(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년10월23일
(11) 등록번호 10-2169598
(24) 등록일자 2020년10월19일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 21/44* (2013.01)
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)
(52) CPC특허분류
G06F 21/62 (2013.01)
G06F 21/445 (2013.01)
(21) 출원번호 10-2019-0016520
(22) 출원일자 2019년02월13일
심사청구일자 2019년02월13일
(65) 공개번호 10-2020-0098872
(43) 공개일자 2020년08월21일
(56) 선행기술조사문헌
KR1020100097430 A*
KR1020160129852 A*
KR1020170004108 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
박기웅
서울특별시 광진구 능동로17길 21, 304호(화양동)
김시은
서울특별시 광진구 동일로36길 14-2, 102호(군자동)
(74) 대리인
양성보

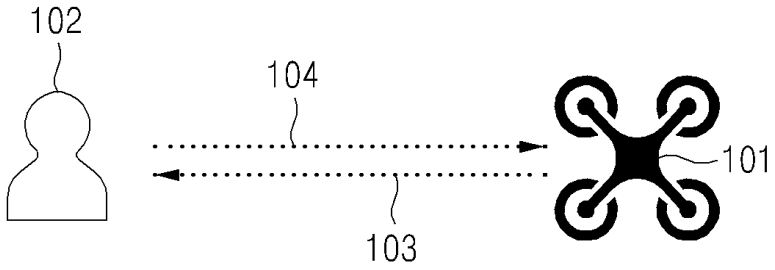
전체 청구항 수 : 총 12 항 심사관 : 지정훈

(54) 발명의 명칭 **무인 항공기를 위한 신뢰성 보장형 원격 데이터 삭제 기술**

(57) 요 약

무인 항공기를 위한 신뢰성 보장형 원격 데이터 삭제 기술이 개시된다. 일 실시예에 따른 원격 데이터 삭제 시스템에 의해 수행되는 원격 데이터 삭제 방법은, 전자 기기가 초기화 과정을 통해 상호 인증한 사용자와의 주기적 인증을 수행하는 단계; 및 상기 전자 기기에서 상기 사용자와의 인증 성공 여부에 따라 변경되는 타이머 기반의 카운터 값에 기초하여 상기 전자 기기에 저장된 데이터를 원격 삭제하는 단계를 포함할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3236 (2013.01)
H04L 9/3273 (2013.01)
H04W 12/0609 (2019.01)
G06F 2221/2143 (2013.01)
H04L 2209/38 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711067615
부처명 과학기술정보통신부
과제관리(전문)기관명 한국연구재단
연구사업명 개인기초연구(과기정통부)(R&D)
연구과제명 클라우드 플랫폼의 심층 보안관제 및 포렌식을 위한 Replayable Cloud-Memory 원천 기술 개발
기 여 율 1/1
과제수행기관명 세종대학교
연구기간 2017.03.01 ~ 2020.02.28
공지예외적용 : 있음

명 세 서

청구범위

청구항 1

원격 데이터 삭제 시스템에 의해 수행되는 원격 데이터 삭제 방법에 있어서,

전자 기기가 초기화 과정을 통해 상호 인증한 사용자와의 주기적 인증을 수행하는 단계; 및

상기 전자 기기에서 상기 사용자와의 인증 성공 여부에 따라 변경되는 타이머 기반의 카운터 값에 기초하여 상기 전자 기기에 저장된 데이터를 원격 삭제하는 단계

를 포함하고,

상기 원격 삭제된 데이터에 대한 삭제 연산을 증명하여 데이터의 삭제를 검증하는 단계

를 더 포함하고,

상기 데이터의 삭제를 검증하는 단계는,

상기 원격 삭제된 데이터에 대한 삭제 연산을 해시 체인에 기반하여 콜드 데이터, 축적 데이터 및 핫 데이터 각각의 삭제 여부를 검증한 증거를 사용자에게 전송하고, 상기 콜드 데이터, 축적 데이터 및 핫 데이터 각각의 삭제 연산을 반복하여 수행하고, 상기 콜드 데이터, 축적 데이터 및 핫 데이터 각각의 마지막 블록이 새로운 값으로 변경될 때까지를 하나의 라운드로 정의하고, 상기 정의된 라운드를 복수 번 진행하여 데이터의 종류와 상관없이 삭제 연산을 수행하고, 상기 복수 번의 라운드를 진행하여 획득된 각 데이터의 마지막 블록의 해시값을 삭제 증거로 사용자에게 전달하는 단계

를 포함하는 원격 데이터 삭제 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 주기적 인증을 수행하는 단계는,

상기 사용자와의 상호 인증이 수행됨에 따라 상기 사용자와 상기 전자 기기간 해시 체인에 기반한 인증 메시지를 교환하는 단계

를 포함하는 원격 데이터 삭제 방법.

청구항 4

제3항에 있어서,

상기 주기적 인증을 수행하는 단계는,

상기 전자 기기에서 상기 사용자로부터 전달된 인증 요청 메시지를 계산한 결과값과 상기 전자 기기에 저장된 해시값을 비교함에 따른 비교 결과가 일치할 경우, 상기 전자 기기의 카운터 값을 재설정하고, 상기 해시값을 업데이트하는 단계

를 포함하는 원격 데이터 삭제 방법.

청구항 5

제4항에 있어서,

상기 주기적 인증을 수행하는 단계는,

상기 전자 기기에서 상기 사용자의 해시값을 전달받지 못할 경우, 특정 주기마다 카운트 값이 변화하는 단계

를 포함하는 원격 데이터 삭제 방법.

청구항 6

제3항에 있어서,

상기 주기적 인증을 수행하는 단계는,

상기 사용자가 상기 전자 기기에게 전달한 인증 요청 메시지에 대한 응답으로 인증 성공 메시지를 미수신한 경우, 상기 전자 기기에게 인증 재요청 메시지가 재전송되는 단계

를 포함하는 원격 데이터 삭제 방법.

청구항 7

제1항에 있어서,

상기 데이터를 원격 삭제하는 단계는,

상기 전자 기기의 카운트 값이 변화함에 따라 카운트 값이 기 설정된 값이 되면, 각 데이터 영역에 대하여 XOR 연산을 진행하여 삭제 연산을 수행하는 단계

를 포함하는 원격 데이터 삭제 방법.

청구항 8

제7항에 있어서,

상기 데이터 영역은,

고정 값을 저장하는 콜드 데이터, 전자 기기에서 촬영을 수행하여 생성되는 데이터를 저장하는 축적 데이터 및 수정된 데이터를 업데이트하는 핫 데이터를 포함하는 데이터 영역으로 분류되는, 원격 데이터 삭제 방법.

청구항 9

제7항에 있어서,

상기 데이터를 원격 삭제하는 단계는,

상기 사용자로부터 수신된 마지막 해시값을 이용하여 콜드 데이터를 삭제하는 단계

를 포함하는 원격 데이터 삭제 방법.

청구항 10

제7항에 있어서,

상기 데이터를 원격 삭제하는 단계는,

축적 데이터 중 임의의 위치에 대한 축적 데이터 값을 통하여 삭제 연산을 수행하는 단계

를 포함하는 원격 데이터 삭제 방법.

청구항 11

제7항에 있어서,

상기 데이터를 원격 삭제하는 단계는,

핫 데이터 중 임의의 위치에 대한 핫 데이터 값을 통하여 삭제 연산을 수행하는 단계

를 포함하는 원격 데이터 삭제 방법.

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

원격 데이터 삭제 시스템에 의해 수행되는 원격 데이터 삭제 방법에 있어서,

전자 기기가 초기화 과정을 통해 상호 인증한 사용자와의 주기적 인증을 수행하는 단계; 및

상기 전자 기기에서 상기 사용자와의 인증 성공 여부에 따라 변경되는 타이머 기반의 카운터 값에 기초하여 상기 전자 기기에 저장된 데이터를 원격 삭제하는 단계

를 포함하고,

상기 주기적 인증을 수행하는 단계는,

상기 전자 기기와 상기 사용자 간에 상기 인증에 사용될 암호화 키를 공유하고, 상기 사용자로부터 상기 공유한 암호화 키를 사용하여 임의의 숫자 데이터(x)와 인증 가능한 최대 횟수(n)에 기반하여 암호화함에 따라 생성된 메시지가 상기 전자 기기에게 전송되고, 상기 전자 기기에서 상기 공유된 암호화 키를 이용하여 상기 메시지를 복호화하여 상기 숫자 데이터 및 상기 인증 가능한 최대 횟수를 확인하고, 상기 확인된 숫자 데이터와 상기 인증 가능한 최대 횟수에 기반한 해시값을 계산하여 상기 인증 가능한 최대 횟수와 상기 계산된 해시값을 저장하고, 상기 계산된 해시값을 상기 사용자에게 전송하고, 상기 사용자로부터 상기 전자 기기로부터 전달받은 해시값에 기반하여 상기 임의의 숫자 데이터와 상기 인증 가능한 최대 횟수를 확인하여 상기 전자 기기와 상기 사용자의 상호 인증을 수행하는 초기화 과정을 수행하는 단계

를 포함하는 원격 데이터 삭제 방법.

