할 수 있다.

[0039] 각 스마트 미터 N_i는 현재 시간 t의 시간당 전력 소모량인 v_{it}를 측정하여 최상위 서버의 공개키로 암호화한 암호화 값 $V_{it} = E(P_C, v_{it})$을 계산하고, 암호화 값을 스마트 미터에 연결된 지역 서버에게 전송할 수 있다(S442, S443).

[0040] 지역 서버는 자신과 연결된 스마트 미터들로부터 전송된 데이터를 종합하여 $U_{j1} = \sum_i V_{it}$ 및 $U_{j2} = \sum_i (V_{it})^n$을 계산한 후 계산된 암호화 값을 최상위 서버에게 전송할 수 있다(S444, S445).

[0041] 최상위 서버는 합산된 암호화 값을 각각 복호화하여 지역 서버별 $\sum_i v_{it} = D(S_C, U_{j1})$ 및 $\sum_i v_{it}^n = D(S_C, U_{j2})$를 계산하여 이상 척도 $k^{n-1}\sum_i v_{it}^n - (\sum_i v_{it})^n$를 판단할 수 있다(S446). 단, k는 S_j가 관장하는 해당 지역의 전체 스마트 미터의 수를 의미할 수 있다. 최상위 서버는 이상 척도에 대한 값이 미리 정해진 임계치 이상일 경우, 특정 전력 소모량이 비정상임을 의미하므로 해당 값을 생성하게 한 합산된 암호화 값과 연관된 지역 서버에게 경고 메시지를 전달할 수 있다(S447).

[0042] 지역 서버는 경고 메시지를 수신할 수 있다(S448). 경고 메시지를 수신한 지역 서버가 관장하는 스마트 미터들을 각각 $N_1, \ldots, N_k$라고 할 때, 지역 서버는 문제의 진원지인 스마트 미터를 판별하기 위하여 $U_{j1}^{(x)} = \sum_{i \neq x} V_{it}$ 및 $U_{j2}^{(x)} = \sum_{i \neq x} (V_{it})^n \ (1 \leq x \leq k)$들을 계산하여 최상위 서버에게 전송할 수 있다(S449, S450). 다시 말해서, $U_{j1}^{(x)}$ 및 $U_{j2}^{(x)}$는 지역 서버에 연결된 모든 스마트 미터들 중 적어도 하나의 스마트 미터만을 제외한 나머지 스마트 미터들에 대해 $U_{j1} = \sum_i V_{it}$ 및 $U_{j2} = \sum_i (V_{it})^n$를 계산한 것을 의미할 수 있다. 단, $(U_{j1}^{(x)}, U_{j2}^{(x)})$들은 $(U_{j1}^{(1)}, U_{j2}^{(1)}), (U_{j1}^{(2)}, U_{j2}^{(2)}), \ldots, (U_{j1}^{(k)}, U_{j2}^{(k)})$ 순이 아닌, 임의로 변경된 순서로 전송될 수 있다.

[0043] 최상위 서버는 지역 서버로부터 순차적으로 전송받은 모든 $(U_{j1}^{(x)}, U_{j2}^{(x)})$에 대해 앞서 설명한 바와 마찬가지의 방식으로(단, k 대신 $k-1$ 이용) 이상 척도에 대한 값을 계산하여 이상이 발견되지 않은 인덱스 정보를 지역 서버에게 회신할 수 있다(S451). 이때, 최상위 서버의 관점에서는 지역 서버로부터 전송 받은 $(U_{j1}^{(x)}, U_{j2}^{(x)})$ 값들의 순서가 무작위순이므로, 이상 척도에 대한 값의 인덱스가 어느 x에 관련된 것인지는 알 수 없다. 지역 서버는 순서 변경에 사용하였던 인덱스 맵핑을 참조하여, 최상위 서버로부터 받은 인덱스 정보가 어느 스마트 미터에 해당하는지를 확인할 수 있다(S452). 예를 들면, 해당하는 스마트 미터가 N_z일 경우, 스마트 미터 N_z에 대해 조치하고 z의 식별 정보(예를 들면, ID 정보)를 최상위 서버에게 통보할 수 있다.

[0044] 최상위 서버는 이상 척도에 대한 값이 기 설정된 임계치 이하일 경우, 다시 말해서, 이상이 발견되지 않을 경우, 지역 서버는 스마트 미터별로 월별 사용량에 대한 암호화 값을 계속 누적할 수 있다(S447). 이때, 각각

의 스마트 미터별로 월별 사용량에 대한 암호화 값을 누적할 수 있다(i 별로 $\sum_t V_{it}$ 계산).

