(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년12월07일
(11) 등록번호 10-1683051
(24) 등록일자 2016년11월30일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) *H04L 12/28* (2006.01)
(52) CPC특허분류
H04L 9/0625 (2013.01)
H04L 12/28 (2013.01)
(21) 출원번호 10-2015-0100899
(22) 출원일자 2015년07월16일
심사청구일자 2015년07월16일
(56) 선행기술조사문헌
KR1020080018768 A
KR1020080075751 A
JP2013015643 A

(73) 특허권자
(주)엔텔스
서울특별시 강남구 학동로 401, 15층 (청담동, 금하빌딩)
(72) 발명자
심재희
서울특별시 광진구 아차산로70길 62, 310동 406호 (광장동, 광장현대3단지아파트)
이훈정
경기도 안산시 상록구 감골2로 12, 405동 204호 (사동, 상록수현대2차아파트)
이상훈
경기도 남양주시 호평로 94, 2014동 1204호 (호평동, 금강아파트)
(74) 대리인
남정길

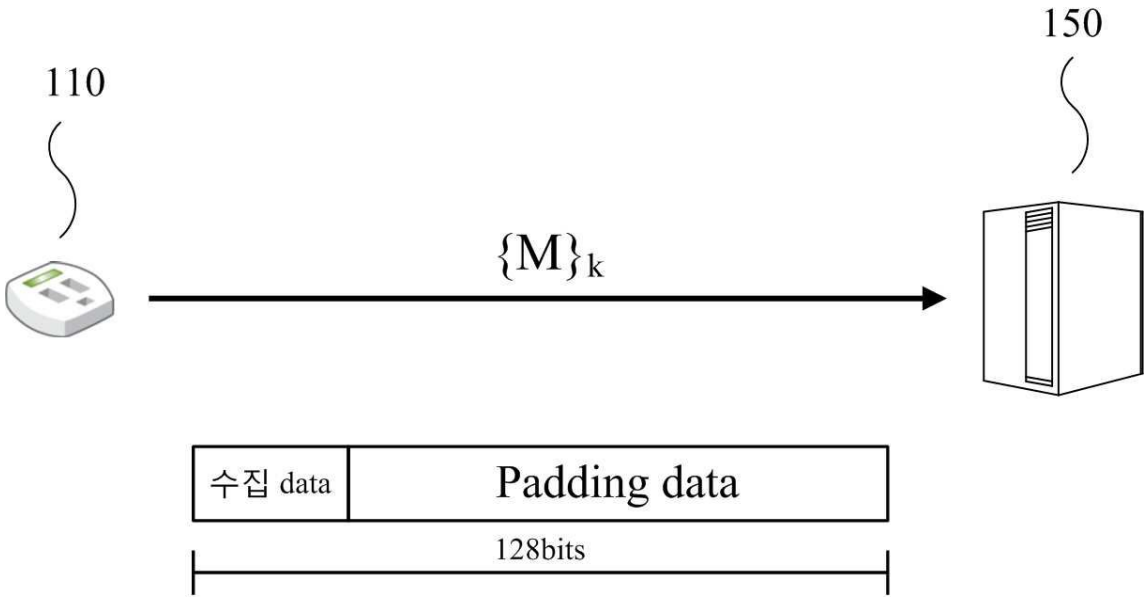
전체 청구항 수 : 총 11 항 심사관 : 문형섭

(54) 발명의 명칭 **IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법 및 IoT 네트워크에서 클라이언트 장치가 서버에 데이터를 전달하는 방법**

(57) 요 약

IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법은 IoT 디바이스가 기준 크기를 갖는 적어도 하나의 데이터를 획득하는 단계, 상기 IoT 디바이스가 상기 적어도 하나의 데이터를 블록 단위로 구분하는 단계, 상기 적어도 하나의 데이터를 구분하는 마지막 블록에서 데이터가 할당되지 않은 영역인 여유 영역의 크기가 상기 기준 크기보다 큰 경우 상기 IoT 디바이스가 기준 시간을 대기하는 단계 및 상기 IoT 디바이스가 상기 대기하는 동안 상기 기준 크기를 갖는 적어도 하나의 추가 데이터를 획득하는 경우 상기 마지막 블록에 상기 추가 데이터를 할당하고, 상기 마지막 블록을 대칭키를 이용하여 암호화하는 단계를 포함한다.

대 표 도 - 도2



(52) CPC특허분류
H04L 9/0618 (2013.01)

명 세 서

청구범위

청구항 1

IoT 디바이스가 기준 크기를 갖는 적어도 하나의 데이터를 획득하는 단계;

상기 IoT 디바이스가 상기 적어도 하나의 데이터를 일정한 크기를 갖는 블록 단위로 분할하여 할당하는 단계;

상기 적어도 하나의 데이터를 할당한 마지막 블록에서 데이터가 할당되지 않은 영역인 여유 영역의 크기가 상기 기준 크기보다 큰 경우 상기 IoT 디바이스가 기준 시간을 대기하는 단계;

상기 IoT 디바이스가 상기 대기하는 동안 상기 기준 크기를 갖는 적어도 하나의 추가 데이터를 획득하는 단계; 및

상기 IoT 디바이스가 상기 적어도 하나의 추가 데이터 중 상기 기준 크기 단위로 상기 여유 영역에 할당될 수 있는 추가 데이터만을 상기 마지막 블록에 추가로 할당하고, 상기 마지막 블록을 대칭키를 이용하여 암호화하는 단계를 포함하는 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법.

청구항 2

제1항에 있어서,

상기 IoT 디바이스는 데이터를 수집하는 센서 장치인 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법.

청구항 3

제1항에 있어서,

상기 IoT 디바이스가 상기 대기하는 동안 상기 추가 데이터를 획득하지 못하는 경우 상기 여유 영역을 패딩하고, 상기 마지막 블록을 상기 대칭키를 이용하여 암호화하는 단계를 더 포함하는 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법.

청구항 4

제1항에 있어서,

상기 적어도 하나의 데이터가 복수의 블록에 할당되는 경우, 상기 IoT 디바이스는 상기 마지막 블록의 제외한 나머지 블록에 할당되는 데이터를 상기 대칭키를 이용하여 암호화하는 단계를 더 포함하는 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법.

