



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0059679
(43) 공개일자 2023년05월03일

- (51) 국제특허분류(Int. Cl.)
G06F 11/14 (2006.01) G06F 21/60 (2013.01)
H04L 9/06 (2006.01)
- (52) CPC특허분류
G06F 11/1448 (2013.01)
G06F 11/1456 (2013.01)
- (21) 출원번호 10-2022-0009953
(22) 출원일자 2022년01월24일
심사청구일자 2022년01월24일
- (30) 우선권주장
1020210143776 2021년10월26일 대한민국(KR)

- (71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
- (72) 발명자
류재철
대전광역시 유성구 어은로 57 한빛아파트 132-801
김근영
대전광역시 유성구 장대로 87 퍼스트캐슬 202호
(뒷면에 계속)
- (74) 대리인
이은철, 김재문

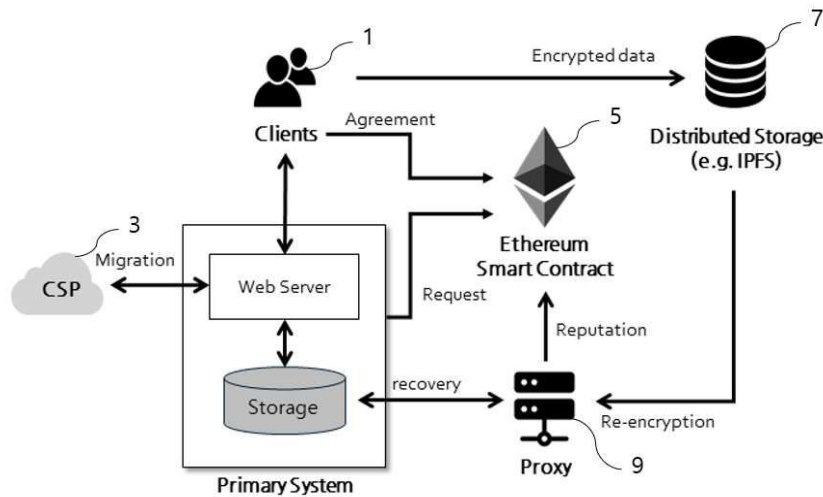
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **블록체인을 이용한 재해 복구 방법**

(57) 요약

본 발명은, 백업단계와 복구단계를 포함하는 재해 복구 방법에 있어서, 상기 백업단계는, (a) 사용자 단말이 제1 개인키와 제1 공개키를 생성하는 단계; (b) 제공자 서버가 제2 개인키와 제2 공개키를 생성하고 제2 공개키를 사용자 단말에 전송하는 단계; (c) 사용자 단말이 제1 공개키로 데이터를 암호화하고 제1 개인키와 제2 공개키로 재암호화키를 생성하는 단계; (d) 사용자 단말이 암호화된 데이터를 분산 스토리지에 저장하는 단계; 및 (e) 사용자 단말이 데이터 복구 시 필요한 권한을 정책으로 작성하기 위해 스마트 컨트랙트를 호출하는 트랜잭션을 제출하는 단계;를 포함하는 것을 일 특징으로 한다.

대표도 - 도2



(52) CPC특허분류

G06F 11/1471 (2013.01)

G06F 21/602 (2013.01)

H04L 9/0643 (2013.01)

H04L 9/50 (2022.05)

H04L 2209/76 (2013.01)

(72) 발명자

김준석

대전광역시 유성구 대학로 53

박준후

대전광역시 유성구 유성대로720번길 6 아인스빌
411호

이 발명을 지원한 국가연구개발사업

과제고유번호	1711125888
과제번호	2020-0-00229-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	블록체인융합기술개발(R&D)
연구과제명	블록체인 기반의 멀티 레벨 인증키 관리 및 복구 응용 플랫폼 개발
기 여 율	1/1
과제수행기관명	아톰릭스랩
연구기간	2020.04.01 ~ 2021.12.31

명세서

청구범위

청구항 1

백업단계와 복구단계를 포함하는 재해 복구 방법에 있어서,

상기 백업단계는,

- (a) 사용자 단말이 제1 개인키와 제1 공개키를 생성하는 단계;
- (b) 제공사 서버가 제2 개인키와 제2 공개키를 생성하고 제2 공개키를 사용자 단말에 전송하는 단계;
- (c) 사용자 단말이 제1 공개키로 데이터를 암호화하고 제1 개인키와 제2 공개키로 재암호화키를 생성하는 단계;
- (d) 사용자 단말이 암호화된 데이터를 분산 스토리지에 저장하는 단계; 및
- (e) 사용자 단말이 데이터 복구 시 필요한 권한을 정책으로 작성하기 위해 스마트 컨트랙트를 호출하는 트랜잭션을 제출하는 단계;를 포함하는 재해 복구 방법.

청구항 2

제 1 항에 있어서,

상기 백업단계는,

- (f) 제공사 서버가 사용자 단말에 복구 동의를 요청하는 단계;를 더 포함하는 것을 특징으로 하는 재해 복구 방법.

청구항 3

제 1 항에 있어서,

상기 (d) 단계는,

사용자 단말이 랜덤 값과 암호화된 데이터의 해시값을 결합한 변환 해시값을 생성하고, 암호화된 데이터, 암호화된 데이터의 해시값, 및 랜덤 값을 번들로 구성하여 분산 스토리지에 저장하는 것을 특징으로 하는 재해 복구 방법.

청구항 4

제 3 항에 있어서,

상기 (d) 단계는,

상기 암호화된 데이터가 분산 스토리지에 저장될 때 식별 값을 반환하는 것을 특징으로 하는 재해 복구 방법.

청구항 5

제 4 항에 있어서,

상기 (e) 단계는,

사용자 단말이 식별 값, 서버의 이더리움 계정 주소, 재암호화키, 및 변환 해시값을 파라미터로 하여 스마트 컨트랙트를 호출하는 것을 특징으로 하는 재해 복구 방법.

청구항 6

백업단계와 복구단계를 포함하는 재해 복구 방법에 있어서,

상기 복구단계는,

(g) 제공자 서버가 스마트 컨트랙트에 데이터 복구를 요청하는 트랜잭션을 제출하는 단계;

(h) 스마트 컨트랙트가 복구 요청을 받고 식별 값을 포함하는 이벤트를 발생시키는 단계;

(i) 프록시가 이벤트를 감지하고 분산 스토리지에서 암호화된 데이터, 암호화된 데이터의 해시값, 및 랜덤 값을 획득한 후 상기 스마트 컨트랙트에 제출하는 단계;

(j) 스마트 컨트랙트가 재암호화를 수행할 프록시를 선택하는 단계;

(k) 선택된 프록시가 상기 암호화된 데이터를 재암호화하여 제공자 서버에 전송하는 단계; 및

(l) 제공자 서버가 전송받은 재암호화된 데이터를 복호화하여 원본 데이터를 획득하는 단계;를 포함하는 재해 복구 방법.

