(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0101870
(43) 공개일자 2018년09월14일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/06* (2006.01)
(52) CPC특허분류
H04L 9/0866 (2013.01)
H04L 9/06 (2013.01)
(21) 출원번호 10-2017-0028373
(22) 출원일자 2017년03월06일
심사청구일자 2017년03월06일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
허준범
경기도 용인시 기흥구 보정로 30, 116동 1102호(보정동, 동아솔레시티아파트)
한창희
인천광역시 남동구 호구포로 924, 109동 2204호(만수동, 햇빛마을벽산아파트)
(74) 대리인
김등용, 김홍석

전체 청구항 수 : 총 8 항

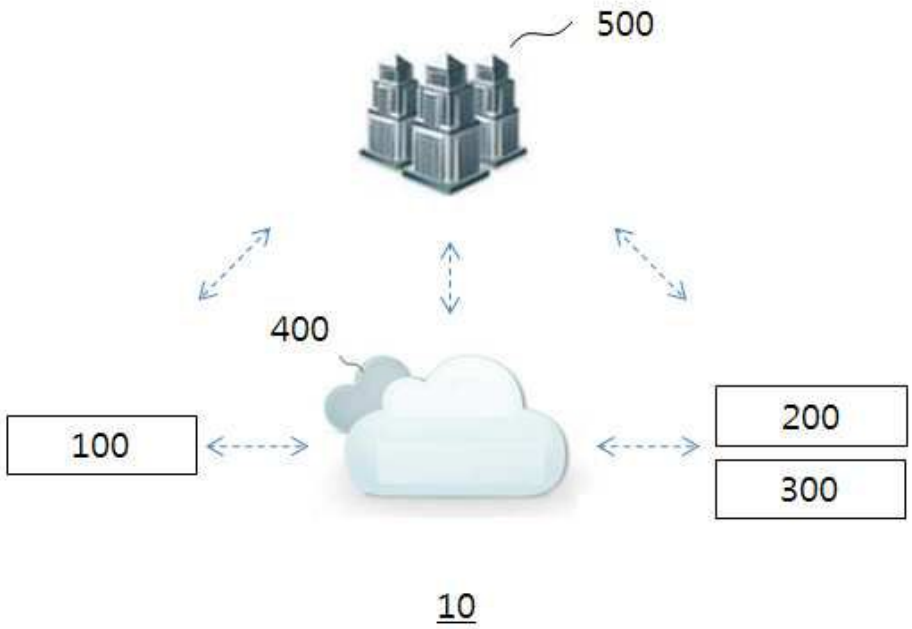
(54) 발명의 명칭 **클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 방법 및 시스템**

(57) 요 약

복수의 사용자 단말, 클라우드 서버, 및 신뢰기관 서버를 포함하는 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 시스템에서의 속성의 개수에 관계없이 항상 일정 크기의 암호문을 보장하며, 암호문이 유출된 경우 사용자의 신원을 추적할 수 있는 속성 기반 암호화를 이용한 데이터 공유 방법이 개시된다. 속성 기

(뒷면에 계속)

대 표 도 - 도1



반 암호화를 이용한 데이터 공유 방법은 신뢰기관 서버가 마스터키(MK) 및 공개키(PK)를 생성하는 셋업 단계, 신뢰기관 서버가 마스터키(MK), 공개키(PK), 각각의 사용자의 ID, 및 사용자의 속성집합을 입력으로 하고, k+2개의 임의의 a, $c \in Z_p^*$, $\{r_1, r_2, \cdots, r_k\} \in Z_p$를 선택하여 비밀키($SK_u$)를 생성하고 해당 사용자 단말에 전송하는 키 생성 단계, 신뢰기관 서버가 비밀키(SK_u) 생성을 위해 선택한 고유의 값(c) 및 사용자(u)의 ID(id_u)를 전체 사용자 ID 테이블(T)에 저장하는 단계, 사용자 단말이 메시지(M)를 공개키(PK) 및 접근제어를 위한 속성집합(W)을 입력으로 암호화하여 암호문(CT)을 생성하고 암호문(CT)을 클라우드 서버에 전송하는 암호화 단계, 사용자 단말이 클라우드 서버에 암호문(CT)을 요청하여 수신하는 암호문 요청 단계, 사용자 단말이 수신한 암호문(CT)을 복호화하여 메시지(M)를 추출하는 복호화 단계를 포함한다.

(52) CPC특허분류
H04L 9/085 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 R0190-16-2011
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보보호핵심원천기술개발
연구과제명 IoT 소프트웨어 보안 취약점 자동 분석 기술 개발
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2016.06.01 ~ 2017.05.31

명 세 서

청구범위

청구항 1

복수의 사용자 단말, 클라우드 서버, 및 신뢰기관 서버를 포함하는 속성 기반 암호화를 이용한 데이터 공유 시스템에서의 속성의 개수에 관계없이 항상 일정 크기의 암호문을 보장하는 속성 기반 암호화를 이용한 데이터 공유 방법에 있어서,

신뢰기관 서버가 임의의 $g \in G_0$, α, $\gamma \in Z_p$를 선택하여 마스터키(MK) 및 공개키(PK)를 생성하는 셋업 단계;

$$\mathrm{MK} = (\alpha, \gamma)$$

$$\mathrm{PK} = (g, g_1, \cdots, g_K, g_{K+2}, \cdots, g_{2K}, v) \in \mathbb{G}_0^{2K+1}$$

상기 신뢰기관 서버가 상기 마스터키(MK), 상기 공개키(PK), 각각의 사용자(u)의 ID(id_u), 및 사용자(u)의 속성집합(L_u)을 입력으로 하고, k+2개의 임의의 a, $c \in Z_p^*$, $\{r_1, r_2, \cdots, r_k\} \in Z_p$를 선택하여 비밀키($SK_u$)를 생성하고 해당 사용자 단말에 전송하는 키 생성 단계;

$$\mathrm{SK}_u = (D = g^{\frac{r\gamma}{a+c}}, \{D_i | i \in \{L_u^+, L_u^-, L_u^*\}\}, D' = c, D'' = g^r, D''' = g^a).$$

(이때, $D_i = g^{\gamma(c\alpha^i + \frac{r_i r}{a+c})}$ 를 만족함)

상기 신뢰기관 서버가 상기 비밀키(SK_u) 생성을 위해 선택한 고유의 값(c) 및 상기 사용자(u)의 ID(id_u)를 전체 사용자 ID 테이블(T)에 저장하는 단계;

상기 복수의 사용자 단말 중 어느 하나가 메시지(M)를 상기 공개키(PK) 및 접근제어를 위한 속성집합(W)을 입력으로 암호화하여 암호문(CT)을 생성하고 암호문(CT)을 클라우드 서버에 전송하는 암호화 단계;

상기 복수의 사용자 단말 중 어느 하나가 클라우드 서버에 암호문(CT)을 요청하고, 클라우드 서버로부터 암호문(CT)을 수신하는 암호문 요청 단계; 및

상기 복수의 사용자 단말 중 어느 하나가 수신한 암호문(CT)을 복호화하여 메시지(M)를 추출하는 복호화 단계;를 포함하는 속성 기반 암호화를 이용한 데이터 공유 방법으로서,

상기 암호화 단계는,

임의의 $t \in Z_p$를 선택하고 대칭키(Key)를 생성하는 과정;

$$Key = e(g_K, g_1)^{kt}$$

상기 대칭키(Key)를 이용한 대칭키 암호문(M_{Key})을 생성하는 과정; 및

상기 공개키(PK), 상기 접근제어를 위한 속성집합(W), 상기 대칭키 암호문(M_{Key})을 입력하여 상기 암호문(CT)를 생성하는 과정;을 포함하는,

$$CT = \left(W, M_{Key}, C_0 = g^t, C_1 = \left(v \prod_{j \in W} g_{K+1-j}\right)^t\right)$$

클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 방법.