[0045] 단계(330)에서 분산 데이터 이상 징후 탐지 시스템은 과금 단계를 수행할 수 있다.

[0046] 지역 서버는 지역 서버가 관리하는 모든 스마트 미터별로 과금기간(예를 들면, 한달)동안 수집된 전력 소모량을 누적하여 $\sum_t V_{it}$ 을 구할 수 있다(S453). 지역 서버는 누적된 전력 소모량에 기초하여 암호화된 암호화 값을 최상위 서버에게 전송할 수 있다(S454). 최상위 서버는 각각의 스마트 미터별로 복호화를 수행하여 $\sum_t v_{it} = D(S_C, \sum_t V_{it})$ 를 계산함으로써 전력 소모량에 따라 과금할 수 있다(S456).

[0047] 분산 데이터 이상 징후 탐지 시스템은 다음과 같은 성질을 만족한다.

[0048] 1. 분산 데이터 이상 징후 탐지 시스템은 이상 데이터를 실시간으로 검출할 수 있다.

[0049] 단계(S446 및 S447)에서 계산하는 이상 척도 $k^{n-1}\sum_i v_{it}^n - (\sum_i v_{it})^n$ 는 분산을 일반화한 개념으로, 정밀도 파라미터 값 n을 2로 하면, $k\sum_i v_{it}^2 - (\sum_i v_{it})^2$ 가 되어 (분산의 k^2 배)임을 알 수 있다. n을 크게하면 개별 데이터 간의 차이를 증폭하는 효과가 있다. 예를 들면, $k = 5$일 때, $(v_{1t}, v_{2t}, v_{3t}, v_{4t}, v_{5t}) = (1,1,1,1,2)$ 라면, n=2일 때 이상 척도에 대한 값은 4(5^2으로 나누면 분산 4/25=0.16)이며, n=3일 때의 이상 척도에 대한 값은 84(5^3으로 나누면 84/125=0.672), n=4 일 때의 이상 척도에 대한 값은 1204(5^4으로 나누면 1204/625=1.9264)이다. 만약, $(v_{1t}, v_{2t}, v_{3t}, v_{4t}, v_{5t}) = (1,1,1,1,1)$ 로 데이터가 모두 일정하다면 이상 척도에 대한 값은 n에 관계없이 0이다. 판별 정밀도 파라미터 n 및 이에 대한 이상 척도의 임계치를 적절히 정함으로써 데이터의 이상 정도(다른 데이터에 비해 상당한 차이가 있는 값이 있는지 여부)를 확인할 수 있다. 단계(S451)에서 $(U_{j1}^{(z)}, U_{j2}^{(z)})$ 에 대한 이상 척도(즉, z 를 제외하고 계산한 값)는 정상이고, $x \neq z$ 인 모든 x 에 대한 $(U_{j1}^{(x)}, U_{j2}^{(x)})$ 의 이상 척도들(즉, z 가 포함되어 계산된 모든 값)이 모두 비정상이라면, N_z 가 이상 데이터를 생성한 것이므로 이를 정확히 검출할 수 있다.

[0050] 2. 분산 데이터 이상 징후 탐지 시스템은 정상적인 누적치를 계산(과금)하는 기능을 제공할 수 있다.

[0051] 지역 서버는 지역 서버가 관리하는 모든 스마트 미터별로 특정 시점 t의 $V_{it} = E(P_C, v_{it})$ 값을 가지고 있으므로, 이를 과금 대상 기간 내 모든 시점에 대해 누적함으로써 $\sum_t V_{it}$ 를 구할 수 있다. 동형 암호의 성질에 의하여 $\sum_t V_{it} = \sum_t E(P_C, v_{it}) = E(P_C, \sum_t v_{it})$ 이므로, 단계(S456)에서 최상위 서버가 과금 데이터를 계산할 수 있다.

[0052] 3. 분산 데이터 이상 징후 탐지 시스템은 스마트 미터별 실시간 데이터에 대한 기밀성을 보장할 수 있다.

