(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년12월28일
(11) 등록번호 10-1580425
(24) 등록일자 2015년12월18일

(51) 국제특허분류(Int. Cl.)
G06F 21/12 (2013.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
G06F 21/121 (2013.01)
H04L 9/32 (2013.01)
(21) 출원번호 10-2015-0002945
(22) 출원일자 2015년01월08일
심사청구일자 2015년01월08일
(30) 우선권주장
1020140166360 2014년11월26일 대한민국(KR)
(56) 선행기술조사문헌
KR1020140089321 A*
KR1020140090408 A*
*는 심사관에 의하여 인용된 문헌
기술이전 희망 : **기술양도, 실시권허여, 기술지도**

(73) 특허권자
숭실대학교산학협력단
서울특별시 동작구 상도로 369 (상도동)
(72) 발명자
이정현
경기 성남시 분당구 수내로 148, 109동 603호 (수내동, 파크타운서안아파트)
(74) 대리인
특허법인태백

전체 청구항 수 : 총 6 항 심사관 : 문남두

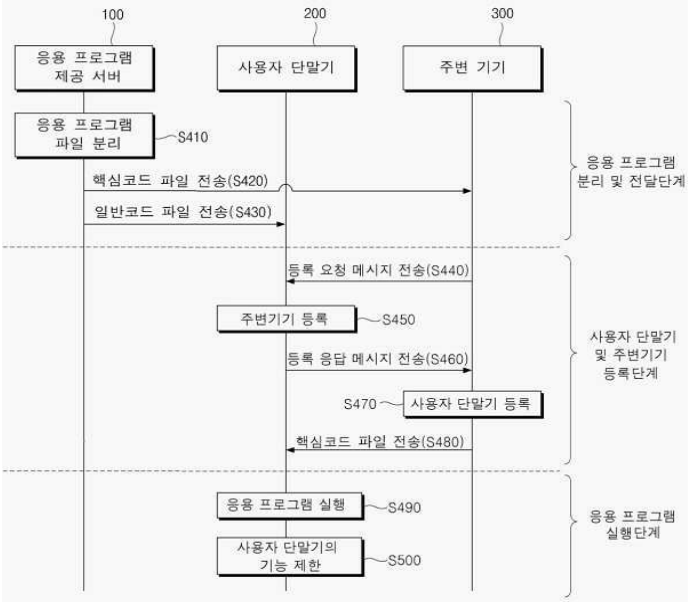
(54) 발명의 명칭 **주변기기와 연동하는 사용자 단말기 및 그것을 이용한 정보 유출 방지 방법**

(57) 요 약

본 발명은 주변기기와 연동하는 사용자 단말기 및 그것을 이용한 정보 유출 방지 방법에 관한 것으로, 본 발명의 일 실시예에 따른 정보 유출을 방지하기 위한 사용자 단말기는 응용 프로그램 제공 서버로부터 상기 응용 프로그램의 일반코드를 수신하여 설치하는 통신부, 상기 응용 프로그램의 핵심코드를 저장한 주변기기로부터 상기 주변

(뒷면에 계속)

대 표 도 - 도4



기기의 고유정보가 포함된 등록요청 메시지를 수신하여 상기 주변기기를 인증하고, 상기 주변기기로 사용자 단말기의 고유정보가 포함된 등록 응답 메시지를 전송하며, 상기 주변기기로부터 상기 응용 프로그램의 상기 핵심코드를 수신하는 인증부, 상기 일반코드 및 상기 핵심코드를 이용하여, 상기 응용 프로그램을 실행시키는 실행부, 그리고 상기 응용 프로그램이 실행되는 동안에는 상기 사용자 단말기의 일부 기능을 제한하도록 제어하는 제어부를 포함한다.

이와 같이 본 발명에 의하면, 정보 유출 수단으로 사용될 위험이 있는 사용자 단말기의 기능을 제한함으로써, 기업 또는 조직의 정보를 보호하고, 기밀 유출을 방지할 수 있다.

이 발명을 지원한 국가연구개발사업
과제고유번호 C0247329
부처명 중소기업청
연구관리전문기관 한국산학연협회
연구사업명 산학연협력 기술개발사업(연구마을)
연구과제명 실행코드 분리 기반 Portable MDM 기술 개발
기 여 율 1/3
주관기관 숭실대학교 산학협력단
연구기간 2014.11.01 ~ 2015.10.31
이 발명을 지원한 국가연구개발사업
과제고유번호 NRF-2013R1A1A2013041
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 일반연구자지원사업
연구과제명 암호 난독화 기반 APK 위변조 탐지 기술 개발
기 여 율 1/3
주관기관 숭실대학교 산학협력단
연구기간 2013.06.01 ~ 2016.05.31
이 발명을 지원한 국가연구개발사업
과제고유번호 NRF-2014K1A1A2043029
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 글로벌연구실(GRL)사업
연구과제명 모바일 시스템 소프트웨어 보안기술 개발
기 여 율 1/3
주관기관 숭실대학교 산학협력단
연구기간 2014.08.01 ~ 2020.07.31

명 세 서

청구범위

청구항 1

응용 프로그램 제공 서버로부터 상기 응용 프로그램의 일반코드를 수신하여 설치하는 통신부,

상기 응용 프로그램의 핵심코드를 저장한 주변기기로부터 상기 주변기기의 고유정보가 포함된 등록요청 메시지를 수신하여 상기 주변기기를 인증하고, 상기 주변기기로 사용자 단말기의 고유정보가 포함된 등록 응답 메시지를 전송하며, 상기 주변기기로부터 상기 응용 프로그램의 상기 핵심코드를 수신하는 인증부,

상기 일반코드 및 상기 핵심코드를 이용하여, 상기 응용 프로그램을 실행시키는 실행부, 그리고

상기 응용 프로그램이 실행되는 동안에는 상기 사용자 단말기의 일부 기능을 제한하도록 제어하는 제어부를 포함하며,

상기 응용 프로그램 제공 서버는 상기 응용 프로그램으로부터 상기 핵심코드를 설정하고, 상기 응용 프로그램에서 상기 핵심코드를 삭제하여 상기 일반코드를 생성하며,

상기 사용자 단말기의 고유정보는 국제모바일기기 식별정보(IMEI; International Mobile Equipment Identity), ANDROID_ID, 시리얼 번호, 휴대폰 번호, 모델 번호, MAC 주소 중에서 적어도 하나를 포함하는 사용자 단말기.

