



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0101896
(43) 공개일자 2015년09월04일

(51) 국제특허분류(Int. Cl.)

H04L 9/08 (2006.01)

(21) 출원번호 10-2014-0089344

(22) 출원일자 2014년07월15일

심사청구일자 2014년07월15일

(30) 우선권주장

1020140023543 2014년02월27일 대한민국(KR)

(71) 출원인

경희대학교 산학협력단

경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)

(72) 발명자

허의남

경기도 용인시 기흥구 사은로126번길 46, 316동 1802호 (보라동, 현대모닝사이드1차아파트)

나상호

경기도 용인시 기흥구 덕영대로 1732, 전자정보대학 331호 (서천동)

박준영

경기도 용인시 기흥구 덕영대로 1732, 전자정보대학 331호 (서천동)

(74) 대리인

특허법인 신지

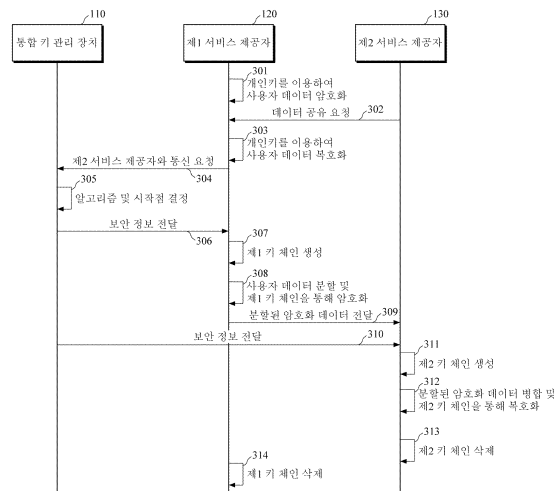
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 인터클라우드 환경에서의 데이터 공유 시스템 및 공유 방법

(57) 요약

본 발명에 따른 인터클라우드 환경에서의 데이터 공유 시스템은 수신된 보안 정보에 기초하여 제1 키체인(Key Chain)을 생성하고, 생성된 제1 키체인을 통해 사용자 데이터를 분할 및 암호화(Encryption)하여 분할된 암호화 데이터를 생성하는 제1 서비스 제공자, 수신된 보안 정보에 기초하여 제2 키체인을 생성하고, 제1 서비스 제공자로부터 수신된 분할된 암호화 데이터를 생성된 제2 키체인으로 병합 및 복호화(Description)하는 제2 서비스 제공자 및 제1 서비스 제공자 및 제2 서비스 제공자에 보안 정보를 제공하는 통합 키 관리 장치를 포함한다.

대표도



특허청구의 범위

청구항 1

수신된 보안 정보에 기초하여 제1 키체인(Key Chain)을 생성하고, 상기 생성된 제1 키체인을 통해 사용자 데이터를 분할 및 암호화(Encryption)하여 분할된 암호화 데이터를 생성하는 제1 서비스 제공자;

수신된 보안 정보에 기초하여 제2 키체인을 생성하고, 상기 제1 서비스 제공자로부터 수신된 상기 분할된 암호화 데이터를 상기 생성된 제2 키체인으로 병합 및 복호화(Description)하는 제2 서비스 제공자; 및

상기 제1 서비스 제공자 및 상기 제2 서비스 제공자에 상기 보안 정보를 제공하는 통합 키 관리 장치;

를 포함하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 시스템.

청구항 2

제1항에 있어서,

상기 통합 키 관리 장치는 상기 제1 서비스 제공자 및 상기 제2 서비스 제공자 사이의 인증을 수행하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 시스템.

청구항 3

제1항에 있어서,

상기 제1 서비스 제공자는 사용자로부터 업로드된 상기 사용자 데이터를 개인키를 이용하여 암호화하여 저장하고, 상기 제2 서비스 제공자로부터 상기 저장된 사용자 데이터의 공유 요청이 수신되면, 상기 저장된 사용자 데이터를 상기 개인키를 이용하여 복호화한 후, 상기 제1 키체인을 이용하여 상기 사용자 데이터를 다시 암호화하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 시스템.

청구항 4

제1항에 있어서,

상기 통합 키 관리 장치는 키체인 알고리즘 및 시작점을 결정하고, 결정된 키체인 알고리즘 및 시작점에 대한 정보를 포함하는 상기 보안 정보를 생성하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 시스템.

청구항 5

제4항에 있어서,

상기 통합 키 관리 장치는

해시 연쇄 함수(Hash Chain Function) 알고리즘 및 테슬라(TESLA) 알고리즘 중에서 어느 하나의 알고리즘을 키체인 알고리즘으로 결정하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 시스템.

청구항 6

제4항에 있어서,

상기 제1 서비스 제공자는 상기 수신된 보안 정보의 키체인 알고리즘에 따라 상기 사용자 데이터를 분할하고, 상기 시작점부터 암호화하여 상기 분할된 암호화 데이터를 생성하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 시스템.

청구항 7

제4항에 있어서,

상기 제2 서비스 제공자는 상기 수신된 보안 정보의 키체인 알고리즘에 따라 상기 분할된 암호화 데이터를 병합하고, 상기 시작점부터 복호화하여 상기 분할된 암호화 데이터로부터 상기 사용자 데이터를 복원하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 시스템.

청구항 8

제1항에 있어서,

상기 제1 서비스 제공자 및 상기 제2 서비스 제공자는 상기 제2 서비스 제공자가 상기 분할된 암호화 데이터를 복호화한 후, 상기 제1 키체인 및 상기 제2 키체인을 삭제하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 시스템.

청구항 9

제1 서비스 제공자 및 제2 서비스 제공자 사이의 데이터 공유 방법에 있어서,

통합 키 관리장치에서 보안 정보를 생성하는 단계;

상기 생성된 보안 정보에 기초하여 상기 제1 서비스 제공자가 제1 키 체인을 생성하는 단계;

상기 제1 서비스 사용자가 상기 제1 키체인을 통해 사용자 데이터를 분할 및 암호화하여 분할된 암호화 데이터를 생성하는 단계;

상기 생성된 보안 정보에 기초하여 상기 제2 서비스 제공자가 제2 키체인을 생성하는 단계;

상기 생성된 제2 키체인에 기초하여 상기 제2 서비스 제공자가 상기 분할된 암호화 데이터를 복호화하는 단계를 포함하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 방법.

청구항 10

제9항에 있어서,

상기 통합 키 관리 장치는 상기 제1 서비스 제공자 및 상기 제2 서비스 제공자 사이의 인증을 수행하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 방법.

