

클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법 및 이를 위한 장치

(기술분류-보안-네트워크-클라우드 보안)

기술성 분석

기술 개요

- 본 기술은 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법 및 장치에 관한 것으로, 디지털포렌식 활동에 필요한 비용과 자원을 절감함으로써 효율성을 향상시킬 수 있음
- 또한, 클라우드 스토리지에 저장된 데이터 중 범죄와 관련된 데이터만 선별적으로 수집함으로써 피압수자의 프라이버시를 강화할 수 있음

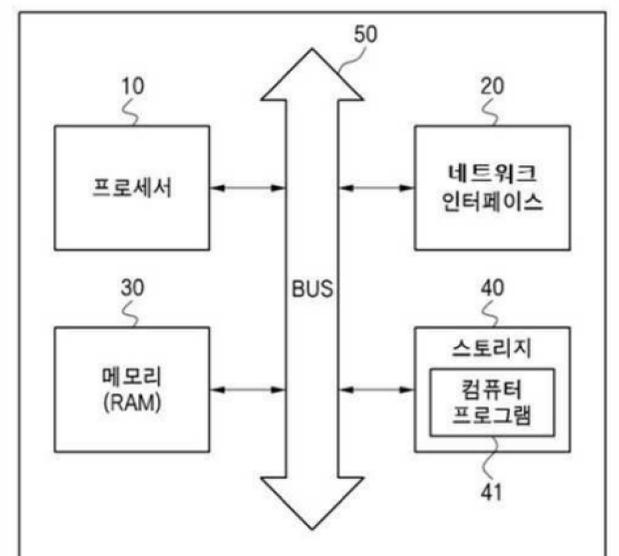
미해결 과제(Unmet needs)

- 기존 디지털포렌식 방법의 문제점
 - 종래 디지털포렌식은 클라우드 스토리지에 저장된 데이터를 수집하기 위해 피압수자의 계정 정보를 확보하여 저장된 데이터를 모두 수집하고 분석하는 원시적인 방법을 사용해왔음
 - 그러나, 클라우드 스토리지에 저장된 데이터가 많아지면서 데이터 수집에 소요되는 시간이 증가하며, 수집한 데이터를 저장할 저장 매체까지 따로 필요한 바, 필요한 비용과 자원이 증가하는 문제점이 있음
 - 또한, 클라우드 스토리지에 저장된 모든 데이터가 범죄와 관련된 데이터가 아님에도 불구하고 일률적으로 수집의 대상이 되어 피압수자의 프라이버시 침해 문제가 존재함

기술적 해결수단(발명의 구성)

- 1) 본 기술의 디지털포렌식 장치의 구성
 - 본 기술에 따른 클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 장치는 프로세서(10), 네트워크 인터페이스(20), 메모리(30), 스토리지(40) 및 이들을 연결하는 데이터 버스(50)를 포함함
 - 프로세서는 각 구성의 전반적인 동작을 제어하며, 네트워크 인터페이스는 장치의 유무선 인터넷 통신을 지원함
 - 메모리는 각종 정보, 명령 및/또는 정보를 저장하며, 본 발명에 따른 디지털포렌식 방법을 수행하기 위해 스토리지로부터 하나 이상의 컴퓨터 프로그램(41)을 로드함
 - 스토리지는 하나 이상의 컴퓨터 프로그램 및 대용량 네트워크 정보를 비임시적으로 저장함
 - 데이터 버스는 프로세서, 네트워크 인터페이스, 메모리 및 스토리지 사이의 명령 및/또는 정보의 이동 경로가 됨

본 발명에 따른 디지털포렌식 장치의 구성



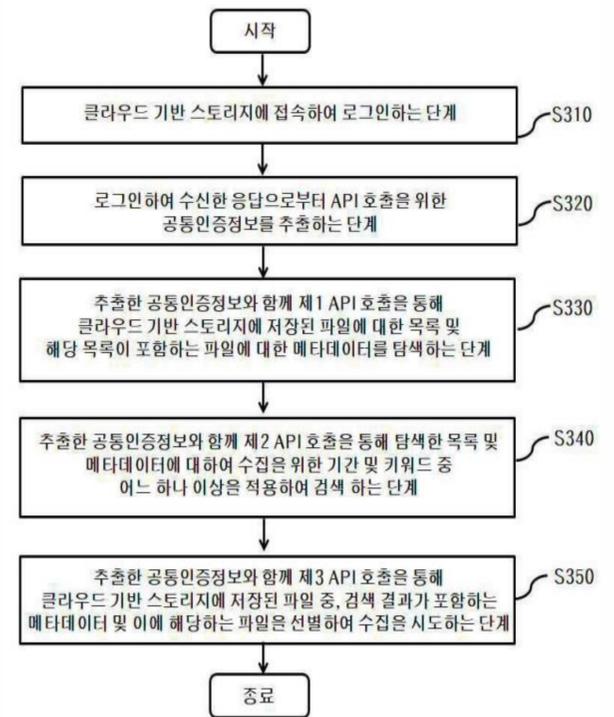
본 기술의 우수성 및 파급 효과

본 기술의 우수성(효과)

- 디지털포렌식 활동의 효율성 향상 및 피압수자의 프라이버시 강화
 - (S310, S320) 클라우드 기반 스토리지에 로그인하여 수신한 응답으로부터 API*호출을 위한 공통인증정보를 추출함
 - (S330) 추출한 공통인증정보와 함께, 스토리지에 저장된 파일에 대한 목록 및 해당 목록이 포함하는 파일에 대한 메타데이터를 탐색하는 제1 API를 호출하여 메타데이터를 탐색함
 - (S340) 추출한 공통인증정보와 함께, 메타데이터 내에서 기간, 키워드 및 썸네일 중 어느 하나 이상을 적용하기 위한 제2 API를 호출하여 검색을 실시함
 - (S350) 추출한 공통인증정보와 함께, 제3 API 호출을 통해 스토리지에 저장된 파일 중, 검색 결과가 포함하는 메타데이터 및 이에 해당하는 파일을 선별하여 수집함
- 따라서, 검색 결과에 포함되는 메타데이터를 우선적으로 선별하여 수집하고, 이에 해당하는 파일들만 선별하여 수집함으로써 스토리지에 저장된 파일 전부에 대한 디지털포렌식 활동이 필요하지 않게 되어 비용과 자원을 절감하여 효율성을 향상시킬 수 있으며, 수집하고자 하는 데이터만을 선별하여 수집할 수 있기 때문에 피압수자의 프라이버시를 강화할 수 있음

* API (Application Programming Interface): 응용 프로그램이 운영 체제나 데이터베이스 관리 시스템 등과 같은 시스템 프로그램과 통신할 때 사용되는 언어나 메시지 형식을 가지며, 프로그램 내에서 실행을 위해 특정 서브루틴에 연결을 제공하는 함수를 호출하는 방식으로 구현됨

본 발명에 따른 디지털포렌식 방법



적용 제품 및 파급 효과

- 디지털포렌식 장치
- 본 기술을 통해 종래 디지털포렌식 활동의 효율성과 피압수자의 프라이버시에 관한 문제점들을 해결함과 동시에 최근의 클라우드 스토리지 서비스에 적합하게 적용될 수 있는 새롭고 진보적인 기술을 제공할 수 있음

지식재산권 현황

발명의 명칭	출원/등록번호	출원/등록일자
클라우드 기반 스토리지의 데이터를 수집하는 디지털포렌식 방법 및 이를 위한 장치	10-2022-0128375	2022.10.07.
패밀리 특허 현황	패밀리 국가	
-	-	