



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0025303
(43) 공개일자 2024년02월27일

(51) 국제특허분류(Int. Cl.)
G06Q 50/06 (2024.01) H02J 3/00 (2006.01)
(52) CPC특허분류
G06Q 50/06 (2024.01)
G06F 21/602 (2013.01)
(21) 출원번호 10-2022-0103351
(22) 출원일자 2022년08월18일
심사청구일자 2022년08월18일

(71) 출원인
인천대학교 산학협력단
인천광역시 연수구 갯벌로 27, 인천대학교 이노베이션센터(송도동)
(72) 발명자
전광길
인천광역시 연수구 해송로 70, 209동 805호(송도동, 송도웹카운티2단지)
(74) 대리인
특허법인충정

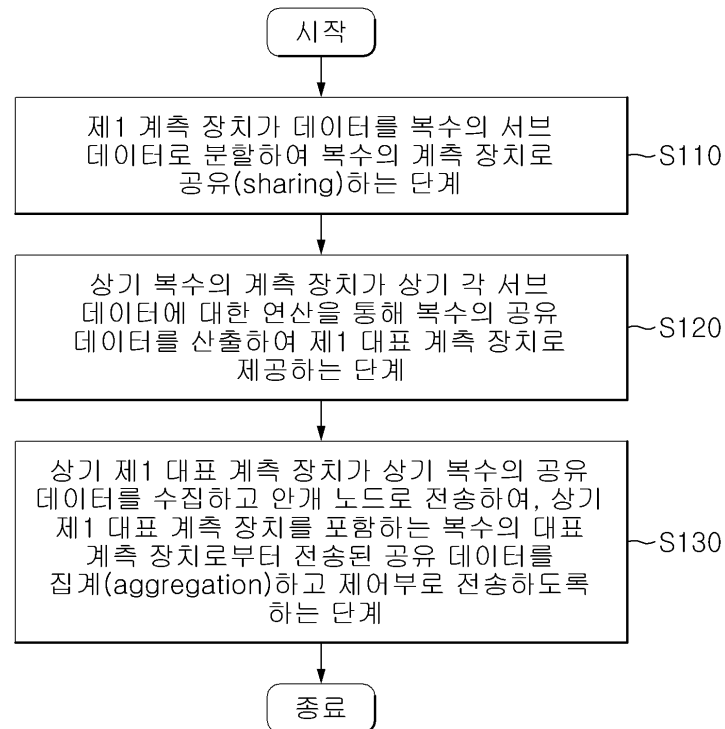
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 스마트 그리드에서의 데이터 처리 방법, 장치 및 시스템

(57) 요약

본 발명은 안개 노드가 구비되는 스마트 그리드에서의 보안 다자간 계산 기반 데이터 집계 방법, 장치 및 시스템에 관한 것으로서, 보다 구체적으로는 스마트 그리드에서 제어 센터와 스마트 미터 사이에 안개 노드를 구비하여 보안 다자간 계산 기반 데이터 집계를 통해 정보에 대한 보안을 확보하면서 효율적으로 데이터를 처리할 수 있는 (뒷면에 계속)

대표도 - 도2



안개 노드가 구비되는 스마트 그리드에서의 보안 다자간 계산 기반 데이터 집계 방법, 장치 및 시스템에 관한 것이다.

본 발명에서는, 제1 계측 장치가 데이터를 복수의 서브 데이터로 분할하여 복수의 계측 장치로 공유(sharing)하는 단계; 상기 복수의 계측 장치가 상기 각 서브 데이터에 대한 연산을 통해 복수의 공유 데이터를 산출하여 제1 대표 계측 장치로 제공하는 단계; 및 상기 제1 대표 계측 장치가 상기 복수의 공유 데이터를 수집하고 안개 노드로 전송하여, 상기 안개 노드가 상기 제1 대표 계측 장치를 포함하는 복수의 대표 계측 장치로부터 전송된 공유 데이터를 집계(aggregation)하고 제어부로 전송하도록 하는 단계;를 포함하는 것을 특징으로 하는 스마트 그리드에서의 데이터 집계 방법을 개시한다.

(52) CPC특허분류

H02J 3/00 (2023.08)

H04L 9/3247 (2013.01)

Y02E 40/70 (2020.08)

Y04S 20/30 (2020.08)

명세서

청구범위

청구항 1

제1 계측 장치가 데이터를 복수의 서버 데이터로 분할하여 복수의 계측 장치로 공유(sharing)하는 단계;
상기 복수의 계측 장치가 상기 각 서버 데이터에 대한 연산을 통해 복수의 공유 데이터를 산출하여 제1 대표 계측 장치로 제공하는 단계; 및
상기 제1 대표 계측 장치가 상기 복수의 공유 데이터를 수집하고 안개 노드로 전송하여, 상기 안개 노드가 상기 제1 대표 계측 장치를 포함하는 복수의 대표 계측 장치로부터 전송된 공유 데이터를 집계(aggregation)하고 제어부로 전송하도록 하는 단계;
를 포함하는 것을 특징으로 하는 스마트 그리드에서의 데이터 집계 방법.

청구항 2

제1항에 있어서,
상기 공유하는 단계는,
상기 제1 계측 장치가 상기 데이터를 다항식을 이용하여 복수의 서버 데이터로 분할하는 단계; 및
상기 제1 계측 장치가 미리 정해진 그룹 내에서 복수의 계측 장치를 랜덤하게 선택하여 상기 복수의 서버 데이터를 전송하는 단계;를 포함하는 것을 특징으로 하는 스마트 그리드에서의 데이터 집계 방법.

청구항 3

제1항에 있어서,
상기 공유하는 단계에서,
상기 제1 계측 장치는 자신을 대신하여 상기 안개 노드로 공유 데이터를 전송할 상기 제1 대표 계측 장치를 선정하여 상기 복수의 계측 장치로 공유하는 것을 특징으로 하는 스마트 그리드에서의 데이터 집계 방법.

청구항 4

제1항에 있어서,
상기 공유하는 단계에서,
상기 제1 계측 장치는 상기 복수의 서버 데이터와 함께 타임 스탬프 정보도 함께 공유하는 것을 특징으로 하는 스마트 그리드에서의 데이터 집계 방법.

청구항 5

제1항에 있어서,
상기 공유하는 단계에서,
상기 제1 계측 장치는 상기 복수의 서버 데이터와 함께 특정한 계측 장치가 연산을 수행하도록 하는 상태 정보도 함께 공유하는 것을 특징으로 하는 스마트 그리드에서의 데이터 집계 방법.

청구항 6

제1항에 있어서,
상기 공유하는 단계에서,
상기 제1 계측 장치는 상기 복수의 서버 데이터에 대한 암호화와 전자 서명을 수행하여 상기 복수의 계측 장치

로 공유하는 것을 특징으로 하는 스마트 그리드에서의 데이터 집계 방법.

청구항 7

제1항에 있어서,

상기 제공하도록 하는 단계에서,

상기 복수의 계측 장치는 라그랑주 보간법(Lagrange Interpolation)을 이용하여 상기 복수의 공유 데이터를 산출하는 것을 특징으로 하는 스마트 그리드에서의 데이터 집계 방법.

청구항 8

제7항에 있어서,

상기 복수의 계측 장치는 상기 복수의 공유 데이터에 대한 암호화와 전자 서명을 수행하여 상기 제1 대표 계측 장치로 제공하는 것을 특징으로 하는 스마트 그리드에서의 데이터 집계 방법.

청구항 9

제1항에 있어서,

상기 전송하도록 하는 단계에서,

상기 제1 대표 계측 장치는 파일리에 암호 시스템(Paillier cryptosystem)을 이용하여 상기 공유 데이터에 대한 암호화를 수행하는 것을 특징으로 하는 스마트 그리드에서의 데이터 집계 방법.

청구항 10

제8항에 있어서,

상기 전송하도록 하는 단계에서,

상기 안개 노드에서는 상기 전자 서명의 검증에 오류가 발생하는 경우 해당 공유 데이터를 폐기하는 것을 특징으로 하는 스마트 그리드에서의 데이터 집계 방법.

발명의 설명

기술 분야

[0001] 본 발명은 스마트 그리드에서의 데이터 처리 방법, 장치 및 시스템에 관한 것으로서, 보다 구체적으로는 스마트 그리드에서 제어 센터와 스마트 미터 사이에 안개 노드를 구비하여 보안 다자간 계산 기반 데이터 집계를 통해 정보에 대한 보안을 확보하면서 효율적으로 데이터를 처리할 수 있는 안개 노드가 구비되는 스마트 그리드에서의 보안 다자간 계산 기반 데이터 집계 방법, 장치 및 시스템에 관한 것이다.

배경 기술

[0002] 최근 통신 인프라, 감지 및 측정 기술을 사용하여 효율성과 신뢰성을 개선할 수 있는 전력 그리드 인프라로서 스마트 그리드(Smart Grid, SG)에 대한 연구가 활발히 이루어지고 있다.

[0003] 스마트 그리드(SG)는 전력망 관련 정보를 교환할 수 있는 양방향 통신을 제공할 수 있으며, 나아가 최신 통신 인프라, 감지 및 측정 기술, 도구를 사용하여 그리드를 보다 안정적이며 안전하고 친환경적으로 구현할 수 있을 뿐만 아니라, 풍력 및 태양광 발전과 같은 친환경 전력원과의 통합도 용이하는 등 다양한 장점을 가질 수 있다.

[0004] 이때, 스마트 그리드에서는 스마트 계량기(Smart Meter, SM)라고 하는 지능형 계량 인프라(Advanced Metering Infrastructure, AMI) 등을 사용하여 산출되는 다양한 정보가 전송될 수 있으므로 다량의 데이터를 효율적으로 처리할 수 있는 구조가 요구된다.

[0005] 나아가, 스마트 그리드에서 전송되는 데이터에는 고객의 식별 정보 및 전력 사용 데이터 등 고객에 대한 정보가 포함될 수 있으므로 공격자가 고객에 대한 민감한 정보를 해킹할 수도 있는 바, 적절한 보안 메커니즘을 통해 고객 관련 정보를 안전하게 관리하지 못한다면 심각한 보안 문제가 초래될 수도 있다.

[0006] 특히, 일반적으로 스마트 그리드의 제어 센터에서는 고객에 대한 세분화된 데이터가 정기적으로 수집될 수 있으며, 이러한 세분화된 데이터에 대하여 적절한 보안 및 개인 정보 보호 메커니즘으로 처리되지 않는 경우 외부로 노출될 수 있으며, 나아가 다량의 데이터를 스마트 계량기(SM)에서 제어 센터로 전송하면서 높은 대기 시간 및 혼잡도, 위치 추적 가능성 등의 보안 위험이 따르게 된다.

