(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년10월11일
(11) 등록번호 10-2715592
(24) 등록일자 2024년10월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01)
(52) CPC특허분류
H04L 63/1433 (2013.01)
H04L 63/1425 (2013.01)
(21) 출원번호 10-2023-0074162
(22) 출원일자 2023년06월09일
심사청구일자 2023년10월06일
(56) 선행기술조사문헌
KR101920613 B1*
KR1020120007842 A*
KR1020230073056 A*
KR1020160114077 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인스피언 주식회사
서울특별시 금천구 벚꽃로 278, 1309호, 1310호, 1311호(가산동, 에스제이테크노빌)
(72) 발명자
신동하
경기도 용인시 수지구 푸른솔로 20, 꽃메마을현대홈타운,554동 403호
송균상
서울특별시 중랑구 양원역로6가길 19, 중랑해모로아파트,101동 903호
최정규
서울특별시 서초구 서초중앙로 200, 삼풍아파트, 6동 902호
(74) 대리인
지관영

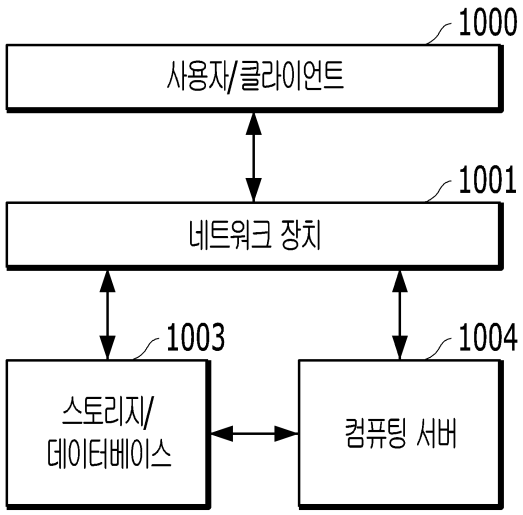
전체 청구항 수 : 총 9 항 심사관 : 문형섭

(54) 발명의 명칭 **데이터 관리 장치, 데이터 관리 방법 및 데이터 관리 프로그램을 저장하는 컴퓨터로 판독 가능한 저장 매체**

(57) 요 약

본 발명은 데이터를 수집하는 단계; 상기 수집된 데이터를 분류하는 단계; 및 상기 데이터에 포함된 적어도 하나의 정보를 매핑하여 사용자 행위 메타데이터를 생성하는 단계를 포함하는, 데이터 관리 방법을 제공한다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

애플리케이션 개발환경 유형 별 키 및 사용자 행위를 식별하기 위한 키 ID를 포함하는 데이터를 수집하는 단계;

상기 수집된 데이터를 분류하고 분석하는 단계;

상기 애플리케이션 개발환경 유형 별 키와 사용자 행위를 식별하기 위한 키 ID를 매핑하여 사용자 행위 메타데이터를 생성하되, 상기 애플리케이션 개발환경 유형 별 키와 사용자 행위를 식별하기 위한 키 ID를 이용하여 사용자 행위를 식별하고, 상기 식별된 사용자 행위를 상기 사용자 행위 메타데이터에 저장하는 단계;

상기 애플리케이션 개발환경 유형은 아키텍처 유형을 포함하되, 상기 아키텍처 유형은 GUI 데이터 유형, json 데이터 유형 및 WEBGUI 데이터 유형 중 적어도 하나인 것을 특징으로 하는, 데이터 관리 방법.

청구항 2

제 1 항에 있어서,

상기 데이터에 개인정보가 포함된 경우, 상기 데이터에 기초하여 개인정보 메타데이터에 포함된 필드를 정의하는 단계;

상기 개인정보의 유형 별로 사용되는 패턴을 저장하는 단계;

개인정보 예외처리 리스트를 생성하는 단계;

상기 개인정보 메타데이터 및 상기 개인정보 예외처리 리스트에 기초하여 개인정보 추출 규칙을 생성하는 단계;

상기 개인정보 추출 규칙에 기초하여 상기 개인정보를 추출하는 단계;

상기 개인정보 유형 별 값 필터를 생성하는 단계; 및

상기 추출된 개인 정보를 상기 값 필터에 기초하여 검증하는 단계를 포함하는, 데이터 관리 방법.

청구항 3

제 1 항에 있어서,

상기 사용자 행위 메타데이터와 저장된 로그 데이터를 매핑하기 위하여 상기 로그 데이터를 인덱스 처리하는 단계를 더 포함하고,

상기 로그 데이터를 인덱스 처리하는 단계는, 상기 인덱스에 텍스트를 추가하는 단계를 더 포함하되, 상기 텍스트는 상기 수집된 데이터 중 상기 사용자 행위와 관련된 텍스트를 AI 엔진을 통하여 분류한 것을 특징으로 하는, 데이터 관리 방법.

청구항 4

제 3 항에 있어서,

상기 로그 데이터에 대한 조회를 요청받는 단계; 및

상기 인덱스에 포함된 상기 분류된 텍스트를 제공하는 단계를 더 포함하는, 데이터 관리 방법.

청구항 5

데이터를 저장하는 데이터베이스; 및

상기 데이터를 처리하는 프로세서를 포함하고,

상기 프로세서는,

애플리케이션 개발환경 유형 별 키 및 사용자 행위를 식별하기 위한 키 ID를 포함하는 데이터를 수집하고,

상기 수집된 데이터를 분류하고 분석하고,

상기 애플리케이션 개발환경 유형 별 키와 사용자 행위를 식별하기 위한 키 ID를 매핑하여 사용자 행위 메타데이터를 생성하되, 상기 애플리케이션 개발환경 유형 별 키와 사용자 행위를 식별하기 위한 키 ID를 이용하여 사용자 행위를 식별하고, 상기 식별된 사용자 행위를 상기 사용자 행위 메타데이터에 저장하고,

상기 애플리케이션 개발환경 유형은 아키텍쳐 유형을 포함하되, 상기 아키텍쳐 유형은 GUI 데이터 유형, json 데이터 유형 및 WEBGUI 데이터 유형 중 적어도 하나인 것을 특징으로 하는, 데이터 관리 장치.

청구항 6

제 5 항에 있어서,

상기 프로세서는,

상기 데이터에 개인정보가 포함된 경우, 상기 데이터에 기초하여 개인정보 메타데이터에 포함된 필드를 정의하고,

상기 개인정보의 유형 별로 사용되는 패턴을 저장하고,

개인정보 예외처리 리스트를 생성하고,

상기 개인정보 메타데이터 및 상기 개인정보 예외처리 리스트에 기초하여 개인정보 추출 규칙을 생성하고,

상기 개인정보 추출 규칙에 기초하여 상기 개인정보를 추출하고,

상기 개인정보 유형 별 값 필터를 생성하고,

상기 추출된 개인 정보를 상기 값 필터에 기초하여 검증하

는, 데이터 관리 장치.

청구항 7

제 5 항에 있어서,

상기 프로세서는

상기 사용자 행위 메타데이터와 저장된 로그 데이터를 매핑하기 위하여 상기 로그 데이터를 인덱스 처리하고,

상기 인덱스에 텍스트를 추가하되, 상기 텍스트는 상기 수집된 데이터 중 상기 사용자 행위와 관련된 텍스트를 AI 엔진을 통하여 분류한 것을 특징으로 하는, 데이터 관리 장치.

청구항 8

제 7 항에 있어서,

상기 프로세서는

상기 로그 데이터에 대한 조회를 요청받는 경우, 상기 인덱스에 포함된 상기 분류된 텍스트를 제공하는, 데이터 관리 장치.

청구항 9

애플리케이션 개발환경 유형 별 키 및 사용자 행위를 식별하기 위한 키 ID를 포함하는 데이터를 수집하는 단계;

상기 수집된 데이터를 분류하고 분석하는 단계;

상기 애플리케이션 개발환경 유형 별 키와 사용자 행위를 식별하기 위한 키 ID를 매핑하여 사용자 행위 메타데이터를 생성하되, 상기 애플리케이션 개발환경 유형 별 키와 사용자 행위를 식별하기 위한 키 ID를 이용하여 사

용자 행위를 식별하고, 상기 식별된 사용자 행위를 상기 사용자 행위 메타데이터에 저장하는 단계;

상기 애플리케이션 개발환경 유형은 아키텍쳐 유형을 포함하되, 상기 아키텍쳐 유형은 GUI 데이터 유형, json 데이터 유형 및 WEBGUI 데이터 유형 중 적어도 하나인 것을 특징으로 하는, 데이터 관리 방법을 컴퓨터에 실행시키기 위한 컴퓨터 프로그램이 저장된 컴퓨터가 판독 가능한 기록 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 데이터 관리 장치, 데이터 관리 방법 및 데이터 관리 프로그램을 저장하는 컴퓨터로 판독 가능한 저장 매체에 관한 것이다.

배 경 기 술

[0003] 기술의 발전으로 인해 데이터의 양과 다양성이 증가함에 따라 데이터 관리의 중요성이 더욱 부각되고 있다. 데이터 관리는 기업이나 조직이 데이터를 효과적으로 수집, 저장, 분석, 활용하는 것을 의미한다.

[0004] 기업의 핵심 기능을 통합적으로 관리하는 Enterprise Resource Planning (ERP) 시스템은 기업 내의 중요한 데이터를 효율적으로 관리하는 도구로 널리 사용된다. 예산 관리, 생산 관리, 재고 관리, 구매 관리 등과 같은 기업의 주요 기능들을 통합하여 한 시스템에서 효과적으로 운영할 수 있다. 이때, 대표적인 ERP 시스템으로 SAP 제품을 예로 들 수 있다.

[0005] 다만, 기존의 시스템에서는 서버와의 통신에서 발생하는 패킷을 일반적인 분석 방법으로는 직접적인 의미를 이해하기 어려울 수 있다. 특히, SAP 시스템과 같이 복잡한 데이터 구조와 특정 프로토콜을 사용하여 데이터를 교환하는 경우에는 패킷으로부터 의미 있는 값을 추출하거나 해석하는 것이 더욱 어렵기 때문에 패킷을 분석하는 방법에 대한 구체적인 방안이 필요하다.

[0006] 또한, 수집되어 분석된 데이터에 개인정보가 포함된 경우, 개인정보를 추출하여 별도로 보관해야 한다. 다만, 개인정보를 추출하는 방법은 다양한 방법이 있는데, 패턴의 정확성 등에 따라 추출 결과가 달라질 수 있으며, 잘못된 패턴 설정으로 인해 부정확한 개인정보 추출이 발생할 수 있는 우려가 있다.

[0007] 또한, 수집되어 분석된 로그 데이터는 데이터베이스 등에서 관리될 수 있으며, 이때 관리되는 로그 데이터들은 구체적으로 사용자의 어떤 업무 행위에 관한 것인지에 대한 구분이 없다.

발명의 내용

해결하려는 과제

[0009] 따라서, 본 발명은 기존 기술의 문제점을 해결하기 위한 사용자 행위를 매핑하여 데이터를 관리하는 데이터 관리 장치, 데이터 관리 방법 및 데이터 관리 프로그램을 저장하는 컴퓨터로 판독 가능한 저장 매체를 제공하고자 한다.

과제의 해결 수단

[0011] 본 발명의 일 실시 예는 데이터를 수집하는 단계; 상기 수집된 데이터를 분류하는 단계; 및 상기 데이터에 포함된 적어도 하나의 정보를 매핑하여 사용자 행위 메타데이터를 생성하는 단계를 포함하는, 데이터 관리 방법을 제공한다.

[0012] 상기 데이터 관리 방법은 애플리케이션 개발환경에서 사용자 행위를 나타내는 키 및 텍스트를 수집하는 단계; AI 엔진을 통하여 상기 수집된 텍스트를 분류하는 단계; 및 상기 애플리케이션 개발환경, 상기 사용자 행위를 나타내는 키 및 상기 분류된 텍스트를 매핑하여 상기 사용자 행위 메타데이터에 저장하는 단계를 포함하는 것을 특징으로 한다.

[0013] 상기 데이터 관리 방법은 상기 사용자 행위 메타데이터와 저장된 로그 데이터를 매핑하기 위하여 상기 로그 데이터를 인덱스 처리하되, 상기 인덱스에 상기 사용자 행위 메타데이터에 포함된 상기 분류된 텍스트를 추가하는 단계를 더 포함하는 것을 특징으로 한다.

[0014] 상기 데이터 관리 방법은 상기 로그 데이터에 대한 조회를 요청받는 단계; 및 상기 인덱스에 포함된 상기 분류된 텍스트를 제공하는 단계를 더 포함하는 것을 특징으로 한다.

[0015] 본 발명의 일 실시 예는 데이터를 저장하는 데이터베이스; 및 상기 데이터를 처리하는 프로세서를 포함하고, 상기 프로세서는, 데이터를 수집하는 단계; 상기 수집된 데이터를 분류하는 단계; 및 상기 데이터에 포함된 적어도 하나의 정보를 매핑하여 사용자 행위 메타데이터를 생성하는, 데이터 관리 장치를 제공한다.

[0016] 상기 프로세서는, 애플리케이션 개발환경에서 사용자 행위를 나타내는 키 및 텍스트를 수집하고, AI 엔진을 통하여 상기 수집된 텍스트를 분류하고, 상기 애플리케이션 개발환경, 상기 사용자 행위를 나타내는 키 및 상기 분류된 텍스트를 매핑하여 상기 사용자 행위 메타데이터에 저장하는 것을 특징으로 한다.

[0017] 상기 프로세서는 상기 사용자 행위 메타데이터와 저장된 로그 데이터를 매핑하기 위하여 상기 로그 데이터를 인덱스 처리하되, 상기 인덱스에 상기 사용자 행위 메타데이터에 포함된 상기 분류된 텍스트를 추가하는 것을 특징으로 한다.

[0018] 상기 프로세서는 상기 로그 데이터에 대한 조회를 요청받는 경우, 상기 인덱스에 포함된 상기 분류된 텍스트를 제공하는 것을 특징으로 한다.

[0019] 본 발명의 일 실시 예는 애플리케이션 개발환경에서 사용자 행위를 나타내는 키 및 텍스트를 수집하고, AI 엔진을 통하여 상기 수집된 텍스트를 분류하고, 상기 애플리케이션 개발환경, 상기 사용자 행위를 나타내는 키 및 상기 분류된 텍스트를 매핑하여 사용자 행위 메타데이터에 저장하는 단계를 수행하는 데이터 관리 프로그램을 저장하는 컴퓨터로 판독 가능한 저장 매체를 제공한다.

발명의 효과

[0021] 본 발명의 일 실시 예에 따르면, ERP 시스템에서의 데이터 관리를 위한 혁신적인 기술을 제공함으로써 기업의 데이터 보안과 모니터링에 대한 요구를 충족시킬 수 있다.

[0022] 또한, 본 발명의 일 실시 예에 따르면, 서버에 대한 모든 접속 기록을 로그로 생성하여 로그 기록에 대한 안정성을 확보할 수 있다는 장점이 있다.

[0023] 또한, 본 발명의 일 실시 예에 따르면, 디피-헬만 알고리즘을 사용하는 경우에도 SSL 암호를 해제하고 로그를 기록하며 안전한 방식으로 업무 시스템으로 전송함으로써 데이터의 무결성과 기밀성을 보장할 수 있다는 장점이 있다.

[0024] 또한, 본 발명의 일 실시 예에 따르면, 개인정보 메타데이터 및 예외처리 리스트를 사용한 다차원 추출 방법을 통해 개인정보 추출에 대한 정확도를 높일 수 있다는 장점이 있다.

[0025] 또한, 본 발명의 일 실시 예에 따르면, 개인정보가 포함된 모든 로그 데이터에 대해 사용자 행위를 매핑할 수 있다는 장점이 있다.

도면의 간단한 설명

[0027] 도 1은 본 발명의 데이터 관리 장치를 설명하기 위한 하드웨어를 개시하는 도면이다.

도 2는 본 발명의 데이터 관리 장치의 일 실시 예를 개시하는 도면이다.

도 3은 본 발명의 데이터 관리 플랫폼의 일 실시 예를 개시하는 도면이다.

도 4는 본 발명의 데이터 관리 방법의 일 실시 예를 설명하는 플로우 차트이다.

도 5는 본 발명의 데이터 관리 방법의 일 실시 예를 개시하는 도면이다.

도 6은 본 발명의 패킷 수집 방법의 일 실시 예를 개시하는 도면이다.

도 7은 본 발명의 패킷 수집 방법의 다른 일 실시 예를 개시하는 도면이다.

도 8은 본 발명의 패킷 수집 방법에 따라 수집한 RFC 프로토콜 기반의 패킷 분석 데이터의 일 실시 예를 개시하는 도면이다.

도 9는 본 발명의 패킷 수집 방법에 따라 수집한 GUI 프로토콜 기반의 패킷 분석 장치의 일 실시 예를 개시하는 도면이다.

도 10은 본 발명의 패킷 수집 방법에 따라 수집한 GUI 프로토콜 기반의 패킷 분석 방법의 일 실시 예를 개시하는 도면이다.

도 11은 본 발명의 패킷 수집 방법에 따라 수집한 GUI 프로토콜 기반의 패킷 분석 데이터의 일 실시 예를 개시하는 도면이다.

도 12는 본 발명의 패킷 수집 방법에 따라 수집한 HTTP/HTTPS 기반의 패킷 분석 방법의 일 실시 예를 개시하는 도면이다.

도 13은 본 발명의 패킷 수집 방법에 따라 수집한 HTTP/HTTPS 기반의 패킷의 분석 데이터의 일 실시 예를 개시하는 도면이다.

도 14는 본 발명의 분석된 패킷에 포함된 데이터 중 개인정보를 추출하는 일 실시 예를 개시하는 도면이다.

도 15는 본 발명의 분석된 패킷에 포함된 데이터를 시각화한 일 실시 예를 개시하는 도면이다.

도 16은 본 발명의 분석된 패킷에 포함된 데이터를 검색하는 일 실시 예를 개시하는 도면이다.

도 17은 본 발명의 데이터 관리 방법에 따라 수집된 데이터를 모니터링하는 일 실시 예를 개시하는 도면이다.

도 18은 본 발명의 데이터 관리 플랫폼이 수집된 패킷을 분배하는 실시 예를 설명하는 도면이다.

도 19는 본 발명의 데이터 관리 플랫폼이 RFC 프로토콜 기반의 패킷을 분석하는 실시 예를 설명하는 도면이다.

도 20은 본 발명의 데이터 관리 플랫폼이 패킷을 분석하는 실시 예를 설명하는 도면이다.

도 21은 본 발명의 데이터 관리 플랫폼이 감사 로그를 저장하고 모니터링하는 실시 예를 설명하는 도면이다.

도 22는 본 발명의 데이터 관리 방법이 수집된 패킷을 분배하는 실시 예를 설명하는 도면이다.

도 23은 본 발명의 데이터 관리 플랫폼이 HTTPS 기반 패킷을 분석하는 실시 예를 설명하는 도면이다.

도 24는 본 발명의 데이터 관리 방법이 HTTPS 기반 패킷을 분석하는 실시 예를 설명하는 도면이다.

도 25는 본 발명의 데이터 관리 방법의 일 실시 예를 설명하는 도면이다.

도 26은 본 발명의 데이터 관리 플랫폼에서 개인정보를 추출하고 저장하는 실시 예를 설명하는 도면이다.

도 27은 본 발명의 데이터 관리 플랫폼에서 사용되는 정규식 패턴의 일 예를 설명하는 도면이다.

도 28은 본 발명의 데이터 관리 플랫폼에서 사용되는 마스킹 패턴의 일 예를 설명하는 도면이다.

도 29는 본 발명의 데이터 관리 플랫폼에서 정의하는 개인정보 메타데이터(1036)의 일 예를 설명하는 도면이다.

도 30은 본 발명의 데이터 관리 플랫폼에서 아키텍처 유형을 구분하여 개인정보를 추출하는 실시 예를 설명하는 도면이다.

도 31은 본 발명의 데이터 관리 플랫폼에서 개인정보 추출 규칙을 생성하는 실시 예를 설명하는 도면이다.

도 32는 본 발명의 데이터 관리 플랫폼에서 개인정보 예외처리 리스트를 생성하는 실시 예를 설명하는 도면이다.

도 33은 본 발명의 데이터 관리 플랫폼의 예외 필터를 생성하는 실시 예를 설명하는 도면이다.

도 34는 본 발명의 데이터 관리 플랫폼에서 추출된 개인정보를 검색하고 출력하는 실시 예를 설명하는 도면이다.

도 35는 본 발명의 데이터 관리 방법이 개인정보를 관리하는 실시 예를 설명하는 도면이다.

도 36은 본 발명의 데이터 관리 방법이 개인정보를 추출하고 저장하는 다른 실시 예를 설명하는 도면이다.

도 37은 본 발명의 데이터 관리 방법에서 개인정보를 관리하는 실시 예를 설명하는 도면이다.

도 38은 본 발명의 데이터 관리 플랫폼에서 사용자 행위를 수집하고 매핑하는 실시 예를 설명하는 도면이다.

도 39는 본 발명의 데이터 관리 플랫폼에서 사용자 행위 메타데이터를 생성하는 실시 예를 설명하는 도면이다.

도 40은 본 발명의 데이터 관리 플랫폼에서 사용자 행위 메타데이터와 로그 데이터를 매핑하는 실시 예를 설명

하는 도면이다.

도 41은 본 발명의 데이터 관리 방법이 사용자 행위 메타데이터를 생성하는 실시 예를 설명하는 도면이다.

도 42는 본 발명의 데이터 관리 방법이 사용자 행위 메타데이터와 로그 데이터를 매핑하는 실시 예를 설명하는 도면이다.

도 43은 본 발명의 데이터 관리 방법이 사용자 행위 메타데이터를 생성하는 실시 예를 설명하는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0028] 이하에서는 도면을 참조하여 다양한 실시예들을 상세히 설명한다. 이하에서 설명되는 실시예들은 여러 가지 상이한 형태로 변형되어 실시될 수도 있다. 실시예들의 특징을 보다 명확히 설명하기 위하여 이하의 실시예들이 속하는 기술분야에서 통상의 지식을 가진 자에게 널리 알려져 있는 사항들에 관해서 자세한 설명은 생략한다.

[0029] 한편, 본 명세서에서 어떤 구성이 다른 구성과 "연결"되어 있다고 할 때, 이는 '직접적으로 연결'되어 있는 경우 뿐 아니라, '그 중간에 다른 구성을 사이에 두고 연결'되어 있는 경우도 포함한다. 또한, 어떤 구성이 다른 구성을 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한, 그 외 다른 구성을 제외하는 것이 아니라 다른 구성들 더 포함할 수도 있다는 것을 의미한다.

[0030] 또한, 본 명세서에서 사용되는 “제 1” 또는 “제 2” 등과 같이 서수를 포함하는 용어는 다양한 구성 요소들을 설 명하는데 사용할 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만 사용된다.

[0031] 또한, 각각의 모듈이 포함하는 기능부(function unit)들은 모듈이 수행하는 기능을 설명하기 위한 논리적 구조이기 때문에, 각각의 기능부가 수행하는 기능은 모듈이 수행할 수 있음은 물론이다. 즉, 각각의 모듈은 모듈 내에 포함된 모든 기능부들을 포함할 필요가 없고, 기능을 수행하기 위한 적어도 하나의 기능부를 포함할 수 있다.

[0032] 이하에서는 첨부한 도면을 참조하여 실시 예를 예시하여 상세히 기술하도록 한다. 실시 예에서 프레임워크, 모듈, 응용 프로그램 인터페이스 등은 물리 장치 결합된 장치로 구현할 수도 있고 소프트웨어로 구현할 수도 있다. 이때, 실시 예가 소프트웨어로 구현될 경우 저장매체에 저장되고 컴퓨터 등에 설치되어 프로세서에 의해 실행될 수 있다.

[0034] 도 1은 본 발명의 데이터 관리 장치를 설명하기 위한 하드웨어를 개시하는 도면이다.

[0035] 본 도면은 후술하는 데이터 관리 플랫폼과 관련된 하드웨어 구성 요소 간의 데이터 송수신에 대한 실시 예를 설명한다.

[0036] 본 발명은 플랫폼을 통하여 사용자에게 제공될 수 있다. 이를 위하여 사용자/클라이언트(1000)는 웹 브라우저 등을 통하여 네트워크 장치(1001)에 접속하여 컴퓨팅 서버(1004)의 제어 하에 별도의 스토리지/데이터베이스(1003)에 저장된 데이터와 애플리케이션을 이용할 수 있게 된다.

[0037] 보다 상세하게는, 사용자/클라이언트(1000)는 클라이언트 단말기를 통하여 서비스(예를 들어, 데이터의 검색, 수정, 삭제 등의 작업)를 요청하고, 컴퓨팅 서버(1004)를 통하여 연산되고 네트워크 장치(1001)를 통하여 수신한 데이터를 화면에 출력할 수 있다. 일 실시 예에서, 사용자/클라이언트(1000)는 본 발명의 데이터 관리 플랫폼에 접근하는 모든 대상을 포함할 수 있다. 즉, 본 도면에서 사용자/클라이언트(1000)는 네트워크 장치(1001)를 이용하여 데이터 관리 플랫폼에 접근할 수 있으며, 네트워크 장치(1001)의 제한을 두지 않는다.

[0038] 네트워크 장치(1001)는 사용자/클라이언트(1000)와 컴퓨팅 서버(1004) 사이에서 데이터 전송을 중개하는 역할을 한다. 여기에서, 네트워크 장치(1001)는 라우터, TAP, 스위치 등을 포함할 수 있다. 라우터는 IP 주소를 이용하여 데이터를 전송하고, 스위치는 MAC 주소를 이용하여 데이터를 전송한다. 여기에서, 라우터와 같은 네트워크 장비(1001)는 SPAN(Switched Port Analyzer) 모드를 이용하여 특정 포트(port)만을 미러링하여 패킷을 데이터 관리 플랫폼(10000)에 전달할 수 있다. 이하에서 자세히 설명하도록 한다.

[0039] TAP(Test Access Point)은 네트워크 상에서 데이터를 수집하는 용도로 사용될 수 있다. 보다 상세하게는, TAP은 네트워크 장치(1001) 중 하나로, 네트워크의 백-본(back-bone) 라인에 추가되어 미러링만 전문적으로 해주는 장치에 대응한다. 즉, Network TAP(Test Access Point, 이하, TAP)을 통해 본 발명의 데이터 관리 플랫폼(10000)에 패킷을 전달할 수 있다. 이에 따라, 네트워크 상에서 송수신되는 데이터 패킷의 흐름에 영향을 주지 않고

패킷을 복사하여 데이터 관리 플랫폼에 전달할 수 있다.

[0040] 스토리지/데이터베이스(1003)는 데이터를 저장하고, 관리할 수 있다. 스토리지는 주로 하드 디스크나 SSD를 이용하여 데이터를 저장하고, 데이터베이스는 구조화된 데이터를 관리하며, 검색 및 수정 등의 작업을 수행할 수 있다.

[0041] 컴퓨팅 서버(1004)는 데이터 처리를 담당한다. 클라이언트(1000)로부터 요청된 작업을 처리하고, 처리 결과를 클라이언트(10000)에게 반환한다. 이를 위해 중앙연산장치(Central Processing Unit, CPU), RAM 등의 하드웨어를 이용하여 계산 작업을 수행할 수 있다. 그리고 컴퓨팅 서버(1004)는 여러 가지 데이터의 입출력을 제어하고 데이터 관리 플랫폼(10000)에서 처리된 데이터를 스토리지/데이터베이스(1003)에 저장할 수 있다. 이때, 본 발명의 데이터 관리 플랫폼(10000)이 수행하는 기능은 컴퓨팅 서버(1004)의 프로세서에 의해 수행될 수 있다. 또한, 컴퓨팅 서버(1004)는 하드웨어 구성 요소 또는 데이터 관리 플랫폼 내의 모듈들의 상태를 모니터링하고 제어하는 시스템 매니저를 포함할 수 있다.

[0042] 이하, 본 발명을 실시하기 위하여 본 도면의 하드웨어 구성요소가 사용될 수 있으며, 상기 하드웨어 구성 요소 간의 데이터 처리(processing) 방법이 포함됨은 물론이다.

[0044] 도 2는 본 발명의 데이터 관리 장치의 일 실시 예를 개시하는 도면이다.

[0045] 이 도면의 실시 예는 데이터 관리 장치를 예시하고 있으며, 데이터 관리 장치를 설명하기 위한 physical) 장치와 논리적인 요소(logical component)를 포함하고 있다.

[0046] 본 발명은 일 실시 예에서 SaaS(Software as a Service) 플랫폼을 통해 사용자에게 제공될 수 있다. SaaS 플랫폼은 클라우드 컴퓨팅 기술을 이용하여 네트워크를 통해 사용자에게 서비스로 제공되는 소프트웨어를 뜻한다. 이를 위하여, 스토리지/데이터베이스(1003), 컴퓨팅 서버(1004) 및 컨테이너 플랫폼(1005)은 사용자/클라이언트(1000)가 데이터 관리 플랫폼(10000) 및 데이터 관리 소프트웨어 패키지(20000)를 클라우드 상에서 이용할 수 있도록 지원할 수 있다.

[0047] 본 발명은 데이터 처리를 위하여 사용자/클라이언트(1000), 스토리지/데이터베이스(1003), 애플리케이션 서버(1002), 컴퓨팅 서버(1004), 컨테이너 플랫폼(1005), 데이터 관리 플랫폼(10000) 및 데이터 관리 소프트웨어 패키지(20000)를 사용할 수 있다.