청구항 2

제1항에 있어서,

상기 응용 프로그램은,

전사적자원관리(ERP), 기업정보포털(EIP), 기업애플리케이션통합(EAI), 그룹웨어(groupware), 지식관리시스템(KMS) 중에서 적어도 하나를 포함하는 사용자 단말기.

청구항 3

제1항에 있어서,

상기 제어부는,

상기 사용자 단말기의 통신 기능, 촬영 기능, 녹음 기능, 저장 기능, 파일 전송 기능, GPS 기능 중에서 적어도 하나의 기능을 제한하는 사용자 단말기.

청구항 4

삭제

청구항 5

사용자 단말기를 이용한 정보 유출 방지 방법에 있어서,

상기 사용자 단말기는, 응용 프로그램 제공 서버로부터 상기 응용 프로그램의 일반코드를 수신하여 설치하는 단계,

상기 응용 프로그램의 핵심코드를 저장한 주변기기로부터 상기 주변기기의 고유정보가 포함된 등록요청 메시지를 수신하여 상기 주변기기를 인증하는 단계,

상기 주변기기로 상기 사용자 단말기의 고유정보가 포함된 등록 응답 메시지를 전송하는 단계,

상기 주변기기로부터 상기 응용 프로그램의 상기 핵심코드를 수신하는 단계,

상기 일반코드 및 상기 핵심코드를 이용하여, 상기 응용 프로그램을 실행시키는 단계, 그리고

상기 응용 프로그램이 실행되는 동안에는 상기 사용자 단말기의 일부 기능을 제한하도록 제어하는 단계를 포함

하며,

상기 응용 프로그램 제공 서버는 상기 응용 프로그램으로부터 상기 핵심코드를 설정하고, 상기 응용 프로그램에서 상기 핵심코드를 삭제하여 상기 일반코드를 생성하며,

상기 사용자 단말기의 고유정보는 국제모바일기기 식별정보(IMEI; International Mobile Equipment Identity), ANDROID_ID, 시리얼 번호, 휴대폰 번호, 모델 번호, MAC 주소 중에서 적어도 하나를 포함하는 정보 유출 방지 방법.

청구항 6

제5항에 있어서,

상기 응용 프로그램은,

전사적자원관리(ERP), 기업정보포털(EIP), 기업애플리케이션통합(EAI), 그룹웨어(groupware), 지식관리시스템(KMS) 중에서 적어도 하나를 포함하는 정보 유출 방지 방법.

청구항 7

제5항에 있어서,

상기 사용자 단말기의 일부 기능을 제한하도록 제어하는 단계는,

상기 사용자 단말기의 통신 기능, 촬영 기능, 녹음 기능, 저장 기능, 파일 전송 기능, GPS 기능 중에서 적어도 하나의 기능을 제한하는 정보 유출 방지 방법.

청구항 8

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 주변기기와 연동하는 사용자 단말기 및 그것을 이용한 정보 유출 방지 방법에 관한 것으로서, 더욱 상세하게는 사내 또는 조직에 반입된 단말기를 통한 내부 정보 유출을 방지할 수 있는 주변기기와 연동하는 사용자 단말기 및 그것을 이용한 정보 유출 방지 방법에 관한 것이다.

배 경 기 술

[0002] 기업이 자사의 기밀정보 및 주요정보를 보호하기 위하여 많은 노력과 비용을 투자하고 있다. 기업의 기밀정보가 유출되는 사례는 크게 외부 침입으로 인한 유출과 내부 사용자에 의한 유출로 나뉘어진다. 초기에는 해킹이나 바이러스와 같은 외부침입에 의한 기밀정보 유출이 많이 발생하였다. 그러나 IT환경이 복잡해지고, 보안 사고의 유형이 지능화됨에 따라 내부자에 의한 정보유출이 크게 증가하였다.

[0003] 각 기업의 보안담당자들은 자사 IT 인프라의 보안성 향상을 위하여 보안 장비를 구매하고, 보안 관제 서비스를 이용하며, 디지털저작관리(DRM), 데이터유출방지(DLP) 솔루션을 적용하고 있다.

[0004] 여기서, 디지털저작관리(DRM, Digital Rights Management)는 디지털 콘텐츠의 불법 복제와 변조를 방지하여 제공자의 권리와 이익을 보호해주는 기술과 서비스를 의미한다. 그리고 데이터유출방지(DLP, Data Loss Prevention)는 기업 내부자의 고의나 실수로 인한 외부로의 정보 유출을 방지하는 솔루션을 의미한다. 데이터유출방지(DLP) 솔루션을 적용하여 사내에서 주고받는 데이터를 내용 또는 형식을 기준으로 탐지하여 중요 정보 유출을 차단할 수 있다.

[0005] 그리고 사내에 반입된 직원 또는 방문객의 사용자 단말기를 통한 정보 유출을 예방하기 위한 솔루션을 적용하는 기업도 많아졌다. 무선 인터넷과 모바일 기기의 발달로 인하여 BYOD(Bring Your Own Device)를 도입하는 기업이 증가하고 있다. 이에 따라 많은 기업에서 사내에 반입된 사용자 단말기에 대한 접근제어를 위하여 유무선네트워크 접근관리(WNAC)솔루션을 도입하고 있다.

[0006] 유무선네트워크접근관리(WNAC)는 사내 네트워크에 접근하는 모든 단말기의 상태를 검사하여 안전이 확보된 단말

기만 접근이 가능하도록 허용한다. 유무선네트워크접근관리(WNAC)는 단독으로 운영되거나, 백신, 디지털저작관리(DRM), 데이터유출방지(DLP)와 같은 다른 보안 솔루션과 결합된 형태로 운영되기도 한다.