[0007] 이에 따라, 스마트 그리드에서 다량의 데이터를 효율적으로 처리할 수 있으며, 나아가 고객 관련 정보에 대한 보안을 강화할 수 있는 방안이 요구되고 있으나, 아직 이에 대한 적절한 해법이 제시되지 못하고 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 대한민국 공개특허공보 제10-2022-0072032호(2022년 6월 2일 공개)

발명의 내용

해결하려는 과제

[0009] 본 발명은 상기와 같은 종래 기술의 문제점을 해결하기 위해 창안된 것으로, 스마트 그리드에서 다량의 데이터를 효율적으로 처리할 수 있으며, 나아가 고객 관련 정보에 대한 보안을 강화할 수 있는 스마트 그리드 시스템을 제공하는 것을 목적으로 한다.

[0010] 그 외 본 발명의 세부적인 목적은 아래에 기재되는 구체적인 내용을 통하여 이 기술 분야의 전문가나 연구자에게 자명하게 파악되고 이해될 수 있을 것이다.

과제의 해결 수단

[0011] 상기 과제를 해결하기 위한 본 발명의 한 측면에 따른 스마트 그리드에서의 데이터 집계 방법은, 제1 계측 장치가 데이터를 복수의 서브 데이터로 분할하여 복수의 계측 장치로 공유(sharing)하는 단계; 상기 복수의 계측 장치가 상기 각 서브 데이터에 대한 연산을 통해 복수의 공유 데이터를 산출하여 제1 대표 계측 장치로 제공하는 단계; 및 상기 제1 대표 계측 장치가 상기 복수의 공유 데이터를 수집하고 안개 노드로 전송하여, 상기 안개 노드가 상기 제1 대표 계측 장치를 포함하는 복수의 대표 계측 장치로부터 전송된 공유 데이터를 집계(aggregation)하고 제어부로 전송하도록 하는 단계;를 포함하는 것을 특징으로 한다.

[0012] 여기서, 상기 공유하는 단계는, 상기 제1 계측 장치가 상기 데이터를 다항식을 이용하여 복수의 서브 데이터로 분할하는 단계; 및 상기 제1 계측 장치가 미리 정해진 그룹 내에서 복수의 계측 장치를 랜덤하게 선택하여 상기 복수의 서브 데이터를 전송하는 단계;를 포함할 수 있다.

[0013] 또한, 상기 공유하는 단계에서, 상기 제1 계측 장치는 자신을 대신하여 상기 안개 노드로 공유 데이터를 전송할 상기 제1 대표 계측 장치를 선정하여 상기 복수의 계측 장치로 공유할 수 있다.

[0014] 또한, 상기 공유하는 단계에서, 상기 제1 계측 장치는 상기 복수의 서브 데이터와 함께 타임 스탬프 정보도 함께 공유할 수 있다.

[0015] 또한, 상기 공유하는 단계에서, 상기 제1 계측 장치는 상기 복수의 서브 데이터와 함께 특정한 계측 장치가 연산을 수행하도록 하는 상태 정보도 함께 공유할 수 있다.

[0016] 또한, 상기 공유하는 단계에서, 상기 제1 계측 장치는 상기 복수의 서브 데이터에 대한 암호화와 전자 서명을 수행하여 상기 복수의 계측 장치로 공유할 수 있다.

[0017] 또한, 상기 제공하도록 하는 단계에서, 상기 복수의 계측 장치는 라그랑주 보간법(Lagrange Interpolation)을 이용하여 상기 복수의 공유 데이터를 산출할 수 있다.

[0018] 이때, 상기 복수의 계측 장치는 상기 복수의 공유 데이터에 대한 암호화와 전자 서명을 수행하여 상기 제1 대표 계측 장치로 제공할 수 있다.

[0019] 또한, 상기 전송하도록 하는 단계에서, 상기 제1 대표 계측 장치는 파일리에 암호 시스템(Paillier cryptosystem)을 이용하여 상기 공유 데이터에 대한 암호화를 수행할 수 있다.

[0020] 나아가, 상기 전송하도록 하는 단계에서, 상기 안개 노드에서는 상기 전자 서명의 검증에 오류가 발생하는 경우 해당 공유 데이터를 폐기할 수 있다.

발명의 효과

[0021] 이에 따라, 본 발명의 일 실시예에 따른 안개 노드가 구비되는 스마트 그리드에서의 보안 다자간 계산 기반 데이터 집계 방법, 장치 및 시스템에서는, 스마트 그리드에서 다량의 데이터를 효율적으로 처리할 수 있으며, 나아가 고객 관련 정보에 대한 보안을 강화할 수 있게 된다.

[0022] 나아가, 본 발명의 일 실시예에 따른 안개 노드가 구비되는 스마트 그리드에서의 보안 다자간 계산 기반 데이터 집계 방법, 장치 및 시스템에서는 담합 공격(colluded attack)을 방지할 수 있을 뿐만 아니라, 내결함성(fault-tolerant)을 가지므로 일부 스마트 계량기(SM)에서 오류가 발생하더라도 데이터의 집계가 가능하며, 나아가 FDI(False Data Injection) 및 재생 공격(replay attack)에 대해서도 효과적인 대응이 가능하게 된다.

도면의 간단한 설명

[0023] 본 발명에 관한 이해를 돕기 위해 상세한 설명의 일부로 포함되는, 첨부도면은 본 발명에 대한 실시예를 제공하고, 상세한 설명과 함께 본 발명의 기술적 사상을 설명한다.

도 1 은 본 발명의 일 실시예에 따른 스마트 그리드(100)의 구성을 설명하는 도면이다.

도 2는 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법의 순서도이다.

도 3 내지 도 4는 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법의 동작을 설명하는 도면이다.

도 5 내지 도 12는 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법 및 시스템의 구체적인 알고리즘을 예시하는 도면이다.

도 13 내지 도 20은 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법의 결과와 성능을 설명하는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0024] 본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 이하에서는 특정 실시예들을 첨부된 도면을 기초로 상세히 설명하고자 한다.

[0025] 이하의 실시예는 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0026] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시 예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0027] 또한, 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되는 것은 아니며, 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0028] 먼저, 도 1에서는 본 발명의 일 실시예에 따른 스마트 그리드(Smart Grid, SG)(100)의 구성을 설명하는 도면을 예시하고 있다. 도 1에서 볼 수 있는 바와 같이, 본 발명의 일 실시예에 따른 스마트 그리드(100)는 제어부(110), 안개 노드(Fog Node, FN)(120) 및 계측 장치(130)를 포함하여 구성될 수 있다.

[0029] 이때, 상기 제어부(110)는 클라우드 시스템으로 구성되는 클라우드 제어 센터(Cloud Control Center, CCC)일 수

있으나, 본 발명이 반드시 이에 한정되는 것은 아니다.

- [0030] 또한, 상기 안개 노드(120)는 상기 클라우드 제어 센터(CCC) 등 제어부(110)와 계측 장치(130) 사이에 위치하여 상기 계측 장치(130)로부터 전송되는 데이터를 처리하거나 상기 제어부(110)로 전송할 수 있다.
- [0031] 또한, 상기 계측 장치(130)는 스마트 미터(Smart Meter) 등과 같은 지능형 계측 인프라(Advanced Metering Infrastructure, AMI)일 수 있으나, 본 발명이 반드시 이에 한정되는 것은 아니며, 이외에도 스마트 그리드(100)에서의 전압, 전류, 전력 등의 물리량을 계측(metering)할 수 있는 다양한 장치가 사용될 수 있다.
- [0032] 또한, 도 2에서는 본 발명의 일 실시예에 따른 스마트 그리드(100)에서의 데이터 집계 방법의 순서도를 도시하고 있으며, 도 3에서는 본 발명의 일 실시예에 따른 스마트 그리드(100)에서의 데이터 집계 방법을 설명하기 위한 도면을 예시하고 있다.
- [0033] 이때, 도 2 및 도 3에서 볼 수 있는 바와 같이, 본 발명의 일 실시예에 스마트 그리드(100)에서의 데이터 집계 방법은, 제1 계측 장치(130a)가 데이터를 복수의 서브 데이터로 분할하여 복수의 계측 장치로 공유(sharing)하는 단계(S110), 상기 복수의 계측 장치가 상기 각 서브 데이터에 대한 연산을 통해 복수의 공유 데이터를 산출하여 제1 대표 계측 장치(130n)로 제공하는 단계(S120) 및 상기 제1 대표 계측 장치(130n)가 상기 복수의 공유 데이터를 수집하고 안개 노드(120)로 전송하여, 상기 안개 노드(120)가 상기 제1 대표 계측 장치(130n)를 포함하는 복수의 대표 계측 장치로부터 전송된 공유 데이터를 집계(aggregation)하고 제어부(110)로 전송하도록 하는 단계(S130)를 포함하여 구성될 수 있다.
- [0034] 여기서, 도 4에서 볼 수 있는 바와 같이, 상기 공유하는 단계(S110)는, 상기 제1 계측 장치(130a)가 상기 데이터를 다항식을 이용하여 복수의 서브 데이터로 분할하는 단계(S111) 및 상기 제1 계측 장치(130a)가 미리 정해진 그룹 내에서 복수의 계측 장치를 랜덤하게 선택하여 상기 복수의 서브 데이터를 전송하는 단계(S112)를 포함할 수 있다.
- [0035] 또한, 상기 공유하는 단계(S110)에서, 상기 제1 계측 장치(130a)는 자신을 대신하여 상기 안개 노드(120)로 공유 데이터를 전송할 상기 제1 대표 계측 장치(130n)를 선정하여 상기 복수의 계측 장치로 공유할 수 있다.
- [0036] 또한, 상기 공유하는 단계(S110)에서, 상기 제1 계측 장치(130a)는 상기 복수의 서브 데이터와 함께 타임 스탬프 정보도 함께 공유할 수 있다.
- [0037] 또한, 상기 공유하는 단계(S110)에서, 상기 제1 계측 장치(130a)는 상기 복수의 서브 데이터와 함께 특정한 계측 장치가 연산을 수행하도록 하는 상태 정보도 함께 공유할 수 있다.
- [0038] 또한, 상기 공유하는 단계(S110)에서, 상기 제1 계측 장치(130a)는 상기 복수의 서브 데이터에 대한 암호화와 전자 서명을 수행하여 상기 복수의 계측 장치로 공유할 수 있다.
- [0039] 또한, 상기 전송하도록 하는 단계(S120)에서, 상기 복수의 계측 장치는 라그랑주 보간법(Lagrange Interpolation)을 이용하여 상기 복수의 공유 데이터를 산출할 수 있다.
- [0040] 이때, 상기 복수의 계측 장치는 상기 복수의 공유 데이터에 대한 암호화와 전자 서명을 수행하여 상기 제1 대표 계측 장치(130n)로 제공할 수 있다.
- [0041] 또한, 상기 전송하도록 하는 단계(S130)에서, 상기 제1 대표 계측 장치(130n)는 파일리에 암호 시스템(Paillier cryptosystem)을 이용하여 상기 공유 데이터에 대한 암호화를 수행할 수 있다.
- [0042] 나아가, 상기 전송하도록 하는 단계(S130)에서, 상기 안개 노드(120)에서는 상기 전자 서명의 검증에 오류가 발생하는 경우 해당 공유 데이터를 폐기할 수 있다.
- [0043] 이에 따라, 본 발명의 일 실시예에 따른 스마트 그리드(100)에서의 데이터 집계 방법에서는, 스마트 그리드(100)에서 다량의 데이터를 효율적으로 처리할 수 있으며, 나아가 고객 관련 정보에 대한 보안을 강화할 수 있게 된다.
- [0044] 이하, 본 발명의 일 실시예에 따른 안개 노드가 구비되는 스마트 그리드(100)에서의 보안 다자간 계산 기반 데이터 집계 방법, 장치 및 시스템에 대한 예시적인 실시 형태들을 첨부된 도면을 참조하여 보다 자세하게 설명한다.
- [0045] 먼저, 도 3을 참조하여 살펴보면, 본 발명의 일 실시예에 따른 스마트 그리드(100)에는 제어부(110), 안개 노드(120), 계측 장치(130)가 구비될 수 있으며, 또한 신뢰 인증부(140)가 구비될 수도 있다.