청구항 11

제9항에 있어서,

상기 제1 서비스 제공자가 사용자로부터 업로드된 상기 사용자 데이터를 개인키를 이용하여 암호화하여 저장하는 단계;

상기 제2 서비스 제공자로부터 상기 저장된 사용자 데이터의 공유 요청이 수신되면, 상기 개인키를 이용하여 상기 저장된 사용자 데이터를 복호화하는 단계; 및

를 더 포함하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 방법.

청구항 12

제9항에 있어서,

상기 통합 키 관리장치에서 보안 정보를 생성하는 단계는,

상기 통합 키 관리 장치가 키체인 알고리즘 및 시작점을 결정하는 단계; 및

결정된 키체인 알고리즘 및 시작점에 대한 정보를 포함하는 상기 보안 정보를 생성하는 단계;

를 포함하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 방법.

청구항 13

제12항에 있어서,

상기 통합 키 관리 장치가 키체인 알고리즘 및 시작점을 결정하는 단계는 해시 연쇄 함수(Has Chain Function) 알고리즘 및 테슬라(TESLA) 알고리즘 중에서 어느 하나의 알고리즘을 키체인 알고리즘으로 결정하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 방법.

청구항 14

제12항에 있어서,
 상기 분할된 암호화 데이터를 생성하는 단계는,
 상기 제1 서비스 제공자가 상기 보안 정보의 키체인 알고리즘에 따라 상기 사용자 데이터를 분할하는 단계; 및
 상기 시작점부터 암호화하여 상기 분할된 암호화 데이터를 생성하는 단계;
 를 포함하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 방법.

청구항 15

제12항에 있어서,
 상기 분할된 암호화 데이터를 복호화하는 단계는,
 상기 제2 서비스 제공자가 상기 보안 정보의 키체인 알고리즘에 따라 상기 분할된 암호화 데이터를 병합하는 단계; 및
 상기 시작점부터 복호화하여 상기 분할된 암호화 데이터로부터 상기 사용자 데이터를 복원하는 단계;
 를 포함하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 방법.

청구항 16

제9항에 있어서,
 상기 분할된 암호화 데이터를 복호화하는 단계 이후, 상기 제1 키체인 및 상기 제2 키체인을 삭제하는 단계;
 를 더 포함하는 것을 특징으로 하는 인터클라우드 환경에서의 데이터 공유 방법.

명세서

기술 분야

[0001] 본 발명은 클라우드 서비스의 보안과 관련된 기술로서, 보다 상세하게는 클라우드 서비스의 보안키 관리 방법에 관한 기술이다.

배경 기술

[0002] 클라우드 컴퓨팅 서비스가 다양해지고 서비스의 질이 향상됨에 따라 단일 클라우드 서비스를 이용하기 보다는 클라우드 서비스 간 연동 및 협업하는 인터클라우드(Inter-Cloud)와 같은 서비스가 늘어나고 있다. 하지만, 서로 다른 클라우드 서비스 제공자를 기반으로 제공되는 인터클라우드 서비스는 몇 가지 문제점을 가지고 있다.

[0003] 모든 클라우드 서비스가 사용자에게 대한 개인키를 생성하여 데이터 암호화 서비스를 제공하고 암호화된 데이터를 다른 클라우드 서비스와 공유하는 경우, 안전한 데이터 공유를 위해서는 데이터가 암호화되어 타 클라우드 서비스 제공자에게 전송되어야 한다. 하지만, 이러한 경우 각 클라우드 서비스에서 제공하는 개인키가 모두 상이하므로 복호화가 불가능하다. 따라서, 각 클라우드 서비스는 사용자의 데이터를 암호화하는 개인키 관리와 데이터 공유를 위한 타 클라우드 서비스와 서로 암호화 및 복호화 가능한 키를 생성 및 관리해야 한다. 이러한 경우, 다양한 클라우드 서비스에 따라 암호화 키의 수가 늘어나기 때문에 키 관리가 어려워 질 수 있다.

[0004] 그리고, 클라우드 서비스 제공자간의 암호화된 데이터를 공유하기 위해서는 복호화가 가능한 키가 필요하다. 하지만, 키가 전달하는 과정이 많아지고 반복되다 보면 키가 노출될 수 있으며, 만약 노출될 경우 개인 데이터에 대한 위협과 관련 모든 클라우드 서비스에 위협이 될 수 있다. 또한, 클라우드 서비스 제공자간의 암호화 통신 세션을 통하여 평문(Pain-text)의 데이터 전송이 가능하지만, 이러한 통신세션이 무력화될 경우 평문의 데이터는 그대로 노출이 될 수 있다. 예를 들어, HTTPS와 같은 암호화 통신프로토콜을 사용할 경우 SSL Strip기법과 같은 패킷 스니핑을 이용한 중간자 공격(Man In The Middle attack, MITM)에 의해 민감한 정보(데이터)가 포함된 메시지가 노출될 수 있다.

[0005] 대한민국 공개특허 제10-2014-0009708호는 클라우드 컴퓨팅 환경에서 암호화를 위한 사용자 단말 장치 및 암호화 방법을 개시하고 있다. 대한민국 공개특허 제10-2014-0009708호는 서버와 단말 사이의 암호화에 있어서 후킹 모듈을 사용해 보안 데이터를 모니터링하는 내용만을 포함하고 있을 뿐, 복잡한 암호화키의 관리 효율을 높여주

지 못한다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 공개특허 제10-2014-0009708호

발명의 내용

해결하려는 과제

[0007] 본 발명이 해결하고자 하는 과제는 서로 다른 클라우드 서비스 제공자 간의 안전한 데이터 공유가 가능하도록 통합적인 키 관리를 제공하고, 키가 노출되더라도 안전하게 서비스를 제공받을 수 있는 안전한 데이터 공유 시스템 및 공유 방법을 제공하는 것이다.

과제의 해결 수단

[0008] 본 발명에 따른 인터클라우드 환경에서의 데이터 공유 시스템은 수신된 보안 정보에 기초하여 제1 키체인(Key Chain)을 생성하고, 생성된 제1 키체인을 통해 사용자 데이터를 분할 및 암호화(Encryption)하여 분할된 암호화 데이터를 생성하는 제1 서비스 제공자, 수신된 보안 정보에 기초하여 제2 키체인을 생성하고, 제1 서비스 제공자로부터 수신된 분할된 암호화 데이터를 생성된 제2 키체인으로 병합 및 복호화(Description)하는 제2 서비스 제공자 및 제1 서비스 제공자 및 제2 서비스 제공자에 보안 정보를 제공하는 통합 키 관리 장치를 포함한다.