청구항 5

제1항에 있어서,

상기 암호화하는 단계는

상기 추가 데이터가 상기 마지막 블록에 할당되고, 이후 상기 마지막 블록에서 데이터가 할당되지 않은 영역이 상기 기준 크기 보다 큰 경우 상기 IoT 디바이스가 기준 시간을 2차 대기하는 단계; 및

상기 IoT 디바이스가 상기 2차 대기하는 동안 상기 기준 크기를 갖는 적어도 하나의 제2 추가 데이터를 획득하는 경우 상기 마지막 블록에 상기 제2 추가 데이터를 할당하고, 상기 마지막 블록을 상기 대칭키를 이용하여 암호화하는 단계를 포함하는 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법.

청구항 6

제1항에 있어서,

상기 암호화하는 단계는

상기 추가 데이터가 상기 마지막 블록에 할당되고, 이후 상기 마지막 블록에서 데이터가 할당되지 않은 영역이 상기 기준 크기 보다 큰 경우 상기 IoT 디바이스가 상기 마지막 블록에서 아직 데이터가 할당되지 않은 영역을 패딩하고, 상기 마지막 블록을 상기 대칭키를 이용하여 암호화하는 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법.

청구항 7

제1항에 있어서,

상기 기준 시간은 상기 IoT 디바이스가 상기 여유 영역을 모두 채울수 있는 추가 데이터를 획득할 때인 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법.

청구항 8

클라이언트 장치가 기준 크기 단위의 데이터를 생성하거나 수집하는 단계;

클라이언트 장치가 일정한 크기의 블록 단위로 상기 데이터를 할당하는 단계;

상기 데이터를 할당한 마지막 블록에서 데이터가 할당되지 않은 영역인 여유 영역의 크기가 기준 크기보다 큰 경우 상기 클라이언트 장치가 다음에 생성되거나 수집되는 추가 데이터를 대기하는 단계;

상기 클라이언트 장치가 상기 추가 데이터를 생성하거나 수집한 경우 상기 추가 데이터 중 상기 기준 크기 단위로 상기 여유 영역에 할당될 수 있는 추가 데이터만을 상기 여유 영역에 추가로 할당하고, 상기 마지막 블록을 대칭키를 이용하여 암호화하는 단계; 및

상기 클라이언트 장치가 암호화한 상기 블록을 서버에 전송하는 단계를 포함하는 IoT 네트워크에서 클라이언트 장치가 서버에 데이터를 전달하는 방법.

청구항 9

제8항에 있어서,

상기 클라이언트 장치가 기준 시간 동안 상기 추가 데이터를 생성하거나 수집하지 못하는 경우 상기 여유 영역을 패딩하고, 상기 마지막 블록을 상기 대칭키를 이용하여 암호화하는 단계를 더 포함하는 IoT 네트워크에서 클라이언트 장치가 서버에 데이터를 전달하는 방법.

청구항 10

제8항에 있어서,

상기 데이터가 복수의 블록에 할당되는 경우, 상기 클라이언트 장치가 상기 마지막 블록의 제외한 나머지 블록에 할당되는 데이터를 상기 대칭키를 이용하여 암호화하고, 상기 나머지 블록에 해당하는 데이터를 상기 서버에 전송하는 단계를 더 포함하는 IoT 네트워크에서 클라이언트 장치가 서버에 데이터를 전달하는 방법.

청구항 11

제8항에 있어서,

상기 암호화하는 단계에서 상기 추가 데이터가 상기 마지막 블록에 할당되고, 이후 상기 마지막 블록에서 데이터가 할당되지 않은 영역인 제2 여유 영역이 존재하는 경우 상기 클라이언트 상기 제2 여유 영역을 패딩하고, 상기 마지막 블록을 암호화하는 IoT 네트워크에서 클라이언트 장치가 서버에 데이터를 전달하는 방법.

발명의 설명

기 술 분 야

[0001] 이하 설명하는 기술은 대칭키를 이용한 블록 암호화 기법에 관한 것이다.

배 경 기 술

[0002] 최근 사물 인터넷(IoT) 관련한 관심이 많아지면서, IoT 디바이스를 이용한 상용 서비스들이 등장하기 시작하고

있다. IoT 네트워크도 통신망을 통산 데이터를 전송하므로, IoT 디바이스가 생성하거나 획득한 데이터를 일정하게 암호화하여 전달해야 한다.

선행기술문헌

특허문헌

[0003] (특허문헌 0001) 한국공개특허 제10-2015-0035971호

발명의 내용

해결하려는 과제

[0004] 종래 대칭키를 이용한 암호화 기법은 마지막 블록에 데이터가 모두 차지 않아도, 데이터가 없는 영역을 의미없는 데이터로 패딩(padding)하고 데이터를 암호화하였다.

[0005] 이하 설명하는 기술은 대칭키를 이용한 블록 암호화 기법에서 마지막 블록에 데이터가 차지 않은 경우라도 추가적인 데이터를 기다렸다가 마지막 블록에 데이터를 추가하고 데이터를 암호화하는 기법을 제공하고자 한다.

과제의 해결 수단

[0006] IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법은 IoT 디바이스가 기준 크기를 갖는 적어도 하나의 데이터를 획득하는 단계, 상기 IoT 디바이스가 블록 단위로 상기 적어도 하나의 데이터를 할당하는 단계, 상기 적어도 하나의 데이터를 할당한 마지막 블록에서 데이터가 할당되지 않은 영역인 여유 영역의 크기가 상기 기준 크기보다 큰 경우 상기 IoT 디바이스가 기준 시간을 대기하는 단계 및 상기 IoT 디바이스가 상기 대기하는 동안 상기 기준 크기를 갖는 적어도 하나의 추가 데이터를 획득하는 경우 상기 마지막 블록에 상기 추가 데이터를 할당하고, 상기 마지막 블록을 대칭키를 이용하여 암호화하는 단계를 포함한다.

