



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0045231
(43) 공개일자 2014년04월16일

(51) 국제특허분류(Int. Cl.)
H04W 12/02 (2009.01) H04W 8/30 (2009.01)
(21) 출원번호 10-2012-0111512
(22) 출원일자 2012년10월08일
심사청구일자 2012년10월08일

(71) 출원인
고려대학교 산학협력단
서울시 성북구 안암로 145 (안암동)
(72) 발명자
안순진
서울 강남구 압구정로 151, 113동 302호 (압구정동, 신현대아파트)
김동완
서울 성북구 안암로 145, 전기전자전파공학과 (안암동5가, 고려대학교)
(74) 대리인
특허법인충현

전체 청구항 수 : 총 12 항

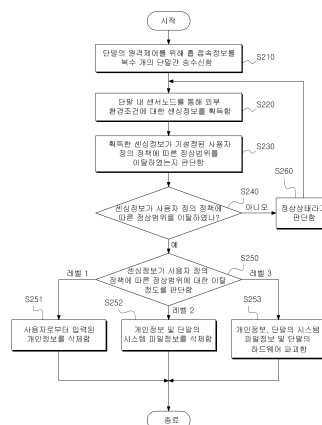
(54) 발명의 명칭 단말간 원격제어를 이용한 개인정보 유출 방지 방법

(57) 요약

본 발명은 단말간 원격제어를 이용한 개인정보 유출 방지 방법에 관한 것으로, 보다 구체적으로는 단말의 원격제어를 위해 복수 개의 단말간 호 접속정보를 송수신하는 단계; 상기 단말 내 센서노드를 통해 외부 환경조건에 대한 센싱정보를 획득하는 단계; 획득한 센싱정보가 기설정된 사용자 정의 정책에 따른 정상범위를 이탈하였는지 여부를 판단하는 단계; 및 상기 센싱정보가 상기 사용자 정의 정책에 따른 정상범위를 이탈하였다고 판단하는 경우, 정상범위 이탈정도에 따라 상기 단말 내 기저장된 사용자의 개인정보를 차등적으로 삭제하도록 제어하는 단계;를 포함한다.

본 발명의 단말간 원격제어를 이용한 개인정보 유출 방지 방법은 원격리에 떨어져 있는 수신단말로 원격제어를 수행하도록 하는 원격제어 트리거정보를 포함하는 호 접속정보를 전송하여 송신단말이 상기 수신단말에 대한 원격제어를 수행할 수 있는 효과가 있다.

대표도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호 2012K1A3A1A09026959

부처명 미래창조과학부

연구사업명 국가간협력기반조성사업

연구과제명 USN 기반 국경 침입 감시 시스템 기술 개발

기 여 율 1/1

주관기관 고려대학교

연구기간 2012.08.01 ~ 2015.07.31

특허청구의 범위

청구항 1

단말의 원격 제어를 위해 복수 개의 단말간 호 접속정보를 송수신하는 단계;

상기 단말 내 센서노드를 통해 외부 환경조건에 대한 센싱정보를 획득하는 단계;

획득한 센싱정보가 기설정된 사용자 정의 정책에 따른 정상범위를 이탈하였는지 여부를 판단하는 단계; 및

상기 센싱정보가 상기 사용자 정의 정책에 따른 정상범위를 이탈하였다고 판단하는 경우, 정상범위 이탈정도에 따라 상기 단말 내 기저장된 사용자의 개인정보를 차등적으로 삭제하도록 제어하는 단계;

를 포함하는 단말간 원격제어를 이용한 개인정보 유출 방지 방법.

