ID 기반 프록시 재암호화 환경에서 공모공격 방지를 위한 기술+

김원빈, 이임영
순천향대학교 컴퓨터학과
e-mail:[wbkim29, imylee]@sch.ac.kr

Scheme for Preventing Attacks in ID-based Proxy Re-Encryption Environments

Won-Bin Kim, Im-Yeong Lee
Dept of Computer Science and Engineering, Soonchunhyang University

요 약

클라우드 스토리지는 다양한 영역에서 이용가능하다. 일반적으로 데이터 저장, 이용에 사용되지만 추가적으로 데이터의 공유에 이용될 수도 있다. 이를 활용하여 단순 데이터 공유 및 데이터 구독 서비스 등 다양한 영역에 이용될 수 있다. 프록시 재암호화는 이러한 환경에서 데이터를 제 3자에게 안전하게 전달하기 위해 제안되었다. 프록시 재암호화는 데이터 소유자가 데이터를 암호화 한 뒤, 프록시에 보관하고, 위임자의 요청에 따라 데이터 소유자가 재암호화 키를 생성하여 프록시가 암호화된 데이터를 재차 암호화 할 수 있도록 한다. 프록시 재암호화는 암호화된 데이터를 제 3자에게 전달하기 위해 복호화 할 필요가 없기 때문에 데이터 원본을 노출 없이 안전하게 전달할 수 있다. 하지만 이러한 과정에서 프록시와 위임자가 결탁하여 데이터 소유자의 개인키를 복구하거나 재암호화 키를 위조하는 등의 위협이 발생할 수 있다. 이를 공모(결탁)공격이라 한다. 본 연구에서는 프록시 재암호화 기술에서 발생할 수 있는 공모공격을 방지하여, 보다 안전하게 이용할 수 있는 방법을 제시한다.

1. 서론

프록시 재암호화는 프록시 서버를 이용하여 데이터를 공유할 수 있는 기술이다. 프록시 재암호화는 프록시에 암호화된 데이터를 저장한 뒤, 프록시가 저장된 데이터를 재암호화하여 제 3자가 복호화할 수 있도록 권한을 위임하는 기술이다. 이러한 프록시 재암호화 기술은 다양한 형태가 제시되었으며, 각 형태별로 재암호화 방법 및 재암호화 키 생성 방법 등이 상이하다. 이 중 ID 기반 프록시 재암호화는 사용자의 공개키를 ID로 사용하여 재암호화 키를 생성하는 방법이다. 따라서 데이터 소유자는 데이터의 복호화 권한을 수신할 위임자를 특정할 수 있어야 한다. 그리고 재암호화 키를 생성하는 과정에서 위임자의 ID를 사용하기 때문에 위임자의 ID인 공개키와 쌍을 이루는 개인키를 소유하지 않으면 재암호화된 데이터를 복호화 할 수 없다. 따라서 소유자가 위임자에게 데이터를 전달하는 과정에서 데이터 원본이 노출되지 않는다. 하지만 ID 기반 중복제거 기술에서 소유자의 개인키를 복구하거나, 재암호화 키를 위조하는 공모(결탁)공격의 위협이 제시되었다.

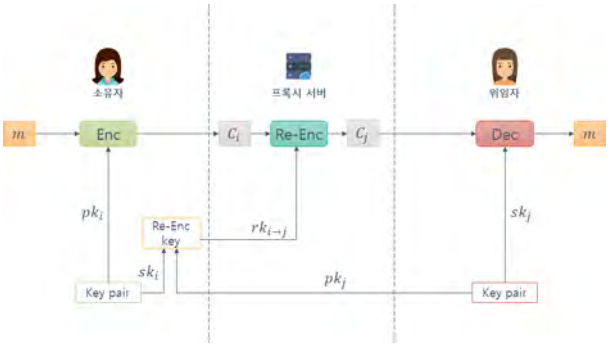
공모공격은 프록시와 위임자가 공모하여 소유자의 소유자의 개인키를 추출하거나, 소유자의 암호문을 권한이 없는 제 3자가 복호화 할 수 있도록 변환하는 재암호화 키를 위조할 수 있는 위협이다. 따라서 데이터 소유자의 의사와 상관없이 데이터의 원본을 유출시킬 수 있다. 이러한 문제를 해결하기 위해서는 소유자가 생성하는 재암호화 키를 소유자 외에는 생성할 수 없으며, 수식 구조 자체에서 소유자의 개인키를 복구해낼 수 없도록 설계가 수행되어야 한다. 본 연구에서는 프록시와 위임자가 결탁하여 무단으로 소유자의 키를 추출하거나 새로운 재암호화 키를 생성할 수 없도록 하는 방법을 제시한다.

2. 관련 연구

2.1 프록시 재암호화

프록시 재암호화 기술은 데이터 소유자인 Alice가 프록시를 이용하여 데이터를 수신할 위임자 Bob에게 데이터 원본의 노출 없이 데이터를 안전하게 전달하는 기술이다[2][3]. 이러한 프록시 재암호화 기술은 ID 기반, 속성기반, 시간 기반 등 다양한 형태가 존재하며, 각 형태에 따라 재암호화 키 및 재암호화 방법 등에서 차이가 나타난다. 본 연구에서는 사용자의 공개키를 ID로 사용하여 재암호화 키를 생성하고 재암호화를 수행하는 방법인 ID 기반 프록시 재암호화 방법이 이용된다.