청구항 7

제 6 항에 있어서,

상기 (j) 단계는,

스마트 컨트랙트가 저장된 변환 해시값과 프록시가 제출한 랜덤 값으로 계산된 암호화된 데이터의 해시값이 일치하는지 판단하고, 일치하는 경우 가장 먼저 제출된 트랜잭션에 의해 재암호화를 수행할 프록시를 선택하는 것을 특징으로 하는 재해 복구 방법.

청구항 8

제 6 항에 있어서,

상기 (l) 단계는,

제공자 서버가 생성한 제2 개인키로 재암호화된 데이터를 복호화하는 것을 특징으로 하는 재해 복구 방법.

청구항 9

제 6 항에 있어서,

(m) 제공자 서버가 프록시에 대한 평판을 스마트 컨트랙트에 제출하는 단계;를 더 포함하는 것을 특징으로 하는 재해 복구 방법.

청구항 10

제 9 항에 있어서,

상기 (j) 단계는,

스마트 컨트랙트가 평판이 일정값 이상인 프록시를 선택하는 것을 특징으로 하는 재해 복구 방법.

발명의 설명

기술 분야

[0001] 본 발명은 재해 복구 방법들에 관한 것으로서, 특히 블록체인과 분산 스토리지를 이용한 프록시 재암호화 기반의 사용자 중심 재해 복구 시스템에 관한 것이다.

배경 기술

[0003] IT 시스템과 인프라가 발전하면서 많은 서비스들이 사용자에게 수준 높은 서비스를 제공하기 위하여 실시간성과 높은 가용성의 보장 요구가 증가하고 있다. 특히, 금융 시스템을 비롯한 중요 데이터를 처리하는 시스템에서는 백업 및 복구 체계를 갖추는 것이 필수적이다. 서비스를 제공하는 기업은 사용자에게 신뢰성을 보장하고, 발생할 수 있는 비상사태에 대비하는 계획을 수립하는 것이 중요하다.

[0004] 재해 복구(Disaster Recovery)는 IT 서비스가 재해 유형으로부터 신속하게 복구하기 위한 준비 및 계획에 관한 절차로, 기후와 같은 자연 재난과 고의적 및 의도된 중단, 정전과 같은 서비스 손실, 시스템 장애 및 해킹에 이르기까지 다양한 환경에서 서비스의 연속성을 보장하는 것을 목표로 한다. 서비스 제공자 입장에서 재해 복구 계획은 시스템으로 인한 손실 및 복구의 최소화를 통해 비즈니스 운영 중단으로 인한 재정적 손실 및 평판 손상을 최소화하기 위한 절차이다. 특히, 데이터 복구 계획은 가능한 한 빠르게 정상 작동으로 복원하는데 필요한 모든 솔루션과 단계를 제공하여 연속성을 유지하는 것이 중요하다. 장애로 인한 운영의 연속성을 보장하기 위한 내결함성과는 달리, 재해복구는 비즈니스 서비스의 심각한 손상 및 장기적인 중단에 초점을 둔다.

[0005] 재해복구 시스템은 대규모의 기업에서 자체적으로 운영하는 형태뿐만 아니라, CSP(Cloud Service Provider)를 통해 제공하는 형태로 발전하였다. 클라우드 컴퓨팅은 전 세계적으로 분산된 리소스를 공유하며 실제로 이용한 리소스만큼의 비용을 지출하도록 구성된다. 이로 인해, 재해복구에 있어 클라우드 컴퓨팅의 적용은 유연성과 비용 효율성, 안전성 및 확장성과 같은 장점이 있다.

[0006] 도 1은 클라우드 기반의 재해 복구 시스템을 나타낸다. 도 1을 참조하면, 재해 복구 서비스는 CSP에 의해 제공될 수 있다. 사용자가 클라이언트 시스템을 통해 서비스를 제공받는 주 시스템(Primary System)에서 필요한 서버와 스토리지 자원 등을 관리하면서, 주기적으로 클라우드 환경에 백업을 시도한다. 재해로 인한 장애가 발생할 경우, 클라우드 환경으로 리디렉션을 시도하거나 클라우드 환경의 데이터를 다시 주 시스템으로 복원하여 사용자에게 계속해서 서비스를 지원할 수 있도록 구성되어있다.

[0007] 하지만, 클라우드 컴퓨팅에 기반한 재해복구 시스템은 구조적으로 다음과 같은 한계점을 가진다. 먼저, CSP에 대한 신뢰성이 집중된다. 이는 잠재적으로 고객과 서비스 기업이 CSP에 대한 의존성을 가지게 되는 구조로 이어진다. 또한, CSP의 단일 지점 장애 문제를 야기한다. 두 번째로는 사용자의 데이터 관리에 대해 개인 정보 보호와 더불어 기밀성 문제를 사용자가 관여할 수 없는 한계점을 가지고 있다.

[0008] 따라서, 재해 복구 환경에서 단일 지점 장애를 없애고, 사용자 중심의 데이터 관리를 위해 블록체인을 활용할 수 있는 재해 복구 방법이 요구되고 있는 실정이다.

선행기술문헌

특허문헌

[0010] (특허문헌 0001) 한국등록특허 제10-2065315호

발명의 내용

해결하려는 과제

[0011] 본 발명은 블록체인과 스마트 컨트랙트를 이용하여 단일 지점 장애를 방지할 수 있고 CSP(Cloud Service Provider)의 의존성이 제거된 재난 복구 방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