[0053] 단계(S444 및 S445)에서 지역 서버는 각각의 개별 스마트 미터의 암호화 값 대신 지역 서버와 연관된 스마트 미터들에 대한 암호화 값을 누적한 암호화 값 $U_{j1} = \sum_i V_{it}$ 및 $U_{j2} = \sum_i (V_{it})^n$ 을 최상위 서버에게 전송하므로, 최상위 서버가 누적한 암호화 값을 복호화하여도 해당 지역의 스마트 미터의 총량인 $\sum_i v_{it}$ 및 $\sum_i v_{it}^n$ 만을 알 수 있다. 단계(S446 및 S447)에서 이상이 발견된 경우, 단계(S449)에서는 지역 서버는 $(U_{j1}^{(1)}, U_{j2}^{(1)}), (U_{j1}^{(2)}, U_{j2}^{(2)}), \ldots, (U_{j1}^{(k)}, U_{j2}^{(k)})$ 들을 최상위 서버에게 전송하고,

$(U_{j1}^{(1)}, U_{j2}^{(1)}), (U_{j1}^{(2)}, U_{j2}^{(2)}), \ldots, (U_{j1}^{(k)}, U_{j2}^{(k)})$를 이용하여 최상위 서버는 $x(1 \le x \le k)$에 대해 v_{xt}를 계산 가능하다. 그러나 지역 서버가 $(U_{j1}^{(1)}, U_{j2}^{(1)}), (U_{j1}^{(2)}, U_{j2}^{(2)}), \ldots, (U_{j1}^{(k)}, U_{j2}^{(k)})$들을 무작위로 순서를 변경하여 전송하였으므로 최상위 서버는 각 v_{xt} 값이 어느 스마트 미터로부터 전송된 것인지를 알 수 없다. 이때, 단계(S451)에서 문제가 있는 z에 대한 정보가 최상위 서버에게 통보되므로 최상위 서버는 이상 척도에 대한 값이 기 설정된 임계치 이상인 스마트 미터에 대한 정보를 알 수 있다. 단계(S451)에서 지역 서버는 최상위 서버로부터 문제가 있는 스마트 미터의 인덱스 정보만을 회신받으므로 개별 스마트 미터들의 사용량 정보 v_{it}들은 알 수 없다.

[0054] 단계(330)의 과금 단계에서 최상위 서버는 특정 스마트 미터의 과금 기간내 총량 데이터만을 확인할 수 있으며, 지역 서버는 누적 연산만 동형 암호 상태로 수행할 뿐 내용은 전혀 알 수 없다. 이에 따라 모든 정상적인 스마트 미터 i 에 대한 특정 시간 t의 실시간 사용량 v_{it} 은 최상위 서버와 지역 서버 모두에게 노출되지 않는다.

[0055] 일 실시예에 따른 분산 데이터 이상 징후 탐지 시스템은 클라우드 환경의 고장 탐지, 분산 침입 탐지, 데이터 마이닝 및 빅데이터 분석 등에 다양하게 적용될 수 있다. 예를 들면, 분산 데이터 이상 징후 탐지 시스템은 클라우드 환경의 고장을 탐지함에 있어서, 클라우드의 노드들을 N_i로 하여 개별 노드들에 존재하는 고객 데이터(패킷 전송 수, 스케줄링 수, 디스크 접속 수 등)의 기밀성은 유지하면서 해당 데이터들의 이상 탐지를 수행할 수 있다.

[0056] 또한, 분산 데이터 이상 징후 탐지 시스템은 분산 침입을 탐지함에 있어서, 감시 대상 시스템들을 노드 N_i들로 하여 개별 노드들에서 일어나는 행위(예를 들면, 패킷 전송 수, 시스템 콜 횟수, 디스크 접속 수 등)의 기밀성은 유지하면서 이상 행위를 탐지하는 것이 가능하다.

[0057] 또한, 분산 데이터 이상 징후 탐지 시스템은 데이터 마이닝 및 빅데이터 분석에 있어서, 개별 데이터 아이템들을 노드 N_i로 하여, 개별 데이터들의 기밀성은 유지하면서 전체적인 통계 특성을 분석하는 것이 가능하다.

[0058] 일 실시예에 따른 분산 데이터 이상 징후 탐지 시스템은 위에서 설명한 실시예에 한정되는 것은 아니며, 개별 데이터의 기밀성을 유지함과 동시에 대량의 데이터 분석을 통한 이상 징후 검출 또는 데이터 신뢰성 검증이 필요한 모든 상황에 적용 가능하다.