청구항 2

제1항에 있어서,

상기 복수 개의 단말 간 호 접속정보를 송수신하는 단계는

상기 복수 개의 단말 중 하나의 송신단말이 원격 제어하고자 하는 상기 복수 개의 단말 중 수신단말로 상기 수신단말에 대해 미리 정의된 원격제어 트리거정보를 포함하는 호 접속정보를 전송하는 과정;

상기 수신단말이 상기 송신단말로부터 상기 호 접속정보를 수신하고, 수신한 호 접속정보 내 포함된 원격제어 트리거정보가 유효한지 여부를 판단하는 과정; 및

상기 수신단말이 수신한 원격제어 트리거정보가 유효하다고 판단한 경우, 원격제어모드로 변환하는 과정;

을 포함하는 것을 특징으로 하는 단말간 원격제어를 이용한 개인정보 유출 방지 방법.

청구항 3

제1항에 있어서,

상기 센싱정보를 획득하는 단계는

상기 단말의 외부 온도 또는 습도에 대한 센싱정보를 획득하는 것을 특징으로 하는 단말간 원격제어를 이용한 개인정보 유출 방지 방법.

청구항 4

제1항에 있어서,

상기 센싱정보가 사용자 정의 정책에 따른 정상범위의 이탈여부를 판단하는 단계는

상기 센싱정보를 기설정된 사용자 정의 정책에 따른 정상범위와 비교하는 과정; 및

상기 센싱정보가 상기 사용자 정의 정책에 따른 정상범위를 벗어나는 경우, 상기 단말의 외부환경에 대하여 이상상태를 판단하는 과정;

을 포함하는 것을 특징으로 하는 단말간 원격제어를 이용한 개인정보 유출 방지 방법.

청구항 5

제1항에 있어서,

상기 단말 내 기저장된 사용자의 개인정보를 삭제하는 단계는

상기 센싱정보가 상기 사용자 정의 정책에 따른 정상범위를 이탈하였다고 판단하는 경우, 이탈정도에 따라 상기 단말 내 기저장된 사용자의 개인정보를 차등적으로 삭제하는 것을 특징으로 하는 단말간 원격제어를 이용한 개인정보 유출 방지 방법.

청구항 6

제5항에 있어서,

상기 단말 내 기저장된 사용자의 개인정보를 삭제하는 단계는

상기 사용자로부터 입력된 개인정보를 삭제하는 제1 삭제과정;

상기 개인정보 및 상기 단말의 시스템 파일정보를 삭제하는 제2 삭제과정; 및

상기 개인정보, 상기 단말의 시스템 파일정보를 삭제하고, 상기 단말의 하드웨어를 파괴하는 제3 삭제과정;

을 상기 센싱정보의 사용자 정의 정책에 따른 정상범위의 이탈상태에 따라 선택하여 수행하는 것을 특징으로 하는 단말간 원격제어를 이용한 개인정보 유출 방지 방법.

청구항 7

제6항에 있어서,

상기 제3 삭제과정은

상기 단말이 하드웨어 파괴 예정을 나타내는 메시지, 이미지 및 경고음 중 적어도 하나를 출력하는 과정;

상기 단말은 기설정된 시간이 경과한 후, 상기 개인정보, 상기 단말의 시스템 파일정보를 삭제하고, 상기 단말의 하드웨어를 파괴하는 과정;

을 포함하는 것을 특징으로 하는 단말간 원격제어를 이용한 개인정보 유출 방지 방법.

청구항 8

제6항에 있어서,

상기 개인정보는

전화번호부, 통화기록, 문자 메시지 및 사진 중 적어도 하나를 포함하는 것을 특징으로 하는 단말간 원격제어를 이용한 개인정보 유출 방지 방법.

청구항 9

제5항에 있어서,

상기 단말 내 기저장된 사용자의 개인정보를 삭제하는 단계는

상기 단말 내 기저장된 사용자의 개인정보를 삭제하기 전, 통신 네트워크에 연결된 데이터 백업 서버로 상기 사용자의 개인정보를 전송하여 백업하는 과정을 수행하는 것을 특징으로 하는 단말간 원격제어를 이용한 개인정보 유출 방지 방법.