- [0013] 상기 목적을 달성하기 위하여 본 발명은, 백업단계와 복구단계를 포함하는 재해 복구 방법에 있어서, 상기 백업 단계는, (a) 사용자 단말이 제1 개인키와 제1 공개키를 생성하는 단계; (b) 제공자 서버가 제2 개인키와 제2 공개키를 생성하고 제2 공개키를 사용자 단말에 전송하는 단계; (c) 사용자 단말이 제1 공개키로 데이터를 암호화하고 제1 개인키와 제2 공개키로 재암호화키를 생성하는 단계; (d) 사용자 단말이 암호화된 데이터를 분산 스토리지에 저장하는 단계; 및 (e) 사용자 단말이 데이터 복구 시 필요한 권한을 정책으로 작성하기 위해 스마트 컨트랙트를 호출하는 트랜잭션을 제출하는 단계;를 포함하는 것을 일 특징으로 한다.
- [0014] 바람직하게는, 상기 백업단계는, (f) 제공자 서버가 사용자 단말에 복구 동의를 요청하는 단계;를 더 포함할 수 있다.
- [0015] 바람직하게는, 상기 (d) 단계는, 사용자 단말이 랜덤 값과 암호화된 데이터의 해시값을 결합한 변환 해시값을 생성하고, 암호화된 데이터, 암호화된 데이터의 해시값, 및 랜덤 값을 변들로 구성하여 분산 스토리지에 저장할 수 있다.
- [0016] 바람직하게는, 상기 (d) 단계는, 암호화된 데이터가 분산 스토리지에 저장될 때 식별 값을 반환할 수 있다.
- [0017] 바람직하게는, 상기 (e) 단계는, 사용자 단말이 식별 값, 서버의 이더리움 계정 주소, 재암호화키, 및 변환 해시값을 파라미터로 하여 스마트 컨트랙트를 호출할 수 있다.
- [0018] 또한 본 발명은, 백업단계와 복구단계를 포함하는 재해 복구 방법에 있어서, 상기 복구단계는, (g) 제공자 서버가 스마트 컨트랙트에 데이터 복구를 요청하는 트랜잭션을 제출하는 단계; (h) 스마트 컨트랙트가 복구 요청을 받고 식별 값을 포함하는 이벤트를 발생시키는 단계; (i) 프록시가 상기 이벤트를 감지하고 분산 스토리지에서 암호화된 데이터, 암호화된 데이터의 해시값, 및 랜덤 값을 획득한 후 스마트 컨트랙트에 제출하는 단계; (j) 스마트 컨트랙트가 재암호화를 수행할 프록시를 선택하는 단계; (k) 선택된 프록시가 상기 암호화된 데이터를 재암호화하여 제공자 서버에 전송하는 단계; 및 (l) 제공자 서버가 전송받은 재암호화된 데이터를 복호화하여 원본 데이터를 획득하는 단계;를 포함하는 것을 다른 특징으로 한다.
- [0019] 바람직하게는, 상기 (j) 단계는, 스마트 컨트랙트가 저장된 변환 해시값과 프록시가 제출한 랜덤 값으로 계산된 암호화된 데이터의 해시값이 일치하는지 판단하고, 일치하는 경우 가장 먼저 제출된 트랜잭션에 의해 재암호화를 수행할 프록시를 선택할 수 있다.
- [0020] 바람직하게는, 상기 (l) 단계는, 제공자 서버가 생성한 제2 개인키로 재암호화된 데이터를 복호화할 수 있다.
- [0021] 바람직하게는, (m) 제공자 서버가 프록시에 대한 평판을 스마트 컨트랙스에 제출하는 단계;를 더 포함할 수 있다.
- [0022] 바람직하게는, 상기 (j) 단계는, 스마트 컨트랙트가 평판이 일정값 이상인 프록시를 선택할 수 있다.

발명의 효과

- [0024] 본 발명에 따르면, 탈중앙화된 인프라를 갖춘 블록체인을 이용하여 단일 지점 장애와 CSP의 의존성 문제를 해결할 수 있다는 이점이 있다.
- [0025] 또한 본 발명은, 분산 스토리지에 데이터를 저장하여 저장 비용을 줄이고 확장성을 높일 수 있다는 이점이 있다.
- [0026] 또한 본 발명은, 프록시 재암호화를 통해 데이터 분산 저장 시 기밀성 문제를 해결할 수 있다는 이점이 있다.

도면의 간단한 설명

- [0028] 도 1은 클라우드 기반의 재해 복구 시스템을 나타낸다.
- 도 2은 본 발명의 실시예에 따른 재난 복구 환경의 구성도를 나타낸다.
- 도 3는 데이터가 복제되는 주기인 RPO(Recovery Point Objective)를 나타낸다.
- 도 4는 본 발명의 실시예에 따른 백업단계의 프로세스를 나타낸다.

도 5는 본 발명의 실시예에 따른 백업단계의 순서도를 나타낸다.

도 6은 본 발명의 실시예에 따른 복구단계의 프로세스를 나타낸다.

도 7은 본 발명의 실시예에 따른 복구단계의 순서도를 나타낸다.

도 8은 본 발명의 실시예에 따른 재암호화 알고리즘을 나타낸다.