청구항 2

제1항에 있어서,

상기 복호화 단계는,

상기 사용자 단말이 모든 $\forall i \in W$ 에 대하여 A_i를 계산하는 과정;

$$A_i = e\left(g_i^{D'}, C_1\right)$$
$$= e\left(g, \left(v \prod_{j \in W} g_{K+1-j}\right)\right)^{\alpha^i t D'}$$
$$= e\left(g, g^{\gamma + \sum_{j \in W} \alpha^{K+1-j}}\right)^{\alpha^i t D'}$$
$$= e\left(g, g\right)^{\alpha^i t D' \gamma + t D' \sum_{j \in W} \alpha^{K+1-j+i}}$$

상기 사용자 단말이 모든 $\forall i \in W$ 에 대하여 B_i를 계산하는 과정;

$$B_i = e\left(C_0, \left(\prod_{j \in W, j \neq i} g_{K+1-j+i}\right)^{D'} \cdot D_i\right)$$
$$= e\left(g, g\right)^{t D' \sum_{j \in W, j \neq i} \alpha^{K+1-j+i} + t\gamma\left(D' \alpha^i + \frac{r_i}{a+c}\right)}$$

상기 사용자 단말이 A_i/B_i를 계산하는 과정;

$$\frac{A_i}{B_i} = e(g,g)^{D' t \alpha^{K+1} - \frac{\gamma t r_i}{a+c}}$$

상기 사용자 단말이 A/B를 계산하는 과정;

$$\frac{A}{B} = \prod_{i \in W} \frac{A_i}{B_i}$$
$$= e(g,g)^{D' k t \alpha^{K+1} - \frac{\gamma t r}{a+c}}$$

상기 사용자 단말이 아래의 식을 만족하는 상기 대칭키(Key)를 복원하는 과정; 및

$$\frac{A}{B} \cdot e\left(D, C_0\right) = \frac{A}{B} \cdot e\left(g^{\frac{\gamma r}{a+c}}, g^t\right)$$
$$= e(g,g)^{D' k t \alpha^{K+1}}.$$

$$\left(\frac{A}{B} \cdot e\left(D, C_0\right)\right)^{\frac{1}{D'}} = e(g,g)^{k t \alpha^{K+1}}$$
$$= e\left(g^{\alpha^K}, g^{\alpha}\right)^{kt}$$
$$= e\left(g_K, g_1\right)^{kt}$$
$$= Key.$$

상기 사용자 단말이 상기 복원된 대칭키(Key)를 이용하여 상기 대칭키 암호문(M_{Key})을 복호화하고 상기 메시지(M)를 추출하는 과정;을 포함하는,

클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 방법.

청구항 3

제1항에 있어서,

상기 암호문 요청 단계 및 복호화 단계는,

상기 사용자 단말이 상기 클라우드 서버에 암호문을 요청하는 과정;

상기 클라우드 서버에 암호문을 요청하는 동안, 상기 사용자 단말이 상기 클라우드 서버에 부분복호키($g_i^{D'}$)를 송신하고 부분 복호를 요청하는 과정;

상기 클라우드 서버가 상기 사용자 단말을 대신하여 모든 $\forall i \in W$ 에 대하여 A_i를 계산하는 과정;

$$A_i = e\left(g_i^{D'}, C_1\right)$$
$$= e\left(g, \left(v \prod_{j \in W} g_{K+1-j}\right)\right)^{\alpha^i t D'}$$
$$= e\left(g, g^{\gamma + \sum_{j \in W} \alpha^{K+1-j}}\right)^{\alpha^i t D'}$$
$$= e\left(g, g\right)^{\alpha^i t D' \gamma + t D' \sum_{j \in W} \alpha^{K+1-j+i}}$$

상기 클라우드 서버가 제1 복호값(A)을 계산하고, 상기 사용자 단말에 상기 암호문(CT) 및 제1 복호값(A)을 전송하는 과정;

$$A = \prod_{i \in W}$$

상기 사용자 단말이 모든 $\forall i \in W$ 에 대하여 B_i 및 제2 복호값(B)을 계산하는 과정;

$$B_i = e\left(C_0, \left(\prod_{j \in W, j \neq i} g_{K+1-j+i}\right)^{D'} \cdot D_i\right)$$
$$= e\left(g, g\right)^{t D' \sum_{j \in W, j \neq i} \alpha^{K+1-j+i} + t\gamma\left(D' \alpha^i + \frac{r_i}{a+c}\right)}$$

$$B = \prod_{i \in W}$$

상기 사용자 단말이 A/B를 계산하는 과정;

$$\frac{A}{B} = \prod_{i \in W} \frac{A_i}{B_i}$$
$$= e(g, g)^{D' k t \alpha^{K+1} - \frac{\gamma t r}{a+c}}$$

상기 사용자 단말이 아래의 식을 만족하는 상기 대칭키(Key)를 복원하는 과정; 및

$$\frac{A}{B}\cdot e(D,C_0)=\frac{A}{B}\cdot e\left(g^{\frac{\gamma r}{a+c}},g^{t}\right)$$
$$=e(g,g)^{D'kt\alpha^{K+1}}.$$

$$\left(\frac{A}{B}\cdot e(D,C_0)\right)^{\frac{1}{D'}}=e(g,g)^{kt\alpha^{K+1}}$$
$$=e\left(g^{\alpha^{K}},g^{\alpha}\right)^{kt}$$
$$=e\left(g_K,g_1\right)^{kt}$$
$$=Key.$$

상기 사용자 단말이 상기 복원된 대칭키(Key)를 이용하여 상기 대칭키 암호문(M_{Key})을 복호화하고 상기 메시지(M)를 추출하는 과정;을 포함하는,

클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 방법.

청구항 4

제1항에 있어서,

상기 신뢰기관 서버가 상기 사용자 단말로부터 비밀키(SK_u)를 수신하여 키 온전성(key sanity)을 체크하고, 비밀키(SK_u)가 유출된 경우 유출된 비밀키(SK_u)를 이용하여 비밀키(SK_u)를 유출한 사용자의 ID(id_u)를 추적하는 단계를 더 포함하는,

클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 방법.