[0007] 그러나 이러한 종래의 솔루션은 보안 정책 집행을 위하여 사용자 단말기에 설치된 관리 프로그램을 통합 관리하기 위한 관리 서버를 필요로 하며, 관리의 대상이 되는 모든 단말기는 항상 네트워크를 통하여 관리 서버와 통신을 해야만 한다. 관리 프로그램과 관리 서버가 정상적으로 통신을 수행하지 못하는 경우, 관리의 대상이 되지 않는 장소인지 여부에 따라 사용자 단말기에 설치된 해당 관리 프로그램의 동작여부가 결정되지 못하는 오작동이 많이 발생한다.

[0008] 본 발명의 배경이 되는 기술은 한국등록특허 제10-1392116호 (2014.05.07 공고)에 개시되어 있다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 주변기기와 연동하는 사용자 단말기 및 그것을 이용한 정보 유출 방지 방법에 관한 것으로서, 더욱 상세하게는 사내 또는 조직에 반입된 단말기를 통한 내부 정보 유출을 방지할 수 있는 주변기기와 연동하는 사용자 단말기 및 그것을 이용한 정보 유출 방지 방법을 제공하는데 목적이 있다.

과제의 해결 수단

[0010] 이러한 기술적 과제를 이루기 위한 본 발명의 실시예에 따른 정보 유출을 방지하기 위한 사용자 단말기는, 응용 프로그램 제공 서버로부터 상기 응용 프로그램의 일반코드를 수신하여 설치하는 통신부, 상기 응용 프로그램의 핵심코드를 저장한 주변기기로부터 상기 주변기기의 고유정보가 포함된 등록요청 메시지를 수신하여 상기 주변기기를 인증하고, 상기 주변기기로 사용자 단말기의 고유정보가 포함된 등록 응답 메시지를 전송하며, 상기 주변기기로부터 상기 응용 프로그램의 상기 핵심코드를 수신하는 인증부, 상기 일반코드 및 상기 핵심코드를 이용하여, 상기 응용 프로그램을 실행시키는 실행부, 그리고 상기 응용 프로그램이 실행되는 동안에는 상기 사용자 단말기의 일부 기능을 제한하도록 제어하는 제어부를 포함한다.

[0011] 또한, 상기 응용 프로그램은, 전사적자원관리(ERP), 기업정보포털(EIP), 기업애플리케이션통합(EAI), 그룹웨어(Groupware), 지식관리시스템(KMS) 중에서 적어도 하나를 포함할 수 있다.

[0012] 또한, 상기 제어부는, 상기 사용자 단말기의 통신 기능, 촬영 기능, 녹음 기능, 저장 기능, 파일 전송 기능, GPS 기능 중에서 적어도 하나의 기능을 제한할 수 있다.

[0013] 또한, 상기 사용자 단말기의 고유정보는 국제모바일기기 식별정보(IMEI; International Mobile Equipment Identity), ANDROID_ID, 시리얼 번호, 휴대폰 번호, 모델 번호, MAC 주소 중에서 적어도 하나를 포함할 수 있다.

[0014] 본 발명의 다른 실시예에 따른 주변기기와 연동하는 사용자 단말기를 이용하여 정보 유출을 방지하기 위한 방법에 있어서 상기 사용자 단말기는, 응용 프로그램 제공 서버로부터 상기 응용 프로그램의 일반코드를 수신하여 설치하는 단계, 상기 응용 프로그램의 핵심코드를 저장한 주변기기로부터 상기 주변기기의 고유정보가 포함된 등록요청 메시지를 수신하여 상기 주변기기를 인증하는 단계, 상기 주변기기로 상기 사용자 단말기의 고유정보가 포함된 등록 응답 메시지를 전송하는 단계, 상기 주변기기로부터 상기 응용 프로그램의 상기 핵심코드를 수신하는 단계, 상기 일반코드 및 상기 핵심코드를 이용하여, 상기 응용 프로그램을 실행시키는 단계, 그리고 상기 응용 프로그램이 실행되는 동안에는 상기 사용자 단말기의 일부 기능을 제한하도록 제어하는 단계를 포함한다.

발명의 효과

[0015] 따라서 본 발명에 따르면 정보 유출 수단으로 사용될 위험이 있는 사용자 단말기의 기능을 제한함으로써, 기업 또는 조직의 정보를 보호하고, 기밀 유출을 방지할 수 있다.

[0016] 또한 서버가 아닌 주변기기를 이용하여 사내에 반입된 사용자 단말기를 관리하므로 사내 단말기 관리 시스템의 오작동을 방지할 수 있고, 사용자가 사내 단말기 관리 시스템의 작동 여부를 직관적으로 확인할 수 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 실시예에 따른 정보 유출 방지 시스템을 나타내는 구성도이다.

도 2는 본 발명의 실시예에 따른 사용자 단말기의 구성을 나타낸 블록도이다.

도 3은 본 발명의 실시예에 따른 주변기기의 구성을 나타낸 블록도이다.

도 4는 본 발명의 실시예에 따른 정보 유출을 방지하는 방법을 설명하기 위한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 그러면 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0019] 이하 첨부된 도면을 참조하면서 본 발명에 따른 바람직한 실시예를 상세히 설명하기로 한다.

[0020] 도 1은 본 발명의 실시예에 따른 정보 유출 방지 시스템을 나타내는 구성도이다. 도 1과 같이 본 발명의 실시예에 따른 정보 유출 방지 시스템은 응용 프로그램 제공 서버(100), 사용자 단말기(200) 및 주변기기(300)를 포함한다.

[0021] 도 1에 나타낸 것처럼, 응용 프로그램 제공 서버(100), 사용자 단말기(200) 및 주변기기(300)는 네트워크(network)를 통해 연결된다. 즉, 도 1과 같이, 네트워크를 통하여 사용자 단말기(200)는 응용 프로그램 제공 서버(100) 및 주변기기(300)와 연결되며, 주변기기(300)는 응용 프로그램 제공 서버(100)와 네트워크를 통하여 연결된다.

