JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 27 No. 4, pp. 53-60, April 2022
https://doi.org/10.9708/jksci.2022.27.04.053

Data access control of KP-ABE scheme for secure communication in drone environment

Yong-Woon Hwang*, Su-Hyun Kim**, Im-Yeong Lee*

*Student, Dept. of Software Convergence, Soonchunhyang University, Asan, Korea
**Researcher, Dept. of ICT Industry Strategy, National IT Industry Promotion Agency, Jincheon, Korea
*Professor, Dept. of Software Convergence, Soonchunhyang University, Asan, Korea

[Abstract]

Recently, as the amount of data collected by drones has rapidly increased, it is necessary to support cloud computing technology that can securely and efficiently store and process data. However, various security threats such as stealing, leaking, or tampering with data communicated by drones can occur due to attackers. Therefore, there is a need for security technology to provide secure communication of data collected from drones. Among various security technologies, the KP-ABE scheme, which is attribute-based encryption, is a security technology that satisfies two characteristics: data encryption and user access control. This paper researched the KP-ABE scheme and proposed a secure data access control scheme to the drone environment. This proposed scheme provides confidentiality and integrity of data communicated in a drone environment and secure access control and availability. In addition, it provides a fast ciphertext search and constant size ciphertext among the requirements to be provided in the KP-ABE scheme.

▸ **Key words**: Drone, Cloud, Access Control, Cryptographic Application, Attribute-Based Encryption

[요 약]

최근 드론으로 수집되는 데이터의 양이 급증함에 따라, 데이터를 안전하고 효율적으로 저장 및 처리할 수 있는 클라우드 컴퓨팅 기술의 지원이 필요하다. 하지만, 드론에서 통신하는 데이터를 공격자로 인해 탈취되거나, 유출, 위·변조 등 다양한 보안 취약점이 발생할 수 있다. 따라서 드론으로부터 수집되어 전송되는 데이터에 보안 기술이 필요하다. 다양한 보안 기술 중 속성기반암호인 KP-ABE 기법은 데이터 암호화와 사용자 접근 제어, 두 가지 특성을 만족시키는 보안 기술이다. 본 논문은 KP-ABE 기법을 연구하고, 이를 드론 환경에 활용하여 안전한 데이터 접근 제어 기법을 제안하고자 한다. 본 제안 기법은 드론 환경에서 통신되는 데이터의 기밀성과 무결성 및 안전한 접근 제어와 가용성이 제공된다. 그리고 KP-ABE 기법에서 제공해야 할 요구사항 중 빠른 암호문 탐색 및 일정 크기 암호문 출력을 제공한다.

▸ **주제어**: 드론, 클라우드, 접근 제어, 암호 응용, 속성기반암호

• First Author: Yong-Woon Hwang, Su-Hyun Kim, Corresponding Author: Im-Yeong Lee
*Yong-Woon Hwang (hyw0123@sch.ac.kr), Dept. of Software Convergence, Soonchunhyang University
**Su-Hyun Kim (ksh34@nipa.kr), Dept. of ICT Industry Strategy, National IT Industry Promotion Agency
*Im-Yeong Lee (imylee@sch.ac.kr), Dept. of Software Convergence, Soonchunhyang University
• Received: 2022. 03. 25, Revised: 2022. 04. 19, Accepted: 2022. 04. 19.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

최근 드론과 ICT(Information and Communications Technology) 기술의 발전으로 인해 우리 주변에서 드론을 쉽게 볼 수 있다. 특히 항공촬영, 건설, 교통, 농업 분야 등 다양한 산업 분야에서 활용되고 있다. 드론으로 수집되는 데이터의 양이 급증함에 따라, 데이터를 안전하고 효율적으로 저장 및 처리할 수 있는 클라우드 컴퓨팅 기술의 지원이 필요하다.

하지만, 드론으로부터 통신되는 데이터를 목표로 공격자(악의적인 사용자)는 컨트롤러나 네트워크를 통해 데이터 위·변조, 데이터 노출을 통한 개인정보 탈취, 중간자 공격 등 다양한 보안 위협을 발생시킬 수 있다. 그림 1과 같이, 공격자로 인해 전달되는 데이터가 유출되거나 손상될 수 있으며, 데이터 변조가 발생할 가능성이 있다. 만약 드론으로 수집된 데이터가 민감한 정보라면, 이는 상당한 보안 위협이 될 것이다[1]. 따라서 드론으로부터 중요한 데이터를 수신받는 환경에서 안전한 통신을 위한 보안 기술이 필요하며, 통신하는 데이터에 대한 무결성과 기밀성을 제공해야 한다. 추가로, 정당한 사용자만 클라우드 서버에 접근하여 드론으로부터 수집된 데이터를 확인할 수 있어야 한다[2-3].

다양한 보안 기술 중 속성기반암호(Attribute Based Encryption)는 데이터 암·복호화와 접근 제어 두 가지 요소를 만족시킬 수 있다. 속성기반암호는 사용자의 다양한 속성을 가지고 암·복호화를 수행하는 암호 기술이다. 특히 IoT(Internet of things)-클라우드 환경에서 데이터 공유 시 데이터 암호화 및 암호문 접근 제어 기술로 많이 사용된다[4-5]. 속성기반암호 기법은 데이터 접근구조 생성 주체가 데이터 소유자일 경우 CP-ABE(Ciphertext-Policy Attribute Based Encryption), 데이터 사용자라면 KP-ABE(Key-Policy Attribute Based Encryption) 기법으로 사용된다. 본 논문은 다수의 드론으로부터 지정된 사용자들에게 데이터가 전달되는 클라우드(N:1) 환경에 적합한 KP-ABE 기법연구를 수행하였다. 현재까지 다양한 KP-ABE 기반의 데이터 접근 제어 기법이 연구되었다. 하지만 기존의 KP-ABE 기법 중 환경에 따라 보안요구사항 및 효율성이 제공되지 않는 기법들이 존재한다.

