(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0016186
(43) 공개일자 2011년02월17일

(51) Int. Cl.
H04L 9/32 (2006.01) *H04L 9/28* (2006.01)
G06F 21/20 (2006.01) *H04W 12/06* (2009.01)
(21) 출원번호 10-2009-0073770
(22) 출원일자 2009년08월11일
심사청구일자 2009년08월11일

(71) 출원인
이화여자대학교 산학협력단
서울 서대문구 대현동 11-1 이화여자대학교내
(72) 발명자
조동섭
서울 송파구 문정동 패밀리아파트 223동 506호
서대희
서울 영등포구 도림동 대우 미래사랑 아파트 101-909
(뒷면에 계속)
(74) 대리인
특허법인우인

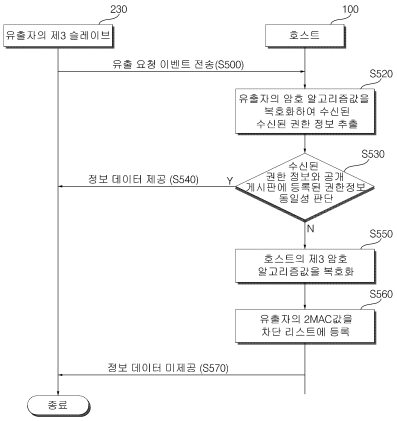
전체 청구항 수 : 총 5 항

(54) 정보 데이터의 권한 변경을 방지하는 방법

(57) 요 약

정보 데이터의 권한 변경을 방지하는 방법이 개시된다. 본 정보 데이터의 권한 변경을 방지하는 방법은, 상기 정보 데이터를 제공받고자 하는 사용자와 사용자 등록 및 상호 인증 과정을 수행하는 단계; 상기 사용자로부터 상기 정보 데이터의 변경된 권한 정보가 암호화된 암호 알고리즘값을 포함하는 이벤트를 수신하는 단계; 상기 이벤트에서 상기 암호 알고리즘값을 복호화하여 상기 정보 데이터의 변경된 권한 정보를 추출하는 단계; 및 상기 추출된 권한 정보가 기등록된 상기 정보 데이터의 권한 정보와 동일하지 않는 경우, 상기 이벤트를 전송한 사용자를 공격자 차단 리스트에 등록하는 단계;를 포함한다. 그리하여 각각의 데이터에 대한 권한 관리 뿐만 아니라 사용자에 대한 명시적 인증을 통해 사용자와 데이터의 안전한 관리가 가능하게 하고, 불법적으로 정보 데이터의 권한을 변경하여 정보 데이터를 외부로 유출하고자 할 때에는 불법 사용자와 사용 디바이스에 대한 추적함으로써 네트워크 및 응용 서비스 발전에 기여하는데 큰 효과가 있다.

대 표 도 - 도5



(72) 발명자

백장미

서울 영등포구 도림동 대우 미래사랑아파트 101-909

박수빈

서울특별시 서초구 방배동 461-1 덕산럭스빌 201호

이 발명을 지원한 국가연구개발사업

과제고유번호 핵C6A1907

부처명 교육과학기술부

연구관리전문기관

연구사업명 2단계 두뇌한국(BK)21 사업

연구과제명 U-Commerce 소프트웨어 여성전문인력양성사업

기여율

주관기관 이화여자대학교 산학협력단

연구기간 2006년 3월 1일 ~ 2013년 2월 28일

특허청구의 범위

청구항 1

정보 데이터의 권한 변경을 방지하는 방법에 있어서,

해쉬 알고리즘을 이용하여 상기 정보 데이터를 제공받고자 하는 사용자와 사용자 등록 및 상호 인증 과정을 수행하는 단계;

상기 사용자로부터 상기 정보 데이터의 변경된 권한 정보가 암호화된 암호 알고리즘값을 포함하는 이벤트를 수신하는 단계;

상기 이벤트에서 상기 암호 알고리즘값을 복호화하여 상기 정보 데이터의 변경된 권한 정보를 추출하는 단계; 및

상기 추출된 권한 정보가 기등록된 상기 정보 데이터의 권한 정보와 동일하지 않는 경우, 상기 이벤트를 전송한 사용자를 공격자 차단 리스트에 등록하는 단계;를 포함하는 것을 특징으로 하는 정보 데이터의 권한 변경을 방지하는 방법.

청구항 2

제 1항에 있어서,

상기 사용자 등록 및 상호 인증 과정을 수행하는 단계는,

상기 사용자로부터 상기 정보 데이터를 제공받고자 하는 정보 요청 이벤트를 수신하는 단계;

호스트의 제2 공개키 서명 알고리즘값(S_{H_2}) 및 호스트의 제3 암호 알고리즘값(V_{H_3})을 생성하여 사용자에게 전송하는 단계;

상기 사용자로부터 사용자의 제2 해쉬 알고리즘값(h_{u_2}) 및 사용자의 제2 암호 알고리즘값(V_{u_2})을 수신받는 단계;

상기 사용자의 제2 암호 알고리즘값(V_{u_2})을 복호화한 뒤 사용자 등록값($f_u(x)$)과 씨드의 타임스탬프(t_{seed})를 획득하고 초기 공유한 씨드를 이용해 데이터 배포에 따른 사용자 등록값($f_u(x)$)을 사용자 정보와 일대일 매칭하여 저장하는 단계;

호스트는 사용자의 2MAC 값 및 호스트의 제3 암호 알고리즘값(V_{H_3})을 산출하는 단계; 및

상기 호스트의 제3 암호 알고리즘값(V_{H_3})을 사용자의 아이디(ID_u), 제공되는 정보 데이터와 일대일 매칭시키는 단계;를 포함하는 것을 특징으로 하는 정보 데이터의 권한 변경을 방지하는 방법.

청구항 3

제 2항에 있어서,

상기 호스트의 제2 공개키 서명 알고리즘값(S_{H_2}) 및 상기 호스트의 제3 암호 알고리즘값(V_{H_3})값은 하기 수학식과 동일한 것을 특징으로 하는 정보 데이터의 권한 변경을 방지하는 방법.

$$e_H = < ID_H, Authorization-information, Contents-list >$$

$$S_{H_2} = Sig(e_H || Contents-list)$$

$$V_{H_3} = E_{sk_{H-u}}(e_H, t_{seed})$$

여기서, 호스트의 이벤트(e_H)는 호스트의 아이디(ID_H), 정보 데이터의 권한 정보($Authorization-information$) 및 정보 데이터의 리스트($Contents-list$)를 포함하며, 호스트의 제2 공개키 서명 알고리즘값(S_{H_2})은 호스트의 이벤트(e_H) 및 정보 데이터의 리스트($Contents-list$)를 인자로 한 공개키 서명 알고리즘화한 값이고, 호스트의 제3 암호 알고리즘값(V_{H_3})은 호스트의 이벤트(e_H) 및 씨드의 타임 스탬프(t_{seed})를 세션키(sk_{H-u})로 암호 알고리즘화한 값이다.

청구항 4

제 2항에 있어서

상기 사용자의 제3 해쉬 알고리즘값(h_{u_2}) 및 상기 사용자의 제2 암호 알고리즘값(V_{u_2})은 하기 수학식과 동일한 것을 특징으로 하는 정보 데이터의 권한 변경을 방지하는 방법.

$$f_u(x) = \frac{1 - 2^{s * seed}}{1 - 2^{s}}$$

$$h_{u_2} = H(Media\ Access\ Control_u || t_{seed})$$

$$V_{u_2} = E_{sk_{H-u}}(f_u(x), t_{seed})$$

여기서, 사용자의 제2 해쉬 알고리즘값(h_{u_2})은 사용자 NIC(Network Interface Card)의 하드웨어 고유 주소값($Media\ Access\ Control_u$) 및 씨드의 타임스탬프(t_{seed})를 해쉬 알고리즘화한 값이고, 사용자의 제2 암호 알고리즘값(V_{u_2})는 사용자 등록값($f_u(x)$)과 씨드의 타임스탬프(t_{seed})를 세션키(sk_{H-u})로 암호 알고리즘화한 값이다. 그리고, 사용자 등록값($f_u(x)$)의 s는 0이 아닌 실수이고, x 는 변수이다.