[0022] 여기서, 네트워크는 사용자 단말들 및 서버들과 같은 각각의 노드 상호 간에 정보 교환이 가능한 연결 구조를 의미하는 것으로, 이러한 네트워크의 일 예는, 인터넷(Internet), LAN(Local Area Network), Wireless LAN(Wireless Local Area Network), WAN(Wide Area Network), PAN(Personal Area Network), 3G, 4G, Wi-Fi 등이 포함되나 이에 한정되지는 않는다.

[0023] 특히, 사용자 단말기(200)와 주변기기(300)는 블루투스(Bluetooth), 지그비(ZigBee), 적외선통신모듈(IrDA, Infrared Data Association) 등을 이용하여 무선 연결될 수 있으며, 유선으로 연결될 수도 있다.

[0024] 먼저, 응용 프로그램 제공 서버(100)는 응용 프로그램의 핵심코드 파일 및 일반코드 파일을 각각 주변기기(300) 및 사용자 단말기(200)로 전송하여 해당 응용 프로그램 파일을 배포한다.

[0025] 여기서 응용 프로그램은 전사적자원관리(ERP), 기업정보포털(EIP), 기업애플리케이션통합(EAI), 그룹웨어(Groupware), 지식관리시스템(KMS) 중에서 어느 하나의 기능을 수행하는 응용 프로그램일 수 있다.

[0026] 응용 프로그램 제공 서버(100)는 응용 프로그램 패키지로부터 디컴파일된 실행 파일을 통하여 핵심코드를 설정할 수 있다. 그리고 응용 프로그램 제공 서버(100)는 응용 프로그램 파일 중에서 핵심코드를 제거하여 일반코드 파일을 생성한다. 이때, 일반코드 파일과 핵심코드 파일은 각각 사용자 단말기(200)와 주변기기(300)에 설치되어 실행될 수 있는 파일 형태일 수 있다.

[0027] 그리고 본 발명의 실시예에 따른 응용 프로그램 제공 서버(100)는 회사의 업무 수행에 필요한 각종 응용 프로그램의 일반코드 파일 및 핵심코드 파일을 저장하며, 사용자 단말기(200) 및 주변기기(300)가 이러한 응용 프로그램의 일반코드 파일 및 핵심코드 파일을 응용 프로그램 제공 서버(100)로부터 다운로드 받아 설치할 수 있도록 한다.

[0028] 여기서 응용 프로그램 제공 서버(100)는 구글 플레이나 애플의 앱스토어와 같은 각종 모바일 애플리케이션 마켓일 수 있으며, 사내 전산망의 메인 서버 또는 단독으로 구성된 서버일 수 있다.

[0029] 다음으로 사용자 단말기(200)는 응용 프로그램 제공 서버(100)로부터 응용 프로그램의 일반코드 파일을 수신하여 설치한다. 그리고 사용자 단말기(200)는 일반코드 파일에 대응하는 핵심코드 파일을 주변기기(300)로부터 수신하기 위하여 주변기기(300)와 유선 또는 무선으로 연결을 수행한다. 사용자 단말기(300)는 주변기기(300)로부터 등록을 요청받아 해당 주변기기(300)를 사용자 단말기(200)에 등록시키고, 해당 주변기기(300)로 사용자 단말기(200)의 등록을 요청하여 주변기기(300)와 연결할 수 있다.

[0030] 또한 사용자 단말기(200)는 사용자 단말기(200)와 연결된 주변기기(300)로부터 응용 프로그램의 핵심코드 파일을 수신하여 해당 응용 프로그램을 실행하고, 해당 응용 프로그램의 실행을 통하여 사용자 단말기(200)의 일부 기능을 제한한다.

[0031] 여기서 사용자 단말기(200)는 통신 기능, 촬영 기능, 녹음 기능, 저장 기능, 파일 전송 기능, GPS 기능 중에서 적어도 하나의 기능을 수행할 수 있는 단말기이다. 사용자 단말기(200)는 문자 메시지를 발송하거나, 음성 통화의 발신, 메신저를 이용한 메시지 발송 등의 기능을 수행할 수 있다. 그리고 사용자 단말기(200)는 동영상이나 사진을 촬영할 수 있는 촬영 기능을 구비할 수 있으며, 음성을 녹음하거나 USB 메모리 기능으로 각종 데이터를 저장할 수 있고, GPS 기능을 이용하여 위치를 추적할 수도 있다.

[0032] 또한, 사용자 단말기(200)는 응용 프로그램을 설치하여 실행할 수 있는 단말기로서, 스마트폰, 스마트 패드, 휴대폰, 노트북 컴퓨터, 태블릿 PC, PDA(Personal Digital Assistant) 등이 해당된다. 특히, 스마트폰 또는 스마트 패드의 경우 응용 프로그램은 기기 상에 애플리케이션으로 제공할 수 있다.

[0033] 여기서 애플리케이션은 단말 상의 응용 프로그램을 의미하며, 예를 들어 모바일 단말(스마트폰)에서 실행되는 앱(app)을 포함한다. 사용자는 앱(app)을 모바일 콘텐츠를 자유롭게 사고 파는 가상의 장터인 모바일 애플리케이션 마켓에서 다운로드 받아 스마트폰 등의 사용자 단말기(200)에 설치하거나, 사내 전산망의 서버로부터 응용 프로그램의 일반코드 파일을 수신하여 사용자 단말기(200)에 설치할 수 있다.

[0034] 그리고 사용자 단말기(200)에 설치된 응용 프로그램은 사용자 단말기(200)의 통신 기능, 촬영 기능, 녹음 기능, 저장 기능, 파일 전송 기능, GPS 기능 중에서 일부의 기능이 사용되지 못하도록 제어할 수 있다.

[0035] 마지막으로 주변기기(300)는 응용 프로그램 제공 서버(100)로부터 응용 프로그램의 핵심코드 파일을 수신하여 주변기기(300)에 설치한다. 그리고 사용자 단말기(200)로 주변기기의 고유정보를 전송하여 등록을 요청하고, 사용자 단말기(200)로부터 사용자 단말기의 고유정보를 수신하여 사용자 단말기(200)를 등록한다. 그리고 등록된 사용자 단말기(200)로 응용 프로그램의 핵심코드를 전송하여, 사용자 단말기(200)가 해당 응용 프로그램을 실행할 수 있도록 한다.