본 논문은 기존의 KP-ABE 기법들을 분석하여, 드론과 클라우드 융합 환경에 적합한 KP-ABE 기법을 제안한다. 세부적으로 드론으로부터 수집된 데이터를 안전하게 드론 서비스 공급자에게 전달할 수 있도록 하는 것이 본 연구의 목표이다.

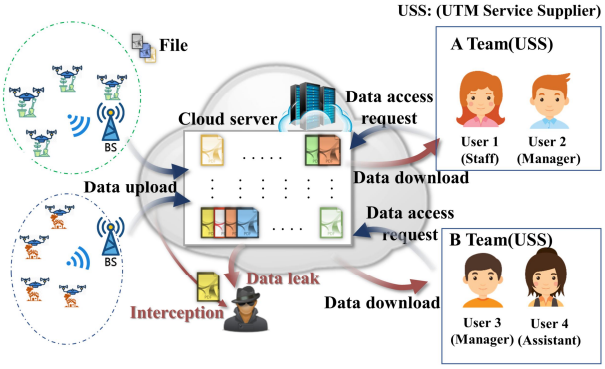


Fig. 1. Security threats in cloud environments for data communication collected by drones

본 제안 기법은 첫째, KP-ABE를 활용하기 때문에 통신되는 데이터의 기밀성과 무결성이 제공된다. 둘째, 암호문에 접근하고자 하는 사용자 중 드론으로부터 수집된 암호문들이 포함하고 있는 속성들을 가진 사용자만이 암호문에 접근하여 복호화를 시도할 수 있으므로, 데이터에 대한 가용성 및 안전한 접근 제어 기능도 제공된다. 셋째, 클라우드 서버에 검색 가능 암호화를 제공하여 저장된 수많은 암호문들을 복호화 과정 없이, 사용자가 요청한 암호문을 빠르게 찾아 제공한다. 마지막으로 통신되는 암호문의 크기가 속성의 개수에 따라 증가하는 문제를 해결하였다.

II. Background

이 장에서는 겹선형 사상과 KP-ABE 모델, 기존에 연구된 KP-ABE 기법에 대해 설명한다.

1. Bilinear Map

겹선형 사상은 최근에는 정보보호를 위한 암호화 도구로 활용되고 있다. 겹선형 페어링 함수를 겹선형 사상이라고 하며, 표기법은 다음과 같다. 동일한 차수 p를 갖는 곱셈 그룹 G_1 및 G_2가 있다고 가정한다. 그룹 내에서 이산로그 문제를 푸는 것이 어렵다고 가정한다. g를 G_1의 생성자 그룹이라고 하고 $e : G_1 \times G_1 \rightarrow G_2$를 다음 속성을 만족하는 겹선형 사상이라고 가정한다[6].

- Bilinearity: 모든 $P, Q \in G_1$, $a, b \in Z_p$에 대해, $e(P^a, Q^b) = e(P, Q)^{ab}$이다.
- Non-degeneracy: 모든 $Q \in G_1$에 대해, $e(P, Q) = 1$이면 $P = 0$ 이다.
- Computability: 모든 $P, Q \in G_1$에 대해 $e(P, Q) \in G_2$를 계산하는 효율적인 알고리즘이 존재한다.

2. KP-ABE

2.1 Access Structure

속성기반암호는 각 엔터티에 대한 속성 집합(예: 소속, 직업)을 사용하여 생성된 접근구조를 기반으로 암복호화를 수행하는 기법입니다. 여기서, 접근구조(Access Structure)는 그림 2의 데이터 사용자들이 가지고 있는 트리 형태의 구조이다. 접근구조는 임계값(Threshold)에 따라 OR 게이트 또는 AND 게이트, 임계값 게이트를 나타낼 수 있다. 일반적으로 모든 노드 $x \in$ AS에 대해 k_x 및 num_x 표기법을 사용하여 x의 임계값과 자식 수를 각각 나타냅니다. 노드 x의 경우 $k_x = 1$이면 x는 OR 게이트를 나타내고, $k_x = num_x$이면 AND 게이트를 나타낸다. $1 < k_x < num_x$이면 x는 임계값 게이트를 나타낸다[7].

2.2 KP-ABE Model

그림 2는 KP-ABE 기법을 활용한 데이터 접근 제어 기법으로 AA(Attribute Authority), 드론(클라우드에 암호문을 전송하는 객체), 데이터 사용자(클라우드에 저장된 암호문의 복호화를 시도하는 사용자) 및 클라우드 서버 총 4가지 참여 객체로 구성되어 있다.