[0048] 이때, 스토리지/데이터베이스(1003) 및 컴퓨팅 서버(1004)는 하드웨어일 수 있으며, 애플리케이션 서버(1002), 컨테이너 플랫폼(1005), 데이터 관리 플랫폼(10000) 및 데이터 관리 소프트웨어 패키지(20000)는 소프트웨어에 대응할 수 있다. 하드웨어에 대하여는 상술한 내용을 참고하도록 하고, 이 도면을 참조하여 데이터 관리 장치의 실시 예를 설명하면 다음과 같다.

[0049] 사용자/클라이언트(1000)는 데이터 처리를 위해 데이터 관리 소프트웨어(20000)에 접속할 수 있다.

[0050] 컨테이너 플랫폼(1005)은 OS(Operating System), 컨테이너(container), 도커(docker) 등으로 구성되어 데이터 처리를 위한 가상 환경을 제공할 수 있다.

[0051] 데이터 관리 플랫폼(10000)은 데이터 관리 소프트웨어 패키지(20000) 내에 포함된 적어도 하나의 엔진 또는 모듈을 제어할 수 있다. 이를 위하여, 데이터 관리 플랫폼(10000)은 내부 데이터베이스(여기에서, 데이터베이스는 데이터 관리 소프트웨어 패키지(20000) 내의 내부 데이터베이스를 의미한다.), 스토리지, 분산 파일 시스템 등의 기술을 사용하여 데이터를 관리할 수 있다. 또한, 데이터 관리 플랫폼(10000)은 데이터 관리 소프트웨어 패키지(20000) 내에 포함된 적어도 하나의 엔진 또는 모듈을 관리하기 위한 시스템 매니저 또는 관리콘솔을 포함할 수 있다.

[0052] 데이터 관리 소프트웨어 패키지(20000)는 수집 모듈(20001), 분석 모듈(20002), 키 관리 모듈(20003), 개인정보 관리 모듈(20004), 모니터링 모듈(20005) 및 AI 엔진(20006) 중 적어도 하나를 포함할 수 있다. 다만, 데이터 관리 소프트웨어 패키지(20000)에 포함된 모듈 및 엔진은 필수적인 구성요소가 아니며 본 발명을 설명하기 위한 요소에 해당한다. 따라서, 데이터 실시 예를 수행하기 위한 다른 이름의 모듈이 포함될 수 있음은 물론이다.

[0053] 수집 모듈(20001)은 다양한 소스에서 데이터를 수집하고 데이터를 처리 파이프 라인으로 전송할 수 있다. 수집 모듈(20001)은 로그, 이벤트, 센서, 웹 서버 등 다양한 소스에서 데이터(예를 들어, 패킷)를 수집할 수 있다. 특히, 수집 모듈(20001)은 로그 수집을 위해 에이전트를 사용할 때 에이전트를 중앙 관리할 수 있다.

[0054] 분석 모듈(20002)은 데이터를 분석하고 가치 있는 인사이트를 도출하는 데 사용될 수 있다. 분석 모듈(20002)은

수집된 패킷을 분석하여 데이터를 추출할 수 있다. 이때, 포함된 데이터가 개인정보인 경우, 개인정보 관리 모듈(20004)을 통하여 개인정보 보호와 관련된 기능을 제공할 수 있다. 또한, 포함된 데이터를 미리 수집된 행위 정보(예를 들어, 조회, 삭제, 추가, 변경, 출력 등을 포함한다.)와 매핑할 수 있다.

[0055] 키 관리 모듈(20003)은 데이터 암호화 및 복호화를 위한 키를 생성, 저장 및 관리할 수 있다. 키 관리 모듈(20003)은 토큰, 대칭 키, 공개 키, 디지털 인증서 등의 기술을 사용하여 키를 관리할 수 있다. 키 관리 모듈(20003)은 데이터에 개인정보가 포함되어 있는 경우, 개인정보를 암호화 및 복호화를 위한 키를 생성, 저장 및 관리할 수 있다. 또한, 키 관리 모듈(20003)은 데이터에 개인정보가 포함되어 있지 않더라도 데이터의 보안을 위하여 토큰, 대칭 키, 공개 키, 디지털 인증서 등의 기술을 사용할 수 있다.

[0056] 개인정보 관리 모듈(20004)은 개인정보 보호와 관련된 기능을 제공할 수 있다. 개인정보 관리 모듈(20004)은 데이터에 개인정보가 포함되어 있는 경우, 개인정보의 수집, 추출, 암호화, 저장, 처리, 검색, 삭제 등을 제어할 수 있다.

[0057] 모니터링 모듈(20005)은 데이터의 검색 및 탐지를 수행할 수 있다. 모니터링 모듈(20005)은 데이터 처리 및 데이터 처리 환경을 모니터링하고 문제를 식별할 수 있다. 또한, 모니터링 모듈(20005)은 로그, 성능 지표, 이벤트 등을 모니터링하고 경고를 생성할 수 있다.

[0058] AI 엔진(20006)은 인공지능 기술(기계 학습을 포함한다.)을 이용하여 데이터 처리 및 데이터 분석 작업을 수행할 수 있다. 특히, 수집되어 저장된 로그에 텍스트가 포함되어 있는 경우, AI 엔진(20006)은 수집된 텍스트를 인공지능을 기반으로 행위를 분류할 수 있다.

[0060] 도 3은 본 발명의 데이터 관리 플랫폼의 일 실시 예를 개시하는 도면이다.

[0061] 이 도면의 실시 예는 데이터 관리 플랫폼(10000)을 예시하고 있으며, 물리적인(physical) 장치와 논리적인 요소(logical component)를 포함하고 있다. 특히, 본 도면에서 데이터 관리 플랫폼(10000)은 상술한 데이터 관리 플랫폼보다 더 넓은 범위에 대응할 수 있다. 예를 들어, 데이터 관리 플랫폼(10000)은 상술한 데이터 관리 소프트웨어 패키지(20000)에서 구현하는 모듈 중 적어도 하나를 포함하고, 물리 장치 상에서 구동되는 응용 프로그래밍 인터페이스 Application Programming Interface, API)를 포함할 수 있다. 물리 장치에 대하여는 상술한 내용을 참고하도록 한다.

[0062] 데이터 관리 플랫폼(10000)은 컴퓨팅 서버(1004)와 스토리지/데이터베이스(1003)의 리소스(resource)를 이용하여 데이터 관리 플랫폼(10000) 내에 포함된 모듈의 기능을 수행할 수 있다. 이때, 시스템 매니저는 데이터 관리 플랫폼(10000) 내의 모듈 또는 엔진 중 적어도 하나를 제어할 수 있으며, 시스템 매니저는 컴퓨팅 서버(1004) 내에 위치하거나 별도로 위치하여 데이터 관리 플랫폼(10000)을 제어할 수 있다.

[0063] 데이터 관리 플랫폼(10000)은 수집 모듈(20001), 분석 모듈(20002), 키 관리 모듈(20003), 개인정보 관리 모듈(20004), 모니터링 모듈(20005) 및 AI 엔진(20006) 중 적어도 하나를 포함할 수 있다. 각각의 모듈에 대한 설명은 상술한 바와 같다.

[0064] 데이터 관리 플랫폼(10000)은 사용자/클라이언트(1000)와 데이터를 송수신하며, 송수신된 데이터에 대하여 수집 모듈(20001), 분석 모듈(20002), 키 관리 모듈(20003), 개인정보 관리 모듈(20004), 모니터링 모듈(20005) 및 AI 엔진(20006)이 수행하는 적어도 하나의 기능을 적용할 수 있다. 이때, 데이터 관리 플랫폼(10000)은 사용자/클라이언트(1000)의 요청에 의해 데이터 관리 플랫폼(10000) 내에 포함된 개별적인 모듈을 단독으로 사용할 수 있다. 예를 들어, 사용자/클라이언트(1000)는 데이터 관리 플랫폼(10000) 내의 키 관리 모듈(20003) 또는 개인정보 관리 모듈(20004)의 기능만을 선택적으로 사용할 수 있다.

[0065] 또한, 도면에 도시되지는 않았으나 데이터 관리 플랫폼(10000)은 내부에 포함된 모듈의 기능을 수행하기 위하여 외부 스토리지/데이터베이스(1003)과는 다른 내부 데이터베이스를 사용할 수 있다.

[0067] 도 4는 본 발명의 데이터 관리 방법의 일 실시 예를 설명하는 플로우 차트이다.

[0068] 본 발명이 개시하는 데이터 관리 방법은 단계(S1000)에서, 패킷을 수집할 수 있다.

[0069] 일 실시 예에서, 패킷을 수집하는 방법은 에이전트(agent) 방식의 클라우드 기반의 패킷 수집 방법 또는 패킷 미러 방식의 패킷 수집 방법을 이용할 수 있다. 자세한 설명은 후술하도록 한다.

[0070] 일 실시 예에서, NIC(Network Interface Card)로부터 패킷을 수집할 수 있다. 여기에서, NIC는 네트워크 연결을 위해 사용되며, 유선 또는 무선 방식으로 네트워크와 연결될 수 있다. NIC는 컴퓨터와 네트워크 간에 데이터 전

송을 가능하게 하기 위해 패킷을 보내고 받는 역할을 하며, 네트워크 카드, LAN 카드, 이더넷 카드 등을 포함할 수 있다.

[0071] 또한, 본 발명이 개시하는 데이터 관리 방법은 수집된 패킷에 필터를 적용할 수 있다.

[0072] 보다 상세하게는, 본 발명의 데이터 관리 방법은 수집된 패킷을 재조합하고 필터링하여 분석 프로세스로 분배할 수 있다. 보다 상세하게는, 패킷의 재조합은 수집된 각각의 네트워크 패킷을 분석 가능한 패킷 형태로 합치는 것을 의미하며, 필터 적용은 기 설정된 필터링 규칙을 이용하여 해당 패킷을 분석할지 여부를 결정하는 설정을 의미한다. 이에 따라, 분석할 대상이 되는 패킷인 경우, 적절한 분석 프로세스로 분배될 수 있다.

[0073] 단계(S2000)에서, 패킷을 분석할 수 있다. 일 실시 예에서, 패킷의 기반이 되는 프로토콜의 종류에 따라 패킷을 분석할 수 있다. 보다 상세하게는, 패킷이 RFC(Remote Function Call) 프로토콜 기반인지, GUI/SNC 프로토콜 기반인지, HTTP/HTTPS 기반인지에 따라 패킷을 분석할 수 있다. 이때, 데이터 관리 방법은 이용 가능한 컴퓨팅 서버의 코어 수 및 트랜잭션 양을 고려하여 프로세스의 개수를 설정할 수 있다. 자세한 설명은 후술하도록 한다.

[0074] 단계(S3000)에서, 데이터를 모니터링할 수 있다. 일 실시 예에서, 분석된 패킷에 포함된 데이터를 모니터링할 수 있다. 또한, 저장된 데이터를 실시간 모니터링하여 이상행위 이벤트를 감지하고, 감지된 이벤트에 대한 경고를 발생시킬 지 여부를 결정할 수 있다.

[0075] 이를 위하여, 일 실시 예에서, 데이터 관리 방법은 분석된 패킷으로부터 데이터를 추출하고, 추출된 데이터를 저장할 수 있다. 데이터 관리 방법은 데이터에 포함된 정보에 따라 다른 방식으로 추출된 데이터를 저장할 수 있다. 예를 들어, 데이터에 개인정보가 저장되어 있는 경우, 개인정보를 추출한 뒤 개인정보를 암호화한 뒤 추출된 데이터를 저장할 수 있다. 또한, 데이터 관리 방법은 패킷 내의 중요 데이터만을 추출함으로써 중요 필드의 검색을 용이하게 하고, 결과적으로 데이터 관리 방법의 성능을 높일 수 있다.

[0077] 도 5는 본 발명의 데이터 관리 방법의 일 실시 예를 개시하는 도면이다.

[0078] 단계(S1010)에서, 패킷을 수집할 수 있다. 일 실시 예에서, 패킷을 수집하는 방법은 에이전트(agent) 방식의 클라우드 기반의 패킷 수집 방법 또는 패킷 미러 방식의 패킷 수집 방법을 이용할 수 있다. 자세한 설명은 후술하도록 한다.

[0079] 단계(S1020)에서, 수집된 패킷에 필터를 적용할 수 있다. 보다 상세하게는, 본 발명의 데이터 관리 방법은 수집된 패킷을 재조합하고 필터링하여 분석 프로세스로 분배할 수 있다.

[0080] 단계(S1030)에서, 필터가 적용된 패킷을 분석할 수 있다.

[0081] 여기에서, 패킷의 기반이 되는 프로토콜의 종류에 따라 다르게 분석할 수 있다. 보다 상세하게는, 단계(S1031)에서, RFC(Remote Function Call) 프로토콜 기반의 패킷을 분석하고, 단계(S1032)에서, GUI 프로토콜 기반의 패킷을 분석하고, 단계(S1033)에서, HTTP/HTTPS 기반의 패킷을 분석할 수 있다.

[0082] 단계(S1031)에서, RFC 프로토콜 기반의 패킷 분석은 네트워크에서 RFC 프로토콜을 사용하는 패킷을 분석하는 과정을 의미한다. RFC는 분산 환경에서 서로 다른 시스템 또는 컴퓨터 간에 함수 호출을 수행하기 위한 프로토콜과 메커니즘으로, RFC는 클라이언트와 서버 모델을 기반으로 작동하며 클라이언트가 원격 시스템에 있는 서버의 함수를 호출하여 원격에서 실행할 수 있도록 한다. 즉, RFC 프로토콜은 원격 함수 호출을 위한 통신 프로토콜이기 때문에 RFC 프로토콜을 사용하는 패킷은 이러한 원격 함수 호출에 대한 정보를 담고 있다.

[0083] 단계(S1032)에서, GUI 프로토콜 기반의 패킷 분석은 클라이언트와 애플리케이션 서버 간에 통신하는 GUI 프로토콜 기반의 패킷을 수집하여, 패킷에 포함된 클라이언트 IP또는 Port, 서버 IP 또는 Port, 패킷 데이터(byte stream) 등을 추출하는 방식이다.

[0084] 단계(S1033)에서, HTTP/HTTPS 기반의 패킷 분석은 웹 브라우저와 서버간 송수신하는 패킷을 미러링하거나 SSL 프로세싱하여 패킷에 포함된 데이터를 추출하는 방식이다.

[0085] 각각에 대한 자세한 분석 방법은 후술하도록 한다.

[0086] 단계(S1040)에서, 분석된 패킷으로부터 개인정보 메타데이터를 활용하여 개인정보를 추출할 수 있다. 일 실시 예에서, 분석된 패킷에 개인정보가 포함되어 있는지 확인하기 위하여, 저장된 개인정보 메타데이터를 사용하여 개인정보를 추출할 수 있다. 이에 대하여는, 후술하도록 한다.

[0087] 단계(S1050)에서, 로그를 저장할 수 있다. 이때, 분석된 패킷에 포함된 유의미한 정보는 로그로 저장될 수 있다. 일 실시 예에서, 데이터 관리 방법은 분석된 정보를 감사 로그(Audit log)에 저장할지 여부를 결정할 수 있다. 또한, 개인정보가 포함된 경우, 개인정보는 패턴화 되어 데이터베이스에 저장될 수 있다. 마지막으로, 데이터 관리 방법은 로그(log) 저장 속도를 높이기 위해 멀티 쓰레딩(multithreading) 방식으로 동작하며, 일시적으로 데이터베이스에 접근이 되지 않는 경우에 대비하여 메모리 큐잉(queuing) 및 파일 큐잉을 수행할 수 있다.

[0088] 단계(S1060)에서, 저장된 로그를 이용하여 이상행위를 감지할 수 있다. 이때, 이상행위가 감지된 경우, 이상행위 감지에 대한 정보를 기록한 새로운 로그를 생성하여 다시 단계(S1050)를 통해 로그를 저장할 수 있다. 또한, 데이터 관리 방법은 사용자로부터 감사 로그(Audit Log)를 요청받는 경우, 수집된 데이터의 화면을 재구현할 수 있다. 보다 상세하게는, GUI 프로토콜은 그래픽 사용자 인터페이스를 표시하고 상호 작용하는데 사용되는 프로토콜로, 이러한 프로토콜을 분석함으로써 사용자의 작업 흐름, 입력, 출력 등을 시각적으로 이해할 수 있으며 시스템의 동작 상태를 파악하고 문제를 진단하는데 도움을 줄 수 있다. 이에 대하여는 이하의 도면에서 자세히 설명하도록 한다.

[0090] 도 6은 본 발명의 패킷 수집 방법의 일 실시 예를 개시하는 도면이다.

[0091] 본 도면은 에이전트(agent) 방식의 클라우드 기반의 패킷 수집 방법에 대하여 설명한다. 보다 상세하게는, 일 실시 예는 적어도 하나 이상의 클라이언트(1000a, 1000b, 1000c), 네트워크(1001), 클라우드 AP(1010), 데이터 관리 플랫폼(10000, 20000)을 포함한다.

[0092] 적어도 하나의 클라이언트(1000a, 1000b, 1000c)는 수집 대상 패킷을 생성하는 기기로, 예를 들어, 서버, 노트북, 스마트폰 등을 포함할 수 있다.

[0093] 네트워크(1001)는 패킷 수집 대상 네트워크로, 클라이언트(1000a, 1000b, 1000c)는 네트워크(1001)에 연결되어 있을 수 있다.

[0094] 클라우드 AP(1010)는 적어도 하나의 AP(1011, 1012, 1013, 1014)를 포함할 수 있다. 여기에서, 적어도 하나의 AP(1011, 1012, 1013, 1014)는 패킷 수집 에이전트와 연결되고, 패킷 수집 에이전트는 AP(1011, 1012, 1013, 1014)에서 생성된 모든 패킷을 수집하고 처리할 수 있다.

[0095] 보다 상세하게는, 패킷 수집 에이전트는 수집된 패킷을 인식할 수 있는 형태로 필터링하고 추출하여 압축하고 암호화할 수 있다. 패킷 수집 에이전트는 AP(1011, 1012, 1013, 1014)와 연결되고, 수집된 패킷을 처리하고 데이터 관리 플랫폼(10000, 20000)으로 전송할 수 있다.

[0096] 데이터 관리 플랫폼(10000, 20000)은 수집된 패킷을 수신하고, 패킷을 분석하고 저장하며, 분석 모듈을 통해 데이터를 분석할 수 있다.

[0097] 이러한 방식으로 클라우드 지원(agent 방식) 기반의 패킷 수집 방법은 높은 확장성과 유연성을 제공하며, 다양한 네트워크 환경에서 적용할 수 있다. 또한, 클라우드 환경에서 데이터를 처리하므로 하드웨어나 소프트웨어 업그레이드나 유지보수가 용이하며, 안정적인 서비스를 제공할 수 있다.

[0098] 본 도면과 같은 에이전트 방식의 클라우드 기반의 패킷 수집 방법은 클라우드를 사용하는 경우 적용이 가능하다.

[0100] 도 7은 본 발명의 패킷 수집 방법의 다른 일 실시 예를 개시하는 도면이다.

[0101] 본 도면은 패킷 미러 방식의 패킷 수집 방법에 대하여 설명한다. 보다 상세하게는, 실시 예는, 일 실시 예는 적어도 하나 이상의 클라이언트(1000a, 1000b, 1000c), 네트워크(1001), 전용선/VPN(1001a), CSP(1015) 및 데이터 관리 플랫폼(10000, 20000)을 포함한다. 상술한 내용과 중복되는 설명은 생략하도록 한다.

[0102] 네트워크(1001)는 전용선/VPN(1001a)에 연결되며, 전용선/VPN(1001a)은 데이터 관리 플랫폼(10000, 20000)과 CSP(Cloud Service Provider, 클라우드 서비스 제공자, 1015) 각각에 연결될 수 있다. 여기에서, CSP는 예를 들어, AWS(Amason Web Service), GCP(Google Cloud Platform), Azure 와 같은 클라우드 서비스 제공자를 의미한다.

[0103] 패킷 미러 방식을 통하여 데이터 관리 플랫폼(10000, 20000)은 네트워크 트래픽을 복제하여 전용선/VPN(1001a)로부터 패킷을 전달받고, 동일한 패킷은 CSP(1015)에 전달될 수 있다.

[0104] 이 방법을 통하여 데이터 관리 플랫폼(10000, 20000)은 수집된 모든 패킷을 캡처하고 분석할 수 있다.

[0105] 본 도면과 같은 패킷 미러 방식의 패킷 수집 방법은 CSP, 자체 클라우드, 애플리케이션 서버에서 제공하는 프라이빗 클라우드(예를 들어, SAP PCE)를 사용하는 경우 적용이 가능하다.

[0107] 본 발명은 상술한 바와 같이 수집된 패킷을 분석할 수 있다. 구체적으로 수집된 패킷은 RFC 프로토콜 기반, GUI 프로토콜 기반, HTTP/HTTPS 기반 중 어느 하나에 해당할 수 있다. 이에 따라, 본 발명의 일 실시 예는 수집된 패킷을 다른 방식으로 분석하고, 저장할 수 있다. 이에 대하여 자세히 설명하도록 한다.

[0109] 도 8은 본 발명의 패킷 수집 방법에 따라 수집한 RFC 프로토콜 기반의 패킷 분석 데이터의 일 실시 예를 개시하는 도면이다.

[0110] 데이터 관리 플랫폼은 프로토콜을 기반으로 한 패킷을 통하여 본 도면에서 도시하는 다양한 데이터를 추출할 수 있다. 본 도면에서는, RFC 프로토콜 기반의 패킷 분석 데이터를 예로 들어 설명하나, RFC 프로토콜 기반의 패킷이 이하의 모든 정보를 포함하는 것은 아니다. 특히, 후술하는 (6) 및 (8)에 포함된 정보는 GUI 프로토콜 기반의 패킷 분석 데이터에 해당한다.

[0111] 보다 상세하게는, 데이터 관리 플랫폼은 RFC 구조 정보를 이용하여 패킷을 분석하고 데이터를 추출할 수 있다. 이때, RFC 구조 정보가 없는 경우, 데이터 관리 플랫폼은 RFC 정보 요청 파일을 생성하여, RFC 정보를 요청할 수 있다. 자세한 설명은 후술하도록 한다.

[0112] (1) 시간(요청 시간, 세션 정보의 시작 시간을 포함한다.)

[0113] (2) 프로토콜 정보(RFC 프로토콜, GUI 프로토콜, HTTP/HTTPS 등을 포함한다.)

[0114] (3) 서버 IP 또는 Port

[0115] (4) 클라이언트 IP 또는 Port(클라이언트가 접속한 지역(region)을 포함한다.)

[0116] (5) 계정(사용자 ID, 사번, 조직이름 등을 포함한다.)

[0117] (6) 트랜잭션명(트랜잭션 코드(T-code)를 포함한다. 여기서 트랜잭션 코드는 트랙잭션을 명시하는 일종의 단축 코드로써 논리적인 업무 프로세스이다.)

[0118] (7) RFC 함수 명

[0119] (8) 이벤트 정보(이벤트는 로그인(성공/실패), 개인정보 입력, 특정 T-Code 접근 여부, SAP ALL 접속 여부, 공통계정 접속 여부, 사용자 오류, 파일 다운로드, 프로그램 덤프, 사용자 암호 변경 여부, 메타 데이터 수정 여부, 중복접속 조회 여부, 특정 GL 계정(GUI 프로토콜의 경우, 계좌(account) 정보 누적 조회 여부 등을 포함한다.)

[0120] (9) 개인정보 개수

[0121] 일 실시 예에서, 데이터 관리 플랫폼은 트랜잭션명과 이벤트 정보를 통하여 패킷이 수행하고자 하는 업무를 판단할 수 있다.

[0123] 도 9는 본 발명의 패킷 수집 방법에 따라 수집한 GUI 프로토콜 기반의 패킷 분석 장치의 일 실시 예를 개시하는 도면이다.

[0124] 본 도면에서는, 본 발명의 패킷 수집 방법에 따라 수집한 패킷이 GUI 프로토콜 기반인 경우, 패킷을 분석하는 실시 예를 설명한다. 일 실시 예는, 사용자/클라이언트(1000, 이하, 클라이언트), 네트워크 장치(1001), 스토리지/데이터베이스(1003), 컴퓨팅 서버(1004), 애플리케이션 서버(1002)를 포함할 수 있다. 상술한 구성과 중복되는 설명은 생략하도록 한다.

[0125] 일 실시 예에서, 상술한 구성 요소를 이용하여 GUI 프로토콜을 기반으로 한 패킷 분석을 수행할 수 있다. 이를 위해서는 클라이언트(1000)에서 발생하는 GUI 프로토콜 기반의 트래픽을 캡처하고 분석하는 것이 필요하다. 이를 위해서는 다음과 같은 작업이 필요하다.

[0126] 클라이언트(1000)는 네트워크 장치(1001)를 이용해 애플리케이션 서버(1002)에 대응하는 애플리케이션을 실행하고, 애플리케이션 시스템에 로그인할 수 있다. 클라이언트(1000)는 애플리케이션을 통하여 필요한 작업을 수행할 수 있다. 클라이언트(1000)는 입력되는 입력 데이터 또는 애플리케이션 서버(1002)를 통하여 수신한 출력 데이터에 대한 정보를 화면에 출력할 수 있다.

[0127] 네트워크 장비(1001)는 클라이언트(1000)와 애플리케이션 서버(1002) 사이의 네트워크 트래픽을 캡처할 수

있다. 특히, 네트워크 장비(1001)는 TAP을 포함할 수 있다. 이를 통해, 예를 들어, 애플리케이션 서버(1002)가 SAP 운영 서버인 경우, SAP 애플리케이션 사용자, SAP EP 서버 및 레거시 시스템에서 SAP 서버와 통신하는 GUI 프로토콜 기반의 패킷을 로깅할 수 있다. 또한, 네트워크 장비(1001)는 스위치를 포함할 수 있다. 이를 통해, SAP 운영 서버로 네트워크를 주고받는 스위치에서 포트 미러를 통하여 SAP 서버에 대한 내부 감사를 수행할 수 있고, SAP 서버에서 사용되는 개인 정보에 대해 모니터링할 수 있다.

[0128] 애플리케이션 서버(1002)에서는 GUI 프로토콜을 기반으로 하는 트래픽이 발생할 수 있다.

[0129] 데이터 관리 플랫폼(10000) 또는 데이터 관리 소프트웨어(20000)는 애플리케이션 서버(1002)에서 발생하는 트래픽을 캡쳐하고, 캡쳐한 트래픽을 분석할 수 있다. 이때, 데이터 관리 플랫폼(10000) 또는 데이터 관리 소프트웨어(20000) 내의 수집 모듈(20001) 및 분석 모듈(20002)을 통해 애플리케이션 서버(1002)에서 발생하는 트래픽을 수집하고 분석할 수 있다. 이에 따라, GUI 프로토콜의 구조와 내용을 이해하고 분석할 수 있다. 이때, 애플리케이션 서버(1002)는 컴퓨팅 서버(1004)의 자원을 이용할 수 있다.

[0130] 스토리지/데이터베이스(1003)는 분석한 결과 또는 애플리케이션 서버(1002)에 필요한 정보를 저장할 수 있다.

[0132] 도 10은 본 발명의 패킷 수집 방법에 따라 수집한 GUI 프로토콜 기반의 패킷 분석 방법의 일 실시 예를 개시하는 도면이다.

[0133] 단계(S2010)에서, 클라이언트 화면에 출력되는 애플리케이션과 애플리케이션 서버 간 송수신되는 패킷을 수집할 수 있다. 보다 상세하게는, 클라이언트와 애플리케이션 서버 간에 통신하는 GUI 프로토콜 기반의 패킷을 분석하고 입출력 데이터 및 모니터링에 필요한 정보를 수집할 수 있다. 여기에서, 입력 데이터는 클라이언트가 클라이언트의 단말기(terminal)을 이용하여 입력하는 사용자 명령어를 포함할 수 있다.

[0134] 클라이언트가 클라이언트 단말기를 통해 사용자 명령어를 입력 데이터로써 입력하면, 입력 데이터는 네트워크를 통해 애플리케이션 서버에 전송된다. 일 실시 예에서, 애플리케이션 서버에 입력 데이터가 전송되는 경우, 입력 데이터는 모니터링 될 수 있다.

[0135] 보다 상세하게는, 데이터 관리 플랫폼은 입력 데이터를 제공받아 분석할 수 있다. 이때, 입력 패킷에 기 설정된 사용자 명령어(예를 들어, 특정 이벤트 발생)가 포함된 경우, 데이터 관리 플랫폼은 접근 제한이 필요하다고 판단할 수 있다. 이에 따라, 데이터 관리 플랫폼은 사용자 명령어(여기에서, 사용자 명령어는 입력 패킷에 포함된 사용자 명령어와 다른 언어로 표현될 수 있다.)를 통해 애플리케이션 서버(1002)에게 클라이언트의 접근을 통제할 수 있다. 이때, 입력 데이터는 SAP DIAG 프로토콜을 통해 SAP 애플리케이션 서버와 송수신되는 데이터를 예로 들 수 있다.

[0136] 또한, 클라이언트 단말기는 애플리케이션 서버에서 출력된 데이터를 출력할 수 있다. 즉, 애플리케이션 서버는 전송되는 입력 데이터에 대한 내용을 검색하면서 검색된 결과에 대한 내용이 포함된 출력 데이터를 클라이언트 단말기에 전송하여 클라이언트 단말기의 화면에 정보가 출력되도록 할 수 있다. 이때, 애플리케이션 서버는 출력 데이터를 출력하되, 출력 데이터는 서버 정보, 트랜잭션 코드(T-code), 프로그램명, 상태 메시지 중 적어도 하나를 포함할 수 있다.