[0036] 여기서 주변기기(300)는 사용자 단말기(200) 및 응용 프로그램 제공 서버(100)와 통신할 수 있고, 응용 프로그램의 핵심코드 파일을 수신하여 저장할 수 있는 전기기기이다. 주변기기(300)는 스마트 와치, 스마트 안경, 스마트 밴드 등의 웨어러블 기기일 수 있으며, 통신이 가능한 외장하드, USB, OTG 등의 저장 매체일 수 있다.

[0037] 또한 활동 추적기, 모바일 포토 프린터, 홈모니터링 장치, 장난감, 의료기기 등의 앱세서리(Appcessory)를 주변기기(300)로 사용할 수 있다. 여기서 앱세서리는 사용자 단말기(200)인 스마트폰이 애플리케이션과 연동되어 스마트폰의 기능을 확장시켜주는 액세서리를 의미한다.

[0038] 그리고 핵심코드 파일을 저장한 주변기기(300)를 회사 또는 조직에서 관리할 수 있다. 회사는 사내의 정보 유출을 방지하기 위하여, 사내에 반입된 사용자 단말기(200)에 응용 프로그램의 일반코드 파일을 설치시키고, 해당 응용 프로그램의 핵심코드 파일이 설치된 주변기기(300)를 사용자 단말기(200)를 소지한 사용자에게 대여한다.

[0039] 일반코드 파일이 설치되지 않았거나 주변기기(300)와 연결되지 않은 사용자 단말기(200)는 사내에서 동작하지 않도록 할 수 있으며, 일반코드 파일이 설치되고, 주변기기(300)와 연결된 사용자 단말기(200)만 사용이 가능하도록 설정할 수 있다. 이때, 사용자 단말기(200)에 설치된 응용 프로그램은 사용이 가능하도록 설정된 사용자 단말기(200)의 여러 기능 중에서 일부의 기능은 사용하지 못하도록 제한할 수 있다.

[0040] 도 2는 본 발명의 실시예에 따른 사용자 단말기의 구성을 나타낸 블록도이다.

[0041] 도 2와 같이, 본 발명의 실시예에 따른 사용자 단말기(200)는 통신부(210), 인증부(220), 실행부(230) 및 제어부(240)를 포함한다.

[0042] 먼저, 통신부(210)는 응용 프로그램 제공 서버(100) 및 주변기기(300)와 통신한다. 특히, 통신부(210)는 응용 프로그램 제공 서버(100)와 Wi-Fi, 3G, 4G, LTE, 와이브로 등의 무선 통신 방식 또는 유선을 통하여 통신하며, 주변기기(300)와 블루투스, 지그비, 적외선통신모듈 등의 근거리 통신 또는 유선을 통하여 통신할 수 있다.

[0043] 통신부(210)는 응용 프로그램 제공 서버(100)로부터 응용 프로그램의 일반코드 파일을 수신하여 사용자 단말기(200)에 해당 응용 프로그램을 설치한다.

[0044] 그리고 통신부(210)는 응용 프로그램 제공 서버(100)로부터 응용 프로그램의 핵심코드 파일을 수신한 주변기기(300)로부터 등록 요청 메시지를 수신하고, 등록 응답 메시지를 주변기기(300)로 전송하며, 주변기기(300)의 인

증을 완료하고 나면 주변기기(300)로부터 응용 프로그램의 핵심코드 파일을 수신한다.

[0045] 다음으로 인증부(220)는 주변기기(300)로부터 수신한 등록 요청 메시지를 이용하여 주변기기(300)를 인증한다. 그리고 인증부(220)는 주변기기(300)의 인증을 완료하고 난 후, 해당 주변기기(300)로 전송할 등록 응답 메시지를 생성하고, 생성한 등록 응답 메시지를 통신부(210)를 통하여 주변기기(300)로 전송한다.

[0046] 그리고 실행부(230)는 응용 프로그램 제공 서버(100)로부터 수신한 일반코드 파일과 주변기기(300)로부터 수신한 응용 프로그램의 핵심코드 파일을 이용하여 응용 프로그램을 실행시킨다.

[0047] 마지막으로 제어부(240)는 응용 프로그램이 실행되는 동안 사용자 단말기(200)의 일부 기능을 제한하도록 제어한다. 제어부(240)는 사용자 단말기(200)의 통신 기능, 촬영 기능, 녹음 기능, 저장 기능, 파일 전송 기능, GPS 기능 중에서 적어도 하나의 기능을 사용하지 못하도록 제어할 수 있다.

[0048] 도 3은 본 발명의 실시예에 따른 주변기기의 구성을 나타낸 블록도이다.

[0049] 도 3에 나타낸 것처럼, 주변기기(300)는 통신부(310)와 저장부(320)를 포함한다.

[0050] 먼저, 통신부(310)는 응용 프로그램 제공 서버(100) 및 사용자 단말기(200)와 통신을 수행한다. 통신부(310)는 후술할 도 4의 응용 프로그램 분리 및 전달단계에서 응용 프로그램 제공 서버(100)로부터 응용 프로그램의 핵심코드 파일을 수신한다.

[0051] 그리고 통신부(310)는 사용자 단말기(200)에 설치된 응용 프로그램이 실행되면, 사용자 단말기(200)로 등록 요청 메시지를 전송한다. 여기서 등록 요청 메시지는 주변기기의 고유정보를 포함한다. 또한 통신부(310)는 사용자 단말기(200)로부터 사용자 단말기의 고유정보가 포함된 등록 응답 메시지를 수신한다.

[0052] 다음으로 저장부(320)는 응용 프로그램 제공 서버(100)로부터 수신한 응용 프로그램의 핵심코드 파일을 저장한다. 그리고 사용자 단말기(200)로부터 수신한 사용자 단말기의 고유정보를 저장하여 해당 사용자 단말기를 등록한다.

[0053] 이하에서는 도 4를 통하여 본 발명의 실시예에 따른 정보 유출을 방지하는 방법에 대하여 더욱 상세하게 설명한다.

[0054] 도 4는 본 발명의 실시예에 따른 정보 유출을 방지하는 방법을 설명하기 위한 순서도이다.