먼저 AA는 초기설정 단계에서 마스터키와 공개파라미터를 생성한다. 데이터 사용자는 자신의 속성을, AA에 전송하여, 비밀키(암호문 복호화 키)를 요청한다. KP-ABE 기법에서 접근구조는 사용자 또는 AA가 생성할 수 있다. AA는 사용자의 비밀키를 생성하여 공개파라미터와 함께 사용자에게 전송해주고, 드론에게 공개파라미터를 전송한다. 드론은 데이터를 전달하고자 하는 사용자들의 속성을 기반으로 암호문을 생성하고, 이를 클라우드 서버에 전송한다. 데이터 사용자는 클라우드 서버로부터 암호문을 요청하여, 전송받고, 접근구조와 AA로부터 받은 비밀키를 기반으로 암호문을 복호화하여 데이터를 획득한다. 그림 2와 같이 접근구조의 속성과 암호문에 포함된 속성이 일치하지 않는 경우 복호화를 수행할 수 없다[5].

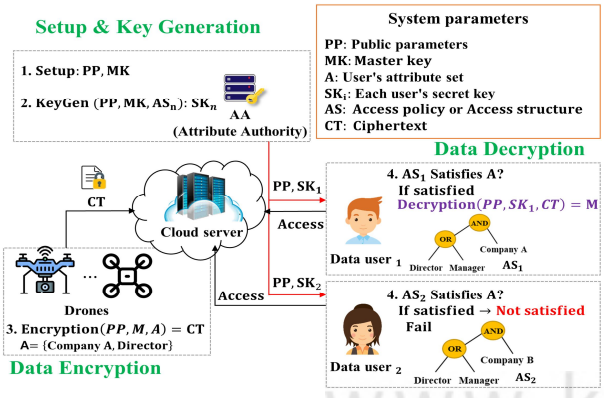


Fig. 2. Data access control using KP-ABE scheme

3. The need for KP-ABE in a drone-cloud environment

드론-클라우드 환경에서 전달되는 데이터의 암호화를 위해 대칭키를 사용할 경우, 사전에 대칭키 배포 및 키 관리에 문제가 발생할 수 있다. 또한, 비대칭 암호화 방식을 사용할 경우, 연산 효율성이 떨어질 수 있으며, 드론과 사용자 간에 데이터를 공유하기 위해 ID나 공개 키와 같은 식별값이 사전에 필요하다. 따라서 N:N 클라우드 환경에서 미리 지정되어 있지 않은 다수의 드론(데이터 업로드자) 또는 사용자들 간의 통신을 통해 데이터를 공유하는 경우 비대칭 암호화 방식은 권장되지 않는다.

속성기반암호는 N:N 통신하는 클라우드 환경에서 데이터 암호화와 접근 제어를 제공하는 보안 기술이다[4-5]. 특히 드론-클라우드 환경을 가정했을 경우, 다수의 드론에서 수집된 데이터를 클라우드를 통해 소수의 사용자(드론에서 지정한 속성을 가진 사용자)에게 안전하게 전달하기 위해 KP-ABE 기법을 활용할 수 있다.

4. Related Works

본 제안 기법을 활용하고자 하는 드론-클라우드 융합 환경에서는 통신하는 데이터의 기밀성, 무결성, 가용성 및 접근 제어가 제공되어야 한다. 추가적으로 속성기반암호 활용 시, 클라우드 서버에서 사용자가 요청한 암호문을 빠르게 탐색하여 제공해야 하며, 통신하는 암호문 크기에 대한 요구사항이 제공되어야 한다. 2006년 Goyal et al.에 의해 초기 KP-ABE 기법이 제안되었고 이를 기반으로 암호문 탐색, 일정 크기 암호문 제공, 속성해지, 접근구조 익명화, 아웃소싱 서버 지원 등 다양한 요구사항을 제공하기 위한 연구가 수행되었다[5]. 본 논문의 관련 연구에서는, 다수 요구사항을 제공하는 KP-ABE 기법 중 일정 크기 암호문 제공과 검색 가능 암호를 제공하는 KP-ABE 기법들에 대해 분석하였다.

Wang et al. 기법 Lai et al. 기법 및 Zhang et al. 기법의 공통된 특징은 일정한 크기의 암호문을 제공하는 것을 중점으로 제안한 KP-ABE 기법이다[8-10]. 3가지 KP-ABE 기법은 암호문에 포함된 다수의 속성의 값들을 집계 연산하여, 하나의 값으로 표기함으로써, 암호문의 크기가 속성의 개수에 영향을 받지 않는다. 추가적으로, Zhang et al. 기법은 검증 가능 아웃소싱 서버를 지원하여, 사용자의 암호문 복호화 연산량의 효율성을 향상시켰다. 하지만 3가지 KP-ABE 기법은 클라우드 서버에서 암호문 탐색 기능이 제공되지 않으며, 사용자가 암호문 요청 시 클라우드 서버는 사용자가 요청한 암호문을 전송해주는 것을 가정한다. 이에, 실제 클라우드 환경에 적용하기

위해 다수의 요구사항을 고려해야 한다.

Yin et al. 기법, Ameri et al. 기법, Li et al. 기법은 검색 가능 암호를 기반으로 암호문을 탐색할 수 있는 KP-ABE 기법이다[11-13]. KP-ABE 기법에 검색 가능 암호의 적용은 기존의 클라우드 서버에서 사용자가 요청한 암호문을 전달해 준다는 가정을 배제한다. 검색 가능 암호가 활용되면, 그림 2에서 사용자가 암호문 요청 시 클라우드 서버에서 암호문 탐색 단계가 추가된다(그림 3 참고). 클라우드 서버는 사용자가 요청한 암호문 탐색 시 저장된 암호문들의 복호화 과정 없이 암호문을 탐색하여, 사용자에게 제공해줄 수 있는 이점이 있으므로 검색 가능 암호화 도입은 효과적이다.