청구항 10

제1항에 있어서,

상기 복수 개의 단말 중 송신단말이 원격 제어 해지정보를 포함하는 호 접속정보를 수신단말로 전송하고, 상기 수신단말이 수신한 호 접속정보 내 원격 제어 해지정보를 확인하여 원격 제어 모드를 종료하는 단계;

를 더 포함하는 것을 특징으로 하는 단말간 원격제어를 이용한 개인정보 유출 방지 방법.

청구항 11

원격제어 하고자 하는 수신단말에 대한 사용자 정의 정책이 기저장된 호 수락 제어서버로 송신단말이 호 접속정보를 전송하는 단계;

상기 수신단말 내 센서노드를 통해 외부 환경조건에 대한 센싱정보를 획득하는 단계;

획득한 센싱정보가 기설정된 사용자 정의 정책에 따른 정상범위를 이탈하였는지 여부를 판단하는 단계; 및

상기 센싱정보가 상기 사용자 정의 정책에 따른 정상범위를 이탈하였다고 판단하는 경우, 정상범위 이탈정도에 따라 상기 단말 내 기저장된 사용자의 개인정보를 차등적으로 삭제하도록 제어하는 단계;

를 포함하는 단말간 원격제어를 이용한 개인정보 유출 방지 방법.

청구항 12

제1항 내지 제11항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

명세서

기술분야

[0001] 본 발명은 단말간 원격제어를 이용한 개인정보 유출 방지 방법에 관한 것으로, 특히 원격제어하고자 하는 단말의 외부 환경상태에 따라 상기 단말에 저장된 사용자 개인정보를 삭제하여 상기 사용자 개인정보가 외부로 유출되는 것을 방지할 수 있는 단말간 원격제어를 이용한 개인정보 유출 방지 방법에 관한 것이다.

배경기술

[0002] IT 기술의 발달에 따라, 이동중에도 데이터를 송수신할 수 있는 이동단말이 나타나게 되었다. 이러한 이동단말은 그 편리함으로 인해 많은 사람들이 사용하고 있지만, 이러한 장점에도 불구하고 이동단말을 사용하는 사용자의 개인 정보에 대한 보안이 취약하다는 문제점이 발생했다.

[0003] 상술한 바와 같이, 단말간 원격제어를 이용한 개인정보 유출 방지 방법에 대한 선행기술을 살펴보면 다음과 같다.

[0004] 선행기술 1은 한국공개특허 제10-2006-0106992호(2006.10.13)로서, 중계서버를 이용한 이동통신 원격제어방법 및 그 장치에 관한 것이다. 이러한 선행기술 1은 일반적인 이동통신단말기의 단문메시지서비스(SMS)를 이용하여 사용자의 가정이나 직장 등 수용가내의 자동화기기를 제어하기 위한 장치와 그 제어방법에 관한 것으로서, 원격지 자동화기기를 제어하기 위해 사용자가 이동통신네트워크를 이용하여 해당기기의 제어서버에 직접 접속하지 않고, 사용자로부터의 제어명령을 받아서 자동화기기 제어서버에 대해 제어명령을 수행하기 위한 일련의 작업신호를 전달하고 상태를 체크해내는 제어명령 중계서버에 SMS를 전송함으로써 원하는 제어를 할 수 있도록 하는 것을 특징으로 한다.

[0005] 또한, 선행기술 2는 한국등록특허 제10-0533570호(2005.12.06)호로서, 이동통신단말기를 이용한 원격지 컴퓨터 제어방법 및 그 시스템에 관한 것이다. 이러한 선행기술 2는 원격제어대상 PC와 이동통신단말기를 연결시켜 PC의 IP어드레스 및 원격제어메뉴 정보와 이동통신단말기의 하드웨어정보 및 개인정보를 교환 동기화 시키는 단계; 무선인터넷에 접속된 이동통신단말기로부터의 송출 IP 어드레스로 원격제어대상 PC와 이동통신단말기가

접속되도록 하는 단계; PC의 원격제어를 위한 이동통신단말의 사용권한을 확인하는 사용자 인증단계; 이동통신 단말기를 이용한 PC원격제어 사용권한 인증 후, 이동통신단말기의 디스플레이 상에서 선택된 원격제어 서비스메뉴 정보를 무선통신망을 통하여 전송받아 해당 서비스메뉴를 실행하는 단계; 및 이동통신단말기로부터 선택된 원격제어명령을 실행한 후, 해당 명령의 실행결과를 무선 통신망을 통하여 이동통신단말기로 송출하는 단계를 포함한다.