[0009] 통합 키 관리 장치는 제1 서비스 제공자 및 제2 서비스 제공자 사이의 인증을 수행할 수 있다. 그리고, 제1 서비스 제공자는 사용자로부터 업로드된 사용자 데이터를 개인키를 이용하여 암호화하여 저장하고, 제2 서비스 제공자로부터 저장된 사용자 데이터의 공유 요청이 수신되면, 저장된 사용자 데이터를 개인키를 이용하여 복호화한 후, 제1 체인키를 이용하여 상기 사용자 데이터를 다시 암호화한다. 이 과정에서, 통합 키 관리 장치는 키체인 알고리즘 및 시작점을 결정하고, 결정된 키체인 알고리즘 및 시작점에 대한 정보를 포함하는 보안 정보를 생성한다. 통합 키 관리 장치는 해시 연쇄 함수(Hash Chain Function) 알고리즘 및 테슬라(TESLA) 알고리즘 등과 같은 키 체인 알고리즘들 중에서 어느 하나의 알고리즘을 선택하여 데이터 암호화에 사용될 키체인 알고리즘으로 결정할 수 있다. 제1 서비스 제공자는 전송할 데이터를 정해진 크기의 데이터 블록(Data Block)으로 분할하고 수신된 보안 정보인 선택된 키체인 알고리즘 정보와 생성된 키 체인을 사용할 시작점에 관한 정보에 따라 키체인 생성과 시작점부터의 키 체인을 이용하여 한 데이터 블록당 하나의 암호화 키로 데이터 블록을 암호화한다. 제2 서비스 제공자는 수신된 보안 정보인 선택된 키체인 알고리즘과 키체인 사용 시작점에 따라 키 체인을 생성 및 시작점의 복호화 키를 이용하여 복호화 및 데이터 병합을 수행한다. 그리고, 제1 서비스 제공자 및 제2 서비스 제공자는 제2 서비스 제공자가 분할된 암호화 데이터를 복호화한 후, 제1 키체인 및 제2 키체인을 삭제한다.

[0010] 본 발명에 따른 인터클라우드 환경에서의 데이터 공유 방법은 먼저, 통합 키 관리장치에서 보안 정보(선택된 키체인 알고리즘 정보와 키체인 사용 시작점 정보)를 생성한다. 그리고, 생성된 보안 정보에 기초하여 제1 서비스 제공자가 제1 키 체인을 생성하고, 제1 키체인을 통해 사용자 데이터를 분할 및 암호화하여 분할된 암호화 데이터를 생성한다. 그리고, 생성된 보안 정보에 기초하여 제2 서비스 제공자가 제2 키체인을 생성하고, 제1 서비스 제공자로부터 수신된 분할된 암호화 데이터를 제2 키체인을 통해 복호화한다.

발명의 효과

[0011] 본 발명에 따른 인터클라우드 환경에서의 데이터 공유 시스템 및 공유 방법은 클라우드 서비스 제공자간의 안전한 데이터 공유와 암호화 키 통합관리로 중복적인 키 관리 시스템 개발을 막아 개발 비용을 절감할 수 있다. 또한, 키가 노출되더라도 통신이 끝난 후에는 키를 삭제하는 일회용 암호화키 사용으로 키가 노출되더라도 시스템 및 데이터에 대한 위협을 줄일 수 있다.

도면의 간단한 설명

[0012] 도 1은 본 발명에 따른 인터클라우드 환경에서의 데이터 공유 시스템의 일 실시예를 나타내는 구성도이다.

도 2는 본 발명의 일 실시예에 따른 인터클라우드 환경에서의 데이터 공유 시스템의 키체인을 설명하기 위한 도면이다.

도 3은 본 발명의 일 실시예에 따른 인터클라우드 환경에서의 데이터 공유 시스템의 데이터 처리 과정을 나타내는 흐름도이다.