하지만 암호문 탐색을 제공하는 3가지 KP-ABE 기법 모두 일정 크기 암호문이 제공되지 않는다[11-13]. 또한, 빅데이터를 관리하는 클라우드에서 암호문을 탐색할 때, 속성값에 따라 암호문 탐색의 횟수가 증가한다. 만일 다수의 암호문이 클라우드 서버에 저장되어 있고 각각 두 개의 속성을 가지고 있다고 가정할 때, 클라우드 서버가 암호문 탐색 시 첫 번째 탐색은 토큰의 첫 번째 속성과 암호문의 첫 번째 속성을 비교하는 것이다. 두 번째 탐색은 토큰의 두 번째 속성과 암호문의 두 번째 속성을 비교하고 일치하는 암호문을 찾는 것이다. 즉, 암호문의 탐색 횟수는 토큰과 암호문에 포함된 속성의 수에 비례하여 증가하기 때문에 비효율적이다.

III. Security Requirements

이 장에서는 드론-클라우드 환경에서의 안전한 데이터 통신을 위해 보안성과 효율성 측면에서 필요한 요구사항을 설명한다.

• **데이터 기밀성과 무결성**: 드론에서 수집된 데이터를 클라우드 전송 시 데이터가 평문인 경우, 데이터 유출, 위·변조 등 다양한 보안 위협이 발생한다. 따라서 통신 구간에서 드론으로부터 전달되는 데이터에 대한 기밀성이 요구되며, 정당한 사용자들만 통신된 데이터를 확인 및 검증할 수 있는 무결성이 제공되어야 한다.

• **데이터 가용성 및 사용자 접근 제어**: 누구든지 암호문에 접근하여 복호화를 시도하여 데이터를 획득할 수 있다면, 이는 잠재적 사이버 보안 위협을 일으킬 수 있다. 따라서, 암호문에 접근하고자 하는 사용자의 속성으로 접근 제어를 제공해야 한다. 그리고, 암호문을 복호화하여 메시지를 확인할 수 있게 데이터에 대한 가용성이 제공되어야 한다. 즉, 암호문에 포함된 속성을 가지지 못한 사용자는 암호문에 접근하더라도 복호화할 수 없어야 한다. 허가된 사용자는 AA에 등록되어 비밀키를 가지며, 암호문에 포함된 속성을 내포한 접근구조를 가진 사용자를 의미한다.

• **암호문 탐색 효율성**: 기존 암호문 탐색이 제공되는 KP-ABE 기법에서는 암호문 탐색은 속성 수에 비례하여 탐색 횟수가 증가한다. 이 문제를 해결하기 위해 암호문에 포함된 속성값들과 사용자가 생성한 토큰의 속성값들을 사전에 집계 연산하여 하나의 값으로 생성한다. 이후, 토큰과 암호문의 집계된 속성값을 비교하여 일치하는 암호문을 찾는다. 결과적으로 암호문 탐색의 수는 토큰 및 암호문에 포함된 속성의 수에 영향을 받지 않기 때문에, 효율적인 암호문 탐색을 제공한다.

• **일정한 크기의 암호문 출력**: 기존 KP-ABE 기법에서 생성된 암호문의 크기는 암호문에 포함된 속성의 수에 비례한다. 이에, 속성의 수와 관계없이 암호문의 크기가 일정하게 출력되어야 한다.

IV. The Proposed Scheme

본 장에서는 제안한 KP-ABE 기반의 데이터 접근 제어 기법에 대해 설명한다. 그림 3은 전체적인 시나리오를 보여주는 그림이며, 이에 대한 설명은 다음과 같다.

4.1 System Entities

본 제안 기법에 참여하는 각 객체 간의 역할은 다음과 같다.

• **드론**: 드론은 전달하고자 하는 데이터를 암호화하여 클라우드에 업로드하는 역할을 수행한다. 여기서 데이터는 일반적인 메시지 또는 영상 데이터 등이 될 수 있으며, 민감하거나 중요한 데이터를 의미한다. 데이터 암호화 시 데이터에 접근하고자 하는 사용자들의 속성으로 암호화하며, 암호문을 표시할 수 있는 키워드 인덱스도 함께 생성하여 클라우드 서버에 업로드한다.

• **클라우드 서버**: 클라우드 서버는 데이터를 저장하는 스토리지 역할을 수행한다. 세부적으로, 드론으로부터 전송받은 암호문을 저장하고 관리하며, 사용자가 암호문 요청 시, 요청한 암호문을 탐색하여, 사용자에게 전송한다.

• **DSS(Drone Service Supplier)**: 드론 서비스 공급자는 드론으로부터 데이터를 수집 및 통산하여 저장된 데이터를 확인하는 역할을 수행한다. 클라우드 서버에 저장된 암호문 중, 접근구조의 속성을 가진 암호문들을 수신받아 복호화하여 데이터를 확인할 수 있다.