[0137] 입력 데이터와 마찬가지로, 데이터 관리 플랫폼은 출력 데이터를 제공받아 분석할 수 있다. 이때, 출력 데이터는 서버 정보, 트랜잭션 코드(T-code), 프로그램명, 상태 메시지 중 적어도 하나를 포함할 수 있다. 입력 데이터와 마찬가지로, 데이터 관리 플랫폼은 분석된 출력 데이터에 기초하여 접근 제한이 필요하다고 판단할 수 있다. 이에 따라, 데이터 관리 플랫폼은 접근을 통제할 수 있다.

[0138] 또한, 출력 데이터는 SAP DIAG 프로토콜을 통해 SAP 애플리케이션 서버와 클라이언트 단말기와 송수신되는 데이터를 예로 들 수 있다.

[0139] 단계(S2020)에서, 수집된 패킷의 분석 여부를 결정할 수 있다. 이를 위하여, 본 발명은 수집된 정보의 분석 여부를 결정하여 성능을 높일 수 있도록 필터링을 수행할 수 있다. 여기에서, 수집된 정보를 분석하지 않기로 결정하는 경우 분석을 진행하지 않고 종료한다.

[0140] 단계(S2030)에서, 패킷을 분석할 수 있다. 일 실시 예에서, 패킷 내의 포함된 정보의 보안을 제어하기 위해 패킷 디코딩 및 프로토콜을 분석할 수 있다. 일 실시 예에서, 입력 데이터 또는 출력 데이터에 대한 클라이언트 IP또는 Port, 서버 IP 또는 Port, 패킷 데이터(byte stream) 등으로 자세하게 분석할 수 있다.

[0141] 단계(S2040)에서, 분석된 패킷에 포함된 데이터를 세션 정보로 구성하여 저장할 수 있다. GUI 프로토콜 기반의

패킷을 분석한 분석 정보와 입출력 데이터를 사용해 세션 정보를 생성하고, 저장할 수 있다. 일 실시 예에서, 저장된 세션 정보는 사용자가 이해하기 쉬운 언어로 클라이언트 화면에 출력될 수 있다.

[0142] 즉, 네트워크 연결 정보 및 입출력 패킷을 분석함으로써, 의미 있는 정보인 입출력 데이터를 용이하게 출력할 수 있어, 클라이언트는 애플리케이션 서버의 GUI 화면과 실질적으로 유사한 형태의 화면을 확인할 수 있다.

[0143] 이와 같이, 클라이언트는 GUI 화면과 실질적으로 유사한 형태로 용이하게 재구현할 수 있기 때문에 애플리케이션 서버 정보, 트랜잭션 코드(T-code), 프로그램명, 상태 메세지, 출력데이터 등을 화면을 통하여 모니터링하면서 용이하게 분석할 수 있다.

[0145] 도 11은 본 발명의 패킷 수집 방법에 따라 수집한 GUI 프로토콜 기반의 패킷 분석 데이터의 일 실시 예를 개시하는 도면이다.

[0146] 일 실시 예에서, GUI 프로토콜을 기반으로 한 패킷으로부터 시간, 프로토콜 정보, 서버/클라이언트 IP 또는 Port, 계정, 트랜잭션명, 이벤트 정보, 개인정보 개수 중 적어도 하나에 대한 데이터를 추출할 수 있다. 각각의 정의에 대한 내용은 상술한 바와 같다.

[0147] 일 실시 예에서, GUI 프로토콜 기반의 패킷의 분석 결과를 본 도면과 같이 “화면 재현”의 형태로 클라이언트에게 제공할 수 있다.

[0148] 보다 상세하게는, 본 발명의 데이터 관리 플랫폼은 클라이언트에게 분석된 패킷에 포함된 데이터를 사용자가 알기 쉬운 방법으로 출력할 수 있다.

[0149] 본 도면을 통하여 예를 들어, 설명하면, 제 1 사용자가 애플리케이션 서버에 접속하여 “1175”을 입력한 경우, 데이터 관리 플랫폼이 “Request Screen”을 통하여 제 1 사용자가 애플리케이션 서버에 접속하여 입력한 화면을 재현한 실시 예를 나타낸다.

[0150] 또한, 제 1 사용자가 애플리케이션 서버에 접속하여 “1175”를 입력한 이후, 애플리케이션 서버로부터 수신하여 출력한 경우, 데이터 관리 플랫폼은 “Response Screen”을 통하여 제 1 사용자가 애플리케이션 서버로부터 수신한 출력 화면을 재현할 수 있다.

[0151] 이를 통하여, 제 2 사용자(예를 들면, 제 1 사용자의 관리자)는 데이터 관리 플랫폼을 이용하여 제 1 사용자가 입력한 데이터를 포함하는 화면과 출력된 데이터를 포함하는 화면을 각각 “Request Screen” 및 “Response Screen”을 통하여 확인할 수 있다.

[0153] 도 12는 본 발명의 패킷 수집 방법에 따라 수집한 HTTP/HTTPS 기반의 패킷 분석 방법의 일 실시 예를 개시하는 도면이다.

[0154] HTTP(Hypertext Transfer Protocol)는 인터넷에서 데이터를 주고받기 위한 프로토콜 중 하나로, HTTP는 기본적으로 평문(Plain Text)을 이용하여 통신하기 때문에, HTTP 패킷을 수집할 수 있다면 누구나 패킷에 포함된 내용을 확인할 수 있다. 즉, HTTP 기반의 패킷은 보안에 취약하기 때문에 이러한 보안 취약점을 보완하기 위해, HTTPS(HTTP Secure) 기반으로 패킷을 송수신하는 경우가 있다.

[0155] HTTPS는 HTTP의 보안 버전으로, SSL(Secure Sockets Layer)이나 TLS(Transport Layer Security) 프로토콜을 이용하여 통신할 수 있다. SSL 프로토콜은 데이터를 암호화하여 전송하기 때문에, 임의의 대상이 패킷을 수집하더라도 SSL 암호를 해제하지 않으면 패킷을 분석할 수 없다.

[0156] 따라서, 본 발명은 HTTPS 기반의 패킷을 분석하기 위해 SSL 프로세싱을 수행할 수 있다. 여기에서, SSL 프로세싱은 HTTPS 통신에서 데이터를 암호화하고 복호화하는 과정을 포함할 수 있다. SSL 프로세싱은 클라이언트와 서버 간의 암호화 키 교환, 인증, 데이터 암호화, 복호화 등을 수행할 수 있다.

[0157] 보다 상세하게, 본 발명의 패킷 수집 방법 중 HTTP/HTTPS 기반의 패킷을 분석하는 방법을 설명하면 다음과 같다.

[0158] 사용자가 웹 브라우저(web browser, 1030)를 실행하면, 웹 브라우저(1030)는 HTTP/HTTPS를 통해 웹 서버에 요청을 보낼 수 있고, 웹 서버에서 응답을 받아와 사용자에게 데이터를 출력할 수 있다.

[0159] 프록시 서버(proxy server)는 클라이언트와 웹 서버(예를 들어, SAP 서버) 사이에서 중계 기능을 수행할 수 있다. 웹 브라우저(1030)에서 웹 서버에 접속할 때, 프록시 서버를 거쳐서 요청과 응답을 주고받을 수 있다. 이를 통해, 사용자의 IP 주소를 숨기거나, 캐싱을 통해 네트워크 성능을 향상시키는 등의 기능을 수행할 수 있다.

[0160] SSL 프로세싱은 HTTPS 연결에서 SSL 인증서를 확인하고, 키 교환 및 암호화/복호화를 수행할 수 있다.

[0161] 데이터 관리 플랫폼은 HTTP/HTTPS 패킷 추출 및 분석을 수행할 수 있다. 이를 위하여, 데이터 관리 플랫폼에 포함된 수집 모듈 및 분석 모듈을 이용할 수 있다. 수집된 패킷이 HTTP 기반의 패킷인 경우, 바로 분석을 수행하고, HTTPS 기반의 패킷인 경우, SSL 프로세싱을 거친 후 분석을 수행할 수 있다. SSL 프로세싱을 통해 복호화된 HTTPS 패킷은 웹 브라우저나 프록시 서버에서 추출되어 분석될 수 있다.

[0162] 데이터 관리 플랫폼은 HTTP 패킷 또는 SSL 프로세싱을 통하여 발생하는 패킷들을 큐(1032, queue)에 저장할 수 있고, 큐(1032)에서 패킷을 추출하여 분석할 수 있다. 여기에서, 큐(1032)의 크기는 SSL 프로세싱의 대역폭과 처리 능력에 따라 결정될 수 있다. 또한, 큐(1032)는 메모리 큐 및 파일 큐를 포함할 수 있다.

[0163] 이에 따라, 본 발명은 HTTP/HTTPS 기반의 패킷을 분석할 수 있으며, HTTPS 기반의 패킷을 분석하기 위하여 SSL 프로세싱을 수행하는 방법에 대하여는 이하에서 자세히 설명하도록 한다.

[0165] 도 13은 본 발명의 패킷 수집 방법에 따라 수집한 HTTP/HTTPS 기반의 패킷의 분석 데이터의 일 실시 예를 개시하는 도면이다.

[0166] 일 실시 예에서, HTTP/HTTPS를 기반으로 한 패킷으로부터 시간, 프로토콜 정보, 서버/클라이언트 IP 또는 Port, 계정, 트랜잭션명, 이벤트 정보, 개인정보 개수 중 적어도 하나에 대한 데이터를 추출할 수 있다. 각각의 정의에 대한 내용은 상술한 바와 같다.

[0167] 일 실시 예에서, HTTP/HTTPS 기반의 패킷 분석 결과를 본 도면과 같이 “데이터”의 형태로 클라이언트에게 제공할 수 있다.

[0168] 데이터 관리 플랫폼은 HTTP/HTTPS 기반의 패킷을 분석하면, html 형태 또는 함수 형태의 데이터를 추출할 수 있다. 이때, 데이터 관리 플랫폼은 html 형태의 경우 웹 페이지를 그대로 출력할 수 있고, 함수 형태의 경우, 함수를 그대로 출력할 수 있다.

[0170] 도 14는 본 발명의 분석된 패킷에 포함된 데이터 중 개인정보를 추출하는 일 실시 예를 개시하는 도면이다.

[0171] 일 실시 예에서, 데이터 관리 플랫폼(10000)은 개인정보 메타데이터를 사용하여 로그 데이터(log data)와 인덱스(index)를 포함하는 감사 로그(Audit log, 1033)로부터 개인정보를 추출할 수 있다.

[0172] 보다 상세하게는, 감사 로그(1033)는 네트워크 상에서 발생하는 이벤트들을 기록한 로그의 집합으로, 로그 데이터(log data) 및 인덱스(index)를 포함할 수 있다. 여기에서, 감사 로그(1033)는 인덱스 처리가 완료된 로그 데이터의 집합일 수 있다.

[0173] 데이터 관리 플랫폼(10000)은 감사 로그에서 개인 정보를 추출하기 위하여 개인정보 메타데이터를 사용할 수 있다. 여기에서, 개인정보 메타데이터는 개인정보가 어떤 형태로 저장되어 있는지, 어떤 필드에 저장되어 있는지, 개인정보 유형 별로 사용되는 정규식 패턴 및 마스킹 패턴 등이 정의되어 있다. 예를 들어, 이름, 주소, 전화번호 등의 개인정보 유형에 대한 메타데이터를 구성할 수 있다. 이에 따라, 분석 모듈은 개인정보 메타데이터를 기반으로 로그 데이터에서 개인정보를 식별하고 추출할 수 있다.

[0174] 일 실시 예에서, 추출된 개인정보는 개인정보 유형 별로 기 설정된 방식에 따라 암호화되어 다시 감사 로그(1033) 또는 데이터 관리 플랫폼(10000) 내부 데이터베이스 상에 저장될 수 있다. 자세한 내용은 후술하도록 한다.

[0175] 일 실시 예에서, 데이터 관리 플랫폼(10000)은 추출된 개인 정보를 사용하여 특정 기간 동안의 로그 데이터를 검색할 수 있고, 관리자나 사용자가 필요할 때 검색하거나 검색된 로그 데이터를 확인할 수 있다. 이에 대하여는 후술하도록 한다.

[0177] 도 15는 본 발명의 분석된 패킷에 포함된 데이터를 시각화한 일 실시 예를 개시하는 도면이다.

[0178] 상술한 실시 예를 통하여 분석된 패킷에 포함되는 데이터는 다음과 같다.

[0179] (1) 세션 정보: 시작 시간, Duration Time, Log ID, Session ID, Context ID

[0180] (2) 접속 정보: 서버 IP, 서버 Port, 서버 Mac, 클라이언트 IP, 클라이언트 Port, 클라이언트 Mac

[0181] (3) SAP 정보: SID, 프로토콜, SAP 인스턴스, 클라이언트

[0182] (4) 프로그램 정보: OK Code, T-code, Title App, Title Main

[0183] (5) CUA(Central User Administration) 정보: CUA Name, CUA Status

[0184] (6) 사용자 정보: 사용자 ID, 사용자 UID, 사용자명

[0185] (7) 이벤트 정보: 이벤트 카테고리, 이벤트 코드, 이벤트 이름, 이벤트 설명, 이벤트 값, 알림 수준

[0186] (8) 사용자 정의 정보: 이벤트, 경고, 이벤트 유형, 이벤트 건수, 경고 건수, 아키텍쳐, 개인정보 존재 여부, 개인정보 유형 건수, 개인정보건수

[0187] 일 실시 예에서, 데이터 관리 플랫폼은 분석된 패킷으로부터 위와 같은 데이터를 추출할 수 있다. 이때, 데이터 관리 플랫폼은 패킷으로부터 추출된 데이터에 개인정보가 포함된 경우, 개인정보에 대한 암호화를 수행하여 저장할 수 있다. 특히, 데이터 관리 플랫폼은 개인정보에 대하여는 별도의 화면으로 출력할 수 있다.

[0188] 이를 통해, 법 및 인증에서 요구하는 모든 사항(계정 정보, 접속일시, 접속지 정보, 처리한 주체 정보, 수행 업무)을 수집할 수 있다. 보다 상세하게는, 계정 정보는 사용자 정보의 사용자 ID, 사번, 조직이름을 통하여, 접속일시는 세션 정보의 시작 시간을 통하여, 접속지 정보는 접속 정보의 클라이언트 IP 또는 Port를 통하여, 처리한 정보주체 정보는 사용자 정의 정보(개인정보 존재 여부, 개인정보 건수, 주민등록번호, 외국인등록번호, 여권 정보 및 카드 정보 등)를 통하여, 수행 업무는 프로그램 정보 및 사용자 정의 정보를 통하여 판단할 수 있다.

[0190] 도 16은 본 발명의 분석된 패킷에 포함된 데이터를 검색하는 일 실시 예를 개시하는 도면이다.

[0191] 일 실시 예에서, 데이터 관리 플랫폼은 상술한 데이터들을 검색하여 사용자에게 검색 결과를 제공할 수 있다.

[0192] 이를 위하여, 본 도면의 (a)와 같이 데이터 관리 플랫폼은 사용자가 쉽게 검색할 수 있도록 검색 인터페이스를 제공할 수 있다. 데이터 관리 플랫폼은 분석된 데이터의 필드를 기준으로 데이터를 검색할 수 있다. 예를 들어, 데이터 필드는 프로토콜, 시스템, 계정, 사번, 서버 IP, 서버 Port, 클라이언트 IP, 클라이언트 Port, 인스턴스명, 트랜잭션명, 프로그램명 등을 포함할 수 있다. 이때, 데이터 관리 플랫폼은 사용자로부터 입력 받은 필드 중 적어도 하나를 기준으로 데이터를 검색하고, 검색 결과를 출력할 수 있다.

[0193] 다른 실시 예에서, 본 도면의 (b)와 같이 데이터 관리 플랫폼은 쿼리(query) 검색 기능을 제공할 수 있다. 예를 들어, 사용자가 protocol_type=GUI를 제 1 쿼리로 입력하고, server_ip=175.117.145.125를 제 2 쿼리로 입력하는 경우, 데이터 관리 플랫폼은 제 1 쿼리 및 제 2 쿼리를 기준으로 데이터를 검색할 수 있다.

[0194] 일 실시 예에서, 검색된 결과는 상술한 바와 같이 “화면 재현” 형태 또는 “데이터” 형태로 출력될 수 있다.

[0196] 도 17은 본 발명의 데이터 관리 방법에 따라 수집된 데이터를 모니터링하는 일 실시 예를 개시하는 도면이다.

[0197] 상술한 바와 같이, 데이터 관리 플랫폼(10000)은 적어도 하나의 클라이언트(1000a, 1000b, 1000c)로부터 네트워크(1001) 및 TAP(1001b)을 통하여 패킷을 수집하고 분석할 수 있다.

[0198] 수집된 패킷은 기 정의된 이벤트에 기초하여 분류되고 저장될 수 있다. 일 실시 예에서, 데이터 관리 플랫폼(10000)은 분석된 패킷으로부터 수집된 데이터를 모니터링할 수 있다.

[0199] 보다 상세하게는, 데이터 관리 플랫폼(10000)은 모니터링 모듈(20005)을 통하여 수집된 데이터에 대한 이상 행위를 감지하여 클라이언트(1000a, 1000b, 1000c)의 사용자에게 알람을 제공할 수 있다. 예를 들어, 데이터 관리 플랫폼(10000)은 대시 보드(Dash board), 이메일, SMS 등을 통하여 사용자에게 수집된 데이터에 대한 이상 행위를 보고(report)할 수 있다.

[0200] 일 실시 예에서, 데이터 관리 플랫폼(10000)은 이상 행위가 감지되는 경우, 클라이언트(1000a, 1000b, 1000c)의 접속을 제어할 수 있다. 예를 들어, 사용자가 클라이언트(1000a, 1000b, 1000c)에 접속하여 수행한 이벤트가 이상 행위로 판단되는 경우, 모니터링 모듈(20005)은 대시 보드 등을 통하여 사용자에게 알람을 제공함과 동시에 클라이언트(1000a, 1000b, 1000c)의 접속을 차단할 수 있다.

[0201] 특히, 데이터 관리 플랫폼(10000)은 클라이언트(1000a, 1000b, 1000c)가 아카이브 파일(Archive File)이 포함된 데이터베이스(1003)에 접근하여 이벤트를 발생시키는 것을 모니터링하여 알람을 제공하거나 접근을 제어할 수 있다. 여기에서, 데이터베이스(1003)는 데이터 관리 플랫폼(10000) 외부에 저장된 저장소(storage) 또는 내부에 저장된 저장소에 대응한다. 또한, 이벤트에 대한 정보는 상술한 내용을 참고하도록 한다.

[0202] 또한, 데이터 관리 플랫폼(1000)은 이상 행위가 아니더라도 기 설정된 이벤트에 해당하는 경우, 클라이언트(1000a, 1000b, 1000c)의 접근을 제어할 수 있다.

[0203] 또한, 데이터 관리 플랫폼(1000)은 클라이언트(1000a, 1000b, 1000c)로부터 입력된 데이터가 개인정보인 경우, 이를 감지하여 보안 담당자에게 예를 들어, 메일로 입력된 데이터를 포함하는 화면을 전송할 수 있다.

[0204] 도 18은 본 발명의 데이터 관리 플랫폼이 수집된 패킷을 분배하는 실시 예를 설명하는 도면이다.

[0205] 일 실시 예에서, 데이터 관리 플랫폼은 수집 모듈(20001)을 통하여 패킷을 수집할 수 있다.

[0206] 보다 상세하게는, 수집 모듈(20001)은 네트워크(예를 들어, 상술한 NIC를 통하여)에서 패킷을 수집할 수 있다. 여기에서, 패킷 수집은 상술한 물리적인 장치 또는 가상 머신에서 실행되는 소프트웨어로 수행될 수 있다. 여기에서, 패킷은 프로토콜 헤더와 페이로드 데이터로 구성된 패킷을 포함할 수 있다.

[0207] 본 발명의 일 실시 예에서, 데이터 관리 플랫폼은 사용자가 애플리케이션 서버에 접근해서 수행하는 모든 행위에 대한 패킷을 수집할 수 있다. 예를 들어, 애플리케이션 사용자는 SAP GUI 프로토콜, RFC 프로토콜, HTTP 등 다양한 프로토콜을 사용하여 SAP 서버에 접근할 수 있다. 뿐만 아니라, 애플리케이션 사용자는 SAP SNC 프로토콜, HTTPS 등을 사용하여서도 SAP 서버에 접근할 수 있다. 각각의 경우에 대하여 자세히 설명하도록 한다.

[0208] 분석 모듈(20002)은 수집 모듈(20001)을 통하여 수집된 패킷을 프로토콜을 기반으로 분배할 수 있다. 보다 상세하게는, 분석 모듈(20002)은 조각난 패킷을 재조립하고, TCP 정보, 프로토콜, 포트(port), IP 주소 등을 기반으로 패킷을 제 1 분석 모듈(20002a), 제 2 분석 모듈(20002b), …등에 분배할 수 있다. 여기에서, 제 1 분석 모듈(20002a) 및 제 2 분석 모듈(20002b)는 예를 든 것으로, 프로토콜에 기초하여, 데이터 관리 플랫폼은 패킷을 분석하기 위한 모듈을 생성할 수 있다.

[0209] 제 1 분석 모듈(20002a) 및 제 2 분석 모듈(20002b)은 패킷을 분석하고, 패킷에 포함된 데이터를 데이터베이스(20007)에 저장할 수 있다.

[0210] 데이터베이스(20007)은 분석된 패킷의 로그 데이터를 저장하고, 필요한 경우 검색 및 조회 기능을 제공할 수 있다.

[0211] 이하에서는, 각각 다른 프로토콜에 대한 패킷 분석 방법에 대하여 자세히 설명하도록 한다.

[0213] 도 19는 본 발명의 데이터 관리 플랫폼이 RFC 프로토콜 기반의 패킷을 분석하는 실시 예를 설명하는 도면이다.

[0214] 일 실시 예에서, 데이터 관리 플랫폼(10000)은 수집 모듈(20001)과 분석 모듈(20002)을 통하여 애플리케이션서버(1002)와 RFC 정보와 패킷에 대한 분석 및 구조 정보를 송수신할 수 있다. 이하에서, 데이터 관리 플랫폼(10000)은 수집 모듈(20001) 또는 분석 모듈(20002)이 수행하는 기능을 지원하기 위한 API를 제공할 수 있다.

[0215] 수집 모듈(20001)은 RFC 패킷 수집부(2001)를 포함할 수 있다. 여기에서, RFC 패킷 수집부(2001)는 수집된 패킷 중 RFC 패킷을 추출하여 분석 모듈(20002)에 전달할 수 있다.

[0216] 분석 모듈(20002)은 RFC 정보 요청부(2002) 및 RFC 패킷 분석부(2003)를 포함할 수 있다. 즉, 분석 모듈(20002)은 수집 모듈(20001)로부터 전달받은 RFC 패킷을 분석할 수 있다. 보다 상세하게는, 데이터 관리 플랫폼(10000) 내에 RFC 구조 정보가 있는 경우, RFC 구조 정보를 이용하여 RFC 패킷을 분석할 수 있다. 반면, 데이터 관리 플랫폼(10000) 내에 RFC 구조 정보가 없는 경우, RFC 정보 요청부(2002)는 RFC 정보 요청 파일을 생성할 수 있다. RFC 정보 요청부(2002)는 RFC 정보 요청 파일을 감지하는 경우, 애플리케이션 서버(1002)에 RFC 구조 정보를 요청할 수 있다. 이에 따라, 데이터 관리 플랫폼(10000)은 애플리케이션 서버(1002)에 RFC 정보를 요청할 수 있고, RFC 구조 정보를 수신할 수 있다. RFC 패킷 분석부(2003) 은 애플리케이션 서버(1002)로부터 수신한 RFC 구조 정보를 이용하여 RFC 패킷을 분석할 수 있다.

[0218] 도 20은 본 발명의 데이터 관리 플랫폼이 패킷을 분석하는 실시 예를 설명하는 도면이다.

[0219] 일 실시 예에서, 데이터 관리 플랫폼(10000)은 수집 모듈(20001)을 통하여 수집된 패킷이 HTTP/HTTPS 기반의 패킷, GUI/SNC 프로토콜 기반의 패킷인 경우, 분석 모듈(20002)을 통하여 패킷을 분석할 수 있다. 이때, 데이터 관리 플랫폼(10000)은 패킷을 분석하는데 사용되는 인증서를 관리하는 데이터베이스(20007)를 유지할 수 있다.

[0220] 보다 상세하게는, 분석 모듈(20002)은 HTTP 패킷 분석부(2004), HTTPS 패킷 분석부(2005), GUI 패킷 분석부(2006) 및 SNC 패킷 분석부(2007)를 포함할 수 있다.

[0221] 여기에서, HTTP 패킷 분석부(2004)는 HTTP 패킷을 분석하고, HTTPS 패킷 분석부(2005)는 HTTPS 패킷을 분석하고, GUI 패킷 분석부(2006)는 GUI 프로토콜 기반 패킷을 분석하고, SNC 패킷 분석부(2007) SNC 프로토콜 기반 패킷 분석을 수행할 수 있다.

[0222] 분석 모듈(20002)은 보안 수준이 상대적으로 낮은 HTTP 패킷 및 GUI 프로토콜 기반의 패킷은 상술한 실시 예에 따라 패킷을 분석할 수 있다.

[0223] 반면, 보안 수준이 상대적으로 높은 HTTPS 패킷 및 SNC 패킷은 데이터베이스(20007)에 저장된 SSL 인증서를 사용하여 암호화된 통신을 복호화하여 패킷을 분석할 수 있다.

[0224] 이에 따라, 데이터 관리 플랫폼(10000)은 암호화된 HTTPS 기반의 패킷을 HTTP 기반의 패킷과 동일하게 데이터를 추출할 수 있다. 마찬가지로, 데이터 관리 플랫폼(10000)은 암호화된 SNC 프로토콜 기반의 패킷을 GUI 프로토콜 기반의 패킷과 동일하게 데이터를 추출할 수 있다.

[0225] HTTPS 패킷을 분석하는 방법에 대하여는 후술하도록 한다. 이때, HTTPS 패킷과 SNC 패킷에 사용되는 인증서는 동일하거나 상이한 인증서에 대응할 수 있다.

[0227] 도 21은 본 발명의 데이터 관리 플랫폼이 감사 로그를 저장하고 모니터링하는 실시 예를 설명하는 도면이다.

[0228] 일 실시 예에서, 데이터 관리 플랫폼(10000)은 상술한 실시 예에 따라 추출한 원본 데이터를 정의된 필드 규칙에 따라 변환하고 가공하여 감사 로그(1033)를 생성할 수 있다. 여기에서, 생성된 감사 로그(1033)는 데이터베이스(20007)에 저장될 수 있다.

[0229] 또한, 데이터 관리 플랫폼(10000)은 가공된 데이터 중에서 개인정보 메타데이터를 이용하여 개인정보를 추출할 수 있다. 이에 따라, 데이터 관리 플랫폼(10000)은 감사 로그(1033)와 개인정보를 각각 데이터베이스(20007)에 저장할 수 있다. 이를 위하여, 분석 모듈(20002)은 감사 로그 저장부(2008)를 더 포함할 수 있다.

[0230] 또한, 분석 모듈(20003)은 상관 분석 규칙 생성부(2009)를 더 포함할 수 있다. 데이터 관리 플랫폼(10000)은 분석 모듈(20002)를 통하여 상관 분석 규칙을 생성할 수 있다. 여기에서, 상관 규칙이란 이상 행위 판단에 대한 규칙을 나타낼 수 있다. 예를 들어, 데이터 관리 플랫폼(10000)은 1초당 데이터가 1-2건 입력되는 경우 정상 행위로 판단하고, 1초당 데이터가 10건 이상 입력되는 경우 이상 행위로 판단할 수 있다. 여기에서, “상관”이라는 표현은 로그(log) 간의 상관성을 나타낼 수 있다. 이때, 데이터 관리 플랫폼(10000)은 상관 규칙에 의해 또 다른 이벤트(로그)를 발생시킬 수 있다. 이때의 로그는 인시던트로 정의할 수 있다. 즉, 데이터 관리 플랫폼(10000)을 통하여 모니터링을 원하는 주체(subject)가 상관 규칙을 생성하고, 데이터 관리 플랫폼(10000)은 상관 규칙에 기초하여 로그들을 분석하고 또 다른 로그인 인시던트를 발생시킬 수 있다.

[0231] 또한, 상관 분석 규칙은 다른 플랫폼에 의해 기 정의된 규칙에 대응할 수 있다. 이에 따라, 데이터 관리 플랫폼(10000)은 생성된 상관 분석 규칙을 이용하여 감사 로그(1033)를 분석하여 이상행위 이벤트를 생성할 수 있다. 이때, 생성된 상관 분석 규칙에 대한 정보 및 이상행위 이벤트에 대한 정보는 데이터베이스(20007)에 저장될 수 있다.

[0232] 데이터 관리 플랫폼(10000)의 모니터링 모듈(20005)는 이상행위 모니터링부(2010)를 더 포함할 수 있다. 이상행위 모니터링부(2010)는 생성된 이상행위 이벤트에 기초하여 저장된 감사 로그(1033), 개인정보 등을 검색 또는 모니터링할 수 있다.

[0233] 이에 따라, 데이터 관리 플랫폼(10000)은 수집, 분석되어 저장된 데이터에서 개인정보를 추출할 수 있고, 추출된 개인정보를 이용하여 사용자 행위를 통계화할 수 있다. 이후, 수집된 사용자 행위 중 위반 행위가 발생한 경우, 데이터 관리 플랫폼(10000)은 사용자를 차단 또는 관리자에게 경고를 제공할 수 있다.

[0235] 도 22는 본 발명의 데이터 관리 방법이 수집된 패킷을 분배하는 실시 예를 설명하는 도면이다.