청구항 16

컴퓨터로 구현되는 컴퓨팅 보호 시스템에 있어서,

컴퓨터에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서

를 포함하고,

상기 적어도 하나의 프로세서는,

전자 기기가 초기화 과정을 통해 상호 인증한 사용자와의 주기적 인증을 수행하는 과정;

상기 전자 기기에서 상기 사용자와의 인증 성공 여부에 따라 변경되는 타이머 기반의 카운터 값에 기초하여 상기 전자 기기에 저장된 데이터를 원격 삭제하는 과정; 및

상기 원격 삭제된 데이터에 대한 삭제 연산을 증명하여 데이터의 삭제를 검증하는 과정

을 포함하고,

상기 데이터의 삭제를 검증하는 과정은,

상기 원격 삭제된 데이터에 대한 삭제 연산을 해시 체인에 기반하여 콜드 데이터, 축적 데이터 및 핫 데이터 각각의 삭제 여부를 검증한 증거를 사용자에게 전송하고, 상기 콜드 데이터, 축적 데이터 및 핫 데이터 각각의 삭제 연산을 반복하여 수행하고, 상기 콜드 데이터, 축적 데이터 및 핫 데이터 각각의 마지막 블록이 새로운 값으로 변경될 때까지를 하나의 라운드로 정의하고, 상기 정의된 라운드를 복수 번 진행하여 데이터의 종류와 상관없이 삭제 연산을 수행하고, 상기 복수 번의 라운드를 진행하여 획득된 각 데이터의 마지막 블록의 해시값을 삭제 증거로 사용자에게 전달하는

원격 데이터 삭제 시스템.

발명의 설명

기 술 분 야

[0001] 아래의 설명은 전자 기기를 위한 신뢰성 보장형 원격 데이터 삭제 시스템 및 그 제공방법에 관한 것이다.

배 경 기 술

[0003] 임베디드 기기가 사용되는 영역이 널리 확장됨에 따라 군사 영역에서도 인력 손실을 줄이기 위한 목적 등으로 드론을 적극적으로 활용하고 있다. 군사용 드론은 원거리 핵심표적 타격임무를 수행하는 무기로써 사용되거나 적의 핵심시설과 표적에 대한 첩보를 수집하는 등의 임무를 수행한다.

[0004] 그러나 임무를 수행하는 드론은 군사 영역과 관련된 기밀 정보를 담고 있는 경우가 많기 때문에 해당 군사 기기가 탈취 혹은 격추를 당하여 기기에 대한 제어권을 상실하게 되면 저장된 기밀 데이터를 탈취당할 가능성이 높아진다. 이에 따라 군사 영역에서 사용되는 드론은 사용자의 제어권을 벗어났을 때 내장된 데이터를 복구가 불가능하도록 완전히 삭제하고 삭제가 진행되었음을 검증할 수 있는 보장 기술이 요구되고 있다.

[0005] 참고자료: KR10-2015-0129601, KR10-1791351

발명의 내용

해결하려는 과제

[0007] 원격에 존재하는 드론과 사용자 간의 주기적 인증을 수행하며 정해진 시간을 경과할 때까지 인증을 수행하지 못할 시 드론에 저장된 데이터를 안전하게 삭제하고 삭제 연산이 수행되었음을 보장하는 증거를 사용자에게 전달하여 드론에 저장된 데이터가 삭제되었음을 보장할 수 있는 방법 및 시스템을 제공할 수 있다.

[0008] 드론에 저장된 데이터를 삭제하는 경우 데이터의 복구가 불가능하도록 하여, 드론을 탈취하거나 획득한 사용자가 추후 데이터를 복구하여 데이터를 사용할 수 있는 위험을 제거할 수 있는 방법 및 시스템을 제공할 수 있다.

[0009] 드론과 사용자간의 통신이 끊어졌음에도 불구하고, 드론에 저장된 데이터를 안전하게 삭제하고, 삭제 연산이 수행되었음을 증명하는 증거를 사용자에게 송신하도록 하여 통신이 끊어진 드론에서 안전하고 증명 가능한 삭제를 수행할 수 있는 방법 및 시스템을 제공할 수 있다.

과제의 해결 수단

[0011] 원격 데이터 삭제 시스템에 의해 수행되는 원격 데이터 삭제 방법은, 전자 기기가 초기화 과정을 통해 상호 인증한 사용자와의 주기적 인증을 수행하는 단계; 및 상기 전자 기기에서 상기 사용자와의 인증 성공 여부에 따라 변경되는 타이머 기반의 카운터 값에 기초하여 상기 전자 기기에 저장된 데이터를 원격 삭제하는 단계를 포함할 수 있다.

[0012] 상기 원격 데이터 삭제 방법은, 상기 원격 삭제된 데이터에 대한 삭제 연산을 증명하여 데이터의 삭제를 검증하는 단계를 더 포함할 수 있다.

[0013] 상기 주기적 인증을 수행하는 단계는, 상기 사용자와의 상호 인증이 수행됨에 따라 상기 사용자와 상기 전자 기기간 해시 체인에 기반한 인증 메시지를 교환하는 단계를 포함할 수 있다.

[0014] 상기 주기적 인증을 수행하는 단계는, 상기 전자 기기에서 상기 사용자로부터 전달된 인증 요청 메시지를 계산한 결과값과 상기 전자 기기에 저장된 해시값을 비교함에 따른 비교 결과가 일치할 경우, 상기 전자 기기의 카운터 값을 재설정하고, 상기 해시값을 업데이트하는 단계를 포함할 수 있다.

[0015] 상기 주기적 인증을 수행하는 단계는, 상기 전자 기기에서 상기 사용자의 해시값을 전달받지 못할 경우, 특정 주기마다 카운트 값이 변화하는 단계를 포함할 수 있다.

[0016] 상기 주기적 인증을 수행하는 단계는, 상기 사용자가 상기 전자 기기에게 전달한 인증 요청 메시지에 대한 응답으로 인증 성공 메시지를 미수신한 경우, 상기 전자 기기에게 인증 재요청 메시지가 재전송되는 단계를 포함할

수 있다.

[0017] 상기 데이터를 원격 삭제하는 단계는, 상기 전자 기기의 카운트 값이 변화함에 따라 카운트 값이 기 설정된 값이 되면, 각 데이터 영역에 대하여 XOR 연산을 진행하여 삭제 연산을 수행하는 단계를 포함할 수 있다.

[0018] 상기 데이터 영역은, 고정 값을 저장하는 콜드 데이터, 전자 기기에서 촬영을 수행하여 생성되는 데이터를 저장하는 축적 데이터 및 수정된 데이터를 업데이트하는 핫 데이터를 포함하는 데이터 영역으로 분류될 수 있다.

[0019] 상기 데이터를 원격 삭제하는 단계는, 상기 사용자로부터 수신된 마지막 해시값을 이용하여 상기 콜드 데이터를 삭제하는 단계를 포함할 수 있다.

[0020] 상기 데이터를 원격 삭제하는 단계는, 상기 축적 데이터 중 임의의 위치에 대한 축적 데이터 값을 통하여 삭제 연산을 수행하는 단계를 포함할 수 있다.

[0021] 상기 데이터를 원격 삭제하는 단계는, 상기 핫 데이터 중 임의의 위치에 대한 핫 데이터 값을 통하여 삭제 연산을 수행하는 단계를 포함할 수 있다.

[0022] 상기 데이터의 삭제를 검증하는 단계는, 상기 원격 삭제된 데이터에 대한 삭제 연산을 해시 체인에 기반하여 콜드 데이터, 축적 데이터 및 핫 데이터 각각의 삭제 여부를 검증한 증거를 사용자에게 전송하는 단계를 포함할 수 있다.

[0023] 상기 데이터의 삭제를 검증하는 단계는, 상기 콜드 데이터, 축적 데이터 및 핫 데이터 각각의 삭제 연산을 반복하여 수행하는 단계를 포함할 수 있다.

[0024] 상기 데이터의 삭제를 검증하는 단계는, 상기 콜드 데이터, 축적 데이터 및 핫 데이터 각각의 마지막 블록이 새로운 값으로 변경될 때까지를 하나의 라운드로 정의하고, 상기 정의된 라운드를 복수 번 진행하여 데이터의 종류와 상관없이 삭제 연산을 수행하고, 상기 복수 번의 라운드를 진행하여 획득된 각 데이터의 마지막 블록의 해시값을 삭제 증거로 사용자에게 전달하는 단계를 포함할 수 있다.

