(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년12월12일
(11) 등록번호 10-1472320
(24) 등록일자 2014년12월08일

(51) 국제특허분류(Int. Cl.)
G06F 21/64 (2013.01) *G06F 15/16* (2006.01)
(21) 출원번호 10-2013-0062073
(22) 출원일자 2013년05월30일
심사청구일자 2013년05월30일
(65) 공개번호 10-2014-0140974
(43) 공개일자 2014년12월10일
(56) 선행기술조사문헌
KR1020110083189 A*
KR1020120029424 A*
JP2011041326 A
JP2005242412 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김승주
서울특별시 송파구 중대로 24 올림픽훼밀리타운아파트 201-1401
박민수
서울특별시 동대문구 이문로1길 16-7 104호
(74) 대리인
특허법인충현

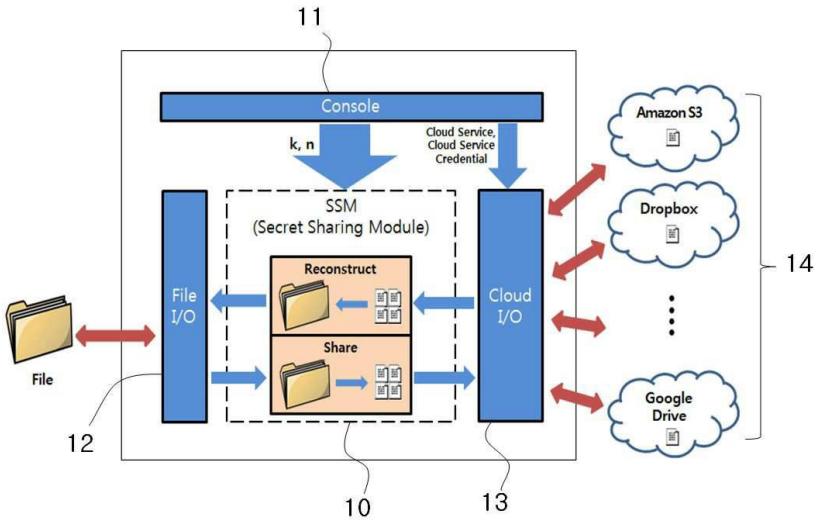
전체 청구항 수 : 총 9 항 심사관 : 구대성

(54) 발명의 명칭 **클라우드 환경에 비밀분산 기법을 이용한 데이터 보호 방법**

(57) 요 약

클라우드 환경에 비밀분산 기법을 이용한 데이터 보호 방법에 관한 것으로, 비밀분산 시스템이 클라우드 서비스에 파일을 업로드 하는 방법은, 클라우드 서비스에 업로드 할 파일을 선택하는 하고, 비밀분산 기법에 기초하여 상기 선택된 파일을 분할하고, 분할된 파일조각을 업로드 하기 위한 복수의 클라우드 서비스를 선택하며, 선택된 복수의 클라우드 서비스에 접속하여 분할된 파일조각을 상기 복수의 클라우드 서비스에 각각 업로드 한다. 또한, 비밀분산 시스템이 클라우드 서비스로부터 파일을 다운로드 하는 방법은,복수의 클라우드 서비스에 접속하여 분할된 파일조각을 검색하여 독출하고, 독출된 파일조각을 다운로드 하며, 비밀분산 기법에 기초하여 다운로드된 파일조각을 재조합한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 H0301-13-1003
부처명 지식경제부
연구관리전문기관 정보통신산업진흥원
연구사업명 대학 IT 연구센터 육성지원사업
연구과제명 클라우드 환경의 스마트 기기와 서비스 보안 기술 개발 및 연구 인력양성
기 여 율 1/1
주관기관 숭실대학교 산학협력단
연구기간 2013.01.01 ~ 2013.12.31

특허청구의 범위

청구항 1

비밀분산 시스템이 클라우드(Cloud) 서비스에 파일을 업로드(Upload) 하는 방법에 있어서,

상기 클라우드 서비스에 업로드 할 파일을 선택하는 단계;

상기 비밀분산 시스템이 비밀분산 기법에 기초하여 상기 선택된 파일을 1 바이트(byte) 내지 4 바이트씩 독출하여 분할하는 단계;

상기 비밀분산 시스템이 상기 분할된 파일조각을 업로드 하기 위한 복수의 클라우드 서비스를 선택하는 단계; 및

상기 비밀분산 시스템이 상기 선택된 복수의 클라우드 서비스에 접속하여 상기 분할된 파일조각을 상기 복수의 클라우드 서비스에 각각 업로드 하는 단계를 포함하되,

상기 비밀분산 기법은 분할시에 결정된 소정개수의 파일조각에 의해서만 재조합이 가능하도록 상기 선택된 파일을 분할함으로써, 데이터 기밀성을 제공하는 것을 특징으로 하는 방법.

청구항 2

제 1 항에 있어서,

상기 파일을 분할하는 단계는,

상기 파일을 분할하기 위한 조각의 개수인 n (n은 2 이상의 정수) 값을 설정하는 단계;

상기 분할된 파일을 재조합 하기 위한 개수인 k (k는 2 이상의 정수) 값을 설정하는 단계; 및

상기 설정된 n 개의 조각만큼 상기 선택된 파일을 분할하는 단계를 포함하되,

상기 k 값은 상기 n 값보다 작거나 같은 것을 특징으로 하는 방법.

청구항 3

제 2 항에 있어서,

상기 비밀분산 기법은,

파일조각을 재조합 하는 과정에서, 상기 클라우드 서비스로부터 획득한 파일조각이 k 개가 존재할 경우 상기 파일조각을 재조합 하여 분할 이전의 원본 파일을 획득할 수 있고, 상기 클라우드 서비스로부터 획득한 파일조각이 k 개 미만으로 존재할 경우 상기 파일조각을 재조합 할 수 없음으로써, 데이터의 기밀성을 제공하며,

상기 재조합에 사용된 파일조각 중 하나 이상의 파일조각에 변조가 발생하여 비정상적인 파일조각이 된 경우 분할 이전의 원본 파일을 획득할 수 없음으로써, 데이터의 무결성을 제공하는 것을 특징으로 하는 방법.