[0236] 단계(S10010)에서, 데이터 관리 방법은 패킷을 수집하고 필터를 적용할 수 있다. 이때, 데이터 관리 방법은 NIC와 같은 네트워크 장비를 통하여 패킷을 수집할 수 있다. 이후, 데이터 관리 방법은 수집된 패킷을 재조합하고, 각각의 네트워크 패킷을 분석 가능한 패킷 형태로 합칠 수 있다.

[0237] 일 실시 예에서, 데이터 관리 방법은 필터링 규칙에 기초하여 패킷을 분석할지 여부를 결정할 수 있다. 여기에서, 필터링 규칙은 데이터 관리 플랫폼에 의해 결정될 수 있다. 보다 상세하게는, 데이터 관리 방법은 상술한 NIC나 라우터와 같은 네트워크 장비를 통하여 패킷을 수집할 수 있다. 이때, 수집되는 모든 패킷을 분석한다면 성능에 이슈가 있을 수 있기 때문에 필터링 규칙에 의해 분석할 패킷을 필터링할 수 있다. 예를 들면, HTTP나

SAP GUI 프로토콜 기반의 패킷은 분석할 필요가 있지만 그 외의 다른 프로토콜로 수집된 패킷은 분석할 필요가 없을 수 있다. 이때, 데이터 관리 방법은 포트 또는 IP 별로 원하는 프로토콜 기반의 패킷만을 분석하도록 수집된 패킷을 필터링할 수 있다. 이때, 사용자는 데이터 관리 방법을 이용하여 직접 필터링 규칙을 설정할 수 있다.

[0238] 단계(S10020)에서, 데이터 관리 방법은 TCP 세션 정보에 기초하여 프로토콜을 구분할 수 있다. 상술한 바와 같이, 데이터 관리 방법은 수집된 패킷을 프로토콜을 기반으로 구분하여 분석할 수 있다.

[0239] 데이터 관리 방법은 단계(S10020)에서 구분된 프로토콜에 기초하여 다른 방법으로 패킷을 분석할 수 있다. 각각에 대한 분석 방법은 상술한 바와 같다.

[0240] 단계(S10030)에서, 데이터 관리 방법은 RFC 프로토콜 기반 패킷을 분석할 수 있다.

[0241] 단계(S10040)에서, 데이터 관리 방법은 GUI/SNC 프로토콜 기반 패킷을 분석할 수 있다.

[0242] 단계(S10050)에서, 데이터 관리 방법은 HTTP/HTTPS 기반 패킷을 분석할 수 있다.

[0243] 단계(S10030) 내지 단계(S10050)에서, 데이터 관리 방법은 패킷을 파싱한 후 분석을 위한 처리 규칙을 수행할 수 있다. 이때, 데이터 관리 방법은 패킷의 바이너리 데이터를 분석하여 각종 데이터(계정 데이터, SID, 화면 입력 데이터, 화면 출력 데이터 등)를 추출할 수 있다. 또한, 처리 규칙은 분석된 패킷 내에 포함된 데이터를 감사 로그(1033)에 저장할 것인지 여부, 분석된 패킷 내에 포함된 데이터의 가공 또는 로깅(logging) 여부, 이벤트 및 경고를 발생시킬지 여부 등을 처리하는 설정을 나타낼 수 있다. 이외에도, 데이터 관리 방법은 불필요한 로그를 필터링하는 필터 규칙과 처리 규칙을 처리하기 위한 데이터를 로딩하는 적제 규칙을 더 수행할 수 있다.

[0244] 단계(S10060)에서, 데이터 관리 방법은 분석된 패킷에 기초하여 감사 로그(1033)를 생성할 수 있다. 이때, 데이터 관리 방법은 로그 저장 속도를 높이기 위하여 멀티 쓰레딩(multi-threading) 방식으로 동작하며 데이터베이스의 접근이 일시적으로 불가능한 경우에 대비하여 메모리 큐잉 및 파일 큐잉을 수행할 수 있다.

[0245] 단계(S10070)에서, 데이터 관리 방법은 생성된 감사 로그(1033)에 대하여 개인정보 메타데이터를 이용하여 개인정보를 추출할 수 있다.

[0246] 단계(S10080)에서, 데이터 관리 방법은 감사 로그(1033)를 저장할 수 있다. 이때, 데이터 관리 방법은 감사 로그(1033)와 개인정보를 각각 저장할 수 있다.

[0247] 단계(S10090)에서, 데이터 관리 방법은 이상행위를 모니터링할 수 있다.

[0249] 도 23은 본 발명의 데이터 관리 플랫폼이 HTTPS 기반 패킷을 분석하는 실시 예를 설명하는 도면이다.

[0250] HTTPS(SSL)로 보호된 웹 브라우저에서의 사용자 행위는 기존의 네트워크 트래픽 미러 기술로는 로그를 기록할 수 없다. 특히, HTTPS 연결 시 키교환을 위해 디피-헬만(Diffie-Hellman) 알고리즘을 사용하는 경우에는 로그를 기록할 수 없다. 여기에서, 디피-헬만(Diffie-Hellman) 알고리즘은 대칭키 암호화 방식에서 사용되는 알고리즘 중 하나로, 키 교환 프로토콜을 안전하게 수행하기 위한 방법에 대응한다.

[0251] 하지만 기업 내 이상행위 및 개인정보 과남용을 모니터링하기 위해서는 웹 브라우저에서의 사용자 행위에 대한 로그를 기록하고 모니터링 해야 하는 요구가 있다.

[0252] 본 발명의 일 실시 예에 따르면, 키교환을 위해 디피-헬만 알고리즘을 사용하는 경우에도 웹 브라우저에서의 사용자 행위에 대한 로그를 기록해 기업 내 이상행위 및 개인정보 과남용을 모니터링할 수 있다.

[0253] 이를 위하여, 데이터 관리 플랫폼(10000)은 디피-헬만 알고리즘을 사용하는 경우에도 사용자 행위를 모니터링할 수 있도록 한다.

[0254] 보다 상세하게는, 데이터 관리 플랫폼(10000)의 분석 모듈(20002)은 프록시 서버 구성부(2011), SSL 설정부(2012), HTTP 요청/응답 데이터 분석부(2013) 및 메시지 데이터 생성부(2014)를 더 포함할 수 있다.

[0255] 여기에서, 프록시 서버 구성부(2011)는 웹 브라우저(1030)와 웹 서버(1034) 사이에 프록시 서버(1031)를 구성할 수 있다. 여기에서, 프록시 서버(1031)는 클라이언트와 서버 간의 네트워크 통신을 중개하는 서버로, 클라이언트는 프록시 서버(1031)를 이용하는 경우 직접 웹 서버(1034)와 통신하지 않고 프록시 서버(1031)를 통하여 간접적으로 통신할 수 있다.

[0256] SSL 설정부(2012)는 프록시 서버(1031)에서 SSL을 설정할 수 있다. 보다 상세하게는, SSL 설정부(2012)는 프록시 서버(1031)를 구성하고, 클라이언트 SSL 설정을 이용하여 웹 브라우저(1030)와 프록시 서버(1031) 간의 SSL 환경을 구성하여 HTTPS 요청/응답에 대한 처리를 수행할 수 있다. 일 실시 예에서, SSL 설정부(2012)는 SSL 설정을 위하여 SSL 인증서를 사용할 수 있다. 여기에서, SSL 인증서는 상술한 패킷을 분석하기 위한 인증서와는 상이한 인증서에 대응할 수 있다. 즉, 이때의 SSL 인증서는 SSL 설정을 지원(support)하기 위한 것에 대응한다.

[0257] HTTPS 요청 데이터를 전달받은 프록시 서버(1031)는 SSL 연결을 일시적으로 중단할 수 있고, HTTP 요청/응답 분석부(2013)를 통해 HTTP 요청/응답 데이터를 처리하고, 다시 SSL 연결을 수행할 수 있다.

[0258] 이에 따라, 메시지 데이터 생성부(2014)는 HTTP 요청/응답 데이터를 조합하여 메시지 데이터(1035)를 생성할 수 있고, 생성된 메시지 데이터(1035)를 큐(1032)에 저장할 수 있다. 여기에서, 큐(1032)는 메모리 큐와 파일 큐를 포함할 수 있다.

[0259] 이후, 데이터 관리 플랫폼(10000)은 큐(1032)에 저장된 메시지 데이터(1035)를 외부로 전송할 수 있다.

[0260] 마지막으로, 데이터 관리 플랫폼(10000)은 서버 SSL 설정을 이용하여 프록시 서버(1031)와 웹 서버(1034) 간의 SSL 환경을 구성하여 HTTPS 요청/응답에 대한 처리를 수행하고, HTTPS 응답 데이터를 전달할 수 있다.

[0261] 이를 통해 디피-헬만 알고리즘을 사용하는 경우에도 웹 브라우저에서의 사용자 행위에 대한 로그를 기록할 수 있다.

[0263] 도 24는 본 발명의 데이터 관리 방법이 HTTPS 기반 패킷을 분석하는 실시 예를 설명하는 도면이다.

[0264] 단계(S20010)에서, 데이터 관리 방법은 HTTPS 기반 패킷을 수집하기 위하여 프록시 서버를 구성하고 클라이언트 SSL을 설정하고, 단계(S20020)에서, 프록시 서버를 구성하고 서버 SSL을 설정할 수 있다. 즉, 데이터 관리 방법은 프록시 서버를 구성하고, 서버 SSL 설정을 이용하여 프록시 서버와 웹 서버 간의 SSL 환경을 구성하여 HTTPS 요청/응답에 대한 처리를 수행하고, HTTPS 응답 데이터를 전달할 수 있다.

[0265] 프록시 서버가 구성되고, SSL이 설정되는 경우, 단계(S20030)에서, 데이터 관리 방법은 HTTPS 패킷을 수집할 수 있다. 상술한 바와 달리, 본 도면의 데이터 관리 방법에서는 HTTPS 패킷을 수집하는 경우를 예를 들어 설명한다.

[0266] HTTPS 연결의 경우 키교환을 위해 디피-헬만 알고리즘을 사용하는데, 디피-헬만 알고리즘을 이용하여 패킷을 암호화하는 경우에는 기존의 네트워크 트래픽 미러 기술로는 사용자 행위에 대한 로그를 기록할 수 없기 때문에 본 발명은 이하의 방법을 제안한다.

[0267] 단계(S20040)에서, 데이터 관리 방법은 HTTPS 요청/응답에 대한 처리를 수행할 수 있다. 즉, 데이터 관리 방법은 프록시 서버를 구성하고, 클라이언트 SSL 설정을 이용하여 웹 브라우저와 프록시 서버 간의 SSL 환경을 구성하여 HTTPS 요청/응답에 대한 처리를 수행할 수 있다. 이후, HTTPS 요청 데이터를 전달받은 프록시 서버는 SSL 연결을 중단하고, HTTP 요청/응답 데이터를 처리한 후 다시 SSL 연결을 수행할 수 있다.

[0268] 단계(S20050)에서, 데이터 관리 방법은 HTTP 요청/응답 데이터를 조합하여 메시지 데이터(1035)를 생성할 수 있다. 이때, 데이터 관리 방법은 불필요한 데이터를 필터링할 수 있다. 보다 상세하게는, 데이터 관리 방법은 HTTP 요청/응답 데이터를 조합하여 메시지 데이터(1035)를 생성할 수 있는데, 로깅(logging)할 때 불필요한 데이터(예를 들어, 이미지 데이터)는 전달하지 않을 수 있다.

[0269] 단계(S20060)에서, 데이터 관리 방법은 생성된 메시지 데이터(1035)를 메모리 큐(queue) 또는 파일 큐 중 적어도 하나에 적재할 수 있다. 보다 상세하게는, 데이터 관리 방법은 메시지 데이터(1035)를 저장하기 위한 큐로 메모리 큐 및 파일 큐를 사용할 수 있다. 이때, 메시지 데이터(1035)를 저장하기 위하여 파일 큐만 사용하는 경우 성능이 낮아질 위험이 있고, 메모리 큐만 사용하는 경우 데이터의 유실이 발생할 수 있기 때문에 두가지 큐를 조합하여 사용할 수 있다.

[0270] 단계(S20070)에서, 데이터 관리 방법은 큐에 적재된 메시지 데이터(1035)를 저장소로 전달하여 저장할 수 있다. 여기에서, 저장소는 상술한 데이터 관리 플랫폼 내에 포함된 데이터베이스에 대응한다.

[0272] 도 25는 본 발명의 데이터 관리 방법의 일 실시 예를 설명하는 도면이다.

[0273] 단계(S30010)에서, 데이터 관리 방법은 네트워크를 통하여 패킷을 수집할 수 있다. 본 발명의 데이터 관리 방법이 네트워크를 통하여 패킷을 수집하는 방법은 도 5 내지 도 7, 도 18 및 도 19의 실시 예를 참고하도록 한다.

[0274] 단계(S30020)에서, 데이터 관리 방법은 수집된 패킷에 포함된 정보에 기초하여 프로토콜을 구분할 수 있다. 본 발명의 데이터 관리 방법이 수집된 패킷에 포함된 정보에 기초하여 프로토콜을 구분하는 방법은 도 5 및 도 18의 실시 예를 참고하도록 한다.

[0275] 단계(S30030)에서, 데이터 관리 방법은 프로토콜에 기초하여 패킷을 분석할 수 있다. 본 발명의 데이터 관리 방법이 프로토콜에 기초하여 패킷을 분석하는 방법은 도 5, 도 8 내지 도 13, 도 18 내지 도 20의 실시 예를 참고하도록 한다.

[0276] 단계(S30040)에서, 데이터 관리 방법은 분석된 패킷에 포함된 정보에 기초하여 로그를 생성할 수 있다. 본 발명의 데이터 관리 방법이 분석된 패킷에 포함된 정보에 기초하여 로그를 생성하는 방법은 도 18 및 도 21의 실시 예를 참고하도록 한다.

[0277] 이를 통하여, 법 또는 규정에서 기준으로 하는 개인정보 처리 시스템에 대한 요구사항(requirements)을 만족시킬 수 있다. 예를 들어, 본 발명에 따르면, “개인정보의 안정성 확보조치 기준 제 8 조”에 의해 개인정보 처리 시스템에 대한 접속기록을 의미적으로 보관 하여야 한다는 조건을 만족할 수 있다.

[0279] 개인정보를 추출하기 위한 방법으로는 주로 정규식(Regular expression)을 이용한 방법이 사용된다. 다만, 정규식을 이용한 방법은 잘못 추출될 우려가 존재한다.

[0280] 이러한 점을 보완하기 위하여 본 발명에서는 개인정보를 추출하기 위하여 정규식 방법 뿐만 아니라 개인정보 메타데이터 및 예외처리 리스트를 사용한 다차원 추출 방법을 통해 개인정보 추출에 대한 정확도를 높일 수 있다.

[0282] 도 26은 본 발명의 데이터 관리 플랫폼에서 개인정보를 추출하고 저장하는 실시 예를 설명하는 도면이다.

[0283] 본 발명의 데이터 관리 플랫폼(10000)에 포함된 개인정보 관리 모듈(20004)는 감사 로그(1033)로부터 개인정보를 추출 위하여 개인정보 유형을 정의할 수 있다. 여기에서, 감사 로그(1033)에는 인덱스(index) 처리가 완료된 로그 데이터(log data)를 포함할 수 있다. 또한, 개인정보 유형은 예를 들어, 주민등록번호, 신용카드 번호, 계좌 번호 등과 같은 개인정보의 종류를 포함할 수 있다.

[0284] 보다 상세하게는, 개인정보 관리 모듈(20004)의 개인정보 유형 분석부(2019)는 개인정보 추출을 위한 개인정보 메타데이터(1036) 생성을 위해 저장된 감사 로그(1033)에서 사용되는 개인정보 유형 및 추출 방식을 분석할 수 있다. 이에 대한 분석 결과를 개인정보 메타데이터(1036)에 저장할 수 있다. 이때, 개인정보 관리 모듈(20004)는 아키텍처(여기에서, 아키텍처는 애플리케이션 개발환경, 화면 사용자 인터페이스(User Interface, UI)를 포함한다.) 유형에 기초하여 개인정보 메타데이터(1036)에 포함된 필드를 정의할 수 있다. 여기에서, 아키텍처 유형은 로그 데이터의 변수 및 값을 분석하는 파서(parser)를 구분하는 정보에 대응한다. 일 실시 예에서, 개인정보 관리 모듈(20004)는 로그 데이터 내 필드 정보에 대하여 프로토콜 유형 및 URL을 기준으로 아키텍처 유형을 구분할 수 있고, 이에 따라 인덱스의 필드 정보를 생성할 수 있다. 또한, 개인정보 메타데이터(1036)는 아키텍처 유형(화면 유형), 화면 정보(level 1, level 2) 및 개인정보 추출 규칙을 포함할 수 있다.

[0285] 이를 위하여, 개인정보 관리 모듈(20004)의 개인정보 패턴 저장부(2020)는 개인정보 유형 별로 사용되는 패턴을 저장할 수 있다. 개인정보 관리 모듈(20004)은 개인정보 유형을 정의하고, 개인정보 유형 별로 사용되는 정규식 패턴 및 마스킹 패턴을 저장할 수 있다. 여기에서, 개인정보 관리 모듈(20004)이 개인정보 유형을 정의하고, 개인정보 유형 별로 사용되는 정규식 패턴을 저장하는 이유는 개인정보 메타데이터(1036)에 포함되는 정보를 생성하기 위함이다.

[0286] 결론적으로, 데이터 관리 플랫폼(10000)은 개인정보 유형을 정의하고, 개인정보 유형 별로 사용되는 정규식 패턴을 저장해 놓음으로써 개인정보 메타데이터(1036)를 생성할 수 있게 되고, 개인정보 메타데이터(1036)와 후술하는 개인정보 예외처리 리스트(1037)를 이용하여 개인정보 추출 규칙을 생성하고, 개인정보 추출 규칙을 이용해 개인정보를 추출할 수 있다.

[0287] 또한, 개인정보 관리 모듈(20004)의 개인정보 예외처리 리스트 생성부(2021)는 개인정보 예외처리 리스트(1037)를 생성할 수 있고, 개인정보 추출 규칙 생성부(2022)는 추출할 개인정보 추출 규칙을 생성할 수 있다. 이때, 개인정보 관리 모듈(20004)는 개인정보 예외처리 리스트(1037)를 생성하기 위하여, 개인정보 메타데이터(1036)를 이용하여 감사 로그(1033)에서 가상으로 추출되는 개인정보 항목을 확인할 수 있고, 추출된 값이나 분석된 변수에 기초하여 예외처리 리스트(1037)에 포함되는 예외처리 규칙을 정의할 수 있다.

[0288] 다른 실시 예에서, 개인정보 관리 모듈(20004)의 개인정보 해쉬 값 수집부(2023)는 개인정보 유형별 해쉬(hash) 값을 수집할 수 있고, 개인정보 유형별 값 필터(value filter)를 생성할 수 있다. 여기에서, 값 필터는 개인정

보 값의 해쉬 값에 대해 블룸-필터 자료 구조를 사용하여 만든 필터에 대응한다. 본 발명에서는, 값 필터를 통해 대량의 데이터 집합에서 비교 값의 포함 여부를 빠르게 확인할 수 있다는 장점이 있다.

[0289] 보다 상세하게는, 개인정보 관리 모듈(20004)는 여러 유형 별로 개인정보 값에 대한 해쉬 값을 수집하여 개인정보 유형 별로 저장할 수 있다. 개인정보 관리 모듈(20004)의 개인정보 값 필터 생성부(2024)는 수집된 개인정보 데이터를 기준으로 개인정보 유형별 값 필터 파일을 생성할 수 있다.

[0290] 이후, 개인정보 관리 모듈(20004)의 개인정보 추출부(2025)는 개인정보를 추출할 수 있고, 개인정보 암호화부(2026)는 추출된 개인정보를 암호화하고, 개인정보 저장부(2027)는 암호화된 개인정보를 저장할 수 있다. 보다 상세하게는, 개인정보 관리 모듈(20004)는 감사 로그(1033)에 포함된 로그 데이터를 아키텍쳐 유형 별로 분석하여 변수 및 값을 추출하고, 추출된 값에 개인정보 (추출) 규칙이 포함된 개인정보 메타데이터(1036)를 이용하여 개인정보를 추출할 수 있다.

[0291] 일 실시 예에서, 개인정보 관리 모듈(20004)는 추출된 개인정보 값의 해쉬 값이 값 필터 내에 포함되어 있는지 검증할 수 있다. 이때, 해쉬 값이 값 필터 내에 포함되어 있는 경우, 개인정보 관리 모듈(20004)는 감사 로그(1033)의 인덱스에 추출된 개인정보를 저장할 수 있다. 반면, 해쉬 값이 값 필터 내에 포함되어 있지 않은 경우, 개인정보 관리 모듈(20004)는 잘못 추출된 것으로 판단하여 추출된 개인정보를 제거할 수 있다.

[0292] 이후, 암호화된 개인정보를 검색하는 경우, 개인정보 관리 모듈(20004)은 암호화된 개인정보를 복호화한 후 마스킹 규칙에 의해 처리된 개인정보를 출력할 수 있다.

[0293] 이하, 개인정보 관리 모듈(20004)이 수행하는 기능은 데이터 관리 플랫폼(10000)이 수행하는 것으로 지칭할 수 있다.

[0294] 이를 통하여, 개인정보 추출에 대한 정확도를 높일 수 있다. 이하, 후술하는 도면을 통하여 본 발명을 상세히 설명하도록 한다.

[0296] 도 27은 본 발명의 데이터 관리 플랫폼에서 사용되는 정규식 패턴의 일 예를 설명하는 도면이다.

[0297] 상술한 실시 예에서, 데이터 관리 플랫폼은 개인정보 유형 별로 사용되는 패턴을 저장할 수 있다. 특히, 데이터 관리 플랫폼은 개인정보 유형 별로 사용될 정규식 패턴 및 마스킹 패턴을 저장할 수 있다.

[0298] 본 도면은 데이터 관리 플랫폼에서 사용되는 개인정보 유형 별 정규식 패턴을 나타낸다. 예를 들어, 개인정보가 주민등록번호인 경우, 정규식 패턴은 “(₩d{6}[,-]-?[1-4]₩d{6})|(₩d{6}[,-]?[1-4])”에 대응할 수 있다. 또한, 다른 예를 들면, 개인정보가 운전면허번호인 경우, 정규식 패턴은 “(₩d{2}-₩d{2}-₩d{6}-₩d{2})”에 대응할 수 있다. 이와 같이, 데이터 관리 플랫폼은 개인정보 유형(주민등록번호, 운전면허번호, 전화번호, 메일주소, 주소, 생년월일, 여권번호, 계좌번호, 신용카드번호, 건강보험번호, 외국인등록 번호 등)에 대하여 각각의 정규식 패턴을 정의할 수 있다. 또한, 각각의 개인정보 유형에 대한 정규식 패턴은 기 설정되어 데이터 관리 플랫폼에 저장될 수 있다. 이때, 본 도면에 포함된 개인정보 유형은 예시일 뿐으로 다른 개인정보 등이 더 포함될 수 있음은 물론이다.

[0300] 도 28은 본 발명의 데이터 관리 플랫폼에서 사용되는 마스킹 패턴의 일 예를 설명하는 도면이다.

[0301] 상술한 실시 예에서, 데이터 관리 플랫폼은 개인정보 유형 별로 사용되는 패턴을 저장할 수 있다. 특히, 데이터 관리 플랫폼은 개인정보 유형 별로 사용될 정규식 패턴 및 마스킹 패턴을 저장할 수 있다.

[0302] 본 도면은 데이터 관리 플랫폼에서 사용되는 개인정보 유형 별 마스킹 패턴을 나타낸다. 마스킹 처리 규칙에는 일부 마스킹, 전체 마스킹, 범위 마스킹, 무작위 마스킹 및 일관성 유지 마스킹 등을 포함할 수 있다.

[0303] 예를 들어, 개인정보가 주민등록번호인 경우, 마스킹 처리 기준이 존재하고, 마스킹 패턴은 “11111-2******”에 대응할 수 있다. 즉, 이 경우에는 주민등록번호에 대한 일부 마스킹 패턴을 적용한 것이다.

[0304] 이때, 마스킹 처리 기준은 기 설정된 값에 따라 다를 수 있으며, 본 도면에서는 java를 기준으로 하였으나 다른 방법의 마스킹 처리 규칙을 적용할 수 있음은 물론이다.

[0305] 데이터 관리 플랫폼은 마스킹 처리 규칙에 따라 개인정보를 유형 별로 마스킹 처리할 수 있다. 상술한 예를 들어, 데이터 관리 플랫폼은 주민등록번호의 뒷자리 중 6자리를 가려서 처리할 수 있으며, 운전면허번호의 경우 뒷자리 3자리만을 마스킹 처리할 수 있다.

[0306] 상술한 실시 예에 따라 마스킹 처리된 개인정보는 이후 개인정보 조회 요청 시 마스킹 처리된 상태로 출력될 수

있다. 이에 따라, 데이터 관리 플랫폼을 이용하는 경우 개인정보에 보안을 가할 수 있다.

[0308] 도 29는 본 발명의 데이터 관리 플랫폼에서 정의하는 개인정보 메타데이터(1036)의 일 예를 설명하는 도면이다.

[0309] 일 실시 예에서, 데이터 관리 플랫폼은 개인정보 메타데이터(1036)를 이용하여 감사 로그에 포함된 개인정보를 추출할 수 있다. 이를 위하여, 데이터 관리 플랫폼은 개인정보 메타데이터(1036)를 생성하고, 저장할 수 있다.

[0310] 데이터 관리 플랫폼은 아키텍처 유형 별로 추출할 개인정보 유형 및 방식을 정의하고 개인정보 메타데이터(1036)에 저장할 수 있다. 여기에서, 아키텍처 유형이란 GUI 데이터인지, json 데이터인지, WEBGUI인지 여부 등을 나타낼 수 있다. 즉, 데이터 관리 플랫폼은 GUI 데이터 별로 추출할 개인정보 유형 및 방식을 정의하고, 개인정보 메타데이터(1036)에 저장할 수 있고, json 데이터 별로 추출할 개인정보 유형 및 방식을 정의할 수 있다.

[0311] 보다 상세하게는, 개인정보 메타데이터(1036)은 아키텍처 유형, 화면 정보(레벨 1), 화면 정보(레벨 2) 및 개인정보 추출 규칙을 포함할 수 있다.

[0312] 여기에서, 아키텍처 유형은 상술한 바와 같이 화면 유형에 대응한다. 실제로 출력되는 화면이 어떤 화면인지에 대한 정보를 포함하고 있다. 일 실시 예에서, 아키텍처 유형에 기초하여 개인정보 추출 규칙이 결정될 수 있다. 또한, 개인정보 메타데이터(1036)는 아키텍처 유형에 대응하는 레벨 1 화면 정보, 레벨 2 화면 정보를 포함할 수 있다.

[0313] 개인정보 추출 규칙은 추출 방식 및 값을 포함할 수 있다. 추출 방식은 값 추출 방식, 변수 추출 방식, 값 컨텐트 추출 방식, 전문 정규식 추출 방식, 복합 개인정보 추출 방식을 예로 들 수 있다. 이하 추출 방식에 대해 설명하도록 한다.

[0314] 값 추출 방식은 추출된 개인정보의 값(value)을 기준으로 개인정보를 추출하는 방식이다. 이때, 본 발명의 데이터 관리 플랫폼은 값 추출 방식의 값(value)에 대하여 개인정보 유형 리스트를 이용할 수 있다.

[0315] 변수 추출 방식은 아키텍처 유형에 포함된 변수(variable)를 기준으로 개인정보를 추출하는 방식이다. 이때, 본 발명의 데이터 관리 플랫폼은 변수 추출 방식의 값에 대하여 개인정보 유형 리스트와 변수명 리스트를 함께 이용할 수 있다. 여기에서, 변수명 리스트는 개인정보 유형에 따른 변수명 리스트에 대응한다. 예를 들어, A 화면(A 유형)에서는 “주민”이 변수명 리스트에 포함될 수 있고, B 화면(B 유형)에서는 “SSN”이 변수명리스트에 포함될 수 있다.

[0316] 전문 정규식 추출 방식은 변수가 존재하지 않은 상태에서 파싱(parsing)이 불가능한 전체 텍스트(full text)를 기준으로 개인정보를 추출하는 방식이다. 이때, 본 발명의 데이터 관리 플랫폼은 전문 정규식 추출 방식의 값에 대하여 개인정보 유형 리스트와 패턴 리스트를 함께 이용할 수 있다. 여기에서, 패턴 리스트는 값에 대한 정규식 뿐만 아니라 정규식의 앞 또는 뒤에 패턴을 추가한 것을 포함할 수 있다. 예를 들어, 데이터 관리 플랫폼은 주민번호가 정규식인 경우, 주민번호 앞에 “:”이 있는 경우를 패턴 리스트에 포함시킬 수 있다.

[0317] 복합 개인정보 추출 방식은 개인정보를 추출할 때 하나의 개인정보를 기준으로 개인정보를 추출하는 것이 아닌 두개 이상의 개인정보를 기준으로 개인정보를 추출하는 방식이다. 일 실시 예에서, 데이터 관리 플랫폼은 아키텍처 유형 별로 “이름”과 “주민등록번호”가 모두 존재할 때만 개인정보로 판단할 수 있다. 반면, 데이터 관리 플랫폼은 아키텍처 유형 별로 “이름” 또는 “주민등록번호” 중 하나만 있는 경우에는 개인정보가 아니라고 판단할 수 있다.

[0318] 이와 같이, 본 발명의 데이터 관리 플랫폼은 개인정보 메타데이터(1036)에 포함된 정보를 바탕으로 개인정보를 추출할 수 있다.

[0320] 도 30은 본 발명의 데이터 관리 플랫폼에서 아키텍처 유형을 구분하여 개인정보를 추출하는 실시 예를 설명하는 도면이다.