[0025] 상기 주기적 인증을 수행하는 단계는, 상기 전자 기기와 상기 사용자 간에 상기 인증에 사용될 암호화 키를 공유하고, 상기 사용자로부터 상기 공유한 암호화 키를 사용하여 임의의 숫자 데이터(x)와 인증 가능한 최대 횟수(n)에 기반하여 암호화함에 따라 생성된 메시지가 상기 전자 기기에게 전송되고, 상기 전자 기기에서 상기 공유된 암호화 키를 이용하여 상기 메시지를 복호화하여 상기 숫자 데이터 및 상기 인증 가능한 최대 횟수를 확인하고, 상기 확인된 숫자 데이터와 상기 인증 가능한 최대 횟수에 기반한 해시값을 계산하여 상기 인증 가능한 최대 횟수와 상기 계산된 해시값을 저장하고, 상기 계산된 해시값을 상기 사용자에게 전송하고, 상기 사용자로부터 상기 전자 기기로부터 전달받은 해시값에 기반하여 상기 임의의 숫자 데이터와 상기 인증 가능한 최대 횟수를 확인하여 상기 전자 기기와 상기 사용자의 상호 인증을 수행하는 초기화 과정을 수행하는 단계를 포함할 수 있다.

[0026] 컴퓨터로 구현되는 컴퓨팅 보호 시스템은, 컴퓨터에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 전자 기기가 초기화 과정을 통해 상호 인증한 사용자와의 주기적 인증을 수행하는 과정; 및 상기 전자 기기에서 상기 사용자와의 인증 성공 여부에 따라 변경되는 타이머 기반의 카운터 값에 기초하여 상기 전자 기기에 저장된 데이터를 원격 삭제하는 과정을 포함할 수 있다.

발명의 효과

[0028] 원격에 존재하는 드론과 사용자간의 카운터 기반의 주기적 인증을 수행하고, 드론에 내장된 카운터 값이 특정 시간을 경과할 때까지 인증이 수행되지 못하면 드론에 저장된 데이터를 삭제할 수 있도록 하여, 드론이 탈취당하거나 예기치 못한 사고로 통신이 끊겨 사용자와 통신이 불가능한 경우에도 드론에 저장된 데이터가 삭제됨으로써 사용자의 제어권을 벗어난 상황에서는 데이터를 사용할 수 없도록 하여 보안을 향상시킬 수 있다.

[0029] 또한, 데이터를 삭제 하는 경우, 데이터의 복구가 불가능하도록 삭제하여 추후 삭제 연산을 종료한 드론이 악의적인 사용자에 의해 탈취되거나 우연히 획득되더라도 데이터를 사용할 수 없도록 할 수 있다.

[0030] 또한, 데이터를 삭제한 이후, 사용자에게 삭제 연산이 수행되었음을 알리는 증거를 전송함으로써, 데이터가 확실히 삭제되었는지 검증할 수 있다.

도면의 간단한 설명

[0032] 도 1은 일 실시예에 따른 원격 데이터 삭제 시스템이 적용되는 환경을 설명하기 위한 도면이다.

도 2는 일 실시예에 따른 원격 데이터 삭제 시스템의 구성을 설명하기 위한 블록도이다.

도 3은 일 실시예에 따른 원격 데이터 삭제 시스템에서 주기적 인증을 수행하는 것을 설명하기 위한 예이다.

도 4는 일 실시예에 있어서, 전자 기기의 타이머 기반의 원격 데이터 삭제 방법을 설명하기 위한 흐름도이다.

도 5는 일 실시예에 따른 원격 데이터 삭제 시스템에서 인증 요청 메시지를 재전송하는 것을 설명하기 위한 예이다.

도 6은 일 실시예에 있어서, 다른 전자 기기의 원격 데이터 삭제 방법을 설명하기 위한 흐름도이다.

도 7은 일 실시예에 따른 원격 데이터 삭제 시스템의 데이터 구조를 설명하기 위한 도면이다.

도 8 내지 도 11은 일 실시예에 따른 원격 데이터 삭제 시스템의 삭제 연산을 설명하기 위한 도면이다.

도 12는 일 실시예에 따른 원격 데이터 삭제 시스템에서 삭제 연산에 대한 증거를 송신하는 것을 설명하기 위한 예이다.

발명을 실시하기 위한 구체적인 내용

[0033] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0035] 아래의 실시예는 원격에 존재하는 무인 비행기(드론)과 사용자 간에 카운터 기반의 주기적인 인증을 수행할 수 있도록 하고, 설정된 시간 내에 인증이 수행되지 못할 경우 무인 비행기에 저장된 데이터를 복구할 수 없는 방식으로 안전하게 삭제한 후 사용자에게 삭제의 증거를 송신하여 사용자가 무인 비행기에 저장된 데이터의 삭제 여부를 증명할 수 있도록 하고, 사용자가 무인 비행기를 잃어버리거나 탈취당한 경우에도 무인 비행기에 저장된 데이터를 읽거나 복구할 수 없도록 만드는 시스템 및 그 제공방법에 관한 것이다.

[0036] 도 1은 일 실시예에 따른 드론을 위한 신뢰성 보장형 원격 데이터 삭제 시스템이 적용되는 환경을 설명하기 위한 도면이다.

[0037] 드론을 위한 신뢰성 보장형 원격 데이터 삭제 시스템(이하, '원격 데이터 삭제 시스템'으로 기재하기로 함.)은 원격에 존재하는 전자 기기(101), 전자 기기(101)와 통신하는 사용자(102)간의 데이터 송수신을 수행하는 환경에서 이루어질 수 있다. 이때, 사용자(102)가 전자 기기(101)에게 인증 메시지(104)를 전송할 수 있고, 전자 기기(101)가 사용자(102)에게 인증 메시지(104)를 수신함에 따라 인증 메시지(104)와 관련하여 인증 확인 메시지(103)로 응답할 수 있다.

[0038] 전자 기기(101)는 컴퓨터 장치로 구현되는 고정형 단말이거나 이동형 단말일 수 있다. 전자 기기(101)의 예를 들면, 스마트폰(smart phone), 휴대폰, 네비게이션, 컴퓨터, 노트북, 디지털방송용 단말, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 태블릿 PC 등이 있다. 전자 기기(101)는 무선 또는 유선 통신 방식을 이용하여 네트워크를 통해 다른 전자 기기(사용자의 전자 기기)/사용자와 통신할 수 있다. 실시예에서는 전자 기기(101)는 드론(UAV)과 같은 군용 장치일 수 있으며, 전자 기기(101) 내에 원격 데이터 삭제 시스템이 플랫폼 또는 프로그램 형태로 구동될 수 있다. 마찬가지로, 원격 데이터 삭제 시스템은 다른 전자 기기에 플랫폼 또는 프로그램 형태로 동작되어 사용자와 드론간 데이터의 송수신을 통하여 드론을 위한 신뢰성 보장형 원격 데이터를 삭제할 수 있다. 예를 들면, 다른 전자 기기는 전자 기기(101)를 제어하는 사용자 단말 또는 서버일 수 있다. 아래의 설명에서는 다른 전자 기기의 설명의 이해를 돕기 위하여 사용자로 기재하기로 한다. 또한, 실시예에서 사용되는 각 변수를 우선적으로 기재하기로 한다.

$K_{x,y}$: x와 y 사이에 교환된 대칭키
E { K, B } : 키 K로 B를 암호화
x : 해시 연산의 대상이 되는 값
n : 해시 연산의 횟수
r : 재전송 비트
i : 인증 횟수
$h(x)$: x 를 해시 연산한 결과값
nonce : 넌스값
al : 이전 인증 이후, 변화한 축적형 데이터의 주소값
hl : 이전 인증 이후, 변화한 핫 데이터의 주소값
av : 임의로 선택된 축적형 데이터의 값과 그에 대한 주소값
hv : 임의로 선택된 핫 데이터의 값과 그에 대한 주소값
α || β : 해당 메시지에는 α와 β가 포함됨을 나타냄
α || (β) : 해당 메시지에는 α가 포함되며, β는 선택적으로 포함됨

[0039]

[0040] 도 2는 일 실시예에 따른 드론을 위한 신뢰성 보장형 원격 데이터 삭제 시스템의 구성을 설명하기 위한 블록도이다.

[0041] 원격 데이터 삭제 시스템(100)은 카운터 모듈(201), 인증 모듈(202), 암복호화 모듈(203), 통신 모듈(204) 및 삭제 모듈(205)을 포함할 수 있다. 구현 예에 따라 원격 데이터 삭제 시스템은 안정성을 위해 보조 전력 모듈을 더 포함할 수 있다.