청구항 4

제 1 항에 있어서,

상기 클라우드 서비스를 선택하는 단계는,

상기 비밀분산 시스템에 연결된 복수의 클라우드 서비스 간의 통신 부하를 미리 검사하는 단계; 및

상기 검사 결과, 통신 부하가 최소인 통신 경로에 연결된 소정 개수의 클라우드 서비스를 선택하는 단계를 포함하는 방법.

청구항 5

삭제

청구항 6

제 1 항에 있어서,

상기 클라우드 서비스는 로컬(Local) 및 상기 비밀분산 시스템에 존재하는 자원을 사용하지 않으며, 네트워크(Network)를 통해 연결된 원격시스템의 자원을 사용하는 것을 특징으로 하는 방법.

청구항 7

제 1 항에 있어서,

상기 클라우드 서비스는,

아이디(ID)와 패스워드(Password)를 이용하여 인증을 받은 후 접속하는 것을 특징으로 하는 방법.

청구항 8

비밀분산 시스템이 클라우드(Cloud) 서비스로부터 파일을 다운로드(Download) 하는 방법에 있어서,

상기 비밀분산 시스템이 복수의 클라우드 서비스에 접속하여 분할된 파일조각을 검색하여 독출하는 단계;

상기 비밀분산 시스템이 상기 독출된 파일조각을 다운로드 하는 단계; 및

상기 비밀분산 시스템이 비밀분산 기법에 기초하여 상기 다운로드된 파일조각을 1 바이트(byte) 내지 4 바이트씩 독출하여 재조합하는 단계를 포함하되,

상기 비밀분산 기법은 분할시에 결정된 소정개수의 파일조각으로 원본 파일을 분할하고, 상기 소정개수의 파일조각에 의해서만 재조합이 가능함으로써, 데이터 기밀성을 제공하는 것을 특징으로 하는 방법.

청구항 9

제 8 항에 있어서,

상기 검색결과,

상기 파일조각이 검색될 경우 상기 파일조각을 상기 클라우드 서비스로부터 다운로드하며,

상기 파일조각이 검색되지 않을 경우 에러 메시지를 출력하는 것을 특징으로 하는 방법.

청구항 10

제 8 항에 있어서,

상기 비밀분산 기법은,

상기 클라우드 서비스로부터 다운로드된 파일조각의 개수와 원본 파일 분할시 재조합을 위해 설정된 값과 일치하는 경우 상기 파일조각을 재조합 하여 분할 이전의 원본 파일을 획득할 수 있고, 상기 클라우드 서비스로부터 다운로드된 파일조각의 개수가 상기 재조합을 위해 설정된 값보다 작은 경우 상기 파일조각을 재조합 할 수 없음으로써, 데이터의 기밀성을 제공하며,

상기 재조합에 사용된 파일조각 중 하나 이상의 파일조각에 변조가 발생하여 비정상적인 파일조각이 된 경우 분할 이전의 원본 파일을 획득할 수 없음으로써, 데이터의 무결성을 제공하는 것을 특징으로 하는 방법.

청구항 11

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 클라우드 환경에서 비밀분산 기법을 이용하는 데이터 보호 기술에 관한 것으로, 비밀분산 시스템이 파일을 다수의 조각으로 분할하고, 분할된 각 조각을 복수의 클라우드 서비스에 저장하여 데이터의 가용성 및 기밀성을 제공하는 방법에 관한 것이다.

배 경 기 술

[0002] IT 인프라가 발전하면서 기존의 출력물로 관리되었던 많은 양의 데이터가 디지털 데이터로 변환되어 저장 및 관리되고 있다. 특히 음악 또는 동영상과 같은 일반적인 데이터뿐만 아니라 기업 기밀 자료, 고객들의 개인 정보 등의 민감한 정보들도 디지털 형태로 저장되고 있다. 이러한 디지털 데이터는 기존의 아날로그 데이터보다 작은 공간을 사용하고, 쉽고 빠르게 생성 및 수정, 공유할 수 있는 장점이 있다. 하지만 USB 메모리와 같이 매우 작은 저장장치에 수백 기가의 자료를 저장할 수 있어, 중요한 정보가 저장된 장치를 분실하거나 도난당할 경우 매우 큰 피해를 입을 수 있다. 특히 데이터 유출이 발생하는 주요 경로에 노트북 또는 이동식 디스크와 같은 저장장치의 도난 및 분실이 높은 비율을 차지하고 있다.

[0003] 이와 같은 데이터 유출을 방지하기 위해 다양한 방법이 사용되고 있으며, 주로 데이터 암호화 방법을 사용한다. 하지만 데이터 암호화 방법은 해당 데이터의 유출 자체를 막는 것이 아니라 데이터가 유출되어도 해당 데이터의 내용을 획득할 수 없도록 하는 것을 목적으로 하는 한계가 있다.

[0004] 한편, 이하에서 인용되는 선행기술문헌에는 공격자가 데이터를 습득할 경우 유출된 데이터를 제어할 수 없는 문제점을 해결하기 위해, 데이터를 LS(Local share)와 RS(Remote share)로 분할한 후 LS는 사용자가 소지하고 RS는 클라우드 서비스에 저장함으로써, 공격자가 LS와 RS 중 하나를 획득하더라도 나머지 하나를 획득하지 못한다면 LS와 RS로 나누기 전의 온전한 데이터를 획득할 수 없도록 하는 방법을 소개하였다. 그러나 이러한 기술은 원래의 데이터를 획득하기 위해서는 2개로 분리된 LS와 RS를 재조합하여야 하고, 이때, LS는 데이터 소유자의 로컬 저장장치에 저장되며, RS와 재조합하기 위해서는 항상 LS를 소지해야 함으로써, 클라우드 서비스를 사용할 때 가장 큰 장점인 데이터 가용성이 낮아지는 한계가 존재한다.

[0005] 이상과 같은 관점에서, 클라우드 환경에서 데이터를 보호하기 위해서는 데이터 복구과정에서 가용성을 보장하고, 데이터의 무결성 및 기밀성 또한 보장하는 기술적 수단이 필요하다는 사실을 알 수 있다.