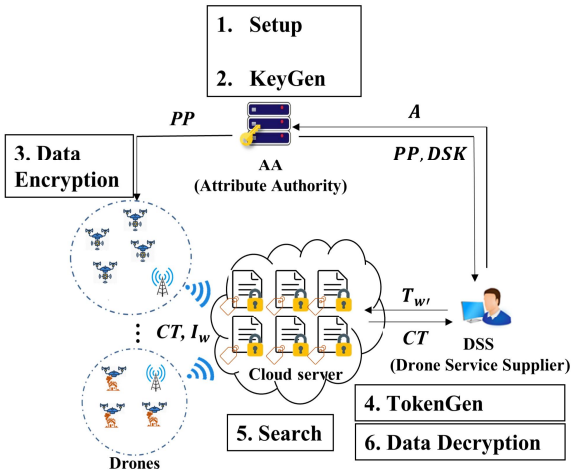


Fig. 3. Proposed Scheme Overall Scenario

• **AA(Attribute Authority)**: AA는 DSS들의 속성을 관리하는 신뢰된 서버로써, 공개파라미터와 DSS들이 요청한 비밀키(암호문 복호화키)를 생성하여 전송해주는 역할을 수행한다.

4.2 System Parameters

- PP, MK : 공개파라미터, 마스터키
- DSK : 데이터 사용자 비밀키(암호문 복호화키)
- A_{u_i}, A : 사용자 속성 데이터, 속성 데이터 집합
- AS : 접근구조(Access Structure)
- $T_{w'}$: 키워드 w'로 생성한 토큰값
- w, w' : 키워드(드론, 데이터 사용자)
- CT, I_w : 암호문, 암호문 인덱스 값
- $H_1(*)$: 암호 해시 함수 $(\{0,1\}^* \rightarrow Z_p^*)$
- $H_2(*)$: 암호 해시 함수 $(\{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow Z_p^*)$

4.3 Procedure

본 제안 기법은 총 6단계로 구성되어 있다. 이에 대한 설명은 다음과 같다.

초기설정 단계 전에 그룹 G와 G_2는 차수 p의 그룹이고, $e: G \times G \rightarrow G_2$는 bilinear map이라고 가정한다. AA는 소수 차수가 p인 타원곡선 점의 그룹 G_T를 생성하고, G_T의 생성자 P를 결정한다. 사용자 속성은 n개의 속성이 있고, 보편적으로 속성 집합을 $A = [Att_1, Att_2, ..., Att_n]$로, 접근구조는 $AS = [AS_1, AS_2, ..., AS_n]$으로 표기한다.

Step 1. AA에서 Setup 과정을 통해, 공개파라미터와 마스터키를 생성하고, 드론에게 공개파라미터를 전송한다(그림 3의 1).

- $Setup(k) = PP, MK$
  - $\alpha, \beta \in Z_p^*, t_i \in$ 생성함

$$PP = \left\{G, G_2, G_T, e, g, \left\{T_i = g^{t_i}\right\}_{i\in[1,n]}, f = g^B, e(g,g)^{\alpha}, H_1, H_2\right\}$$

$$MK = \left\{\alpha, \{t_i\}_{i\in[1,n]} RIGHT\right.$$

Step 2. DSS가 AA에게 속성값을 전송하여, 비밀키를 요청하면, AA는 사용자가 보내준 속성값들을 기반으로 접근구조를 만들고 이에 대응되는 비밀키를 생성한다. 그리고, DSS에게 공개파라미터와 비밀키를 전송한다(그림 3의 2).

- $KeyGen(PP, A, MK) = DSK$
  - $r_i \in Z_p^*$선택, $r = \sum_{i=1}^{n} r_i$

$$D_i = g^{\alpha + r}, \quad D_i' = g^{r_i}, \quad D_{i,j} = g^{t_n A} \text{or} \quad g^{t_{n+1} A},$$

$$DSK = \left\{AS, D_i, D_i', \{D_{i,1}\}_{i\in[1,n]}, \ H_1(Att_i)^{\beta}_{i\in[1,n]}\right\}$$

Step 3. 드론은 수집된 메시지를 대칭키로 암호화하고, 대칭키를 전달하고자 하는 DSS 속성들과 공개파라미터로 암호화를 수행한다. 이때, 암호문과 이를 표시할 수 있는 키워드 w를 선택하여, 암호문 인덱스 I_w를 생성한다. 드론은 CT와 I_w를 클라우드 서버에 전송·저장한다(그림 3의 3).

- $Encrypt(PP, M, A, w) = CT, I_w$
  - 메시지 M 선택 및 암호화 $C_0 = Enc_{mkey}(M)$
  - $s_i, s' \in Z_p^*$선택, $s = \sum_{i=1}^{n} s_i$,
  - 암호문을 표시할 수 있는 word 선택(w)

$$C_1 = mkey \cdot e(g,g)^{\alpha s}, \quad C_2 = h^s,$$

$$C_3 = g^s \cdot \prod_{i\in 1}^{n} g^{t_i Att_i}, C_4 = \prod_{i=1}^{n} H_1(Att_i)^s$$

$$\widetilde{C}_1 = e\left(f, \ g^{ws'}\right), \quad \widetilde{C}_2 = \ g^{ss'}, V = (g^{H(M)}, g^{H(mkey)})$$

$$CT = \{A, C_0, C_1, C_2, C_3, VRIGHT\{\widetilde{C}_1, \ \widetilde{C}_2, C_4 RIGHT$$

Step 4. 사용자는 비밀키와 암호문을 찾기 위한 키워드 w'를 선택하여, 암호문을 탐색할 수 있는 토큰 $T_{w'}$을 생성한다. 사용자는 클라우드 서버에 토큰을 보내, 암호문을 요청한다(그림 3의 4).