발명을 실시하기 위한 구체적인 내용

- [0029] 이하, 첨부된 도면들에 기재된 내용들을 참조하여 본 발명을 상세히 설명한다. 다만, 본 발명이 예시적 실시 예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일 참조부호는 실질적으로 동일한 기능을 수행하는 부재를 나타낸다.
- [0030] 본 발명의 목적 및 효과는 하기의 설명에 의해서 자연스럽게 이해되거나 보다 분명해 질 수 있으며, 하기의 기재만으로 본 발명의 목적 및 효과가 제한되는 것은 아니다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이, 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다.
- [0031] 도 2은 본 발명의 실시예에 따른 재난 복구 시스템의 구성도를 나타낸다. 도 2를 참조하면, 재난 복구 시스템은 사용자 단말(1), 제공자 서버(3), 스마트 컨트랙트(5), 분산 스토리지(7), 및 프록시(9)를 포함할 수 있다.
- [0032] 재난 복구 시스템은 재난 발생 전 서비스를 유지하기 위한 주 시스템(Primary 혹은 Main System)과 재난 상황에 대비하기 위한 예비 시스템(Secondary 혹은 Serve)으로 구성될 수 있다. 재난 복구 시스템은 재난 복구 서비스를 제공하는 서버와 데이터를 저장하는 스토리지로 구분될 수 있다. 재난 복구 시스템은 주 시스템과 예비 시스템이 물리적으로 분리되어 있는 것이 바람직하다.
- [0033] 재난 복구 시스템은 데이터의 재난 발생 전 백업 절차와 재난 발생 후의 복구 절차로 구성될 수 있다. 재난 복구 시스템은 주 시스템에서 서브 시스템으로 데이터가 백업될 수 있다.
- [0034] 도 3는 데이터가 복제되는 주기인 RPO(Recovery Point Objective)를 나타낸다. 도 3을 참조하면, 복구는 재난이 발생하면 마지막 백업 시점까지 가능할 수 있다. RTO(Recovery Time Objectice)는 재난 발생 후 복구되기까지 걸리는 시간을 의미한다. 재난 복구의 비용은 RTO의 수준이 높을수록 높게 책정된다.
- [0035] 재난 복구 시스템은 블록체인을 이용할 수 있다. 재난 복구 시스템이 이용하는 블록체인은 네트워크 참여자들의 합의 프로토콜에 의해 탈중앙화 환경에서 원장을 구성할 수 있다. 재난 복구 시스템은 누구나 합의에 참여할 수 있어 단일 지점 장애가 없는 무허가형(Permissionless) 블록체인을 이용할 수 있다. 재난 복구 시스템은 과거 내역에 대한 비가역성을 가지는 블록체인의 성질에 따라 위조를 방지할 수 있다. 이를 통해, 재난 복구 시스템은 블록체인에 저장된 트랜잭션과 상태에 대한 신뢰성을 확보할 수 있다.
- [0036] 재난 복구 시스템은 복구 단계에서 사용자의 개입을 요구하지 않도록 자동화될 수 있다. 재난 복구 시스템은 이더리움의 트랜잭션 비용을 최소화하도록 구성될 수 있다. 재난 복구 시스템은 스마트 컨트랙트(5)가 접근 제어에 대한 역할을 수행하여 모든 요청과 관리에 대한 신뢰성을 확보할 수 있다.
- [0037] 사용자 단말(1)은 제공자 서버(3)에 백업할 데이터를 전송할 수 있다. 사용자 단말(1)은 개인정보와 관련된 데이터를 암호화하여 분산 스토리지(7)에 저장할 수 있다. 사용자 단말(1)은 이더리움 주소(addr)를 가질 수 있다. 사용자 단말(1)은 데이터에 대한 접근 정책을 구성하기 위한 스마트 컨트랙트(5)를 호출하는 트랜잭션을 작성할 수 있다. 사용자 단말(1)은 데이터 복구에 동의하기 위해 스마트 컨트랙트를 호출하는 트랜잭션을 작성할 수 있다.
- [0038] 제공자 서버(3)는 사용자에게 서비스를 제공하기 위한 환경을 구축할 수 있다. 제공자 서버(3)는 사용자 단말(1)에서 전송받은 데이터를 저장할 수 있다. 제공자 서버(3)는 이더리움 주소(addr)를 가질 수 있다. 제공자 서버(3)는 재난 발생 시 스마트 컨트랙트(5)를 호출하여 복구를 요청할 수 있다.
- [0039] 스마트 컨트랙트(5)는 블록체인에서 실행되는 프로그램으로 솔리디티와 같은 언어로 개발될 수 있다. 스마트 컨트랙트(5)는 이더리움 내에서 구현될 수 있다. 스마트 컨트랙트(5)는 사용자 단말(1)의 정책과 제공자 서버(3)의 요청을 관리할 수 있다. 스마트 컨트랙트(5)는 정확한 재암호화를 프록시(9)가 수행할 수 있도록 평판 관리

를 할 수 있다.

- [0040] 분산 스토리지(7)는 P2P 환경에서 참여자들의 저장 공간을 활용하여 데이터를 공유하는 시스템일 수 있다. 분산 스토리지(7)는 재난 복구 과정에서 필요한 사용자의 데이터를 저장하기 위한 공간으로 활용될 수 있다. 분산 스토리지(7)는 블록체인에 데이터를 직접 저장하지 않음으로써 저장 비용을 줄이고, 확장성을 높일 수 있다.
- [0041] 분산 스토리지(7)는 CID(Content ID)를 고유한 식별자로 가진 데이터가 저장될 수 있다. 식별자를 통해 누구나 암호화된 데이터에 접근할 수 있으나 복호화할 수는 없다.
- [0042] 프록시(9)는 분산 스토리지(9)의 사용자 단말(1) 데이터를 재암호화하여 제공자 서버(3)에 전송할 수 있다. 프록시(9)는 개인의 데이터를 분산 저장하기 위해 필요한 기밀성 문제를 재암호화를 통해 해결할 수 있다. 프록시(9)는 탈중앙화 환경에서 평판 시스템에 기반한 다수로 운영되어 단일 지점 장애를 방지할 수 있다. 프록시(9)는 이더리움 주소($addr_P$)를 가질 수 있다. 프록시(9)는 분산 스토리지(9)에 접근할 수 있는 클라이언트가 구축될 수 있다.
- [0043] 프록시 재암호화는 양자 간의 데이터 교환에서 기밀성을 제공하는 암호 체계이다. 프록시 재암호화는 비밀키를 공유하지 않고 암호화된 데이터 교환을 가능하게 할 수 있다.
- [0044] 재해 복구 방법은 백업단계와 복구단계를 포함할 수 있다. 재해 복구 방법은 블록체인을 적용하여 탈중앙화된 인프라를 통해 데이터의 단일 지점 장애와 제공자의 의존성 문제를 해결할 수 있다. 재해 복구 방법은 사용자가 데이터를 직접 제어 및 관리할 수 있도록 스마트 컨트랙트를 활용할 수 있다.
- [0045] 도 4는 본 발명의 실시예에 따른 백업단계의 프로세스를 나타내고, 도 5는 본 발명의 실시예에 따른 백업단계의 순서도를 나타낸다. 도 4 및 도 5를 참조하여 본 발명에 따른 재해 복구 방법의 백업단계에 대해 살펴보면 아래와 같다.
- [0046] 먼저, 사용자 단말(1)이 제1 개인키(sk_U)와 제1 공개키(pk_U)를 생성할 수 있다. 여기서, 제1 개인키는 데이터 재암호화를 위한 키일 수 있다.
- [0047] 또한, 제공자 서버(3)가 제2 개인키(sk_s)와 제2 공개키(pk_s)를 생성하고 제2 공개키를 사용자 단말(1)에 전송할 수 있다. 여기서, 제2 개인키는 데이터 복호화를 위한 키일 수 있다. 사용자 단말(1)과 제공자 서버(3)가 각각 개인키와 공개키를 생성하는 단계에는 일정한 순서가 정해진 것이 아니다.
- [0048] 이어서, 사용자 단말(1)이 제1 공개키(pk_U)로 데이터(m)를 암호화하여 암호화된 데이터($c_1 = Enc(pk_U, m)$)를 생성할 수 있다. 또한, 사용자 단말(1)이 제1 개인키(sk_U)와 제2 공개키(pk_s)로 재암호화키($rk = ReKeyGen(sk_U, pk_s)$)를 생성할 수 있다. 사용자 단말(1)은 백업 요청에 동의가 있는 경우에만 데이터(m)를 암호화하고 재암호화키(rk)를 생성할 수 있다.
- [0049] 뒤이어, 사용자 단말(1)이 암호화된 데이터(c_1)를 분산 스토리지(7)에 저장할 수 있다. 구체적으로 사용자 단말(1)이 랜덤 값(r)과 암호화된 데이터의 해시값($h_c = Hash(c_1)$)을 결합한 변환 해시값($s = Hash(h_c || r)$)을 생성하고, 암호화된 데이터(c_1), 암호화된 데이터의 해시값(h_c), 및 랜덤 값(r)을 번들($bundle = c_1, h_c, r$)로 구성하여 분산 스토리지(7)에 저장할 수 있다. 여기서, 랜덤 값(r)은 가장 먼저 재암호화를 수행할 프록시(9)를 선택하기 위한 값으로 사용될 수 있다. 암호화된 데이터(c_1)는 분산 스토리지(7)에 저장될 때 식별 값($cid_{bundle} = Hash(bundle)$)을 반환할 수 있다.
- [0050] 다음으로, 사용자 단말(1)이 데이터 복구 시 필요한 권한을 정책으로 작성하기 위해 스마트 컨트랙트(5)를 호출하는 트랜잭션을 제출할 수 있다. 구체적으로, 사용자 단말(1)이 식별 값(cid_{bundle}), 서버의 이더리움 계정 주