선행기술문헌

비특허문헌

[0006] (비특허문헌 0001) CLOUD SHREDDER: Removing the Laptop On-road Data Disclosure Threat in the Cloud Computing Era, 2011 International Joint Conferrence of IEEE TrustCom, Nan Zhang, 2011, 공개

발명의 내용

해결하려는 과제

[0007] 본 발명이 해결하고자 하는 기술적 과제는, 데이터를 암호화하여 유출된 데이터의 내용을 확인할 수 없도록 하는 종래의 방식에서 유출된 데이터를 공격자가 시간제한 없이 데이터 복호화 시도를 할 수 있다는 단점을 해결하고, 로컬 저장장치와 클라우드 서비스에 저장된 각각의 분할된 파일을 조합하는 방식이 데이터의 가용성을 훼손하는 단점을 해결함으로써, 기존의 데이터 보호 방법의 데이터 기밀성, 가용성 및 무결성이 훼손되는 한계를 극복하고자 한다.

과제의 해결 수단

[0008] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 비밀분산 시스템이 클라우드(Cloud) 서비스에 파일을 업로드(Upload) 하는 방법에 있어서, 상기 클라우드 서비스에 업로드 할 파일을 선택하는 단계; 상기 비밀분산 시스템이 비밀분산 기법에 기초하여 상기 선택된 파일을 분할하는 단계; 상기 비밀분산 시스템이 상기 분할된 파일조각을 업로드 하기 위한 복수의 클라우드 서비스를 선택하는 단계; 및 상기 비밀분산 시스템이 상기 선택된 복수의 클라우드 서비스에 접속하여 상기 분할된 파일조각을 상기 복수의 클라우드 서비스에 각각 업로드 하는 단계를 포함하되, 상기 비밀분산 기법은 분할시에 결정된 소정개수의 파일조각에 의해서만 재조합이 가능하도록 상기 선택된 파일을 분할함으로써, 데이터 기밀성을 제공할 수 있다.

[0009] 일 실시예에 따른 상기 파일을 분할하는 단계는, 상기 파일을 분할하기 위한 조각의 개수인 n (n은 2 이상의 정수) 값을 설정하는 단계; 상기 분할된 파일을 재조합 하기 위한 개수인 k (k는 2 이상의 정수) 값을 설정하는 단계; 및 상기 설정된 n 개의 조각만큼 상기 선택된 파일을 분할하는 단계를 포함하되, 상기 k 값은 상기 n 값

보다 작거나 같을 수 있다.

[0010] 일 실시예에 따른 상기 비밀분산 기법은, 파일조각을 재조합 하는 과정에서, 상기 클라우드 서비스로부터 획득한 파일조각이 k 개가 존재할 경우 상기 파일조각을 재조합 하여 분할 이전의 원본 파일을 획득할 수 있고, 상기 클라우드 서비스로부터 획득한 파일조각이 k 개 미만으로 존재할 경우 상기 파일조각을 재조합 할 수 없음으로써, 데이터의 기밀성을 제공하며, 상기 재조합에 사용된 파일조각 중 하나 이상의 파일조각에 변조가 발생하여 비정상적인 파일조각이 된 경우 분할 이전의 원본 파일을 획득할 수 없음으로써, 데이터의 무결성을 제공할 수 있다.

[0011] 일 실시예에 따른 상기 선택된 파일을 분할하는 단계는, 상기 선택된 파일을 1 바이트(byte) 내지 4 바이트씩 독출하여 분할할 수 있다.

[0012] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 비밀분산 시스템이 클라우드(Cloud) 서비스로부터 파일을 다운로드(Download) 하는 방법에 있어서, 상기 비밀분산 시스템이 복수의 클라우드 서비스에 접속하여 분할된 파일조각을 검색하여 독출하는 단계; 상기 비밀분산 시스템이 상기 독출된 파일조각을 다운로드 하는 단계; 및 상기 비밀분산 시스템이 비밀분산 기법에 기초하여 상기 다운로드된 파일조각을 재조합하는 단계를 포함하되, 상기 비밀분산 기법은 분할시에 결정된 소정개수의 파일조각으로 원본 파일을 분할하고, 상기 소정개수의 파일조각에 의해서만 재조합이 가능함으로써, 데이터 기밀성을 제공할 수 있다.

[0013] 일 실시예에 따른 상기 비밀분산 기법은, 상기 클라우드 서비스로부터 다운로드된 파일조각의 개수와 원본 파일 분할시 재조합을 위해 설정된 값과 일치하는 경우 상기 파일조각을 재조합 하여 분할 이전의 원본 파일을 획득할 수 있고, 상기 클라우드 서비스로부터 다운로드된 파일조각의 개수가 상기 재조합을 위해 설정된 값보다 작은 경우 상기 파일조각을 재조합 할 수 없음으로써, 데이터의 기밀성을 제공하며, 상기 재조합에 사용된 파일조각 중 하나 이상의 파일조각에 변조가 발생하여 비정상적인 파일조각이 된 경우 분할 이전의 원본 파일을 획득할 수 없음으로써, 데이터의 무결성을 제공할 수 있다.

[0014] 일 실시예에 따른 상기 다운로드된 파일조각을 재조합 하는 단계는, 상기 다운로드된 파일조각을 1 바이트(byte) 내지 4 바이트씩 독출하여 재조합할 수 있다.

발명의 효과

[0015] 본 발명의 실시예들은, 비밀분산 시스템이 파일을 분할하여 클라우드 서비스에 분할된 파일조각을 업로드 하고, 업로드된 파일조각을 비밀분산 시스템으로 다운로드하여 분할시에 결정된 소정개수의 파일조각에 의해서만 재조합이 가능하도록 파일을 분할함으로써, 데이터의 가용성 및 기밀성을 보장할 수 있다. 또한 재조합시에 사용된 파일조각 중 하나 이상의 파일조각이 변조가 발생하여 비정상적일 경우 원본 파일을 획득할 수 없음으로써, 데이터의 무결성 또한 보장할 수 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명의 실시예들이 채택하고 있는 클라우드 환경에서 비밀분산 기법을 이용한 데이터 보호 방법을 도시한 도면이다.

도 2는 본 발명의 일 실시예에 따른 비밀분산 시스템이 클라우드 서비스에 파일을 업로드 하는 방법을 설명하기 위한 흐름도이다.

도 3은 본 발명의 일 실시예에 따른 비밀분산 시스템이 클라우드 서비스에 파일을 업로드 하는 방법을 세부적으로 설명하기 위한 흐름도이다.

도 4는 본 발명의 일 실시예에 따른 비밀분산 시스템이 클라우드 서비스로부터 파일을 다운로드 하는 방법을 설명하기 위한 흐름도이다.