[0042] 카운터 모듈(201)은 드론이 사용자와의 인증을 받은 시점부터 카운트를 하기 위해 사용된다.

[0043] 인증 모듈(202)과 통신 모듈(204)은 사용자와의 주기적 인증을 위해 사용된다.

[0044] 통신 모듈(204)는 사용자와 전자 기기가 서로 통신하기 위한 기능을 제공할 수 있다. 사용자와 전자 기기가 서로 통신함에 있어서, 통신 방식은 제한되지 않으며, 네트워크가 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, 네트워크는, 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, 네트워크는 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.

[0045] 암복호화 모듈(203)은 전자 기기가 주기적 인증을 수행할 때 사용하는 암호 연산과 해시 연산을 수행하기 위해 사용된다.

[0046] 삭제 모듈(205)은 전자 기기에 내장된 카운터 값이 특정 값에 도달할 때까지 인증을 수행하지 못한 경우, 삭제 연산을 수행하고 삭제 증거를 사용자에게 송신하기 위해 사용된다.

[0047] 추가적으로 전자 기기의 전원이 꺼진(off) 후에도 독립적으로 작동하기 위한 보조 전력 모듈을 포함할 수 있다.

[0048] 도 3은 일 실시예에 따른 원격 데이터 삭제 시스템에서 주기적 인증을 수행하는 것을 설명하기 위한 예이다.

[0049] 도 3에서는 사용자(102)와 전자 기기(101)간 주기적 인증을 수행하는 것을 설명하기로 한다. 이때, 전자 기기(101)는 무인 항공기일 수 있다.

[0050] 원격 데이터 삭제 시스템에서 사용하는 암호화는 전자 기기(101)와 사용자가 암호화된 메시지를 복호화하는데 동일한 키를 사용하며, 주기적 인증을 수행하기 전에, 전자 기기(101)와 사용자(102)는 안전하게 암호화 키(305)를 공유할 수 있으며, 암호화 키는 노출되지 않음을 가정할 수 있다.

[0051] 사용자(102)는 공유한 암호화 키를 사용하여 임의의 숫자 데이터(x)와 인증 가능한 최대 횟수(n)에 기반하여 암호화함에 따라 생성된 메시지(302)를 전자 기기에게 전송할 수 있다($E\{K_{User,Drone}, x \,||\, n \,||\, \text{nonce}\}$)(306). 이때, 임의의 숫자 데이터를 시드값으로 사용할 수 있다.

[0052] 전자 기기(101)는 사용자(102)로부터 전송된 메시지(302)를 공유된 암호화 키를 이용하여 복호화하여 숫자 데이

터 및 인증 가능한 최대 횟수를 확인하고, 확인된 숫자 데이터와 인증 가능한 최대 횟수에 기반한 해시값($h^n(x)$)을 계산할 수 있다. 전자 기기(101)는 인증 가능한 최대 횟수와 계산된 해시값을 저장(303)하고, 계산된 해시값을 사용자에게 전송할 수 있다($E\{K_{User,Drone}, h^n(x) \| n \| nonce\}$)(304). 사용자(102)로부터 전자 기기(101)로부터 전달받은 해시값에 기반하여 임의의 숫자 데이터와 인증 가능한 최대 횟수를 확인하여 전자 기기(101)와 사용자(102)의 상호 인증을 수행하는 초기화 과정(305)을 수행할 수 있다. 이때, 사용자(102)와 동일한 키를 공유한 전자 기기(101)만이 암호화된 메시지를 복호화하여 인증 가능한 최대 횟수와 숫자 데이터를 알아낼 수 있으며, 해시 함수는 단방향 함수이므로 사용자(102)는 전자 기기(101)가 정확한 인증 가능한 최대 횟수와 숫자 데이터를 받았는지 확인하고 상대방이 전자 기기(101)임을 확신할 수 있다.

[0053] 이러한 초기화 과정(305)을 통해 상호 인증한 전자 기기(101)와 사용자(102)는 주기적인 인증을 수행할 수 있다. 전자 기기(101)와 사용자(102)의 상호 인증이 수행됨에 따라 사용자(102)와 전자 기기(101)간 해시 체인에 기반한 인증 메시지를 교환할 수 있다. 예를 들면, 사용자(102)로부터 인증 요청 메시지($E\{K_{User,Drone}, h^{n-i}(x) \| r \| nonce\}$)(306)가 전자 기기(101)에게 전송될 수 있다. 인증 요청 메시지를 수신한 전자 기기(101)가 인증 요청 메시지를 계산하여 결과값을 저장할 수 있다(307). 전자 기기(101)가 인증 요청 메시지를 계산한 결과값과 전자 기기(101)에 저장된 해시값을 비교한 비교 결과에 기초하여 인증 성공 메시지($E\{K_{User,Drone}, n-i \| nonce \| hl \| al\}(\| hv \| av)$)(308)를 사용자(102)에게 전달할 수 있다. 다시 말해서, 전자 기기(101)는 카운트 값의 재설정을 완료한 것과 관련된 인증 성공 메시지를 사용자(102)에게 전달하게 된다.

[0054] 구체적으로, 도 4를 참고하여, 타이머 기반의 원격 데이터 삭제 방법을 설명하기로 한다. 전자 기기는 위치를 이동하면서, 통신을 대기할 수 있다(유휴 상태)(401). 전자 기기는 사용자로부터 인증 요청 메시지를 수신할 수 있다(402). 전자 기기는 사용자로부터 전달된 전자 기기에게 인증 요청 메시지를 계산한 결과값과 전자 기기에 저장된 해시값을 비교하여 인증 성공 여부를 판단할 수 있다(403). 이때, 전자 기기는 인증 요청 메시지를 계산한 결과값과 전자 기기에 저장된 해시값을 비교한 비교 결과가 일치하지 않을 경우, 통신 대기 상태로 되돌아갈 수 있다. 또한, 비교 결과가 일치할 경우, 전자 기기의 카운터 값을 재설정(reset)하고, 해시값을 업데이트할 수 있다(404). 카운트 값을 재설정한 상태에서, 통신이 양호하면 메시지의 교환을 여러 번(인증 가능한 최대 횟수만큼) 반복할 수 있다. 이때, 인증 가능한 최대 횟수를 초과할 경우, 사용자와 전자 기기는 다시 새로운 인증 가능한 최대 횟수와 임의의 숫자 데이터를 교환할 수 있다.

[0055] 전자 기기는 카운트 값을 재설정함에 따라 특정 주기마다 카운트 값을 변화시킬 수 있다(405). 일례로, 전자 기기는 특정 시간까지 사용자의 인증 요청 메시지를 수신하지 못할 경우, 기 설정된 주기마다 카운트 값을 변화시킬 수 있다. 예를 들면, 1초마다 카운트 값이 1씩 감소할 수 있다. 이외에도, 주기적 또는 비주기적으로 카운트 값이 증가 또는 감소할 수 있다. 이때, 전자 기기와 사용자의 주기적 인증이 계속하여 성공적으로 실행될 경우, 전자 기기는 반복적으로 전자 기기에 내장된 카운트 값을 재설정하여 데이터 삭제 연산을 수행하게 되는 카운트 값에 도달하지 않게 된다.

[0056] 전자 기기에서 카운트 값이 변화함에 따라 기 설정된 값(예를 들면, 0)이 되면, 각 데이터 영역에 대하여 삭제 연산을 수행하여 데이터를 원격 삭제할 수 있다(406). 이때, 기 설정된 값은 삭제 연산을 수행하는 되는 카운트 값을 의미할 수 있다. 전자 기기는 원격 삭제된 데이터에 대한 삭제 연산을 증명하여 데이터의 삭제 여부를 검증할 수 있다. 다시 말해서, 전자 기기에서 사용자에게 삭제 증거를 송신할 수 있다(407).

[0057] 도 5는 일 실시예에 따른 원격 데이터 삭제 시스템에서 인증 요청 메시지를 재전송하는 것을 설명하기 위한 예이다.

[0058] 도 5에서는 사용자(102)와 전자 기기(101) 사이에 통신이 끊겼을 경우, 인증 재요청 메시지를 전송하는 것을 설명하기로 한다. 다시 말해서, 도 4에서 메시지 인증에 실패한 경우 인증 재요청 메시지를 전송할 수 있다. 예를 들면, 사용자로부터 전자 기기에 대한 제어권이 상실되는 것과 같이 어떠한 이유로 통신이 끊어질 수 있다.