[0321] 일 실시 예에서, 데이터 관리 플랫폼(10000)의 아키텍처 유형 분석부(2029)는 감사 로그(1033)로부터 아키텍처 유형을 구분한 뒤, 개인정보 추출부(2025)를 통하여 아키텍처 유형 별로 정의된 개인정보 메타데이터(1036)를 이용하여 개인정보를 추출할 수 있다.

[0322] 보다 상세하게는, 데이터 관리 플랫폼(10000)은 아키텍처 유형에 기초하여 개인정보 메타데이터(1036)에 포함되는 필드를 정의할 수 있다. 여기에서, 아키텍처 유형은 로그 데이터의 변수 및 값을 분석하는 파서를 구분하는 정보에 대응한다. 즉, 아키텍처 유형에 따라 변수 및 값을 분석하기 위한 파싱(parsing) 방법이 달라진다. 따라

서, 데이터 관리 플랫폼(10000)은 아키텍처 유형에 기초하여 개인정보 메타데이터(1036)에 포함되는 필드를 정의해야 한다.

[0323] 일 실시 예에서, 데이터 관리 플랫폼(10000)의 아키텍처 유형 분석부(2029)는 감사 로그(1033) 내에 포함된 로그 데이터 내의 필드 정보에 대하여 프로토콜 유형 및 URL을 기준으로 아키텍처 유형을 구분할 수 있고, 이에 따라 인덱스의 필드 정보를 생성할 수 있다.

[0324] 이에 따라, 데이터 관리 플랫폼(10000)의 개인정보 추출부(2025)는 아키텍처 유형 별로 정의된 개인정보 메타데이터(1036) 및 상술한 예외처리 리스트(1037) 중 적어도 하나를 활용하여 개인정보를 추출할 수 있다.

[0325] 이후, 데이터 관리 플랫폼은 추출된 개인정보를 암호화하고, 암호화된 개인정보를 저장할 수 있다.

[0327] 도 31은 본 발명의 데이터 관리 플랫폼에서 개인정보 추출 규칙을 생성하는 실시 예를 설명하는 도면이다.

[0328] 일 실시 예에서, 데이터 관리 플랫폼은 개인정보 추출 규칙을 생성할 수 있다. 이를 위하여, 본 도면에서는 개인정보 추출 규칙을 생성하는 사용자 인터페이스를 설명한다. 개인정보 추출 규칙을 생성하기 위하여, 사용자 인터페이스는 기본 정보, 값 정규식 추출 정보, 변수 기반 추출 정보 중 적어도 하나를 포함할 수 있다.

[0329] 보다 상세하게는, 기본 정보는 개인정보 추출 규칙을 적용할 대상을 나타낸다. 여기에서, 기본 정보는 로그 유형, 레벨 1(화면, 트랜잭션), 레벨 2(프로그램, 서비스) 중 적어도 하나를 포함할 수 있다. 이에 따라, 사용자는 로그 유형(예를 들어, SAP GUI 로그), 레벨 1 또는 레벨 2 중 적어도 하나를 개인정보 추출 규칙을 적용할 대상으로 입력할 수 있다.

[0330] 또한, 값 정규식 추출 정보는 개인정보 추출 방식 별로 추출할 개인 정보를 포함할 수 있다. 보다 상세하게는, 전체 개인정보가 존재하며, 데이터 관리 플랫폼은 사용자로부터 추출할 개인정보를 선택받을 수 있다. 이에 따라, 데이터 관리 플랫폼은 개인정보 추출 방식 별로 로그에서 값을 추출한 후 정규식 패턴과 비교하여 개인정보를 판단할 수 있다. 이를 위하여, 데이터 관리 플랫폼은 상술한 실시 예인 개인정보 유형별로 저장된 정규식 패턴 파일을 이용할 수 있다.

[0331] 또한, 데이터 관리 플랫폼은 로그 유형별로 분석된 변수의 값을 이용하여 개인정보 추출 규칙을 생성할 수 있다. 이를 위하여, 데이터 관리 플랫폼은 사용자로부터 변수 기반 추출 정보를 입력 받을 수 있다.

[0333] 도 32는 본 발명의 데이터 관리 플랫폼에서 개인정보 예외처리 리스트를 생성하는 실시 예를 설명하는 도면이다.

[0334] 일 실시 예에서, 데이터 관리 플랫폼은 개인정보 예외처리 리스트(1037)를 생성할 수 있다. 보다 상세하게는, 데이터 관리 플랫폼은 감사 로그(1033)로부터 개인정보 메타데이터(1036)를 이용하여 가상으로 추출되는 개인정보 항목을 확인할 수 있다. 즉, 데이터 관리 플랫폼은 개인정보 메타데이터(1036)에 포함된 항목(예를 들어, 상술한 key/value, 화면명/필드명 등)을 이용하여 개인정보를 가상으로 추출할 수 있다. 여기에서, 가상으로 추출된 개인정보 항목은 원본 로그 데이터에서 본 발명의 실시 예에 따라 생성된 개인정보 메타데이터(1036)의 항목을 기준으로 출력된 후보 데이터(candidate data)에 대응한다.

[0335] 데이터 관리 플랫폼은 추출된 값 또는 분석된 변수를 기준으로 예외처리 리스트(1037)를 생성할 수 있다. 보다 상세하게는, 데이터 관리 플랫폼은 개인정보 메타데이터(1036)에 포함된 항목을 기준으로 예외처리 리스트(1037)를 생성할 수 있다.

[0336] 이때, 데이터 관리 플랫폼은 개인정보 메타데이터(1036)에 포함된 아키텍처 유형, 화면 정보 및 개인정보 추출 규칙 중 적어도 하나를 예외처리 리스트(1037)를 생성할 수 있다. 예를 들어, 데이터 관리 플랫폼은 예외처리 리스트를 생성할 때, “제 1 아키텍처(UI) 유형에서 해당 키는 개인정보가 아니기 때문에 추출하지 않는다” 또는 “제 2 아키텍처(UI) 유형에서 해당 값은 개인정보가 아니기 때문에 추출하지 않는다”와 같이 등록할 수 있다.

[0337] 예를 들면, 데이터 관리 플랫폼은 감사 로그(1033)에서 가상의 개인정보로 “계좌번호”를 추출할 수 있다. 여기에서, “계좌번호”는 후보 데이터에 대응한다. 또한, 개인정보 메타데이터(1036)의 화면명/필드명에는 A제품/시리얼 넘버가 포함되어 있을 수 있다. 여기에서, A제품의 시리얼 넘버는 개인정보에 해당하지 않는다고 가정한다. 이때, A제품에 대한 시리얼 넘버가 개인정보인 “계좌번호”와 동일한 경우, 데이터 관리 플랫폼은 추출된 “계좌번호”는 개인정보가 아닌 것으로 판단하여 예외처리 리스트(1037)에 등록할 수 있다.

[0338] 즉, 데이터 관리 플랫폼은 상술한 실시 예에 따라 정의된 개인정보 메타데이터(1036)를 참고하여, 가상으로 추

출되는 개인정보를 확인할 수 있다. 이때의 개인정보는 정확한 개인정보가 아닌 후보 데이터이기 때문에, 후보 데이터에 대하여 개인정보 메타데이터(1036)에 포함된 항목을 기준으로 예외처리 리스트(1037)를 생성할 수 있다.

[0339] 일 실시 예에서, 데이터 관리 플랫폼은 감사 로그(1033)에서 개인정보를 추출할 때, 예외처리 리스트(1037)에 포함된 항목을 제외하고 개인정보를 추출할 수 있다.

[0340] 이에 따라, 잘못된 개인정보를 추출할 확률을 낮추는 장점이 있다.

[0342] 도 33은 본 발명의 데이터 관리 플랫폼의 예외 필터를 생성하는 실시 예를 설명하는 도면이다.

[0343] 일 실시 예에서, 데이터 관리 플랫폼은 상술한 방법으로 예외처리 리스트를 생성할 수 있다. 본 도면에서는 예외처리 리스트를 생성하기 위한 예외 필터 사용자 인터페이스를 설명한다. 예외 필터 사용자 인터페이스는 적어도 하나의 개인정보 항목을 포함할 수 있다.

[0344] 일 실시 예에서, 데이터 관리 플랫폼은 사용자로부터 개인정보 항목에 대한 예외 필터 정보를 입력받을 수 있다. 여기에서, 예외 필터 정보는 아키텍쳐 유형(UI 유형), 레벨 1(화면, 트랜잭션), 값, 레벨 2(프로그램, 서비스), 변수 중 적어도 하나를 포함할 수 있다.

[0345] 본 도면의 예를 들어 설명하면, 데이터 관리 플랫폼은 사용자로부터 예외 필터 정보로 “아키텍쳐 유형=SAP GUI ” “레벨 1=SE16” “레벨 2=SAPMF02D-7230” “변수=RDTMS_VAL2” “값=8201301037329”를 수신할 수 있다.

[0346] 이에 따라, 데이터 관리 플랫폼은 사용자로부터 입력받은 예외 필터 정보를 이용하여 예외처리 리스트를 생성할 수 있다.

[0348] 도 34는 본 발명의 데이터 관리 플랫폼에서 추출된 개인정보를 검색하고 출력하는 실시 예를 설명하는 도면이다.

[0349] 본 발명의 데이터 관리 플랫폼(10000)에 포함된 개인정보 관리 모듈(20004)의 개인정보 복호화부(2028)은 암호화된 개인정보를 복호화할 수 있다. 보다 상세하게는, 사용자가 데이터 관리 플랫폼(10000)의 모니터링 모듈(20005)를 통하여 개인정보 검색을 요청하는 경우, 데이터 관리 플랫폼(10000)은 암호화된 개인정보를 복호화할 수 있다. 이때, 데이터 관리 플랫폼(10000)은 감사 로그(1033)에 포함된 데이터를 이용하여 개인정보를 복호화할 수 있다.

[0350] 일 실시 예에서, 개인정보 관리 모듈(20004)는 데이터베이스(20007)에 포함된 암호화 키를 이용하여 암호화된 개인정보를 복호화할 수 있다. 이후, 개인정보 관리 모듈(20004)의 마스킹 처리부(2029)는 복호화된 개인정보를 마스킹 처리하여 모니터링 모듈(20005)에게 제공할 수 있다. 여기에서, 개인정보를 마스킹 처리하는 방법은 상술한 바와 같다. 이에 따라, 모니터링 모듈(20005)는 개인정보 관리 모듈(20004)에 의해 마스킹 처리된 개인정보를 출력하여 사용자에게 제공할 수 있다.

[0351] 이를 통하여, 데이터 관리 플랫폼은 추출된 개인정보에 대한 검색 요청이 있는 경우, 암호화 키에 기반하여 개인정보를 복호화한 뒤 마스킹 처리하여 사용자에게 제공할 수 있다. 이에 따라, 개인정보 보호에 기여할 수 있다.

[0353] 도 35는 본 발명의 데이터 관리 방법이 개인정보를 관리하는 실시 예를 설명하는 도면이다.

[0354] 단계(S40010)에서, 데이터 관리 방법은 개인정보 유형을 분석할 수 있다. 이를 위하여, 데이터 관리 방법은 감사 로그에서 사용되는 개인정보 유형을 분석할 수 있다.

[0355] 단계(S40020)에서, 데이터 관리 방법은 개인정보 유형을 정의하고, 개인정보 유형 별로 사용되는 패턴을 저장할 수 있다. 데이터 관리 방법은 개인정보 유형 별로 사용되는 정규식 패턴 및 마스킹 패턴을 저장할 수 있다. 이에 따라, 데이터 관리 방법은 키/값 또는 화면명/필드명이 포함된 개인정보 메타데이터(1036)를 생성할 수 있다. 개인정보 메타데이터(1036)를 생성하는 구체적인 방법은 상술한 바와 같다.

[0356] 단계(S40030)에서, 데이터 관리 방법은 개인정보 예외처리 리스트(1037)를 생성할 수 있다. 데이터 관리 방법은 개인정보 메타데이터(1036)를 이용하여 감사 로그에서 가상으로 추출되는 개인정보 항목을 확인할 수 있고, 추출된 값 또는 분석된 변수에 기초하여 예외처리 리스트(1037)에 포함되는 예외처리 규칙을 정의할 수 있다. 이에 따라, 데이터 관리 방법은 개인정보 예외처리 리스트(1037)를 생성할 수 있다.

[0357] 단계(S40040)에서, 데이터 관리 방법은 개인정보 메타데이터(1036) 및 예외처리 리스트(1037)에 기초하여 개인

정보 추출 규칙을 생성할 수 있다.

[0358] 단계(S40050)에서, 데이터 관리 방법은 개인정보 추출 규칙에 기초하여 개인정보를 추출할 수 있다.

[0359] 단계(S40060)에서, 데이터 관리 방법은 추출된 개인정보를 암호화하여 저장할 수 있다. 일 실시 예에서, 데이터 관리 방법은 추출된 개인정보를 암호화하기 위한 암호화 키를 생성할 수 있다.

[0360] 단계(S40070)에서, 데이터 관리 방법은 개인정보 검색 요청 시 암호화된 개인정보를 복호화할 수 있다. 이때, 데이터 관리 방법은 개인정보 검색 요청 시 생성된 암호화키를 이용하여 암호화된 개인정보를 복호화할 수 있다.

[0361] 단계(S40080)에서, 데이터 관리 방법은 복호화된 개인정보를 마스킹 처리할 수 있다. 개인정보를 마스킹 처리하는 방법에 대하여는 상술한 바와 같다.

[0362] 단계(S40090)에서, 데이터 관리 방법은 마스킹 처리된 개인정보를 출력할 수 있다. 이를 통하여, 복호화된 개인정보는 마스킹 처리되어 출력되기 때문에 개인정보의 검색을 요청한 사용자는 개인정보를 침해하지 않으면서 데이터베이스 내의 개인정보를 검색하고 이용할 수 있다.

[0364] 또한, 정규식 패턴 방식으로 추출된 개인정보의 경우 잘못 추출될 우려가 있다. 이에 따라, 본 발명에서는 상술한 실시 예 이외에도 개인정보가 잘못 추출될 위험을 줄이기 위하여 실제로 로그 상에 존재하는 개인정보를 블룸-필터(Bloom filter)화 시킬 수 있다. 즉, 추출된 개인정보에 블룸-필터를 적용하여 개인정보라고 판단되는 경우에만 추출하여 개인정보 추출의 정확도를 높일 수 있다. 이하에서 자세히 설명하도록 한다.

[0366] 도 36은 본 발명의 데이터 관리 방법이 개인정보를 추출하고 저장하는 다른 실시 예를 설명하는 도면이다.

[0367] 단계(S50010)에서, 데이터 관리 방법은 개인정보에 대한 해쉬(hash) 값을 수집할 수 있다. 보다 상세하게는, 데이터 관리 방법은 개인정보 암호화 솔루션과 같이 개인정보를 관리하는 시스템/플랫폼으로부터 여러 유형의 개인정보 값에 대한 해쉬 값을 수집할 수 있다. 여기에서, 개인정보를 관리하는 시스템/플랫폼은 외부 서버에 존재할 수 있다. 일 실시 예에서, 데이터 관리 방법은 수집된 해쉬 값을 개인정보 유형 별로 저장할 수 있다.

[0368] 단계(S50020)에서, 데이터 관리 방법은 개인정보 유형 별 값 필터(value filter)를 생성할 수 있다. 여기에서, 값 필터는 개인정보 값의 해쉬 값에 대해 블룸-필터 자료 구조(bloom filter data structure)를 사용하여 만든 필터에 대응한다.

[0369] 단계(S50030)에서, 데이터 관리 방법은 개인정보를 추출할 수 있다. 일 실시 예에서, 감사 로그 내 로그 데이터를 아키텍쳐 유형 별로 분석하여 변수 및 값을 추출하고, 추출된 값에 개인정보 추출 규칙을 적용하여 개인정보를 추출할 수 있다. 이에 대하여는 상술한 바와 같다.

[0370] 단계(S50040)에서, 데이터 관리 방법은 개인정보 값을 검증할 수 있다. 즉, 상술한 내용에 더불어 추출된 개인정보 값을 검증하기 위하여 값 필터를 사용할 수 있다.

[0371] 단계(S50050)에서, 개인정보에 대한 해쉬 값이 값 필터 내에 포함되어 있는 경우, 단계(S50060)에서, 데이터 관리 방법은 인덱스에 추출된 개인정보를 저장할 수 있다. 보다 상세하게는, 추출한 개인정보에 대한 해쉬 값이 블룸-필터 자료 구조를 사용하여 만든 값 필터 내에 포함되어 있는 경우, 데이터 관리 방법은 추출한 개인정보를 진짜(real) 개인정보인 것으로 판단할 수 있다. 이에 따라, 데이터 관리 방법은 감사 로그 내 추출된 개인정보에 대하여 진짜 개인정보라는 인덱스를 저장할 수 있다.

[0372] 단계(S50070)에서, 데이터 관리 방법은 개인정보에 대한 해쉬 값이 값 필터 내에 포함되어 있지 않은 경우, 단계(S50080)에서, 데이터 관리 방법은 추출된 개인정보를 제거할 수 있다. 보다 상세하게는, 추출한 개인정보에 대한 해쉬 값이 블룸-필터 자료 구조를 사용하여 만든 값 필터 내에 포함되어 있지 않은 경우, 데이터 관리 방법은 추출한 개인정보를 가짜(fake) 개인정보인 것으로 판단할 수 있다. 이에 따라, 데이터 관리 방법은 추출한 개인정보가 잘못 추출된 것으로 판단하여 추출된 개인정보를 제거할 수 있다. 여기에서, 추출된 개인정보를 제거한다는 것은 데이터를 자체를 제거하는 것이 아닌 개인정보로서의 가치를 잃는 것을 의미할 수 있다.

[0373] 이에 따라, 본 발명에서는, 블룸-필터 자료 구조를 이용하여 대량으로 관리되는 개인정보와 개인정보로 추출된 값을 빠르게 비교할 수 있다. 또한, 값을 검증하기 힘든 유형의 개인정보에 대한 오류를 제거할 수 있다.

[0375] 도 37은 본 발명의 데이터 관리 방법에서 개인정보를 관리하는 실시 예를 설명하는 도면이다.

[0376] 단계(S60010)에서, 데이터 관리 방법은 데이터를 분석할 수 있다. 본 발명의 데이터 관리 방법이 데이터를 분석

하는 방법은 도 2 내지 도 5, 도 8 내지도 26, 도 29, 도 30 및 도 35의 실시 예를 참고하도록 한다.

[0377] 단계(S60020)에서, 데이터 관리 방법은 분석된 데이터로부터 개인정보를 추출할 수 있다.

[0378] 본 발명의 데이터 관리 방법이 개인정보를 추출하는 방법은 도 5, 도 14, 도 26, 도 35 및 도 36의 실시 예를 참고하도록 한다.

[0380] 애플리케이션 상에서 수행하는 사용자의 업무 행위는 개발자의 취향 및 개발 표준에 따라 상이하게 표현된다. 즉, 본 발명을 통하여 사용자의 업무 행위를 기초로 하는 데이터에 대한 “조회, 삭제, 추가, 변경, 프린트”와 같은 사용자 행위의 구분을 용이하게 하고자 한다.

[0381] 따라서, 본 발명은 애플리케이션의 메뉴 및 아이콘의 텍스트를 수집하고, 인공지능을 기반으로 자동으로 분류하여 법적으로 요구하는 사용자 행위에 대한 상세 구분을 할 수 있다.

[0382] 또한, 감사 로그(audit log) 시스템에서 발생하는 이벤트 및 사용자의 활동 등의 정보를 기록한 로그로, 보안 및 감사 추적 등을 위해 사용될 수 있다. 여기에서, 감사 로그는 로그 데이터 및 로그 데이터에 대응하는 인덱스를 포함할 수 있다.

[0383] 로그 데이터는 일반적으로 시간, 이벤트/행위, 사용자/주체, 대상/객체, 결과 등의 정보로 구별되며, 각각의 로그 데이터는 하나의 레코드(Record)를 형성하며, 여러 개의 레코드가 연속적으로 기록될 수 있다.

[0384] 또한, 감사 로그의 데이터는 데이터베이스 등에서 인덱싱 처리되어 관리되는 것이 일반적이다. 이때, 로그 데이터의 검색 및 분석을 효율적으로 수행하기 위해 각 로그 레코드에 대한 인덱스도 함께 관리될 수 있다. 여기에서, 인덱스는 보통 검색에 사용되는 필드와 검색 속도를 향상시키기 위한 키(Key) 등의 정보를 포함한다.

[0385] 예를 들어, 시간, 이벤트/행위, 사용자/주체, 대상/객체 등의 필드를 가진 감사 로그에서 사용자가 특정 파일을 삭제한 기록을 검색하기 위해, 시간 필드와 대상 필드를 조합하여 인덱스를 생성할 수 있다. 이렇게 생성된 인덱스를 활용하면, 검색 시간을 대폭 줄일 수 있다는 장점이 있다.

[0386] 뿐만 아니라, 인덱스에 사용자 행위를 매핑하면, 로그 데이터를 사용자 행위를 기준으로 분류할 수 있어 보안 분석이나 모니터링에 용이하다는 장점이 있다.

[0387] 본 발명의 데이터 관리 플랫폼은 감사 로그에 포함된 로그 데이터를 인공지능을 기반으로 분류된 사용자 행위를 기준으로 인덱싱 처리해 사용자가 사용자 행위를 기준으로 로그 데이터를 검색할 수 있도록 한다. 이하, 본 발명에 대해 자세히 설명한다.

[0389] 도 38은 본 발명의 데이터 관리 플랫폼에서 사용자 행위를 수집하고 매핑하는 실시 예를 설명하는 도면이다.

[0390] 본 발명의 데이터 관리 플랫폼(10000)은 수집 모듈(20001), 분석 모듈(20002), 모니터링 모듈(20005) 및 AI 엔진(20006)을 이용하여 사용자 행위를 수집하고, 로그 데이터와 매핑하여 인덱스 처리한 후 로그 데이터 조회 요청에 따라 사용자 행위로 인덱스 처리된 로그 데이터를 제공할 수 있다.

[0391] 보다 상세하게는, 수집 모듈(20001)을 사용하여 사용자 행위에 대응하는 키 및 텍스트를 수집할 수 있다. 이때, 수집 모듈(20001)은 애플리케이션 개발환경에 연결하여 사용자 행위를 수집할 수 있다. 애플리케이션 개발환경에서는 사용자 행위를 선택하는 메뉴, 아이콘에 대한 키 및 텍스트를 보관하고 있다. 이에 따라, 본 발명의 데이터 관리 플랫폼(10000)에 포함된 수집 모듈(20001)은 이러한 사용자 행위에 대응하는 키 및 텍스트를 수집할 수 있다.

[0392] AI 엔진(20006)은 수집된 텍스트를 인공지능(AI)을 기반으로 사용자 행위(action)을 분류할 수 있다. 예를 들어, 사용자 행위는 조회, 삭제, 추가, 변경, 프린트 등의 사용자의 업무 행위를 포함할 수 있다. 이를 위하여, AI 엔진(20006)은 기계학습(machine learning), 딥 러닝(deep learning), 자연어 처리(Natural Language Processing, NLP), 규칙 기반 접근(Rule-Based Approach) 등의 방법을 사용할 수 있다.

[0393] 분석 모듈(20002)은 분류된 사용자 행위에 대한 데이터를 키(key) 및 사용자 행위(action)로 구분하여 사용자 행위 메타데이터(1038)를 생성할 수 있다. 이때, 사용자 행위 메타데이터(1038)는 데이터 관리 플랫폼(10000) 내부 데이터베이스(20007) 안에 저장될 수 있다.

[0394] 분석 모듈(20002)은 저장된 사용자 행위 메타데이터(1038)와 감사 로그(1033) 안에 포함된 로그 데이터를 매핑할 수 있다. 이때, 분석 모듈(20002)는 로그 데이터와 사용자 행위 메타데이터(1038)을 매핑하기 위하여, 로그 데이터를 인덱스 처리할 때 애플리케이션 개발환경 유형 별 키로 사용할 수 있는 필드와 사용자 행위 메타데이

터(1038) 내에 키 정보를 매핑하여 인덱스의 사용자 행위 필드에 저장할 수 있다.

[0395] 여기에서, 키 정보는 사용자 행위를 나타내는 식별 정보를 나타낸다. 일 실시 예에서, 데이터 관리 플랫폼(10000)은 사용자 행위를 텍스트로 저장하지 않고, 사용자 행위를 식별하기 위한 축약된 ID(Identification)로 저장할 수 있다. 예를 들어, 데이터 관리 플랫폼(10000)은 사용자 행위가 “조회”인 경우, 키 정보로 “R”을 저장하고, 사용자 행위가 “삭제”인 경우, 키 정보로 “D”를 저장하고, 사용자 행위가 “수정”인 경우, 키 정보로 “U”를 저장하고, 사용자 행위가 “프린트”인 경우, 키 정보로 “P”를 저장할 수 있다.

[0396] 사용자는 모니터링 모듈(20005)를 통하여 로그를 조회할 수 있다. 일 실시 예에서, 모니터링 모듈(20005)은 데이터베이스(20007) 내 감사 로그(1033)에 포함된 로그 데이터를 제공할 때, 인덱스의 사용자 행위 필드를 참조하여 사용자에게 정보를 제공할 수 있다.

[0397] 이하, 데이터 관리 플랫폼(10000) 내부의 각각의 모듈에서 수행되는 기능은 데이터 관리 플랫폼(10000)이 수행하는 것으로 기재하도록 한다.

[0399] 도 39는 본 발명의 데이터 관리 플랫폼에서 사용자 행위 메타데이터를 생성하는 실시 예를 설명하는 도면이다.

[0400] 일 실시 예에서, 데이터 관리 플랫폼(10000)은 상술한 AI 엔진을 통하여 사용자 행위에 대응하는 키 및 텍스트를 수집할 수 있고, 수집된 텍스트를 인공지능을 기반으로 사용자 행위로 분류할 수 있다. 이에 따라, 데이터 관리 플랫폼(10000)은 수집된 사용자 행위에 대응하는 키 및 텍스트에 대하여 사용자 행위 메타데이터(1038)를 생성할 수 있다.

[0401] 보다 상세하게는, 데이터 관리 플랫폼(10000)은 사용자 행위 메타데이터(1038)를 생성하기 위하여, 애플리케이션 개발환경 유형 별 키 및 사용자 행위 키를 매핑할 수 있다. 즉, 사용자 행위 메타데이터(1038)는 애플리케이션 개발환경 유형 별 키, 사용자 행위 키, 사용자 행위를 필드로 가질 수 있다.

[0402] 여기에서, 애플리케이션 개발환경 유형은 상술한 아키텍처 유형, 화면 유저 인터페이스 유형을 포함할 수 있다. 즉, 애플리케이션 개발환경 유형은 애플리케이션 개발환경 내에서 사용자 업무 행위로 사용할 수 있는 정보 필드를 나타낸다. 예를 들어, 화면에 존재하는 메뉴 아이콘, ok 아이콘, cancel 아이콘 등을 포함할 수 있다. 또한, 사용자 행위 키는 상술한 사용자 행위를 식별하기 위한 ID를 나타낸다. 따라서, 데이터 관리 플랫폼(10000)은 사용자 행위 메타데이터(1038) 내에 애플리케이션 개발환경 유형 별 키 및 사용자 행위 키를 매핑할 수 있다.

[0403] 예를 들어, 애플리케이션 개발환경 유형별 키가 “제 1 애플리케이션에서 del 키”라면, 상술한 AI 엔진 및 분석 모듈을 통하여, 데이터 관리 플랫폼(10000)은 사용자 행위 키 “D”와 매핑하여 사용자 행위 메타데이터(1038)를 생성할 수 있다. 이때, 데이터 관리 플랫폼(10000)은 애플리케이션 개발환경 유형 별 키인 “제 1 애플리케이션에서 del 키”와 사용자 행위 키인 ”D”의 사용자 행위가 “삭제”임을 사용자 행위 메타데이터(1038)에 함께 저장할 수 있다.

[0405] 도 40은 본 발명의 데이터 관리 플랫폼에서 사용자 행위 메타데이터와 로그 데이터를 매핑하는 실시 예를 설명하는 도면이다.

[0406] 일 실시 예에서, 데이터 관리 플랫폼(10000)은 저장된 사용자 행위 메타데이터(1038)와 감사 로그(1033)에 포함된 로그 데이터를 매핑할 수 있다.

[0407] 보다 상세하게는, 데이터 관리 플랫폼(10000)은 로그 데이터와 사용자 행위 메타데이터(1038)을 매핑하기 위하여, 로그 데이터를 인덱스 처리할 수 있다. 구체적으로, 데이터 관리 플랫폼(10000)은 상술한 실시 예를 통하여 사용자 행위 메타데이터(1038) 내의 애플리케이션 개발환경 유형 별 키 필드와 사용자 행위 키 필드를 매핑할 수 있다. 또한, 일 실시 예에서, 데이터 관리 플랫폼(10000)은 인덱스의 사용자 행위 필드에 사용자 행위 메타데이터(1038)의 사용자 행위를 저장할 수 있다.

[0408] 이에 따라, 감사 로그(1033)에 저장된 제 1 로그 데이터가 사용자가 제 1 애플리케이션 화면에서 del 키를 누르는 로그를 나타내는 경우, 데이터 관리 플랫폼(10000)은 제 1 로그 데이터를 조회하는 요청을 수신하는 경우, 매핑된 사용자 행위인 “삭제”를 바로 제공할 수 있다.

[0409] 이렇게 인덱스에 사용자 행위를 매핑하면, 로그 데이터를 사용자 행위를 기준으로 분류할 수 있어 보안 분석이나 모니터링에 용이하다는 장점이 있다.