[0007] IoT 네트워크에서 클라이언트 장치가 서버에 데이터를 전달하는 방법은 클라이언트 장치가 데이터를 생성하거나 수집하는 단계, 클라이언트 장치가 블록 단위로 상기 데이터를 할당하는 단계, 상기 데이터를 할당한 마지막 블록에서 데이터가 할당되지 않은 영역인 여유 영역의 크기가 기준 크기보다 큰 경우 상기 클라이언트 장치가 다음에 생성되거나 수집되는 추가 데이터를 대기하는 단계, 상기 클라이언트 장치가 상기 추가 데이터를 생성하거나 수집한 경우 상기 여유 영역에 상기 추가 데이터를 할당하고, 상기 마지막 블록을 대칭키를 이용하여 암호화하는 단계 및

[0008] 상기 클라이언트 장치가 암호화한 상기 블록을 서버에 전송하는 단계를 포함한다.

발명의 효과

[0009] 이하 설명하는 기술은 특히 IoT 디바이스와 같이 아주 작은 데이터를 수집하는 장치에서 데이터를 효율적으로 전송할 수 있는 암호화 기법이다. 이하 설명하는 기술은 한번에 최대한 많은 데이터를 전송하여 통신 채널의 혼잡도를 떨어뜨리고, 동시에 IoT 디바이스의 에너지도 절약할 수 있다.

도면의 간단한 설명

[0010] 도 1은 IoT 네트워크 시스템에 대한 구성을 도시한 예이다.

도 2는 종래 대칭키 기반의 블록 암호화 기법에 대한 예이다.

도 3은 대칭키 기반의 블록 암호화 기법에 대한 다른 예이다.

도 4는 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법에 대한 순서도의 예이다.

도 5는 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법에서 마지막 블록 구성을 도시한 예이다.

도 6은 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법에 대한 순서도의 다른 예이다.

도 7는 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법에서 마지막 블록 구성을 도시한 다른 예이다.

발명을 실시하기 위한 구체적인 내용

[0011] 이하 설명하는 기술은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 이하 설명하는 기술을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 이하 설명하는 기술의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0012] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 해당 구성요소들은 상기 용어들에 의해 한정되지는 않으며, 단지 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 이하 설명하는 기술의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0013] 본 명세서에서 사용되는 용어에서 단수의 표현은 문맥상 명백하게 다르게 해석되지 않는 한 복수의 표현을 포함하는 것으로 이해되어야 하고, "포함한다" 등의 용어는 설시된 특징, 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 의미하는 것이지, 하나 또는 그 이상의 다른 특징들이나 개수, 단계 동작 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 배제하지 않는 것으로 이해되어야 한다.

[0014] 도면에 대한 상세한 설명을 하기에 앞서, 본 명세서에서의 구성부들에 대한 구분은 각 구성부가 담당하는 주기능 별로 구분한 것에 불과함을 명확히 하고자 한다. 즉, 이하에서 설명할 2개 이상의 구성부가 하나의 구성부로 합쳐지거나 또는 하나의 구성부가 보다 세분화된 기능별로 2개 이상으로 분화되어 구비될 수도 있다. 그리고 이하에서 설명할 구성부 각각은 자신이 담당하는 주기능 이외에도 다른 구성부가 담당하는 기능 중 일부 또는 전부의 기능을 추가적으로 수행할 수도 있으며, 구성부 각각이 담당하는 주기능 중 일부 기능이 다른 구성부에 의해 전담되어 수행될 수도 있음은 물론이다.

[0015] 또, 방법 또는 동작 방법을 수행함에 있어서, 상기 방법을 이루는 각 과정들은 문맥상 명백하게 특정 순서를 기재하지 않은 이상 명기된 순서와 다르게 일어날 수 있다. 즉, 각 과정들은 명기된 순서와 동일하게 일어날 수도 있고 실질적으로 동시에 수행될 수도 있으며 반대의 순서대로 수행될 수도 있다.

[0016] IoT 네트워크에서 IoT 디바이스는 일반적으로 특정 데이터를 생성하거나 수집하는 장치이다. IoT 디바이스가 생성하거나 수집한 데이터를 네트워크를 통해 해당 데이터를 저장하거나 관리하는 객체에 전달된다. IoT 디바이스가 생성하거나 수집한 데이터는 별도의 데이터베이스에 저장될 수도 있다. IoT 디바이스가 생성하거나 수집한 데이터를 이용하여 특정한 서비스를 제공하는 서버는 해당 데이터를 이용하여 서비스를 제공한다. IoT 네트워크에서도 클라이언트 장치에 해당하는 IoT 다비아스와 서버 사이에 단대단(end-to-end) 암호화 기법을 사용한다. 일반적으로 이때 사용되는 암호화 기법은 단말과 서비스 서버가 동일한 비밀키를 사용하여 데이터를 암호화하고 복호화하는 대칭키 암호화 기법이다. 대칭키 암호화 기법은 일반적으로 데이터를 일정한 크기를 갖는 블록 단위로 구분하여, 블록 단위로 암호화를 수행한다. 대표적인 대칭키 암호화 기법은 64비트 길이의 블록을 사용하는 DES(Data Encryption Standard)와 128비트 길이의 블록을 사용하는 AES(Advanced Encryption Standard)가 있다. DES는 56 비트의 길이를 갖는 대칭키를 사용하고, AES는 128, 192 또는 256비트의 길이를 갖는 대칭키를 사용한다. 대칭키 암호화 기법에 대해 널리 알려진 부분에 대해서는 상세한 설명을 생략한다.

[0017] 도 1은 IoT 네트워크 시스템(100)에 대한 구성을 도시한 예이다. 도 1에서 좌측에 IoT 디바이스(110)를 몇 가지 도시하였다. 도 1에 도시한 IoT 디바이스는 센서 장치(110A), 조명기구(110B) 및 자동차의 위치 추적 장치(110C)를 예로 도시하였다. 센서 장치(110A)는 온도, 압력, 습도, 조도 등과 같은 환경 정보를 측정하는 장치에 해당한다. 조명기구(110B)는 건물이나 가정에서 사용되는 것으로 조명기구(110B)는 조명기구의 동작 상태(on 또는 off)를 전달하거나, 현재 가동중인 시간 정보 등을 전달할 수 있다. 위치 추적 장치(110C)는 자동차의 현재 위치 정보를 전달한다. 위치 추적 장치(110C)는 GPS 장치 등과 같은 좌표 측정 장치에서 획득한 정보를 전송한다. 이와 같이 IoT 디바이스는 기본적으로 용량이 작은 정보를 전송한다. 온도, 습도, 동작 상태, 시간, 위치 정보와 같은 데이터는 비교적 작은 비트 단위로 전달이 가능하다. 예를 들어 IoT 디바이스는 8비트 단위의 데이터를 수집할 수 있다. 위치 정보 경우 정교한 위치 정보라면 보다 많은 비트가 필요할 수도 있겠다. IoT 디바이스가 수집하는 데이터의 종류에 따라 다르겠지만, IoT 디바이스가 수집하는 데이터는 몇 비트에서 몇십 비트일 것이다.