[0059] 사용자와 전자 기기와의 인증이 i(i는 자연수)번 수행된 상태를 가정하는 환경에서, 사용자(102)가 인증 요청 메시지($E\{K_{User,Drone}, h^{n-i}(x) \| r \| nonce\}$)(502)를 전자 기기(101)에게 전송하였으나, 전자 기기(101)가 인증 요청 메시지를 수신하지 못한 경우, 전자 기기에 저장된 값은 업데이트되지 않으며, 전자 기기에

내장된 카운터 값 역시 리셋되지 않는다(501). 이러한 인증을 수행하지 못한 전자 기기(101)는 사용자(102)에게 인증을 수행했음을 알리는 인증 확인 메시지를 보내지 않는다.

[0060] 사용자(102)로부터 전송된 인증 요청 메시지에 대한 전자 기기의 인증 확인 메시지를 수신하지 못한 사용자는 전자 기기(101)에게 인증을 다시 요청하는 인증 재요청 메시지($E\{K_{User,Drone}, h^{n-i}(x) \| r=1 \| nonce\}$)(503)를 전송할 수 있다. 이때, 인증 재요청 메시지는 이미 메시지를 전송하였으나, 메시지에 대한 응답을 수신하지 못한 인증 요청 메시지(502)에 포함된 동일한 값과 함께 리플레이 공격을 방지하기 위한 넌스값, 재전송임을 알리는 비트(r 비트)가 암호화되어 포함될 수 있다. 사용자로부터 인증 재요청 메시지를 수신한 전자 기기(101)는 r 비트를 확인하고 재전송을 인식하여 전자 기기에 저장된 해시값과 수신된 결과값이 동일한지 확인할 수 있다. 이러한 값이 동일할 경우, 전자 기기는 다음 해시값에 대한 요청을 의미하는 값(n-i)를 다시 사용자에게 전송할 수 있다. 구체적으로, 사용자가 인증 요청 메시지를 보내고 전자 기기가 해당 메시지를 정상적으로 수신하여 해시값을 업데이트하고 카운트 값을 리셋시킨 후, 전자 기기가 응답 메시지를 보냈으나 사용자가 응답 메시지를 수신하지 못한 경우가 존재할 수 있기 때문에 재전송의 경우, 전자 기기는 사용자로부터 전달받은 값에 대한 해시 계산을 하지 않았음에도 불구하고 전자 기기에 저장되어 있는 값과 일치할 경우, 응답 메시지만을 전송할 수 있다. 이때, 해시값 및 카운트 값의 업데이트는 없다. 만약, 수신한 결과값의 해시 계산 결과값이 전자 기기에 저장된 값과 일치할 경우, 저장된 해시값과 카운트 값을 업데이트한다. 다시 말해서, 재전송의 상황에서는 저장된 해시값과 수신된 값이 동일할 경우, 카운트가 리셋되지 않는다. 사용자와 전자 기기는 다시 정상적인 통신을 시작할 수 있다.

[0061] 또한, 인증 재요청 메시지를 전송하는 횟수가 설정될 수 있다. 인증 재요청 메시지를 전송하는 횟수는 시스템을 사용하는 목적과 요구하는 보안강도에 따라 제한없이 설정의 변경이 가능하다. 예를 들면, 사용자(102)가 한 번 또는 복수 번 전송한 인증 재요청 메시지를 전자 기기(101)가 수신하지 못한 경우, 전자 기기(101)는 전자 기기(101)에 저장된 데이터에 대해 복구가 불가능하고 사용자(102)가 삭제되었음을 식별할 수 있는 삭제 연산을 수행할 수 있다. 전자 기기(101)로부터 삭제 연산이 수행되었음을 알리는 삭제 증거 송신 메시지($h(m) \| hl \| al$)(504)를 사용자(102)에게 특정 주파수를 사용하여 전송할 수 있다. 이때, 전자 기기(101)는 삭제 연산에 대한 삭제 증거 송신 메시지(504)를 전송한 이후에도, 다시 삭제 연산에 대한 검증을 수행함으로써 삭제 증거 송신 메시지(504)를 계속적으로 사용자(102)에게 전달할 수 있다.

[0062] 도 6을 참고하면, 사용자의 원격 데이터 삭제 방법을 설명하기 위한 흐름도이다. 사용자와 전자 기기 사이에서 진행되는 삭제 프로토콜을 사용자 관점에서 설명하기로 한다. 사용자는 통신을 대기할 수 있다(유휴 상태)(601). 사용자는 $\frac{\delta}{2(1+\gamma)}sec$ 마다 전자 기기에게 메시지를 송신할 수 있다(602). 이때, δ는 카운트 최대값(카운트가 δ에 도달하면 삭제 시작), γ는 인증 재요청 횟수를 의미한다. 사용자는 메시지를 전자 기기에게 전달함에 따라 전자 기기로부터 메시지를 수신할 수 있다(603). 이때, 전자 기기로부터 수신된 메시지에 기초하여 인증 성공 여부를 판단할 수 있다(605). 예를 들면, 사용자는 전자 기기로부터 수신된 메시지가 인증 성공 메시지일 경우, 해시값을 업데이트할 수 있고(606), 통신을 대기할 수 있다(601). 또한, 사용자로부터 $\frac{\delta}{2(1+\gamma)}sec$ 마다 전자 기기에게 메시지를 전송하였음에도 $\frac{\delta}{2(1+\gamma)}sec$ 동안 전자 기기로부터 메시지를 미수신할 경우, 인증 재요청 메시지를 전송할 수 있다(604). 전자 기기가 인증 재요청 메시지를 수신할 경우, 인증 재요청 메시지에 대한 응답으로 메시지를 수신할 수 있다(603). 마찬가지로, 메시지에 기초하여 인증 성공 여부를 판단할 수 있다(605).

[0063] 도 7은 일 실시예에 따른 원격 데이터 삭제 시스템의 데이터 구조를 설명하기 위한 도면이다. 데이터 영역은 콜드 데이터(701), 축적 데이터(702) 및 핫 데이터(703)를 포함하는 영역으로 구성될 수 있다. 이때, 사용자는 각각의 데이터 영역의 주소를 확실히 하고 있다고 가정하기로 한다. 콜드 데이터(701)는 전자 기기가 사용자의 제어권에 의하여 조작될 때 저장되고 원격에 존재할 때 변하지 않는 데이터를 의미할 수 있으며, 예를 들면, 펌웨어 같은 것이 해당될 수 있다. 이러한 콜드 데이터(701)는 고정된 값으로서, 사용자의 제어권에서 벗어난 경우에는 이륙부터 착륙까지 값이 변하지 않는다. 원격 데이터 삭제 시스템에서는 콜드 데이터의 값과 메모리 상의 위치를 사용자가 정확히 알고 있음을 가정한다. 이는 전자 기기가 전송하는 삭제 증거에 대한 증명력을 보

장하기 때문에 콜드 데이터는 단 한번의 수정도 있어서는 안되기 때문에 수정과 쓰기 권한을 제거하여 읽기만 가능하도록 구현될 수 있다.

[0064] 축적 데이터(702)는 정보 수집용 데이터로서, 촬영을 수행하여 생성되는 데이터를 의미한다. 축적 데이터(702)는 원격에서 데이터가 생성된 후에 수정되는 않는다. 축적 데이터의 특징상 한 번 기록된 이후, 보통 삭제되지 않기 때문에 원격 데이터 삭제 시스템에서는 축적 데이터를 새로운 종류의 콜드 데이터로써 분리하였다. 축적 데이터가 생성될 경우, 전자 기기는 사용자에게 인증 확인 메시지를 보내는 순간, 수정된 축적 데이터의 메모리 위치 값을 함께 전송한다. 또한, 삭제 증거의 증명력을 높이기 위해 임의의 시간에 축적 데이터 중 임의의 블록을 선택하여 해당 블록의 메모리 위치 값과 메모리의 값을 전송한다.

[0065] 핫 데이터(703)는 전자 기기 내에서 계속하여 수정될 가능성이 높은 데이터를 업데이트할 수 있다. 시스템의 콜드 데이터(601)와 축적 데이터(602)를 제외한 데이터로도 정의할 수 있다. 핫 데이터의 경우 계속하여 변하기 때문에 전자 기기 내의 메모리에 저장된 데이터를 통해 삭제 증거를 계산하는 사용자는 핫 데이터의 수정 연산에 대해 알고 있어야 한다. 핫 데이터가 수정될 경우, 전자 기기는 사용자에게 인증 확인 메시지를 보내는 순간, 수정된 핫 데이터의 메모리 위치와 핫 데이터의 값을 같이 전송한다.

[0066] 도 8 내지 도 11은 일 실시예에 따른 원격 데이터 삭제 시스템의 삭제 연산을 설명하기 위한 도면이다.