발명의 내용

해결하려는 과제

- [0006] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 원격제어하고자 하는 단말에 내장된 센서노드를 통해 상기 단말의 외부 환경조건을 측정하고, 측정된 환경조건에 따라 상기 단말에 저장된 사용자의 개인정보를 차등적으로 삭제함으로써, 상기 단말에 저장된 사용자의 개인정보가 외부로 유출되는 것을 방지할 수 있는 단말 간 원격제어를 이용한 개인정보 유출 방지 방법을 제공하고자 한다.

과제의 해결 수단

- [0007] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 단말간 원격제어를 이용한 개인정보 유출 방지 방법은 단말의 원격 제어를 위해 복수 개의 단말간 호 접속정보를 송수신하는 단계; 상기 단말 내 센서노드를 통해 외부 환경조건에 대한 센싱정보를 획득하는 단계; 획득한 센싱정보가 기설정된 사용자 정의 정책에 따른 정상범위를 이탈하였는지 여부를 판단하는 단계; 및 상기 센싱정보가 상기 사용자 정의 정책에 따른 정상범위를 이탈하였다고 판단하는 경우, 정상범위 이탈정도에 따라 상기 단말 내 기저장된 사용자의 개인정보를 차등적으로 삭제하도록 제어하는 단계;를 포함한다.
- [0008] 보다 바람직하게는 상기 복수 개의 단말 중 하나의 송신단말이 원격 제어하고자 하는 상기 복수 개의 단말 중 수신단말로 상기 수신단말에 대해 미리 정의된 원격제어 트리거정보를 포함하는 호 접속정보를 전송하는 과정; 상기 수신단말이 상기 송신단말로부터 상기 호 접속정보를 수신하고, 수신한 호 접속정보 내 포함된 원격제어 트리거정보가 유효한지 여부를 판단하는 과정; 및 상기 수신단말이 수신한 원격제어 트리거정보가 유효하다고 판단한 경우, 원격제어모드로 변환하는 과정;을 포함하는 복수 개의 단말 간 호 접속정보를 송수신하는 단계를 포함할 수 있다.
- [0009] 특히, 상기 단말의 외부 온도 또는 습도에 대한 센싱정보를 획득하는 센싱정보를 획득하는 단계를 포함할 수 있다.
- [0010] 보다 바람직하게는 상기 센싱정보를 기설정된 사용자 정의 정책에 따른 정상범위와 비교하는 과정; 및 상기 센싱정보가 상기 사용자 정의 정책에 따른 정상범위를 벗어나는 경우, 상기 단말의 외부환경에 대하여 이상상태를 판단하는 과정;을 포함하는 센싱정보가 사용자 정의 정책에 따른 정상범위의 이탈여부를 판단하는 단계를 포함할 수 있다.
- [0011] 특히, 상기 센싱정보가 상기 사용자 정의 정책에 따른 정상범위를 이탈하였다고 판단하는 경우, 이탈정도에 따라 상기 단말 내 기저장된 사용자의 개인정보를 차등적으로 삭제하는 단말 내 기저장된 사용자의 개인정보를 삭제하는 단계를 포함할 수 있다.
- [0012] 보다 바람직하게는 상기 사용자로부터 입력된 개인정보를 삭제하는 제1 삭제과정; 상기 개인정보 및 상기 단말의 시스템 파일정보를 삭제하는 제2 삭제과정; 및 상기 개인정보, 상기 단말의 시스템 파일정보를 삭제하고, 상기 단말의 하드웨어를 파괴하는 제3 삭제과정;을 상기 센싱정보의 사용자 정의 정책에 따른 정상범위의 이탈상태에 따라 선택하여 수행하는 단말 내 기저장된 사용자의 개인정보를 삭제하는 단계를 포함할 수 있다.
- [0013] 보다 바람직하게는 상기 단말이 하드웨어 파괴 예정을 나타내는 메시지, 이미지 및 경고음 중 적어도 하나를 출력하는 과정; 상기 단말은 기설정된 시간이 경과한 후, 상기 개인정보, 상기 단말의 시스템 파일정보를 삭제하고, 상기 단말의 하드웨어를 파괴하는 과정;을 포함하는 제3 삭제 과정을 포함할 수 있다.
- [0014] 특히, 전화번호부, 통화기록, 문자 메시지 및 사진 중 적어도 하나를 포함하는 개인정보를 포함할 수 있다.