- [0046] 이때, 상기 신뢰 인증부(140)는 Trusted Authority(TA)일 수 있으며, 이때 TA의 주요 역할은 스마트 그리드(SG)의 주요 구성 요소(entity)들을 생성하고 등록하는 것이다. 이에 따라, 스마트 그리드(SG)에 구성 요소가 추가되거나 제거되면 TA 데이터베이스에서 해당 세부 정보를 업데이트하게 된다. TA는 스마트 미터(SM)에 결합이 있는 경우에도 유용할 수 있으며, 이때 TA는 스마트 미터(SM)를 관리하는 공급 업체 등에 통보하여 오류가 발생한 스마트 미터(SM)를 보완하도록 처리할 수 있다.
- [0047] 또한, 상기 제어부(110)는 클라우드 제어 센터(CCC)일 수 있으며, 클라우드 제어 센터(CCC)는 매우 신뢰할 수 있는 기관으로서, CCC는 안개 노드(FN)을 통한 계량 데이터 수집을 담당하고, 또한 수집된 데이터를 기반으로 다양한 분석을 수행하며 수요 대응, 예측, 과금 등 스마트 그리드(SG) 운영을 관리하게 된다.
- [0048] 또한, 상기 안개 노드(120)는 스마트 미터(SM)과 클라우드 제어 센터(CCC) 사이에 위치하는 중간 노드로서, 스마트 미터(SM)의 데이터를 수집하여 클라우드 제어 센터(CCC)에 제공하게 된다.
- [0049] 또한, 상기 계측 장치(130)는 스마트 미터(SM)일 수 있으며, 보다 구체적인 예를 들어 HAN(Home Area Network)에 설치된 AMI(Advanced Metering Infrastructure) 장치로서 고객 구내에서 사용 데이터를 수집하고 안개 노드(FN)를 통해 클라우드 제어 센터(CCC)로 제출할 수 있으며, 클라이언트의 사용 데이터를 암호화된 형식으로 전송하는 것이 가능하다.
- [0050] 이때, 본 발명에서 상기 계측 장치(130) 중 대표 계측 장치는 DSM(Designated Smart Meter)로서 인접 스마트 미터(SM)로부터 공유되는 데이터를 수집하여 재구성할 수 있으며, 나아가 전자 서명을 생성하여 스마트 미터(SM)를 대신해 안개 노드(FN)로 제출할 수 있다.
- [0051] 또한, 본 발명의 일 실시예에 따른 스마트 그리드(100)에서, 상기 안개 노드(FN)와 클라우드 제어 센터(CCC)는 고객의 스마트 미터(SM) 데이터를 보안 특성으로 인해 확인할 수 없으며, 이때 고객의 스마트 미터(SM) 데이터는 Paillier 암호 시스템을 통해 인코딩되어 될 수 있으며, 이에 따라 Paillier 암호화의 동형 속성으로 인해 안개 노드(FN) 또는 기타 엔티티(entity)는 스마트 미터(SM) 정보를 확인하기 어렵다. 또한, 스마트 미터(SM)의 소스는 ECDSA(Elliptic Curve Digital Signature Scheme)을 통해 안개 노드(FN)에 의해 검증될 수 있다.
- [0052] 이어서, 상기 안개 노드(FN)에서는 복수의 스마트 미터(SM)로부터 데이터를 수집하여 집계(aggregation)할 수 있다. 이에 따라, 상기 클라우드 제어 센터(CCC)는 최종 집계 데이터를 관독하게 된다.
- [0053] 이때, 본 발명에서는 공격자의 모델로서 다음과 같은 전제 하에서 아래와 같은 공격을 수행할 수 있다고 가정한다.
- [0054] 1. 공격자는 스마트 미터(SM)와 클라우드 제어 센터(CCC) 간의 통신을 도청할 수 있다.
- [0055] 2. 공격자는 스마트 미터(SM)에서 안개 노드(FN)로 또는 안개 노드(FN)에서 클라우드 제어 센터(CCC)로 전송되는 메시지를 조작할 수 있다.
- [0056] 3. 스마트 미터(SM) 구성에 대한 지식이 있는 내부 공격자는 측정 데이터를 조작할 수 있다.
- [0057] 4. 오작동으로 인해 스마트 미터(SM) 데이터가 안개 노드(FN)에 도달할 수도 있다.
- [0058] 5. 클라우드 제어 센터(CCC)와 안개 노드(FN)은 함께 결탁하여 스마트 미터(SM) 데이터를 확인하거나 공개할 수 있습니다.
- [0059] 6. 공격자는 재생 공격(replay attack), FDI(False Data Injection), 메시지 변조 공격(message modification attack), 무단 접근(unauthorized access) 등의 공격을 수행할 수 있다.
- [0060] 7. 또한 본 발명에서는 클라우드 제어 센터(CCC)와 연기 노드(FN)은 신뢰할 수 없는 엔티티(entity)일 수 있고, 모든 스마트 미터(SM)가 정상 동작하지 않을 수 있으며, 통신 채널도 안전하지 않을 수 있다.
- [0061] 이에 대하여, 본 발명의 일 실시예에 따른 스마트 그리드(100)에서의 데이터 집계 방법 및 시스템의 구성 및 동작을 살펴보면 아래와 같다.
- [0062] 앞서 설명한 바와 같이, 상기 신뢰 인증부(140)는 Trusted Authority (TA)일 수 있으며, 이때 TA는 Paillier 암호 시스템을 사용하여 스마트 미터(SM), 안개 노드(FN) 및 클라우드 제어 센터(CCC)에 대한 키 생성을 담당할 수 있고, 생성된 키는 암호화 및 암호 해독 목적으로 사용될 수 있다. 보다 구체적으로, TA는 또한 스마트 미터(SM) 및 안개 노드(FN)에 대한 한 쌍의 개인(private) 및 공개(public) 키를 생성할 수 있고, 이러한 키는 디지털 서명 생성 및 검증에 사용될 수 있다.

- [0063] 또한, 상기 계측 장치(130)는 스마트 미터(SM)일 수 있으며, 이때 스마트 미터(SM)는 연기 노드(FN)와 사용 데이터를 공유하는 역할을 수행할 수 있다. 이때, 각 SM_i 는 고유 포인트(unique point) $x_i \in \mathbb{Z}_p$ 를 선택하게 되고, 또한 $n-1$ 차원($n-1$ degree)의 랜덤 비밀 다항식(random secret polynomial) $f_i(x)$ 도 선택할 수 있으며, 이때 $f_i(x) = s$ 가 된다(여기서, s 는 SM_i 의 개인 비밀 정보(private secret)가 됨). 이어서, SM_i 는 상기 x_i 를 이웃 스마트 미터(SM)로 배포하게 된다.
- [0064] 이때, 상태 값(r 이 0 또는 1)에 따라 스마트 미터(SM)는 공유 데이터를 계산하거나 계산하지 않을 수도 있으며, 이어서 상기 SM_i 에 대하여 다른 스마트 미터(SM)가 모두 공유 데이터를 계산하여 제1 대표 계측 장치(130n)인 SM_{Lagg} 와 공유할 수 있다. 이에 따라, 상기 SM_{Lagg} 는 SM_i 를 대신하여 최종적인 비밀 데이터를 계산하는 역할을 수행하게 되며, 나아가 상기 SM_{Lagg} 는 Paillier 암호화를 통해 데이터를 암호화하고 디지털 서명을 생성하여 안개 노드(FN)로 제출할 수 있다.
- [0065] 이에 따라, 상기 안개 노드(FN)에서는 각 스마트 미터(SM)로부터 전송되는 비밀 데이터의 디지털 서명을 확인하고 집계(aggregation)를 수행할 수 있다. 이때, 안개 노드(FN)는 또한 집계된 데이터에 대한 디지털 서명을 생성할 수 있으며, 서명 및 집계 데이터는 클라우드 제어 센터(CCC)로 전송될 수 있다.
- [0066] 이어서, 클라우드 제어 센터(CCC)는 안개 노드(FN)에서의 전자 서명을 확인하고 개인키로 수신한 데이터를 복호화할 수 있다.
- [0067] 또한, 다음 데이터 수집 슬롯에 대해 동일한 사이클이 반복될 수 있다.
- [0068] 이와 같이, 본 발명에는 (i) 키 생성, (ii) 스마트 미터(SM)에서의 비밀 공유 생성 및 공유 (iii) 인접한 스마트 미터(SM)에 의한 공유 계산 (iv) 대표 스마트 미터(Aggregator SM)에서의 공유 집계 (v) 연기 노드(FN)에서의 집계 및 (vi) 클라우드 제어 센터(CCC)에서 복호화를 포함할 수 있다.
- [0069] 이와 관련하여, 본 발명에서 사용하는 기호 목록과 그에 대한 설명은 도 5에 정리되어 있다.
- [0070] (i) 키 생성
- [0071] 먼저 키 생성 작업에서는 스마트 미터(SM), 연기 노드(FN) 및 클라우드 제어 센터(CCC)에서의 암호화, 암호 해독, 서명 생성 및 확인을 위해 사용되는 개인(private) 및 공개(public) 키를 생성하게 된다. 이때, Paillier 공개 키는 동형 데이터 암호화에 필요하고 개인 키는 동형 복호화에 필요하다.
- [0072] 보다 구체적으로, Paillier 암호 시스템에서 TA는 두 개의 큰 소수를 선택하고 공개 키(N, g) 및 개인 키(λ, μ)를 산출할 수 있으며, 또한 TA는 스마트 미터(SM) 및 안개 노드(FN)에 대한 개인 및 공개 키 쌍 (s_k^{sm}, p_k^{sm}) 및 (s_k^{fn}, p_k^{fn}) 도 생성할 수 있다. 이러한 키는 전자 서명의 생성 및 검증에 사용될 수 있다. 키 생성 완료 이후 집계 과정에서는 TA의 역할이 없으며 스마트 그리드(SG) 네트워크에 가입하거나 탈퇴하는 경우 스마트 미터(SM)를 추가하거나 제거하는 경우에만 필요하게 된다.
- [0073] 상기 (i) 키 생성 단계에 대한 구체적인 알고리즘 1은 도 6에 도시되어 있다.
- [0074] (ii) SM에서의 비밀 공유 생성 및 공유
- [0075] 본 작업에서 SM_i 는 다항식 함수 $f(x)$ 를 이용하여 스마트 미터(SM) 데이터를 분할하게 된다. 이때, SM_i 는 그룹(예를 들어, 도 3의 (A)) 내에서 이웃 SM(SM_{jList})을 무작위로 선택하고(수학식 1) SM 데이터의 일부를 포인트 형태로 이웃 SM과 공유할 수 있다.
- [0076] [수학식 1]
- $$SM_{jList} = RandomListGen(SM_i)$$
- [0077]
- [0078] 이때, SM_i 는 SM_{Lagg} 를 선택하여 지정하게 되며, 상기 SM_{Lagg} 는 SM_i 이웃으로부터 받은 공유 값을 재구성하고 SM_i 를 대신하여 연기 노드(FN)로 제출하게 된다.