-
  - 탐색하려는 암호문 키워드 w' 선택, 토큰 생성

$$T_{w'} = e\left(\prod_{i=1}^{n} H_1(Att_i)^{\beta},\ g^{w'}\right)$$

Step 5. 클라우드 서버는 사용자로부터 받은 $T_{w'}$와 서버에 저장된 암호문 CT의 I_w을 비교하며, 사용자가 원하는 암호문을 탐색한다. 탐색 결과는 {0,1}로 나타나며, 검색된 암호문들을 사용자에게 전송한다(그림 3의 5).

- $Search(I_w, T_{w'}) = e(\tilde{C}_2,\ T_{w'}) = e(\tilde{C}_1, C_4)$

Step 6. 사용자는 DSK, PP를 가지고 클라우드 서버로부터 받은 CT에 포함된 사용자의 속성값과 자신이 가지고 있는 접근구조에 지정된 속성값을 비교 연산하여, 복호화를 수행한다. x는 사용자 접근구조의 말단 노드(속성값)를 의미한다. 복호화가 올바르게 수행되면, 대칭키를 추출할 수 있으며, 이를 가지고 암호문 C_0을 복호화하여 메시지를 획득할 수 있다. 그리고 획득한 키와 메시지를 검증함으로써, 메시지의 무결성을 확인할 수 있다(그림 3의 6).

- $Decrypt(CT, AS, DSK, PP) = M$
  - 속성값이 접근구조에 만족할 경우: $D_{i,j} = (g^{t_n})^{x_n}$
  - 속성값이 접근구조에 만족하지 않을 경우:

$$D_{i,j} = (g^{t_{n+1}})^{x_n}$$

$$\frac{e\left(C_2, \prod_{j\in A} D_{i,j}\right)}{e\left(C_3, f \bullet \prod_{i\in A} D_i'\right)} = \frac{e\left(g^{\beta s}, g^{\sum_{i=1}^{n} t_n x_n}\right)}{e\left(\left(g^s, g^{\sum_{i=1}^{n} t_n x_n}\right), (g^{\beta}, g^{r})\right)} = e(g,g)^{-sr}$$

$$mkey' = \frac{C_1}{e(C_2, D_i) \bullet C} = \frac{mkey \bullet e(g,g)^{\alpha s}}{e(g^s, g^{\alpha+r}) \bullet e(g,g)^{-sr}}$$

$$= \frac{M \bullet e(g,g)^{\alpha s}}{e(g,g)^{\alpha s + rs - rs}},\ M = Dec_{mkey'}(C_0)$$

$$V' = V = (g^{H(M')} g^{H(mkey')}) = (g^{H(M)} g^{H(mkey)})$$

V. Analysis of the proposed scheme

• **데이터 기밀성과 무결성:** 본 제안 기법은 속성기반암호의 한 종류인 KP-ABE를 사용하여 통신하는 데이터를 암호화하였다. 암호문에 포함된 속성 $A = [Att_1, Att_2, \cdots, Att_n]$들을 가지고 있는 DSS만이 암호문을 복호화하여 데이터를 획득할 수 있다. 이에 드론에서 수집된 데이터를 DSS의 속성으로 암호화하여 데이터를 전송하면, 속성을 가지고 있는 DSS들만 데이터를 확인할 수 있다. 이에 공유되는 암호문(데이터)에 대한 기밀성이 제공된다. 또한, DSS는 복호화하여 획득한 대칭키와 메시지를 $V = V'$ 검증과정을 통해 메시지에 대한 무결성을 확인할 수 있다.

• **데이터 가용성 및 사용자 접근 제어:** 드론에서 수집된 데이터를 DSS의 속성으로 암호화하여 클라우드 저장하면, 허가된 DSS만이 암호문에 접근하여 암호문을 복호화할 수 있어야 한다. 즉, 암호문에 접근 가능한 DSS는 암호문에 포함된 속성을 내포한 접근구조를 가지고 있어야만 접근이 가능하다. AA로부터 수신받은 비밀키와 찾고자 하는 암호문 키워드 w', 속성 등으로 토큰을 생성해서 클라우드 서버에 보내주면 클라우드 서버는 토큰값과 암호문 인덱스값이 일치하는 암호문들을 DSS에게 전송한다. 이후 DSS는 접근구조와 비밀키로 암호문을 복호화하여 데이터를 획득할 수 있다. 다시 말해, AA로부터 등록되지 않았거나, 암호문에 포함된 속성을 내포한 접근구조를 가지고 있지 못한 DSS는 암호문을 수신받아도 복호화를 성공적으로 수행할 수 없다. 이에 본 제안 기법은 드론으로부터 암호화되어 통신되는 암호문에 대한 가용성 및 접근 제어가 제공된다.