+ 이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2016R1D1A1B03935917)



(그림 1) ID 기반 프록시 재암호화 개요

ID 기반 프록시 재암호화 방법은 (그림 1)과 같이 소유자 Alice가 위임자 Bob의 공개키를 이용하여 암호화를 재암호화 키를 생성하고, 이 재암호화 키로 재암호화를 수행한다. 따라서 재암호화 된 암호문은 위임자 Bob 이외에는 복호화 할 수 없다. 또한 전달 과정에서 프록시 서버는 암호문을 복호화하지 않기 때문에 원본 노출의 위험이 없다 [1].

2.2 공모공격

ID 기반 프록시 재암호화 방법에서는 재암호화 키 생성 과정에 위임자의 공개키가 사용된다. 또한 생성된 재암호화 키는 프록시 서버에 위탁되어 프록시 서버가 안전하게 보관하는걸 전제로 한다. 하지만 위임자에 의해 오염된 프록시 서버가 위임자와 공모하여 재암호화 키를 위임자에게 제공하고, 위임자는 자신의 개인키를 재암호화 키와 결합하여 소유자의 개인키를 추출하거나 제 3자의 공개키를 삽입하여 새로운 재암호화 키를 생성할 수 있다. 이러한 공격으로 인해 데이터 소유자는 허가하지 않은 제 3자에게 자신의 중요한 데이터를 노출시킬 수 있게 된다. 따라서 공모공격의 방지를 위해서는 프록시와 위임자가 서로 정보를 결합하여 특정 데이터를 추출하거나 새로운 데이터를 생성할 수 없도록 설계해야만 한다.

4. 제안방식

본 장에서는 제안방식의 보안 요구사항을 설명하고, 이에 따른 제안방식을 설명한다.

4.1 보안 요구사항

본 연구는 다음과 같은 사항을 요구한다.

- 기밀성(Confidentiality) : 클라우드 스토리지에 업로드 된 데이터는 정당한 소유자 이외에는 원본을 확인할 수 없도록 해야 한다.
- 단방향성(Unidirectional) : 소유자가 위임자에게 데이터를 전달하기 위해 생성한 재암호화 키 $rk_{A\to B}$는 소유자의 암호데이터 C_A를 위임자가 복호화 할 수 있는 데이터 D_B로 재암호화 하는데만 이용될 수 있으며, C_B로부터 D_A를 생성하는데에는 이용할 수 없어야 한다.
- 공모공격 저항(Collusion resistance) : 프록시 서버와 복호위임자의 결탁을 통해 재암호화 키의 위조 또는 데이터 제공자의 개인키가 복구될 수 없어야 한다.

4.2 Setup(1^λ)

공개 parameter를 생성하여 분산된 사용자에게 공개하며, 마스터 비밀 키(MSK)를 생성하여 안전하게 보관한다.

4.3 KeyGen($param, MSK, id_A$)

PKG는 공개 parameter와 마스터 비밀 키를 입력하여 사용자의 개인키와 공개키를 출력하고 안전한 채널로 사용자에게 각각 전송한다.

4.4 Encrypt($param, id_A, m$)

데이터 제공자는 공개 parameter, 자신의 id_A와 함께 암호화하려는 메시지 m을 입력하여 first-level 암호문 $C_A = (C_1, C_2, C_3, C_4, C_5$를 획득하고, 이를 프록시 서버에 저장한다.

4.5 RKGen($param, sk_{id_A}, id_B$)

데이터 제공자는 공개 parameter와 자신의 개인키 sk_A와 복호화 위임자의 id_B를 입력하여 재암호화 키 $rk_{A\to B}$를 생성한다.

4.6 Re-encrypt($param, rk_{A\to B}, C_A$)

프록시 서버는 암호문 C_A와 $rk_{A\to B}$를 이용해 재암호화를 수행하여 second-level 암호문 $D_B = (D_1, D_2, D_3, D_4, D_5$를 획득한다.

4.7 Decrypt($param, sk_{A\text{ or }B}, C_A$ or D_B)

복호화 단계에서는 암호문이 first-level 암호문인지, second-level 암호문인지 판단하여 복호화를 수행한다.

5. 결론

본 제안방식은 ID 기반 프록시 재암호화 방법에서 발생할 수 있는 공모공격을 방지하는데 주안점을 두었다. 공모공격은 소유자가 허가하지 않은 제 3자가 무단으로 데이터 원본을 획득할 수 있는 위협을 보여준다. 이 위협은 경우에 따라서 중요한 정보의 유출로 이어질 수 있기 때문에 매우 심각하게 다뤄져야 할 위협이다. 이를 해결하기 위해 본 제안방식은 무작위의 parameter를 생성하고 이를 재암호화 키 생성에 포함시킨다. 이를 통해 제 3자가 무단으로 재암호화 키를 위조할 수 없으며, 재암호화키로부터 소유자의 개인키를 추출할 수 없다. 결과적으로, 본 제안방식은 클라우드 스토리지 환경에서 데이터 제공자에게 더욱 향상된 안전성을 제공할 수 있다.

참고문헌

[1] 박승환, et al. "스마트카드를 이용한 프록시 재 암호화 기법 기반 콘텐츠 공유 메커니즘에 관한 연구." 정보보호학회논문지 21.3 (2011): 131-141.

[2] Paul, Arinjita, et al. "A CCA-Secure Collusion-Resistant Identity-Based Proxy Re-Encryption Scheme." International Conference on Provable Security. Springer, Cham, (2018). pp. 111-128.