분산환경에서 사용자 데이터 공유를 위한 접근제어 방식에 관한 연구

박기성, 노성기
한국전자통신연구원

ks.park@etri.re.kr, sknoh@etri.re.kr

A Study on the Access Control Scheme for User Data Sharing in Distributed Environments

Park Ki Sung, Noh Sung Kee
Electronics and Telecommunications Research Institute

요 약

최근 사용자 데이터 프라이버시의 중요성이 강조됨에 따라 사용자의 데이터 주권을 보장하기 위한 연구가 활발히 이루어지고 있다. 그러나 기존 중앙집중형 구조에서는 클라우드와 같은 제 3 신뢰기관이 데이터의 관리 권한을 가지고 있으므로 사용자 데이터 주권이 보장되지 않는 문제점이 있다. 본 논문에서는 분산환경에서 사용자 직접 자신의 데이터를 관리하고 공유할 수 있는 분산접근제어 방식을 제안한다.

Ⅰ. 서 론

유럽의 General Data Protection Regulation (GDPR) [1] 및 국내 마이데이터 사업 등 개인이 생산한 데이터의 프라이버시 및 데이터 관리 주권에 대한 관심이 높아지고 있다. 기존의 데이터 관리 시스템의 경우 클라우드와 같은 제 3 신뢰기관이 사용자의 데이터를 관리하고 해당 데이터를 분석 및 가공하여 자사 정책 개선과 광고 서비스에 활용하고 있다. 이러한 제 3 신뢰기관 의존형 데이터 생태계에서 사용자는 자신의 데이터 및 키를 직접적으로 관리하는데 어려움이 있다. 이러한 중앙집중형 데이터 생태계를 벗어나기 위하여 블록체인과 같은 분산환경에서 사용자의 데이터 주권과 프라이버시를 보장하기 위한 접근제어 및 인증 기술에 대한 연구가 수행되고 있다.

대표적인 사용자 중심의 접근제어 기술로는 Key Aggregate Searchable Encryption (KASE) [2]가 있으며 KASE 기술은 사용자가 자신의 데이터 암호화 및 복호화에 해당하는 키를 스스로 관리할 수 있는 특징이 있다. 최근 KASE 기법의 특징을 이용한 접근제어 방식에 대한 연구가 활발히 진행되고 있다 [3-4]. 그러나 이러한 KASE 를 활용한 접근제어 연구들 또한 실제 데이터는 클라우드에 저장하고 관리하므로 클라우드가 단일 지점 장애 문제 및 DDoS 공격 등에 노출되는 경우 전체 데이터 시스템이 동작하지 않는 문제가 발생할 수 있다. 본 논문에서는 분산환경에서 사용자가 직접 데이터를 저장 및 관리할 수 있는 KASE 기반 분산접근제어 방식을 제안한다.

Ⅱ. 관련 연구

2.1. Key Aggregate Searchable Encryption

KASE 는 2014 년 Cui 등이 제안한 방식으로 여러 데이터에 해당하는 비밀 키를 단일 크기의 집계 키로 생성하여 원하는 조합의 데이터 집합을 복호화 할 수 있는 방식이다. 또한 암호화된 데이터는 키워드를 통하여 검색 가능하여 데이터를 효율적으로 관리할 수 있는 장점이 있다. KASE 방식은 초기 시스템 파라미터와 데이터 사이즈, 키 쌍을 생성하는 Setup 단계, 키워드를 이용한 데이터 암호화 단계, 데이터 검색을 위한 트랩도어 생성 단계, 데이터 복호화 단계로 구성되며 KASE 의 개념도는 그림 1 과 같다.

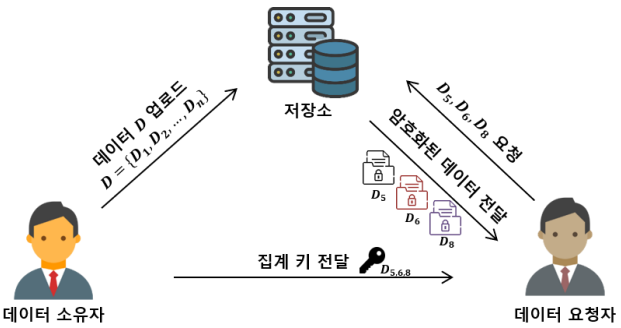

그림 1. 제안하는 분산접근제어 방식

Ⅱ. 분산 접근제어 시스템 모델

제안하는 분산접근제어 방식은 KASE 기법을 기반으로 사용자 데이터를 관리하며 분산 환경에서 제 3 신뢰기관 없이 사용자가 자신의 데이터를 관리 및 공유할 수 있다. 제안하는 접근제어 방식은 그림 2 와 같다.

3.1. 시스템 모델

제안하는 분산접근제어 방식은 데이터 소유자, 신뢰에이전트 및 데이터 요청자로 구성되며 각 구성 노드는 다음과 같다.