소($addr_s$), 재암호화키(rk), 및 변환 해시값(s)을 파라미터로 하여 스마트 컨트랙트(5)를 호출할 수 있다. 여기서, 각 파라미터는 사용자 단말(1)이 관리하는 정책에 값으로 저장되어, 권한을 확인할 때 활용될 수 있다. 사용자 단말(1)과 제공자 서버(3)는 스마트 컨트랙트(5)로 제출한 트랜잭션이 실행되면 등록된 결과를 이벤트로 확인할 수 있다.

[0051] 위 프로세스에 앞서, 제공자 서버(3)가 사용자 단말(1)에 복구 동의를 요청할 수 있다. 제공자 서버(3)는 재해 발생 이후 자동으로 데이터를 복구할 수 있도록 사용자 단말(1)에 동의를 요청할 수 있다. 제공자 서버(3)는 사용자 단말(3)이 복구에 동의한 경우 재암호화키(rk)를 생성할 수 있는 제2 공개키(pk_s)를 전송할 수 있다.

[0052] 데이터 복구 권한에 대한 동의 알고리즘은 다음과 같다. 스마트 컨트랙트(5)는 제공자 서버(3)의 데이터 복구에 동의하는 절차와 취소하는 절차로 구성될 수 있다. 스마트 컨트랙트(5)는 사용자 단말(1)을 등록하고, 사용자별로 프록시(9)를 지정할 수 있다. 스마트 컨트랙트(5)는 초기 등록과정에서 owner로 지정된 호출자만이 데이터를 등록 및 취소할 수 있도록 구성될 수 있다. 스마트 컨트랙트(5)는 사용자가 등록한 목록에 있는 프록시(9)만을 선택할 수 있다. 프록시(9)는 등록 시 예치금이 지불된 경우에만 지정될 수 있다.

[0053] 스마트 컨트랙트(5)는 사용자 단말(1)이 제공자 서버(3)에 대해 데이터 활용 동의를 취소하는 호출을 한 경우에는 기존에 등록된 데이터를 삭제할 수 있다. 스마트 컨트랙트(5)는 삭제 권한을 갖은 정책을 생성한 사용자 단말(1)에 의해서만 등록된 데이터를 삭제할 수 있다.

[0054] 도 6은 본 발명의 실시예에 따른 복구단계의 프로세스를 나타내고, 도 7은 본 발명의 실시예에 따른 복구단계의 순서도를 나타낸다. 도 6 및 도 7을 참조하여 본 발명에 따른 재해 복구 방법의 복구단계에 대해 살펴보면 아래와 같다. 복구단계는 사용자 단말(1)이 제공자 서버(3)의 데이터 활용에 대한 동의를 취소하기 위해 스마트 컨트랙트(5)의 상태를 변경하지 않는 한, 제공자 서버(3)에게 데이터 복구를 동의한 것으로 간주하여 복원을 수행할 수 있다.

[0055] 먼저, 제공자 서버(3)가 스마트 컨트랙트(5)에 데이터 복구를 요청하는 트랜잭션을 제출할 수 있다.

[0056] 스마트 컨트랙트(5)는 데이터 복구를 요청하는 제공자 서버(3)의 이더리움 주소($addr_s$)가 데이터의 식별 값(cid_{bundle})에 대해 복구 권한이 허가된 주소일 경우에는 요청 리스트를 생성할 수 있다. 여기에서, 요청 리스트에는 요청자와 사용자 단말(1)의 주소, 및 요청한 시간이 기록될 수 있다.

[0057] 뒤이어, 스마트 컨트랙트(5)가 복구 요청을 받고 식별 값(cid_{bundle})을 포함하는 이벤트를 발생시킬 수 있다.

스마트 컨트랙트(5)는 트랜잭션의 송신자인 제공자 서버(3)의 이더리움 주소($addr_s$)가 등록된 주소일 경우, 프록시(9)가 확인할 수 있는 이벤트를 발생시킬 수 있다. 스마트 컨트랙트(5)는 제공자 서버(3)의 이더리움 주소($addr_s$), 분산 스토리지의 식별 값(cid_{bundle}), 및 재암호화키(rk)를 포함하는 이벤트를 발생시킬 수 있다. 스마트 컨트랙트(5)가 발생시킨 이벤트는 프록시(3)에 전달될 수 있다.

[0058] 다음으로, 프록시(9)가 상기 이벤트를 감지하고 분산 스토리지(7)에서 암호화된 데이터(c_1), 암호화된 데이터의 해시값(h_c), 및 랜덤 값(3)을 획득한 후 스마트 컨트랙트(5)에 제출할 수 있다. 프록시(9)는 이벤트로 확인한 식별 값(cid_{bundle})으로 분산 스토리지(7)에 접근할 수 있다.

[0059] 이어서, 스마트 컨트랙트(5)가 재암호화를 수행할 프록시(9)를 선택할 수 있다. 구체적으로, 스마트 컨트랙트(5)가 저장된 변환 해시값(s)과 프록시(9)가 제출한 랜덤 값(r)으로 계산된 암호화된 데이터의 해시값(h_c)이 일치하는지 판단하고, 일치하는 경우 가장 먼저 제출된 트랜잭션에 의해 재암호화를 수행할 프록시(9)를 선택할 수 있다.

[0060] 스마트 컨트랙트(5)는 평판이 일정값 이상인 프록시(9)를 선택할 수 있다. 즉, 스마트 컨트랙트(5)는 분산된 환경의 프록시(9)를 평판 시스템에 의해 운영하여, 사용자가 평판에 따라 특정 프록시(9)만 재암호화에 참여하게

할 수 있다.

[0061] 그리고, 선택된 프록시(9)가 상기 암호화된 데이터(C_1)를 재암호화하여 재암호화된 데이터($C_2 = ReEnc(rk_{U-S} C_1)$)를 제공자 서버(3)에 전송할 수 있다.