청구항 5

마스터키(MK), 공개키(PK), 및 각각의 사용자 ID에 대응하는 비밀키(SK_u)를 생성하고, 상기 마스터키(MK), 상기 공개키(PK), 상기 비밀키(SK_u), 및 전체 사용자 ID 테이블(T)을 관리하는 신뢰기관 서버;

네트워크를 통해 암호문(CT) 또는 부분복호값(A)을 송신하거나 암호문(CT) 또는 부분복호키($g_i^{D'}$)를 수신하는 통신부, 상기 암호문(CT) 저장하는 저장부, 및 상기 암호문(CT)에 대한 부분복호 요청을 수신한 경우 상기 암호문을 부분적으로 복호하여 부분복호값(A)을 계산하는 부분복호부를 구비한 클라우드 서버; 및

메시지(M)를 암호화하여 암호문(CT)을 생성하는 암호화 모듈, 암호문(CT)을 복호화하는 복호화 모듈, 및 네트워크를 통해 암호문(CT) 또는 부분복호키($g_i^{D'}$)를 송신하고, 암호문(CT) 또는 부분복호값(A)을 수신하는 통신 모듈을 구비한 복수의 사용자 단말;을 포함하되,

상기 신뢰기관 서버는,

임의의 $g\in G_0$, α , $\gamma\in Z_p$를 선택하여 상기 마스터키(MK) 및 상기 공개키(PK)를 생성하고,

$$\mathrm{MK}=(\alpha,\gamma)$$

$$\mathrm{PK}=(g,g_1,\cdots,g_K,g_{K+2},\cdots,g_{2K},v)\in\mathbb{G}_0^{2K+1}$$

상기 마스터키(MK), 상기 공개키(PK), 각각의 사용자(u)의 ID(id_u), 및 사용자(u)의 속성집합(L_u)을 입력으로 하고, k+2개의 임의의 a, $c\in Z_p^*$, $\{r_1, r_2,\cdots, r_k\}\in Z_p$를 선택하여 상기 비밀키($SK_u$)를 생성하고, 상기 비밀키($SK_u$) 생성을 위해 선택한 고유의 값(c) 및 상기 사용자(u)의 ID(id_u)를 전체 사용자 ID 테이블(T)에 저장하며,

$$\mathrm{SK}_u = (D = g^{\frac{r\gamma}{a+c}}, \{D_i | i \in \{L_u^+, L_u^-, L_u^*\}\}$$
$$, D' = c, D'' = g^r, D''' = g^a).$$

(이때, $D_i = g^{\gamma\left(c\alpha^i + \frac{r_i t'}{a+c}\right)}$ 를 만족함)

상기 사용자 단말의 암호화 모듈은,

임의의 $t \in Z_p$를 선택하여 대칭키(Key)를 생성하고, 상기 대칭키(Key)를 이용하여 대칭키 암호문(M_{Key})을 생성하며,

$$Key = e(g_K, g_1)^{kt}$$

상기 공개키(PK), 접근제어를 위한 속성집합(W), 상기 대칭키 암호문(M_{Key})을 입력하여 상기 암호문(CT)를 생성하는,

$$CT = \left(W, M_{Key}, C_0 = g^t, C_1 = \left(v \prod_{j \in W} g_{K+1-j}\right)^t\right)$$

클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 시스템.

청구항 6

제5항에 있어서,

상기 사용자 단말의 복호화 모듈은,

모든 $\forall i \in W$ 에 대하여 A_i 및 B_i를 계산하고,

$$A_i = e\left(g_i^{D'}, C_1\right)$$
$$= e\left(g, \left(v \prod_{j \in W} g_{K+1-j}\right)\right)^{\alpha^i t D'}$$
$$= e\left(g, g^{\gamma + \sum_{j \in W} \alpha^{K+1-j}}\right)^{\alpha^i t D'}$$
$$= e\left(g, g\right)^{\alpha^i t D' \gamma + t D' \sum_{j \in W} \alpha^{K+1-j+i}}$$

$$B_i = e\left(C_0, \left(\prod_{j \in W, j \neq i} g_{K+1-j+i}\right)^{D'} \cdot D_i\right)$$
$$= e\left(g, g\right)^{tD' \sum_{j \in W, j \neq i} \alpha^{K+1-j+i} + t\gamma\left(D'\alpha^i + \frac{r_i}{a+c}\right)}$$

A_i/B_i 및 A/B를 계산하여,

$$\frac{A_i}{B_i} = e(g, g)^{D' t \alpha^{K+1} - \frac{\gamma t r_i}{a+c}}$$

$$\frac{A}{B} = \prod_{i \in W} \frac{A_i}{B_i}$$
$$= e(g,g)^{D'kt\alpha^{K+1} - \frac{\gamma tr}{a+c}}$$

아래의 식을 만족하는 상기 대칭키(Key)를 복원하고,

$$\frac{A}{B} \cdot e(D, C_0) = \frac{A}{B} \cdot e\left(g^{\frac{\gamma r}{a+c}}, g^t\right)$$
$$= e(g,g)^{D'kt\alpha^{K+1}}.$$

$$\left(\frac{A}{B} \cdot e(D, C_0)\right)^{\frac{1}{D'}} = e(g,g)^{kt\alpha^{K+1}}$$
$$= e\left(g^{\alpha^K}, g^{\alpha}\right)^{kt}$$
$$= e(g_K, g_1)^{kt}$$
$$= Key.$$

상기 복원된 대칭키(Key)를 이용하여 상기 대칭키 암호문(M_{Key})을 복호화하고 상기 메시지(M)를 추출하는,

클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 시스템.

청구항 7

제5항에 있어서,

상기 사용자 단말이 상기 클라우드 서버에 암호문(CT)을 요청하는 동안, 상기 사용자 단말이 상기 클라우드 서버에 부분복호키($g_i^{D'}$)를 송신하고 부분 복호를 요청하는 경우,

상기 클라우드 서버의 상기 부분복호부가 상기 사용자 단말을 대신하여 모든 $\forall i \in W$에 대하여 A_i를 및 부분복호값(A)을 계산하는 하고, 상기 사용자 단말에 상기 암호문(CT) 및 부분복호값(A)을 전송하며,

$$A_i = e\left(g_i^{D'}, C_1\right)$$
$$= e\left(g, \left(v \prod_{j \in W} g_{K+1-j}\right)\right)^{\alpha^i tD'}$$
$$= e\left(g, g^{\gamma + \sum_{j \in W} \alpha^{K+1-j}}\right)^{\alpha^i tD'}$$
$$= e(g,g)^{\alpha^i tD'\gamma + tD' \sum_{j \in W} \alpha^{K+1-j+i}}$$

$$A = \prod_{i \in W}$$

상기 사용자 단말의 복호화 모듈이 모든 $\forall i \in W$ 에 대하여 B_i, B, 및 A/B를 계산하여,

$$B_i = e\left(C_0, \left(\prod_{j \in W, j \neq i} g_{K+1-j+i}\right)^{D'} \cdot D_i\right)$$
$$= e(g,g)^{tD' \sum_{j \in W, j \neq i} \alpha^{K+1-j+i} + t\gamma\left(D'\alpha^i + \frac{r_i}{a+c}\right)}$$

$$B = \prod_{i \in W}$$

$$\frac{A}{B} = \prod_{i \in W} \frac{A_i}{B_i}$$
$$= e(g,g)^{D'kt\alpha^{K+1} - \frac{\gamma tr}{a+c}}$$

아래의 식을 만족하는 상기 대칭키(Key)를 복원하고,

$$\frac{A}{B} \cdot e(D, C_0) = \frac{A}{B} \cdot e\left(g^{\frac{\gamma r}{a+c}}, g^t\right)$$
$$= e(g,g)^{D'kt\alpha^{K+1}}.$$

$$\left(\frac{A}{B} \cdot e(D, C_0)\right)^{\frac{1}{D'}} = e(g,g)^{kt\alpha^{K+1}}$$
$$= e\left(g^{\alpha^K}, g^{\alpha}\right)^{kt}$$
$$= e(g_K, g_1)^{kt}$$
$$= Key.$$

상기 사용자 단말의 복호화 모듈이 상기 복원된 대칭키(Key)를 이용하여 상기 대칭키 암호문(M_{Key})을 복호화하고 상기 메시지(M)를 추출하는,

클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 시스템.