• **암호문 탐색 횟수 및 효율성**: 본 제안 기법은 암호문 인덱스의 포함된 속성값을 $C_4 = \prod_{i=1}^{n} H_1(Att_i)^s$, 사용자가 생성한 토큰에 포함된 속성값 또한 $T_{w'} = e\left(\prod_{i=1}^{n} H_1(Att_i)^k,\ g^{w'}\right)$으로 사전에 집계 연산을 수행하였다. 이는 각각의 속성값 {{A학교}, {학생}}들을 {{A학교}, {학생}}=C_4와 같이 하나의 속성값으로 집계 연산하여 표현할 수 있다. 암호문 탐색 시 암호문 인덱스 속성값과 토큰의 속성값 중 C_4과 일치하는 암호문만 찾으면 되기 때문에 속성의 개수와 상관없다. 이에 본 제안 기법은 암호문 탐색 시 속성의 개수에 영향을 받지 않음으로, 표 1의 기존의 KP-ABE 기법과 비교하여,

Table 1. Comparison of Ciphertext Search Operations between Existing KP-ABE Schemes and Proposed Scheme

	Yin et al. scheme	Ameri et al. scheme	Li et al. scheme	Proposed scheme
Ciphertext index operation	$(n+1)T_E + E + nH$	$(n+4)T_E + (n+2)H + 5M$	$(n+6)T_E + T_M + 2H$	$P + (n+4)T_E + (n-1)T_M + nH$
Ciphertext search operation	$2nP + nE$	$(2n+1)P + 1E$	$(2n+1)P + nT_E + nT_M$	$3P + (n-1)T_M + nT_E$

P :Pairing operation; M :Multiplication operation; E :Exponentiation operation; n : Number of attributes; H: Hash function; T_E: Exponentiation in G; T_M: Multiplication in G;

암호문 탐색 횟수가 속성의 개수에 영향을 받지 않는 장점이 있다. 하지만 사전에 속성값이 미리 집계되기 때문에 암호화 단계(인덱스 생성)와 토큰 생성단계에서 기존 KP-ABE 기법보다 연산량이 많다는 단점이 존재한다. 연산량 수행 시 3.50GHz Intel Core i5-4690 프로세서와 8GB RAM이 장착된 Windows 시스템을 이용하였으며, 페어링 기반 암호화 라이브러리를 참조하였다[14-15]. 본 제안 기법에 반영하여, 암호문 탐색 연산량을 계산하였을 경우 속성의 개수가 5개일 경우 약 15.43ms, 10개일 경우 약 22.83ms가 측정되었다. 이는 속성의 개수에 따라 암호문 탐색 연산량은 늘어나지만, 클라우드 환경에서 충분히 암호문을 탐색할 수 있는 연산량을 가진다.

• **일정한 크기의 암호문 출력:** 암호화 수행 시 암호문의 크기를 일정하게 출력하기 위해서는 위에서 언급한 것과 같이 암호문에 포함된 속성값들을 집계해야 한다. 이는 연산량이 줄어든다는 의미가 아니라, 다수의 속성을 $C_3 = g^s \cdot \prod_{i \in 1}^{n} g^{t_i Att_i}$와 같이 하나의 값으로 표현함으로써, 속성의 개수에 상관없이 암호문의 크기를 일정하게 출력된다. 이는 통신되는 암호문 크기에 영향을 주기 때문에, 필요한 요구사항 중 하나이다.

VI. Conclusions

본 논문에서는 드론 환경에서 안전한 통신을 위해 KP-ABE 기반의 데이터 접근 제어 기법을 제안하였다. 본 제안 기법은 드론으로부터 통신하는 데이터에 대한 기밀성과 무결성이 제공되며, 암호문에 대한 접근 제어 및 가용성이 제공된다. 그리고, 사용자(DSS)가 암호문 요청 시 클라우드 서버는 암호문 복호화 과정 없이 암호문을 탐색하여, 사용자에게 제공해준다. 토큰과 암호문에 포함된 속성의 사전 집계 연산을 통해 속성의 개수에 영향을 받지 않고 1번의 암호문 탐색으로 사용자가 원하는 암호문을 탐색하여 제공하기 때문에, 기존 KP-ABE와 비교하여 효율적인 암호문 탐색을 제공한다. 마지막으로, 속성 집계 연산을 통해 일정 크기 암호문을 제공하여, 암호문에 포함된 속성의 개수에 따라 암호문의 크기가 증가하는 문제점을 해결하였다.

본 논문에서 제안한 기법은 다수의 드론과 소수의 드론 서비스 공급자가 이용하고 있는 N:1 클라우드 환경을 대상으로 적용할 수 있다. 특히, 통신되는 데이터가 민감하거나 중요하여, 보안 기술이 필요한 드론-클라우드 환경에 활용될 수 있다. 그리고 이를 확장하여 다수의 사용자 간의 데이터를 공유할 수 있는 IoT-Cloud 환경 등에 적용할 수 있다[16-17].

향후 연구로는 제안한 KP-ABE 모델을 실제 드론 환경에 적용하여, 드론으로부터 수집되는 데이터에 대한 보안성(안전성) 및 통신에 대한 연산량 등을 측정하기 위한 연구가 필요할 것으로 사료된다.

ACKNOWLEDGEMENT

This research was supported by the Republic of Korea's MSIT (Ministry of Science and ICT), under the High-Potential Individuals Global Training Program (2021-0-01516) supervised by the IITP (Institute of Information and Communications Technology Planning & Evaluation) and was supported by National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2022R1A2B5B01002490).