[0411] 도 41은 본 발명의 데이터 관리 방법이 사용자 행위 메타데이터를 생성하는 실시 예를 설명하는 도면이다.

[0412] 단계(S60030)에서, 데이터 관리 방법은 애플리케이션 개발환경에서 사용자 행위를 나타내는 메뉴, 버튼 또는 아이콘 등에 대한 키(key) 및 텍스트(text)를 수집할 수 있다. 보다 상세하게는, 애플리케이션 개발환경에서는 사용자 행위를 선택하는 메뉴에 대한 키 및 텍스트를 보관할 수 있다. 이에 따라, 데이터 관리 방법은 애플리케이션 개발환경에 연결하여 사용자 행위를 선택하는 메뉴에 대한 키 및 텍스트를 수집할 수 있다. 예를 들어, 데이터 관리 방법은 제 1 애플리케이션 개발환경에 연결하여, 제 1 애플리케이션 개발 환경에서 사용자 행위인 “삭제”를 나타내는 제 1 아이콘에 대한 키 및 텍스트 “”를 수집할 수 있다.

[0413] 이때, 인공지능을 통하여 수집된 텍스트를 분류하기 때문에, 완벽하게 동일한 단어를 사용하지 않더라도 그 의미가 동일한 경우 동일한 사용자 행위로 분류될 수 있다. 예를 들어, 애플리케이션 개발환경에 따라 사용자 행위를 나타내는 버튼에 대응하는 텍스트가 다를 수 있다. 예를 들어, 제 1 애플리케이션 개발환경에서는 삭제를 나타내는 버튼에 대응하는 텍스트가 “delete”지만, 제 2 애플리케이션 개발환경에서는 삭제를 나타내는 버튼에 대응하는 텍스트가 “remove”일 수 있다. 이 경우, 본 발명의 데이터 관리 방법에 따르면, 다른 애플리케이션 개발환경에서 다른 텍스트를 쓰더라도 의미가 동일한 경우 동일한 사용자 행위로 분류할 수 있다.

[0414] 본 발명의 데이터 관리 방법이 사용자 행위를 나타내는 키 및 텍스트를 수집하는 방법은 도 38의 실시 예를 참고하도록 한다.

[0415] 단계(S60040)에서, 데이터 관리 방법은 AI 엔진을 통하여 수집된 텍스트를 분류할 수 있다. 상술한 예를 참고하면, 데이터 관리 방법은 AI 엔진을 통하여 “delete”라는 텍스트를 사용자 행위인 “삭제”로 분류할 수 있다.

[0416] 단계(S60050)에서, 데이터 관리 방법은 분류된 데이터를 사용자 행위 메타데이터로 저장할 수 있다. 상술한 바와 같이, 데이터 관리 방법은 제 1 애플리케이션 개발환경에서, 제 1 아이콘에 대한 키 및 텍스트 “”를 사용자 행위 “삭제”와 매핑하여 사용자 행위 메타데이터에 저장할 수 있다.

[0418] 도 42는 본 발명의 데이터 관리 방법이 사용자 행위 메타데이터와 로그 데이터를 매핑하는 실시 예를 설명하는 도면이다.

[0419] 단계(S60060)에서, 데이터 관리 방법은 로그 데이터와 사용자 행위 메타데이터를 매핑하기 위한 메모리를 캐싱할 수 있다. 여기에서, 사용자 행위 메타데이터 상술한 바와 같은 방법으로 생성되어 저장된 것을 특징으로 한다. 일 실시 예에서, 데이터 관리 방법은 로그 데이터와 사용자 행위 메타데이터를 빠르게 매핑하기 위하여 매핑할 정보를 메모리에 캐싱(caching)할 수 있다. 즉, 데이터 관리 방법은 로그 데이터와 사용자 행위 메타데이터 중 매핑할 정보를 데이터베이스 상에서 조회하는 것이 아니라, 미리 메모리에 읽어 두어 빠르게 접근하도록 할 수 있다.

[0420] 단계(S60070)에서, 데이터 관리 방법은 로그 데이터와 사용자 행위 메타데이터를 매핑한 후 인덱스 처리할 수 있다. 보다 상세하게는, 데이터 관리 방법은 로그 데이터를 인덱스 처리할 때, 애플리케이션 개발환경 유형 별 키 필드와 사용자 행위 키 필드를 매핑하여 인덱스의 사용자 행위 필드에 저장할 수 있다. 일 시 예에서, 데이터 관리 방법은 로그 데이터를 인덱스 처리할 때, 인덱스의 사용자 행위 필드에 사용자 행위 메타데이터의 사용자 행위를 저장할 수 있다.

[0421] 단계(S60080)에서, 데이터 관리 방법은 로그 조회를 요청받는 경우, 인덱스의 사용자 행위 필드를 참조하여 정보를 제공할 수 있다.

[0422] 이를 통해, 개인정보가 포함된 모든 로그 데이터에 대해 사용자 행위를 매핑할 수 있다.

[0424] 도 43은 본 발명의 데이터 관리 방법이 사용자 행위 메타데이터를 생성하는 실시 예를 설명하는 도면이다.

[0425] 단계(S70010)에서, 데이터 관리 방법은 데이터를 수집할 수 있다. 본 발명의 데이터 관리 방법이 데이터를 수집하는 방법은 도 2 내지 도 7 및 도 38의 실시 예를 참고하도록 한다.

[0426] 단계(S70020)에서, 데이터 관리 방법은 수집된 데이터를 분류할 수 있다. 본 발명의 데이터 관리 방법이 데이터를 분류하는 방법은 도 38, 도 39 및 도 41의 실시 예를 참고하도록 한다.

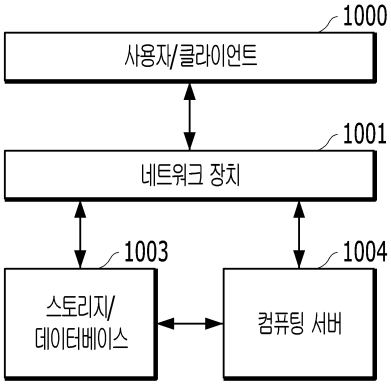
[0427] 단계(S70030)에서, 데이터 관리 방법은 데이터에 포함된 적어도 하나의 정보를 매핑하여 사용자 행위 메타데이터를 생성할 수 있다. 본 발명의 데이터 관리 방법이 사용자 행위 메타데이터를 생성하는 방법은 도 39 및 도 41의 실시 예를 참고하도록 한다.

부호의 설명

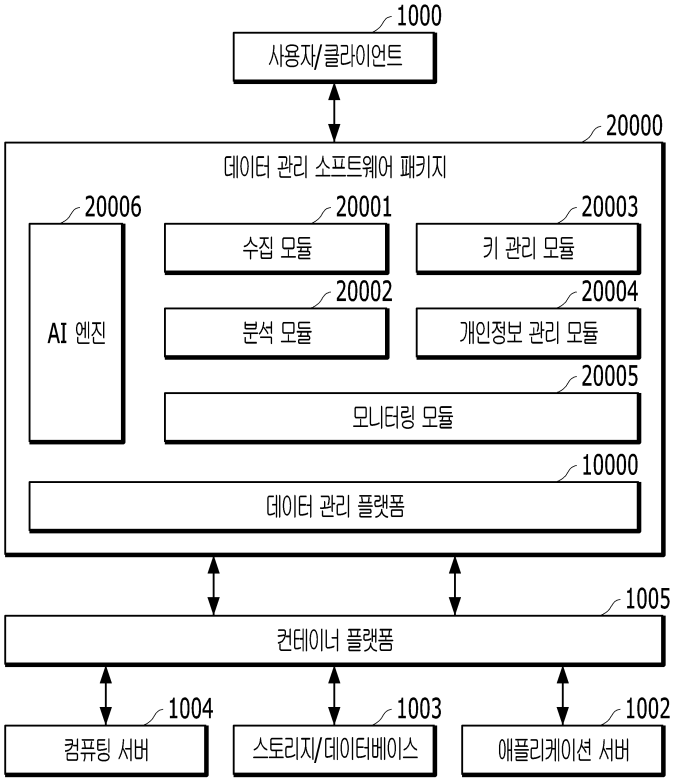
[0429] 10000: 데이터 관리 플랫폼

도면

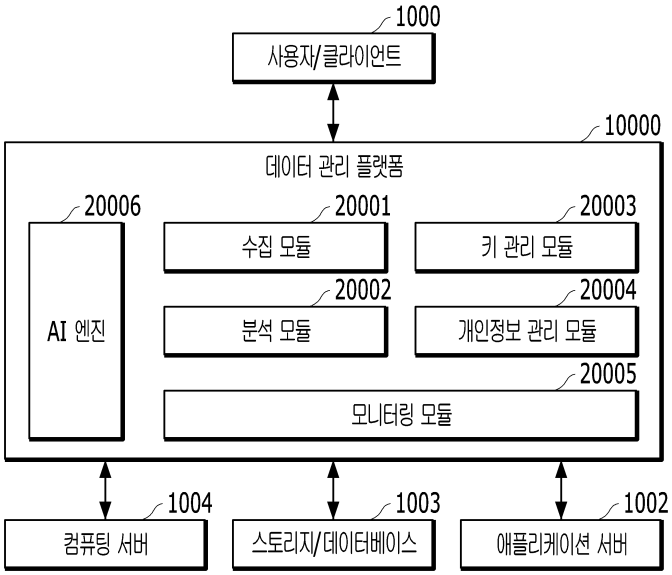
도면1



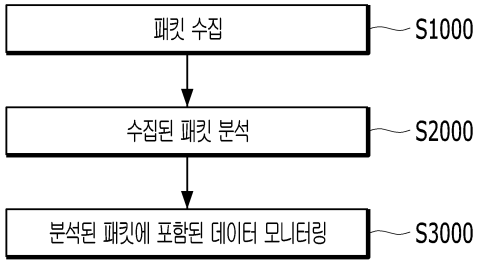
도면2



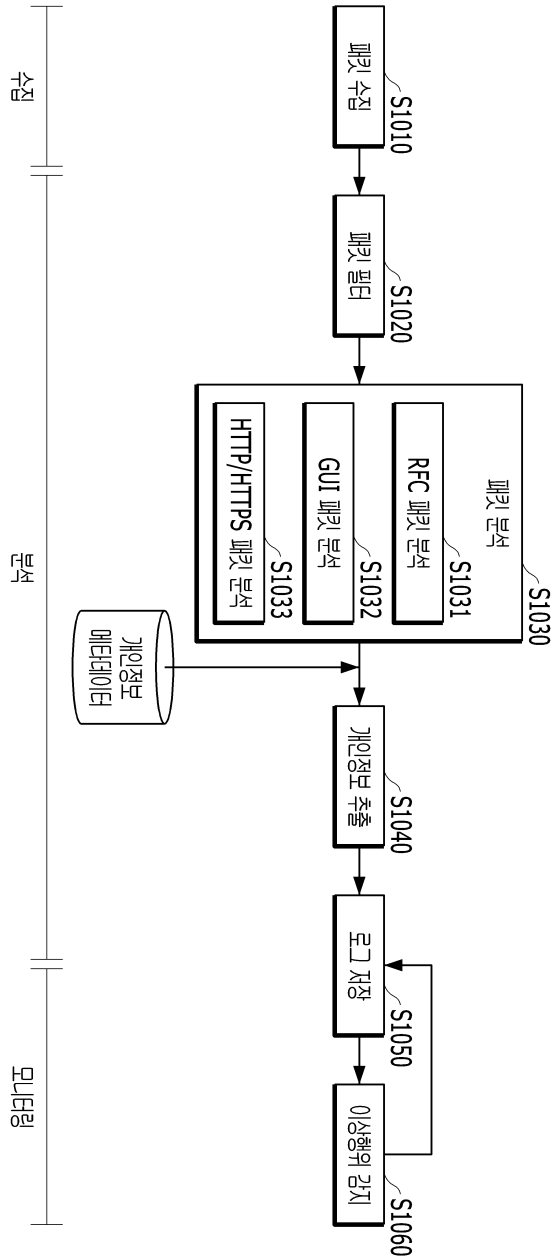
도면3


1000
사용자/클라이언트
10000
데이터 관리 플랫폼
20006
AI 엔진
20001
수집 모듈
20003
키 관리 모듈
20002
분석 모듈
20004
개인정보 관리 모듈
20005
모니터링 모듈
1004
컴퓨팅 서버
1003
스토리지/데이터베이스
1002
애플리케이션 서버

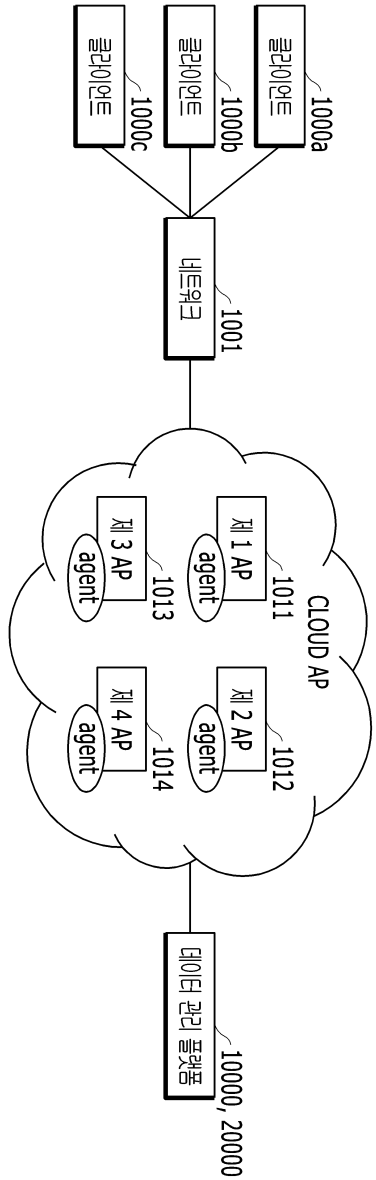
도면4


패킷 수집
S1000
수집된 패킷 분석
S2000
분석된 패킷에 포함된 데이터 모니터링
S3000

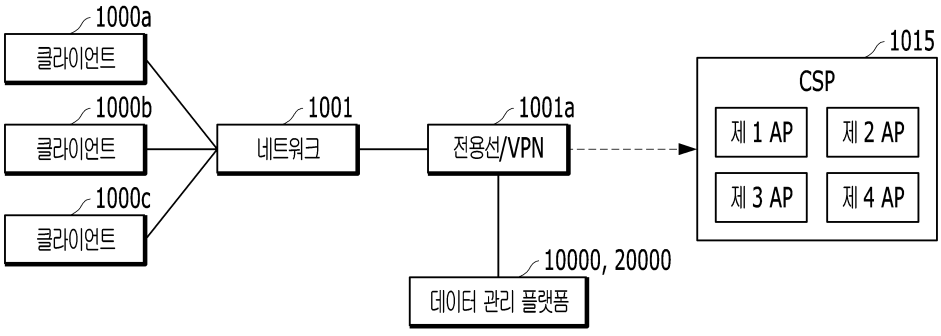
도면5


수집
분석
모니터링
패킷 수집
S1010
패킷 필터
S1020
패킷 분석
S1030
RFC 패킷 분석
S1031
GUI 패킷 분석
S1032
HTTP/HTTPS 패킷 분석
S1033
개인정보 메타데이터
개인정보 추출
S1040
로그 저장
S1050
이상행위 감지
S1060

도면6


클라이언트
1000c
클라이언트
1000b
클라이언트
1000a
네트워크
1001
CLOUD AP
제 3 AP
agent
1013
제 1 AP
agent
1011
제 4 AP
agent
1014
제 2 AP
agent
1012
데이터 관리 플랫폼
10000, 20000

도면7


1000a
클라이언트
1000b
클라이언트
1000c
클라이언트
1001
네트워크
1001a
전용선/VPN
1015
CSP
제 1 AP
제 2 AP
제 3 AP
제 4 AP
10000, 20000
데이터 관리 플랫폼

도면8

요청시간	프로토콜	서버 IP	클라이언트 IP	계정	트랜잭션명	이벤트	개인정보건수	내역
2019-05-07 16:54:14	RFC	175.117.145.57	192.168.0.182	10077	RS_SCRP_GF_PROCESS_640	미지정	9	Instance_name=bobae-PC user_uid=ok_code=dympro_name=alert_level=even t_category=event_count=alert_count=A RCH=SAP REC PERINF=에 PERINF_TYP_C NT=1 OK CODE=user name=미지정 okco
2019-05-07 16:54:11	RFC	175.117.						
2019-05-07 13:52:07	RFC	175.117.						
2019-05-07 13:52:05	RFC	175.117.						
2019-05-07 13:52:03	RFC	175.117.						
2019-05-07 13:51:47	RFC	175.117.						

2019-05-07 16:54:14

닫기 [-]

상세 내용 | 개인 정보 | 화면 재현 | 데이터 | 메시지

Request Screen

CONNECTION_PARAMS	LANGU	DISPLAY	TERMINAL	SYSTEM	USERID	PROTVERS	PROGLENGTH	WDWHANDLE
	Eb	bobae-PC bobae-PC S	41 10077 751 40	331180				

HEADER	PROG	DNUM	TYPE	FNUM	DGRP	BZMX	BZBR	MILL	MICO	MALI	MACO	NOLI	NCCO	VALP	CUAN	HDAT
	YBB_BCALV_GRID_DEMO 0100 0100	G D					20190	507164	747							
	30117192 37 0 0 40122 0															

STATUS_PARAM	ACTIVITY	MODUS	SAVED	NEXT_PREV	SHOWVERS	CUSTOMIZE	EXTEND	EXTENDED	GENERATED	ACTIVE	W899	ACTIVE_WD	FILED_IND
	Dympro STFFFFFATTFullSc	re	en				00	0					

Tables : FIELDS

FELDNAME	INTTYP	FELDFORMAT	LAENGE	FLG1	FLG2	FLG3	FNB1	FNB2	LINE	COLN	LOOPTYPE	LOOPBEGIN	LOOPBLOCK	LOOPREPEAT	FNKY	DI
%#AUTOTEXT001 0CHAR																

Response Screen

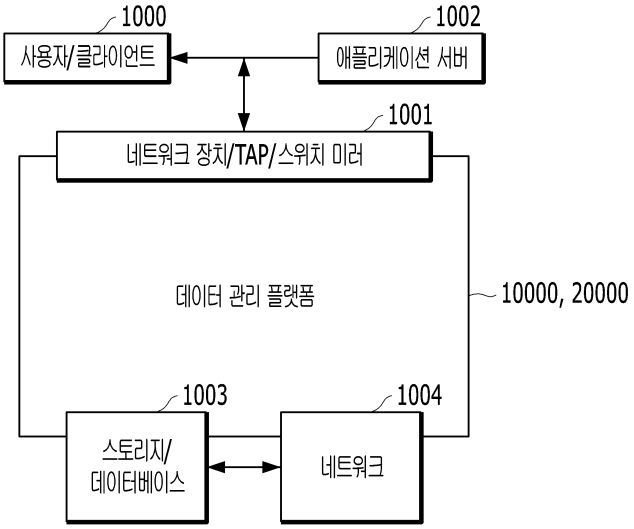
HEADER	PROG	DNUM	TYPE	FNUM	DGRP	BZMX	BZBR	MILL	MICO	MALI	MACO	NOLI	NCCO	VALP	CUAN	HDAT	SPR
	YBB_BCALV_GRID_DEMO 0100 0100	G D					20190	507164	747								
	30117192 37 0 0 40122 0																

STATUS_PARAM	ACTIVITY	MODUS	SAVED	NEXT_PREV	SHOWVERS	CUSTOMIZE	EXTEND	EXTENDED	GENERATED	ACTIVE	W899	ACTIVE_WD	FILED_IND	MES
	RFinish STFFFFFATTFullSc	re	en				00	0						

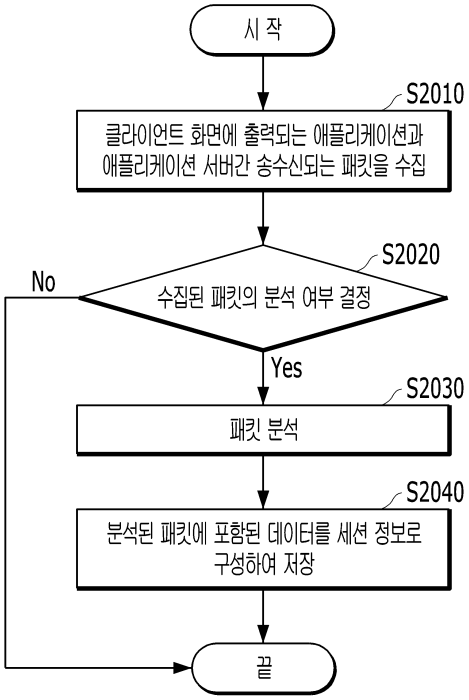
Tables : FIELDS

FELDNAME	INTTYP	FELDFORMAT	LAENGE	FLG1	FLG2	FLG3	FNB1	FNB2	LINE	COLN	LOOPTYPE	LOOPBEGIN	LOOPBLOCK	LOOPREPEAT	FNKY	DI
%#AUTOTEXT001 0CHAR																
2200000003000 3 2 0 0 0 0 0 0																
BCALV_GRID_DEMO_0100_CONT1																
8900300003000 3 2 0 0 0 230 1																

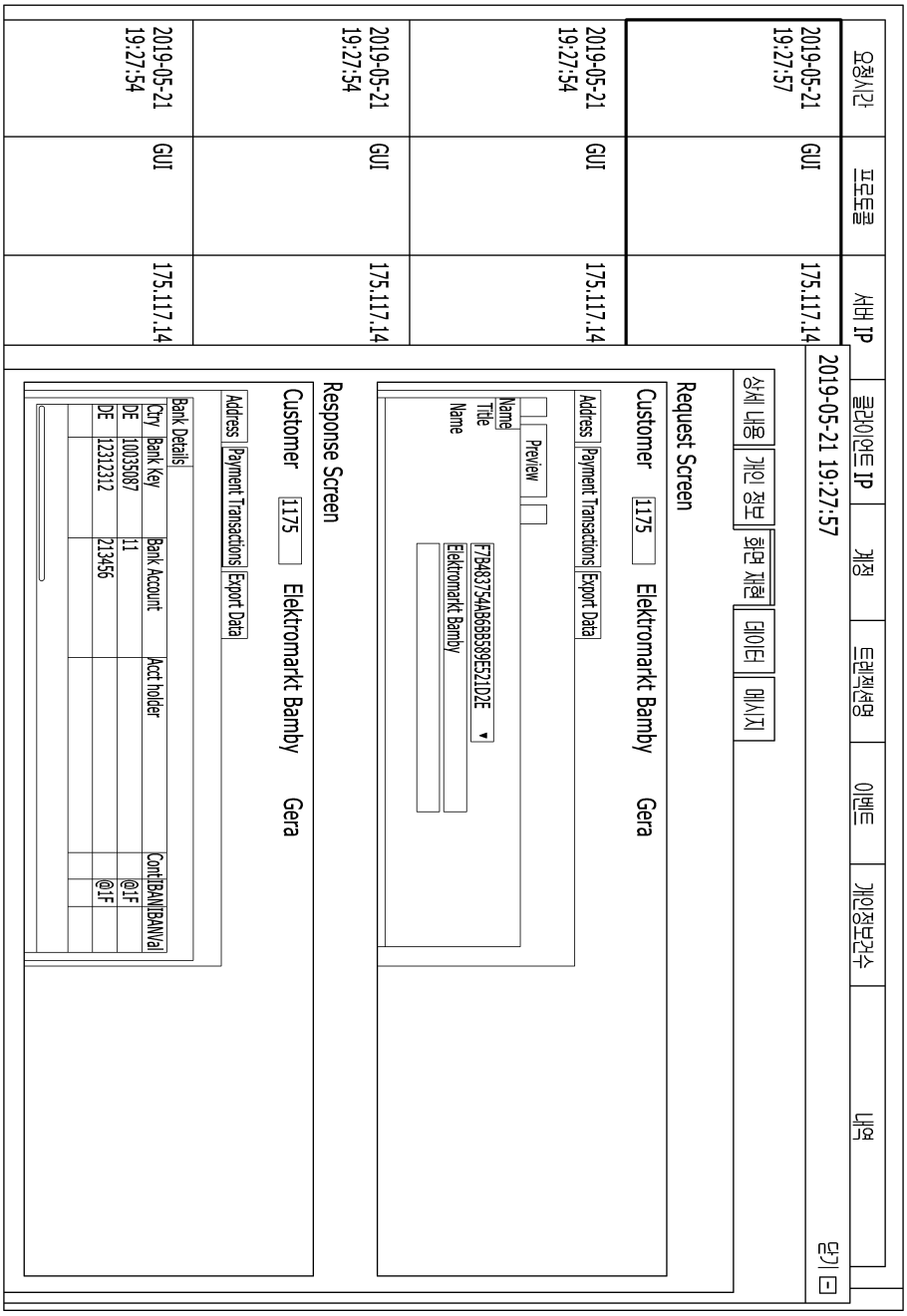
도면9


1000
사용자/클라이언트
1002
애플리케이션 서버
1001
네트워크 장치/TAP/스위치 미러
데이터 관리 플랫폼
10000, 20000
1003
스토리지/
데이터베이스
1004
네트워크

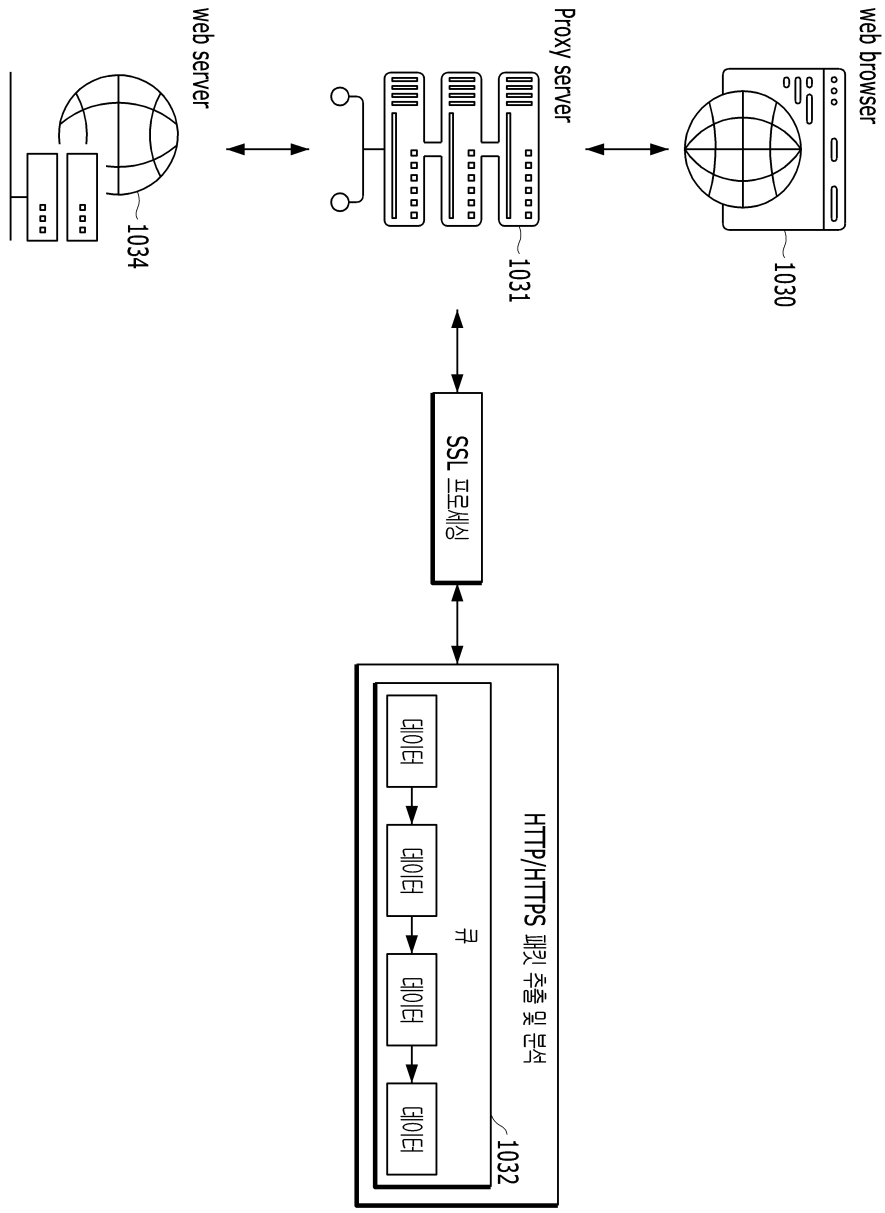
도면10


시 작
S2010
클라이언트 화면에 출력되는 애플리케이션과
애플리케이션 서버간 송수신되는 패킷을 수집
S2020
No
수집된 패킷의 분석 여부 결정
Yes
S2030
패킷 분석
S2040
분석된 패킷에 포함된 데이터를 세션 정보로
구성하여 저장
끝

