Multi Authority Attribute-Based Encryption 시스템에서 탈중앙화된 보증금 관리 프로토콜을 이용한 공모공격의 방지

노시완*, 장설아**, 이경현***

*부경대학교 일반대학원 정보보호학과

**부경대학교 일반대학원 인공지능융합학과

***부경대학교 IT융합응용공학과

nosiwan@pukyong.ac.kr, seolahh1020@gmail.com, khrhee@pknu.ac.kr

A Security Deposit Protocol to Prevent Collusion Attacks in the Multi-Authority Attribute-Based Encryption System

Siwan Noh*, SeolAh Jang**, and Kyung-Hyune Rhee***

*Department of Information Security, Graduate School, Pukyong National University

**Department of Interdisciplinary Graduate Program of Artificial Intelligence on Computer, Pukyong National University

***Department of IT Convergence and Application Engineering, Pukyong National University

요 약

속성기반암호는 특유의 유연성으로 다양한 환경에서 활용되고 있는 암호 기술이다. 다중기관 속성기반암호 시스템은 여러 기관이 사용자의 속성을 발급 및 관리하는 모델로 사용자는 여러 기관에 속하면서 각 기관으로부터 속성을 발급받아 시스템에서 사용한다. 전통적인 다중기관모델에서의 공모공격 방지는 중앙관리기관으로부터 사용자마다 고유한 정보를 발급받아 키 생성에 사용하여 다른 사용자 간의 공모를 원천적으로 차단하고 있으나 이로 인해 중앙관리기관에 대한 의존성이 문제가 된다. 본 논문에서는 중앙기관에 의존하지 않고 사용자 스스로 보증금을 등록하고 이 보증금을 출금하기 위한 정보가 공모공격에서 노출되도록 하여 합리적인 사용자로 하여금 공모공격의 동기를 잃도록 하는 방법을 제안한다.

I. 서론

속성기반암호(Attribute-Based Encryption, ABE)[1]는 암호화 통신을 위해 수신자를 특정할 필요가 없어 기존의 일대일 암호통신 기법보다 유연하게 활용이 가능한 암호기술이다. 메시지 송신자는 수신자의 고유한 정보 대신 수신자의 속성(소속, 직위 등)를 사용하여 암호화를 수행하고 해당 속성을 가진 사용자들은 누구나 암호문을 복호화할 수 있다. 사용자의 속성은 사용자가 소속된 기관에서 속성을 검증하고 사용자가 보유하고 있는 속성의 집합에 해당하는 비밀키를 생성함으로서 관리되어진다. 단일기관(Single Authority) ABE에서는 하나의 기관이 모든 사용자의 속성을 관리하지만 다중기관(Multi Authority) ABE에서는 각 기관이 각자의 속성들을 관리하고 사용자에게 발급한다. 즉, 사용자는 여러 기관에 속해서 각 기관들로부터 서로 다른 혹은 동일하지만 발급 주체가 다른 속성과 이에 해당하는 비밀키를 발급받아 사용하게 된다.

공모공격(Collusion Attack)은 여러 사용자 혹은 기관들이 공모하여 개인이 보유한 속성만

으로는 복호화할 수 없는 암호문을 복호화하거나 검증되지 않은 속성의 비밀키를 생성하는 등 악의적인 목적으로 자신이 가진 키를 공유하는 공격이다. 현재 사용되는 대부분의 다중기관 ABE 모델에서는 사용자 간의 공모공격을 방지하기 위해서 사용자 비밀키의 생성과정에서 사용자마다 서로 다른 고유한 비밀 값을 사용하여 공모공격을 방지한다[2]. 하지만 비밀 값을 결정하는 중앙기관(CA)의 단일 장애점 문제(Single point of failure) 및 사용자와 CA가 공모하여 다른 사용자의 비밀키를 생성할 수 있는 등 많은 한계가 존재한다[3].

본 논문에서는 기존 CA가 사용자마다 고유하게 결정하던 비밀값을 사용자가 스스로 결정하게 하되 이로 인해 발생할 수 있는 사용자의 악의적인 행동을 방지하기 위한 보증금 프로토콜을 제안한다.

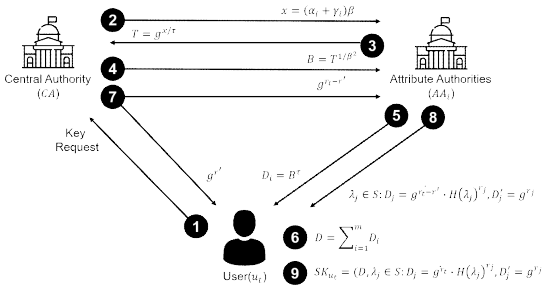
II.제안 모델

2.1 시스템 모델

Hur는 [4]에서 CA와 각 속성 발급기관들이 공동으로 사용자의 키생성 알고리즘을 수행하는 분산된 속성기반암호 모델을 제시하였다. 이 장에서는 Hur의 모델에 보증금 프로토콜을 적용하여 사용자의 공모공격 참여를 회피할 수 있는 모델을 제안한다. 제안 모델에서 고려하는 위협 모델은 다음과 같다.

- **사용자들 간**의 공모: 사용자들은 자신이 가진 속성키를 대가를 받고 공격자에게 공유할 수 있다. 공격자는 공유받은 속성키로 현재 가진 속성으로는 복호화할 수 없는 암호문을 복호화할 수 있다.
- **사용자와 CA**의 공모: CA는 이미 비밀키를 발급받은 사용자로부터 키를 공유받아 제3의 다른 사용자의 비밀키를 속성발급기관의 참여 없이 생성할 수 있다.