REFERENCES

[1] X. Zheng, Z. Cai, and Y. Li, “Data Linkage in Smart IoT Systems: A Consideration from Privacy Perspective,” IEEE Communications Magazine, Vol. 56, No. 9, pp. 55-61, September 2018. DOI: 10.1109/MCOM.2018.1701245

[2] J. P. Yaacoub, H. Noura, O. Salman, and A. Chehab, “Security analysis of drones systems: Attacks, limitations, and recommendations,” Internet of Things, Vol. 11, No. 100218, pp. 1-39, May 2020. DOI:https://doi.org/10.1016/j.iot.2020.100218

[3] M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy, N. M. Noor, and A. Bala, “Internet of drones security and privacy issues: Taxonomy and open challenges,” IEEE Access, Vol. 9, pp. 57243-57270, April 2021. DOI: 10.1109/ACCESS.2021.3072030

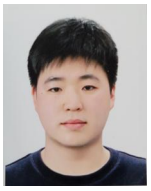
[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” In 2007 IEEE symposium on security and privacy (SP’07), pp. 321-334, 2007.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” In Proceedings of the 13th ACM conference on Computer and communications security, pp. 89-98, 2006.

[6] M. Abdalla, M. Bellare, and P. Rogaway, “The oracle

diffie-hellman assumptions and an analysis of dhies," In Cryptographers' Track at the RSA Conference, pp. 143−158, 2001.
[7] C. Hu, J. Yu, X. Cheng, Z. Tian, and L. Sun, "CP-ABSC: An attributebased signcryption scheme to secure multicast communications in smart grids," In Mathematical foundations of computer science, Vol. 1, No. 1, pp. 77-100, February 2018. DOI: 10.3934/mfc.2018005
[8] C. J. Wang, and J. F. Luo, "A key-policy attribute-based encryption scheme with constant size ciphertext," In 2012 Eighth International Conference on Computational Intelligence and Security, Guangzhou, China, 2012, pp.447-451.
[9] J. Lai, R. H. Deng, Y. Li, and J. Weng, "Fully secure key-policy attributebased encryption with constant-size ciphertexts and fast decryption," In Proceedings of the 9th ACM symposium on Information, computer and communications security, pp. 239-248, 2014.
[10] K. Zhang, J. Gong, S. Tang, J. Chen, X. Li, H. Qian, and Z. Cao, "Practical and efficient attribute-based encryption with constant-size ciphertexts in outsourced verifiable computation," In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, pp.269-279, 2016.
[11] H. Yin, Y. Xiong, J. Zhang, L. Ou, S. Liao, and Z Qin, "A key-policy searchable attribute-based encryption scheme for efficient keyword search and fine-grained access control over encrypted data," Electronics. Vol. 8, No. 3, pp. 1-20, February 2019. DOI: https://doi.org/10.3390/electronics8030265
[12] M. H. Ameri, M. Delavar, J. Mohajeri, and M. Salmasizadeh, "A keypolicy attribute-based temporary keyword search scheme for secure cloud storage," IEEE Transactions on Cloud Computing. Vol. 8, No. 3, pp. 660-671, April 2018. DOI: 10.11 09/TCC.2018.2825983
[13] J. Li, M. Wang, Y. Lu, Y. Zhang, and H. Wang, "ABKS-SKGA: Attributebased keyword search secure against keyword guessing attack," Computer Standards & Interfaces. Vol. 74, pp. 1-7, February 2021. DOI: https://doi.org/10.1016/j.csi.2020.103471
[14] Y. W. Hwang, and I. Y. Lee, "A Study on CP-ABE-Based Medical Data Sharing System with Key Abuse Prevention and Verifiable Outsourcing in the IoMT Environment," Sensors. Vol. 20, No. 17, pp.1-23, August 2020. DOI: https://doi.org/10.33 90/s20174934
[15] Lynn, B., The pairing-based cryptography (PBC) library, http:// crypto.stanford.edu/pbc
[16] B. Girgenti, P. Perazzo, C. Vallati, F. Righetti, G. Dini, and G. Anastasi, "On the feasibility of attribute-based encryption on constrained IoT devices for smart systems," In 2019 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 225-232, 2019.
[17] S. Y. Tan, K. W. Yeow, and S. O. Hwang, "Enhancement of a lightweight attribute-based encryption scheme for the Internet of Things," IEEE Internet of Things Journal, Vol. 6, No. 4, pp. 6384-6395, February 2019. DOI: 10.1109/JIOT.2019.2900631

Authors



Yong-Woon Hwang received the B.S., M.S. degrees in Department of Computer Science Engineering from Soonchunhyang University (SCH), Asan, South Korea, in 2016, 2018 and 2004, respectively.

He is now a Ph.D. candidate in the Department of Software Convergence from Soonchunhyang University (SCH), Asan, South Korea, in 2018. His research interests include Cloud Security, Cryptography, Attribute-based Encryption, Data Sharing.

Su-Hyun Kim received the B.S., M.S. and Ph.D. degrees in Department of Computer Science Engineering from Soonchunhyang University (SCH), Asan, South Korea, in 2010, 2012 and 2016, respectively.

He is currently a Manager in the ICT Industry Strategy at National IT Industry Promotion Agency (NIPA), Jincheon, South Korea. Recently, he has been actively working in the area of NPU (Neural Processing Unit), in particular with respect to government policies. His research interest includes cryptographic protocol, IoT security, AI security.

Im-Yeong Lee received the B.S. degree in electronic engineering from Hongik University, Seoul, in 1981, and the M.S. and Ph.D. degrees in information and communication engineering from Osaka University, Osaka, Japan, in 1986 and 1989, respectively. He is currently a Professor with the Department of Computer Software Engineering, Soonchunhyang University (SCH), Asan, South Korea. His research interests include information security, cryptographic protocol, information theory, and data communication.