청구항 8

제5항에 있어서,

상기 신뢰기관 서버가 상기 사용자 단말로부터 비밀키(SK_u)를 수신하여 키 온전성(key sanity)을 체크하고, 비밀키(SK_u)가 유출된 경우 유출된 비밀키(SK_u)를 이용하여 비밀키(SK_u)를 유출한 사용자의 ID(id_u)를 추적하는,

클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 장치 및 방법에 관한 것으로서, 특히, 사용자별 할당된 속성값을 기반으로 공유 데이터에 대한 접근제어를 지원하며 또한 사용자의 비밀키가 유출될 시 이를 탐지하는 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 본 발명은 속성의 개수에 관계없이 항상 일정 크기의 암호문을 보장하는 속성 기반 암호화를 이용한 클라우드 컴퓨팅 환경에서의 데이터 공유 기술을 제시한다.

[0003] ID 기반 암호는 특정한 ID를 기반으로 데이터를 암호화한다. 사용자가 해당 데이터를 복호하려면 ID가 일치해야 한다. 이는 다수 사용자 환경에서의 데이터 공유에 부적합하다. 속성 기반 암호는 다수의 속성(예, 학위, 나이, 성별, 직위 등)을 기반으로 데이터를 암호화한다. 사용자가 해당 데이터를 복호하려면 속성 별 조건(예, 석사학위 이상, 35세 미만, 남자, 대리급 이상)을 만족해야 한다. 이는 다수 사용자 환경에서의 데이터 공유에 적합하다. 하지만 대부분의 속성 기반 암호는 속성의 개수에 비례하여 데이터의 크기가 증가하기 때문에 스토리지 측면에서 비효율적이다. 사용자의 신원정보(예, ID)를 비밀키에 삽입함으로써, 추후 비밀키의 불법복제를 막는 기법이 존재하나, 비밀키로부터 신원정보를 복원함으로써 키 유출을 탐지하는데 부적합하다.

[0004] 또한, 클라우드 서버는 사용자의 ID를 기반으로 데이터에 대한 접근제어를 지원한다. 하지만 이러한 방법은 해당 ID를 가진 사용자만 데이터에 접근할 수 있다는 점에서, 다수 사용자를 대상으로 하는 데이터 공유에 적합하지 않다. 다수의 속성을 기반으로 세분화된 접근제어를 지원하는 기법들이 존재하지만, 기존 기법들은 대부분 속성의 개수에 비례하여 공유 데이터의 크기가 증가하기 때문에 스토리지 측면에서 비효율적이다. 데이터 공유 환경에서 악의적인 사용자는 자신의 비밀키를 불법적으로 유출함으로써, 권한이 없는 제3자가 데이터에 접근하게끔 할 수 있다.

[0005] 따라서, 클라우드 컴퓨팅 환경에서 발생할 수 있는 상기와 같은 문제점을 해결하기 위해 속성의 개수에 관계없이 공유 데이터의 크기를 일정하게 유지할 수 있고 유출된 비밀키를 이용하여 비밀키를 유출한 사용자의 신원을 추적할 수 있는 보다 효율적인 데이터 공유 기법이 필요하다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) KR 1464727 B1

(특허문헌 0002) KR 1593165 B1

(특허문헌 0003) US 8615668 B2

(특허문헌 0004) JP 5650630 B2

비특허문헌

[0007] (비특허문헌 0001) J. Li, K. Ren, Z. Wan, Privacy-aware attribute-based encryption with user accountability, Information Security. Springer Berlin Heidelberg, (2009) 347-362.

(비특허문헌 0002) Z. Liu, Z. Cao, D. Wong, White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures, Information Forensics and Security, IEEE Transactions on, (2013) 76-88.

(비특허문헌 0003) Z. Liu, Z. Cao, D. Wong, Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on ebay, Proceedings of the 2013 ACM SIGSAC conference on Computer communications security, 2013, pp. 475-486.

발명의 내용

해결하려는 과제

[0008] 본 발명이 이루고자 하는 기술적인 과제는 다양한 사용자 환경에서 데이터를 공유할 수 있는 속성 기반의 사용자 접근제어 및 비밀키 유출 탐지를 위한 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 방법 및 시스템을 제공하는 것이다.

과제의 해결 수단

[0009] 본 발명의 실시 예에 따른 복수의 사용자 단말, 클라우드 서버, 및 신뢰기관 서버를 포함하는 속성 기반 암호화를 이용한 데이터 공유 시스템에서의 속성의 개수에 관계없이 항상 일정 크기의 암호문을 보장하는 속성 기반 암호화를 이용한 데이터 공유 방법은, 신뢰기관 서버가 임의의 $g \in G_0$, α, $\gamma \in Z_p$를 선택하여 마스터키(MK) 및 공개키(PK)를 생성하는 셋업 단계, 상기 신뢰기관 서버가 상기 마스터키(MK), 상기 공개키(PK), 각각의 사용자(u)의 ID(id_u), 및 사용자(u)의 속성집합(L_u)을 입력으로 하고, k+2개의 임의의 a, $c \in Z_p^*$, $\{r_1, r_2, \cdots, r_k\} \in Z_p$를 선택하여 비밀키($SK_u$)를 생성하고 해당 사용자 단말에 전송하는 키 생성 단계, 상기 신뢰기관 서버가 상기 비밀키(SK_u) 생성을 위해 선택한 고유의 값(c) 및 상기 사용자(u)의 ID(id_u)를 전체 사용자 ID 테이블(T)에 저장하는 단계, 상기 복수의 사용자 단말 중 어느 하나가 메시지(M)를 상기 공개키(PK) 및 접근제어를 위한 속성집합(W)을 입력으로 암호화하여 암호문(CT)을 생성하고 암호문(CT)을 클라우드 서버에 전송하는 암호화 단계, 상기 복수의 사용자 단말 중 어느 하나가 클라우드 서버에 암호문(CT)을 요청하고, 클라우드 서버로부터 암호문(CT)을 수신하는 암호문 요청 단계, 상기 복수의 사용자 단말 중 어느 하나가 수신한 암호문(CT)을 복호화하여 메시지(M)를 추출하는 복호화 단계를 포함하되, 상기 암호화 단계는, 임의의 $t \in Z_p$를 선택하고 대칭키(Key)를 생성하는 과정, 상기 대칭키(Key)를 이용한 대칭키 암호문(M_{Key})을 생성하는 과정, 및 상기 공개키(PK), 상기 접근제어를 위한 속성집합(W), 상기 대칭키 암호문(M_{Key})을 입력하여 상기 암호문(CT)를 생성하는 과정을 포함한다.