[0079] [수학식 2]

$$[0080] \quad SM_{Lagg} = RandomSMsel(SM_i)$$

[0081] 또한, 수학식 3과 같이 SM_i 는 암호화된 비밀 부분 (x_i, y_i) 및 서명 σ_{smi} 을 이웃 SM과 공유하게 된다. 이때, 상
태 값 r 은 이웃 SM의 비밀 공유 계산을 촉진하는 데 사용될 수 있으며, 보다 구체적으로 $r = 0$ 이면 특정 이웃
SM이 비밀 공유 값을 계산하는 것이 선택 사항으로 처리될 수 있음을 의미하게 된다. 또한, 타임스탬프 t_i 는 현
재의 타임 스탬프를 나타내게 된다.

[0082] [수학식 3]

$$[0083] \quad c_i = Enc((x_i, y_i), SM_{Lagg}, t_i, r)$$

[0084] 상기 (ii) SM에서의 비밀 공유 생성 및 공유 단계에 대한 구체적인 알고리즘 2는 도 7에 도시되어 있다.

[0085] (iii) 인접한 스마트 미터(SM)에 의한 공유 계산

[0086] 본 작업에서 SM_i 이웃은 자신의 공유 가치 $Value_j$ 를 계산하여 SM_{Lagg} 로 제출하게 된다. 이때, 수학식 4는 SM_i 의
모든 이웃이 라그랑주 보간법(Lagrange Interpolation)을 통해 공유 가치를 계산하는 데 사용될 수 있으며, 이
를 통해 수학식 5 및 수학식 6의 암호화 및 서명 생성이 $Value_j$ 에 기반하여 수행될 수 있다.

[0087] [수학식 4]

$$[0088] \quad Value_j = f(x_j)l(x_j)$$

[0089] [수학식 5]

$$[0090] \quad c_j = Enc(Value_j, t_i)$$

[0091] [수학식 6]

$$[0092] \quad \sigma_{smj} = s_k^{smj} (H(c_j \parallel t_i))$$

[0093] 상기 (iii) 인접한 스마트 미터(SM)에 의한 공유 계산 단계에 대한 구체적인 알고리즘 3은 도 8에 도시되어 있
다.

[0094] (iv) 대표 스마트 미터(Aggregator SM)에서의 공유 집계

[0095] 본 작업에서 SM_{Lagg} 는 SM_i 이웃이 제출한 공유 값을 집계하게 된다. 집계된 데이터에 대해 Paillier 암호 시스템
방식을 통해 암호화를 수행하고 디지털 서명을 생성하며, 서명 σ_{smi} 와 함께 암호문 c_i 는 SM_i 를 대신하여 각 연기
노드(FN)로 제출된다.

[0096] [수학식 7]

$$[0097] \quad SM_{val} = \sum_{k=1}^d c_k$$

[0098] [수학식 8]

$$[0099] \quad c_i = Enc(SM_{val}) = g^{SM_{val}} h^{rt}$$

[0100] [수학식 9]

$$\sigma_{smLagg} = s_k^{smLagg} (H(c_i \parallel t_i))$$

[0101]

[0102] 상기 (iv) 대표 스마트 미터(Aggregator SM)에서의 공유 집계 단계에 대한 구체적인 알고리즘 4는 도 9에 도시되어 있다.

[0103] (v) 연기 노드(FN)에서의 집계

[0104] 본 작업에서 연기 노드(FN)는 암호문 c_i 의 공개 키 P_k^{sm} 을 통해 스마트 미터(SM)의 서명과 신원을 확인하게 된다. 이때, SM_i의 전자 서명 σ_{smi} 가 검증되지 않은 경우 데이터가 삭제될 수 있다. 이에 따라, 연기 노드(FN)은 연결된 스마트 미터(SM)로부터 수신한 데이터를 집계(aggregation)하게 된다

[0105] [수학식 10]

$$C_{fn} = \prod_{i=1}^n c_i$$

[0106]

[0107] 데이터가 집계되면 연기 노드(FN)는 수학식 11과 같이 집계된 암호문 데이터에 디지털 서명을 생성하게 된다

[0108] [수학식 11]

$$\sigma_{fn} = s_k^{fn} (H(C_{fn} \parallel t_i))$$

[0109]

[0110] 상기 (v) 연기 노드(FN)에서의 집계 단계에 대한 구체적인 알고리즘 5는 도 10에 도시되어 있다.

[0111] (vi) 클라우드 제어 센터(CCC)에서 복호화

[0112] 본 작업에서 클라우드 제어 센터(CCC)는 디지털 서명을 확인하고 연결된 연기 노드(FN)에서 집계된 데이터의 복호화를 수행하게 된다. 이때 서명이 유효하면 수학식 12 내지 수학식 13을 통해 복호화를 수행하게 된다

[0113] [수학식 12]

$$C_I = \left(g^{r \sum_i^n m_i} h^r \right)^{t^{-1}}$$

[0114]

[0115] [수학식 13]

$$ch^{-r} = g^{r \sum_i^n m_i}$$

[0116]

[0117] 이때, 클라우드 제어 센터(CCC)는 이산 대수를 통해 $g^{r \sum_i^n m_i}$ 를 계산하고 수학식 14와 같이 Pollard의 람다 방법을 사용하여 M_{sum} 을 산출하게 된다.

[0118] [수학식 14]

$$M_{sum} = \sum_i^n m_i$$

[0119]

[0120] 상기 (vi) 클라우드 제어 센터(CCC)에서 복호화 단계에 대한 구체적인 알고리즘 6은 도 11에 도시되어 있다.

[0121] 이에 따라, 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법은 도 12와 같이 수행될 수 있다. 도 12의 블록도에서는 스마트 미터(SM), 연기 노드(FN), 클라우드 제어 센터(CCC) 간의 데이터 집합 흐름을 나타낸다. 도 12에서 SM_i는 자신의 비밀을 분할하고 그룹의 이웃 스마트 미터(SM)와 비밀의 일부분을 공유하게 된다. 이에 따라, 이웃 스마트 미터(SM)는 자신의 부분을 계산하고 그 결과를 대표 스마트 미터(Aggregator

SM)와 공유한다. 대표 스마트 미터(Aggregator SM)은 이웃 스마트 미터(SM)로부터 수신한 값을 기반으로 최종 비밀 값을 재구성한다. 재구성 후 데이터는 Paillier 암호 시스템을 통해 암호화되고 서명은 ECDSA를 사용하여 생성되며, 상기 데이터와 서명 둘 다 집계(aggregation)를 위해 연기 노드(FN)로 제출된다.

[0122] 이에 따라, 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법에서는 다음과 같이 개인 정보 보호와 FDI(False Data Injection) 및 재생 공격(replay attack)에 효과적으로 대응할 수 있게 된다.

[0123] (1) 먼저, 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법에서 SM 미터링 데이터는 담합 공격으로부터 보호될 수 있다.

[0124] 보다 구체적으로, 본 발명에서 SM_i 데이터는 SMPC(Secure Multi-Party Computation)를 통해 통신하며 실제 ID는 통신 중에 숨겨지게 된다. 여기서, SM_i 는 이웃 SM과 아래 수학식 15와 같이 다항식 함수 $f(x)$ 를 사용하여 점 형태로 비밀을 배포하게 된다. 이때, 이웃 SM은 라그랑주 보간법(Langrage Interpolation) $P(x)$ 를 사용하여 비밀 공유 값을 계산하고 SM_i 가 지명한 SM_{Lagg} 로 전송하여 이웃 SM으로부터의 데이터 수집을 처리하게 된다. SM_{Lagg} 는 이웃 SM으로부터 수신된 데이터를 집계하고 SM_i 를 대신하여 안개 노드(FN)로 전송한다. 안개 노드(FN), 클라우드 제어 센터(CCC) 및 일부 스마트 미터(SM)가 담합하여 공격에 사용되더라도 SM_i 데이터를 재구성할 수 없으며, SM_i 데이터의 재구성을 위해서는 충분한 수의 이웃 스마트 미터(SM)가 해킹되어 공격에 가담하여야 가능할 수 있다.

[0125] [수학식 15]

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1}$$

[0126]

[0127] 여기서 a_0 은 SM 비밀 데이터 S이고, $a_1, a_2, \dots, a_{k-1}$ 은 무작위로 선택된 양의 정수이다. 이에 따라, 상기 $f(x)$ 를 통해 구성을 공유하고 점(x, y)을 생성하며, 상기 점을 SM_j 와 공유하게 된다. 다른 스마트 미터(SM)에서 산출된 공유치는 아래 수학식 16과 같이 라그랑주 보간법(Langrage Interpolation)을 통해 계산될 수 있다.

[0128] [수학식 16]

$$P(x) = \sum_{j=1}^k p_{j(x)}$$

[0129]

[0130] 모든 공유치는 SM_{Lagg} 에 의하여 합산되어 산출될 수 있다.

[0131] [수학식 17]

$$P_j(x) = y_i \prod_{m=1, m \neq j}^k \frac{x - x_m}{x_j - x_m}$$

[0132]

[0133] (2) 또한, 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법에서, 사용 데이터를 제출한 스마트 미터(SM)가 도용된 경우에도 소스 스마트 미터(SM)의 실제 신원이 노출되는 것을 방지할 수 있다.