청구항 5

제 2항에 있어서,

상기 사용자의 2MAC값 및 상기 호스트의 제3 암호 알고리즘값(V_{H_3})은 하기 수학식과 동일한 것을 특징으로 하는 정보 데이터 권한 변경을 방지하는 방법.

$$2MAC = H(Media\ Access\ Control_u \| t_{seed}) \oplus H(ID_u \| IP_u \| seed)$$

$$V_{H_3} = E_{p_H}(2MAC | Media\ Access\ Control_u \| ID_u \| IP_u \| t_{seed})$$

여기서, 사용자의 2MAC값은 사용자 NIC(Network Interface Card)의 하드웨어 고유 주소값($Media\ Access\ Control_u$) 및 씨드의 타임스탬프(t_{seed})를 해쉬 알고리즘화한 값과, 사용자의 아이디(ID_u), 사용자의 아이피(IP_u) 및 씨드($seed$)를 해쉬 알고리즘화한 값의 논리합이다. 그리고, 사용자의 제2암호 알고리즘값은 2MAC값, 사용자 NIC(Network Interface Card)의 하드웨어 고유 주소값($Media\ Access\ Control_u$), 사용자의 아이디(ID_u), 사용자의 아이피(IP_u) 및 씨드의 타임스탬프(t_{seed})를 호스트의 공개키로 암호 알고리즘화한 값이다.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 정보 데이터 관리 방법 및 시스템에 관한 에 관한 것으로, 특히 정보 데이터의 권한 변경을 방지하는 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 지식 관리 시스템에서 불법적인 내부 사용자에 의한 정보의 외부 유출을 방지하기 위한 방식으로, 종래 기술은 크게 2가지로 요약할 수 있다.

[0003] 첫번째로 DLP (Data Loss Prevention)방식은 내부 인터넷 환경에서 데이터를 형식이나 내용 등을 기준으로 중요 정보에 대한 외부 불법 유출을 방지하는 방식이다. 제안된 방식은 에이전트 기반의 멀티캐스트 방식으로 사용자를 그룹화하고 이를 통해 효율적인 관리가 가능한 계층적인 구조를 갖는다. 특히, 사용자의 이동성을 고려하여 핸드오프가 가능하게 하였으며, 멀티캐스트 사용자의 안전한 인증을 통해 전체적인 네트워크의 안전성과 효율성을 갖도록 하였다.

[0004] 그러나 본 방식의 경우 멀티캐스트 사용자를 위한 데이터의 권한 설정이 이루어지지 않고 각각의 에이전트를 통해 상호 운용성만을 제공하여, 내부 유출 방지가 요구되는 데이터에 대한 별도의 보안 서비스를 제공하지 못하고 있다. 또한 사용자에 대한 인증과 인가에 대한 서비스를 제공한다. 특히, 멀티캐스트 사용자의 인증을 위하여 사용되는 에이전트에 대한 별도의 보안 서비스를 제공하지 못하고 있다.

[0005] 따라서 사용자의 인증을 기반으로 데이터를 접근할 수 있는 사용자들을 위한 멀티캐스트 방식을 제시하였다. 그러나 이는 유동적으로 변화할 수 있는 사용자들에 대해서 적용성의 한계성을 갖고 있으며, 이로 인해 사용자들의 현실적인 데이터 접근을 어렵게 한다. 또한 데이터가 외부 유출하고자 할 경우 이를 차단할 수 있는 서비스를 제공하지 못한다.

[0006] 두 번째로 제시된 방식은 통합 보안 관리 시스템을 기반으로 데이터의 모니터링을 통해 내부 데이터에 대한 불법적인 외부 유출을 방지하기 위한 방식이다.

[0007] 제안된 방식은 ESM(Enterprise Security Management)를 기반으로 기업 환경에서 문서 시스템의 보안, 사용자 관리 등의 방식을 제공한다. 그러나 본 방식의 경우 개인 PC를 중심으로 접근하여 전체적인 네트워크 관리 측면에서 원천적인 정보 유출 방안에 이르지 못하고 있으며 효율성 측면과 정책적인 측면에서 적용의 한계성이 지적되고 있다. 특히, 사용자의 개인 디바이스를 중심으로 데이터에 대한 안전성을 확보하고 이를 통해 내부 데이터의 외부 유출을 방지하고자 하였다. 그러나 사용자의 인증이 아닌 응용 프로그램의 제어를 통해 데이터 유출을 방지한다. 따라서 사용자의 개인 정보에 기반한 인증 뿐만 아니라 통신의 안전성 확보를 위한 추가적인 서비스

를 제공해야 한다. 또한 구조적인 신뢰성을 확보하기 위하여 통합 보안 관리 시스템을 기반으로 사용자 및 데이터의 외부 유출을 방지하고자 하였다.

[0008] 그러나 내부적으로 많은 데이터가 사용되는 환경의 경우 모든 데이터에 대한 모니터링이 현실적으로 불가능하고 응용 프로그램의 모니터링을 통해 내부 데이터 유출의 취약성을 내포하고 있다. 따라서 신뢰적인 개체를 통해 안전한 사용자 및 데이터 관리 구조가 요구된다. 이와 더불어 응용 프로그램의 모니터링을 통해 내부 데이터의 유출을 방지하고자 하였으나, 불법적인 데이터의 유출이 발생하거나 유출이 시도될 경우 이를 차단하거나 추적할 수 없어 이를 위한 별도의 보안 서비스가 요구된다.

[0009] 이를 방지하기 위해서는 내부 사용자들에 대한 데이터가 공유되고 사용될 때 데이터에 대한 권한을 설정하고 사용자들의 데이터에 대한 사용 및 처리가 명시적으로 관리되고 있음을 확인할 수 있는 서비스가 요구된다.

발명의 내용

해결 하고자하는 과제

[0010] 본 발명은 상기한 문제점을 해결하기 위해 사용자들에 대한 데이터가 공유되고 사용될 때 데이터에 대한 권한을 설정하고 사용자들의 데이터에 대한 사용 및 처리가 명시적으로 관리할 수 있어 정보 데이터의 권한 변경을 방지는 방법 및 시스템을 제공한다.

과제 해결수단

[0011] 상기 목적을 달성하기 위한 본 발명에 따른, 정보 데이터의 권한 변경을 방지하는 방법은 상기 정보 데이터를 제공받고자 하는 사용자와 사용자 등록 및 상호 인증 과증을 수행하는 단계; 상기 사용자로부터 상기 정보 데이터의 변경된 권한 정보가 암호화된 암호 알고리즘값을 포함하는 이벤트를 수신하는 단계;상기 이벤트에서 상기 암호 알고리즘값을 복호화하여 상기 정보 데이터의 변경된 권한 정보를 추출하는 단계; 및 상기 추출된 권한 정보가 기등록된 상기 정보 데이터의 권한 정보와 동일하지 않는 경우, 상기 이벤트를 전송한 사용자를 공격자 차단 리스트에 등록하는 단계;를 포함한다.