[0055] 도 4에 나타낸 것처럼, 정보 유출을 방지하는 방법에 있어서 S410 단계 내지 S430 단계는 응용 프로그램 분리 및 전달단계를 나타내고, S440 단계 내지 S480 단계는 사용자 단말기와 주변기기의 등록 단계를 나타내며, S490 단계 및 S500 단계는 응용 프로그램 실행 단계를 나타낸다. 설명의 편의상 상기와 같이 크게 세 개의 단계로 나누어 설명하기로 한다.

[0056] 먼저, 응용 프로그램 제공 서버(100)는 S410 단계 내지 S430 단계를 통하여 응용 프로그램 분리 및 전달단계를 수행한다.

[0057] 응용 프로그램 제공 서버(100)는 응용 프로그램 파일을 핵심코드 파일과 핵심코드가 분리된 일반코드 파일로 분리한다(S410). 즉, 응용 프로그램 제공 서버(100)는 응용 프로그램 패키지로부터 디컴파일된 실행 파일 또는 소스 코드를 통하여 핵심 코드를 설정하여 핵심코드 파일을 생성한다. 그리고 응용 프로그램 제공 서버(100)는 응용 프로그램 파일 중에서 핵심코드를 삭제하여 일반코드로만 이루어진 일반코드 파일을 생성한다.

[0058] 그리고 응용 프로그램 제공 서버(100)는 분리된 핵심코드 파일을 주변기기(300)로 전송하여 저장시킨다(S420). 이때, 응용 프로그램 제공 서버(100)는 주변기기(300)로 핵심코드 파일을 전달하는 과정에서 Wi-Fi, 3G, 4G, LTE, 와이브로 등의 무선 통신 방식을 통하여 통신할 수 있으며, 보안을 강화하기 위하여 근거리 통신 또는 유선을 통하여 핵심코드를 전달할 수 있다.

[0059] 또한, 사용자가 사용자 단말기(200)를 통하여 응용 프로그램 제공 서버(100)에 접속하면, 응용 프로그램 제공 서버(100)는 일반코드 파일을 사용자 단말기(200)로 다운로드 방식으로 전송한다(S430). 사용자 단말기(200)는 3G, 4G, Wi-Fi 등의 네트워크를 이용하여 설치하고자 하는 응용 프로그램의 일반코드 파일을 다운로드 받아 설치할 수 있다.

[0060] 본 발명의 실시예에 따른 정보 유출 방지 시스템은 사용자로부터 사용자 단말기(200)에 설치된 응용 프로그램의 최초 실행을 입력 받았을 때 또는 주변기기(300)가 사용자 단말기(200)와 유선 연결되었을 때, 사용자 단말기(200) 및 주변기기(300) 등록 단계를 수행할 수 있다.

[0061] 응용 프로그램 분리 및 전달단계가 수행되고 난 후, 사용자 단말기(200)와 주변기기(300)는 S440 단계 내지 S480 단계를 통하여 서로의 고유정보를 등록하여 연결한다. 사용자 단말기(200)와 주변기기(300)가 상호 기 등록되어 페어링 연결되어 있는 경우, S440 단계 내지 S470 단계는 생략될 수 있다.

[0062] 핵심코드 파일을 저장한 주변기기(300)는 사용자 단말기(200)로 등록 요청 메시지를 전송한다(S440). 여기서 등록 요청 메시지는 주변기기의 고유정보를 포함하며, 주변기기의 고유정보는 주변기기(300)의 시리얼 넘버일 수 있다.

[0063] 다음으로 사용자 단말기(200)는 수신한 등록 요청 메시지에 포함된 주변기기의 고유정보를 이용하여 해당 주변기기(300)를 등록시키고(S450), 주변기기(300)로 등록 응답 메시지를 전송한다(S460).

[0064] 여기서, 등록 응답 메시지는 사용자 단말기의 고유정보를 포함하며, 사용자 단말기(200)는 주변기기(300)로 등록 응답 메시지를 전송하여 주변기기(300)가 사용자 단말기(200)에 등록되었음을 알리고, 주변기기(300)에 사용자 단말기(200)의 등록을 요청한다.

[0065] 이때, 사용자 단말기 고유정보는 사용자 단말기(200)의 국제모바일기기 식별정보(IMEI; International Mobile Equipment Identity), ANDROID_ID, 시리얼 번호, 휴대폰 번호, 모델 번호, MAC 주소 중에서 적어도 하나를 포함할 수 있다.

[0066] 국제모바일기기 식별코드(IMEI)는 휴대폰마다 부여되는 고유 식별번호이다. 세계이동통신사업자연합(GSMA)의 가이드라인에 따라 휴대폰 제조 업체는 제조한 휴대폰을 출고할 때, 각각의 휴대폰에 국제모바일기기 식별코드(IMEI)를 부여한다. 국제모바일기기 식별코드(IMEI)는 승인코드 8자리, 모델 일련번호 6자리, 검증용 숫자 1자리 등 총 15자리로 구성되며, 주로 분실 단말기 및 도난 단말기에 대한 통화차단을 목적으로 관리된다.

[0067] 본 발명의 실시예에 따른 정보 유출 방지 시스템은 사용자 단말기(200)가 최초 부팅될 때 생성되어 저장되는 64-bit의 고유 값인 ANDROID_ID, 사용자 단말기(200)가 생산될 때 할당된 시리얼 넘버, 사용자 단말기(200)의 모델 번호, 휴대폰 번호 등을 사용자 단말기 고유정보로 활용할 수 있다. 또한 Wi-Fi, 블루투스(Bluetooth)를 사용하는 사용자 단말기(200)의 MAC 주소를 사용자 단말기 고유정보로 사용할 수 있다.

[0068] 또한 사용자 단말기(200)는 사용자로부터 실행을 요청받은 응용 프로그램의 식별정보를 등록 응답 메시지와 함께 주변기기(300)로 전송할 수 있다. 사용자 단말기(200)에 설치된 복수의 응용 프로그램 중에서 핵심코드 파일을 요청하는 응용 프로그램의 식별정보를 주변기기(300)로 전송함으로써, 주변기기(300)로부터 해당 응용 프로그램의 핵심코드 파일을 수신할 수 있다.