도 4는 본 발명의 일 실시예에 따른 인터클라우드 환경에서의 데이터 공유 방법을 나타내는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0013] 이하, 본 발명의 실시예를 첨부된 도면들을 참조하여 상세하게 설명한다. 본 명세서에서 사용되는 용어 및 단어들은 실시예에서의 기능을 고려하여 선택된 용어들로서, 그 용어의 의미는 발명의 의도 또는 관례 등에 따라 달라질 수 있다. 따라서 후술하는 실시예에서 사용된 용어는, 본 명세서에 구체적으로 정의된 경우에는 그 정의에 따르며, 구체적인 정의가 없는 경우는 당업자들이 일반적으로 인식하는 의미로 해석되어야 할 것이다.
- [0014] 도 1은 본 발명에 따른 인터클라우드 환경에서의 데이터 공유 시스템의 일 실시예를 나타내는 구성도이다.
- [0015] 도 1을 참조하면, 본 발명에 따른 인터클라우드 환경에서의 데이터 공유 시스템은 통합 키 관리 장치(110), 제1 서비스 제공자(120) 및 제2 서비스 제공자(130)를 포함할 수 있다.
- [0016] 통합 키 관리 장치(110)는 제1 서비스 제공자(120)로부터 사용자 데이터를 제2 서비스 제공자(130)와 공유하겠다는 요청이 수신되면, 제1 서비스 제공자(120) 및 제2 서비스 제공자(130)에 대한 인증을 수행한다. 그리고, 통합 키 관리 장치(110)는 키체인 알고리즘 정보 및 시작점 정보를 포함하는 보안 정보를 제1 서비스 제공자(120) 및 제2 서비스 제공자(130)로 전달한다.
- [0017] 제1 서비스 제공자(120) 및 제2 서비스 제공자(130)는 사용자에게 클라우드 서비스를 제공하는 클라우드 서비스 제공자를 나타낸다. 그리고, 제1 서비스 제공자(120) 및 제2 서비스 제공자(130)는 사용자의 데이터를 안전하게 저장 및 관리하기 위한 개인키를 생성한다. 제1 서비스 제공자(120) 및 제2 서비스 제공자(130)는 생성된 개인키를 이용하여 사용자로부터 업로드(Upload)된 데이터를 개인키를 이용하여 암호화(Encryption)하여 저장한다. 제1 서비스 제공자(120)에서 생성된 개인키와 제2 서비스 제공자(130)에서 생성된 개인키는 서로 상이하다. 즉, 서로 다른 클라우드 서비스 제공자는 각각의 개인키를 이용하여 사용자의 데이터를 암호화하여 저장한다.
- [0018] 사용자는 서로 다른 클라우드 서비스 제공자(110,120) 사이에서 업로드된 데이터를 공유할 수 있다. 예를 들어, 사용자는 제1 서비스 제공자(120)에 업로드된 데이터를 제2 서비스 제공자(130)를 통해 공유할 수 있다. 제1 서비스 제공자(120)는 제2 서비스 제공자(130)로부터 데이터 공유 요청이 수신되면, 소정의 인증 절차를 거쳐 제2 서비스 제공자(130)를 승인한다.
- [0019] 제2 서비스 제공자(130)가 인증되면, 제1 서비스 제공자(120)는 통합 키 관리 장치(110)에 제2 서비스 제공자(130)와의 통신을 요청한다. 통합 키 관리 장치(110)로부터 보안 정보가 전달되면, 제1 서비스 제공자(120)는 수신된 보안 정보에 기초하여 제1 키체인(Key Chain)을 생성한다. 그리고, 제1 서비스 사용자(110)는 제1 키체인에 기초하여 사용자의 데이터를 일정크기로 세분화하여 둘 이상의 사용자 데이터로 분할하고 분할된 둘 이상의 사용자 데이터를 키체인으로 암호화하여 제2 서비스 사용자(120)로 전달한다. 보안 정보는 키체인 알고리즘에 따라 사용자 데이터를 분할 및 암호화하기 위한 정보로서 후술하는 도 2에서 추가적으로 설명하도록 한다.
- [0020] 제1 서비스 제공자(120)는 저장된 사용자 데이터가 개인키를 통해 암호화되어 있다면, 키체인을 통해 분할 및 암호화하기 이전에 개인키를 통해 복호화를 먼저 수행할 수 있다. 그리고, 제1 서비스 제공자(120)는 암호화된 사용자 데이터를 제2 서비스 사용자(120)로 전달할 때, 암호통신 프로토콜을 이용하여 이중 암호화하여 전달할 수 있다.
- [0021] 제2 서비스 제공자(130)는 사용자 데이터를 공유하기 위해 제1 서비스 제공자(120)에 데이터 공유 요청을 전달한다. 제1 서비스 제공자(120)가 제2 서비스 제공자(130)를 인증하면, 통합 키 관리 장치(110)로부터 키체인 알고리즘의 종류 및 시작점 정보가 포함된 보안 정보를 수신한다. 제2 서비스 제공자(130)로 전달된 보안 정보는 제1 서비스 제공자(120)로 전달된 보안 정보와 동일하다. 제2 서비스 제공자(130)는 수신된 보안 정보에 기초하여 제2 키체인을 생성한다. 제1 키체인 및 제2 키체인은 동일한 보안 정보에 따라 생성되었기 때문에, 서로 동일한 키체인이 된다.

- [0022] 그리고, 제2 서비스 제공자(130)는 제1 서비스 제공자(120)로부터 수신된 분할된 암호화 데이터를 생성된 제2 키체인을 이용하여 복호화한다. 제1 서비스 제공자(120)로부터 수신된 분할된 암호화 데이터는 보안 정보에 기초하여 생성된 키체인을 통해 분할 및 암호화되어 있다. 제2 서비스 제공자(130)는 제1 서비스 제공자(120)와 보안 정보를 이용하여 제1 키체인과 동일한 제2 키체인을 생성한다. 그리고, 제2 서비스 제공자(130)는 수신된 분할 및 암호화 된 사용자 데이터를 제1 키체인과 동일한 제2 키체인을 이용하여 순서대로 복호화 및 데이터 병합을 수행한다.
- [0023] 제2 서비스 제공자(130)에서 사용자 데이터를 복호화하는데 이용된 제2 키체인과 제1 서비스 제공자(120)에서 사용자 데이터를 암호화하는데 이용된 제1 키체인은 은 사용자 데이터를 복호화한 후 삭제된다. 제1 서비스 제공자(120) 및 제2 서비스 제공자(130) 사이의 데이터 공유가 끝난 경우, 제1 서비스 제공자(120) 및 제2 서비스 제공자(130)는 생성된 키체인을 삭제하여 키 노출을 최소화한다.
- [0024] 도 2는 본 발명의 일 실시예에 따른 인터클라우드 환경에서의 데이터 공유 시스템의 키체인을 설명하기 위한 도면이다.
- [0025] 도 2를 참조하면, 본 발명의 일 실시예에 따른 인터클라우드 환경에서의 데이터 공유 시스템의 제1 서비스 제공자(120) 및 제2 서비스 제공자(130)에서 생성하는 키체인은 해시 연쇄 함수(Hash Chain Function) 알고리즘 또는 테슬라 알고리즘 등을 기반으로 생성될 수 있다.
- [0026] 해시 연쇄 함수는 키를 연속적으로 생성하여 데이터의 조각을 해시 함수 기반으로 암호화하여 제공한다. 컴퓨터 보안에서 해시 연쇄 함수는 암호화 키 또는 패스워드를 일회성 키로 만들어내는 방법 중 하나이다. 해시 연쇄는 데이터의 조각을 연속적으로 암호화하기 때문에 부인방지를 위해 연대표(순번)를 기록하여 데이터와 함께 전송한다. 해시 연쇄 함수를 이용한 키체인 암호화 기법은 문자 x 값으로 암호화 해시 함수 $h(x)$ 를 연속적으로 적용하는 암호화 알고리즘이다. 해시 연쇄 함수는 예를 들어, $h(h(h(h(x))))$ 이 될 때 해시 체인 길이(Length)는 4이며 $h^4(x)$ 라고 표기할 수 있다. 또 다른 키체인 생성 방법으로 테슬라 알고리즘을 이용할 수 있다. 테슬라 기법은 키 생성이 역방향으로 이루어지기 때문에 사전에 데이터의 크기를 알고 있어야 한다.
- [0027] 본 발명의 일 실시예에 따른 인터클라우드 환경에서의 데이터 공유 시스템은 이와 같은 방법을 이용하여 키체인을 생성하고, 생성된 키체인을 통해 사용자 데이터를 분할/암호화 및 병합/복호화한다.
- [0028] 통합 키 관리 장치(110)는 제1 서비스 제공자(120) 및 제2 서비스 제공자(130)로 보안 정보를 전달한다. 통합 키 관리 장치(110)로부터 전달되는 보안 정보는 키체인 알고리즘 종류, 시작점 정보를 포함한다. 제1 서비스 제공자(120) 및 제2 서비스 제공자(130)는 수신된 보안 정보에 포함된 키체인 알고리즘 종류, 시작점 정보 및 체인 길이 정보를 이용하여 키체인을 생성한다. 키체인 알고리즘 종류는 다양한 키체인 알고리즘 중에서 선택된 키체인 알고리즘의 종류를 나타낸다. 그리고, 시작점 정보는 키체인이 몇 번째 암호화 키부터 생성될 지를 나타내는 시작점에 대한 정보이다. 그리고, 체인 길이 정보는 생성되는 키체인의 개수로서, 사용자 데이터의 분할 개수를 나타낸다. 체인 길이 정보는 사용자 데이터의 파일 크기 및 사전 설정에 따라 달라질 수 있다.
- [0029] 도 2는 해시 체인 함수를 이용한 키체인 알고리즘의 실시예를 나타낸다. 제1 서비스 제공자(120)는 수신된 보안 정보(211)를 통해 키체인 알고리즘의 종류가 해시 체인 알고리즘이고, 시작점이 3이라는 것을 확인한다. 그리고, 제1 서비스 제공자(120)는 수신된 사용자 데이터를 분할(212)하고, 수신된 보안정보(211)를 통해 키체인(213)을 생성한다. 다음으로, 분할된 사용자 데이터를 키체인을 통해 암호화(214)하여 제2 서비스 제공자(130)로 전달한다. 제2 서비스 제공자(130)는 수신된 보안정보(221)를 통해 키체인(222)을 생성하고, 생성된 키체인(222)을 통해 암호화 데이터(214)를 복호화(223)하고, 병합(224)하여 사용자 데이터를 복원한다.
- [0030] 예를 들어, 보안 정보에 포함된 키체인 알고리즘이 해시 체인 함수이고, 시작점 정보가 4번이고 체인 길이(사용자 데이터의 분할 개수)가 10개일 경우, 제1 서비스 제공자(120)는 사용자 데이터를 10개의 조각으로 분할하고, 해시 체인 함수에 정해진 x 값을 이용하여 키체인 4번부터 13번까지 데이터 조각 10개에 대해서 암호화를 수행한다. 해시 체인 함수에서 정해진 x 값은 사전에 제1 서비스 제공자(120) 및 제2 서비스 제공자(130)에서 정의된 값으로, 해쉬 연쇄 알고리즘에서 사용되는 변수이다. x 값을 이용하여 첫 번째 키체인을 생성하고, 첫 번째 키체인 값을 이용하여 두 번째 키체인값을 생성한다. 따라서, x 는 키체인을 생성하는 첫 번째 변수가 되기 때문에, 제1 서비스 제공자(120) 및 제2 서비스 제공자(130) 모두 사전에 x 값을 알고 있어야 한다.
- [0031] 그리고, 제1 서비스 제공자(120)는 시작점 정보 4에 기반하여, $h^4(x)$ 부터 $h^{13}(x)$ 까지 총 10개의 키 값을 생성하고, 10개로 분할된 사용자 데이터와 10개의 키를 대응시켜 암호화하여, 제1 암호화 데이터(Encrypted Data 1)부터 제10 암호화 데이터(Encrypted Data 10)를 포함하는 분할된 암호화 데이터를 생성한다. 즉, 제1 서비스 제공