[0012] 그리고, 상기 사용자 등록 및 상호 인증 과정을 수행하는 단계는, 상기 사용자로부터 상기 정보 데이터를 제공받고자 하는 정보 요청 이벤트를 수신하는 단계;호스트의 제2 공개키 서명 알고리즘값(S_{H_2}) 및 호스트의 제3 암호 알고리즘값(V_{H_3})을 생성하여 사용자에게 전송하는 단계; 상기 사용자로부터 사용자의 제2 해쉬 알고리즘값(h_{u_2}) 및 사용자의 제2 암호 알고리즘값(V_{u_2})을 수신받는 단계;상기 사용자의 제2 암호 알고리즘값(V_{u_2})을 복호화한 뒤 사용자 등록값($f_u(x)$)과 씨드의 타임스탬프(t_{seed})를 획득하고 초기 공유한 씨드를 이용해 데이터 배포에 따른 사용자 등록값($f_u(x)$)을 사용자 정보와 일대일 매칭하여 저장하는 단계; 호스트는 사용자의 2MAC 값 및 호스트의 제3 암호 알고리즘값(V_{H_3})을 산출하는 단계; 및 상기 호스트의 제3 암호 알고리즘값(V_{H_3})을 사용자의 아이디(ID_u), 제공되는 정보 데이터와 일대일 매칭시키는 단계;를 포함하는 것이 바람직하다.

[0013] 또한, 상기 호스트의 제2 공개키 서명 알고리즘값(S_{H_2}) 및 상기 호스트의 제3 암호 알고리즘값(V_{H_3})값은 하기 수학식과 동일한 것을 특징으로 하는 정보 데이터의 권한 변경을 방지하는 방법.

$$e_H = < ID_H, Authorization-information, Contents-list >$$

$$S_{H_2} = Sig(e_H || Contents-list)$$

$$V_{H_3} = E_{sk_{H-u}}(e_H, t_{seed})$$

[0014]

[0015] 여기서, 호스트의 이벤트(e_H)는 호스트의 아이디(ID_H), 정보 데이터의 권한 정보($Authorization-information$) 및 정보 데이터의 리스트($Contents-list$)를 포함하며, 제2 공개키 서명 알고리즘값(S_{H_2})은 호스트의 이벤트(e_H) 및 정보 데이터의 리스트($Contents-list$)를 인자로 한 공개키 서명 알고리즘화한 값이고, 호스트의 제3 암호 알고리즘값(V_{H_3})은 호스트의 이벤트(e_H) 및 씨드의 타임 스탬프(t_{seed})를 세션키(sk_{H-u})로 암호 알고리즘화한 값이다.

[0016] 그리고, 상기 사용자의 제2 해쉬 알고리즘값(h_{u_2}) 및 상기 사용자의 제2 암호 알고리즘값(V_{u_2})은 하기 수학식과 동일한 것이 바람직하다.

$$f_u(x) = \frac{1 - 2^{s*seed}}{1 - 2^s}$$

$$h_{u_2} = H(Media\ Access\ Control_u || t_{seed})$$

$$V_{u_2} = E_{sk_{H-u}}(f_u(x), t_{seed})$$

[0017]

[0018] 여기서, 사용자의 제2 해쉬 알고리즘값(h_{u_2})은 사용자 NIC(Network Interface Card)의 하드웨어 고유 주소값($Media\ Access\ Control_u$) 및 씨드의 타임스탬프(t_{seed})를 해쉬 알고리즘화한 값이고, 사용자의 제2 암호 알고리즘값(V_{u_2})는 사용자 등록값($f_u(x)$)과 씨드의 타임스탬프(t_{seed})를 세션키(sk_{H-u})로 암호 알고리즘화한 값이다. 그리고, 사용자 등록값($f_u(x)$)의 s는 0이 아닌 실수이고, x 는 변수이다.

[0019] 또한, 상기 사용자의 2MAC값 및 상기 호스트의 제3 암호 알고리즘값(V_{H_3})은 하기 수학식과 동일한 것이 바람직하다.

$$2MAC = H(Media\ Access\ Control_u || t_{seed}) \oplus H(ID_u || IP_u || seed)$$

$$V_{H_3} = E_{p_H}(2MAC || Media\ Access\ Control_u || ID_u || IP_u || t_{seed})$$

[0020]

[0021] 여기서, 사용자의 2MAC값은 사용자 NIC(Network Interface Card)의 하드웨어 고유 주소값($Media\ Access\ Control_u$) 및 씨드의 타임스탬프(t_{seed})를 해쉬 알고리즘화한 값과, 사용자의 아이디(

ID_u), 사용자의 아이피(IP_u) 및 씨드($seed$)를 해쉬 알고리즘화한 값의 논리합이다. 그리고, 사용자의 제2암호 알고리즘값은 2MAC값, 사용자 NIC(Network Interface Card)의 하드웨어 고유 주소값($Media\ Access\ Control_u$), 사용자의 아이디(ID_u), 사용자의 아이피(IP_u) 및 씨드의타임스탬프(t_{seed})를 호스트의 공개키로 암호 알고리즘화한 값이다.

효 과

[0022] 본 발명에 의하면, 각각의 데이터에 대한 권한 관리 뿐만 아니라 사용자에 대한 명시적 인증을 통해 사용자와 데이터의 안전한 관리가 가능하게 하고, 불법적으로 정보 데이터의 권한을 변경하여 정보 데이터를 외부로 유출하고자 할 때에는 불법 사용자와 사용 디바이스에 대한 추적함으로써 네트워크 및 응용 서비스 발전에 기여하는데 큰 효과가 있다.

발명의 실시를 위한 구체적인 내용

[0023] 이하에서는 도면을 참조하여 본 발명을 보다 상세하게 설명한다.

[0024] 도 1은 본 발명의 일 실시예에 정보 데이터의 관리 시스템을 도시한 도면이다. 도 1에 도시된 바와 같이, 정보 데이터의 관리 시스템은 호스트(100), 상기한 정보 데이터를 호스트(100)에 등록하거나 정보 데이터를 제공받는 복수 개의 슬레이브(200)를 포함한다.

[0025] 호스트(100)는 슬레이브(200)의 사용자로부터 정보 데이터 및 상기한 정보 데이터에 대한 권한 정보를 수신하고 이를 등록한다. 그리고, 슬레이브(200)의 사용자와 상호 인증 과정을 통해 특정 슬레이브(200)의 사용자에게 정보 데이터를 제공할 뿐만 아니라, 정보 데이터의 권한을 변경하여 정보 데이터를 유출하고자 하는 자를 추출하고, 추출된 자의 사용을 차단하는 기능을 수행한다.

[0026] 복수 개의 슬레이브(200)의 사용자는 상호 인증을 통해 정보 데이터를 호스트(100)에 등록하거나, 호스트(100)에 등록된 정보 데이터를 제공받는다.

[0027] 이하에서는 정보 데이터를 생성한 자의 인증과 정보 데이터에 대한 권한 위임 과정, 사용자와 호스트(100)간의 상호 인증 과정, 호스트의 사용자에게로의 정보 데이터 제공 과정, 권한없는 사용자를 차단하는 과정 등을 도면을 첨부하면서 상세히 설명한다.

[0028] 도2는 본 발명의 일 실시예에 따른 정보 데이터를 생성한 정보 생성자의 인증과 정보 데이터에 대한 권한 위임 과정을 설명하는 흐름도이다. 정보 생성자는 제1 슬레이브(210)의 사용자라고 가정하면 이해가 용이하다. 그리고, 정보 생성자는 제1 슬레이브(210)에서 각종 정보를 생성하여 호스트(100)로 전송하기 때문에 정보 생성자의 인증과 정보 데이터에 대한 권한 위임은 제1 슬레이브(210)와 호스트(100)간의 통신을 통해 수행된다.

[0029] 도 2에 도시된 바와 같이, 정보 생성자는 제1 슬레이브(210)를 통해 자신이 생성한 정보 데이터의 권한 위임을 위하여 호스트(100)에 정보 생성자의 아이디(ID), 정보 데이터의 유형($Content\ type$), 정보 생성자가 요구하는 정보 데이터의 권한($authorization$), 타임스탬프(t)를 포함하는 권한 요청 이벤트($e_{cc} = < ID, Content\ type, authorization, t >$)를 생성하여 전송한다(S210).