[0067] 원격 데이터 삭제 시스템은 전자 기기의 카운트 값이 변화함에 따라 카운트 값이 기 설정된 값이 되면, 각 데이터 영역에 대하여 XOR 연산을 진행하여 삭제 연산을 수행할 수 있다. 예를 들면, 사용자로부터 해시값을 수신하지 못하는 경우, 전자 기기에 내장된 카운터를 리셋할 수 없는 경우, 카운터는 지정된 시간에 도달하게 되고, 전자 기기에 저장된 데이터를 삭제하기 시작한다.

[0068] 도 8을 참고하면, 콜드 데이터의 삭제 연산을 수행하는 것을 설명하기 위한 예이다. 전자 기기가 특정 시간 내에 인증 과정을 수행하지 못한 경우, 콜드 데이터의 삭제 연산을 수행할 수 있다. 전자 기기 내에서 삭제 연산이 수행되는 경우, 전자 기기는 첫 번째로 콜드 데이터에 대한 삭제 연산을 진행할 수 있다. 콜드 데이터는 사용자가 데이터의 메모리 상의 위치와 값을 알고 있으므로 선행 작업이 필요 없이 삭제 연산을 바로 진행할 수 있다. 예를 들면, 전자 기기는 콜드 데이터의 특정 블록의 메모리와 사용자로부터 수신된 마지막 해시값의 XOR 연산을 수행하여 계산된 값으로 콜드 데이터의 특정 블록을 삭제할 수 있다. 삭제 연산은 콜드 데이터의 첫 번째 블록을 전자 기기가 사용자로부터 전달받은 마지막 해시값으로 덮어쓴 후(801), 첫 번째 블록과 두 번째 블록의 XOR 연산을 시작할 수 있다. 콜드 데이터의 첫 번째 블록과 두 번째 블록의 XOR 연산을 수행한 연산값을 두 번째 블록에 덮어쓴 후, 콜드 데이터의 두 번째 블록과 세 번째 블록의 XOR 연산을 진행할 수 있다. 콜드 데이터의 두 번째 블록과 세 번째 블록의 XOR 연산의 연산값 역시 콜드 데이터의 세 번째 블록에 저장할 수 있다. 이러한 과정을 콜드 데이터의 마지막 블록까지 계속하여 수행한다.

[0069] 두 번째 콜드 데이터부터의 삭제 연산은 다음과 같은 수학식 1로 나타낼 수 있다.

[0070] 수학식 1:

[0071] $$C_n` = C_n \oplus C_{n-1}`$$

[0072] 도 9를 참고하면, 축적 데이터의 삭제 연산을 수행하는 것을 설명하기 위한 예이다. 전자 기기가 특정 시간 내에 인증 과정을 수행하지 못한 경우, 축적 데이터의 삭제 연산을 수행할 수 있다. 전자 기기는 축적 데이터 중 임의의 위치에 대한 축적 데이터 값을 통하여 삭제 연산을 수행할 수 있다. 예를 들면, 시스템의 축적 데이터에 대한 삭제 연산은 전자 기기와 사용자간의 인증이 끊어진 후, 변경된 축적 데이터의 위치를 메인 메모리 상에 저장한 후, 임의로 선택된 데이터 블록(902)을 제외한 축적 데이터에 대해 콜드 데이터의 최종 연산 결과값으로 덮어쓸 수 있다(901). 이러한 선행 작업 이후, 도 9에 도시된 바와 같이, 축적 데이터의 블록과 임의로 선택된 축적 데이터의 블록의 해시값과 XOR 연산을 수행하고, 연산을 수행한 연산값을 해당하는 축적 데이터의 블록에 덮어씌울 수 있다.

[0073] 임의로 선택된 데이터 블록의 삭제 연산은 수학식 2와 같이 나타낼 수 있다. 그 이외의 축적 데이터 블록들은 수학식 1과 동일한 방식으로 계산될 수 있다.

[0074] 수학식 2:

[0075] $$A_n` = h(A_n) \oplus A_{n-1}`$$

[0076] 이때, 축적 데이터의 경우, Y_n-Y_{n-1}에 비례하여 임의의 블록 개수의 일부 비율(α 퍼센트)를 선정할 수 있다. 또한, Y_n 시간에 임의의 블록을 선정한다면 Y_{n-1} 시간부터 현재 Y_n 사이에 생성된 임의 블록 개수의 α 퍼센트를 선정할 수 있다. 여기서, Y_n는 임의의 시간을 나타낸다.

[0077] 도 10을 참고하면, 핫 데이터의 삭제 연산을 수행하는 것을 설명하기 위한 예이다. 예를 들면, 전자 기기는 핫 데이터 중 특정 핫 데이터 값(임의의 핫데이터 값)을 기준으로 특정 핫 데이터의 이전 핫 데이터 값을 사용하여 삭제 연산을 수행할 수 있다. 또는, 전자 기기는 핫 데이터 중 임의의 위치에 대한 핫 데이터 값을 통하여 삭제 연산을 수행할 수도 있다. 핫 데이터에 대한 삭제 연산은 전자 기기와 사용자간의 인증이 끊어진 후에 변경된 핫 데이터의 위치를 메인 메모리 상에 저장한 후, 해당 데이터의 위치를 콜드 데이터 삭제 연산 최종값으로 덮어쓸 수 있다(1001). 이러한 선행 작업 이후 핫 데이터에 대한 삭제 연산을 축적 데이터 삭제 연산과 같은 방식으로 진행할 수 있다. 다시 말해서, 핫 데이터의 블록과 임의로 선택된 핫 데이터의 블록의 해시값과 XOR 연산을 수행하고, 연산을 수행한 연산값을 해당하는 핫 데이터의 블록에 덮어씌울 수 있다.

[0078] 임의로 선택된 핫 데이터 블록의 삭제 연산은 수학식 3과 같이 나타낼 수 있다. 그 외의 핫 데이터 블록들은 수학식 1과 동일한 방식으로 계산될 수 있다.

[0079] 수학식 3:

[0080] $$H_n` = h(H_n) \oplus H_{n-1}`$$

[0081] 핫 데이터의 경우, 핫 데이터에 할당된 메모리 영역에 비례하여 β 개의 임의의 블록을 선정할 수 있다.

[0082] 도 11을 참고하면, 각각의 데이터의 삭제 연산을 반복하여 수행할 수 있다. 마지막 블록이 새로운 값으로 덮어씌워질 때까지를 하나의 라운드로 정의할 수 있다. 원격 데이터 삭제 시스템은 복구 불가능한 데이터 삭제를 목표로 하기 때문에 마지막 블록과 첫 번째 블록의 XOR 연산 값을 첫 번째 블록에 덮어쓰는 것을 시작으로 두 번째 라운드를 시작할 수 있다. 복수 번의 라운드를 진행하여 전자 기기의 메모리를 획득하였더라도 데이터를 복구할 수 없도록 한다. 두 번째 라운드부터는 원격 데이터 삭제 시스템에서 분류한 데이터 종류와 관계없이 삭제 연산을 수행할 수 있다. 복수 번의 라운드를 진행하여 하나의 라운드가 종료될 때마다 메모리의 마지막 블록의 해시값을 사용자에게 삭제 증거로써 전달할 수 있다. 예외적으로 첫번째 라운드는 축적 데이터의 마지막 블록값과 핫 데이터의 마지막 블록값을 XOR한 후, 해시 연산값을 삭제 증거로써 전송한다.

[0083] 데이터 삭제 연산은 전자 기기에 저장된 데이터에 대해 종속성을 가지므로, 전자 기기가 수중에 없는 사용자는 삭제가 성공적으로 수행되었다는 증거를 생성할 수 없다.

[0084] 도 12는 일 실시예에 따른 원격 데이터 삭제 시스템에서 삭제 연산에 대한 증거를 송신하는 것을 설명하기 위한 예이다.

[0085] 사용자(102)는 특정 주파수를 수신할 수 있는 안테나(1201)를 소유하고 있다고 가정할 수 있다. 특정 주파수를 통하여 연산 최종 결과값(H_n''또는, H_n'''또는 H_n''''...등)이 생성될 때마다 삭제 증거를 사용자에게 송신할 수 있다. 이때, 첫번째 송신 메시지에는 삭제 연산의 증거와 함께 인증이 끊긴 이후에 변화한 메모리에 대한 정보를 포함할 수 있다. 첫번째 송신 메시지 이외에는 변화한 메모리 정보를 포함할 필요가 없다. 삭제 연산의 증거는 64바이트의 크기를 가지며, 인증이 끊긴 이후 변화한 데이터의 주소값에 대한 정보가 추가적으로 전송되어야 한다. 예를 들면, 삭제 연산의 증거는 FSK라는 이진 저주파수를 통해 전달되며, 원격 데이터 삭제 시스템에서 사용자는 이진 저주파수를 수신할 수 있는 안테나(1201)를 소지하고 있음을 가정으로 한다.