- [0015] 특히, 상기 단말 내 기저장된 사용자의 개인정보를 삭제하기 전, 통신 네트워크에 연결된 데이터 백업 서버로 상기 사용자의 개인정보를 전송하여 백업하는 과정을 수행하는 단말 내 기저장된 사용자의 개인정보를 삭제하는 단계를 포함할 수 있다.
- [0016] 보다 바람직하게는 상기 복수 개의 단말 중 송신단말이 원격 제어 해지정보를 포함하는 호 접속정보를 수신단말로 전송하고, 상기 수신단말이 수신한 호 접속정보 내 원격 제어 해지정보를 확인하여 원격 제어 모드를 종료하는 단계;를 더 포함할 수 있다.
- [0017] 위와 같은 과제를 해결하기 위한 본 발명의 다른 실시 예에 따른 단말간 원격제어를 이용한 개인정보 유출 방지 방법은 원격제어 하고자 하는 수신단말에 대한 사용자 정의 정책이 기저장된 호 수락 제어서버로 송신단말이 호 접속정보를 전송하는 단계; 상기 수신단말 내 센서노드를 통해 외부 환경조건에 대한 센싱정보를 획득하는 단계; 획득한 센싱정보가 기설정된 사용자 정의 정책에 따른 정상범위를 이탈하였는지 여부를 판단하는 단계; 및 상기 센싱정보가 상기 사용자 정의 정책에 따른 정상범위를 이탈하였다고 판단하는 경우, 정상범위 이탈정도에 따라 상기 단말 내 기저장된 사용자의 개인정보를 차등적으로 삭제하도록 제어하는 단계;를 포함한다.

발명의 효과

- [0018] 본 발명의 단말간 원격제어를 이용한 개인정보 유출 방지 방법은 원거리에 떨어져 있는 수신단말로 원격제어를 수행하도록 하는 원격제어 트리거정보를 포함하는 호 접속정보를 전송하여 송신단말이 상기 수신단말에 대한 원격제어를 수행할 수 있는 효과가 있다.
- [0019] 또한, 본 발명의 단말간 원격제어를 이용한 개인정보 유출 방지 방법은 원거리에 떨어져 있는 단말의 외부 환경조건을 측정하고, 측정된 외부 환경조건이 기설정된 임계치를 이탈하는 경우에는 이탈정도에 따라 상기 단말에 저장된 사용자의 개인정보를 차등적으로 삭제함으로써, 상기 사용자의 개인정보가 외부로 유출되는 것을 방지할 수 있는 효과가 있다.
- [0020] 더불어, 본 발명의 단말간 원격제어를 이용한 개인정보 유출 방지 방법은 단말에 저장된 사용자의 개인정보를 삭제하기에 앞서, 상기 단말에 저장된 사용자의 개인정보를 데이터 백업 서버로 전송함으로써, 상기 사용자의 개인정보가 단말에서 불가피하게 삭제되더라도, 해당 개인정보가 필요한 경우에는 데이터 백업 서버에 접속하여 백업된 사용자의 개인정보를 용이하게 획득할 수 있는 효과가 있다.