자(120)는 $\text{Data1} + \text{key}(h^4(x)) = \text{Encrypted Data 1}$ 부터 $\text{Data10} + \text{key}(h^{13}(x)) = \text{Encrypted Data 10}$ 으로 10개의 데이터 조각을 암호화한다. 분할된 암호화 데이터가 생성되면, 제1 서비스 제공자(120)는 10개의 암호화된 데이터를 포함하는 분할된 암호화 데이터를 제2 서비스 제공자(130)로 전달한다.

[0032] 제2 서비스 제공자(110)는 제1 서비스 제공자(120)와 동일하게, 수신된 보안 정보에 기초하여 제2 키체인을 생성하고, 생성된 키체인을 통해 제1 서비스 제공자(120)로부터 수신된 10개의 암호화된 데이터를 포함하는 분할된 암호화 데이터를 병합 및 복호화한다. 그리고, 제1 서비스 제공자(120) 및 제2 서비스 제공자(130)는 작업 종료 후 생성된 키체인을 삭제하여 키체인 노출을 최소화한다.

[0033] 도 2의 실시예에서는 해시 체인 알고리즘을 사용하였으며, 테슬라 알고리즘 및 해시 체인 알고리즘 중에서 어느 하나의 알고리즘을 선택하는 것으로 기재되어 있으나, 키체인 알고리즘의 종류를 상술한 두 가지 알고리즘으로 한정하는 것은 아니며, 일반적으로 사용되는 키체인 알고리즘을 제약 없이 적용할 수 있다.

[0034] 도 3은 본 발명의 일 실시예에 따른 인터클라우드 환경에서의 데이터 공유 시스템의 데이터 처리 과정을 나타내는 흐름도이다.

[0035] 도 3을 참조하면, 본 발명의 일 실시예에 따른 인터클라우드 환경에서의 데이터 공유 시스템의 데이터 처리 과정은 먼저, 사용자로부터 사용자 데이터를 수신한 제1 서비스 제공자(120)는 수신된 사용자 데이터를 개인키를 이용하여 암호화하여 저장한다(301). 제1 서비스 제공자(120)는 사용자에게 클라우드 서비스를 제공한다. 따라서, 사용자는 본인이 소유한 데이터를 제1 서비스 제공자(120)에 전달하여 저장할 수 있다. 제1 서비스 제공자(120)는 사용자로부터 데이터가 수신되면, 수신된 데이터를 저장하기 전에 보안을 위하여 일반적으로 이용되는 개인키를 통해 데이터를 암호화하여 저장할 수 있다. 그리고, 제2 서비스 제공자(130)로부터 데이터 공유 요청이 수신(302)되면, 제1 서비스 제공자(120)는 개인키를 이용하여 저장된 사용자 데이터를 복호화한다(303). 인터클라우드 환경에서 사용자는 하나의 클라우드 서비스에 업로드한 데이터를 다른 클라우드 서비스를 통해 공유할 수 있다. 따라서, 이와 같은, 클라우드 공유 서비스를 위해 제2 서비스 제공자(130)는 제1 서비스 제공자(130)로 사용자 데이터의 공유를 요청한다. 제1 서비스 제공자(130)는 데이터 공유 이전에, 제2 서비스 제공자(130)가 사용자에게 승인된 대상인지를 판단하여 제2 서비스 제공자(130)를 승인할 수 있다. 제1 서비스 제공자(130)는 301 단계에서 개인키를 이용하여 암호화한 사용자 데이터를 공유할 수 있도록 복호화한다. 그리고, 제1 서비스 제공자(120)는 통합 키 관리 장치(110)에 제2 서비스 제공자(130)와의 통신을 요청한다(304).