[0018] IoT 디바이스(110)가 수집한 데이터는 네트워크(130)를 통해 데이터를 이용하여 서비스를 제공하는 서버(150)에 전달된다. 네트워크(130)는 애드혹 네트워크(Ad-Hoc network), 이동통신 네트워크, 근거리 네트워크(Zigbee

등), 인터넷 등 다양한 네트워크가 사용될 수 있다.

[0019] 사용자는 스마트폰 또는 PC와 같은 사용자 단말(50)을 통해 서비스 서버(150)로부터 IoT 디바이스(110)가 수집한 데이터를 확인할 수 있다. 또는 사용자는 서비스 서버(150)가 가공한 데이터로 제공하는 서비스를 받을 수도 있다.

[0020] IoT 네트워크 시스템(100)에서 IoT 디바이스(110)과 서버(150)는 대칭키 암호화/복호화를 사용하여 데이터를 전달한다. IoT 디바이스(110)는 수집한 데이터를 암호화하여 전달하고, 서버(150)는 수신한 데이터를 복호한다. 경우에 따라서는 서버(150)가 일정한 제어 명령을 암호화하여 IoT 디바이스(110)에 전달할 수도 있다.

[0021] 도 2는 종래 대칭키 기반의 블록 암호화 기법에 대한 예이다. 도 2는 IoT 디바이스(110)가 서버(150)에 데이터를 전달하는 과정을 예로 도시하였다. 종래 대칭키를 이용한 블록 암호화 기법은 데이터를 블록 단위로 구분하여 암호화를 수행한다. M은 암호화하고자 하는 블록 단위 메시지를 의미하고, k는 대칭키를 의미한다. 도 2는 128 비트 길이의 블록을 갖는 AES와 같은 암호화 기법을 예로 도시하였다.

[0022] 데이터의 크기에 따라 블록을 모두 채우지 못하는 경우가 발생할 수 있다. 이 경우 암호화 장치는 도 2의 하단과 같이 블록에서 데이터를 할당하지 못한 영역은 패딩(padding)한다. 이하 블록에서 의미 있는 데이터가 채워지지 못한 빈 영역을 여유 영역이라고 명명한다. 패딩은 규약에 따라 의미 없는 일정한 데이터를 채워넣는 과정을 의미한다. 암호화 장치는 블록을 패딩으로 모두 채우고, 블록을 암호화한다. 복호 장치는 데이터를 복호하면서 패딩 데이터를 구별할 수 있다. 따라서 패딩에 사용하는 데이터는 암호화 기법에서 사전에 정의된 데이터 형태를 가져야 한다.

[0023] 도 3은 대칭키 기반의 블록 암호화 기법에 대한 다른 예이다. 도 3은 제안하는 암호화 기법에 대한 하나의 예에 해당한다. 한편 IoT 디바이스(110)는 일정한 기준 크기를 갖는 데이터를 수집하거나 생성한다. IoT 디바이스(110)가 생성하거나 수집하는 데이터의 기본 단위의 크기를 기준 크기라고 명명한다.

[0024] IoT 디바이스(110)가 생성하거나 수집하는 데이터는 도 3에서 "수집 data"로 표시한 블록의 크기를 갖는다고 가정한다. 도 2에서는 IoT 디바이스(110)가 하나의 기준 크기를 갖는 데이터만이 블록에 채워진 경우에도 나머지 여유 영역에 패딩을 하였다. 도 3에서는 IoT 디바이스(110)가 일차적으로 하나의 기준 크기를 갖는 데이터만이 블록에 채워진 경우라도, 곧바로 패딩하지 않고, 추가적인 데이터가 수집되는 것을 대기한다. 추가적인 데이터가 발생하면, IoT 디바이스(110)는 여유 영역에 추가적인 데이터를 채워넣는다. 도 3에서는 IoT 디바이스(110)가 추가적인 데이터를 채워넣고, 블록에서 기준 크기보다 작은 여유 영역은 패딩하였다. 이후 IoT 디바이스(110)는 블록을 암호화하여 서버(150)에 전달할 수 있다.

[0025] 도 4는 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법(200)에 대한 순서도의 예이다.

[0026] IoT 디바이스는 먼저 데이터를 획득한다(210). 데이터는 IoT 디바이스가 수집한 데이터 또는 IoT 디바이스가 특정 정보를 기반으로 생성한 데이터에 해당한다.

[0027] IoT 디바이스가 데이터를 블록 단위로 구분하여 암호화를 수행한다(220). 220 과정은 IoT 디바이스가 기준 크기의 데이터를 복수개 수집하여, 수집한 전체 데이터가 복수의 블록으로 구분되는 경우를 전제한 것이다. 220 과정은 블록이 모두 채워지는 경우 IoT 디바이스가 채워지는 블록을 암호화하는 과정이다. 물론 암호화 기법에 따라 블록이 채워지는 때마다 암호화를 진행할 수도 있고, 암호화할 모든 블록이 확정되면 모든 블록에 대한 암호화를 수행할 수도 있을 것이다.

[0028] IoT 디바이스는 데이터를 채우고 있는 현재 블록(데이터가 복수의 블록으로 구분된다면 마지막 블록)의 여유 영역이 기준 크기보다 큰지 여부를 확인한다(230). 여유 영역과 비교대상이 되는 기준 크기는 다양한 값이 사용될 수 있다. 다만 기본적으로 IoT 디바이스가 수집하는 데이터의 기준 크기(수 비트~ 수십 비트)를 사용한다고 가정한다.

[0029] 블록의 여유 영역의 크기가 기준 크기보다 작다면(no), IoT 디바이스는 해당 블록의 여유 영역을 패딩하고, 해당 블록을 암호화한다(260).