도면의 간단한 설명

- [0021] 도 1은 본 발명의 일 실시 예에 따른 단말간 원격제어를 이용한 개인정보 유출 방지 방법을 구현하기 위한 무선 네트워크 시스템 구성도이다.
- 도 2는 본 발명의 다른 실시 예에 따른 단말간 원격제어를 이용한 개인정보 유출 방지 방법의 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0022] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 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 한정되는 것은 아니다.
- [0023] 이하, 도 1을 참조하여, 본 발명의 일 실시 예에 단말간 원격제어를 이용한 개인정보 유출 방지 방법을 구현하는 무선 네트워크 시스템에 대하여 간략히 설명하도록 한다.
- [0024] 도 1은 본 발명의 일 실시 예에 따른 단말간 원격제어를 이용한 개인정보 유출 방지 방법을 구현하기 위한 무선 네트워크 시스템 구성도이다.
- [0025] 도 1에 도시된 바와 같이, 본 발명의 무선 네트워크 시스템(100)은 복수 개의 이동단말 중 송신단말(110)이 제어하고자 하는 특정 단말(이하, 수신단말이라고 한다.)에 대한 호 접속정보를 포함하는 신호를 기지국(120)으로 전송하면, 상기 기지국(120)으로부터 호 수락 제어서버(130: Call Admission Control Server)가 수신한 호 접속정보에 해당하는 단말과 연결된 게이트웨이(140)로 호 접속정보를 포함하는 신호를 전송하고, 상기 게이트웨이(140)와 센서 네트워크를 이루고 있는 수신단말(150)로 수신한 상기 신호를 전달하여, 상기 수신단말(150)이

원격제어모드로 변환함으로써, 상기 송신단말(110)이 원거리에 존재하는 수신단말(150)을 원격제어 할 수 있다. 이때, 상기 무선 네트워크 시스템은 GSM, W-CDMA, WiMAX, LTE 등으로 통신망이 구축되어 있다.