도 5는 본 발명의 일 실시예에 따른 비밀분산 시스템이 클라우드 서비스로부터 파일을 다운로드 하는 방법을 세부적으로 설명하기 위한 흐름도이다.

도 6은 본 발명의 일 실시예에 따른 클라우드 환경에서 비밀분산 시스템을 사용하여 데이터를 보호하는 방법을 기존의 다른 데이터 보호방법과 비교하여 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0017] 본 발명의 실시예들을 설명하기에 앞서 본 발명의 실시예들이 구현, 활용되는 환경에서 발생하고 있는 문제점을 제시하고, 이에 기초하여 안출된 본 발명의 기본 아이디어를 제시하도록 한다.

[0018] 앞서 지적한 바와 같이, 종래의 로컬 저장장치와 클라우드 서비스에 저장된 각각의 분할된 파일을 조합하기 위해서는 로컬 저장장치를 항상 소지해야 하며, 로컬 저장장치를 소지하지 않을 경우 원본 파일을 획득할 수 없음으로써, 클라우드 서비스의 최대 장점인 가용성이 훼손되었다. 따라서, 본 발명의 실시예들은 비밀분산 시스템이 파일을 분할하고, 상기 분할된 파일을 클라우드 서비스에 각각 업로드 하며, 상기 클라우드 서비스로부터 상기 비밀분산 시스템이 파일조각을 다운로드 하여 재조합함으로써, 데이터의 가용성, 기밀성 및 무결성을 보장할 수 있는 기술적 수단을 제안하고자 한다.

[0019] 도 1은 본 발명의 실시예들이 채택하고 있는 클라우드 환경에서 비밀분산 기법을 이용하여 데이터를 보호하는 기본 아이디어를 도시한 도면이다.

[0020] 파일I/O(File Input/Output)(12)는 사용자로부터 보호할 파일을 입력받고, 해당 파일을 분할하기 위해 비밀분산모듈(SSM: Secret Sharing Module)(10)로 전달한다. 상기 파일을 전달받은 콘솔(Console)(11)은 파일 업로드 시 분할할 조각의 수를 나타내는 n (n은 2 이상의 정수)과 재조합에 필요한 조각의 수를 나타내는 k (k는 2 이상의 정수)값을 비밀분산모듈(10)에 입력한다. 여기서, 비밀분산모듈(10)은 파일I/O(12)으로부터 전달받은 파일을 사용자가 입력한 k, n 값을 이용하여 k개 이상을 모을 경우 재결합할 수 있는 n 개의 조각으로 분할하여 클라우드I/O(13)에 전달한다. 이제, 클라우드I/O(13)는 비밀분산모듈(10)로부터 분할된 조각들을 전달받아 복수의 클라우드 서비스(14)에 각각 업로드 한다. 이때 사용자로부터 아이디(ID)와 패스워드(Password)를 입력받거나 미리 입력된 아이디와 패스워드를 이용한다.

[0021] 한편, 분할된 파일을 클라우드 서비스로부터 다운로드하여 재조합하기 위해, 클라우드I/O(13)는 사용자로부터 입력받거나 미리 입력된 아이디와 패스워드를 이용하여 파일조각들이 저장되어 있는 복수의 클라우드 서비스(14)에 접근하고, 해당 파일조각들을 다운로드 하여 비밀분산모듈(10)에게 전달한다. 파일조각들을 전달받은 비밀분산모듈(10)은 다수의 파일조각을 재결합하여 온전한 하나의 파일을 생성하여 파일I/O(12)에 전달한다. 이때, 해당 조각은 상기 콘솔(11)로부터 입력받은 k 개 이상이어야 하며, k 개 미만일 경우 파일 생성이 불가능하다. 마지막으로, 파일I/O(12)는 비밀분산모듈(10)로부터 전달받은 파일을 시스템에 저장한다.

[0022] 이하에서는 첨부된 도면을 참조하여 본 발명의 실시예들을 보다 구체적으로 설명한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 또한, 도면 전체에 걸쳐 동일한 구성 요소들은 가능한 한 동일한 도면 부호로 나타내고 있음에 유의하여야 한다.

[0023] 도 2는 본 발명의 일 실시예에 따른 비밀분산 시스템이 클라우드 서비스에 파일을 업로드 하는 방법을 설명하기 위한 흐름도이다.

[0024] S201 단계에서, 비밀분산 시스템은 파일을 분할하여 클라우드 서비스에 업로드 할 대상 파일을 선택할 수 있다.

[0025] S202 단계에서, 상기 비밀분산 시스템은 상기 선택된 파일을 비밀분산 기법에 기초하여 상기 선택된 파일을 분할할 수 있다.

[0026] S203 단계에서, 상기 비밀분산 시스템은 상기 분할된 파일조각을 업로드 하기 위한 복수의 클라우드 서비스를 선택할 수 있다.

[0027] S204 단계에서, 상기 비밀분산 시스템이 상기 선택된 복수의 클라우드 서비스에 접속하여 상기 분할된 파일조각을 상기 복수의 클라우드 서비스에 각각 업로드 할 수 있다.

[0028] 도 3은 본 발명의 일 실시예에 따른 비밀분산 시스템이 클라우드 서비스에 파일을 업로드 하는 방법을 세부적으로 설명하기 위한 흐름도이다.

[0029] S301 단계에서, 비밀분산 시스템은 파일을 분할하여 클라우드 서비스에 업로드 할 대상 파일을 선택할 수 있다.

[0030] S302 단계에서, 비밀분산 시스템은 비밀분산 기법에 기초하여, 상기 파일을 분할하기 위한 조각의 개수인 n (n은 2 이상의 정수) 값을 설정하며, 상기 분할된 파일을 재조합 하기 위한 개수인 k (k는 2 이상의 정수) 값을 설정할 수 있다.

[0031] 여기서, 상기 비밀분산 기법은 데이터를 n(n은 정수)조각으로 분할하면 k(k는 정수)개 이상을 모을 경우 분할 이전의 데이터를 복원할 수 있지만, k 개 이하의 조각으로부터는 데이터에 대한 아무런 정보도 얻을 수 없다.

[0032] S303 단계에서, 비밀분산 시스템은 상기 비밀분산 기법에 기초하여, 설정된 k 및 n 값이 상기 비밀분산 기법에 적용 가능한 정상적인 값인지를 확인하여 도출할 수 있다.