[0030] 블록의 여유 영역의 크기가 기준 크기보다 크다면(yes), IoT 디바이스는 기준 시간을 대기하면서 추가 데이터를 획득하는지 여부를 확인한다(240). 기준 시간은 IoT 디바이스가 수집하는 데이터의 특성, IoT 디바이스의 에너지 상태, IoT 디바이스를 이용한 서비스의 양태 등에 따라 다른 값이 사용될 수 있다. 대기하는 기준 시간 내에 IoT 디바이스가 추가 데이터를 수집하는 경우, IoT 디바이스가 추가 데이터를 여유 영역에 할당한다(250). 이후

IoT 디바이스는 해당 블록에서 아직 남아 있는 여유 영역을 패딩하고, 해당 블록을 암호화한다(260).

[0031] 도 5는 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법(200)에서 마지막 블록 구성을 도시한 예이다. 도 5(a)는 230 단계에서 여유 영역이 기준 크기 보다 큰 경우를 도시한다. 도 5(b)는 250 단계에서 기준 시간 내에 추가 데이터를 수집한 경우 IoT 디바이스가 추가 데이터를 도 5(a)의 여유 영역에 할당하고, 나머지 부분을 패딩한 경우를 도시한다. 도 5에서 수집 데이터는 IoT 디바이스가 수집한 의미 있는 데이터를 의미한다.

[0032] 도 5(c)는 240 단계에서 IoT 디바이스가 기준 시간 동안 대기하였는데, 기준 시간 내에 추가 데이터가 도착하지 않은 경우 해당 블록의 여유 영역을 모두 패딩한 상태를 도시한다. IoT 디바이스가 수집한 데이터를 서버가 일정한 서비스를 제공하는데 서비스를 제공하는 시간이 너무 지체된다면 바람직하지 않다. 따라서 일정한 기준 시간만을 대기하고, 대기 중인 시간 내에 추가 데이터가 수집되지 않는 다면, IoT 디바이스가 여유 영역을 패딩하여 암호화하는 것이 바람직할 수 있다.

[0033] 도 4에서는 기준 시간에 추가 데이터가 도착하는지 여부에 따라 블록의 구성이 달라진다. 그러나, 시간이 아닌 블록의 여유 영역의 크기를 기준으로 삼을 수도 있다. 도 5(d)는 도 5(a)의 상태에서 추가 데이터를 기다렸다가 해당 블록에 추가 데이터를 할당한 상태를 도시한다. 도 4 및 도 5(b)에서는 기준 시간 내에 추가 데이터가 도달하는지를 기준으로 추가 데이터를 블록에 할당하였지만, 도 5(d)는 현재 블록에 남아 있는 여유 영역이 기준 크기보다 큰지 여부만을 기준으로 한 경우이다. 즉, IoT 디바이스는 현재 블록에 남아 있는 여유 영역이 기준 크기보다 크다면 무조건 대기하여 다음 추가 데이터를 여유 영역에 할당한다. IoT 디바이스는 남아 있는 여유 영역이 기준 크기보다 작은 경우에만 남은 여유 영역을 패딩하고, 해당 블록을 암호화한다.

[0034] 도 6은 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법(300)에 대한 순서도의 다른 예이다. 도 6의 블록 암호화 방법(300)이 도 4의 블록 암호화 방법(200)과 다른 점은 블록 암호화 방법(300)은 블록에 여유 공간을 두지 않는 다는 점이다. 따라서 블록 암호화 방법(300)에서는 데이터의 전달 시간이 늦어질 수 있다. 서비스의 종류에 따라 데이터 수집의 실시간성이 필요 없는 경우 사용하는 것이 바람직하다.

[0035] IoT 디바이스는 먼저 데이터를 획득한다(310). IoT 디바이스가 데이터를 블록 단위로 구분하여 암호화를 수행한다(320). 320 과정은 IoT 디바이스가 기준 크기의 데이터를 복수개 수집하여, 수집한 전체 데이터가 복수의 블록으로 구분되는 경우를 전제한 것이다. 320 과정은 블록이 모두 채워지는 경우 IoT 디바이스가 채워지는 블록을 암호화하는 과정이다.

[0036] IoT 디바이스는 데이터를 채우고 있는 현재 블록(데이터가 복수의 블록으로 구분된다면 마지막 블록)의 여유 영역이 존재하는지 여부를 확인한다(330). 현재 블록에 여유 영역이 없다면 IoT 디바이스는 해당 블록을 암호화한다(370).

[0037] 현재 블록에 여유 영역이 존재한다면, IoT 디바이스는 추가 데이터를 획득할 때까지 대기한다(340). 추가 데이터를 획득한 경우 IoT 디바이스는 여유 영역에 추가 데이터를 할당한다(350). IoT 디바이스가 350 단계에서 추가 데이터를 할당한 상태에서 현재 블록에 여유 영역이 존재하는지 여부를 확인한다(360). 여유 영역이 아직도 남아 있다면, IoT 디바이스는 다시 추가 데이터를 대기한다. 현재 블록에 여유 영역이 없다면, IoT 디바이스는 해당 블록을 암호화 한다(370).

[0038] 도 6에서는 모든 블록을 채운 경우를 예로 설명하였다. 그러나 반드시 모든 블록을 채울 필요가 없을 수 있다. 시스템의 필요에 따라 남아 있는 여유 영역의 크기가 특정한 크기보다 작다면 IoT 디바이스가 남은 영역을 패딩하고, 해당 블록을 암호화할 수도 있을 것이다.

[0039] 도 7는 IoT 네트워크에서 대칭키를 이용한 블록 암호화 방법(300)에서 마지막 블록 구성을 도시한 다른 예이다. 도 7(a)는 현재 블록에 여유 영역이 있는 상태를 도시한다. 도 7(b)는 IoT 디바이스가 1차적으로 추가 데이터를 대기하고, 블록을 채웠는데, 아직도 일정한 여유 영역이 남아 있는 상태를 도시한다. 이 경우 IoT 디바이스는 2차적으로 추가 데이터를 대기할 수 있다. IoT 디바이스는 2차 추가 데이터를 수집한 경우 남아 있는 여유 영역을 도 7(c)와 같이 모두 채워 넣을 수 있다. 도 7(c)는 블록에 패딩된 데이터가 전혀 없는 상태를 도시한다. 도 7(c)와 같이 모든 블록에 의미 있는 실제 수집 데이터를 채우는 경우, IoT 디바이스가 수집하는 하나의 단위의 데이터가 일부만 블록에 할당될 수 있다. 도 7(c)는 IoT 디바이스가 수집하는 하나의 단위 데이터가 일부만 해당 블록 마지막에 채워진 경우이다. 이 경우 IoT 디바이스는 다음 블록의 처음에 도 7(d)와 같이 하나의 단위 데이터의 나머지 부분을 할당한다. 즉, 수집 data A 및 수집 data B는 IoT 디바이스가 수집하는 하나의 단위 데이터이다.