[0086] 사용자는 다음과 같이 계산하여 계산 결과와 수신한 삭제 연산의 증거(1202)를 비교하여 전자 기기의 삭제가 진행되었는지 확인할 수 있다. 사용자는 콜드 데이터의 메모리 위치와 값, 축적 데이터의 메모리 위치(aln), 임의로 선택한 축적 데이터의 값과 임의로 선택된 데이터 블록(802)의 위치, 핫 데이터의 메모리 위치와 값(hln),

마지막으로 전송한 해시값(801), 인증이 끊긴 이후 변화한 데이터의 주소값을 알고 있다.

C_n	콜드 데이터 영역에서 n번째 메모리 블록에 위치하는 메모리 값
A_{aln}	수신한 축적 데이터의 위치(al)를 오름차순으로 정렬했을 때 n번째 주소값에 존재할 메모리 값
H_{hln}	수신한 핫 데이터의 위치(hl)를 오름차순으로 정렬했을 때 n번째 주소값에 존재할 메모리 값
$N`$	삭제 연산을 통해 변환된 N값
$h(x)$	x에 대해 해시 연산한 값

[0087]

$$C_n' = h_{n-1}(x) \oplus C_1 \oplus C_2 \oplus C_3 \oplus \dots \oplus C_n$$

$$A_{aln}' = C_n' \oplus A_{al1} \oplus A_{al2} \oplus A_{al3} \oplus h(A_{al4}) \oplus \dots \oplus A_{aln}$$

$$H_{hln}' = C_n' \oplus H_{hl1} \oplus h(H_{hl2}) \oplus H_{hl3} \oplus \dots \oplus H_{hln}$$

$$Proof1 = h(A_{aln}' \oplus H_{hln}')$$

$$Proof'' = h(H'') = h(Proof1 \oplus C_1' \oplus C_2' \oplus C_3' \oplus \dots \oplus C_n' \oplus A_{al1}' \oplus A_{al2}' \oplus A_{al3}' \oplus \dots \oplus A_{aln}' \oplus H_{hl1}' \oplus H_{hl2}' \oplus H_{hl3}' \oplus \dots \oplus H_{hln}')$$

...

$$\boldsymbol{Proof''''} = h(H'''') = h(Proof'''' \oplus C_1'''' \oplus C_2'''' \oplus C_3'''' \oplus \dots \oplus C_n'''' \oplus A_{al1}'''' \oplus A_{al2}'''' \oplus A_{al3}'''' \oplus \dots \oplus A_{aln}'''' \oplus H_{hl1}'''' \oplus H_{hl2}'''' \oplus H_{hl3}'''' \oplus \dots \oplus H_{hln}'''')$$

[0088]

[0089] 일 실시예에 따른 원격 데이터 삭제 시스템은 무인 항공기가 촬영을 수행하여 생성되는 데이터를 축적 데이터라는 새로운 종류의 데이터로 분류하고, 원격에서 데이터가 생성된 후에 수정되지 않는다는 축적 데이터의 특징을 삭제 방법에 이용한다. 또한, 원격에 존재하는 무인 항공기와 사용자간의 통신이 끊어진 경우에도 카운터 기반을 통해 무인 항공기에 저장된 데이터를 삭제하고 각 데이터에 종속적인 삭제 연산 증거를 사용자에게 전송한다. 또한, 통신이 끊긴 이후에 삭제 검증의 완성도를 높이기 위해 삭제 연산을 반복적으로 수행하는 Best effort 방식을 사용한다. 또한, 상황에 맞게 변수(핫 데이터의 메모리 용량 등)가 조정되더라도 보안성이 일반화된다.

[0090] 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.

[0091] 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 장치에 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.

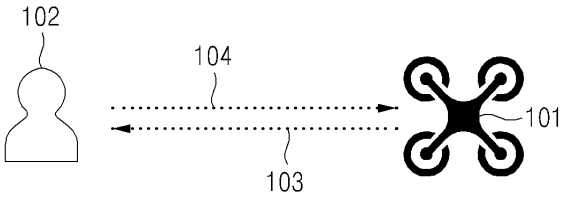
[0092] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic 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.

[0093] 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.

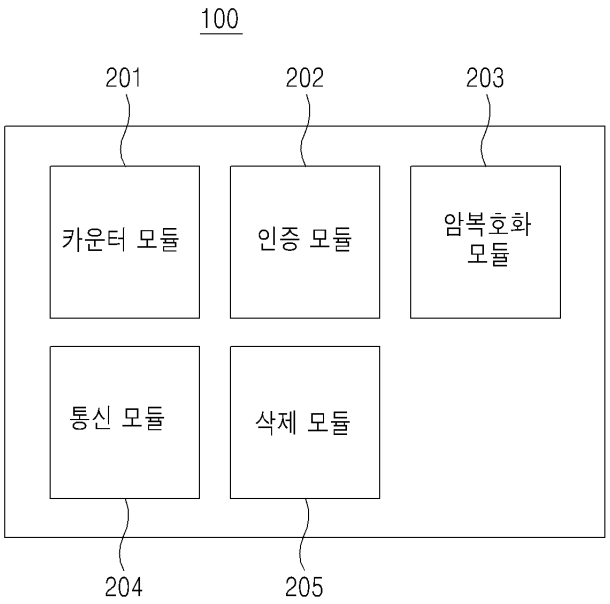
[0094] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