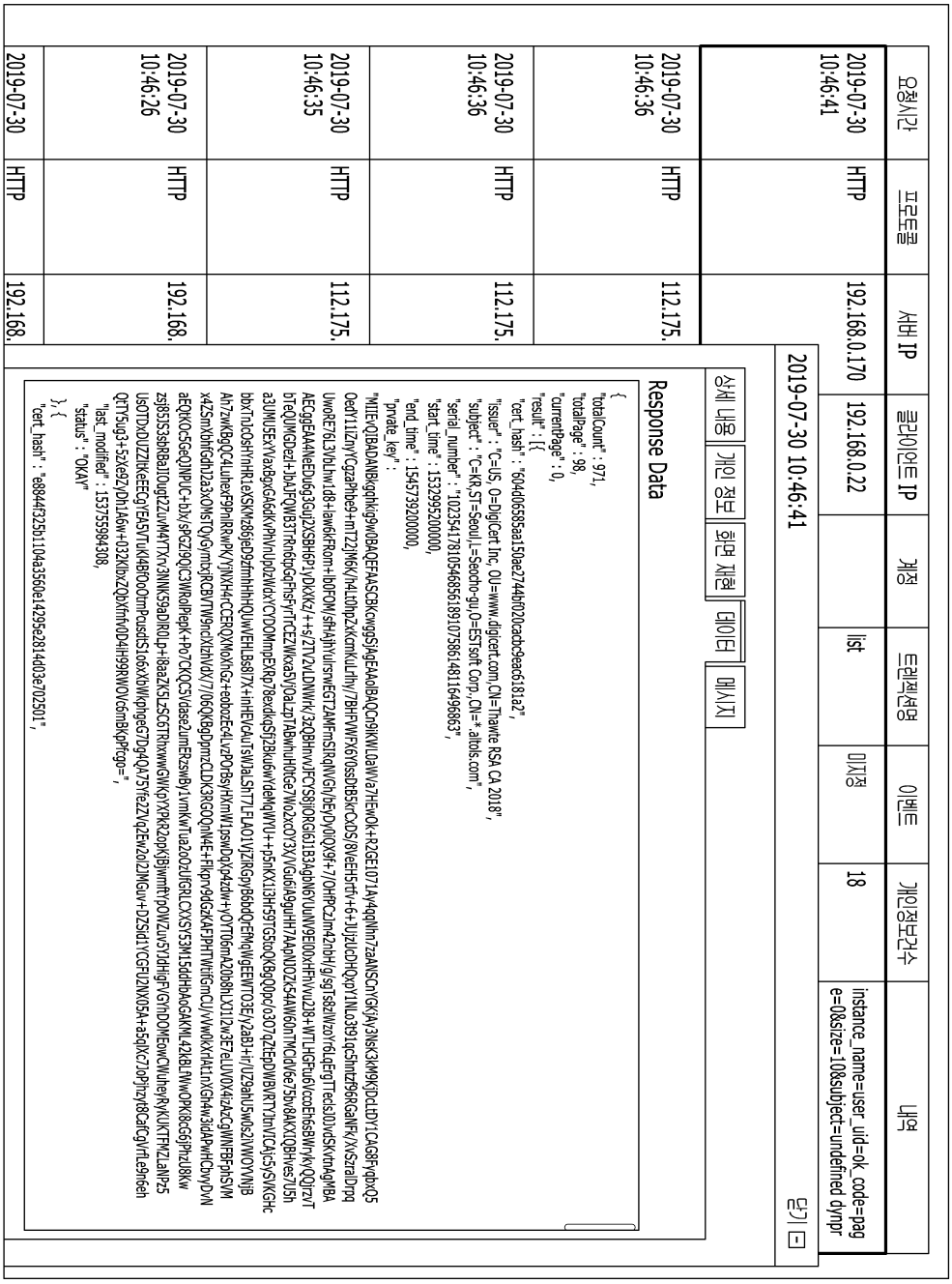
도면11


요청시간
프로토콜
서버 IP
클라이언트 IP
계정
트랜잭션명
이벤트
개인정보검수
내역
2019-05-21 19:27:57
GUI
175.117.14
2019-05-21 19:27:54
GUI
175.117.14
2019-05-21 19:27:54
GUI
175.117.14
2019-05-21 19:27:54
GUI
175.117.14
닫기
상세 내용
개인 정보
화면 재현
데이터
메시지
Request Screen
Customer 1175 Elektromarkt Bamby Gera
Address
Payment Transactions
Export Data
Preview
Name
Title
Name
F7B48375AB6BB589E521D2E
Elektromarkt Bamby
Response Screen
Customer 1175 Elektromarkt Bamby Gera
Address
Payment Transactions
Export Data
Bank Details
Ctry
Bank Key
Bank Account
Acct holder
ContIBANIBANVal
DE
10035087
11
@1JF
DE
12312312
213456
@1JF

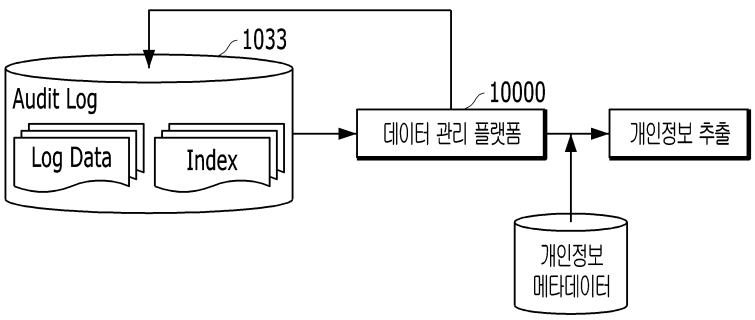
도면12


web server
Proxy server
web browser
1034
1031
1030
SSL 프로세싱
HTTP/HTTPS 패킷 추출 및 분석
데이터
데이터
큐
데이터
데이터
1032

도면13


요청시간
프로토콜
서버 IP
클라이언트 IP
계정
트랜잭션명
이벤트
개인정보건수
내역
2019-07-30 10:46:41
HTTP
192.168.0.170
192.168.0.22
list
18
instance_name=user_uid=ok_code=page=08size=10&subject=undefined dynpr
2019-07-30 10:46:41
닫기
상세 내용
개인 정보
화면 재현
데이터
메시지
Response Data
2019-07-30 10:46:36
HTTP
112.175.
2019-07-30 10:46:35
HTTP
112.175.
2019-07-30 10:46:26
HTTP
192.168.
2019-07-30
HTTP
192.168.

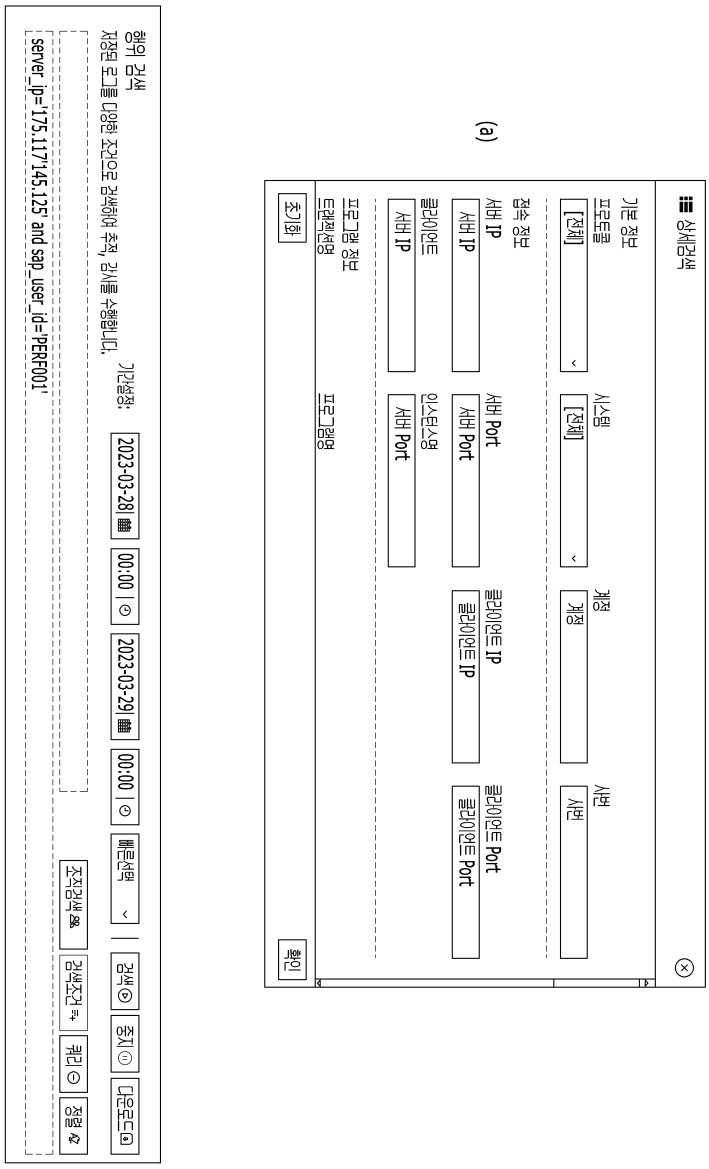
도면14


1033
Audit Log
Log Data
Index
10000
데이터 관리 플랫폼
개인정보 추출
개인정보
메타데이터

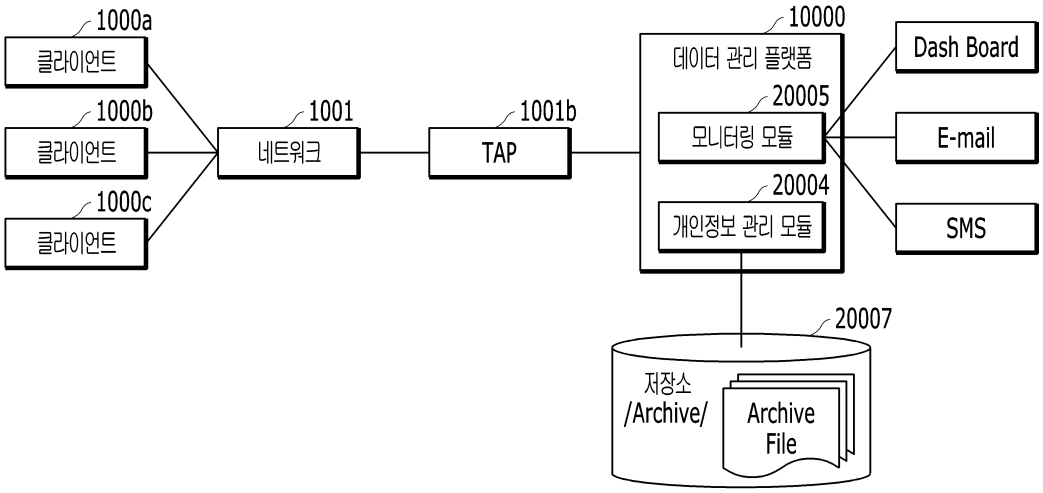
도면15

상세 내용
개인 정보
화면 재현
데이터
메시지
세션 정보
시작 시간: 2019-06-21 14:51:18
Duration Time: 1267 ms
Log ID: 19865976090657136
Session ID: 5a4af8fa-0bc7-476e-aedf-9e162e013f6e
Context ID: 29E893E9227EF181A71D005056C000008
접속 정보
서버 IP: 175.117.145.125
서버 Port: 3201
서버 Mac: 88:36:6C:D6:55:9C
클라이언트 IP: 192.168.0.167
클라이언트 Port: 5951
클라이언트 Mac: 44:8A:5B:40:01:22
SAP 정보
SID: INP
프로토콜: GUI
SAP 인스턴스: inspien02_INP_01
클라이언트: 800
프로그램 정보
OK Code: FN:8
TCode: SE38
Title App: SAP R/3 (1) INP
Title Main: Access Control Demo
Dynpro Name: SAPMSSY0
Dynpro Number: 0120
상세 내용
개인 정보
화면 재현
데이터
메시지
CUA Name: SAPMSSY0
CUA Status: STLI
사용자 정보
사용자 ID: BCADMIN
사용자 UID: BCADMIN
사용자 명: 미지정
이벤트 정보
이벤트 카테고리: Security Action
이벤트 코드: USRDWN
이벤트 이름: 파일 다운로드
이벤트 설명: 사용자 다운로드
이벤트 값: BCADMIN
알림 수준: Warning
사용자 정의 정보
이벤트: 파일 다운로드
경고: WARN
이벤트유형: SECACT
이벤트 건수: 1
경고 건수: 1
아키텍쳐: SAP GUI
개인정보존재: 예
개인정보유형건수: 2
개인정보건수: 6
주민번호(요청):
주민번호(응답): 700610-1020977, 701228-1044041, 770620-1234567

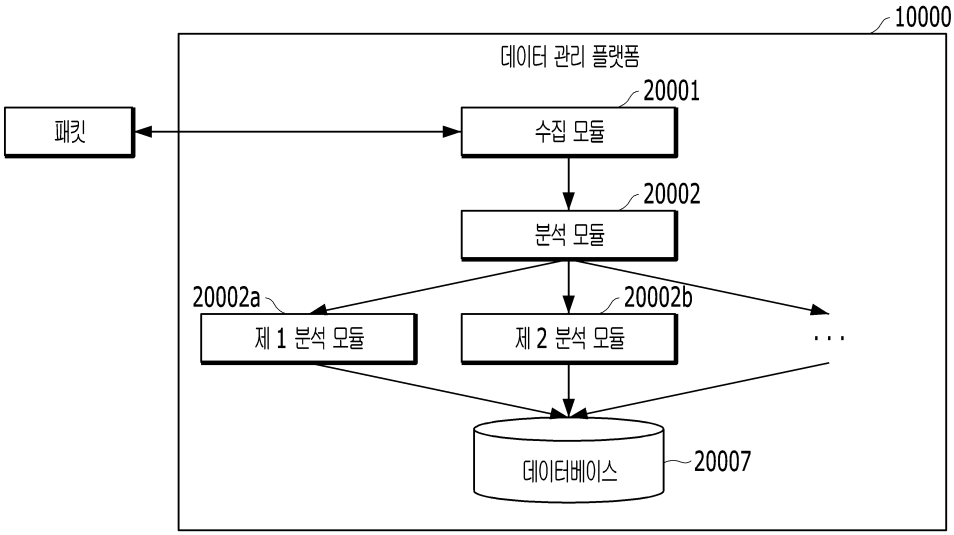
도면16


(a)
상세검색
기본 정보
프로토콜
[전체]
시스템
[전체]
계정
계정
사번
사번
접속 정보
서버 IP
서버 IP
서버 Port
서버 Port
클라이언트 IP
클라이언트 IP
클라이언트 Port
클라이언트 Port
인스턴스명
서버 IP
서버 Port
프로그램 정보
트랜잭션명
프로그램명
초기화
확인
(b)
헤더 검색
저장된 로그를 다양한 조건으로 검색하여 추적, 감시를 수행합니다.
기간설정:
2023-03-28
00:00
2023-03-29
00:00
빠른선택
검색
중지
다운로드
조건검색 On
검색조건 1
쿼리
정렬
server_ip='175.117.145.125' and sap_user_id='PERF001'

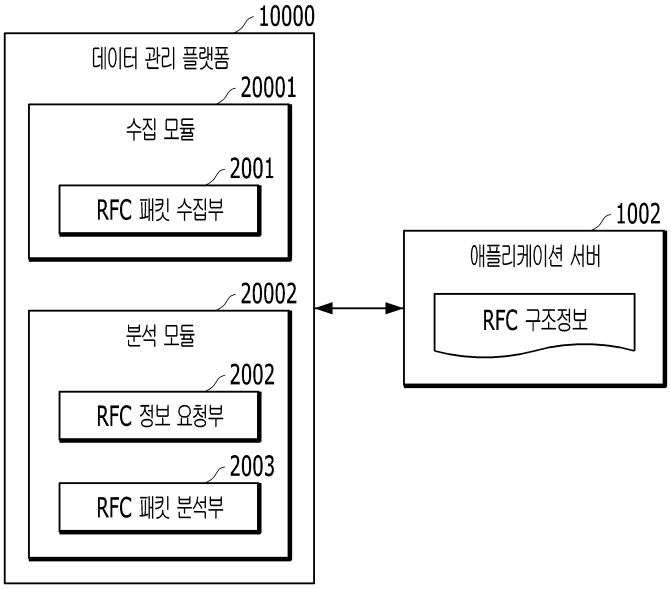
도면17


1000a
클라이언트
1000b
클라이언트
1000c
클라이언트
1001
네트워크
1001b
TAP
10000
데이터 관리 플랫폼
20005
모니터링 모듈
20004
개인정보 관리 모듈
Dash Board
E-mail
SMS
20007
저장소
/Archive/
Archive
File

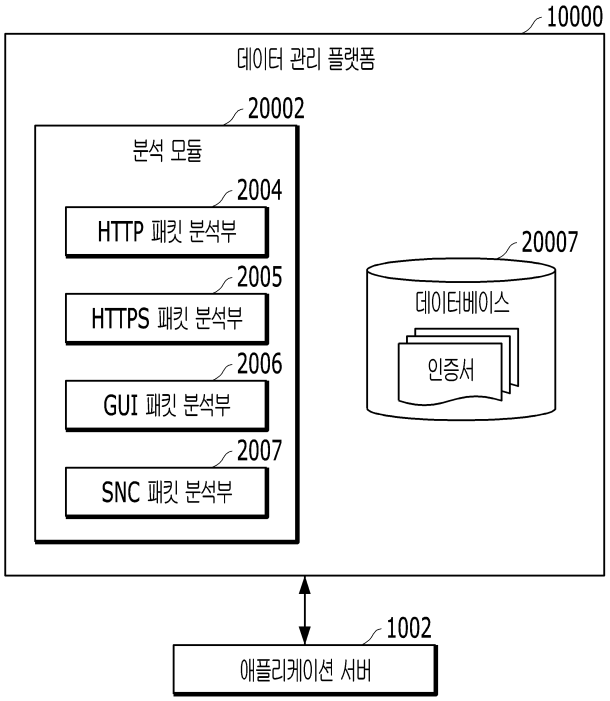
도면18


10000
데이터 관리 플랫폼
패킷
20001
수집 모듈
20002
분석 모듈
20002a
제 1 분석 모듈
20002b
제 2 분석 모듈
...
데이터베이스
20007

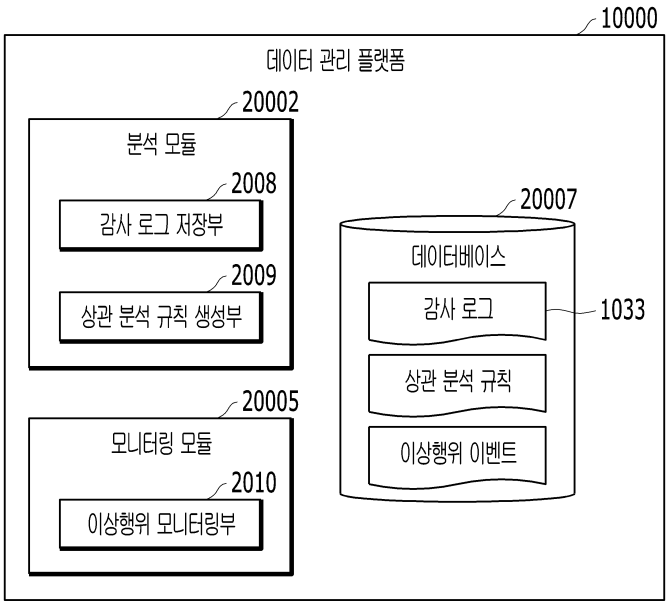
도면19


10000
데이터 관리 플랫폼
20001
수집 모듈
2001
RFC 패킷 수집부
20002
분석 모듈
2002
RFC 정보 요청부
2003
RFC 패킷 분석부
1002
애플리케이션 서버
RFC 구조정보

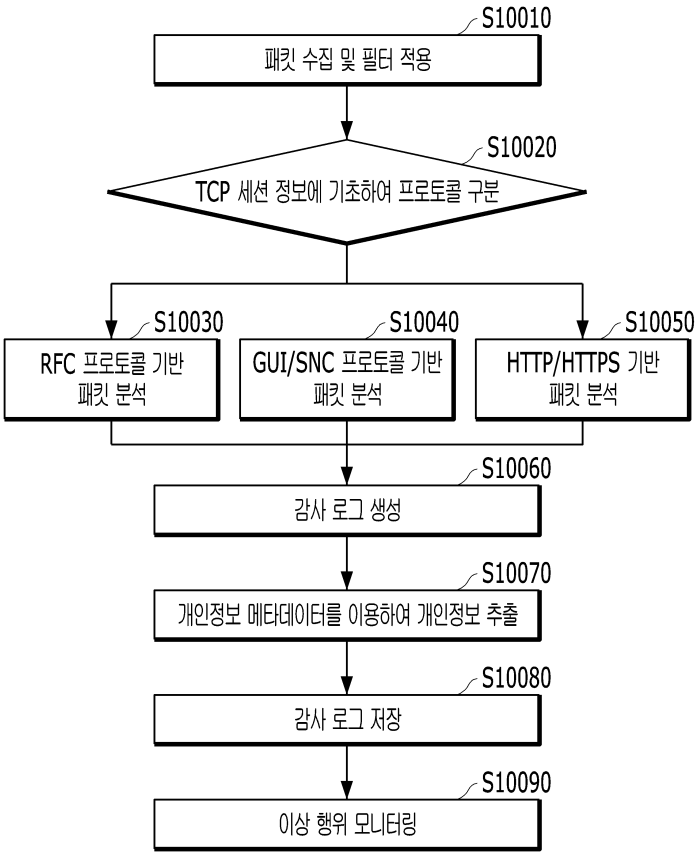
도면20


10000
데이터 관리 플랫폼
20002
분석 모듈
2004
HTTP 패킷 분석부
2005
HTTPS 패킷 분석부
2006
GUI 패킷 분석부
2007
SNC 패킷 분석부
20007
데이터베이스
인증서
1002
애플리케이션 서버

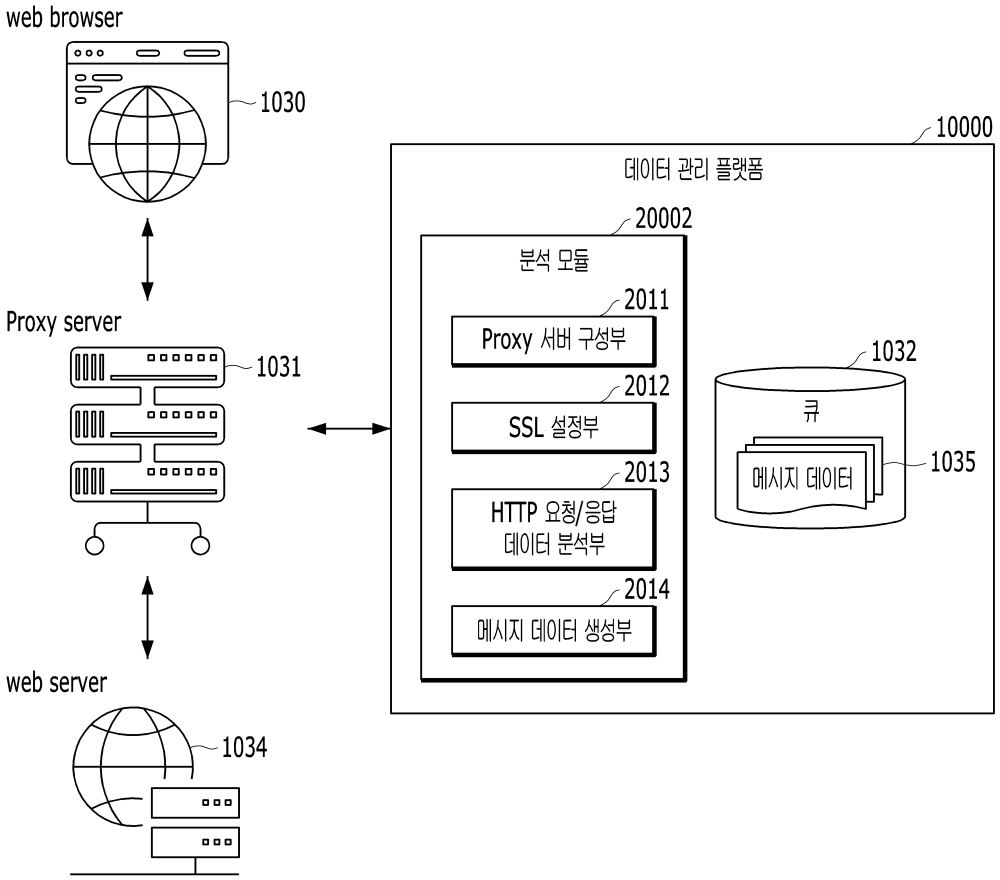
도면21


10000
데이터 관리 플랫폼
20002
분석 모듈
2008
감사 로그 저장부
2009
상관 분석 규칙 생성부
20005
모니터링 모듈
2010
이상행위 모니터링부
20007
데이터베이스
감사 로그
1033
상관 분석 규칙
이상행위 이벤트

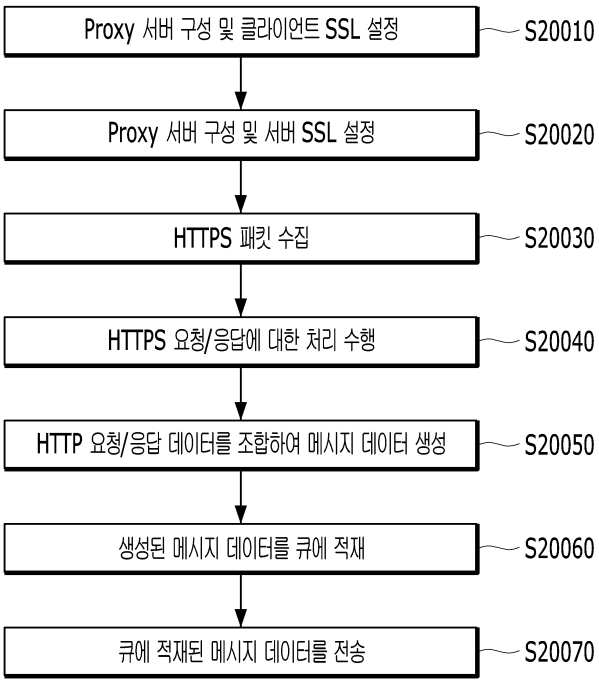
도면22


S10010
패킷 수집 및 필터 적용
S10020
TCP 세션 정보에 기초하여 프로토콜 구분
S10030
RFC 프로토콜 기반 패킷 분석
S10040
GUI/SNC 프로토콜 기반 패킷 분석
S10050
HTTP/HTTPS 기반 패킷 분석
S10060
감사 로그 생성
S10070
개인정보 메타데이터를 이용하여 개인정보 추출
S10080
감사 로그 저장
S10090
이상 행위 모니터링

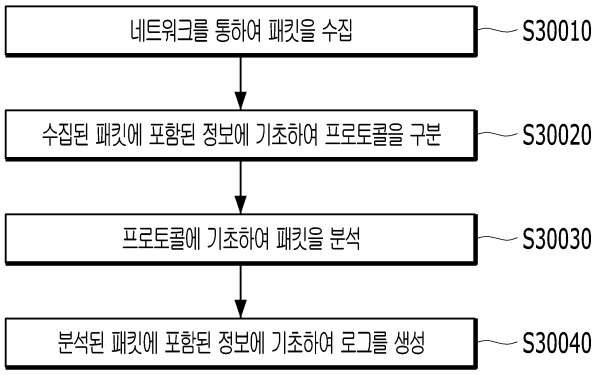
도면23


web browser
1030
10000
데이터 관리 플랫폼
20002
분석 모듈
2011
Proxy 서버 구성부
2012
SSL 설정부
2013
HTTP 요청/응답
데이터 분석부
2014
메시지 데이터 생성부
1032
큐
메시지 데이터
1035
Proxy server
1031
web server
1034

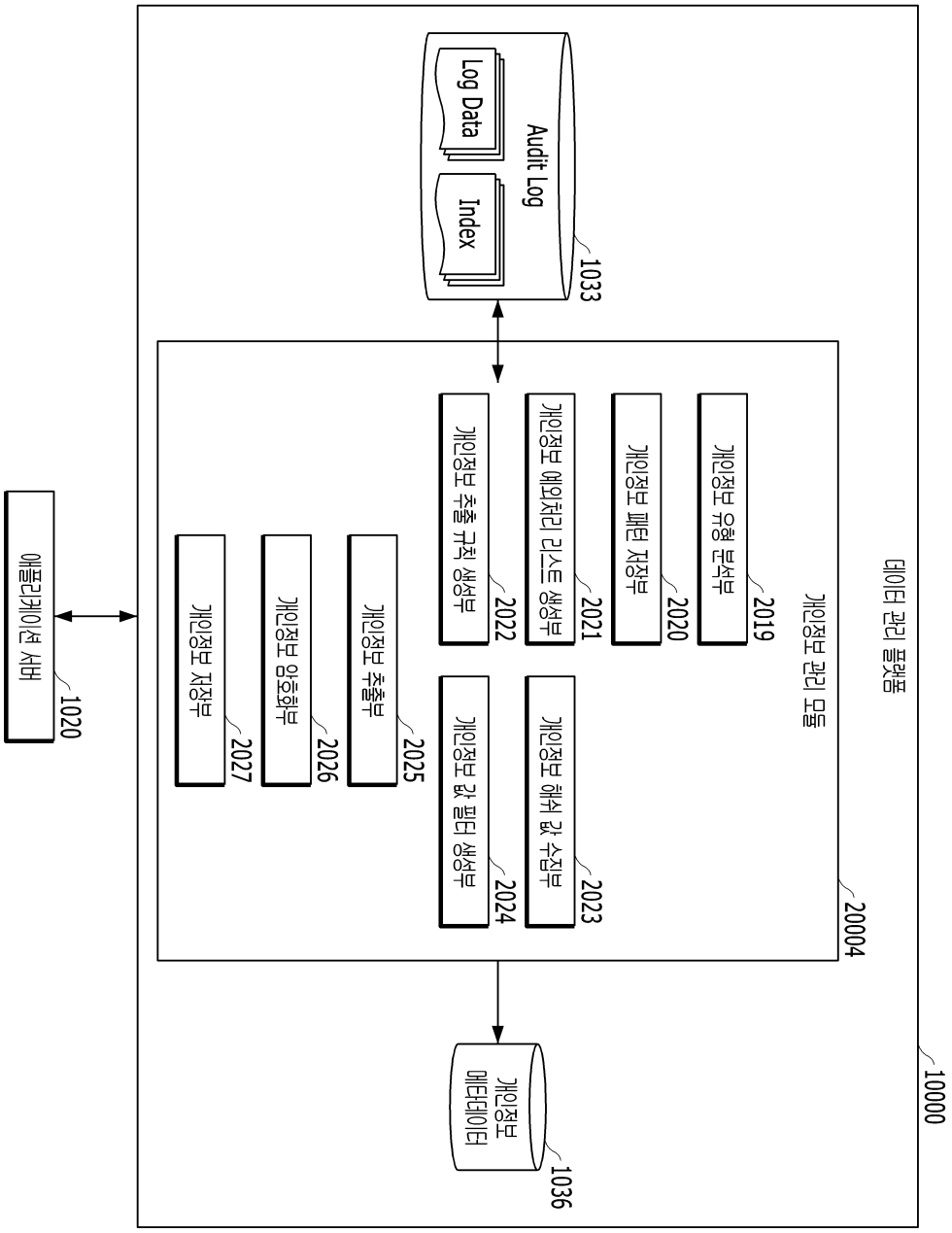
도면24


Proxy 서버 구성 및 클라이언트 SSL 설정
S20010
Proxy 서버 구성 및 서버 SSL 설정
S20020
HTTPS 패킷 수집
S20030
HTTPS 요청/응답에 대한 처리 수행
S20040
HTTP 요청/응답 데이터를 조합하여 메시지 데이터 생성
S20050
생성된 메시지 데이터를 큐에 적재
S20060
큐에 적재된 메시지 데이터를 전송
S20070