[0033] 이때, 상기 비밀분산 기법에 기초하여 설정된 상기 k 및 상기 n 값이 2 이상의 정수이고, 상기 k 값은 상기 n 값보다 작거나 같을 경우는 304단계로 진행하여 상기 설정된 n 개의 파일조각으로 분할할 수 있다.

[0034] 반면, 상기 비밀분산 기법에 기초하여 설정된 상기 k 및 상기 n 값이 2 미만의 정수이거나 상기 k 값은 상기 n 값보다 클 경우 S302 단계로 진행하여 상기 n 값 및 상기 k 값을 재입력할 수 있다.

[0035] S304 단계에서, 비밀분산 시스템은 상기 S302 단계에서 설정된 파일을 분할하기 위한 조각의 개수인 n 개의 파일로 분할한다.

[0036] 여기서, 분할되는 조각의 값이 n 의 값이고, 분할하고자 하는 비밀의 값이 m 의 값이며, p 는 상기 n 값에 1을 더한 소수보다 크거나 같고, 상기 m 값에 1을 더한 소수보다 크거나 같다라고 가정하면, 현재 대부분 사용되는 비밀분산 기법은 상기 n 값과 상기 m 값이 상기 p 값보다 작아야만 동작한다. 즉 $p > \max(m,n)$일 때만 동작한다. 이는 연산 결과가 중복되지 않기 위해 필요한 조건이며, 이를 만족하지 않을 경우 아래와 같은 문제가 발생한다.

[0037] 상기 p 의 값이 예를 들어, 17일 경우 상기 m 의 값이 이보다 크다면 mod 17 연산 결과가 동일한 문제가 발생할 수 있다. 즉 연산과정 중 20 mod 17 = 3과 3 mod 17 경우 연산 결과가 동일한 3이며, 이를 복원할 때 복원된 값이 20인지 3인지 분별할 수 없는 문제가 발생한다. 따라서 비밀분산 기법은 상기 m 값보다 큰 상기 p 값을 가져야 하고 매우 큰 데이터의 경우 이보다 큰 소수인 상기 p 값을 찾는 것이 불가능하다. 즉 일반적으로 사용되는 비밀분산 기법은 큰 데이터를 분할할 수 없는 한계가 있으며 통상적으로 1024비트(bit)(128바이트(byte)), 2048비트(256바이트)의 값에 대해 비밀분산 기법을 적용한다. 하지만 본 발명에서 사용하는 비밀분산 방법의 경우 데이터 자체를 분할해야 하므로 매우 큰 상기 p 값이 필요하다. 이를 해결하기 위해 1 바이트 단위로 비밀분산 기법을 적용하였으며 이는 상기 p 값이 최소 257 보다 큰 값이라면 정상적으로 동작이 가능하고, 기밀성도 보장된다. 즉 예를 들어 5메가바이트(Mbytes) 이상의 파일의 경우 5메가바이트의 파일 전체에 대해 비밀분산 기법을 적용하지 않고,파일의 내용중 1바이트의 데이터에만 비밀분산 기법을 적용하고, 이를 5M(5000000) 만큼 반복하여 파일을 분할한다. 이러한 방법을 통해 대용량 파일의 분할을 해결할 수 있다. 이 방법은 조금 수정하여 2바이트, 4바이트 크기의 블록 단위 변환으로 사용할 수도 있다.

[0038] 또한, 분할된 파일조각은 파일헤더에 순차적으로 숫자를 태그(tagging)하여 각각의 파일조각이 구분되도록 할 수 있다.

[0039] S305 단계에서, 비밀분산 시스템은 S304 단계에서 분할된 파일조각을 업로드 하기 위한 복수의 클라우드 서비스를 선택할 수 있다.

[0040] 여기서, 상기 클라우드 서비스는 로컬(Local) 및 상기 비밀분산 시스템에 존재하는 자원을 사용하지 않으며, 네트워크(Network)를 통해 연결된 원격시스템의 자원을 사용할 수 있다. 또한, 클라우드 서비스를 선택함에 있어서, 상기 비밀분산 시스템에 연결된 복수의 클라우드 서비스 간의 통신 부하를 미리 검사하고, 상기 검사 결과, 통신 부하가 최소인 통신 경로에 연결된 S302 단계에서 설정된 n 개의 클라우드 서비스를 선택할 수 있다.

[0041] S306 단계에서, 비밀분산 시스템은 S305 단계에서 선택된 복수의 클라우드 서비스에 접속하기 위한 인증절차를 진행하게 된다. 여기서, 상기 인증절차는 아이디와 패스워드를 통해 인증받는 절차이며, 상기 인증절차가 정상적으로 완료되면 상기 클라우드 서비스에 접속할 수 있다.

[0042] S307 단계에서, 비밀분산 시스템은 S306 단계에서 클라우드 서비스에 접속하기 위해 인증 수단으로 입력한 아이디와 패스워드가 인증을 위해 미리 정해진 값과 일치하는지를 확인한다.

[0043] 확인결과, 상기 입력된 아이디와 패스워드가 인증을 위해 미리 정해진 값과 일치하지 않을 경우, S306 단계로 진행하여 다시 아이디와 패스워드를 입력하게 된다. 반면, 상기 입력된 아이디와 패스워드가 인증을 위해 미리 정해진 값과 일치할 경우, S308 단계로 진행한다.

[0044] S308 단계에서, 비밀분산 시스템은 S304 단계에서 분할된 파일조각을 S305 단계에서 선택된 복수의 클라우드 서비스에 각각 업로드 할 수 있다.

[0045] 도 4는 본 발명의 일 실시예에 따른 비밀분산 시스템이 클라우드 서비스로부터 파일을 다운로드 하는 방법을 설명하기 위한 흐름도이다.

[0046] S401 단계에서 비밀분산 시스템은 복수의 클라우드 서비스에 접속하여 분할된 파일조각을 검색하여 독출할 수 있다.

[0047] S402 단계에서 비밀분산 시스템은 S401 단계에서 독출된 파일조각을 다운로드 할 수 있다.

[0048] S403 단계에서 비밀분산 시스템은 비밀분산 기법에 기초하여 S402 단계에서 다운로드된 파일조각을 재조합할 수 있다.