[0040] 본 실시예 및 본 명세서에 첨부된 도면은 전술한 기술에 포함되는 기술적 사상의 일부를 명확하게 나타내고 있

는 것에 불과하며, 전술한 기술의 명세서 및 도면에 포함된 기술적 사상의 범위 내에서 당업자가 용이하게 유추할 수 있는 변형 예와 구체적인 실시예는 모두 전술한 기술의 권리범위에 포함되는 것이 자명하다고 할 것이다.

부호의 설명

[0041] 100 : IoT 네트워크 시스템

110 : IoT 디바이스

110A, 110B, 110C : IoT 디바이스

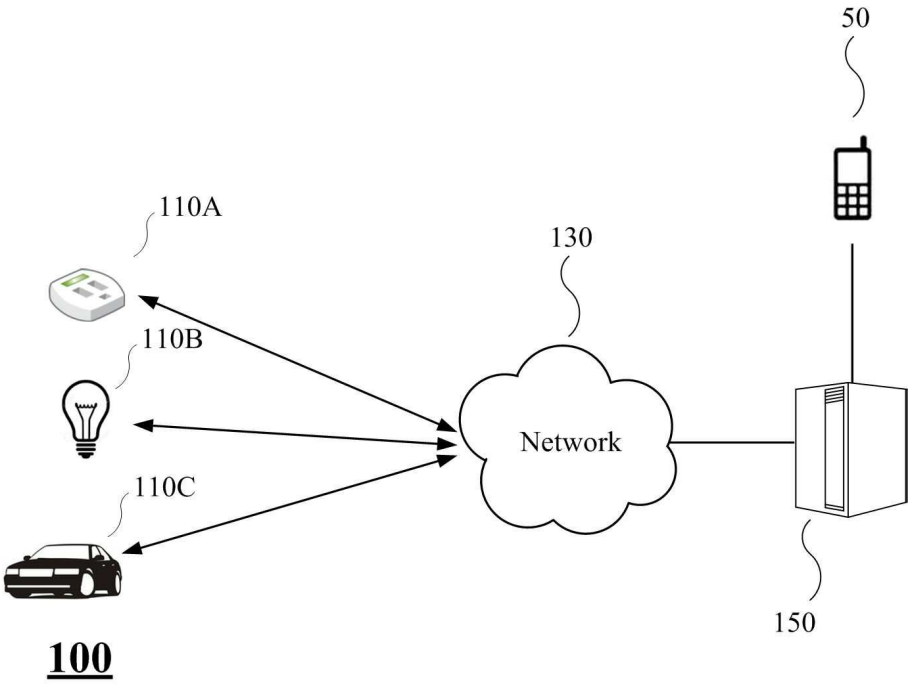
130 : 네트워크

150 : 서버

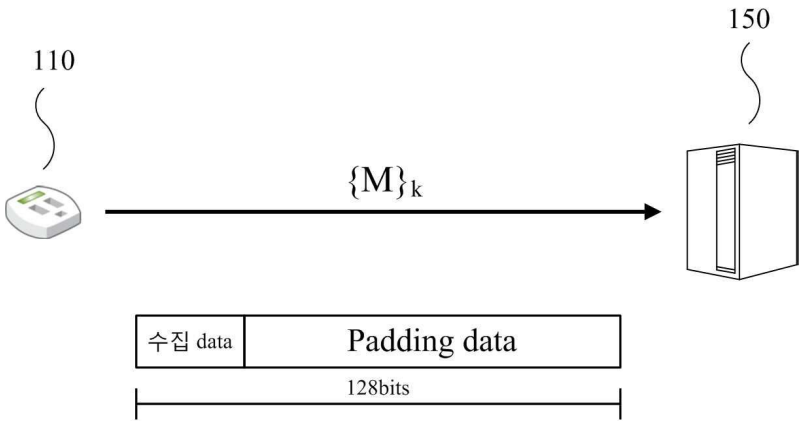
50 : 사용자 단말

도면

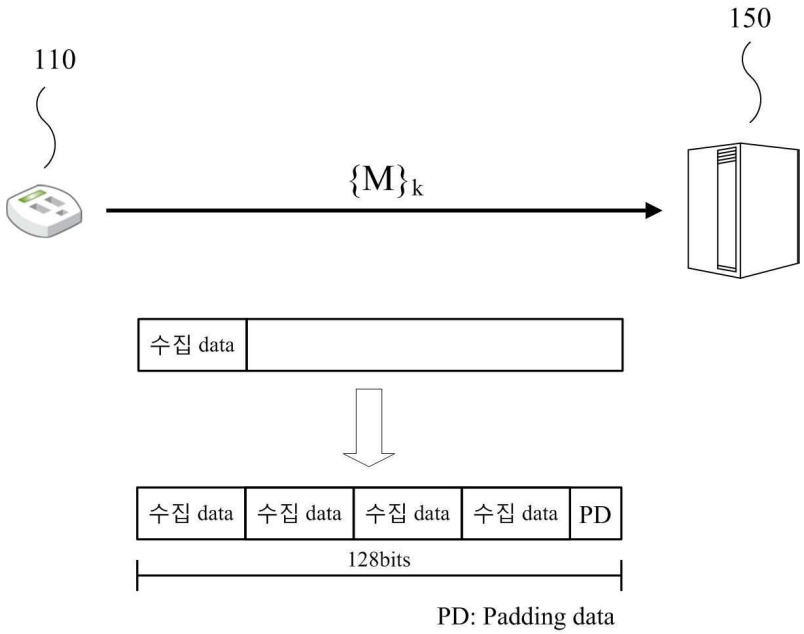
도면1