도면25


네트워크를 통하여 패킷을 수집
S30010
수집된 패킷에 포함된 정보에 기초하여 프로토콜을 구분
S30020
프로토콜에 기초하여 패킷을 분석
S30030
분석된 패킷에 포함된 정보에 기초하여 로그를 생성
S30040

도면26


데이터 관리 플랫폼
10000
Audit Log
Log Data
Index
1033
개인정보 관리 모듈
20004
개인정보 유형 분석부
2019
개인정보 패턴 저장부
2020
개인정보 예외처리 리스트 생성부
2021
개인정보 추출 규칙 생성부
2022
개인정보 해쉬 값 수집부
2023
개인정보 값 필터 생성부
2024
개인정보 추출부
2025
개인정보 암호화부
2026
개인정보 저장부
2027
개인정보 메타데이터
1036
애플리케이션 서버
1020

도면27

<정규식 패턴>

개인정보	정규식
주민등록번호	(\d{6}[,-]-?[1-4]\d{6})|(\d{6}[,-]?[1-4])
운전면허번호	(\d{2}-\d{2}-\d{6}-\d{2})
전화번호	(\d{2,3}[,-]-?\d{2,4}[,-]-?\d{4})
메일주소	(([\w!-_\.])*@([\w!-_\.])*\.[\w]{2,3})
주소	(([가-힣]+(\d{1,5}|\d{1,5}(,|.)\d{1,5}|)+(읍|면|동|개리))(^구|)((\d{1,5}(~|-)\d{1,5}|\d{1,5})(개리)|))([](산(\d{1,5}(~|-)\d{1,5}|\d{1,5}))|)|(([가-힣]|(\d{1,5}(~|-)\d{1,5})|\d{1,5})+(로|길)))
생년월일	(\d{0,4}(년생|월생|세|살))
여권번호	([a-zA-Z]{1}|[a-zA-Z]{2})\d{8}
계좌번호	([0-9,\-]{3,6}\-[0-9,\-]{2,6}\-[0-9,\-])
신용카드번호	34569][0-9]{3}[-~.[ ]][0-9]{4}[-~.[ ]][0-9]{4}[-~.[ ]][0--9]{4}
건강보험번호	[1257][-~.[:space:]][0-9]{10}
외국인등록번호	([01][0-9]{5}[[:space:]~-]+[1-8][0-9]{6}|[2-9][0-9]{5}[[:space:]~-]+[1256][0-9]{6})

도면28

<마스킹 패턴>

개인정보	마스킹 처리 규칙	마스킹 패턴
주민등록번호	R/(\d{2}(0[1-9]|1[0-2])(0[1-9]|[12]\d|3[0-1])-?[1-4]\d{6})/$1******	901214-2******
운전면허번호	R/(.+)[\d-]{4}/$1****	13111234****
전화번호	R/(02|[3456]\d{1,2}|14[6-9]|15[5-9])-?[0-9]{3,4}-?)[0-9]{4}/$1****	02-3695-****
휴대폰번호	R/(01[0167]89)-?[0-9]{3,4}-?)[0-9]{4}/$1****	010-8574-****
메일주소	R/[0-9a-zA-Z_-]{3}([0-9a-zA-Z_-]+@[0-9a-zA-Z_-]+(\.[a-zA-Z0-9]+){1,2})/***$1	***spo@naver.com
여권번호	R/([a-zA-Z\d]{2}\d{7})/**$1	**3457821
계좌번호	R/([\d-]+)[\d-]{4}/$1****	1002034014****
신용카드번호	R/[\d-]{8}(.+)/*********$1	********43142548
건강보험번호	R/([\d-]{8})\d{4}/$1****	13452587****
외국인등록번호	R/(\d{2}(0[1-9]|1[0-2])(0[1-9]|[12]\d|3[0-1])-?[5-8]\d{6})/$1******	890514-5******

도면29

1036

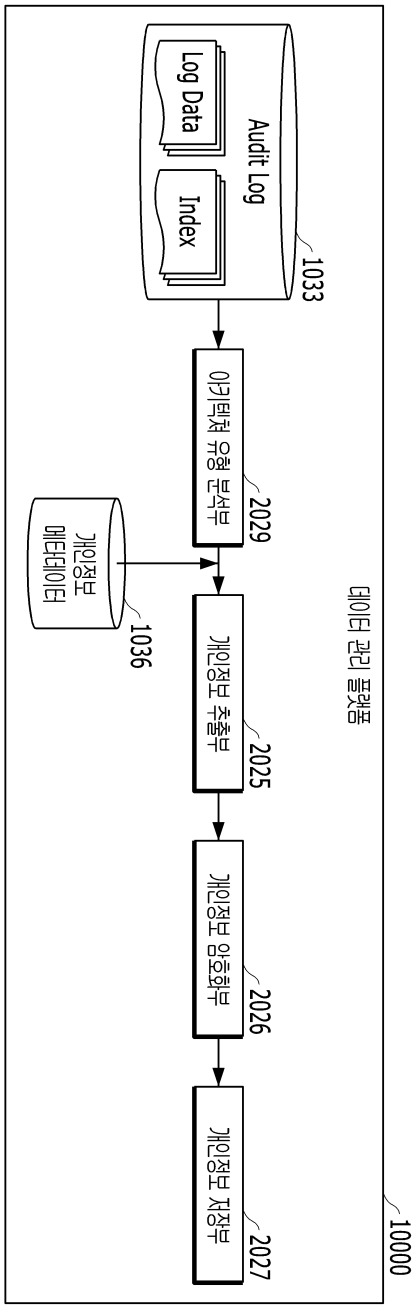
<개인정보 메타 데이터>

아키텍처 유형	화면 정보(level1)	화면 정보(level2)	개인정보 추출 규칙
SAPGUI	SE11	---	
WEBGUI	---	---	

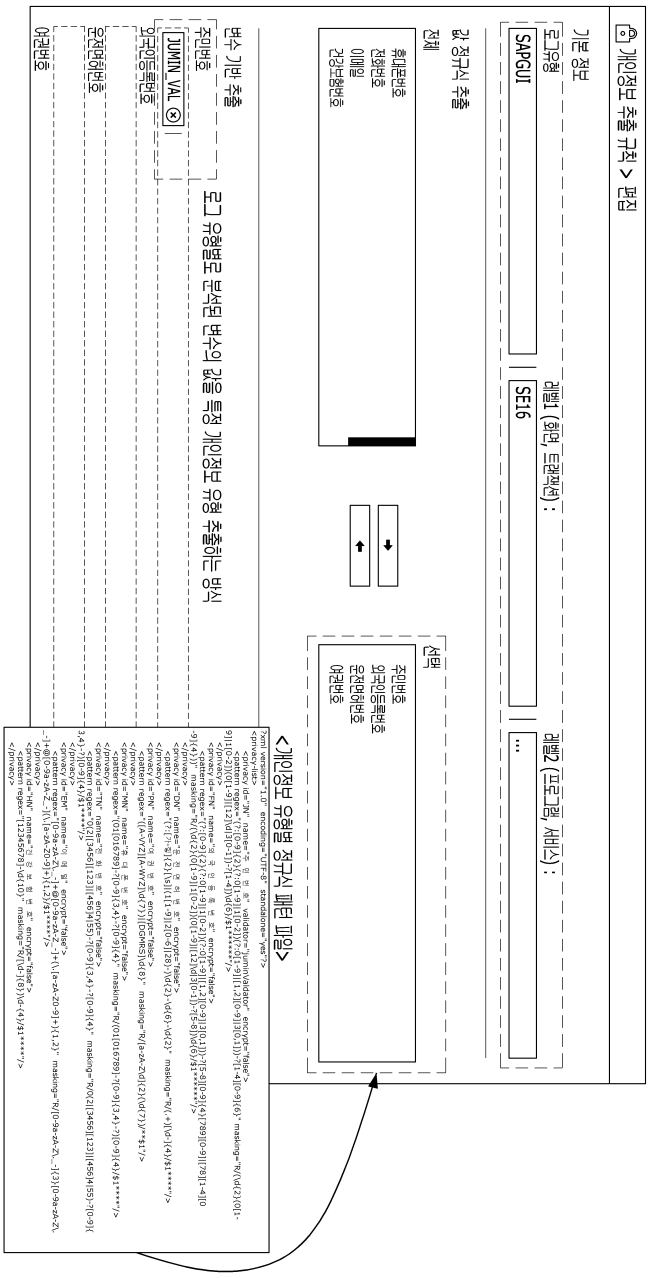
<개인정보 추출 규칙>

추출 방식	값
value-match (값 추출 방식)	개인정보 유형 리스트
variable-match (변수 추출 방식)	개인정보 유형 + 변수 명 리스트
value-content-match (값 컨텐츠 추출 방식)	개인정보 유형 리스트
content-match (전문 정규식 추출 방식)	개인정보 유형 + 패턴 리스트
composite (복합 개인정보 추출 방식)	개인정보 유형 리스트

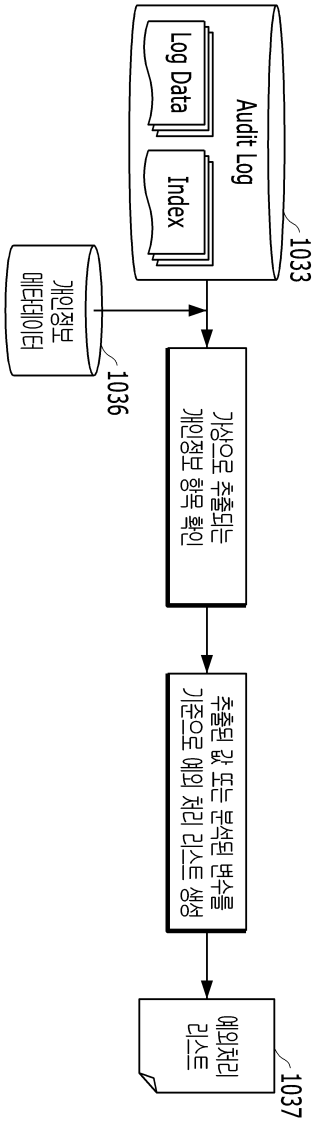
도면30


Audit Log
Log Data
Index
1033
아키텍처 유형 분석부
2029
개인정보 메타데이터
1036
개인정보 추출부
2025
개인정보 암호화부
2026
개인정보 저장부
2027
데이터 관리 플랫폼
10000

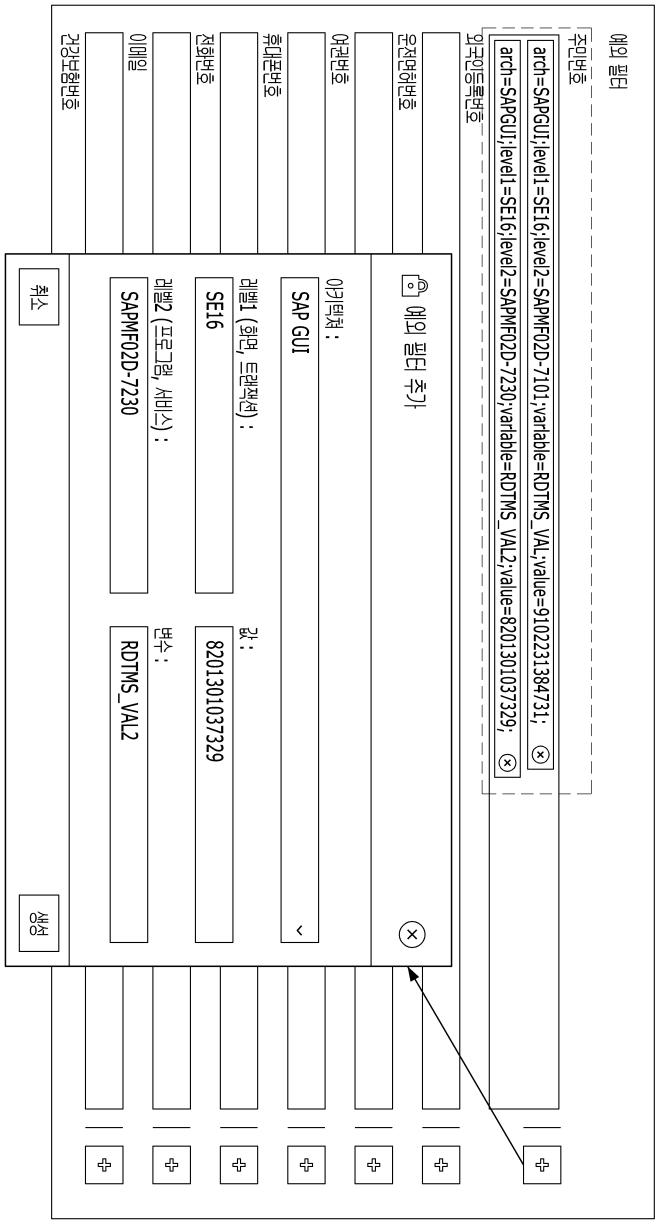
도면31


개인정보 추출 규칙 > 편집
기본 정보
로그유형
SAPGUI
테이블(헤더, 크레딧) :
SE16
테이블2(로그, 서비스) :
...
값 정규식 추출
전체
휴대폰번호
전화번호
이메일
건강보험번호
선택
주민번호
외국인등록번호
운전면허번호
여권번호
변수 기반 추출
로그 유형별로 분석된 변수의 값을 특정 개인정보 유형 추출하는 방식
주민번호
JUMIN_VAL
외국인등록번호
운전면허번호
여권번호
<개인정보 유형별 정규식 패턴 파일>

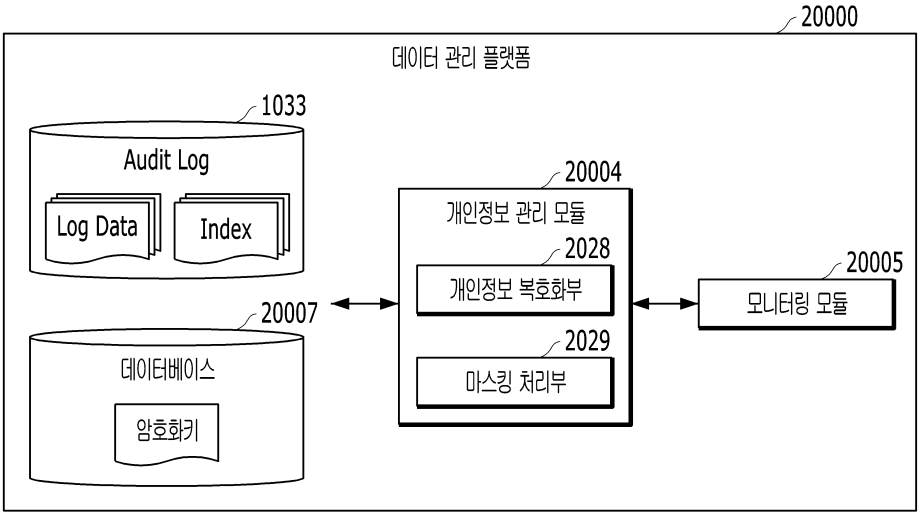
도면32


Audit Log
Log Data
Index
1033
개인정보
메타데이터
1036
가상으로 추출되는
개인정보 항목 확인
추출된 값 또는 분석된 변수를
기준으로 예외 처리 리스트 생성
예외처리
리스트
1037

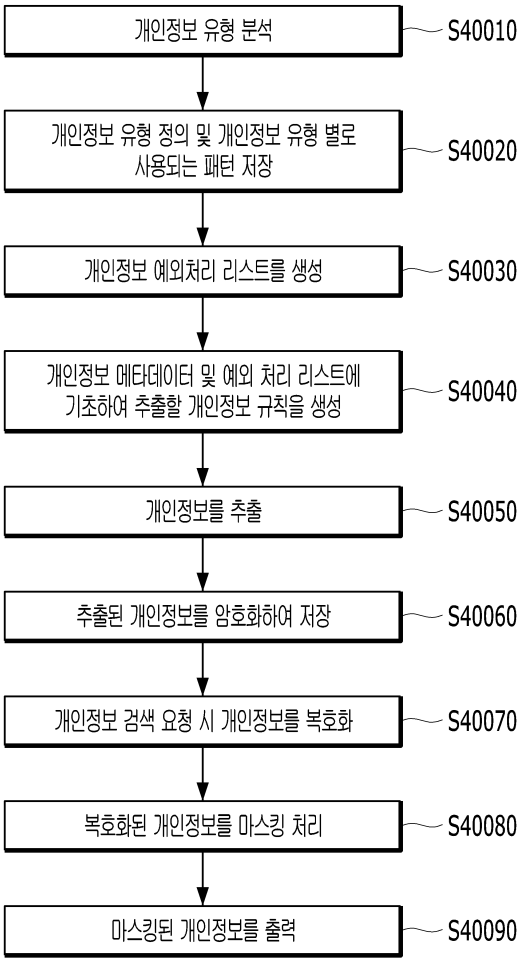
도면33


예외 필터
주민번호
arch=SAPGUI;level1=SE16;level2=SAPMF02D-7101;variable=RDTMS_VAL;value=9102231384731;
arch=SAPGUI;level1=SE16;level2=SAPMF02D-7230;variable=RDTMS_VAL2;value=8201301037329;
외국인등록번호
운전면허번호
여권번호
휴대폰번호
전화번호
이메일
건강보험번호
예외 필터 추가
아키텍쳐 :
SAP GUI
레벨1 (화면, 트랜잭션) :
SE16
값 :
8201301037329
레벨2 (프로그램, 서비스) :
SAPMF02D-7230
변수 :
RDTMS_VAL2
취소
생성

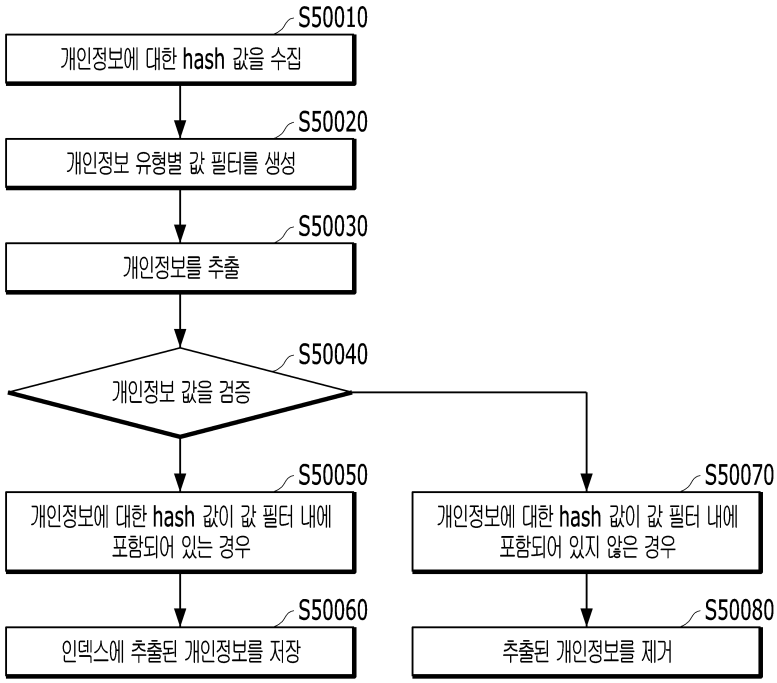
도면34


20000
데이터 관리 플랫폼
1033
Audit Log
Log Data
Index
20004
개인정보 관리 모듈
2028
개인정보 복호화부
2029
마스킹 처리부
20005
모니터링 모듈
20007
데이터베이스
암호화키

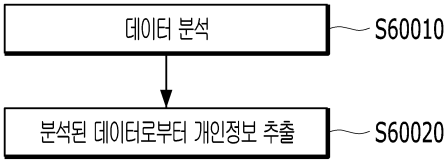
도면35


개인정보 유형 분석
S40010
개인정보 유형 정의 및 개인정보 유형 별로 사용되는 패턴 저장
S40020
개인정보 예외처리 리스트를 생성
S40030
개인정보 메타데이터 및 예외 처리 리스트에 기초하여 추출할 개인정보 규칙을 생성
S40040
개인정보를 추출
S40050
추출된 개인정보를 암호화하여 저장
S40060
개인정보 검색 요청 시 개인정보를 복호화
S40070
복호화된 개인정보를 마스킹 처리
S40080
마스킹된 개인정보를 출력
S40090

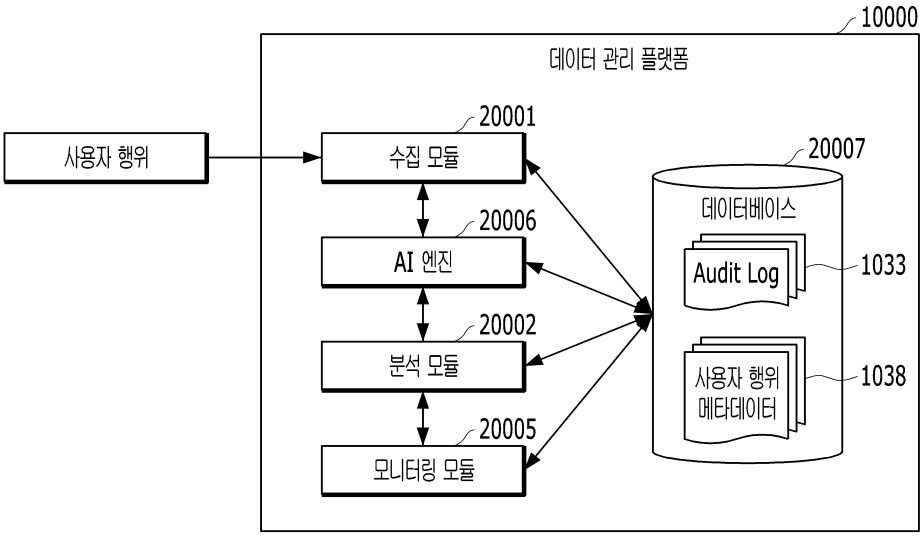
도면36



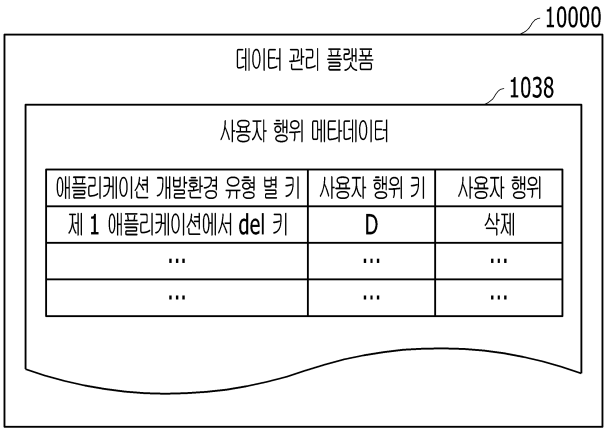
도면37



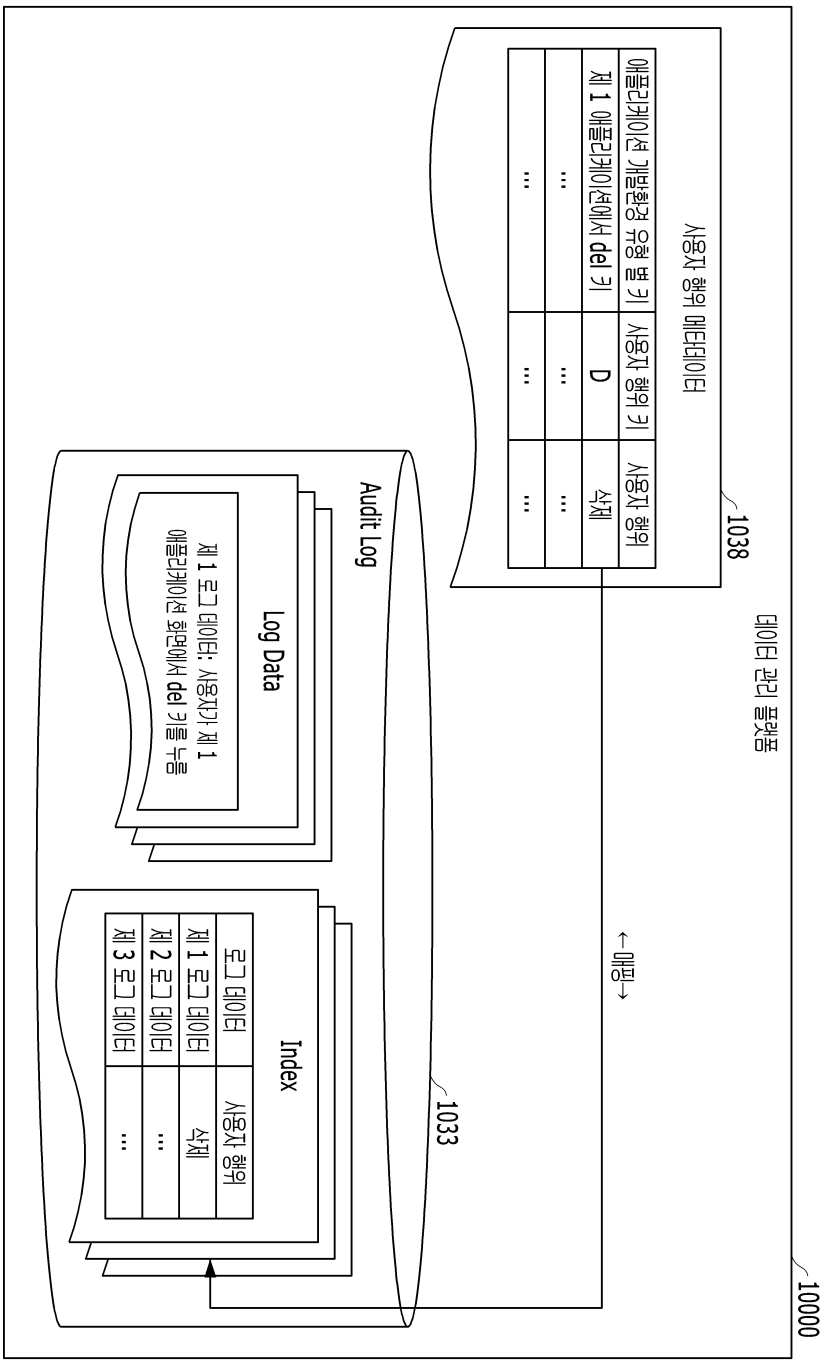
도면38



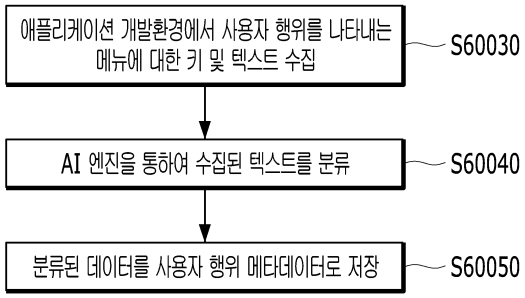
도면39


10000
데이터 관리 플랫폼
1038
사용자 행위 메타데이터
애플리케이션 개발환경 유형 별 키
사용자 행위 키
사용자 행위
제 1 애플리케이션에서 del 키
D
삭제
…
…
…
…
…
…

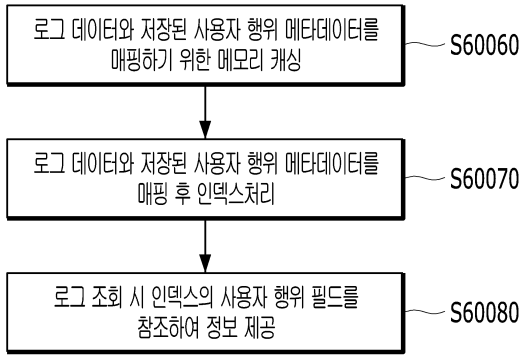
도면40


10000
데이터 관리 플랫폼
1038
사용자 행위 메타데이터
애플리케이션 개발환경 유형 별 키
사용자 행위 키
사용자 행위
제 1 애플리케이션에서 del 키
D
삭제
1033
Audit Log
Log Data
제 1 로그 데이터: 사용자가 제 1 애플리케이션 화면에서 del 키를 누름
Index
로그 데이터
사용자 행위
제 1 로그 데이터
삭제
제 2 로그 데이터
제 3 로그 데이터
← 매핑 →

도면41



도면42



도면43