[0049] 도 5는 본 발명의 일 실시예에 따른 비밀분산 시스템이 클라우드 서비스로부터 파일을 다운로드 하는 방법을 세부적으로 설명하기 위한 흐름도이다.

[0050] S501 단계에서 비밀분산 시스템은 접속 가능한 클라우드 서비스를 검색하여 상기 검색된 클라우드 서비스에 접속할 수 있다.

[0051] S502 단계에서, 비밀분산 시스템은 S501 단계에서 검색된 복수의 클라우드 서비스에 접속하기 위한 인증절차를 진행하게 된다. 여기서, 상기 인증절차는 아이디와 패스워드를 통해 인증받는 절차이며, 상기 인증절차가 정상적으로 완료되면 상기 클라우드 서비스에 접속할 수 있다.

[0052] S503 단계에서, 비밀분산 시스템은 S502 단계에서 클라우드 서비스에 접속하기 위해 인증 수단으로 입력한 아이디와 패스워드가 인증을 위해 미리 정해진 값과 일치하는지를 확인한다.

[0053] 확인결과, 상기 입력된 아이디와 패스워드가 인증을 위해 미리 정해진 값과 일치하지 않을 경우, S502 단계로 진행하여 다시 아이디와 패스워드를 입력하게 된다. 반면, 상기 입력된 아이디와 패스워드가 인증을 위해 미리 정해진 값과 일치할 경우, S504 단계로 진행한다.

[0054] S504 단계에서, 비밀분산 시스템은 현재 접속된 클라우드 서비스에 분할된 파일조각이 존재하는지 검색한다.

[0055] 여기서, 상기 분할된 파일조각이 검색하여 도출될 경우 S505 단계로 진행하여 상기 도출된 파일조각을 다운로드하며, 반면, 상기 분할된 파일조각이 검색하여 도출되지 않을 경우 S506 단계로 진행하여 에러메시지를 출력할 수 있다.

[0056] 또한, 상기 분할된 파일조각을 검색하는 것은 분할시 파일헤더에 태깅된 숫자에 기초하여 검색할 수 있으며, S501 단계에서 접속 가능 클라우드 서비스가 하나 이상일 경우 상기 비밀분산 시스템은 복수의 클라우드 서비스에 동시에 접속하여 분할된 파일조각을 검색할 수 있으며, 상기 비밀분산 시스템은 로컬 리소스의 부하여부를 판단하여 순차적으로 복수의 클라우드 서비스에 접속하여 분할된 파일조각을 검색할 수 있다.

[0057] S505 단계에서, 비밀분산 시스템은 클라우드 서비스로부터 분할된 파일조각을 다운로드할 수 있다.

[0058] S507 단계에서, 비밀분산 시스템은 S505 단계에서 다운로드된 파일조각을 비밀분산 기법에 기초하여 재조합할 수 있다.

[0059] 여기서 비밀분산 기법은 분할시에 결정된 파일 재조합에 필요한 k 개수의 파일조각으로 원본 파일을 분할하고, 상기 k 개수의 파일조각에 의해서만 재조합이 가능함으로써 데이터의 기밀성을 제공할 수 있다.

[0060] S508 단계에서, 비밀분산 시스템은 S506 단계에서 재조합에 사용된 파일조각의 개수를 분할시 설정한 파일 재조합에 필요한 개수인지를 확인할 수 있다.

[0061] 여기서, 상기 파일 재조합에 사용된 파일조각의 개수가 분할시 설정한 파일 재조합에 필요한 개수인 k 값보다 미만일 경우 S506단계로 진행하여 에러메시지가 발생하며, 분할 이전의 원본 파일의 복구가 불가능하다. 반면, 상기 파일 재조합에 사용된 파일조각의 개수가 분할시 설정한 파일 재조합에 필요한 개수인 k 개수일 경우 S509 단계로 진행할 수 있다.

[0062] S509 단계에서, 비밀분산 시스템은 올바른 S507 단계에서 파일 재조합에 사용된 파일조각이 올바른 파일조각인지 검사할 수 있다.

[0063] 여기서, 상기 파일 재조합에 사용된 파일조각 중 하나 이상의 파일조각에 변조가 발생하여 비정상적인 파일조각이 된 경우, S511 단계로 진행하여 비정상적인 파일을 생성하고, 분할 이전의 원본 파일을 획득할 수 없다, 반면, 상기 파일 재조합에 사용된 파일조각이 모두 변조가 발생하지 않은 정상적인 파일조각일 경우, 무결성이 보장되는 원본 파일을 생성할 수 있다.

[0064] S510 단계에서, 비밀분산 시스템은 분할된 파일조각을 재조합하여 분할 이전의 원본 파일을 생성할 수 있다.

[0065] 도 6은 본 발명의 일 실시예에 따른 클라우드 환경에서 비밀분산 시스템을 사용하여 데이터를 보호하는 방법을 기존의 다른 데이터 보호방법과 비교하여 도시한 도면이다.

[0066] 상기된 본 발명의 실시예들에 따르면, 비밀분산 시스템이 비밀분할 기법에 기초하여 파일을 분할하고, 클라우드 서비스에 분할된 파일조각을 업로드 하며, 업로드된 파일조각을 비밀분산 시스템으로 다운로드하여 분할시에 결정된 소정개수의 파일조각에 의해서만 재조합이 가능하도록 파일을 분할함으로써, 데이터의 가용성 및 기밀성을 보장할 수 있다.

[0067] 또한, 사용자가 다수의 클라우드 서비스의 아이디와 패스워드를 다르게 설정한다면 공격자가 하나의 클라우드 서비스에 대한 아이디와 패스워드를 획득하더라도 하나의 상기 하나의 클라우드 서비스에 업로드된 파일조각만 획득할 수 있다. 하지만, 파일분할 이전의 원본 파일을 획득하기 위해서는 다른 클라우드 서비스에 저장된 파일조각들이 필요하다. 따라서 공격자는 각 클라우드 서비스에 접근할 수 있는 아이디와 패스워드를 모두 획득해야 하므로 각 클라우드 서비스에 대한 추가적인 공격이 필요하다. 이는 공격자로 하여금 많은 시간과 노력을 소요하게 만든다. 더욱이 파일 소유자가 패스워드를 주기적으로 변경한다면 패스워드가 변경되기 전까지 제한된 시간 내에 모든 클라우드 서비스의 아이디와 패스워드를 획득해야 하는 어려움이 있다. 특히 데이터를 로컬 디스크에 저장하지 않고, 클라우드서비스에 저장하기 때문에 노트북, USB 메모리와 같은 데이터가 저장된 기기나 저장장치를 분실하여도 데이터를 안전하게 보호할 수 있다. 또 네트워크에 연결만 할 수 있다면 데이터 조각들을 다운로드하여 원래의 파일을 생성할 수 있기 때문에 종래의 기술이 제공하지 못했던 높은 데이터 가용성도 제공받을 수 있다.