제안 모델의 핵심 개념은 Hur의 모델(그림 1)의 키생성 과정에서 CA가 사용자마다 고유하게 결정하던 값인 $r_t = \sum_{i=1}^{m} \gamma_i$를 사용자가 스스로 선택하는 것이다. 선택한 값을 CA가 알지 못하는 환경에서 사용자, CA, 그리고 각 속성 발급기관들이 협력하여 사용자의 비밀키를 생성한다. 하지만 사용자가 자신이 가진 값 r_t를 공모공격에 사용하지 않음을 보장할 수 없다는 문제가 발생한다.



[그림 1] [4]의 키 생성 프로세스

2.2 제안 모델

본 논문에서는 2.1절의 두 가지의 공모공격에 대한 저항성을 보장하기 위한 방법으로 블록체인 스마트계약을 사용한 보증금 프로토콜을 사용한다. 사용자는 시스템에 참여하기 전에 스마트계약에 보증금을 납부한다. 보증금은 사용자가 지정한 어떤 값에 대한 지식을 보임으로서 출금할 수 있다. 만약 사용자가 공모공격에 참여할 경우 공격과정에서 상대방에게 노출하는 값으로 상대방은 공모자의 보증금을 출금할 수 있게 된다. 시스템의 모든 참여자가 합리적인 선택을 하고 공모공격의 참여자들이 서로 신뢰하는 관계가 아니라고 가정할 때 제안 방법을 통해 공모공격을 회피하는 것이 가능하다. 자세한 보증금 프로토콜은 다음과 같다.

(1) 사용자는 CA에게 키생성을 요청한다.

(2) CA는 보증금 관리를 위한 스마트계약의 주소를 사용자에게 전달한다.

(3) 사용자는 랜덤한 $r_t = \sum_{i=1}^{m} \gamma_i$를 선택하고 hvalue$= H(r_t)$를 계산한다($H$는 해시함수).

(4) 계산한 hvalue와 함께 보증금을 스마트계약에 제출한다(스마트계약은 그림 2의 출금 알고리즘과 같이hvalue의 Pre-image를 출금을 위한 조건으로 설정한다).

(5) 스마트계약에 보증금이 등록된 후 사용자, CA, 그리고 각 속성발급기관은 다자간계산(Multi-party computation)을 사용하여 Hur 모델의 키생성 과정을 수행한다(여기서 사용자의 입력값은 r_t, CA와 각 속성발급기관의 입력은 각자의 마스터키이다).

withdraw($\mathcal{D}_U$, SC, proof, addr$_x$)

If SC.hvalue ≠ H(proof) return 0
SC.setstate(closed)
return Send($\mathcal{D}_U$, addr$_x$)

[그림 2] 보증금 출금 알고리즘

2.3 공모공격 저항성

- **사용자들 간**의 공모: 공격자 A와 B는 속성키를 결합하기 위해 동일한 값 $r_A = r_B$를 각각 CA와의 키 생성에 사용할 수 있다. 현실적인 가정에서 공모공격을 원하는 사용자들이 공격에 필요한 속성을 모두 가지고 있기는 어렵기 때문에 필요한 속성을 지닌 사용자에게 대가를 지불하고 속성키의 공유를 요청할 것이다. 하지만 이 경우 두 사용자의 보증금을 출금하기 위한 조건이 동일한 값으로 설정되어 상대에게 보증금이 노출될 수 있어 공격이 성사되지 않을 것이다.
- **사용자와 CA**의 공모: Hur 모델에서 CA는 속성발급 기관의 참여없이 임의 사용자의 비밀키를 생성하기 위해서 시스템의 사용자로부터 사용자의 비밀키를 전달받아 다음과 같이 키생성에 필요한 속성발급기관의 비밀정보(g^{α})를 추출할 수 있다. 제안 모델에서는 CA가 선택하던 r_t를 사용자의 비밀정보로 설정하여 CA와 공모하기 위해서는 이 비밀정보를 CA에게 노출해야하므로 보증금이 노출될 수 있어 공격이 성사되지 않을 것이다.

$$D^{\beta}/g^{r_t} = \left(g^{\frac{(\alpha_1+\ldots+\alpha_m)+r_t}{\beta}}\right)^{\beta} \times g^{-r_t} = g^{(\alpha_1+\ldots+\alpha_m)+r_t+(-r_t)} = g^{(\alpha_1+\ldots+\alpha_m)}$$

III. 결론

본 논문에서는 다중기관 속성기반암호 시스템에서 공모공격을 방지하기 위한 새로운 방법을 제시하였다. 전통적인 방법은 신뢰하는 CA에 의존하였으나 제안 방법은 사용자 개인의 이익을 위해 스스로 정직하게 행동하게 하는 방법으로 탈중앙화라는 기존 연구의 방향에 적합하다.

[사사표기]

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업의 연구결과로 수행되었음(2020-0-01596)

[참고문헌]

[1] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in AnnualInternational Conference on the Theory and Applications of CryptographicTechniques. Springer, 2005, pp. 457

[2] M. Chase, “Multi-authority attribute based encryption,” in Theory of cryp-tography conference. Springer, 2007, pp. 515 - 534.

[3] E. Meamari, H. Guo, C.-C. Shen, and J. Hur, “Collusion Attacks on De-centralized Attributed-Based Encryption: Analyses and a Solution,” arXivpreprint arXiv:2002.07811, 20

[4] J. Hur and K. Kang, “Secure data retrieval for decentralized disruption-tolerant military networks,” IEEE/ACM transactions on networking, vol. 22,no. 1, pp. 16 - 26, 2012, publisher: IEE