[0010] 본 발명의 실시 예에 따른 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 시스템은 마스터키(MK), 공개키(PK), 및 각각의 사용자 ID에 대응하는 비밀키(SK_u)를 생성하고, 상기 마스터키(MK), 상기 공개키(PK), 상기 비밀키(SK_u), 및 전체 사용자 ID 테이블(T)을 관리하는 신뢰기관 서버, 네트워크를 통해 암호문(CT) 또는 부분복호값(A)을 송신하거나 암호문(CT) 또는 부분복호키($g_i^{D'}$)를 수신하는 통신부, 상기 암호문(CT) 저장하는 저장부, 및 상기 암호문(CT)에 대한 부분복호 요청을 수신한 경우 상기 암호문을 부분적으로 복호하여 부분복호값(A)을 계산하는 부분복호부를 구비한 클라우드 서버, 및 메시지(M)를 암호화하여 암호문(CT)을 생성하는 암호화 모듈, 암호문(CT)을 복호화하는 복호화 모듈, 및 네트워크를 통해 암호문(CT) 또는 부분복호키($g_i^{D'}$)를 송신하고, 암호문(CT) 또는 부분복호값(A)을 수신하는 통신 모듈을 구비한 복수의 사용자 단말을 포함하되,

[0011] 상기 신뢰기관 서버는 임의의 $g \in G_0$, α, $\gamma \in Z_p$를 선택하여 상기 마스터키(MK) 및 상기 공개키(PK)를 생성하고, 상기 마스터키(MK), 상기 공개키(PK), 각각의 사용자(u)의 ID(id_u), 및 사용자(u)의 속성집합(L_u)을 입력으로 하고, k+2개의 임의의 a, $c \in Z_p^*$, $\{r_1, r_2, \cdots, r_k\} \in Z_p$를 선택하여 상기 비밀키($SK_u$)를 생성하고, 상기 비밀키($SK_u$) 생성을 위해 선택한 고유의 값(c) 및 상기 사용자(u)의 ID(id_u)를 전체 사용자 ID 테이블(T)에 저장하며,

[0012] 상기 사용자 단말의 암호화 모듈은 임의의 $t \in Z_p$를 선택하여 대칭키(Key)를 생성하고, 상기 대칭키(Key)를 이용하여 대칭키 암호문(M_{Key})을 생성하며, 상기 공개키(PK), 접근제어를 위한 속성집합(W), 상기 대칭키 암호문(M_{Key})을 입력하여 상기 암호문(CT)를 생성한다.

발명의 효과

[0013] 본 발명의 실시 예에 따른 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 방법 및 시스템에 의할 경우, 다수의 속성 (예, 학위, 나이, 성별, 직위 등)을 기반으로 세분화된 접근제어 기법을 클라우드 환경에 적용함으로써, 다양한 사용자 환경에서 데이터를 공유할 수 있는 효과가 있다.

[0014] 또한, 본 발명의 실시 예에 따른 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 방법 및 시스템에 의할 경우, 속성의 개수에 관계없이 공유 데이터의 크기를 항상 일정하게 유지할 수 있다.

[0015] 또한, 본 발명의 실시 예에 따른 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 방법 및 시스템에 의할 경우, 유출된 비밀키를 이용하여 비밀키를 유출한 사용자의 신원을 추적할 수 있다.

도면의 간단한 설명

[0016] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 시스템의 개략도이다.

도 2는 도 1에 도시된 사용자 단말의 기능 블럭도이다.

도 3은 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 방법을 설명하기 위한 흐름도이다.

도 4는 도 3의 복호화 단계를 보다 세부적으로 도시한 도면이다.

도 5는 도 3의 추적 단계를 보다 세부적으로 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0017] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0018] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0019] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0020] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0021] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0022] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0023] 우선, 본 발명에서 이용하는 겹선형 함수(Bilinear Map)와 암호화 기법들을 설명한다. G와 G_T가 위수를 소수 p로 갖는 순환 군(group)이라 할 때, 아래와 같은 조건을 만족하는 함수 $e: G \times G \rightarrow G_T$ 를 겹선형 함수라 한다.

[0024] 겹선형성(Bilinearlity) : 임의의 $g \in G$ 와 $a, b \in Z_p^*$ 에 대하여 $e(g^a, g^b) = e(g, g)^{ab}$ 을 만족한다.

[0025] 비소실성(Non-degeneracy) : $e(g,g) \neq 1$을 $g \in G$ 만족하는 가 존재한다.

[0026] 계산 가능성(Computability) : 임의의 $g, h \in G$에 대해서 $e(g,h)$를 계산하는 효율적인 알고리즘이 존재한다.

[0027] 이하, 도 1 및 도 2를 참조하여, 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 시스템에 대해 상술한다.

[0028] 도 1은 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 시스템(10)을 도시하고, 도 2는 도 1에 도시된 사용자 단말의 기능 블럭도를 도시한다.

[0029] 도 1을 참조하면, 속성 기반 암호화를 이용한 데이터 공유 시스템(10)은 복수의 단말(100, 200, 300), 클라우드 서버(400), 신뢰기관 서버(500)를 포함한다.

[0030] 신뢰기관 서버(500)는 마스터키(MSK) 및 공개키(PK)를 생성할 수 있다. 또한, 신뢰기관 서버(500)는 마스터키(MSK), 공개키(PK), 사용자 u의 속성집합(L_u), 및 사용자 u의 ID(ID_u)를 입력으로 하여, 각각의 사용자에 대응하는 비밀키(SK_u)를 생성할 수 있다.

[0031] $$\mathbf{KeyGen}(\mathrm{MK}, \mathrm{PK}, L_u, id_u) \rightarrow (\mathrm{SK}_u)$$

[0032] 비밀키(SK_u)는 해당 사용자의 단말에 전송한다. 신뢰기관 서버(500)는 비밀키(SK_u) 생성을 위하여 선택한 임의의 값 c를 상기 비밀키(SK_u)와 함께 전체 사용자 ID 테이블(T)에 저장한다.

[0033] 신뢰기관 서버는 주기적으로 사용자 단말로부터 비밀키(SK_u)를 수신하여 키 온전성(key sanity)을 체크하고, 비밀키(SK_u)가 유출된 경우 유출된 비밀키(SK_u)를 이용하여 비밀키(SK_u)를 유출한 사용자의 ID(id_u)를 추적한다.

[0034] 각각의 사용자 단말(100, 200, 300)은 네트워크 망을 통하여 클라우드 서버(400) 또는 신뢰기관 서버(500)와 통신할 수 있다. 일 실시예에 따른 네트워크 망은, 개방형 인터넷, 폐쇄형 인트라넷을 포함한 유선 인터넷망, 이동 통신망과 연동된 무선 인터넷 통신망뿐만 아니라, 각종 데이터 통신이 가능한 컴퓨터 네트워크 등의 가능한 통신 수단을 포함하는 넓은 개념이다.

[0035] 사용자 단말(100, 200, 300) 중 하나 이상의 단말은 데이터(M, 메시지)을 암호화하여 암호문(CT)를 생성하고, 암호문(CT)을 클라우드 서버(400)에 전송하여 저장한다.

[0036] 사용자 단말(100, 200, 300) 중 하나 이상의 단말은 클라우드 서버(400)에 암호문(CT)를 요청하고, 클라우드 서버(400)로부터 수신한 암호문(CT)을 복호화하여 메시지(M)를 추출한다.

[0037] 사용자 단말이 클라우드 서버(400)에 암호문(CT)을 요청하는 동안, 사용자 단말은 클라우드 서버(400)에 부분적 복호(Partial Decryption)를 요청할 수 있다.

[0038] 클라우드 서버(400)는 일부 복호화된 제1 복호값(A)을 계산하여 사용자 단말에 전송하고, 사용자 단말은 제2 복호값(B)을 계산한다. 사용자 단말은 제2 복호값(B) 및 클라우드 서버(400)로부터 수신한 제1 복호값(A)을 이용하여 나머지 복호화를 수행하고 메시지(M)을 추출한다.

[0039] 클라우드 서버가 A를 계산하여 사용자 단말에 송신하는 경우, 통신 비용(communication cost)을 절감할 수 있는 효과 및 계산 시간을 단축할 수 있는 효과가 있다.

[0040] 클라우드 서버(400)는 네트워크를 통해 암호문(CT) 또는 부분복호값(A)을 송신하거나 암호문(CT) 또는 부분복호키($g_i^{D'}$)를 수신하는 통신부, 상기 암호문(CT) 저장하는 저장부, 및 상기 암호문(CT)에 대한 부분복호 요청을 수신한 경우 상기 암호문을 부분적으로 복호하여 부분복호값(A, 또는 '제1 복호값'이라 함)을 계산하는 부분복호부를 포함한다.