[0059] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0060] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로,

또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

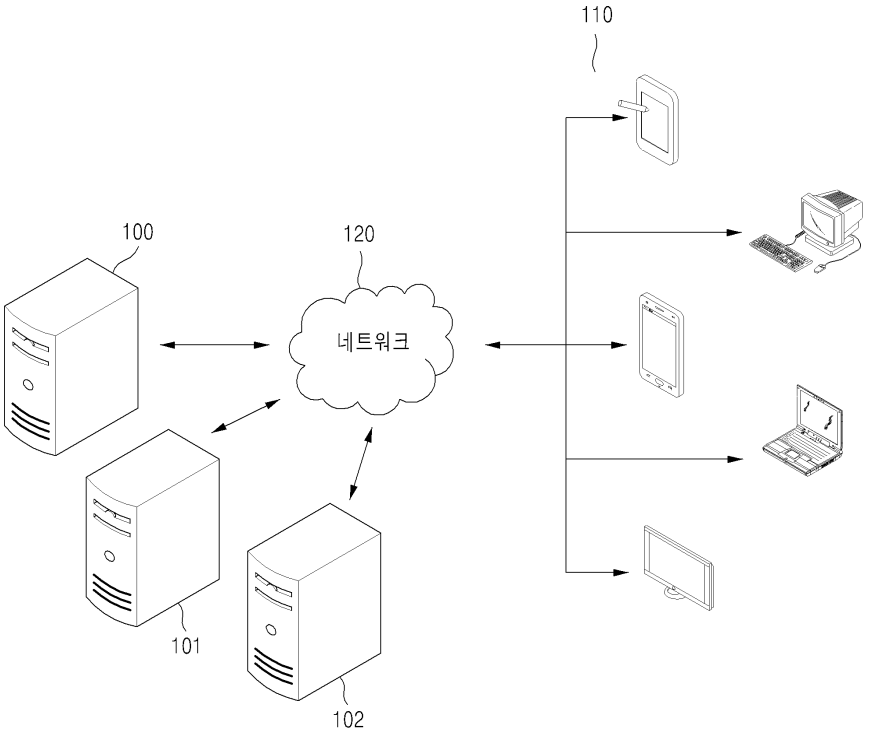
[0061] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0062] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

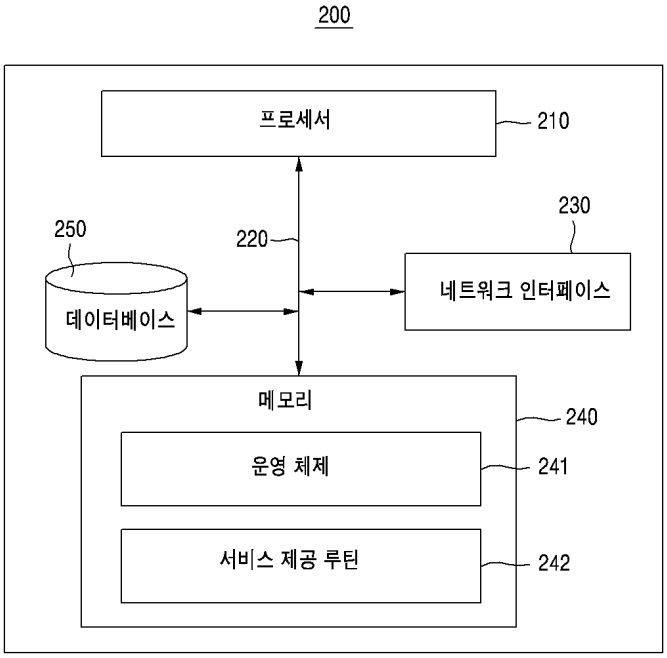
[0063] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