[0030] 호스트(100)는 정보 생성자의 권한 요청 이벤트(e_{cc})를 수신하고, 호스트의 제1 해쉬 알고리즘값(C_{H_1}) 및 호스트의 제1 암호 알고리즘값(V_{H_1})을 하기 수학식 1과 같이 산출하여 제1 슬레이브(210)의 정보 생성자에게 전송한다(S220).

수학식 1

$$AID_H = (ID_H)^{r_{H_1}^{-1}}$$

$$C_{H_1} = H(AID_H, SR, t_{H_1})^{r_{H_1}^{-1}}$$

$$V_{H_1} = E_{p_{cc}}(r_{H_1} \| t_{H_1})$$

[0031]

[0032] 수학식 1에 도시된 바와 같이, 호스트의 아이디 변형 값(AID_H)은 밑을 호스트의 아이디(ID_H)하고, 지수를 호스트의 제1 의사 난수(r_{H_1})의 역수로 하는 지수 함수이며, 호스트의 제1 해쉬 알고리즘값(C_{H_1})은, 호스트의 아이디 변형값(AID_H), 서비스 요청 메시지(SR), 호스트의 제1 타임스탬프(t_{H_1})를 포함하는 해쉬값을 밑으로 하고, r_{H_1}의 역수를 지수로 하는 지수 함수이다. 그리고, 호스트의 제1 암호 알고리즘값(V_{H_1})은 호스트의 제1 의사 난수(r_{H_1}) 및 호스트의 제1 타임스탬프(t_{H_1})을 암호 알고리즘화한 값이다.

[0033] 정보 생성자는 제1 슬레이브(210)를 통해 호스트의 제1 해쉬 알고리즘값(C_{H_1}) 및 호스트의 제1 암호 알고리즘값(V_{H_1})을 수신하고, 호스트의 제1 해쉬 알고리즘값(C_{H_1})에 대한 무결성을 검증한다(S230). 구체적으로, 정보 생성자는 수신된 호스트의 제1 암호 알고리즘값(V_{H_1})을 개인키를 이용하여 복호화함으로써 제1 예상 호스트의 의사난수($r_H^{-1'}$)를 획득한다. 그리고, 이를 기반으로 제1 예상 호스트 아이디의 변형값(AID_H')을 산출한 후 제1 예상 허쉬 알고리즘값($C_H' = H(AID_H', SR, t_H)^{r_H^{-1'}}$)을 산출하여, 제1 예상 해쉬 알고리즘값(C_H')이 호스트(100)로부터 전송된 호스트의 제1 해쉬 알고리즘값(C_{H_1})과 동일하면, 호스트의 제1 해쉬 알고리즘값(C_{H_1})은 무결성이 검증되었다고 한다.

[0034] 무결성이 검증되었다고 판단되면(S230-Y), 정보 생성자는 정보 생성자의 암호 알고리즘값(V_{cc})을 하기 수학식 2와 같이 산출하여 호스트(100)로 전송한다(S240).

수학식 2

[0035]
$$V_{cc} = E_{p_H}(Digital-Contents_{list}, Authorization-information_{cc}, ID_{cc}, t_{cc})$$

[0036] 수학식 2에 도시된 바와 같이, 정보 생성자의 암호 알고리즘값(V_{cc})은, 호스트에서 제공되는 데이터 목록 중 정보 데이터가 속하는 항목 정보($Digital-Contents_{list}$), 정보 데이터에 설정하고자 하는 권한 정보($Authorization-information_{cc}$), 정보 생성자의 아이디(ID_{cc}) 및 정보 생성자의 타임스탬프(t_{cc})을 암호 알고리즘화한 값이다.

[0037] 호스트(100)는 정보 생성자의 암호 알고리즘값(V_{cc})을 호스트의 개인키를 이용하여 복호화함으로써, 정보 데이터에 설정하고자 하는 권한 정보($Authorization-information_{cc}$), 정보 생성자의 아이디(ID_{cc})를 추출한다(S250).

[0038] 그리고, 상기한 정보들을 공개키 서명 알고리즘화한 하기 수학식 3과 같은 호스트의 제1 공개키 서명 알고리즘값(S_{H_1})을 산출한다. 그리고, 그 값을 공개 게시판에 게시한다(S260).

수학식 3

[0039] $$S_{H_1} = Sig(Authorization-information_{cc}, ID_{cc})$$

[0040] 이와 같은 방법으로, 시스템은 정보 생성자의 인증과 정보 생성자에 의해 생성된 정보 데이터의 권한을 설정한다.

[0041] 도 3은 본 발명의 일 실시예에 따른 정보 데이터의 사용을 위한 사용자 등록 및 상호 인증 과정을 설명하는 흐름도이다. 여기서 사용자는 제1 내지 제3 슬레이브(230)의 사용자 모두가 될 수 있다. 그리고, 사용자가 작업하고 있는 슬레이브(200)와 호스트(100)간의 통신을 통해 사용자 등록 및 상호 인증이 수행되는데, 간단히 사용자와 호스트(100)간의 통신으로 설명한다.

[0042] 호스트(100)에 등록된 정보 데이터를 사용하고자 하는 사용자는 사용자 등록을 요구하는 등록 요구 메시지를 생성하여 호스트(100)에 전송한다(S310).

[0043] 상기한 등록 요구 메시지를 수신받은 호스트(100)는 사용자가 사용자 등록을 요구하는 메시지를 보낸 시간을 씨드($seed$)로 하여, 호스트의 제2 해쉬 알고리즘값(h_{H_2}) 및 호스트의 제2 암호 알고리즘값(V_{H_2})을 하기 수학식 4와 같이 설정하고, 그 값들을 사용자에게 전송한다(S320).

수학식 4

[0044] $$h_{H_2} = H(r_{H_2}, seed)$$

$$V_{H_2} = E_{p_u}(seed, r_{H_2}, t_{H_2})$$

[0045] 수학식 4에 도시된 바와 같이, 호스트의 제2 해쉬 알고리즘값(h_{H_2})은 호스트의 제2 의사 난수(r_{H_2}) 및 씨드($seed$)를 해쉬 알고리즘화한 값이고, 호스트의 제2 암호 알고리즘값(V_{H_2})은 씨드($seed$), 호스트의 제2 의사 난수(r_{H_2}), 및 호스트의 제2 타임 스탬프(t_{H_2})를 사용자의 공개키로 암호 알고리즘화한 값이다.

[0046] 사용자는 호스트의 제2 해쉬 알고리즘값(h_{H_2}) 및 호스트의 제2 암호 알고리즘값(V_{H_2})을 수신하고, 호스트의 제2 암호 알고리즘값(V_{H_2})을 사용자의 개인키로 복호화한 뒤 씨드($seed$)와 호스트의 제2 의사 난수(r_{H_2})를 획득한다(S330).

[0047] 그리고, 사용자는 호스트의 제2 의사 난수(r_{H_2})와 동일한 사용자의 제1 의사 난수(r_{u_1})를 선택한 후 사용자의 제1 암호 알고리즘값(V_{u_1})을 하기 수학식 5와 같이 설정하여 호스트(100)에 전송한다(S340).

수학식 5

$$t_{u_1} = r_{u_1} * t_{H_2} - t_{seed}$$

$$V_{u_1} = E_{p_H}(r_{u_1}, u_{info}, t_{u_1})$$

[0048]

[0049] 수학식 5에 대해 설명하면, 사용자의 제1 타임스탬프(t_{u_1})는 사용자의 제1 의사 난수(r_{u_1})와 호스트의 제2 의사 난수(r_{H_2})의 곱으로부터 씨드의 타임스탬프(t_{seed})를 뺀 값이고, 사용자의 제1 암호 알고리즘값(V_{u_1})은 사용자의 제1 의사 난수(r_{u_1}), 사용자 정보(u_{info}), 사용자의 제1 타임스탬프(t_{u_1})를 호스트의 공개키로 암호 알고리즘화한 값이다.