[0036] 제1 서비스 제공자(120)로부터 제2 서비스 제공자와의 통신 요청이 수신되면, 통합 키 관리 장치(110)는 키체인을 생성하기 위한 알고리즘 및 시작점을 결정한다(305). 본 발명에서 사용되는 키체인은 해시 연쇄 함수 알고리즘 또는 테슬라 알고리즘 등의 키체인을 이용할 수 있다. 따라서, 통합 키 관리 장치(110)는 해시 연쇄 함수 알고리즘 또는 테슬라 알고리즘 등 중에서 키체인을 생성하기 위한 알고리즘을 결정한다. 그리고, 통합 키 관리 장치(110)는 결정된 키체인 알고리즘에 따라 시작점을 결정한다. 알고리즘 및 시작점이 결정되면, 통합 키 관리 장치(110)는 결정된 알고리즘 및 시작점에 대한 정보를 포함하는 보안 정보를 생성하여 제1 서비스 제공자(120)로 전달한다(306).

[0037] 통합 키 관리 장치(110)로부터 보안 정보가 수신되면, 제1 서비스 제공자(120)는 수신된 보안 정보에 기초하여 제1 키체인을 생성한다(307). 통합 키 관리 장치(110)로부터 전달되는 보안 정보는 키체인 알고리즘 정보 및 시작점 정보를 포함한다. 제1 서비스 제공자(120)는 수신된 보안 정보에 포함된 키체인 알고리즘 정보 및 시작점 정보를 이용하여 제1 키체인을 생성한다. 그리고, 제1 서비스 제공자(120)는 생성된 제1 키체인을 통해 사용자 데이터를 분할하여 암호화한다(308). 제1 서비스 제공자(120)는 사용자 데이터를 분할하고, 보안 정보에 포함된 키체인 알고리즘에 따라 암호화한다. 예를 들어, 보안 정보에 포함된 키체인 알고리즘이 해시 체인 함수이고, 시작점 정보가 4이며 제1 서비스 제공자(120)가 데이터가 10조각으로 분할한 경우, 제1 서비스 제공자(120)는 시작점 정보 4에 기반하여, $h4(x)$ 부터 $h13(x)$ 까지 총 10개의 키 값을 생성하고, 10개로 분할된 사용자 데이터와 10개의 키를 대응시켜 암호화하여, 제1 암호화 데이터(Encrypted Data 1)부터 제10 암호화 데이터(Encrypted Data 10)를 포함하는 분할된 암호화 데이터를 생성한다. 분할된 암호화 데이터가 생성되면, 제1 서비스 제공자(120)는 분할된 암호화 데이터를 제2 서비스 제공자(130)로 전달한다(309).

[0038] 그리고, 통합 키 관리 장치(110)는 305 단계에서 결정된 알고리즘 및 시작점을 포함하는 보안 정보를 제2 서비스 제공자(130)로 전달한다(310). 통합 키 관리 장치(110)로부터 보안 정보가 수신되면, 제2 서비스 제공자(130)는 307 단계와 동일하게 수신된 보안 정보에 기초하여 제2 키체인을 생성한다(311). 제1 키체인 및 제2 키체인은 동일한 보안 정보에 의해 생성되기 때문에, 서로 동일한 키체인이 된다. 310 단계 및 311 단계는 반드시

시 309 단계 이후에 수행되는 것은 아니며, 306 단계 및 307 단계와 동일한 시점에 실행될 수 있다.

[0039] 그리고, 제1 서비스 제공자(120)로부터 수신된 분할된 암호화 데이터를 병합하고, 생성된 제2 키체인을 이용하여 복호화한다(312). 제2 서비스 제공자(130)에서 생성된 제2 키체인은 제1 서비스 제공자(120)에서 분할된 암호화 데이터를 분할 및 암호화하는데 이용된 제1 키체인과 동일한 키체인이다. 따라서, 제2 서비스 제공자(130)는 분할된 암호화 데이터를 하나의 데이터로 병합하고, 제1 키체인과 동일한 제2 키체인을 이용하여 병합된 데이터를 복호화하여 사용자 데이터를 복원함으로써, 제1 서비스 제공자(120)와 사용자 데이터를 공유할 수 있다. 제2 서비스 제공자(130)에서 분할된 암호화 데이터의 병합 및 복호화가 완료되면, 제2 서비스 제공자(130)는 생성된 제2 키체인을 삭제한다(313). 그리고, 제1 서비스 제공자(120)도 생성된 제1 키체인을 삭제한다(314). 제1 키체인 및 제2 키체인을 암호화 및 복호화를 수행하여 데이터 공유를 완료한 후 삭제하여 키 노출을 최소화할 수 있다.

[0040] 도 4는 본 발명의 일 실시예에 따른 인터클라우드 환경에서의 데이터 공유 방법을 나타내는 흐름도이다.

[0041] 도 4를 참조하면, 본 발명의 일 실시예에 따른 인터클라우드 환경에서의 데이터 공유 방법은 먼저, 사용자로부터 제1 서비스 제공자로 업로드된 사용자 데이터를 개인키로 암호화하여 저장한다(S401). 제1 서비스 제공자는 사용자에게 클라우드 서비스를 제공한다. 따라서, 사용자는 본인이 소유한 데이터를 제1 서비스 제공자에 전달하여 저장할 수 있다. 제1 서비스 제공자는 사용자로부터 데이터가 수신되면, 수신된 데이터를 저장하기 전에 보안을 위하여 일반적으로 이용되는 개인키를 통해 데이터를 암호화하여 저장할 수 있다. 그리고, 제2 서비스 제공자로부터 데이터 공유 요청이 수신되면, 제1 서비스 제공자는 개인키를 이용하여 저장된 사용자 데이터를 복호화한다(S402). 인터클라우드 환경에서 사용자는 하나의 클라우드 서비스에 업로드한 데이터를 다른 클라우드 서비스를 통해 공유할 수 있다. 따라서, 이와 같은, 클라우드 공유 서비스를 위해 제2 서비스 제공자는 제1 서비스 제공자로 사용자 데이터의 공유를 요청한다. 제1 서비스 제공자는 데이터 공유 이전에, 제2 서비스 제공자가 사용자에게 승인된 대상인지를 판단하여 제2 서비스 제공자를 승인할 수 있다. 제1 서비스 제공자는 S401 단계에서 개인키를 이용하여 암호화한 사용자 데이터를 공유할 수 있도록 복호화한다.