- [0026] 특히, 상기 송신단말 및 수신단말은 음성 및 데이터 통신 서비스를 이용할 수 있도록 설계된 단말로서, 예를 들면 스마트폰, 휴대전화, PDA 등이 사용될 수 있다.
- [0027] 또한, 기지국(120)은 기저대역 신호처리, 유무선 변환 및 무선신호의 송수신등을 수행하여 이동단말과 직접적으로 연결되는 이동통신망 종단장치를 말한다.
- [0028] 도 2는 본 발명의 다른 실시 예에 따른 단말간 원격제어를 이용한 개인정보 유출 방지 방법의 순서도이다.
- [0029] 도 2에 도시된 바와 같이, 본 발명의 단말간 원격제어를 이용한 개인정보 유출 방지 방법은 먼저, 복수 개의 이동단말 중 원격제어하고자 하는 송신단말이 원격제어의 대상이 되는 수신단말로 상기 수신단말과의 통신접속을 위한 호 접속정보를 앞서 도 1을 통해 설명한 무선 네트워크 시스템을 통해 전송한다(S210).
- [0030] 이러한 호 접속정보는 통화서비스, 데이터 서비스를 수행하기 위한 호 연결 절차를 나타내는 정보로서, 특히, 상기 수신단말에 대하여 미리 설정된 원격제어 트리거 정보를 포함하여, 호 접속이 연결되면, 상기 수신단말이 원격제어모드로 변환한다.
- [0031] 즉, 복수 개의 단말 중 하나의 송신단말이 원격 제어하고자 하는 상기 복수 개의 단말 중 수신단말로 상기 수신단말에 대해 미리 정의된 원격제어 트리거정보를 포함하는 호 접속정보를 전송하고, 상기 수신단말이 상기 송신단말로부터 상기 호 접속정보를 수신하고, 수신한 호 접속정보가 유효한지 여부를 판단하여, 호 접속 연결한 후, 상기 호 접속정보 내 원격제어 트리거정보가 존재하는 경우에, 상기 수신단말은 자신을 원격제어모드로 변환할 수 있다.
- [0032] 이처럼, 송신단말에 의해 원격제어가 수행되는 수신단말은 내부에 구비되는 센서노드를 통해 외부 환경조건에 대한 센싱정보를 획득한다(S220). 이때, 상기 센서노드는 열감지센서 또는 습도감지센서 중 적어도 하나를 포함하는 것으로, 상기 수신단말에 부착되어, 상기 수신단말의 외부 환경 조건 예를 들면, 외부 온도, 습도 등을 센싱하여 센싱정보를 획득할 수 있다.
- [0033] 상기 수신단말이 센서노드를 통해 획득한 외부 환경조건에 대한 센싱정보가 기설정된 사용자 정의 정책에 따른 정상범위를 이탈하였는지 여부를 판단한다(S230). 이때, 상기 사용자 정의 정책이란, 상기 수신단말의 외부 환경조건에 대해 센싱한 센싱정보의 정상여부를 판단하기 위한 기준 정보로서, 사용자에게 의해 정의 및 변경이 가능하다. 예를 들어, 상기 사용자 정의 정책은 측정 온도가 60도 미만인 경우에, 상기 수신단말의 외부 온도상태는 정상이라고 판단하거나, 또는 측정 습도가 30% 미만인 경우, 상기 수신단말의 외부 습도상태가 정상이라고 판단할 수 있다.
- [0034] 만약, 상기 수신단말이 측정한 센싱정보가 사용자 정의 정책에 따른 정상범위 예를 들면, 온도는 60도 또는 습도는 30% 를 초과하는지 여부를 판단한다(S240).
- [0035] 만약 상기 센싱정보가 기설정된 사용자 정의 정책에 따른 정상범위를 이탈하는 경우에는 그 이탈정도를 판단한다(S250).
- [0036] 예를 들어, 상기 센싱정보가 열감지센서에 의해 60도 온도를 5분동안 측정된 경우에, 이탈정도는 사용자 정의 정책에 의해 미리 설정된 레벨 1에 해당한다고 판단한다. 이러한 레벨 1은 사용자에게 의해 수신단말로 입력된 개인정보를 삭제한다. 이때, 상기 개인정보는 사용자에게 의해 입력된 정보로서, 전화번호부, 통화기록, 문자메시지, 사진 중 적어도 하나의 정보를 나타낸다.
- [0037] 또는 상기 센싱정보가 열감지센서에 의해 60도 온도를 10분 동안 측정된 경우에, 이탈정도는 사용자 정의 정책에 의해 미리 설정된 레벨 2에 해당한다고 판단한다. 이러한 레벨 2는 앞서 레벨 1에 해당하는 사용자로부터 입력된 개인정보와, 이에 더하여 수신단말의 시스템 파일정보를 삭제한다.
- [0038] 또는 상기 센싱정보가 열감지센서에 의해 70도 온도를 10분 동안 측정된 경우에, 이탈정도는 사용자 정의 정책에 의해 미리 설정된 레벨 3에 해당한다고 판단한다. 이러한 레벨 3은 수신단말의 하드웨어 파괴 예정을 나타내는 내용에 대한 메시지, 이미지 및 경고음 중 적어도 하나를 상기 수신단말의 외부로 표시하여 사용자에게 알려준다.
- [0039] 이후, 기설정된 시간 내 사용자로부터 별도의 입력이 없는 경우에, 상기 수신단말은 앞서 레벨 2에 해당하는 사용자로부터 입력된 개인정보 및 수신단말의 시스템 파일정보를 삭제하고, 상기 수신단말의 하드웨어를 파괴한다