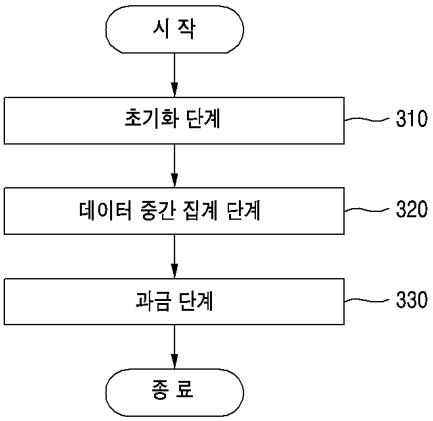
도면1



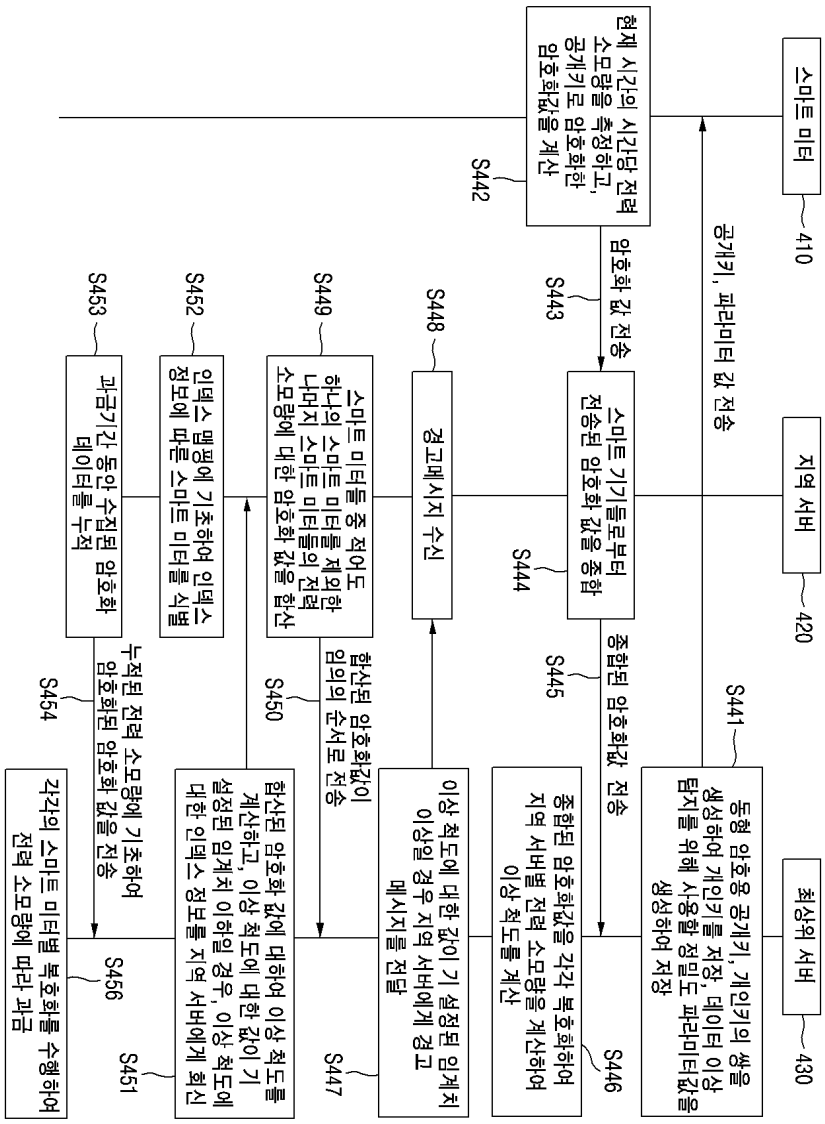
도면2


200
프로세서
210
230
250
220
네트워크 인터페이스
데이터베이스
메모리
240
운영 체제
241
서비스 제공 루틴
242

도면3


시 작
초기화 단계
310
데이터 중간 집계 단계
320
과금 단계
330
종 료

도면4


스마트 미터
410
현재 시간의 시간당 전력 소모량을 측정하고, 공개키로 암호화한 암호화값을 계산
S442
암호화 값 전송
S443
공개키, 파라미터 값 전송
지역 서버
420
스마트 기기들로부터 전송된 암호화 값을 종합
S444
종합된 암호화값 전송
S445
최상위 서버
430
동형 암호용 공개키, 개인키의 쌍을 생성하여 개인키를 저장, 데이터 이상 탐지를 위해 사용할 정밀도 파라미터값을 생성하여 저장
S441
종합된 암호화값을 각각 복호화하여 지역 서버별 전력 소모량을 계산하여 이상 척도를 계산
S446
이상 척도에 대한 값이 기 설정된 임계치 이상일 경우 지역 서버에게 경고 메시지를 전달
S447
경고메시지 수신
S448
스마트 미터들 중 적어도 하나의 스마트 미터를 제외한 나머지 스마트 미터들의 전력 소모량에 대한 암호화 값을 합산
S449
합산된 암호화값이 임의의 순서로 전송
S450
합산된 암호화 값에 대하여 이상 척도를 계산하고, 이상 척도에 대한 값이 기 설정된 임계치 이하일 경우, 이상 척도에 대한 인덱스 정보를 지역 서버에게 회신
S451
인덱스 맵핑에 기초하여 인덱스 정보에 따른 스마트 미터를 식별
S452
과금기간 동안 수집된 암호화 데이터를 누적
S453
누적된 전력 소모량에 기초하여 암호화된 암호화 값을 전송
S454
각각의 스마트 미터별 복호화를 수행하여 전력 소모량에 따라 과금
S456