[0042] 제1 서비스 제공자 및 제2 서비스 제공자 사이의 사용자 데이터 공유를 위해 통합 키 관리 장치는 키체인을 생성하기 위한 알고리즘 및 시작점을 결정하여 보안 정보를 생성하고, 생성된 보안 정보를 제1 서비스 제공자 및 제2 서비스 제공자로 전달한다(S403). 본 발명에서 사용되는 키체인은 해시 연쇄 함수 알고리즘 또는 테슬라 알고리즘 기반의 키체인을 이용할 수 있다. 따라서, 통합 키 관리 장치는 해시 연쇄 함수 알고리즘 또는 테슬라 알고리즘 중에서 키체인을 생성하기 위한 알고리즘을 결정한다. 그리고, 통합 키 관리 장치는 결정된 키체인 알고리즘에 따라 시작점을 결정한다. 알고리즘 및 시작점이 결정되면, 통합 키 관리 장치는 결정된 알고리즘 및 시작점에 대한 정보를 포함하는 보안 정보를 생성하여 제1 서비스 제공자 및 제2 서비스 제공자로 전달한다.

[0043] 통합 키 관리 장치로부터 보안 정보가 수신되면, 제1 서비스 제공자는 수신된 보안 정보에 기초하여 제1 키체인을 생성한다(S404). 통합 키 관리 장치로부터 전달되는 보안 정보는 키체인 알고리즘 정보 및 시작점 정보를 포함한다. 제1 서비스 제공자는 수신된 보안 정보에 포함된 키체인 알고리즘 정보 및 시작점 정보를 이용하여 제1 키체인을 생성한다. 그리고, 제1 서비스 제공자는 생성된 제1 키체인을 통해 사용자 데이터를 분할하여 암호화한다(S405). 제1 서비스 제공자는 보안 정보에 포함된 키체인 알고리즘에 따라 사용자 데이터를 분할하고, 암호화한다. 그리고, 분할된 암호화 데이터가 생성되면, 제1 서비스 제공자는 분할된 암호화 데이터를 제2 서비스 제공자로 전달한다(S406).

[0044] 통합 키 관리 장치로부터 보안 정보가 수신되면, 제2 서비스 제공자는 수신된 보안 정보에 기초하여 제2 키체인을 생성한다(S407). 제1 키체인 및 제2 키체인은 동일한 보안 정보에 의해 생성되기 때문에, 서로 동일한 키체인이 된다. 그리고, 제1 서비스 제공자로부터 수신된 분할된 암호화 데이터를 생성된 제2 키체인을 이용하여 병합하고, 복호화한다(S408). 제2 서비스 제공자에서 생성된 제2 키체인은 제1 서비스 제공자에서 분할된 암호화 데이터를 분할 및 암호화하는데 이용된 제1 키체인과 동일한 키체인이다. 따라서, 제2 서비스 제공자는 제1 키체인과 동일한 제2 키체인을 이용하여 분할된 암호화 데이터를 하나의 데이터로 병합하고, 병합된 데이터를 복호화하여 사용자 데이터를 복원함으로써, 제1 서비스 제공자와 사용자 데이터를 공유할 수 있다. 제2 서비스 제공자에서 분할된 암호화 데이터의 병합 및 복호화가 완료되면, 제1 서비스 제공자 및 제2 서비스 제공자는 생성된 제1 키체인 및 제2 키체인을 삭제한다(S409). 제1 키체인 및 제2 키체인을 암호화 및 복호화를 수행하여 데이터 공유를 완료한 후 삭제하여 키 노출을 최소화할 수 있다.

[0045]

상술한 내용을 포함하는 본 발명은 컴퓨터 프로그램으로 작성이 가능하다. 그리고 상기 프로그램을 구성하는 코드 및 코드 세그먼트는 당분야의 컴퓨터 프로그래머에 의하여 용이하게 추론될 수 있다. 또한, 상기 작성된 프로그램은 컴퓨터가 읽을 수 있는 기록매체 또는 정보저장매체에 저장되고, 컴퓨터에 의하여 관독되고 실행함으로써 본 발명의 방법을 구현할 수 있다. 그리고 상기 기록매체는 컴퓨터가 관독할 수 있는 모든 형태의 기록매체를 포함한다.

[0046]

이상 바람직한 실시예를 들어 본 발명을 상세하게 설명하였으나, 본 발명은 전술한 실시예에 한정되지 않고, 본 발명의 기술적 사상의 범위 내에서 당분야에서 통상의 지식을 가진자에 의하여 여러 가지 변형이 가능하다.

부호의 설명

[0047]