[0068] 한편, 본 발명은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0069] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현하는 것을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

[0070] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

[0071] 10 : 비밀분산모듈(Secret sharing module)

11 : 콘솔(Console)

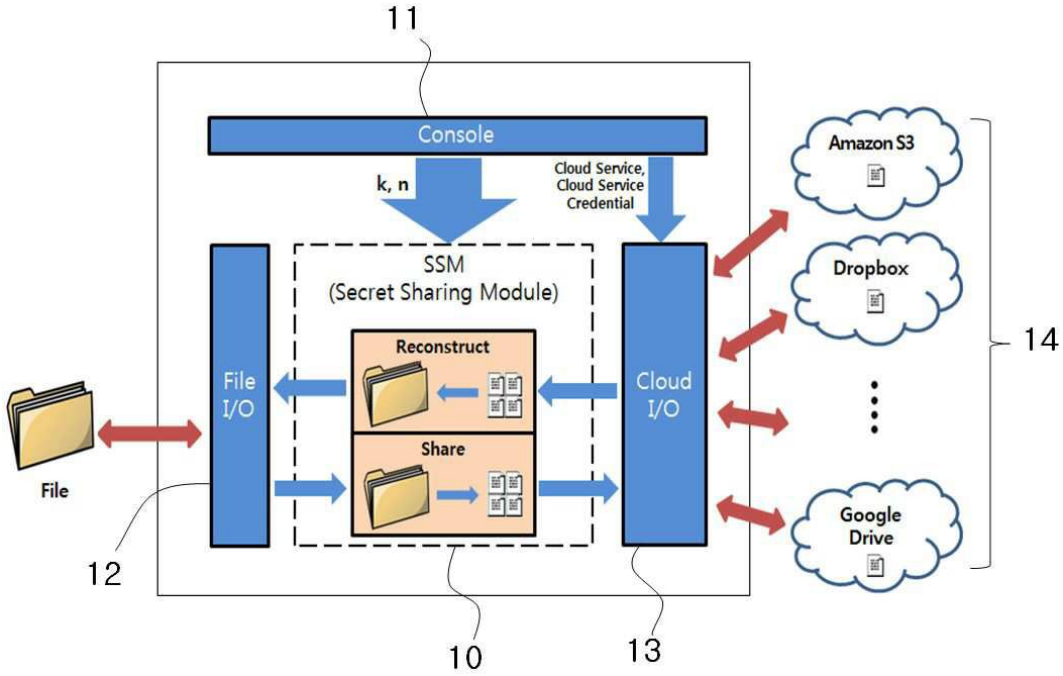
12 : 파일I/O(FIle Input/Output)

13 : 클라우드I/O(Cloud I/O)

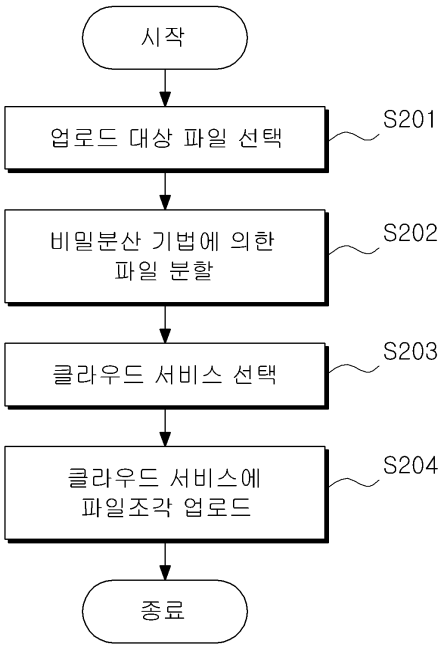
14 : 클라우드 서비스(Cloud Service)

도면

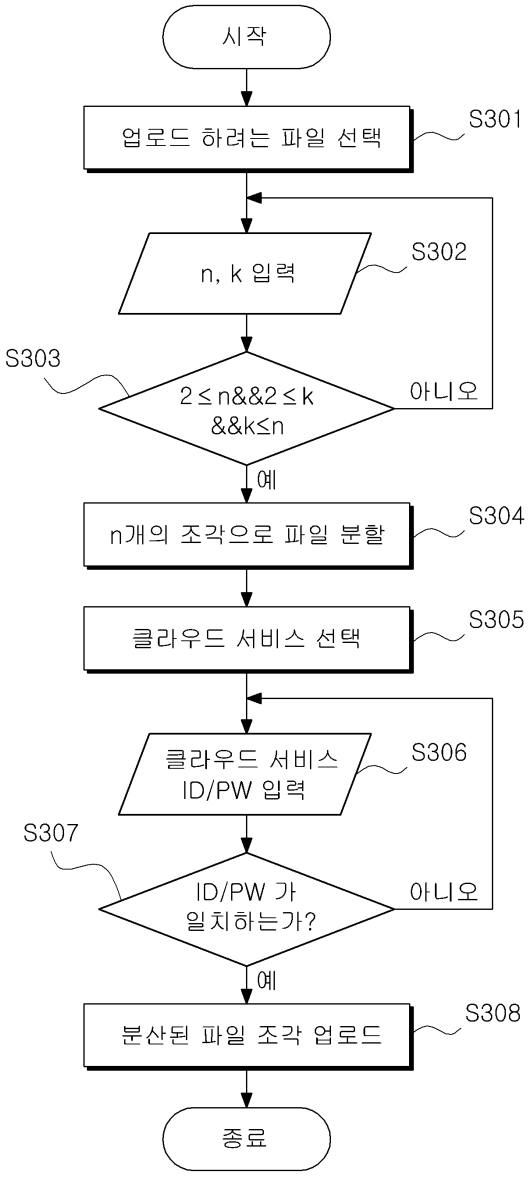
도면1


11
Console
k, n
Cloud Service,
Cloud Service
Credential
SSM
(Secret Sharing Module)
Reconstruct
Share
File
I/O
Cloud
I/O
File
12
10
13
Amazon S3
Dropbox
Google
Drive
14