[0069] 다음으로 등록 응답 메시지를 수신한 주변기기(300)는 해당 사용자 단말기(200)를 등록시킨다(S470). 이때, 주변기기(300)는 사용자 단말기(200)의 국제모바일기기 식별정보(IMEI), ANDROID_ID, 시리얼 번호, 휴대폰 번호, 모델 번호, MAC 주소 중에서 적어도 하나를 이용하여 해당 사용자 단말기(200)를 등록할 수 있다.

[0070] 그리고 사용자 단말기(300)의 등록을 완료한 주변기기(300)는 사용자 단말기(200)로 응용 프로그램의 핵심코드 파일을 전송한다(S480). S460 단계에서 주변기기(300)가 사용자 단말기(200)로부터 응용 프로그램의 식별정보를 수신한 경우, 주변기기(300)는 응용 프로그램의 식별정보에 대응하는 응용 프로그램의 핵심코드 파일을 사용자 단말기(200)로 전송한다.

[0071] S440 단계 내지 S480 단계를 통하여 사용자 단말기(200)와 주변기기(300)의 연결이 완료되면, 사용자 단말기(200)와 주변기기(300)는 S490 단계 및 S500 단계를 통하여 응용 프로그램을 실행한다.

[0072] 주변기기(300)로부터 핵심코드 파일을 수신한 사용자 단말기(200)는 응용 프로그램을 실행한다(S490). 사용자 단말기(200)는 응용 프로그램의 일반코드 파일과 핵심코드 파일을 이용하여 해당 응용 프로그램을 실행할 수 있다.

[0073] S490 단계에서 응용 프로그램이 실행되면, 사용자는 실행된 응용 프로그램을 이용하여 각종 업무를 처리할 수 있다. 이때, 응용 프로그램은 회사의 업무를 처리할 수 있도록 지원하는 전사적자원관리(ERP), 기업정보포털(EIP), 기업애플리케이션통합(EAI), 그룹웨어(Groupware), 지식관리시스템(KMS) 등의 각종 응용 프로그램 또는 시스템일 수 있다.

[0074] 반면, 사용자 단말기(200)가 핵심코드 파일이 저장된 주변기기(300)와 연결이 해제되면, 정보 유출 방지 시스템은 해당 사용자 단말기(200)의 모든 기능 제어를 해제하고 종료된다. 단, 보안을 강화하기 위하여 주변기기(300)에 연결 상태를 로그 형태로 기록하여 저장할 수 있다.

[0075] 다음으로 사용자 단말기(200)에 설치된 응용 프로그램은 사용자 단말기(200)에 내장된 일부 기능의 사용을 제한한다(S500). 여기서 제한되는 기능은 통신 기능, 촬영 기능, 녹음 기능, 저장 기능, 파일 전송 기능, GPS 기능과 같이 사내의 기밀 정보를 외부로 유출시킬 위험이 있는 기능을 의미한다.

[0076] 응용 프로그램이 실행되면, 사용자 단말기(200)는 통신 기능이 제한되어 문자 메시지의 발송, 음성 또는 영상 통화의 발신, 메신저의 메시지 발송이 제한될 수 있다. 또한, 사용자 단말기(200)는 촬영 기능이 제한되어 동영상 또는 사진 촬영을 하지 못하도록 제한될 수 있으며, 녹음 기능이 제한되어 회의 시 녹취, 통화 내용의 녹음이 제한될 수 있다.

[0077] 또한 사용자 단말기(200)는 저장 기능이 제한되어 USB 메모리 기능을 이용한 사내의 PC에 저장된 데이터 유출을 방지할 수 있다. 그리고 타인에게 파일을 전송하지 못하도록 제한되거나, 보안이 필요한 위치 정보가 유출되지 못하도록 GPS 기능이 제한될 수도 있다.

[0078] 이와 같이 본 발명의 실시예에 따르면, 정보 유출 수단으로 사용될 위험이 있는 사용자 단말기의 기능을 제한함으로써, 기업 또는 조직의 정보를 보호하고, 기밀 유출을 방지할 수 있다.

[0079] 또한 서버가 아닌 주변기기를 이용하여 사내에 반입된 사용자 단말기를 관리하므로 사내 단말기 관리 시스템의 오작동을 방지할 수 있고, 사용자가 사내 단말기 관리 시스템의 작동 여부를 직관적으로 확인할 수 있다.

[0080] 이상에서 본 발명의 바람직한 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

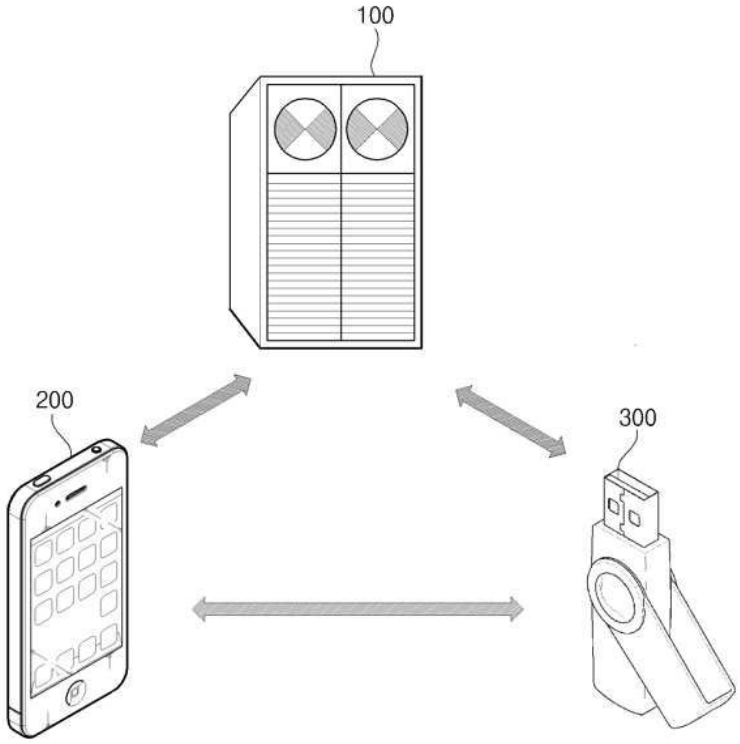
부호의 설명

[0081]