[0062] 또한, 제공자 서버(3)가 전송받은 재암호화된 데이터(C_2)를 복호화하여 원본 데이터를 획득할 수 있다. 제공자 서버(3)는 백업단계에서 생성한 제2 개인키로 재암호화된 데이터를 복호화할 수 있다.

[0063] 최종 단계에서, 제공자 서버(3)가 프록시(9)에 대한 평판을 스마트 컨트랙트(5)에 제출할 수 있다. 프록시(9)는 평판 관리를 위해 스마트 컨트랙트(5)에 리스트에 등록되어야 한다. 프록시(9)는 등록을 위해 예치금을 일정량 이상 필요하며, 등록된 경우 평판이 초기화될 수 있다. 이러한, 평판 시스템은 오라클 시스템을 구현한 Augur나 Chainlink와 같은 플랫폼과 유사하다.

[0064] 도 8은 본 발명의 실시예에 따른 재암호화 알고리즘을 나타낸다. 도 8을 참조하면, 재난 복구 방법은 프록시(9)에서 암호화된 데이터(C_1)를 재암호화하여 분산 스토리지(7)의 기밀성을 제공할 수 있다. 분산 스토리지(7)는 블록체인 플랫폼에 비용 효과적인 데이터 저장소를 제공하지만, 기밀성을 탈중앙화 환경에서 구현하기에 어려움이 있다. 따라서, 본 발명에서는 이를 해결하기 위해 재암호화를 활용하였다.

[0065] 재암호화 알고리즘은 데이터 소유주(Alice)의 공개키로 암호화한 데이터를 수신자(Bob)의 개인키로 복호화할 수 있도록 구성될 수 있다. 이를 위해서 암호화된 데이터를 재암호화를 하여 수신자(Bob)에게 전달하는 중개자인 프록시(9)가 필요하다. 프록시(9)에게 전달되는 데이터는 소유주(Alice)의 공개키로 암호화되어 있고, 재암호화된 데이터는 수신자(Bob)의 개인키로만 복호화할 수 있기 때문에 데이터 전달과정에서 기밀성이 유지될 수 있다. 재암호화 알고리즘은 암호화 방향 여부에 따라 단방향 및 양방향으로 구분할 수 있으나, 본 발명에서는 유형에 상관없이 적용될 수 있다.

[0067] 이하에서는 본 발명의 시뮬레이션 결과를 설명한다.

[0068] 구현 범위는 프록시 재암호화를 구성하는 각 개체의 시스템과 블록체인에 배포된 스마트 컨트랙트(5)로 나뉜다. 프록시 재암호화 알고리즘으로는 Identity 기반의 프록시 재암호화로, rust 언어로 구현된 recrypt API를 제공한다. recrypt API에서 구현된 알고리즘은 재암호화 속도 측면에서 장점을 가진다. 분산 스토리지(7)로는 IPFS의 go언어 버전인 go-ipfs를 활용하였다. 테스트 수행 프로그램은 프록시 재암호화 알고리즘과 동일하게 rust 언어로 구현되었고, 컴파일러는 rustc 1.56.0 버전을 사용하였다. 프록시 재암호화가 수행되는 환경은 Intel(R) Core(TM) i7-9700F @3.00GHz CPU와 32GB 메모리이며, 운영체제는 Ubuntu 18.04.5 LTS이다.

[0069] 스마트 컨트랙트(5)는 이더리움 플랫폼에서 가장 많이 활용되는 Solidity로 구현하였으며, 컴파일러는 solc 0.8.4 버전을 사용하였다. 스마트 컨트랙트 배포 이더리움 테스트넷인 Kovan Network 하였고, 베를린 하드포크 기준 EVM을 활용하여 비용을 측정하였다.

[0070] 재해복구 시스템에서 복구와 관련된 주요 성능 지표는 RTO이다. RTO는 재해 발생 이후부터 정상적인 서비스를 할 수 있는 상황까지의 시간을 의미한다. 본 시스템에서는 데이터 요청 시점부터 복구까지의 시간을 RTO로 정의한다. RTO는 [수학식 1]로 나타낼 수 있다. 여기에서, $T_{S \rightarrow SC}$ 는 서버의 데이터 복구 요청 트랜잭션 발생부터, 프록시가 이를 확인하기까지의 시간, $T_{P \rightarrow SC}$ 는 프록시가 요청을 확인 후 분산 스토리지에 접근하여 스마트 컨트랙트로부터 선정되는 이벤트를 확인하기까지 소요되는 시간, $T_{P \rightarrow S}$ 는 선정된 프록시가 재암호화를 수행하여 서버에 전송 후, 서버가 데이터를 복호화하는 시간을 나타낸다.

[0072] [수학식 1]

$$RTO = T_{S \rightarrow SC} + T_{P \rightarrow SC} + T_{P \rightarrow S}$$

[0075] $T_{S \rightarrow SC}$ 와 $T_{P \rightarrow SC}$ 는 이더리움 네트워크의 블록 생성 시간과 프록시가 IPFS로부터 저장되어 있는 암호화된 데이터를 다운로드 시간이 포함되기 때문에 블록 생성시간과 데이터 다운로드 시간을 더하여 측정하였고, $T_{P \rightarrow S}$ 는 재암호화 후 데이터를 전송하여 복호화하기까지 걸리는 시간이 포함되므로 recrypt API를 이용해 128bit의 보안 강도를 기준으로 성능을 측정하였다. 이더리움 네트워크의 블록 평균 생성시간은 데이터의 무관하며 최근 100개 블록의 평균 생성시간은 13.42초이다. 파일 다운로드, 재암호화, 복호화에 대한 시간 측정 결과는 [Table 1]와 같이 나타내었으며 측정된 각 결과는 100회 수행에 대한 평균값을 나타낸다.

[0077] [Table 1]

	0.1KB	1KB	10KB
IPFS Download	0.13s	0.21s	0.25s
ReEnc	0.68s	2.05s	21.3s
Dec	0.87s	2.62s	27.3s
RTO	15.1s	18.3s	62.27s

[0078]

[0080] 시뮬레이션 결과를 바탕으로 재난 복구 성능 지표인 RTO를 계산해보면 데이터 크기가 0.1KB일 때 15.1초, 1KB일 때 18.3초, 10KB일 때 62.26초임을 알 수 있다. 측정 시간은 384byte를 기준으로 선형적으로 증가한다. 따라서, 대용량 암호화가 필요한 데이터의 경우, 하이브리드 암호화를 활용하여 대칭키 값에 대해서 프록시 재암호화를 쓰는 것이 효율적임을 알 수 있다.