[0134] 이에 따라, 본 발명에서는 공격자가 스마트 미터(SM) 세트를 손상시키는 경우에도 소스 스마트 미터(SM)의 실제 신원은 공격자로부터 노출되는 것이 방지될 수 있다. 보다 구체적으로, 본 발명에서는 수정된 샤미르의 비밀 구조(modified Shamir's secret scheme)를 이용하여 스마트 미터(SM)가 그룹으로 나누어 질 수 있다(도 3의 (A)). 이에 따라, SM_i 가 특정 안개 노드(FN)로 데이터를 공유하고자 할 때 포인트(x,y) 형태로 데이터를 배포하게 되며, 상기 포인트는 그룹 내의 이웃 스마트 미터(SM)와 공유된다. 또한, SM_i 는 이웃 스마트 미터(SM)로부터 계산된 일부 계산치를 수신하여 집계할 SM_{Lagg} 를 지정한다. 이에 따라, SM_{Lagg} 는 SM_i 를 대신하여 집계된 값을 안개 노드(FN)로 전송한다. 상기 프로세스는 데이터 집계(aggregation)에 자신의 데이터를 반영하고자 하는 모든 스마트 미터(SM)에 의해 반복하여 수행될 수 있다. 이때, 공격자 A가 SM_{Lagg} 를 손상시키는 경우에도 상기 데이터에서 소스 SM_i 를 식별할 수 없으며, 암호화된 값 c_i 는 모든 이웃 스마트 미터(SM)와 공유된다.

[0135] [수학식 18]

$$c_i = Enc((x_i, y_i), SM_{Lagg}, t_i, r)$$

[0136]

[0137] 이때, 공유 데이터 Value_j는 각 이웃 스마트 미터(SM)에 의하여 산출될 수 있다.

[0138] [수학식 19]

$$Value_j = f(x_j)l(x_j)$$

[0139]

[0140] 또한, 암호화된 값은 이웃 스마트 미터(SM)에서 지정된 스마트 미터(SM_{agg})로 공유된다.

[0141] [수학식 20]

$$c_j = Enc(Value_j, t_i)$$

[0142]

[0143] 이에 따라, 상기 계산된 공유값은 아래 수학식 21과 같이 집계(aggregation)될 수 있다.

[0144] [수학식 21]

$$SM_{val} = \sum_{k=1}^d c_k$$

[0145]

[0146] 최종적으로, 암호화된 값(C_{smval})은 SM_i를 대신하여 SM_j에 의하여 제출되게 된다.

[0147] (3) 또한, 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법에서는, 클라우드 제어 센터(CC C)가 침해되더라도 개별 사용자의 데이터가 노출되는 것을 방지할 수 있게 된다.

[0148] 보다 구체적으로, 클라우드 제어 센터(CCC) 내부의 일부 서버가 내부 공격이나 오작동으로 인해 훼손된 경우에도 공격자는 스마트 미터(SM)의 개별 데이터가 아닌 데이터 집계(aggregation) 값만을 얻을 수 있으며, 이는 클라우드 제어 센터(CCC)가 개별 스마트 미터(SM) 데이터가 아닌 안개 노드(FN)에서 집계된 데이터를 수신하기 때문이다. 이에 따라, 클라우드 제어 센터(CCC)는 집계된 데이터를 복호화한 후 총 소비 사용량 값만 얻을 수 있다.

[0149] [수학식 22]

$$C_I = \left(g^{r \sum_i^n m_i} h^r \right)^{r^{-1}}$$

[0150]

[0151] 이때, 수학식 22의 양변을 h^r 로 나누면 수학식 23 이 되고, 이로부터 수학식 24가 산출될 수 있다.

[0152] [수학식 23]

$$\frac{C_I}{h^r} = g^{r \sum_i^n m_i} \frac{h^r}{h^r}$$

[0153]

[0154] [수학식 24]

$$C_I h^{-r} = g^{r \sum_i^n m_i}$$

[0155]

[0156] 이에 따라, 클라우드 제어 센터(CCC)는 이산 로그(discrete log)를 통해 수학식 25를 산출할 수 있게 된다.

[0157] [수학식 25]

$$M_{sum} = \sum_i^n m_i$$

[0158]

[0159] (4) 또한, 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법에서는, 공격자가 재생 공격을 통해서도 집계된 데이터 값을 변경할 수 없게 된다.

[0160] 즉, 본 발명에서는 악의적인 사용자가 개별 스마트 미터(SM) 통신을 관찰하고 일부 오래된 패킷을 다시 보내더라도 이러한 패킷을 식별할 수 있다. 보다 구체적으로, 본 발명에서 스마트 미터(SM)가 제출하는 모든 데이터 패킷에는 t_i 값으로 타임스탬프가 지정되고, 아래 수학식 26 및 수학식 27에서 암호문 c_i 와 전자 서명 σ_{smi} 는 타임스탬프 t_i 를 포함하며, 안개 노드(FN)이 수신한 데이터의 타임스탬프가 더 오래된 기간인 경우 폐기된다.

[0161] [수학식 26]

$$c_i = E(m_i) = g^{rm_i} h^t$$

[0162]

[0163] [수학식 27]

$$\sigma_{smi} = s_k^{sm}(H(c_i \parallel t_i))$$

[0164]

[0165] (5) 또한, 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법에서는, 공격자가 안개 노드(FN)로 가장할 수 없게 된다.

[0166] 보다 구체적으로, 본 발명에서 공격자가 실제 스마트 미터(SM)의 식별 부호(ID)를 숨겨 가짜 데이터 패킷을 보내려고 하면 전자 서명 인증 메커니즘을 통해 식별될 수 있다. 본 발명에서, 모든 스마트 미터(SM) sm_i 는 암호문 c_i 에서 개인 키 s_k^{sm} 를 사용하여 현재 타임스탬프 t_i 를 사용해 전자 서명 σ_{smi} 를 생성하게 되며, 또한 이는 해당 연기 노드(FN)로 제출된다.

[0167] [수학식 28]

$$\sigma_{smi} = s_k^{sm}(H(c_i \parallel t_i))$$

[0168]

[0169] 이때, 연기 노드(FN)는 아래 수학식 29를 사용하여 전자 서명 σ_{fni} 를 생성하게 된다.

[0170] [수학식 29]

$$\sigma_{fni} = p_k^{sm}(H(c_i) \parallel t_i)$$

[0171]

[0172] 이때, σ_{smi} 및 σ_{fni} 의 값이 동일하면 암호문 c_i 가 허용되고 수신된 데이터가 유효한 소스에서 온 것으로 판단될 수 있으며, 그렇지 않으면 어떤 외부의 공격자가 FDI 공격을 통해 전송 중인 데이터를 수정하였다고 판단할 수 있다.

[0173] 도 13은 종래 기술에 따른 방식들과 본 발명에서의 보안 속성을 비교하여 도시하고 있으며, 도 13에서 볼 수 있는 바와 같이 본 발명에서 제안된 방식은 보안 집계 과정에서 담합 공격 저항성(Colluding Resistance)의 추가적인 속성을 가지게 된다.

[0174] 보다 구체적으로, 본 발명에서 개인 정보는 파일리에(Paillier) 동형 암호화를 통해 달성될 수 있으며, 무결성 및 인증은 타원 곡선 기반 디지털 서명(ECDSA)을 통해 수행될 수 있다.

[0175] 본 발명에서는 FDI 공격에 의하여 전송 중 패킷을 수정하면 원본과 대상의 전자 서명을 비교하여 식별 가능하고, 재생 공격에 대해서는 모든 메시지의 타임 스탬프를 통해 식별되어 타임스탬프를 기반으로 오래된 패킷은 거부될 수 있으며, 스마트 미터(SM)에 결함이 있는 경우 집계 프로세스는 이에 의존하지 않고 신속하게 완료될 수 있다.