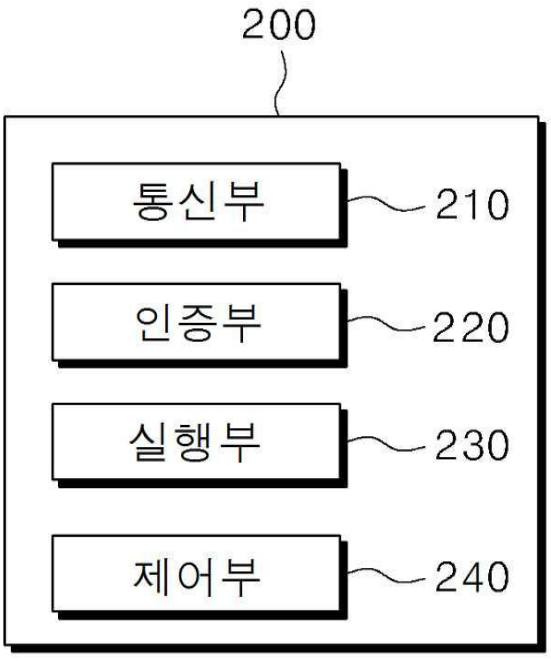
100 : 응용 프로그램 제공 서버	200 : 사용자 단말기
210 : 통신부	220 : 인증부
230 : 실행부	240 : 제어부
300 : 주변기기	310 : 통신부
320 : 저장부	

도면

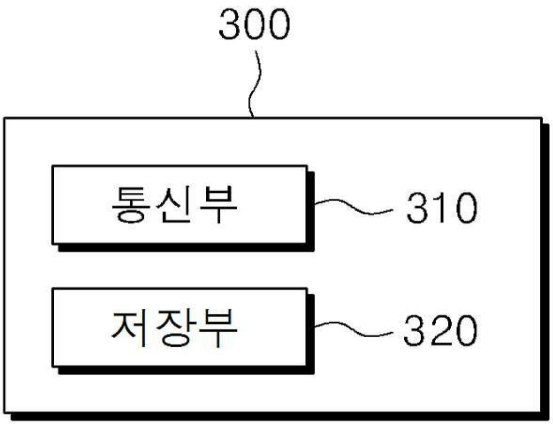
도면1



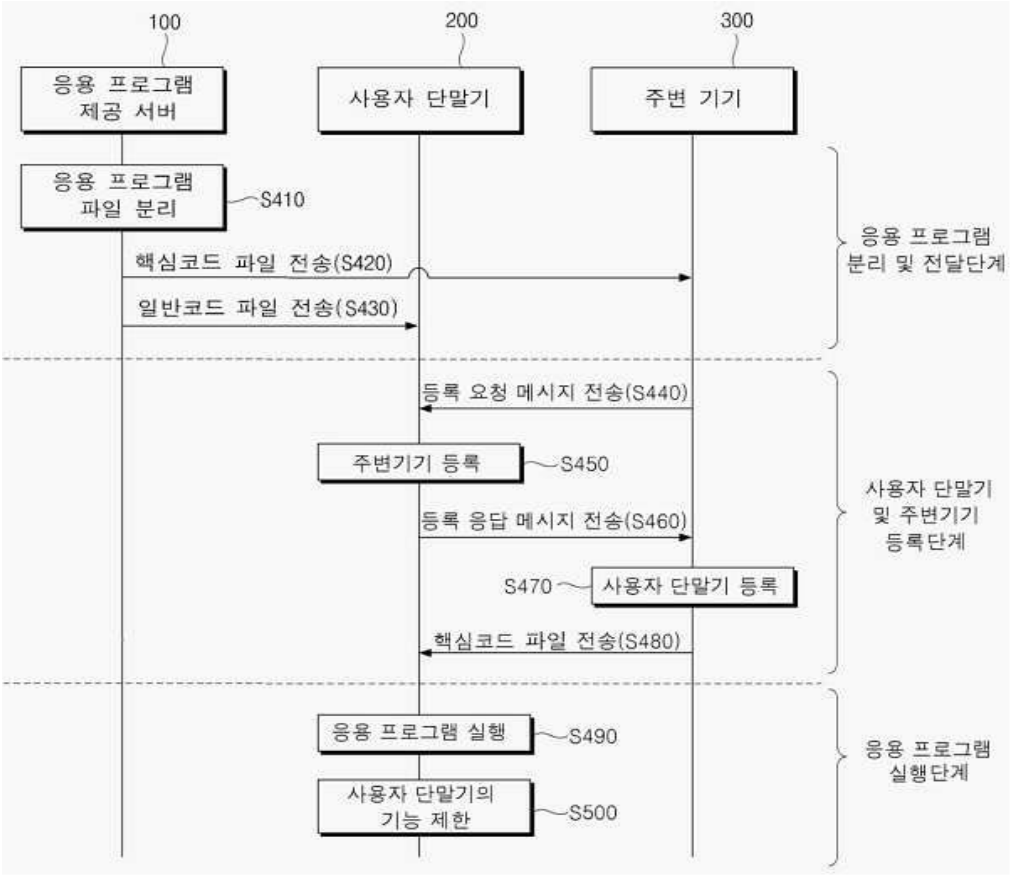
도면2



도면3


300
통신부
310
저장부
320

도면4


100
200
300
응용 프로그램 제공 서버
사용자 단말기
주변 기기
응용 프로그램 파일 분리
S410
핵심코드 파일 전송(S420)
일반코드 파일 전송(S430)
응용 프로그램 분리 및 전달단계
등록 요청 메시지 전송(S440)
주변기기 등록
S450
등록 응답 메시지 전송(S460)
S470
사용자 단말기 등록
핵심코드 파일 전송(S480)
사용자 단말기 및 주변기기 등록단계
응용 프로그램 실행
S490
사용자 단말기의 기능 제한
S500
응용 프로그램 실행단계