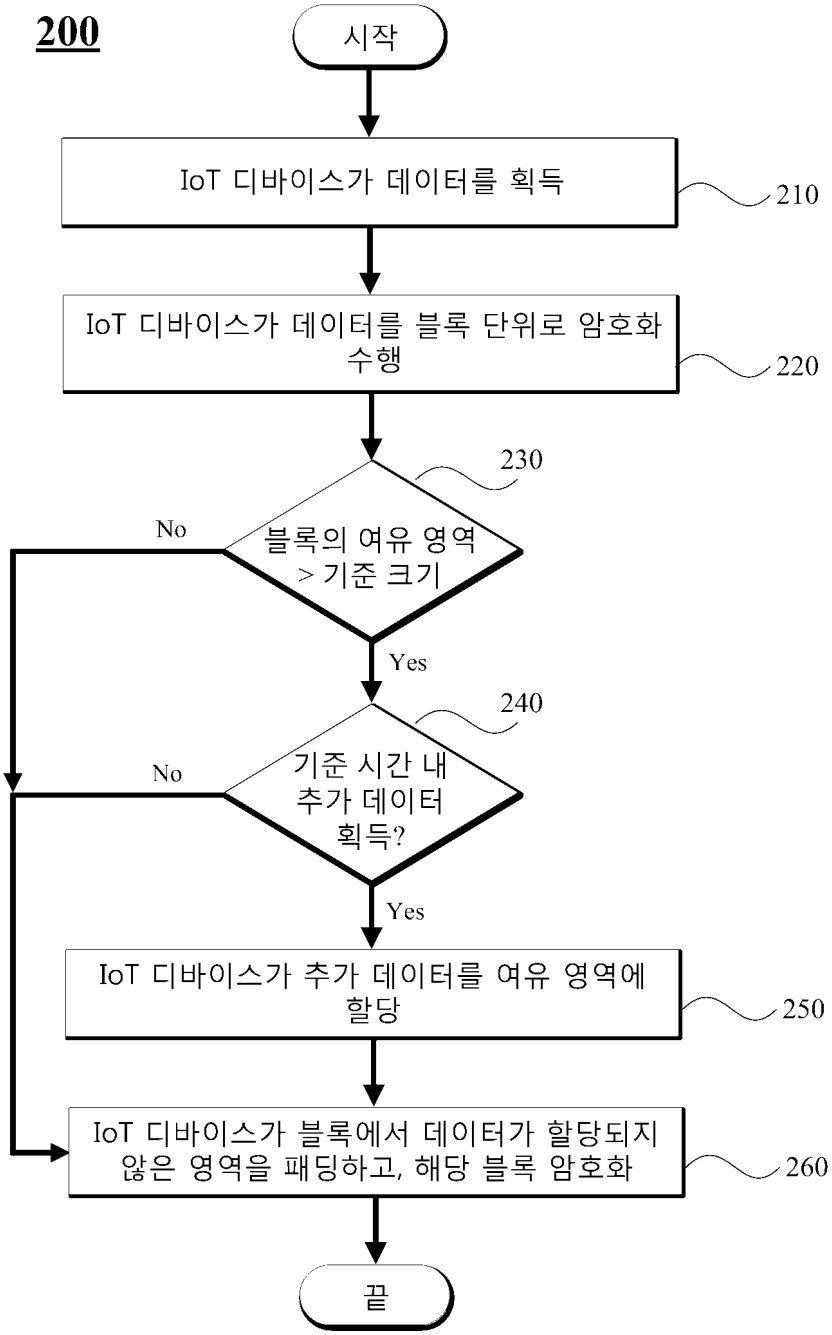
도면2



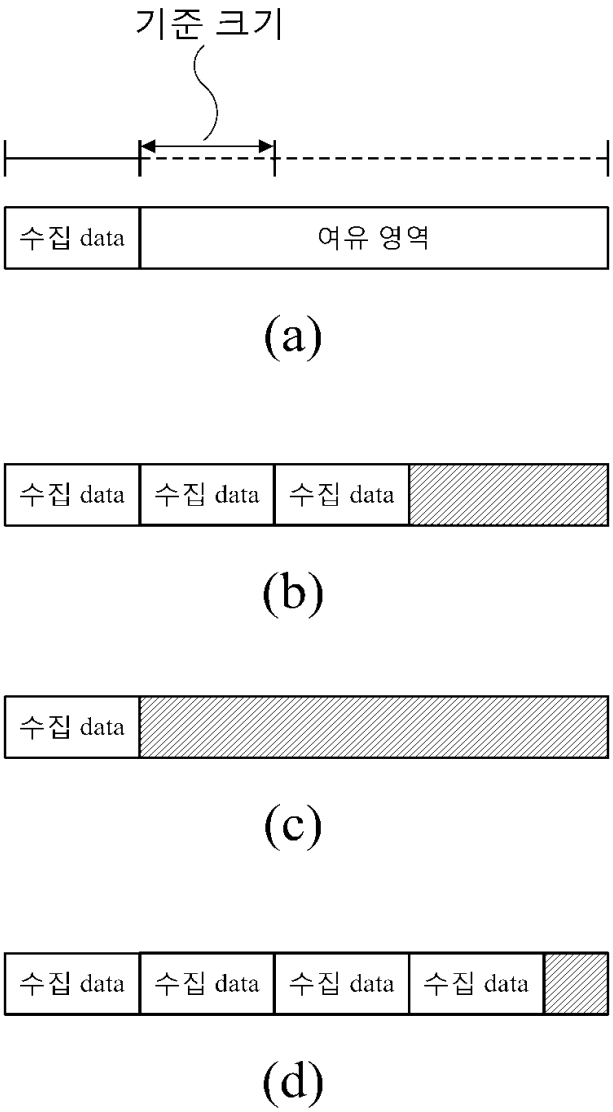
도면3


110
150
{M}k
수집 data
수집 data
수집 data
수집 data
수집 data
PD
128bits
PD: Padding data

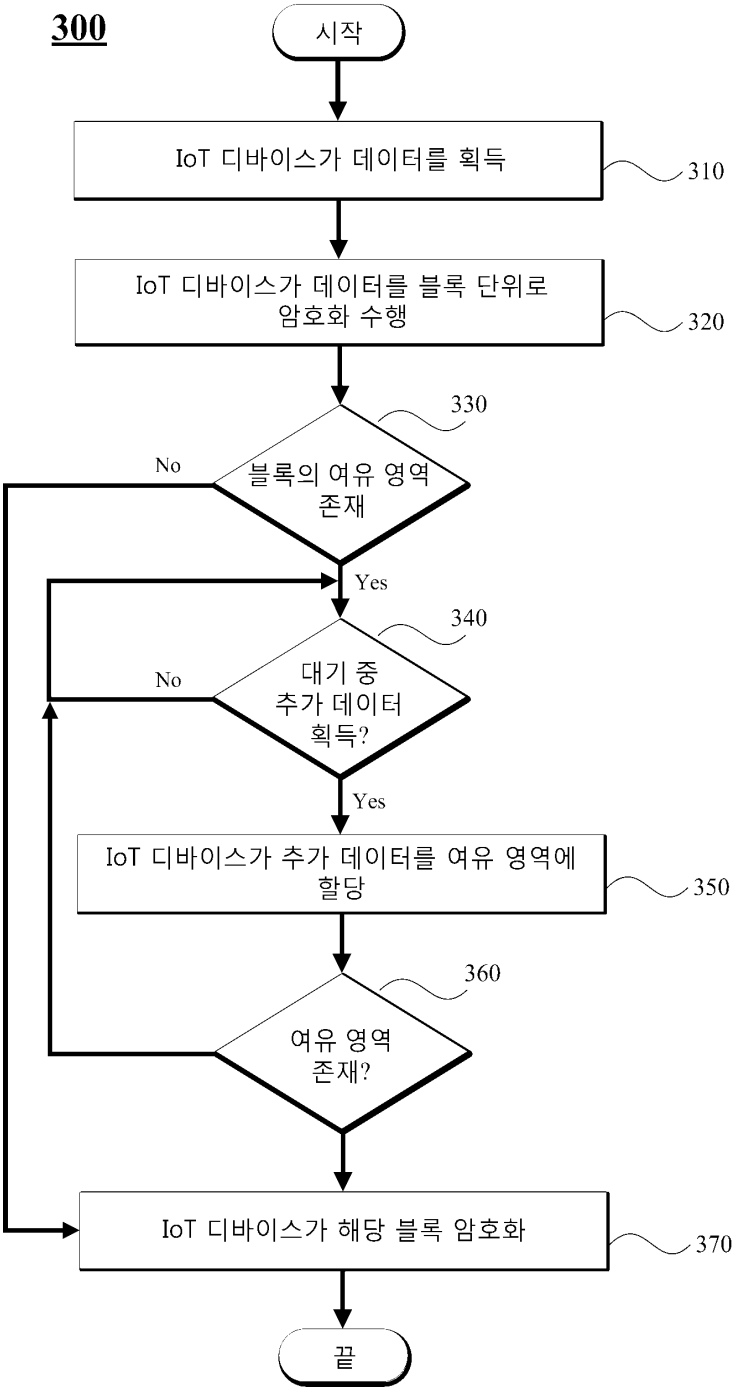
도면4


200
시작
IoT 디바이스가 데이터를 획득
210
IoT 디바이스가 데이터를 블록 단위로 암호화 수행
220
230
블록의 여유 영역 > 기준 크기
No
Yes
240
기준 시간 내 추가 데이터 획득?
No
Yes
IoT 디바이스가 추가 데이터를 여유 영역에 할당
250
IoT 디바이스가 블록에서 데이터가 할당되지 않은 영역을 패딩하고, 해당 블록 암호화
260
끝

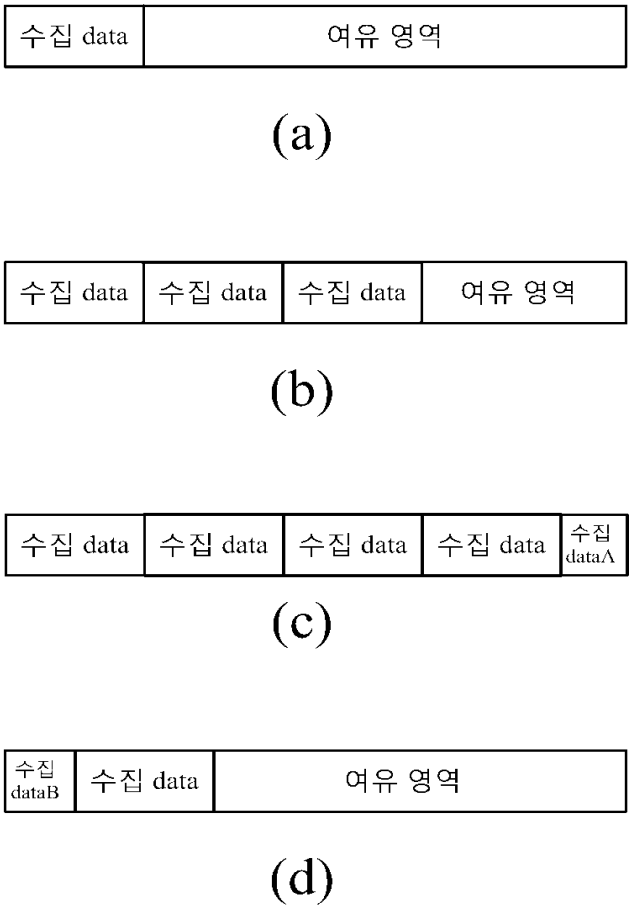
도면5


기준 크기
수집 data
여유 영역
(a)
수집 data
수집 data
수집 data
(b)
수집 data
(c)
수집 data
수집 data
수집 data
수집 data
(d)

도면6


300
시작
IoT 디바이스가 데이터를 획득
310
IoT 디바이스가 데이터를 블록 단위로 암호화 수행
320
330
블록의 여유 영역 존재
No
Yes
340
대기 중 추가 데이터 획득?
No
Yes
IoT 디바이스가 추가 데이터를 여유 영역에 할당
350
360
여유 영역 존재?
IoT 디바이스가 해당 블록 암호화
370
끝

도면7


수집 data
여유 영역
(a)
수집 data
수집 data
수집 data
여유 영역
(b)
수집 data
수집 data
수집 data
수집 data
수집 dataA
(c)
수집 dataB
수집 data
여유 영역
(d)