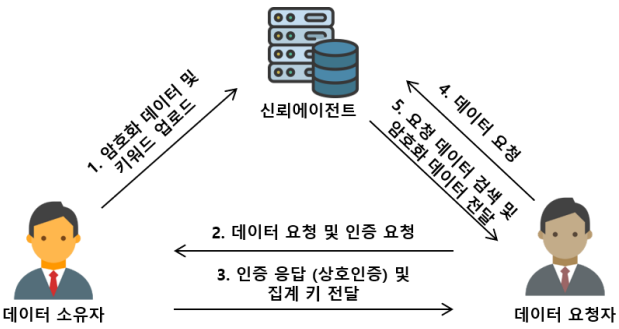

그림 2. 제안하는 분산접근제어 방식

- 데이터 소유자는 데이터 소유주로 자신의 데이터에 대한 관리 권한을 가지고 있으며 자신의 데이터 공유 및 활용을 위하여 데이터를 암호화한 후 신뢰에이전트에 암호화된 데이터를 업로드한다. 데이터 소유자는 자신의 선택한 보안 레벨에 따라 신뢰에이전트에 데이터 복호화를 위한 집계 키를 할당하거나 신뢰에이전트에게 집계 키 생성 권한을 부여할 수 있다.
- 신뢰에이전트는 사용자가 구축한 자신이 관리하는 서버로 기존 클라우드 서버의 데이터 저장 및 데이터 공유 기능을 수행한다. 신뢰에이전트는 항상 온라인 상태로 동작하고 있으므로 데이터 소유자가 오프라인 상태일 때 사용자가 설정한 보안 레벨에 따라 접근 가능한 데이터를 공유할 수 있다.
- 데이터 요청자는 데이터 소유자의 데이터를 공유 받기 원하는 대상으로 데이터 소유자에게 데이터 공유를 요청한다.

3.2. 데이터 접근제어 흐름도

제안하는 시스템의 데이터 접근제어 흐름도는 다음과 같다.

1) 데이터 소유자 및 데이터 사용자는 KASE 기법을 사용하기 시스템 공개 파라미터 및 키 쌍을 생성한다.
2) 데이터 소유자는 자신이 공유할 데이터를 선택하고 이를 키워드, 키워드 검증 값과 함께 데이터를 암호화한 후 자신의 신뢰에이전트에 업로드 한다.
3) 신뢰에이전트는 암호화된 데이터, 키워드 및 키워드 검증 값을 저장하고 추후 데이터 검색 시 이를 활용한다.
4) 데이터 요청자는 자신이 원하는 데이터를 얻기 위하여 데이터 소유자에게 데이터를 요청한다.
5) 데이터 사용자는 데이터 요청자와 상호인증을 수행한 후 요청받은 데이터에 대한 단일 집계 키를 생성하여 데이터 요청자에게 전달한다.
6) 데이터 요청자는 수신한 집계 키 및 키워드 값을 이용하여 신뢰에이전트에 데이터를 요청한다. 사용자가 신뢰에이전트에게 상호인증 및 집계 키 공유 단계를 위임한 경우 신뢰에이전트가 대리 수행할 수 있다.
7) 신뢰에이전트는 데이터 요청자의 요청 정보에 따라 암호화된 데이터를 검색하고 해당 데이터 사용자에게 전달한다.
8) 데이터 사용자는 최종적으로 집계 키를 사용하여 암호화된 데이터를 복호화 한다.

3.3. 향후 연구

제안하는 분산형 접근제어 시스템을 블록체인상에서 구축하기 위하여 시스템 설계를 보완하고 성능 분석 및 보안 분석을 수행할 예정이며 이를 기반으로 실제 블록체인 네트워크에서 제안한 방식을 구현하여 제안한 방식의 실현 가능성을 검증할 예정이다.

IV. 결론

최근 개인이 생산한 데이터에 대한 프라이버시에 대한 관심이 증가함에 따라 사용자의 데이터 주권을 보장하기 위한 다양한 연구가 수행되고 있다. 그러나 기존의 데이터 접근제어 시스템의 경우 제 3 신뢰기관에 의존한 중앙집중형 구조로 실제 사용자의 데이터 관리 및 공유는 제 3 신뢰기관을 통하여 이루어진다. 본 논문에서는 이러한 문제를 개선하기 위하여 분산 환경에서 사용자가 데이터 주권을 가지는 KASE 기반 분산접근제어 방식을 제안하였다. 제안한 방식을 통하여 사용자는 스스로 자신의 키를 관리하고 데이터에 대한 접근제어 기능을 수행하므로 제 3 신뢰기관 없이 사용자 데이터 주권을 보장할 수 있다. 향후 제안한 방식을 직접 활용한 실제 분산 환경에서 시스템을 구축할 예정이다.

ACKNOWLEDGMENT

본 연구는 한국전자통신연구원 연구운영비지원사업의 일환으로 수행되었음. [22ZR1300, 지능형 사이버 보안 및 신뢰 인프라 기술 연구]

참 고 문 헌

[1] Proposal for a regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In General Data Protection Regulation, European Parliament, January 2016, 2016.

[2] Cui, B., Liu, Z., and Wang, L. “Key Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage,” IEEE Transactions on Computers, vol. 65, no. 8, pp. 2374-2385, 2016.

[3] Lee, J., Kim, M., Oh, J., Park, Y., Park, K., and Noh, S. “A Secure Key Aggregate Searchable Encryption with Multi Delegation in Cloud Data Sharing Service,” Applied Sciences, vol. 11, no. 19, pp. 8841-8860, 2022.

[4] Pareek, G., and Purushothama, B. R. “KAPRE: Key-aggregate proxy re-encryption for secure and flexible data sharing in cloud storage.” Journal of Information Security and Applications, vol. 63, pp. 103009-103029, 2021.