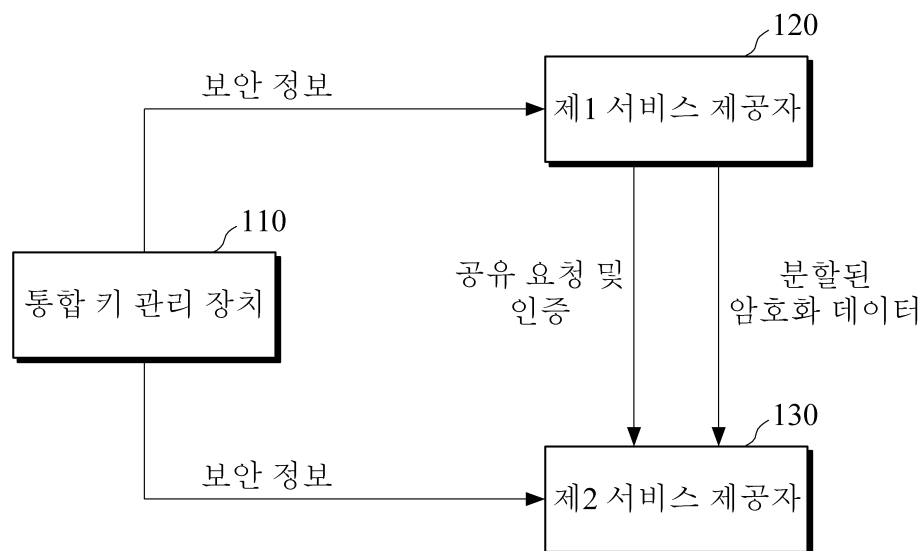
110: 통합 키 관리 장치

120: 제1 서비스 제공자

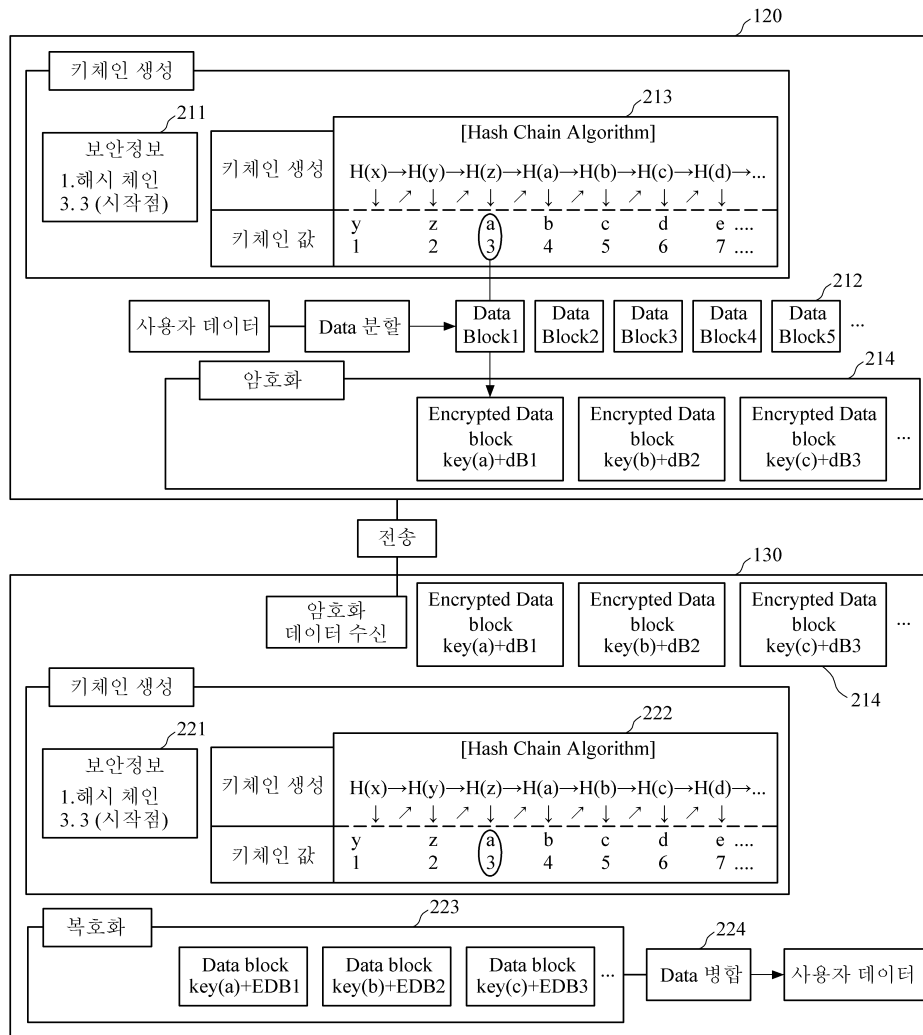
130: 제2 서비스 제공자

도면

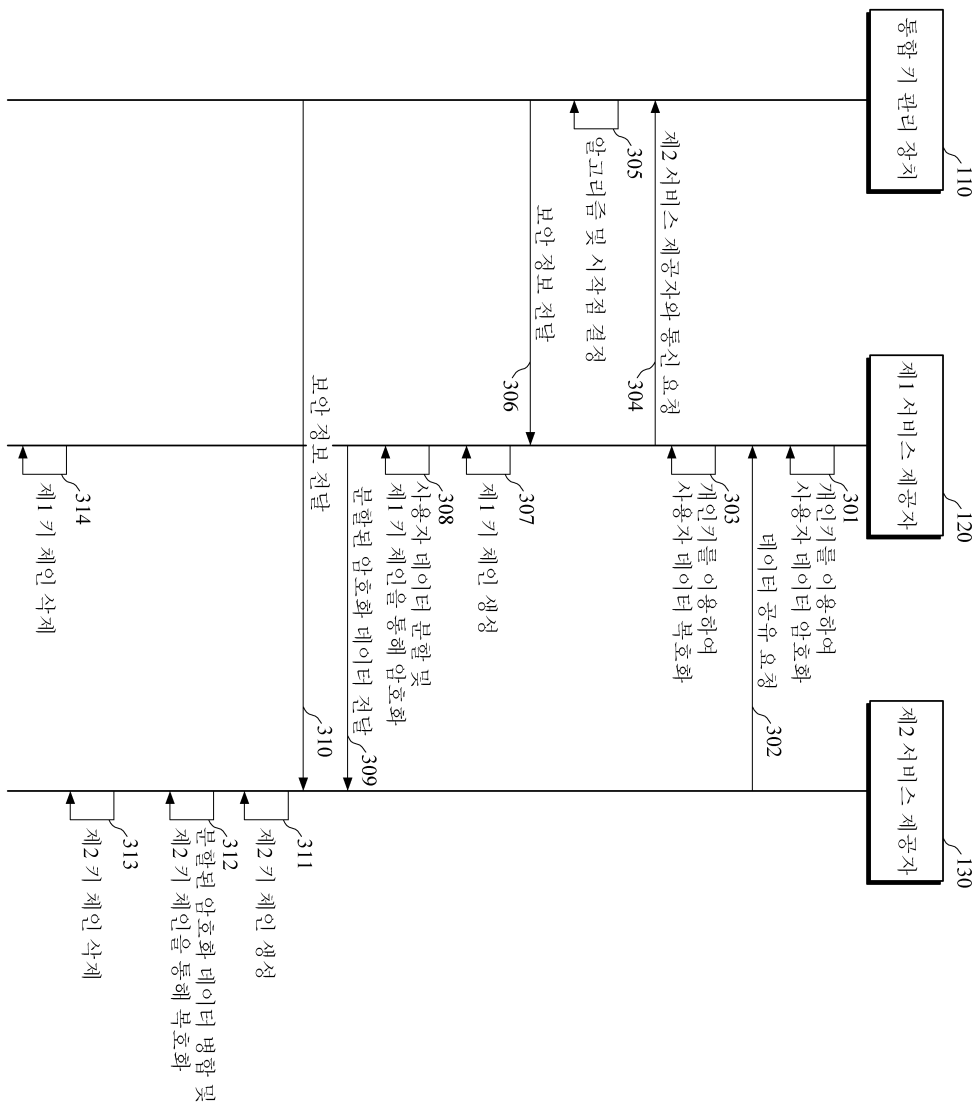
도면1



도면2



도면3



도면4