[0041] 도 2를 참조하면, 사용자 단말(100, 200, 300)은 암호화 모듈(110), 복호화 모듈(130), 통신 모듈(170), 메모리(180), 및 제어 모듈(190)을 포함한다.

[0042] 본 명세서에서 사용되는 모듈이라 함은 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를

구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 모듈은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나 한 종류의 하드웨어를 의미하는 것은 아니다.

[0043] 사용자 단말의 암호화 모듈(110)은 제어 모듈(190)의 제어 하에, 암호화 알고리즘을 수행하여 메시지(M)를 암호화한다. 이때, 암호화 모듈(110)은 공개키(PK), 접근제어를 위한 속성집합(W), 및 메시지(M)를 입력으로 하여, 암호문(CT)를 생성한다.

[0044] $$\mathbf{Encrypt}(\mathrm{PK}, W, M) \rightarrow (CT)$$

[0045] 사용자 단말의 복호화 모듈(130)은 제어 모듈(190)의 제어 하에, 복호화 알고리즘을 수행하여 클라우드 서버(400)로부터 수신된 암호문(CT)을 복호화한다. 복호화 모듈(130)은 공개키(PK), 사용자의 비밀키(SK_U), 및 암호문(CT)을 입력으로 하여, 메시지(M) 혹은 복호실패($\perp$)를 반환한다.

[0046] $$\mathbf{Decrypt}(\mathrm{PK}, \mathrm{SK}_u, CT) \rightarrow M \text{ or } \perp.$$

[0047] 사용자 단말의 통신 모듈(170)은 제어 모듈(190)의 제어 하에, 클라우드 서버(400) 또는 신뢰기관 서버(500)와 유선 또는 무선 통신망을 통하여 통신을 수행할 수 있다. 예를 들어, 통신 모듈(170)은 네트워크를 통해 클라우드 서버(400)에 암호문(CT) 또는 부분복호키($g_i^{D'}$)를 송신하고, 클라우드 서버(400)로부터 암호문(CT) 또는 부분복호값(A)을 수신할 수 있다. 또한, 신뢰기관 서버(500)에서 키 온전성 체크를 요청하는 경우 신뢰기관 서버(500)에 사용자의 비밀키(SK_u)를 송신할 수 있다.

[0048] 사용자 단말의 메모리(180)는 프로그램 메모리와 데이터 메모리를 포함할 수 있다. 상기 프로그램 메모리에는 제1 단말(100)의 동작을 제어하기 위한 프로그램들이 저장될 수 있다. 상기 데이터 메모리에는 상기 프로그램들을 수행하는 과정 중에 발생하는 데이터들이 저장될 수 있다.

[0049] 사용자 단말의 제어 모듈(190)은 사용자 단말의 전반적인 동작을 제어한다. 즉, 암호화 모듈(110), 복호화 모듈(130), 통신 모듈(170), 및 메모리(180)의 동작을 제어할 수 있다.

[0050] 이하, 도 3 내지 도 5를 참조하여, 본 발명의 일 실시예에 따른 기반 데이터 공유 시스템을 이용한 사용자별 할당된 속성값을 기반으로 공유 데이터에 대한 접근제어를 지원하고 사용자의 비밀키가 유출될 시 이를 탐지하는 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 방법에 대하여 자세히 살펴보도록 한다.

[0051] 도 3은 도 1에 도시한 기반 데이터 공유 시스템을 이용한 클라우드 컴퓨팅 환경에서의 속성 기반 암호화를 이용한 데이터 공유 방법을 설명하기 위한 흐름도이다. 도 4는 도 3의 복호화 단계(S400)를 보다 세부적으로 도시한 도면이고, 도 5는 도 3의 탐색 단계(S500)를 보다 세부적으로 도시한 도면이다.

[0052] 본 발명에서 사용자는 다음과 같은 k개의 속성 $\{A_1, A_2, \cdots, A_k\}$ 을 가지며, 각각의 속성은 $A_i \in \{A_i^+, A_i^-, A_i^*\}$ 와 같이 세 가지 유형의 값 중 하나를 가진다. 예를 들어, +로 표기된 속성은 사용자가 해당 속성(A_i)을 가지고 있음을 나타내고, -로 표기된 속성은 사용자가 해당 속성(A_i)을 갖고 있지 않거나 해당 속성(A_i)이 사용자의 적절한 속성이 아님을 나타낸다. *로 표기된 속성은 사용자가 해당 속성에 무관함을 의미한다.

[0053] *셋업 단계*

[0054] 사용자 단말이 메시지(M)에 관한 암호문(CT)를 생성하기 위한 사전 단계로, 신뢰기관 서버(500)는 k를 입력으로 하여, 임의의 $g \in \mathbb{G}_0$, $\alpha, \gamma \in \mathbb{Z}_p$ 를 선택하여 마스터키(MK)와 공개키(PK)를 각각 생성한다(S100).

[0055] $$\mathbf{Setup}(k) \rightarrow (\mathrm{MK}, \mathrm{PK})$$

[0056] $$\mathrm{MK} = (\alpha, \gamma)$$

[0057] $$\mathrm{PK} = (g, g_1, \cdots, g_K, g_{K+2}, \cdots, g_{2K}, v) \in \mathbb{G}_0^{2K+1}$$

[0058] *키 생성 단계*

[0059] 신뢰기관 서버는 마스터키(MK), 공개키(PK), 사용자 u의 속성집합(L_u), 그리고 사용자 u의 ID(id_u)를 입력으로 하고, k+2개의 임의의 $a, c \in \mathbb{Z}_p^*, \{r_1, r_2, \cdots, r_k\} \in \mathbb{Z}_p$ 를 선택하여 아래와 같이 비밀키(SK_u)를 생성한다(S200).

[0060] $$\mathbf{KeyGen}(\mathrm{MK}, \mathrm{PK}, L_u, id_u) \rightarrow (\mathrm{SK}_u)$$

[0061] $$\mathrm{SK}_u = (D = g^{\frac{r\gamma}{a+c}}, \{D_i | i \in \{L_u^+, L_u^-, L_u^*\}\}, D' = c, D'' = g^r, D''' = g^a).$$

[0062] 이때, $D_i = g^{\gamma(c\alpha^i + \frac{r_i'}{a+c})}$ 을 만족한다.

[0063] 비밀키(SK_u)는 해당 사용자에게 발급되고, (c, id_u) 은 전체 사용자 ID 테이블(T)에 저장된다.

[0064] 비밀키(복호화키)에 고유한 값(c)을 추가하여 복호 권한을 불법적으로 공유하는 경우 사용자의 식별 가능한 정보를 찾을 수 있도록 한다.

[0065] *암호화 단계*

[0066] 복수의 사용자 단말(100, 200, 300) 중 어느 하나의 사용자 단말에서 메시지(M)를 암호화하여 암호문(CT)을 생성한다(S300). 사용자 단말에서 생성된 암호문(CT)은 클라우드 서버(400)에 전송한다.

[0067] 사용자 단말은 공개키(PK), 접근제어를 위한 속성집합(W)을 이용하여 암호문(CT)을 생성한다.

[0068] 구체적으로, 임의의 $t \in \mathbb{Z}_p$ 를 선택하고, 아래와 같이 대칭키(Key, 일회성 대칭키)를 생성한다.