[0050] 호스트(100)는 수신된 사용자의 제1 암호 알고리즘값(V_{u_1})을 복호화하여, 사용자의 제1 의사 난수(r_{u_1}), 사용자 정보(u_{info}), 및 사용자의 제1 타임스탬프(t_{u_1})를 획득하고, 사용자 정보(u_{info})와 씨드($seed$)를 일대일 매칭시켜 DB에 저장하여 등록한다(S350).

[0051] 상기와 같은 과정을 수행한 후 호스트(100) 및 사용자 각각은 비밀 통신을 위한 하기 수학식 6과 같은 공통된 세션키(sk_{H-u_1})를 생성한다(S360).

수학식 6

$$sk_{H-u} = H(seed, t_{u_1})$$

[0052]

[0053] 수학식 6과 같이, 세션키(sk_{H-u})는 씨드($seed$)와 사용자의 제1 타임스탬프(t_{u_1})를 해쉬 알고리즘화한 값이다.

[0054] 도 4는 본 발명의 일 실시예에 따른 호스트가 사용자에게 정보 데이터를 제공하는 과정을 도시한 흐름도이다.

[0055] 사용자는 제공받고자 하는 정보 데이터를 호스트(100)에서 검색한다(S410).

[0056] 검색된 정보 데이터를 제공받고자 사용자는 2MAC값을 생성한 뒤 정보 데이터를 제공받고자 하는 정보 요청 이벤트(e_{u_1})를 하기 수학식 7과 같이 생성하여 호스트(100)로 전송한다(S420).

수학식 7

$$h_{u_1} = H(ID_u \| IP_u)$$

$$e_{u_1} = < ID_u, Contents - Request, Contents\ type, h_{u_1} >$$

[0057]

[0058] 수학식 7에 도시된 바와 같이, 사용자의 제1 해쉬 알고리즘값(h_{u_1})은 사용자의 아이디(ID_u) 및 사용자의 아이피(IP_u)를 인자로 한 해쉬 알고리즘화한 값이고, 요청 이벤트 메시지(e_{u_1})는 사용자의 아이디(ID_u), 정보 데이터를 요청하는 정보($Contents - Request$), 정보 데이터의 타입($Contents\ type$) 및

사용자의 제1 해쉬 알고리즘값(h_{u_1})이 포함되어 있다.

[0059] 호스트(100)는 해당 데이터에 대한 정보 생성자에 의해 설정된 권한 정보를 포함하는 호스트의 제1 공개키 서명 알고리즘값(S_{H_1})을 공개 게시판에서 검색한 후 호스트의 제2 공개키 서명 알고리즘값(S_{H_2}) 및 호스트의 제3 암호 알고리즘값(V_{H_3})을 하기 수학식 8과 같이 생성하여 사용자에게 전송한다(S430).

수학식 8

$$e_H = < ID_H, Authorization-information, Contents-list >$$

$$S_{H_2} = Sig(e_H \| Contents-list)$$

$$V_{H_3} = E_{sk_{H-u}}(e_H, t_{seed})$$

[0060]

[0061] 여기서, 호스트의 이벤트(e_H)는 호스트의 아이디(ID_H), 정보 데이터의 권한 정보($Authorization-information$) 및 정보 데이터의 리스트($Contents-list$)를 포함하며, 제2 공개키 서명 알고리즘값(S_{H_2})은 호스트의 이벤트(e_H) 및 정보 데이터의 리스트($Contents-list$)를 인자로 한 공개키 서명 알고리즘화한 값이고, 호스트의 제3 암호 알고리즘값(V_{H_3})은 호스트의 이벤트(e_H) 및 씨드의 타임 스탬프(t_{seed})를 세션키(sk_{H-u})로 암호 알고리즘화한 값이다.

[0062] 사용자는 제2 공개키 서명 알고리즘값(S_{H_2}) 및 호스트의 제3 암호 알고리즘값(V_{H_3})을 수신한 후, 호스트의 공개키로 호스트의 제2 공개키 서명 알고리즘값(S_{H_2})를 복호화하여 호스트의 이벤트(e_H) 및 정보 데이터의 리스트($Contents-list$)를 추출한다(S440).

[0063] 또한, 사용자는 기설정된 세션키(sk_{H-u})로 호스트의 제3 암호 알고리즘값(V_{H_3})을 복호화하여 호스트의 이벤트(e_H) 및 씨드의 타임 스탬프(t_{seed})를 추출한다(S440).

[0064] 호스트의 제3 암호 알고리즘값(V_{H_3})에서 복호화된 호스트의 이벤트(e_H)가 호스트의 제2 공개키 서명 알고리즘값(S_{H_2})에서 복호화된 호스트의 이벤트(e_H)와 동일하고, 씨드의 타임 스탬프(t_{seed})가 기저장된 값과 동일한지 여부로 검증을 수행한다(S460).

[0065] 검증이 올바르면(S460-Y), 사용자는 하기 수학식 9와 같은 사용자의 제2 해쉬 알고리즘값(h_{u_2}) 및 사용자의 제2 암호 알고리즘값(V_{u_2})을 산출하여 호스트(100)에 전송한다(S470).

수학식 9

$$f_u(x) = \frac{1 - 2^{s*seed}}{1 - 2^{s}}$$

$$h_{u_2} = H(Media\ Access\ Control_u || t_{seed})$$

$$V_{u_2} = E_{sk_{H-u}}(f_u(x), t_{seed})$$

[0066]

[0067] 수학식 9에 도시된 바와 같이, 제2 해쉬 알고리즘값(h_{u_2})은 사용자 NIC(Network Interface Card)의 하드웨어 고유 주소값($Media\ Access\ Control_u$) 및 씨드의 타임스탬프(t_{seed})를 해쉬 알고리즘화한 값이고, 사용자의 제2 암호 알고리즘값(V_{u_2})는 사용자 등록값($f_u(x)$)과 씨드의 타임스탬프(t_{seed})를 세션키(sk_{H-u})로 암호 알고리즘화한 값이다. 그리고, 사용자 등록값($f_u(x)$)의 s는 0이 아닌 실수이고, x 는 변수이다.

[0068] 호스트(100)는 사용자의 제2 암호 알고리즘값(V_{u_2})을 복호화한 뒤 사용자 등록값($f_u(x)$)과 씨드의 타임스탬프(t_{seed})를 획득하고 초기 공유한 씨드를 이용해 데이터 배포에 따른 사용자 등록값($f_u(x)$)을 사용자 정보와 일대일 매칭하여 저장한다(S480).

[0069] 그리고, 호스트(100)는 하기 수학식 10과 같이 사용자의 2MAC 값 및 호스트의 제3 암호 알고리즘값(V_{H_3})을 산출하고, 호스트의 제3 암호 알고리즘값(V_{H_3})을 사용자의 아이디(ID_u), 제공되는 정보 데이터와 일대일 매칭시킨 뒤 공개 게시판에 공고한다(S490).

수학식 10

$$2MAC = H(Media\ Access\ Control_u || t_{seed}) \oplus H(ID_u || IP_u || seed)$$

$$V_{H_3} = E_{p_H}(2MAC || Media\ Access\ Control_u || ID_u || IP_u || t_{seed})$$

[0070]

[0071] 도 10에 도시된 바와 같이, 사용자의 2MAC값은 사용자 NIC(Network Interface Card)의 하드웨어 고유 주소값($Media\ Access\ Control_u$) 및 씨드의 타임스탬프(t_{seed})를 해쉬 알고리즘화한 값과, 사용자의 아이디(ID_u), 사용자의 아이피(IP_u) 및 씨드($seed$)를 해쉬 알고리즘화한 값의 논리합이다. 그리고, 사용자의 제3 암호 알고리즘값은 2MAC값, 사용자 NIC(Network Interface Card)의 하드웨어 고유 주소값($Media\ Access\ Control_u$), 사용자의 아이디(ID_u), 사용자의 아이피(IP_u) 및 씨드의 타임스탬프(t_{seed})를 호스트의 공개키로 암호 알고리즘화한 값이다.