- [0176] 아래에서는 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법에 대한 성능을 검증하는 실험예를 통하여 본 발명에서의 계산 비용, 통신 비용, 내결함성에 대하여 평가하고 설명한다.
- [0177] (가) 실험 설정
- [0178] 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법의 구현을 위해 PyCharm IDE와 함께 Python 3.8.1 언어를 사용하였으며, 실험 결과는 Intel Core i7-8550U, 1.8GHz CPU, 8GB DDR3 RAM 및 Windows 10 운영체제가 탑재된 시스템을 이용하여 아일랜드(Irish) 스마트 그리드(SG) 데이터 세트를 통해 산출되었다. 길이가 512비트인 두 개의 큰 소수 q_1 및 q_2 는 파일리에(Paillier) 키 생성에 사용되고 ECDSA SHA-256 비트 해시가 서명 생성에 사용되었다. 또한, 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법에서 스마트 그리드 모델에는 각각의 스마트 미터(SM)로부터 소비 데이터를 수신하는 n 개의 안개 노드(FN)가 구비된다.
- [0179] (나) 성능 결과
- [0180] (나-1) 계산 비용
- [0181] 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법에서 계산 비용은 (i) 스마트 미터(SM)에서 암호화에 필요한 시간, (ii) 안개 노드(FN)에서의 데이터 집계, (iii) 클라우드 제어 센터(CCC)에서의 복호화로 나누어 산출될 수 있다. 이때, 결과 계산을 위해 3개의 안개 노드 fn_1 , fn_2 및 fn_3 이 고려되었으며, 각 안개 노드에는 100~1000 개의 스마트 미터가 부착된다. 이때 계산된 비용은 밀리 초(ms) 단위로 산출되었다. 도 14에서는 10개의 스마트 미터(SM) 그룹에 대한 비밀 생성, 배포 및 재구성 비용을 나타내며, 도 15에는 안개 노드(FN) 및 클라우드 제어 센터(CCC) 수준에서의 집계(aggregation) 비용이 도시되어 있다. 또한 도 16에서는 이와 유사하게 스마트 미터(SM), 안개 노드(FN), 클라우드 제어 센터(CCC) 레벨에서의 암호화 운용 비용을 도시하고 있다.
- [0182] 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법은 기존의 최신 안개 노드 기반 스마트 그리드(SG) 방식과 비교될 수 있다. 이때, 도 9의 알고리즘 4를 사용하여 암호화 비용을 계산한 결과는 도 17과 같으며, 도 18에서 볼 수 있는 바와 같이 본 발명에 따른 암호화 비용이 살림 등(Saleem et al.)[7]의 경우보다 적고, 토니알리 등(Tonyali et al.)[8]과 비슷하며, 바오 등(Bao et al.)[5]보다는 큰 것을 알 수 있다.
- [0183] 또한, 도 19에서 볼 수 있는 바와 같이 본 발명에 따른 복호화 비용도 기존의 세 가지 방식 모두보다 적음을 알 수 있다. 이때, 본 발명과 기존의 [7], [8]은 파일리에(Paillier) 암호화 방식을 사용하고 있으나, 살림 등(Saleem et al.)[7]에서는 암호화하는 동안 추가 비밀 키 값을 사용하고 있으며, 바오 등(Bao et al.)[5]에서는 대칭 AES 암호화를 사용하므로 암호화 비용이 적다. 바오 등(Bao et al.)[5] 및 살림 등(Saleem et al.)[7]의 암호 해독 비용의 경우 불량 스마트 미터(SM)가 있는 경우 신뢰 인증부(TA)(140)에 연락하여 실패한 스마트 미터(SM) 상태 및 비밀 재구성을 확인해야 하기 때문에 본 발명보다 비용이 커지게 되며, 암호 해독 활동은 실패한 스마트 미터(SM) 데이터에 따라 달라지게 되나, 본 발명의 경우 살림 등(Saleem et al.)[7]보다 우수한 결과를 나타내는 것을 확인할 수 있다. 이는 본 발명에서 내결함성 집계를 수행하기 위해 모든 스마트 미터(SM) 간에 비밀 매개변수 분포가 필요하지 않기 때문으로, 본 발명에서는 바로 집계 및 암호 해독 작업을 수행하게 되며, 결함이 있는 스마트 미터(SM)가 있는 경우 안개 노드(FN)는 해당 목록을 브로드캐스트(broadcast)하게 된다. 이때, 안개 노드(FN)가 결함이 있는 스마트 미터(SM)로부터 데이터를 수신하면 집계 데이터에 포함되며, 응답하지 않으면 안개 노드(FN)는 작동하는 스마트 미터(SM)의 집계 데이터와 함께 결함이 있는 스마트 미터(SM) 목록을 클라우드 제어 센터(CCC)로 보내게 된다.
- [0184] (나-2) 통신비
- [0185] 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법에서 통신 비용은 비밀 분배 및 재구성(스마트 미터(SM)에서 안개 노드(FN)로, 안개 노드(FN)에서 클라우드 제어 센터(CCC)로)을 위해 하나의 스마트 미터(SM)에서 이웃 스마트 미터(SM)로 전송하는 메시지의 수와 크기를 계산하여 비교할 수 있다. 이때, 본 발명에서 스마트 미터(SM)에서 안개 노드(FN)까지 전송하는 모든 메시지의 크기는 [스마트 미터(SM)의 숫자] x [1024비트 암호화 데이터 + 512비트 서명 + 32비트 타임 스탬프]가 된다. 반면, 살림 등(Saleem et al.)[7]의 메시지 크기는 [스마트 미터(SM)의 숫자] x [1024비트 암호화 데이터 + 512비트 서명 + 32비트 타임 스탬프 + 512 비밀 매개변수 크기]가 되며, 입니다. 토니알리 등(Tonyali et al.)[8]의 메시지 크기는 [스마트 미터(SM)의 숫자] x [32비트 데이터 크기 + 256비트 서명 + 32비트 타임 스탬프]가 된다. 또한, 바오 등(Bao et al.)[5]에서의 스마트 미터(SM)에서 클러스터 헤드로의 통신의 경우 [256비트 암호화 데이터 + 20비트 스마트 미터(SM) 식별 부

호(ID) + 20비트 클러스터 헤드 식별 부호(ID) + 32비트 타임 스탬프 + 512 비밀 매개변수 크기]가 된다. 살렘 등(Saleem et al.)[7]의 경우 모든 스마트 미터(SM)에 대해 비밀 매개변수를 생성해야 하는 요구 사항이 있으며 이것이 없으면 복호화 과정을 완료할 수 없다.

[0186] 반면, 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법에서는 상기와 같은 요구 사항이 없으며, 이와 관련하여 도 20에는 스마트 미터(SM)에서 연기 노드(FN)로의 통신 오버헤드를 비교하여 도시하고 있다. 이때, 기존의 [5], [7], [8] 및 본 발명에 따른 스마트 미터(SM)에서 연기 노드(FN)까지의 메시지 크기는 각각 840, 2080, 320, 1568비트가 된다. 바오 등(Bao et al.)[5]의 경우 통신 오버헤드는 대칭 암호화 방식의 사용으로 인해 더 적으며, 또한 토니알리 등(Tonyali et al.)[8]의 경우에는 사용 데이터에만 32비트를 사용하게 된다.

[0187] (나-3) 결함 허용

[0188] 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법에서는 일부 스마트 미터(SM)가 어떤 이유로든 데이터를 제출하지 않은 경우 연기 노드(FN)는 실패한 스마트 미터(SM) 목록을 브로드캐스트(broadcast)하고 데이터 제출을 요청하게 된다. 이 목록을 기반으로 활성 스마트 미터(SM)는 이전에 데이터 제출을 위해 지명된 파트너에게 연락하여 현재 기간에 대한 데이터를 제공하도록 요청한다. 이때 파트너가 응답하지 않으면 스마트 미터(SM)는 다음 데이터 제출 라운드를 위해 파트너를 조정하게 된다. 이어서, 다음 라운드에서는 이전 라운드와 현재 라운드에 대한 사용 데이터를 함께 제출한다. 연기 노드(FN)는 집계된 데이터와 실패한 스마트 미터(SM) 목록을 클라우드 제어 센터(CCC)로 제출하게 된다. 이에 따라, 클라우드 제어 센터(CCC)는 집계된 데이터를 해독하고 사용 정보를 계산하게 된다. 이때, 기존의 [5] 및 [7]에서 모든 스마트 미터(SM)의 데이터가 수신되고 결함이 있는 스마트 미터(SM)의 경우 더미 값이 조정될 때까지 암호 해독 활동이 완료될 수 없게 된다. 반면, 본 발명의 일 실시예에 따른 스마트 그리드에서의 데이터 집계 방법에서는 그러한 요구 사항이 없으며 사용 가능한 스마트 미터(SM)만으로 복호화 과정을 처리할 수 있게 된다.

[0189] 이에 따라, 본 발명의 일 실시예에 따른 안개 노드가 구비되는 스마트 그리드에서의 보안 다자간 계산 기반 데이터 집계 방법, 장치 및 시스템에서는, 스마트 그리드에서 다량의 데이터를 효율적으로 처리할 수 있으며, 나아가 고객 관련 정보에 대한 보안을 강화할 수 있게 된다.

[0190] 나아가, 본 발명의 일 실시예에 따른 안개 노드가 구비되는 스마트 그리드에서의 보안 다자간 계산 기반 데이터 집계 방법, 장치 및 시스템에서는 담합 공격(colluded attack)을 방지할 수 있을 뿐만 아니라, 내결함성(fault-tolerant)을 가지므로 일부 스마트 계량기(SM)에서 오류가 발생하더라도 데이터의 집계가 가능하며, 나아가 FDI(False Data Injection) 및 재생 공격(replay attack)에 대해서도 효과적인 대응이 가능하게 된다.

[0191] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서 본 발명에 기재된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의해서 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