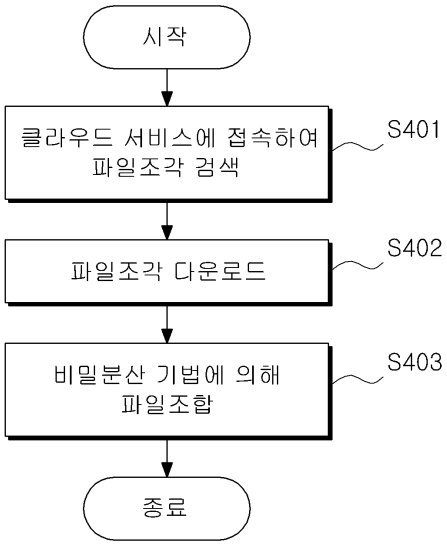
도면2


시작
업로드 대상 파일 선택
S201
비밀분산 기법에 의한
파일 분할
S202
클라우드 서비스 선택
S203
클라우드 서비스에
파일조각 업로드
S204
종료

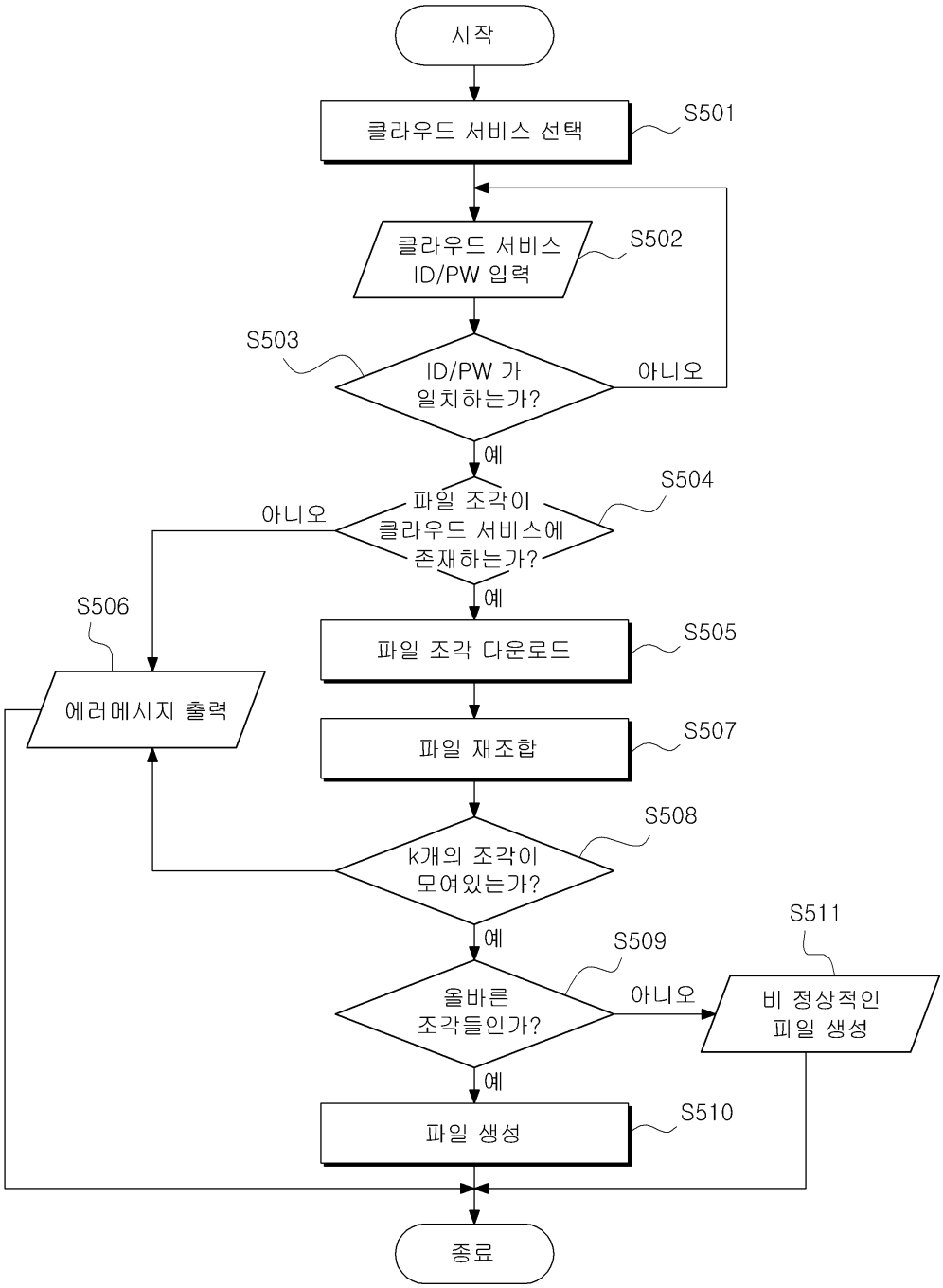
도면3


시작
업로드 하려는 파일 선택
S301
n, k 입력
S302
S303
2≤n&&2≤k
&&k≤n
아니오
예
n개의 조각으로 파일 분할
S304
클라우드 서비스 선택
S305
클라우드 서비스
ID/PW 입력
S306
S307
ID/PW 가
일치하는가?
아니오
예
분산된 파일 조각 업로드
S308
종료

도면4


시작
클라우드 서비스에 접속하여 파일조각 검색
S401
파일조각 다운로드
S402
비밀분산 기법에 의해 파일조합
S403
종료

도면5


시작
클라우드 서비스 선택
S501
클라우드 서비스
ID/PW 입력
S502
S503
ID/PW 가
일치하는가?
아니오
예
파일 조각이
클라우드 서비스에
존재하는가?
S504
아니오
예
S506
파일 조각 다운로드
S505
에러메시지 출력
파일 재조합
S507
k개의 조각이
모여있는가?
S508
예
S509
올바른
조각들인가?
아니오
S511
비 정상적인
파일 생성
예
파일 생성
S510
종료