[0069] $$Key = e(g_K, g_1)^{kt}$$

[0070] 다음, 아래와 같이 암호문(CT)를 생성한다.

[0071] $$\mathbf{Encrypt}(\mathrm{PK}, W, M) \rightarrow (CT)$$

[0072] $$CT = \left(W, M_{Key}, C_0 = g^t, C_1 = \left(v \prod_{j \in W} g_{K+1-j}\right)^t\right)$$

[0073] 이때, M_{Key} 는 일반적인 대칭키 암호를 이용한 대칭키 암호문($\{M\}_t^{Key}$)을 의미한다.

[0074] *복호화 단계*

[0075] 사용자 단말은 클라우드 서버(400)에 암호문(CT)을 요청하고, 클라우드 서버(400)로부터 암호문(CT)을 수신한다. 클라우드 서버(400)로부터 암호문(CT)을 수신한 사용자 단말은 상기 암호문(CT)을 복호화하여 메시지(M)를 추출한다(S400).

[0076] 먼저 사용자 단말은 사용자의 속성집합(L_u)이 접근제어를 위한 속성집합(W)을 만족하는지 판단한다. 사용자의 속성집합(L_u)이 접근제어를 위한 속성집합(W)을 만족하지 않는다면, 복호실패 $\perp$을 반환한다. 사용자의 속성집합이 접근제어를 위한 속성집합을 만족한다면, 암호문(CT)을 복호하여 메시지(M)를 추출한다.

[0077] $$\mathbf{Decrypt}(\mathrm{PK}, \mathrm{SK}_u, CT) \rightarrow M \text{ or } \perp.$$

[0078] 암호문(CT)을 복호하기 위하여, 사용자 단말은 모든 $\forall i \in W$ 에 대하여 아래와 같이 A_i를 계산한다.

[0079]
$$A_i = e\left(g_i^{D'}, C_1\right)$$
$$= e\left(g, \left(v \prod_{j \in W} g_{K+1-j}\right)\right)^{\alpha^i t D'}$$

[0080]
$$= e\left(g, g^{\gamma + \sum_{j \in W} \alpha^{K+1-j}}\right)^{\alpha^i t D'}$$
$$= e\left(g, g\right)^{\alpha^i t D' \gamma + t D' \sum_{j \in W} \alpha^{K+1-j+i}}$$

[0081] 다음, 사용자 단말은 아래와 같이 B_i를 계산한다.

[0082]
$$B_i = e\left(C_0, \left(\prod_{j \in W, j \neq i} g_{K+1-j+i}\right)^{D'} \cdot D_i\right)$$
$$= e\left(g, g\right)^{t D' \sum_{j \in W, j \neq i} \alpha^{K+1-j+i} + t\gamma\left(D' \alpha^i + \frac{r_i}{a+c}\right)}$$

[0083] 다음, 사용자 단말은 아래와 같이 A_i/B_i를 계산한다.

[0084]
$$\frac{A_i}{B_i} = e(g,g)^{D' t \alpha^{K+1} - \frac{\gamma t r_i}{a+c}}$$

[0085] 다음, 사용자 단말은 아래와 같이 A/B를 계산한다.

[0086]
$$\frac{A}{B} = \prod_{i \in W} \frac{A_i}{B_i}$$
$$= e(g,g)^{D' k t \alpha^{K+1} - \frac{\gamma t r}{a+c}}$$

[0087] 또는, 사용자 단말을 제1 복호값(A) 및 제2 복호값(B)을 계산하여 A/B를 계산한다.

[0088] 다음, 사용자 단말은 아래의 식을 계산하여 대칭키(Key)를 복원한다.

[0089]
$$\frac{A}{B} \cdot e\left(D, C_0\right) = \frac{A}{B} \cdot e\left(g^{\frac{\gamma r}{a+c}}, g^t\right)$$
$$= e(g,g)^{D' k t \alpha^{K+1}}.$$

[0090]
$$\left(\frac{A}{B} \cdot e\left(D, C_0\right)\right)^{\frac{1}{D'}} = e(g,g)^{k t \alpha^{K+1}}$$
$$= e\left(g^{\alpha^K}, g^{\alpha}\right)^{kt}$$
$$= e\left(g_K, g_1\right)^{kt}$$
$$= Key.$$

[0091] 대칭키(Key)를 복원한 후, 대칭키 암호문 M_{Key} 를 복호하여 메시지(M)을 추출한다.

[0092] 이때, 제1 복호값(A)는 클라우드 서버(400)에서 계산할 수 있다(도 4 참고). 즉, 클라우드 서버(400)가 사용자 단말을 대신하여 암호문을 부분적으로 복호화할 수 있다. 본 발명에서의 $g_i^{D'}$ 는 공개적으로 알려져 있고 다른

암호문에도 재사용될 수 있다. 따라서, 사용자 단말이 클라우드 서버(400)에 암호문(CT)을 요청(S410)하는 동안 상기 사용자 단말이 부분복호키($g_i^{D'}$) 클라우드 서버(400)로 보내면서 클라우드 서버(400)에서의 부분 복호를 요청(S420)하는 경우 클라우드 서버(400)는 사용자를 대신하여 A_i 및 제1 복호값(A)을 계산할 수 있다.

[0093] $$A = \prod_{i \in W}$$

[0094] 사용자 단말은 클라우드 서버(400)로부터 제1 복호값(A)를 수신하고, 제2 복호값(B)를 계산하여, 나머지 복호화를 수행하고 메시지(M)을 추출한다(S430).

[0095] $$B = \prod_{i \in W}$$

[0096] 클라우드 서버가 제1 복호값(A)를 계산하여 사용자 단말에 송신하는 경우, 통신 비용(communication cost)을 절감할 수 있는 효과 및 계산 시간을 단축할 수 있는 효과가 있다.

[0097] *추적 단계*

[0098] 신뢰기관 서버(500)는 공개키(PK), 사용자 단말로부터 수신한 비밀키(SK_u), 전체 사용자 ID 테이블(T)를 입력으로 하여 원래 키 소유자의 ID를 추적한다(S500). 키 신뢰도를 주기적으로 요청하는 신뢰기관 서버(500)가 주기적으로 키 온전성 체크(key sanity check)를 요청하고, 사용자 단말을 이에 응답한다. 구체적인 추적 방법은 아래와 같다.

[0099] 도 5에 도시된 바와 같이, 먼저, 신뢰기관 서버(500)가 사용자 단말에 키 온전성 체크(key sanity check)를 요청(S510)한다. 사용자 단말은 신뢰기관 서버(500)의 요청에 대한 응답으로 비밀키(SK_u, 사용자키)를 신뢰기관 서버(500)에 전송(S520)한다. 다음, 신뢰기관 서버(500)는 수신한 비밀키(SK_u)를 확인하고 원래 키 소유자의 ID를 추적(S530)한다.

[0100] 신뢰기관 서버(500)는 공개키(PK), 사용자 단말로부터 수신한 비밀키(SK_u), 전체 사용자 ID 테이블(T)를 입력으로 하여 아래와 같이 원래 키 소유자의 ID를 추적한다.

[0101] $$\mathbf{Trace}(\mathrm{PK}, \mathrm{SK}_u, T) \rightarrow id_u \text{ or } \top$$

[0102] 본 발명에 따른 추적 방법은 사용자 속성을 자주 수정하는 경우에 적합하다. 예를 들어, 온라인 소셜 네트워크에서 사용자는 소셜 연락처에 다른 속성 및 키를 할당하여 그룹을 만든 다음 지정된 속성에 따라 액세스 정책을 지정한다. 이때, 그룹은 동적이므로 사용자 속성은 시간이 지남에 따라 변경된다.