[0072] 이와 같은 방식으로, 사용자 등록 및 상호 인증을 수행한다.

[0073] 도 5는 본 발명의 일 실시예에 따른 정보 데이터의 권한을 변경한 사용자를 차단시키는 방법에 제공되는 흐름도이다.

[0074] 설명의 편의를 위해 정보 데이터를 유출하고자 하는 자를 유출자라고 한다. 그리고, 여기서 유출자는 호스트(100)와 사용자 등록 및 상호 인증 과정을 거친 제1 내지 제3 슬레이브(200)의 사용자 중 어느 하나의 사용자인데, 설명의 편의를 위해 유출자는 제3 슬레이브(230)를 통해 호스트(100)와 통신한다고 가정한다.

[0075] 외부 유출 권한이 없는 정보 데이터를 외부로 유출하고자 할 경우, 사용자는 정보 데이터의 권한을 변경시키는 정보 및 유출 요청 메시지를 포함하는 유출 요청 이벤트를 하기 수학식 11과 같이 생성하여 호스트(100)로 전송한다(S510).

수학식 11

$$h_{u_a} = H(ID_{u_a} \| Digital\ Data \| E_{sk_{H-u_a}}(f_{u_a}(x) \| Authorization-information_{cc}'))$$

[0076]
$$e_{u_a} = < ID_{u_a}, Outflow-Request, h_{u_a} >$$

[0077] 도 11에 도시된 바와 같이, 유출자의 암호 알고리즘값($E_{sk_{H-u_a}}$)은 유출자의 등록값($f_{u_a}(x)$)과 변경된 권한 정보($Authorization-information_{cc}'$)를 유출자의 세션키(sk_{H-u_a})로 암호 알고리즘화한 값이며, 유출자의 해쉬 알고리즘값(h_{u_a})은 유출자의 아이디(ID_{u_a}), 유출하고자 하는 정보 데이터($Digital\ Data$) 및 유출자의 암호 알고리즘값($E_{sk_{H-u_a}}$)를 해쉬 알고리즘화한 값이다. 그리고, 유출 요청 이벤트(e_{u_a})에는 유출자의 아이디(ID_{u_a}), 유출 요청 정보($Outflow-Request$) 및 유출자의 해쉬 알고리즘값(h_{u_a})을 포함한다.

[0078] 유출 요청을 받은 호스트(100)는 유출자의 아이디(ID_{u_a})를 기반으로 유출자와 함께 공유하는 세션키(sk_{H-u_a})를 추출하여 유출자의 암호 알고리즘값($E_{sk_{H-u_a}}$)을 복호화한 뒤 수신된 권한 정보($Authorization-information_{cc}'$)를 추출한다(S520).

[0079] 그리고, 수신된 권한 정보와 공개 게시판에 등록된 권한 정보가 동일한지 판단한다(S530).

[0080] 수신된 권한 정보와 공개 게시판에 등록된 권한 정보가 동일하면(S530-Y), 호스트(100)는 정보 데이터를 제공한다(S540).

[0081] 그러나, 수신된 권한 정보와 공개 게시판에 등록된 권한 정보가 다르다고 판단되면(S530-N), 호스트(100)는 공개 게시판에 공개된 호스트의 제3 암호 알고리즘값(V_{H_3})(여기서 호스트의 제3 암호 알고리즘값이라 함은 유출자와 호스트(100)간의 통신을 통해 획득된 값이다.)을 호스트의 개인키로 복호화하여 2MAC값, 유출자의 NIC(Network Interface Card)의 하드웨어 고유 주소값($Media\ Access\ Control_{u_a}$), 유출자의 ID(ID_{u_a}), 유출자의 IP(IP_{u_a}) 및 씨드의 타임스탬프(t_{seed})를 획득한다(S550).

[0082] 그리고, 씨드의 타임스탬프(t_{seed})와 씨드($seed$)를 초기화한 뒤 유출자의 2MAC 값을 공격자 차단 리스트에 등록한다(S560).

[0083] 그리고, 호스트(100)는 유출자에게 정보 데이터를 제공하지 않는다(S570).

[0084] 또한, 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명

의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

도면의 간단한 설명

[0085] 도 1은 본 발명의 일 실시예에 정보 데이터의 관리 시스템을 도시한 도면,

[0086] 도2는 본 발명의 일 실시예에 따른 정보 데이터를 생성한 정보 생성자의 인증과 정보 데이터에 대한 권한 위임 과정을 설명하는 흐름도,

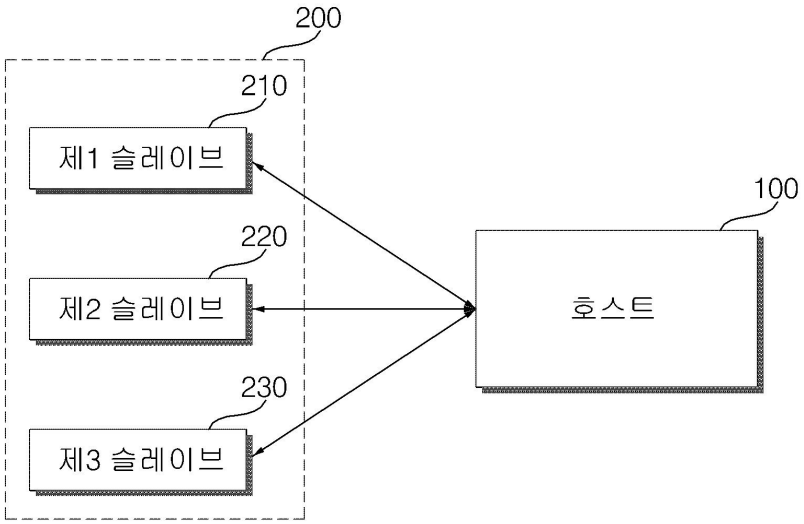
[0087] 도 3은 본 발명의 일 실시예에 따른 정보 데이터의 사용을 위한 사용자 등록 및 상호 인증 과정을 설명하는 흐름도,