[0192] 100 : 스마트 그리드

110 : 제어부

120 : 안개 노드

130 : 계측 장치

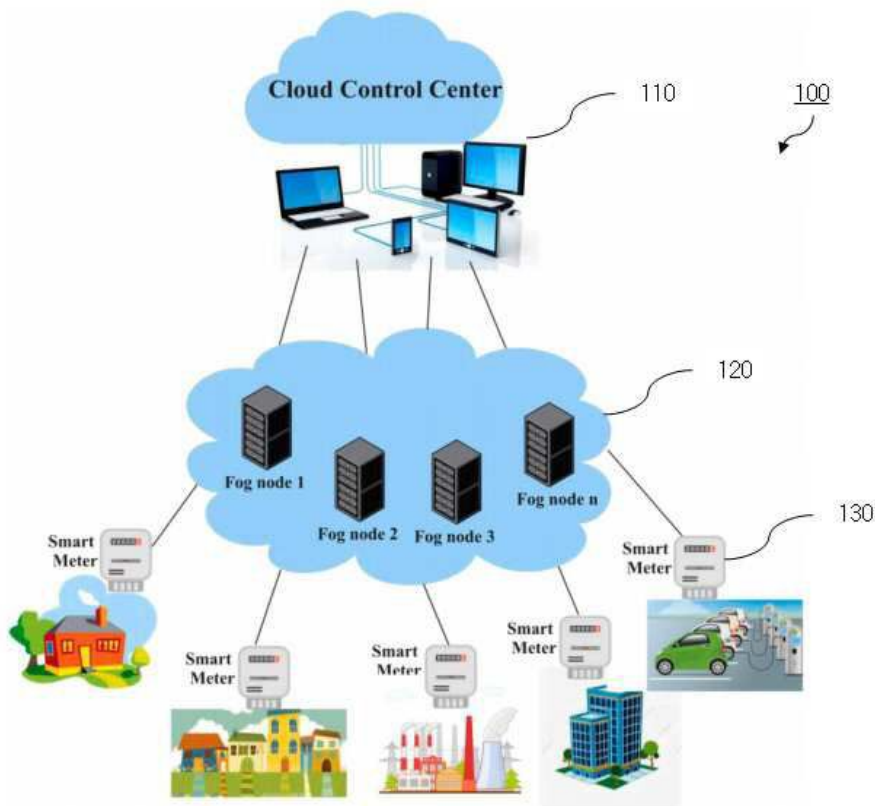
130a : 제1 계측 장치

130n : 제1 대표 계측 장치

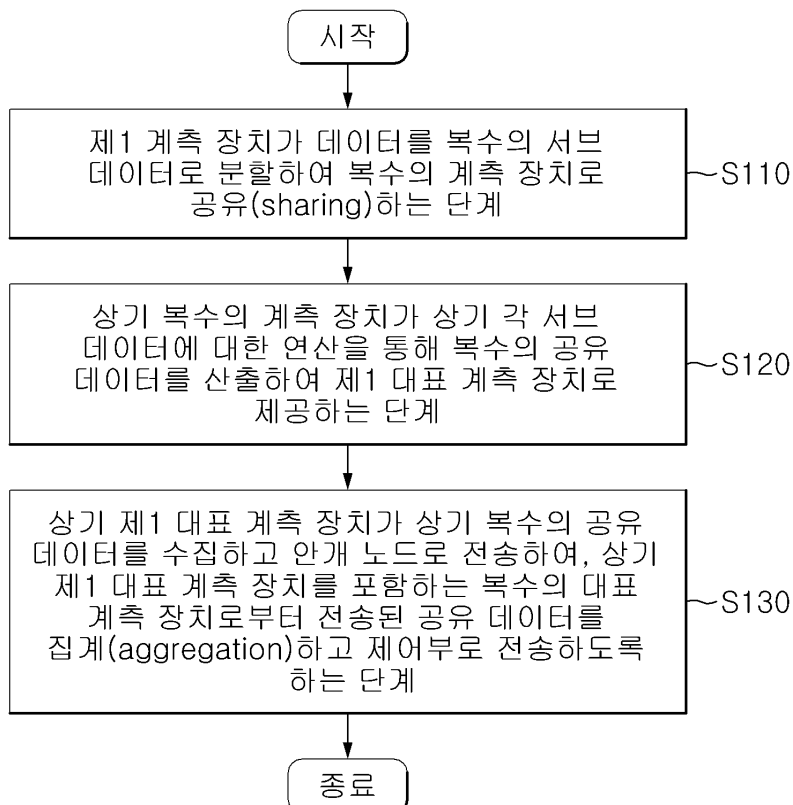
140 : 신뢰 인증부

도면

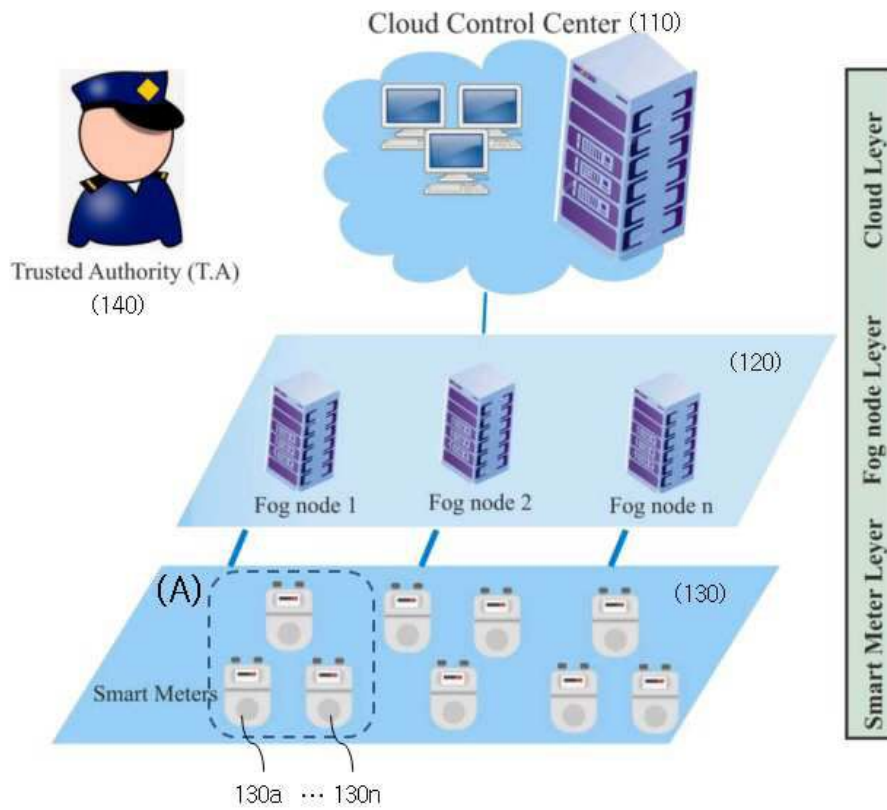
도면1



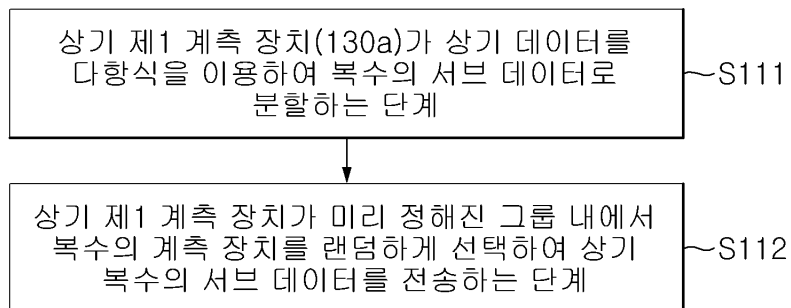
도면2



도면3



도면4



Symbol	Description
SM	Smart Meter
FN	Fog Node
CCC	Cloud Control Center
(λ, μ)	Private Key for Pailier
(N, g)	Public parameters of Pailier
m_i	Message text
R	Status bit (0 or 1)
$c(x, y)$	SM Responsible for final value calculation on behalf of SM _i
t_i	Timestamp
σ_i	Signature of Meter m_i
σ_{fn}	Fog Node Signature
C_{fn}	All SMs aggregated ciphertext
Agg_{val}	Aggregated value at CCC
$H(c_i)$	SHA-256 based hash function
M	Usage data after decryption at CCC
s_k^{fn}	The Private key used by FN for Signature generation
p_k^{fn}	The Public key used by FN for Signature verification
s_k^{sm}	The Private key used by SM for Signature generation
p_k^{sm}	The Public key used by SM for Signature verification
S	Every SM secret value

도면5

도면6

```

1: Procedure Key Generation
2: Input: Large Prime numbers  $p, q$ ,  $N = p \cdot q$ , Function  $L(x) = \frac{x-1}{N}$ 
3: Output: Public Key is  $pk=(N, g)$  and private key is  $sk=(\lambda, \mu)$ 
4: TA computes  $N = p \cdot q$  by choosing two large prime numbers  $p, q$ 
5: Compute  $\lambda = \text{ lcm}(p-1, q-1)$ .
6: Define a function  $L(x) = \frac{x-1}{N}$ 
7: Select a generator  $g \in \mathbb{Z}_{N^2}^*$ 
8: Compute  $\mu = (L(g^\lambda \bmod N^2))^{-1} \bmod N$ 
9: Generate  $s_k^{sm}, p_k^{sm}, s_k^{fn}, p_k^{fn}$  for signature generation and verification
10: Return  $pk=(N, g)$ ,  $sk=(\lambda, \mu)$ ,  $s_k^{sm}, p_k^{sm}, s_k^{fn}$ , and  $p_k^{fn}$ 
11: end procedure

```

도면7

```

1: Procedure Secret Shares Creation and Sharing
2: Input: Message  $m_i$ , time  $t_i$ ,  $S M_i$ 
3: Output: Cipher  $c_i$ , Signature  $\sigma_{sm_i}$ ,  $S M_i$ 
4:  $f(x) = \text{polynomial}(d)$ 
5:  $S M_{Lagg} = \text{RandomSMsel}(S M_i)$ 
6:  $S M_{jList} = \text{RandomListGen}(S M_i)$ 
7: for  $i=0; i < S M_i; i++$  do
8:   if  $S M_i$  in  $S M_{jList}$  then
9:      $r=1$ 
10:  else
11:     $r=0$ 
12:     $c_i = \text{Enc}((x_i, y_i), S M_{Lagg}, t_i, r)$ 
13:     $\sigma_{sm_i} = s_k^{sm_i} (H(c_i) || t_i)$ 
14:  Return  $(\sigma_{sm_i}, c_i, S M_i)$ 
15: end procedure

```

도면8

```

1: Procedure Share calculation by Neighbors SMs
2: Input:  $S M_{Lagg}$ ,  $c_i$ ,  $\sigma_{sm_i}$ ,  $S M_i$ 
3: Output:  $c_j$ ,  $\sigma_{sm_j}$ ,  $S M_j$ ,  $S M_i$ 
4:  $\sigma_{S M_j} = p_k^{sm_i} (H(c_i) || t_i)$ 
5: if  $\sigma_{S M_j} = \sigma_{sm_i}$  then
6:   Signature is verified and  $c_i$  is accepted
7:    $Value_j = f(x_j) * I(x_j)$ 
8:    $c_j = Enc(Value_j, t_i)$ 
9:    $\sigma_{sm_i} = s_k^{sm_j} (H(c_j) || t_i)$ 
10: else
11:   Signature is non-verified and  $c_i$  is discarded
12: Return ( $c_j$ ,  $\sigma_{sm_j}$ ,  $S M_j$ ,  $S M_i$ )
13: end procedure

```

도면9

```

1: Procedure Share Aggregation at Aggregator SM
2: Input:  $c_j$ ,  $\sigma_{sm_j}$ ,  $S M_j$ ,  $S M_i$ 
3: Output:  $c_{sm_{val}}$ ,  $\sigma_{S M_{Lagg}}$ ,  $S M_{Lagg}$ 
4:  $\sigma_{S M_{Lagg}} = p_k^{sm_j} (H(c_j) || t_i)$ 
5: if  $\sigma_{S M_{Lagg}} = \sigma_{sm_j}$  then
6:   Signature is verified and  $c_j$  is accepted
7:    $S M_{val} = \sum_{k=1}^d c_k$ 
8: else
9:   Signature is rejected and  $c_i$  is discarded
10:  $c_{sm_{val}} = Enc(S M_{val}, t_i)$ 
11:  $\sigma_{S M_{Lagg}} = p_k^{S M_{Lagg}} (H(*c_{sm_{val}}) || t_i)$ 
12: Return ( $c_{sm_{val}}$ ,  $\sigma_{S M_{Lagg}}$ ,  $S M_{Lagg}$ )
13: end procedure

```

도면10

```

1: Procedure Aggregation at FN
2: Input:  $c_{sm\_val}$ ,  $\sigma_{SM\_Lagg}$ ,  $SM\_Lagg$ 
3: Output:  $C^{fn\_agg}$ ,  $\sigma_{fn\_i}$ 
4:  $\sigma_{fn\_i} = p_k^{SM\_Lagg} (H(c_i) || t_i)$ 
5: if  $\sigma_{fn\_i} = \sigma_{SM\_Lagg}$  then
6:   Signature is verified and  $c_{sm\_val}$  is accepted
7:    $fn\_agg = \prod_{i=1}^W c_{sm\_val}$ 
8: else
9:   Signature is rejected and  $c_{sm\_val}$  is discarded
10:  $C^{fn\_agg} = Enc(fn\_agg, t_i)$ 
11: Return ( $C^{fn\_agg}, \sigma_{fn\_i}$ )
12: end procedure