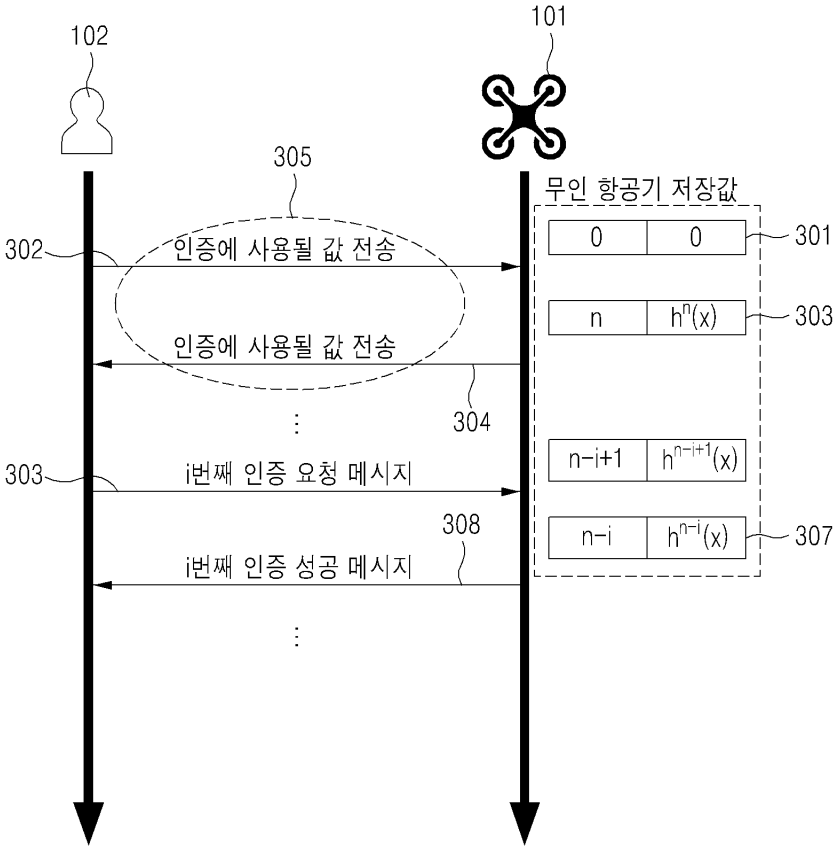
도면1



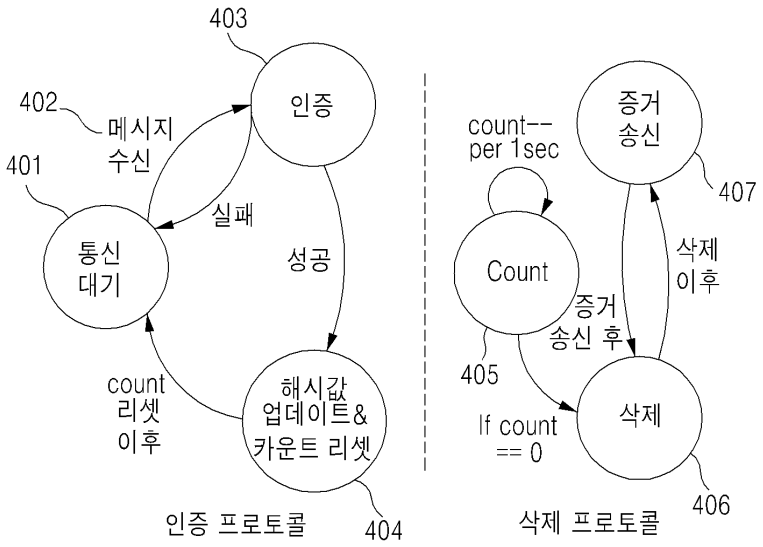
도면2


100
201
202
203
카운터 모듈
인증 모듈
암복호화 모듈
통신 모듈
삭제 모듈
204
205

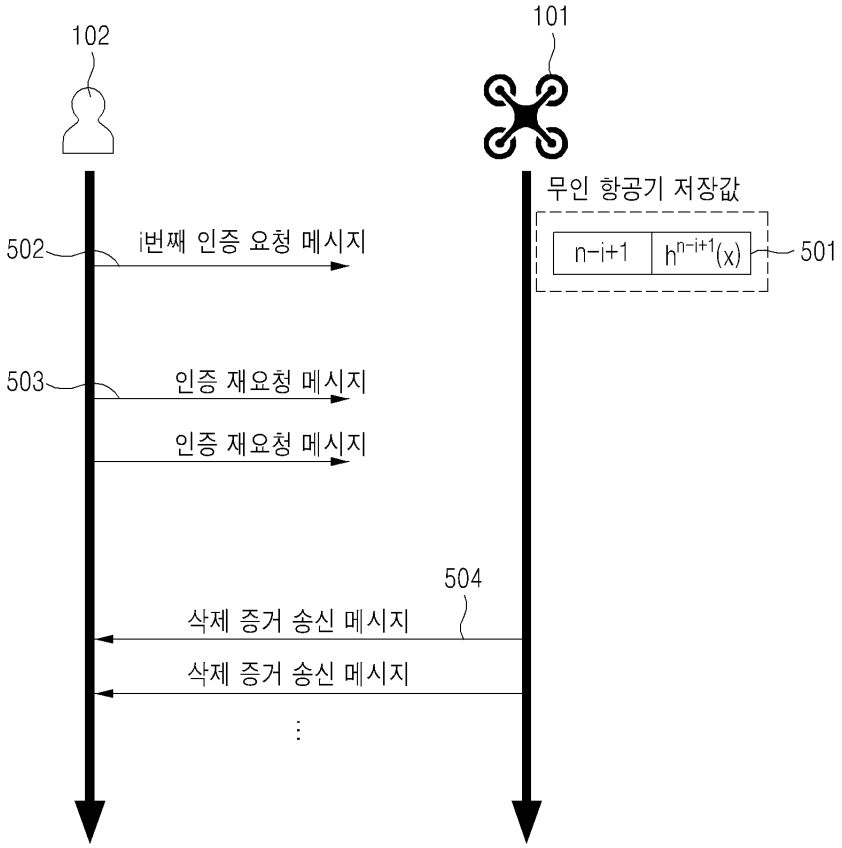
도면3


102
101
305
무인 항공기 저장값
302
인증에 사용될 값 전송
인증에 사용될 값 전송
0
0
301
n
$h^n(x)$
303
304
n-i+1
$h^{n-i+1}(x)$
303
i번째 인증 요청 메시지
308
n-i
$h^{n-i}(x)$
307
i번째 인증 성공 메시지

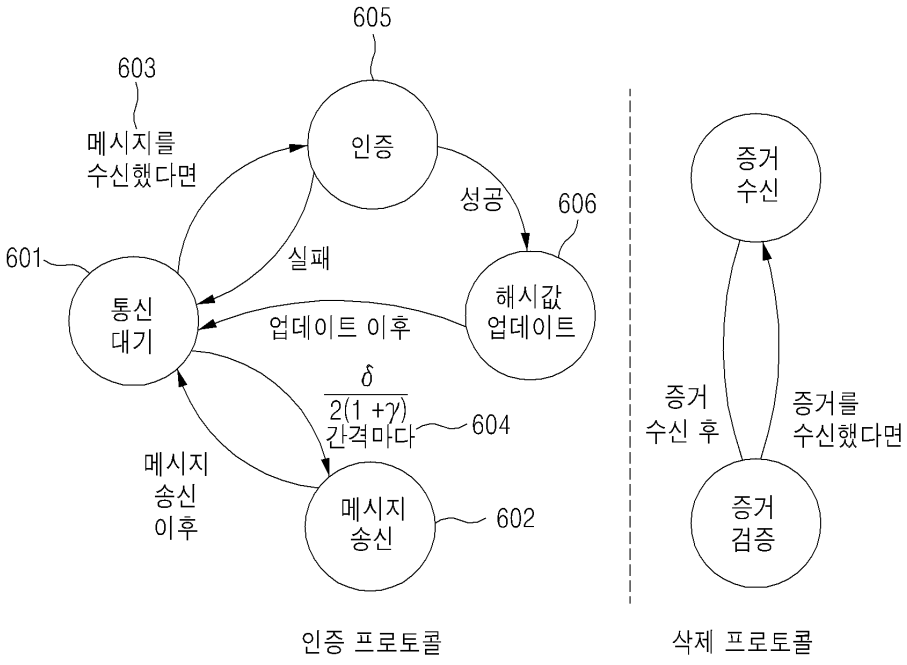
도면4


403
인증
402
메시지
수신
401
실패
통신
대기
성공
count
리셋
이후
해시값
업데이트&
카운트 리셋
404
인증 프로토콜
count--
per 1sec
증거
송신
407
Count
삭제
이후
증거
송신 후
405
If count
== 0
삭제
406
삭제 프로토콜

도면5


102
101
무인 항공기 저장값
n-i+1
$h^{n-i+1}(x)$
501
502
i번째 인증 요청 메시지
503
인증 재요청 메시지
인증 재요청 메시지
504
삭제 증거 송신 메시지
삭제 증거 송신 메시지
⋮

도면6



인증 프로토콜 삭제 프로토콜

도면7

도면8

C_1	C_2	C_3	C_4	C_5
…	…	…	…	…
…	…	…	…	…
…	…	…	C_{n-1}	C_n

$C_1` = C_1 \oplus h^{n-i}(x)$ ~ 801

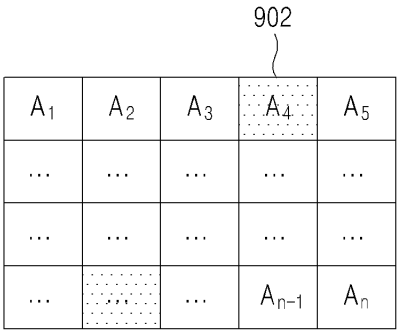
$C_2` = C_2 \oplus C_1`$

$C_3` = C_3 \oplus C_2`$

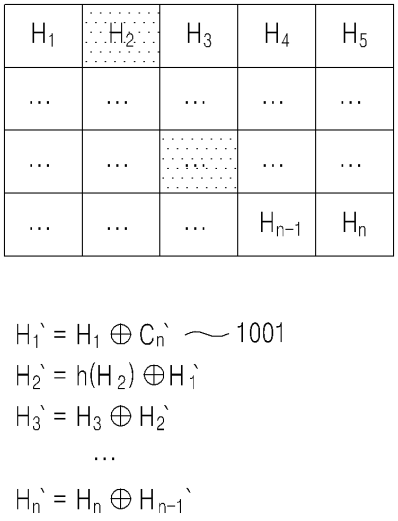
…

$C_n` = C_n \oplus C_{n-1}`$

도면9


902
A1 A2 A3 A4 A5
An-1 An
A1` = A1 ⊕ Cn` 901
A2` = A2 ⊕ A1`
A3` = A3 ⊕ A2`
A4` = h(A4) ⊕ A3`
An` = An ⊕ An-1`

도면10


H1 H2 H3 H4 H5
Hn-1 Hn
H1` = H1 ⊕ Cn` 1001
H2` = h(H2) ⊕ H1`
H3` = H3 ⊕ H2`
Hn` = Hn ⊕ Hn-1`

도면11

$C_1'' = C_1' \oplus H_n'$

$C_2'' = C_2' \oplus C_1'$

...

$C_n'' = C_n' \oplus C_{n-1}''$

$A_1'' = A_1' \oplus C_n''$

$A_2'' = A_2' \oplus A_1''$

...

$H_n'' = H_n' \oplus H_{n-1}''$

C_1'	...	...	...
C_2'	...	...	...
C_3'	...	...	...
C_4'	...	...	C_{n-1}'
C_5'	...	...	C_n'

A_1'	...	...	...
A_2'	...	...	...
A_3'	...	...	...
C_4'	...	...	A_{n-1}'
A_5'	...	...	A_n'

H_1'	...	...	...
H_2'	...	...	...
H_3'	...	...	...
H_4'	...	...	H_{n-1}'
H_5'	...	...	H_n'

도면12