[0103] 비밀키(SK_u)가 불법적으로 공유되었는지 여부는 비밀키(SK_u)가 잘 형성되었는지 여부를 확인하여 비밀키(SK_u)가 정당한 키 생성 단계(KeyGen)를 통한 실제 출력임을 나타냄으로써 결정한다.

[0104] 아래의 수식을 만족하면, 비밀키(SK_u)가 잘 형성된 것으로 판단한다.

[0105] $$D' \in \mathbb{Z}_p^*, D, D_i, D'' \in \mathbb{G}_0^{2K+1},$$
$$e\left(D''' \cdot g^{D'}, D\right) = e\left(v, D''\right) \neq 1.$$

[0106] 만약 상기 수식을 만족한다면, 신뢰기관 서버(500)는 전체 사용자 ID 테이블(T)에서 D'를 탐색한 후, 최종적으로 id_u를 반환한다. 즉, 잘 형성된 비밀키(SK_u)로 확인된 경우 신뢰기관 서버(500)는 해당 비밀키(SK_u)에 상응하는 id_u를 출력한다. 이때, 신뢰기관 서버(500)와 통신하는 사용자 단말의 아이디가 출력된 아이디와 일치하지 않는다면, 해당 비밀키가 유출되었다고 판단한다.

[0107] 만약 상기 수식을 만족하지 않는다면, 신뢰기관 서버(500)는 비밀키(SK_u)에 대한 탐색을 중지하고 탐색실패($\top$)를 반환한다. 이 경우, 신뢰기관 서버(500)는 사용자 단말이 전송한 비밀키가 키 생성 단계(KeyGen)에 의해 만들어진 것이 아니라 무작위로 생성한 값이며, 따라서 해당 사용자 단말은 합법적 사용자가 아니라고

판단한다.

[0108] 올바른 형식의 암호 해독 키(비밀키)는 올바르게 구성된 암호 해독 프로세스에서 올바르게 작동한다는 것을 보증한다.

[0109] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0110] 10 : 속성 기반 암호화를 이용한 데이터 공유 시스템

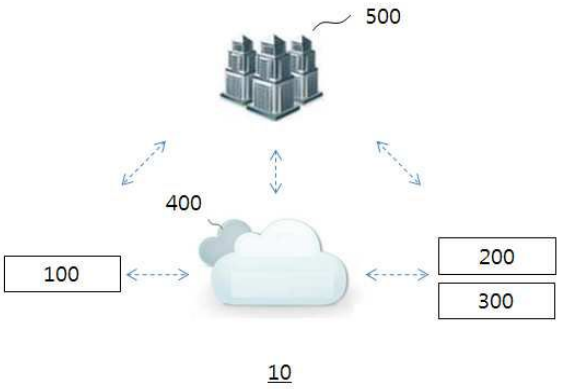
100, 200, 300 : 사용자 단말

400 : 클라우드 서버

500 : 신뢰기관 서버

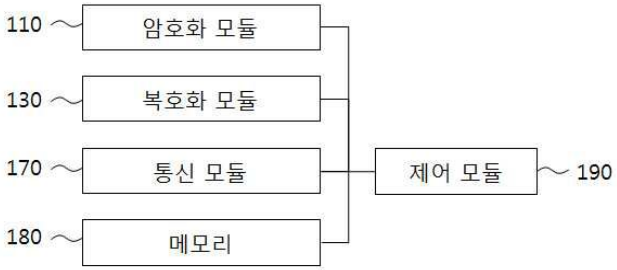
도면

도면1



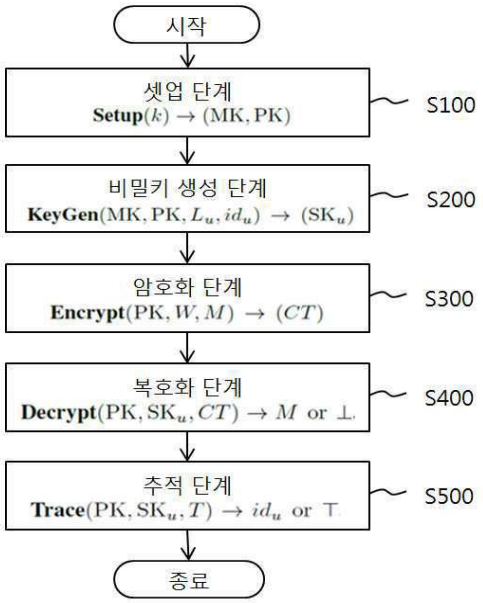
10

도면2

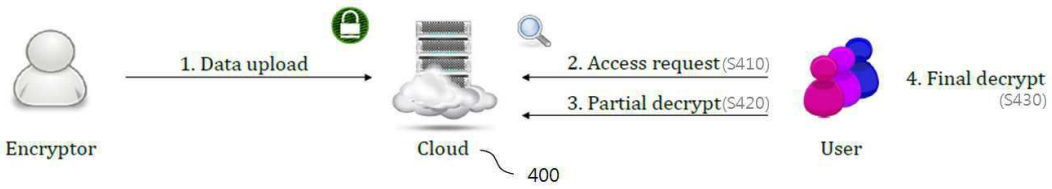


100

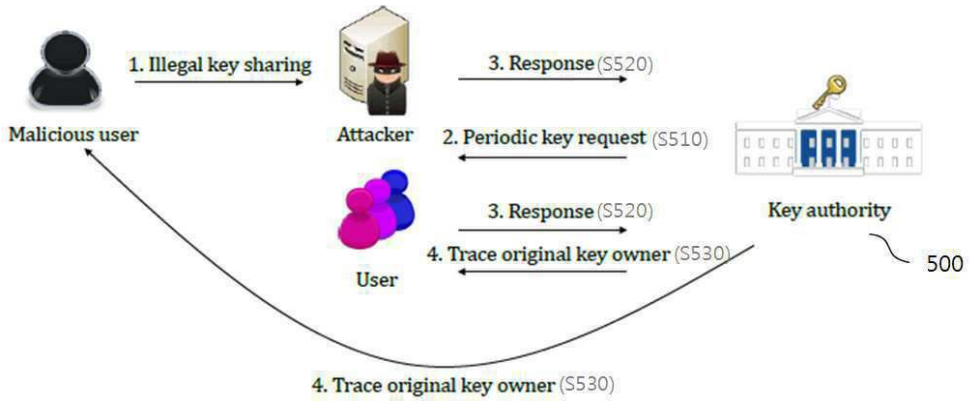
도면3


시작
셋업 단계
Setup(k) → (MK, PK)
S100
비밀키 생성 단계
KeyGen(MK, PK, L_u, id_u) → (SK_u)
S200
암호화 단계
Encrypt(PK, W, M) → (CT)
S300
복호화 단계
Decrypt(PK, SK_u, CT) → M or ⊥
S400
추적 단계
Trace(PK, SK_u, T) → id_u or ⊤
S500
종료

도면4


1. Data upload
2. Access request (S410)
3. Partial decrypt (S420)
4. Final decrypt
(S430)
Encryptor
Cloud
400
User

도면5


1. Illegal key sharing
3. Response (S520)
Malicious user
Attacker
2. Periodic key request (S510)
Key authority
3. Response (S520)
4. Trace original key owner (S530)
User
500
4. Trace original key owner (S530)