[0081] 스마트 컨트랙트에서 비용은 트랜잭션에 부과한 가격으로 설정된다. [Table 2]에서 제시한 값은 EVM에서 산정하는 함수별 실행 gas 비용을 나타낸다.

[0083] [Table 2]

Function Name	Caller	Cost[gas]
Deployment	-	2,789,868
userInit	User	45,460
addProxy	User	70,991
removeProxy	User	21,711
recoveryAgree	User	94,881
cancel	User	20,555
request	Server	95,967
response	Proxy	130,007
registerProxy	Proxy	56,819
submitReputation	Server	38,518

[0084]

[0086] gas 비용이란, 이더리움 노드들에서 트랜잭션별로 호출된 함수를 실행한 후, EVM 내에 정의된 명령에 따라 부과되는 비용을 의미한다. 해당 비용은 동일한 EVM 내에서 고정된 비용이며, 실제 트랜잭션에 사용되는 gas 비용은

사용자가 부과한 gas 가격에 따라 달라질 수 있다.

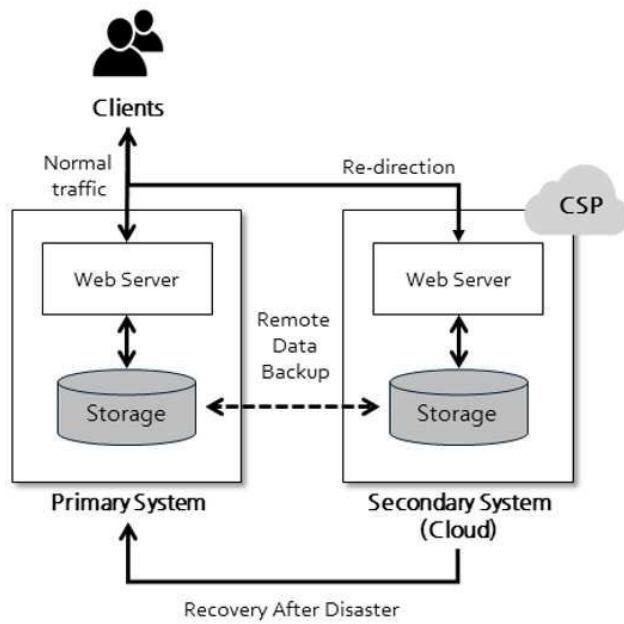
- [0087] 재암호화 서비스를 위한 컨트랙트를 하나로 구성하여 배포할 경우, 필요한 gas 비용은 2,789,868로 측정되었다. 각 호출자(Caller)에 따라 수행하는 함수에 대한 비용은 대부분 100,000 gas 아래로 나타난다. 가장 큰 비용을 처리하는 프록시가 응답을 호출하는 비용은 가스 가격을 27Gwei 기준으로 하였을 때, 약 \$10.92만큼 소모된다. 또한, 가장 낮은 취소 트랜잭션은 \$1.72 만큼의 비용을 지출한다. 트랜잭션 비용을 고려하면 보다 더 측정될 수 있지만, 전체적으로 \$1~10 수준의 범위에서 서비스를 수행할 수 있다.
- [0088] 본 발명의 주된 목적 중 하나는 재해복구 상에서 데이터를 처리할 때 발생하는 단일 지점 장애를 없애고, 분산된 환경에서 사용자 중심으로 데이터를 관리하는 것이다. 블록체인은 탈중앙화 네트워크 내에서 작동하기 때문에 접근 제어를 수행하는 스마트 컨트랙트(5)와 데이터가 저장되는 분산 스토리지(7)의 도입으로 단일 지점 장애가 발생하지 않도록 구성되었기 때문에 사용자의 데이터에 대한 가용성이 보장된다.
- [0089] 추가적으로 기밀성을 위해 단일 프록시(9)가 아닌 평판에 기반한 다중 프록시(9) 환경을 고려하므로, 가용성을 확보할 수 있다. 이 같은 방법은 파일을 저장하거나 제어 방식을 변경하기 위해 제3 자를 신뢰할 필요가 없으며, 기존에 클라우드 환경에서 발생할 수 있는 서비스 거부 공격과 같은 위협에 안전하다.
- [0090] 본 발명에서는 분산 스토리지(7)에 프록시 재암호화로 암호화된 상태의 데이터를 저장한다. 따라서, 사용자의 정보가 포함된 원본 데이터는 분산된 환경에서 드러나지 않으며, 프록시(9)가 재암호화를 수행하는 동안에도 여전히 기밀성이 유지된다. 데이터는 재암호화 키를 생성할 때 참여한 서버의 개인키로만 복호화 할 수 있으며, 사용자의 허가를 통해 복구할 수 있다.
- [0091] 블록체인의 합의는 기록된 트랜잭션에 비가역성을 부여하여 무결성을 유지한다. 특히, 스마트 컨트랙트(5)에 구현된 로직은 신뢰할 수 있는 실행을 보장한다.
- [0092] 블록체인에서 인증은 개인키의 소유권으로 관리된다. 사용자 단말(1)과 제공자 서버(3), 프록시(9)는 각 계정으로 생성한 개인키를 통한 트랜잭션으로 등록 및 취소 과정을 수행하며, 한번 등록된 이 후 스마트 컨트랙트(5)에 의해 트랜잭션에 따라 인증 절차는 자동적으로 수행될 수 있다.
- [0093] 이상에서 대표적인 실시예를 통하여 본 발명을 상세하게 설명하였으나, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리 범위는 설명한 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 특허청구범위와 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태에 의하여 정해져야 한다.

부호의 설명

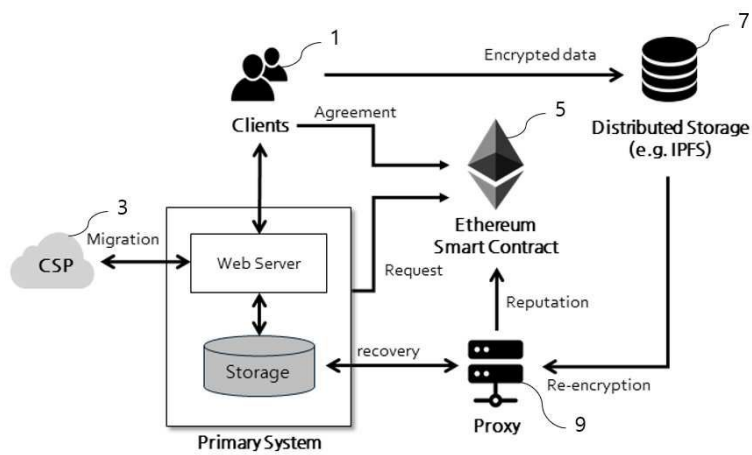
- [0095]
- 1 : 사용자 단말
 - 3 : 제공자 서버
 - 5 : 스마트 컨트랙트
 - 7 : 분산 스토리지
 - 9 : 프록시