```

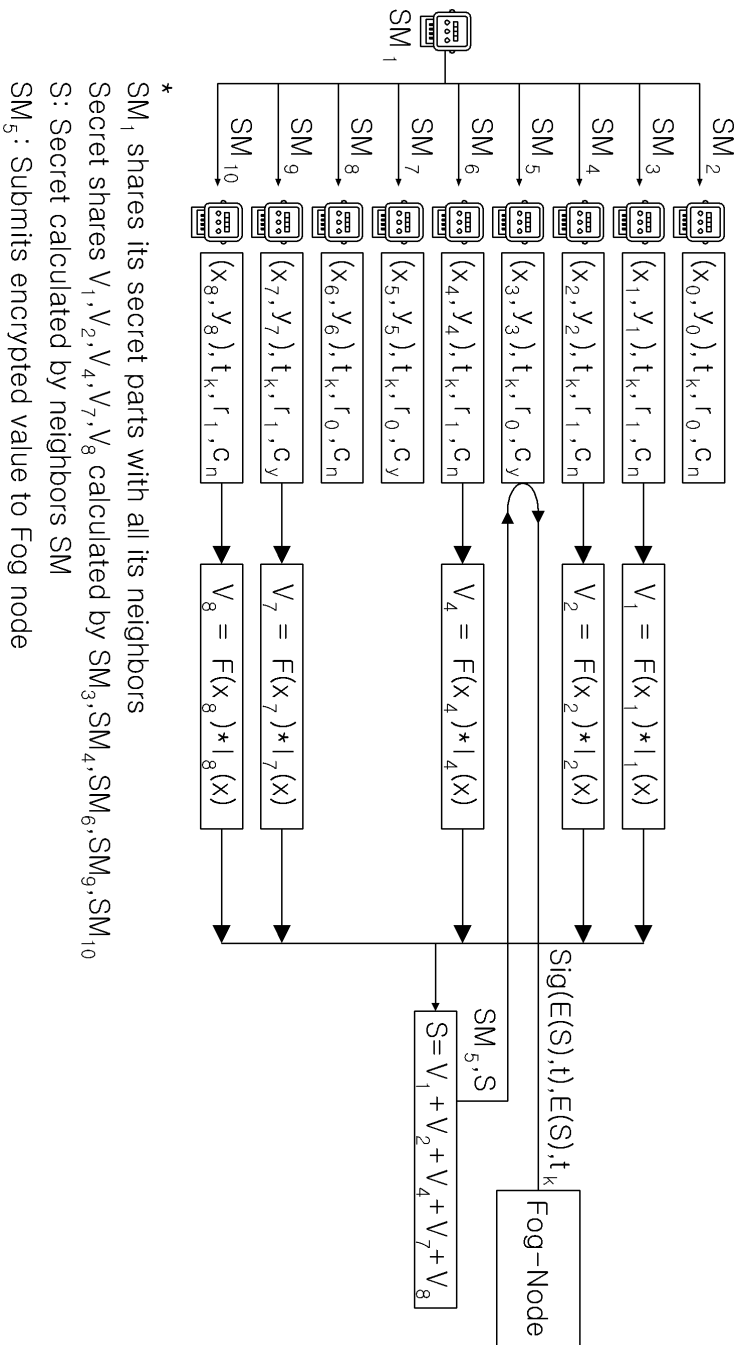
도면11

```

1: Procedure Decryption at CCC
2: Input:  $C^{fn\_agg}$ ,  $\sigma_{fn\_i}$ 
3: Output: M
4:  $\sigma_{cc} = p_k^{fn} (H(C^{fn\_agg}) || t_i)$ 
5: if  $\sigma_{cc} = \sigma_{fn\_i}$  then
6:   Signature is verified and  $C^{sm\_val}$  is accepted
7: else
8:   Signature is rejected and  $C^{sm\_val}$  is discarded
9:  $C^{fn\_all} = \sum_{fog=1}^n C^{fn\_agg}$ 
10:  $C_d = C^{fn\_all}$ 
11:  $C_d = g^{r \sum_{i=1}^n m_i} h^r$ 
12:  $C_d = \frac{g^{r \sum_{i=1}^n m_i}}{h^{-r}}$ 
13:  $C_d h^{-r} = g^{r \sum_{i=1}^n m_i}$ 
14: CCC through discrete log get  $M = g^{r \sum_{i=1}^n m_i}$ 
15: Return (M)
16:
17: end procedure

```

도면12



도면13

Comparison of Security Properties.				
Properties	[5]	[7]	[8]	Proposed Scheme
Privacy	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes
FDI	Yes	Yes	Yes	Yes
Colluding Resistance	No	No	No	Yes
Fault Tolerance	Yes	Yes	Yes	Yes

도면14

Group-wise Secret Distribution and Reconstruction Time.

Group	Time Taken (ms)
Group#1	2.96
Group#2	5.004
Group#3	5.94
Group#4	3.9899
Group#5	3.989
Group#6	3.99

Aggregation Cost at Fog Nodes.

SMPC based Aggregation Cost					
Fn ₁ Level		Fn ₂ Level		Fn ₃ Level	
				CCC Level	
#of SMS	Time(ms)	#of SMS	Time(ms)	#of SMS	Time(ms)
100	16.95	100	16.25	100	17.15
200	22.96	200	23.00	200	23.05
400	66.60	300	56.52	300	56.52
600	101.94	400	66.60	400	66.45
800	114.75	500	77.84	500	77.25
1000	181.55	600	101.43	800	114.93
					2400
					50.35
					69.01
					179.64
					234.99
					269.84
					397.91

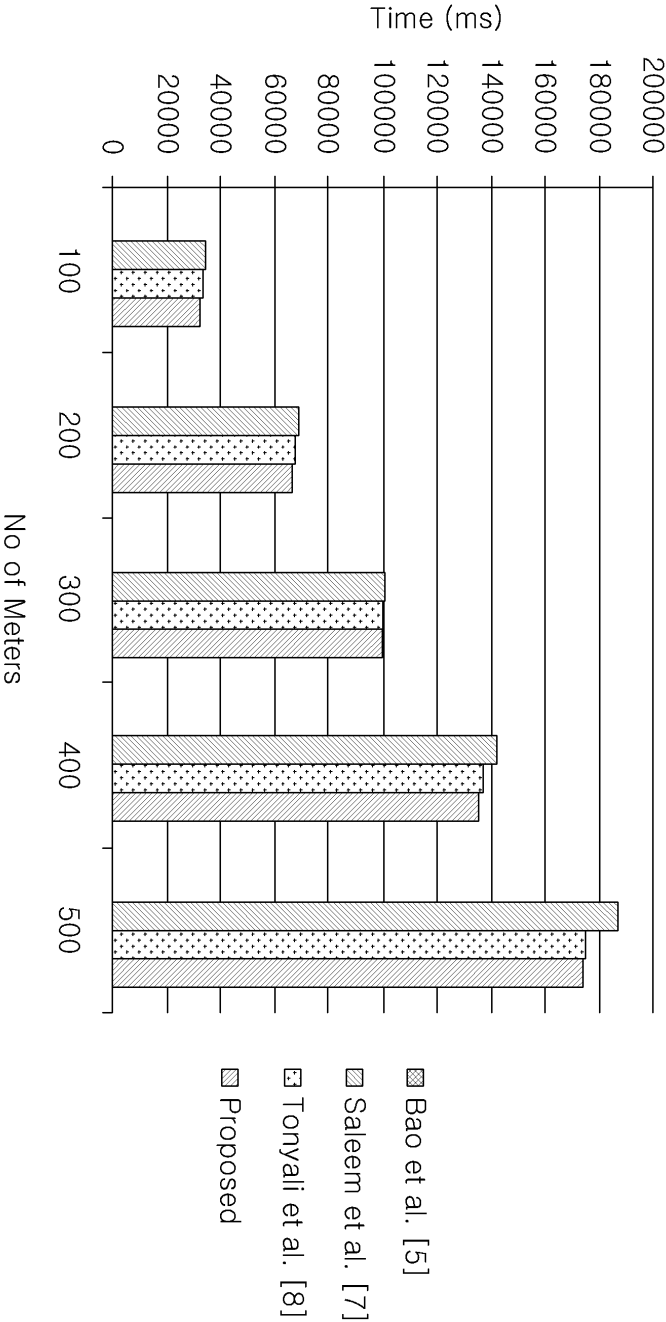
도면16

Cryptographic Operation Computation Cost.				
Level	Encryption	Signature-Generation	Signature-Verification	Decryption
SM ₁	329 per SM	4 per SM	-	-
FN ₁	-	4 per FN	10 per FN	-
CCC	-	-	11 per FN	91.75 per 100 SM

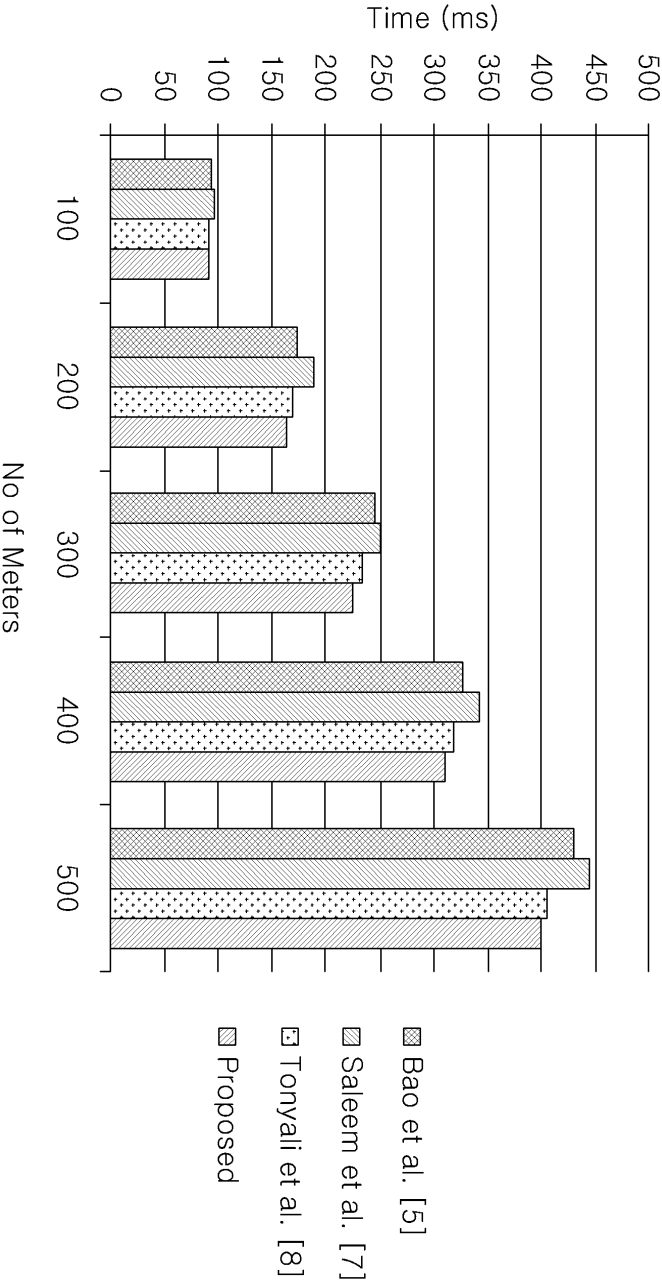
도면17

Encryption Cost at the SM Level.				
No. of SM	Bao et al.[5]	Saleem et al.[7]	Tonayli et al.[8]	Proposed Scheme
100	599	34163.76	33987.22	33022.68
200	614	69156.90	67256.45	66491.57
300	625	10122.78	100348.23	99673.23
400	640	141900.11	336963.76	135889.75
500	661	18723.45	175127.96	174653.61

도면18



도면19



도면20