[0088] 도 4는 본 발명의 일 실시예에 따른 호스트가 사용자에게 정보 데이터를 제공하는 과정을 도시한 흐름도, 그리고,

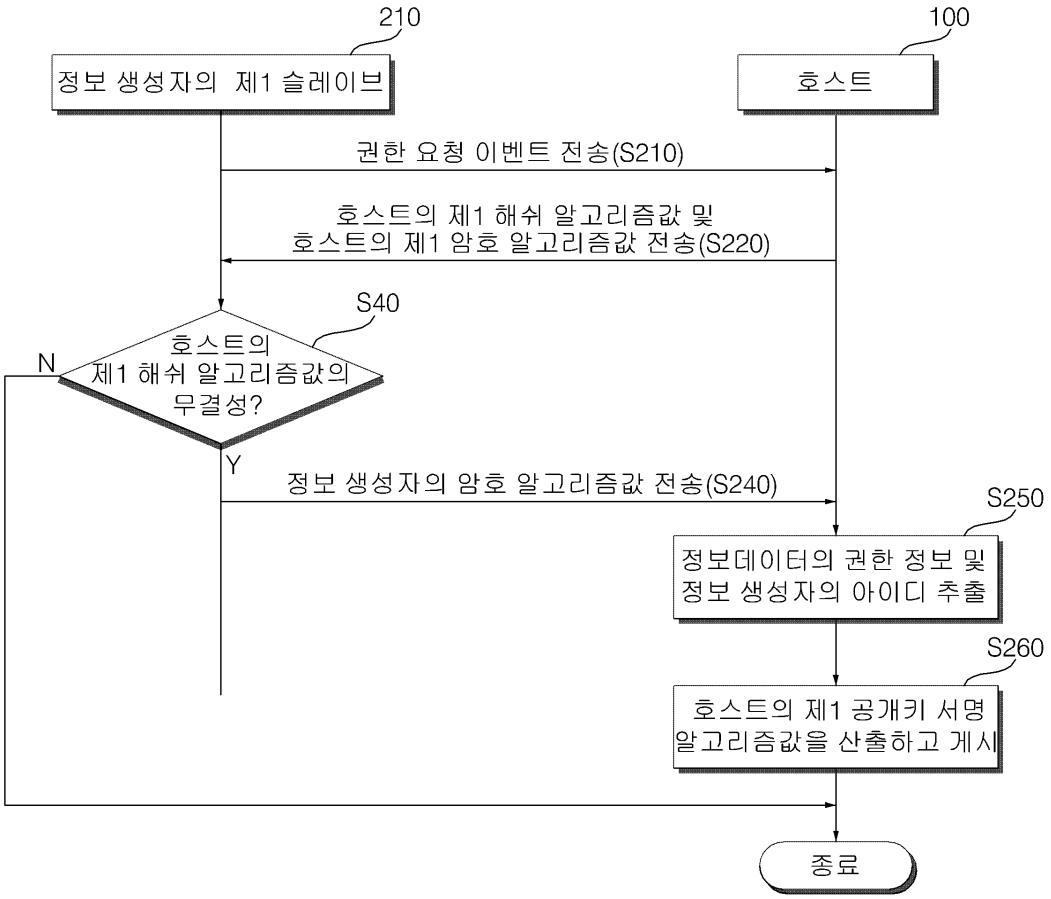
[0089] 도 5는 본 발명의 일 실시예에 따른 정보 데이터의 권한을 변경한 사용자를 차단시키는 방법에 제공되는 흐름도이다.