도면

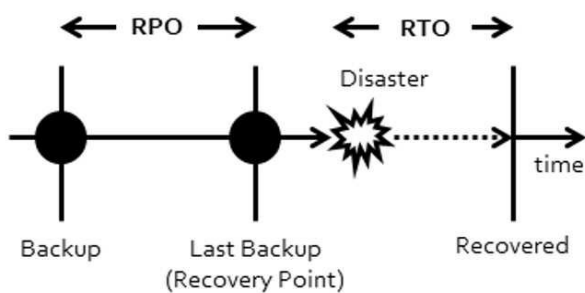
도면1



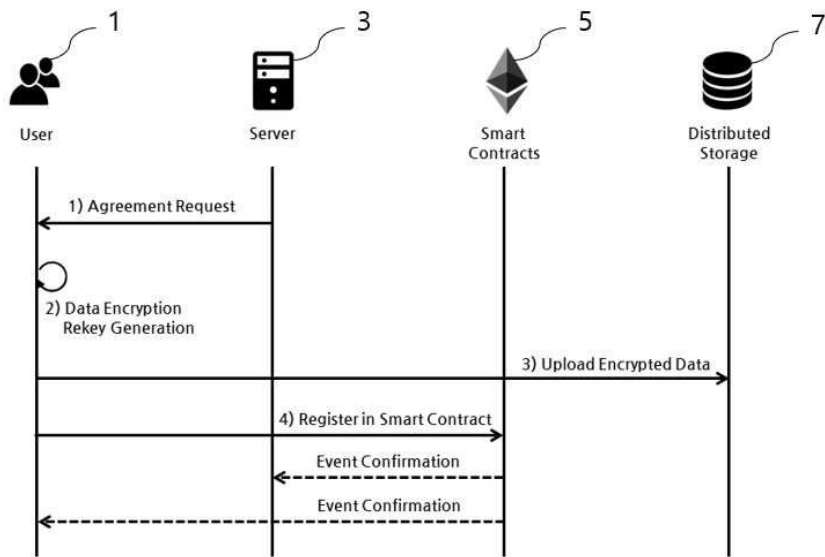
도면2



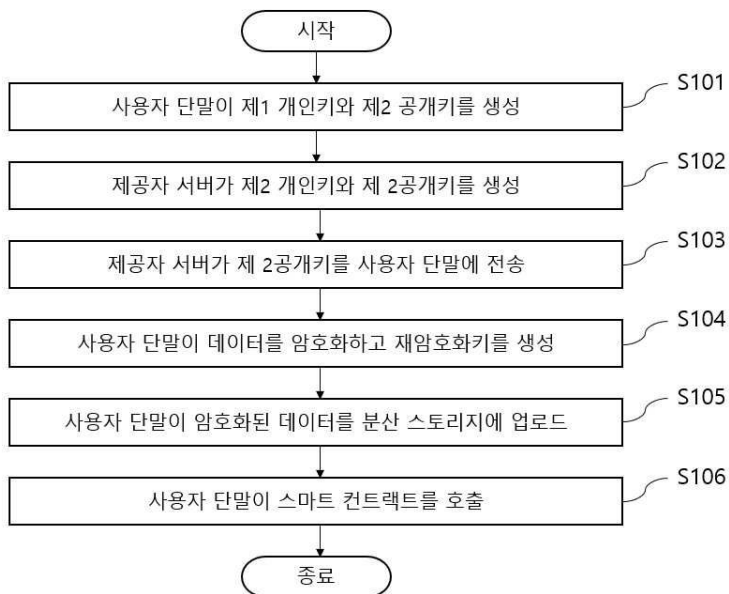
도면3



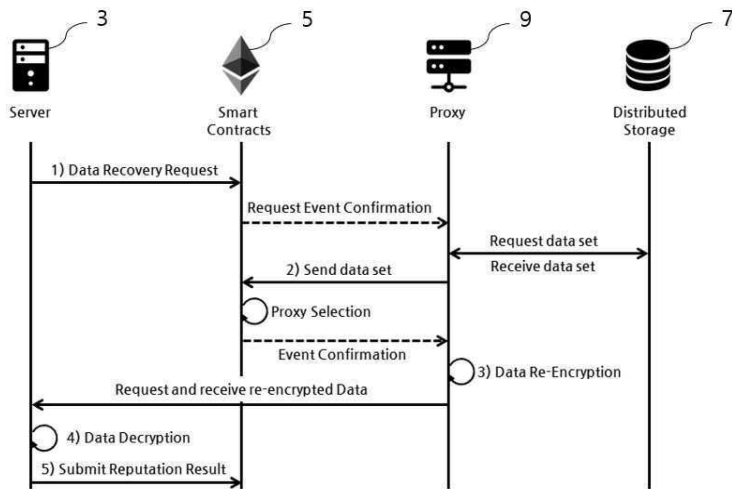
도면4



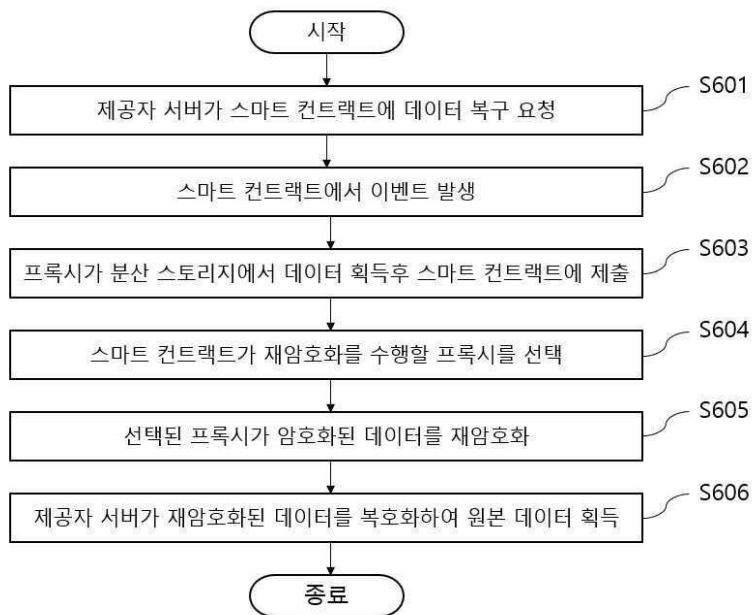
도면5



도면6



도면7



도면8