도면

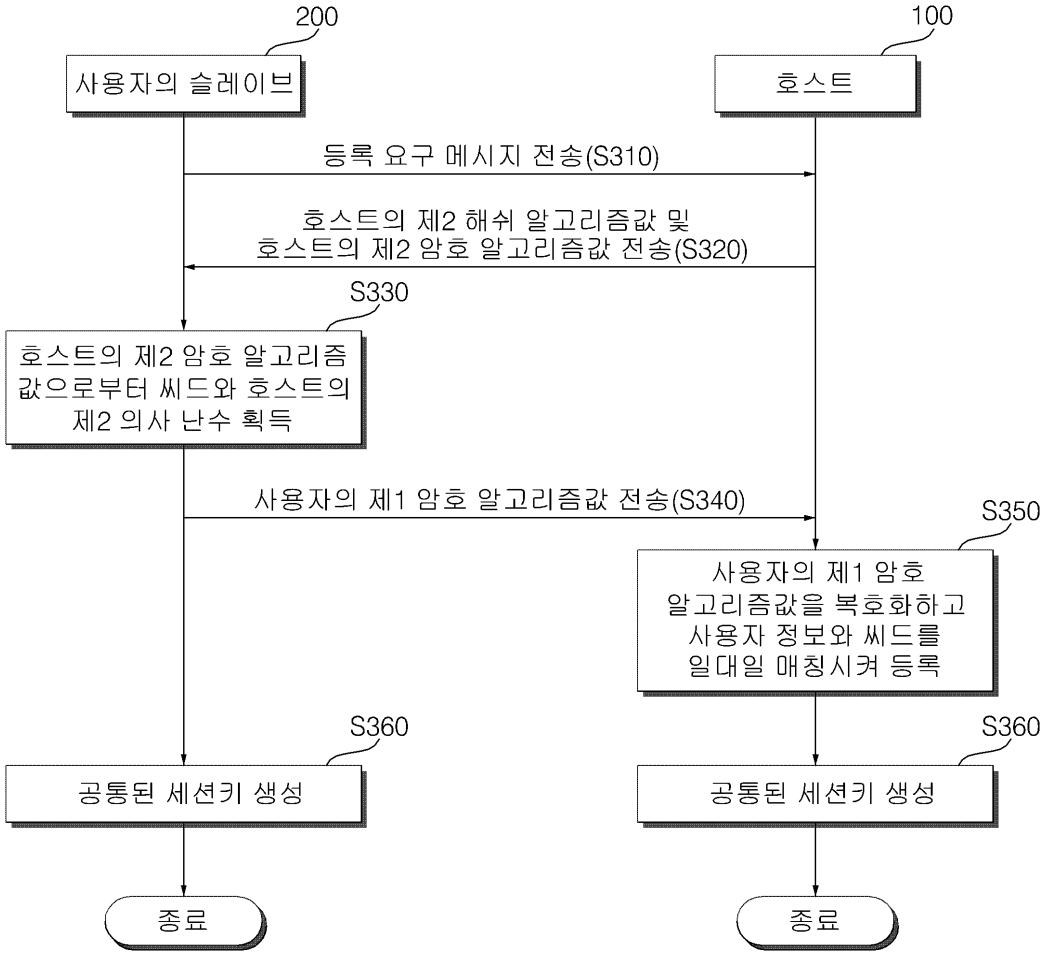
도면1



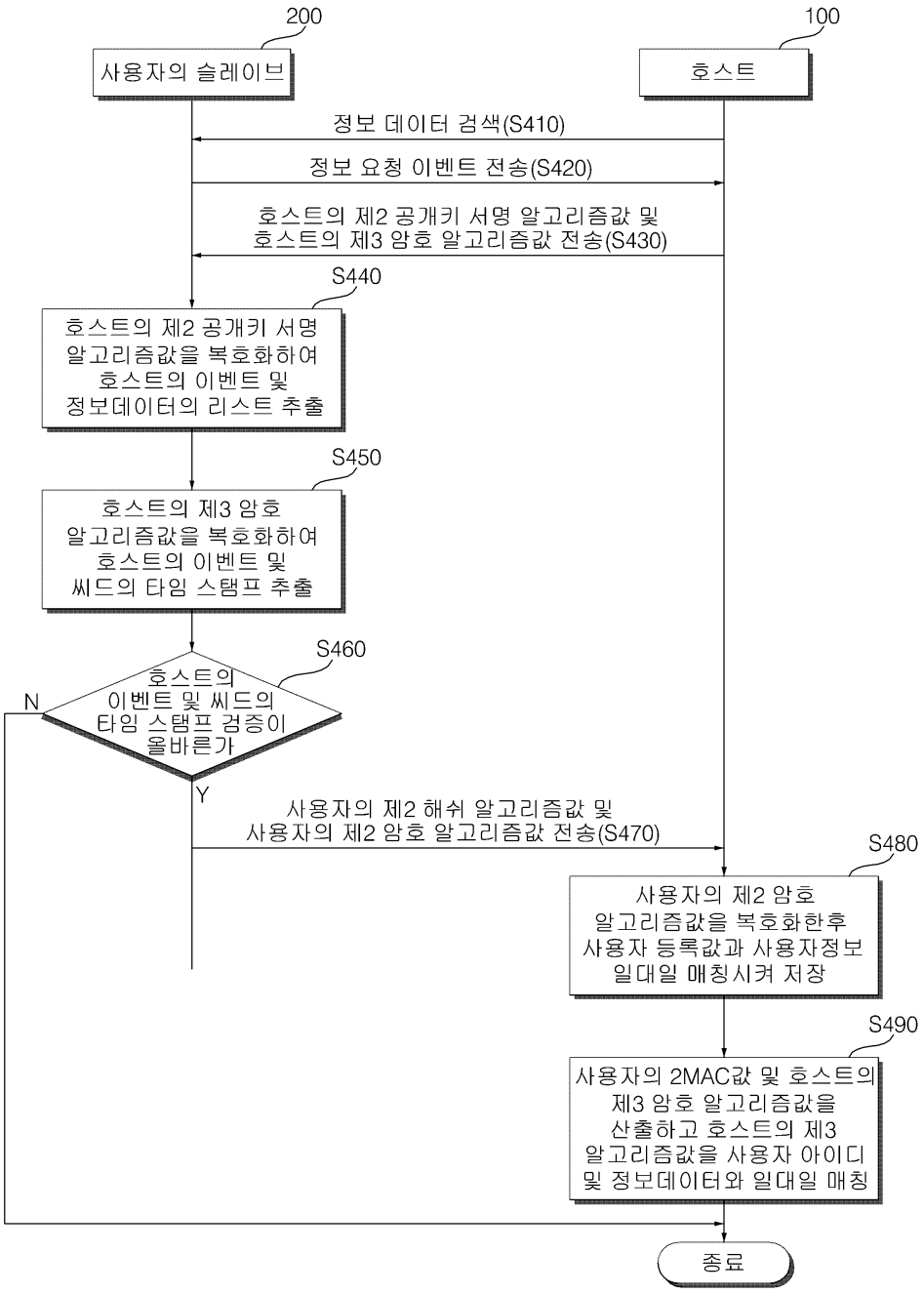
도면2


210
100
정보 생성자의 제1 슬레이브
호스트
권한 요청 이벤트 전송(S210)
호스트의 제1 해쉬 알고리즘값 및
호스트의 제1 암호 알고리즘값 전송(S220)
S40
호스트의
제1 해쉬 알고리즘값의
무결성?
N
Y
정보 생성자의 암호 알고리즘값 전송(S240)
S250
정보데이터의 권한 정보 및
정보 생성자의 아이디 추출
S260
호스트의 제1 공개키 서명
알고리즘값을 산출하고 게시
종료

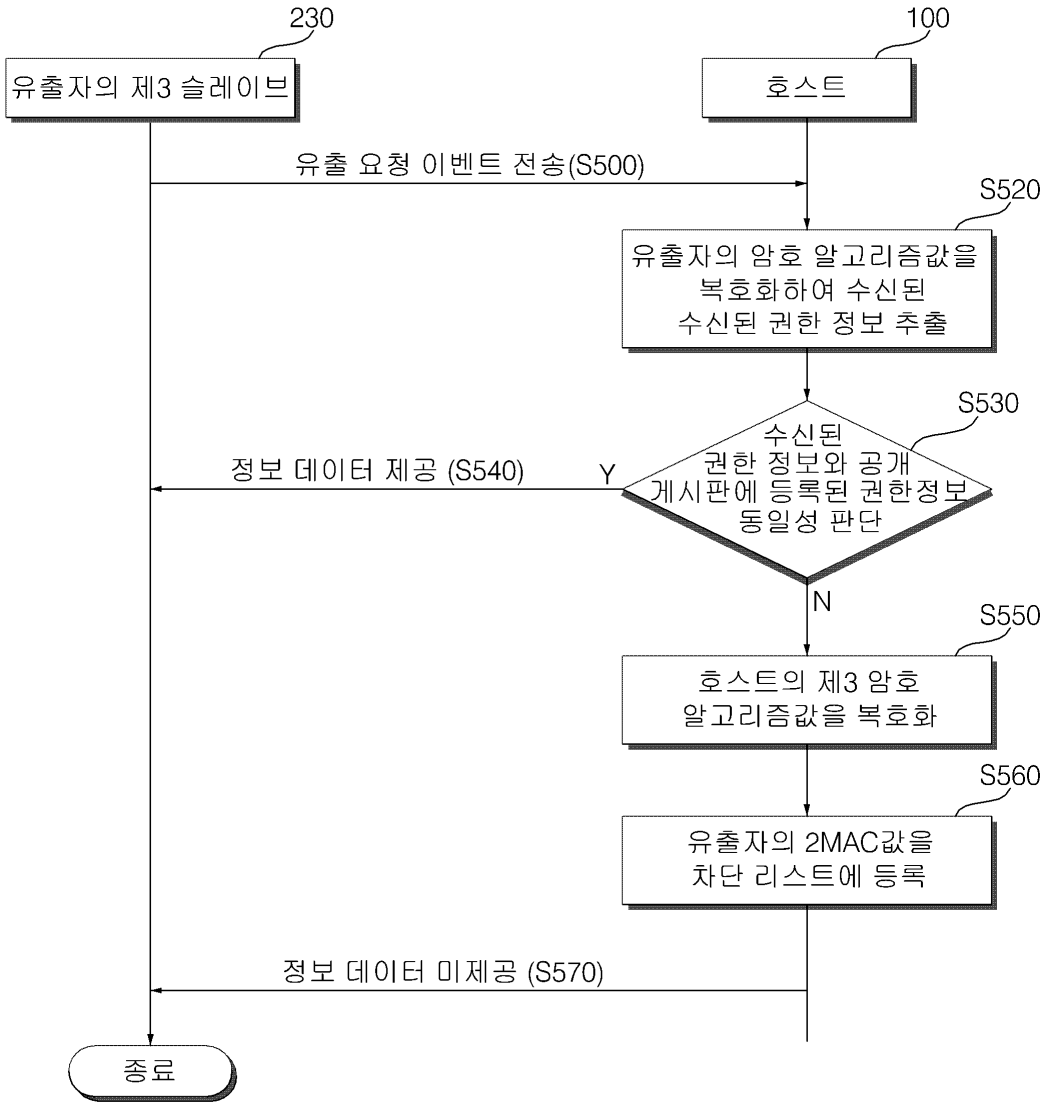
도면3


200
100
사용자의 슬레이브
호스트
등록 요구 메시지 전송(S310)
호스트의 제2 해쉬 알고리즘값 및
호스트의 제2 암호 알고리즘값 전송(S320)
S330
호스트의 제2 암호 알고리즘
값으로부터 씨드와 호스트의
제2 의사 난수 획득
사용자의 제1 암호 알고리즘값 전송(S340)
S350
사용자의 제1 암호
알고리즘값을 복호화하고
사용자 정보와 씨드를
일대일 매칭시켜 등록
S360
S360
공통된 세션키 생성
공통된 세션키 생성
종료
종료

도면4


200
100
사용자의 슬레이브
호스트
정보 데이터 검색(S410)
정보 요청 이벤트 전송(S420)
호스트의 제2 공개키 서명 알고리즘값 및
호스트의 제3 암호 알고리즘값 전송(S430)
S440
호스트의 제2 공개키 서명
알고리즘값을 복호화하여
호스트의 이벤트 및
정보데이터의 리스트 추출
S450
호스트의 제3 암호
알고리즘값을 복호화하여
호스트의 이벤트 및
씨드의 타임 스탬프 추출
S460
호스트의
이벤트 및 씨드의
타임 스탬프 검증이
올바른가
N
Y
사용자의 제2 해쉬 알고리즘값 및
사용자의 제2 암호 알고리즘값 전송(S470)
S480
사용자의 제2 암호
알고리즘값을 복호화한후
사용자 등록값과 사용자정보
일대일 매칭시켜 저장
S490
사용자의 2MAC값 및 호스트의
제3 암호 알고리즘값을
산출하고 호스트의 제3
알고리즘값을 사용자 아이디
및 정보데이터와 일대일 매칭
종료

도면5


230
유출자의 제3 슬레이브
100
호스트
유출 요청 이벤트 전송(S500)
S520
유출자의 암호 알고리즘값을
복호화하여 수신된
수신된 권한 정보 추출
S530
수신된
권한 정보와 공개
게시판에 등록된 권한정보
동일성 판단
Y
정보 데이터 제공 (S540)
N
S550
호스트의 제3 암호
알고리즘값을 복호화
S560
유출자의 2MAC값을
차단 리스트에 등록
정보 데이터 미제공 (S570)
종료