(S253). 이러한 레벨 3의 경우에는 수신단말의 외부 환경상태가 회복 불가능의 심각한 상태로 판단한 것이다. 따라서, 상기 수신단말의 하드웨어를 파괴하기 위해, 상기 수신단말의 CPU와 ROM으로 전원이 인가되는 전원부에 스위치회로를 추가로 구성하고, 상기 레벨 3에 해당하는 명령이 발생하는 경우에, 상기 수신단말은 상기 CPU와 ROM에 인가되는 전원의 극성을 반대로 변경하여 인가함으로써, 상기 수신단말의 하드웨어를 물리적으로 파괴할 수 있게 된다.

- [0040] 특히, 상기 수신단말에 기저장된 사용자의 개인정보를 삭제하기에 앞서, 상기 수신단말은 통신 네트워크에 연결된 데이터 백업 서버로 상기 사용자의 개인정보를 전송하여, 상기 사용자의 개인정보를 백업한다.
- [0041] 이러한 상기 수신단말에 대한 원격제어모드를 해지하기 위해서는 송신단말이 원격 제어 해지정보를 포함하는 호 접속정보를 상기 수신단말로 전송하는 경우에만 상기 수신단말에 대한 원격제어모드가 해지될 수 있을 뿐, 상기 수신단말이 스스로 원격제어모드의 해지를 수행할 수 없다.
- [0042] 또한, 상술한 실시 예 외에도, 상기 단말간 호 접속정보를 송수신하는 단계를 대신하여, 송신단말이 원격제어하고자 하는 수신단말로 직접적으로 원격제어 트리거정보를 포함하는 호 접속정보를 전송하는 것이 아닌, 호 수락 제어 서버에 기설정된 사용자 정의 정책을 미리 저장하여 기저장된 호 수락 제어서버로 송신단말이 호 접속정보를 전송한다.
- [0043] 이후, 수신단말의 원격제어과정을 송신단말이 직접 수행하는 것이 아닌, 기정의된 사용자 정의 정책을 호 수락 제어서버에 미리 저장함으로써, 수신단말이 측정한 센싱정보가 사용자 정의 정책에 따른 정상범위를 벗어나 이탈하였다고 판단한 경우, 상기 호 수락 제어서버에 저장된 사용자 정의 정책에 의해 수신단말의 원격제어가 수행될 수 있다.
- [0044] 또한, 이러한 본 발명은 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체에 저장될 수 있다. 이때, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.
- [0045] 본 발명의 단말간 원격제어를 이용한 개인정보 유출 방지 방법은 원거리에 떨어져 있는 수신단말로 원격제어를 수행하도록 하는 원격제어 트리거정보를 포함하는 호 접속정보를 전송하여 송신단말이 상기 수신단말에 대한 원격제어를 수행할 수 있는 효과가 있다.
- [0046] 또한, 본 발명의 단말간 원격제어를 이용한 개인정보 유출 방지 방법은 원거리에 떨어져 있는 단말의 외부 환경조건을 측정하고, 측정한 외부 환경조건이 기설정된 임계치를 이탈하는 경우에는 이탈정도에 따라 상기 단말에 저장된 사용자의 개인정보를 차등적으로 삭제함으로써, 상기 사용자의 개인정보가 외부로 유출되는 것을 방지할 수 있는 효과가 있다.
- [0047] 더불어, 본 발명의 단말간 원격제어를 이용한 개인정보 유출 방지 방법은 단말에 저장된 사용자의 개인정보를 삭제하기에 앞서, 상기 단말에 저장된 사용자의 개인정보를 데이터 백업 서버로 전송함으로써, 상기 사용자의 개인정보가 단말에서 불가피하게 삭제되더라도, 해당 개인정보가 필요한 경우에는 데이터 백업 서버에 접속하여 백업된 사용자의 개인정보를 용이하게 획득할 수 있는 효과가 있다.
- [0048] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

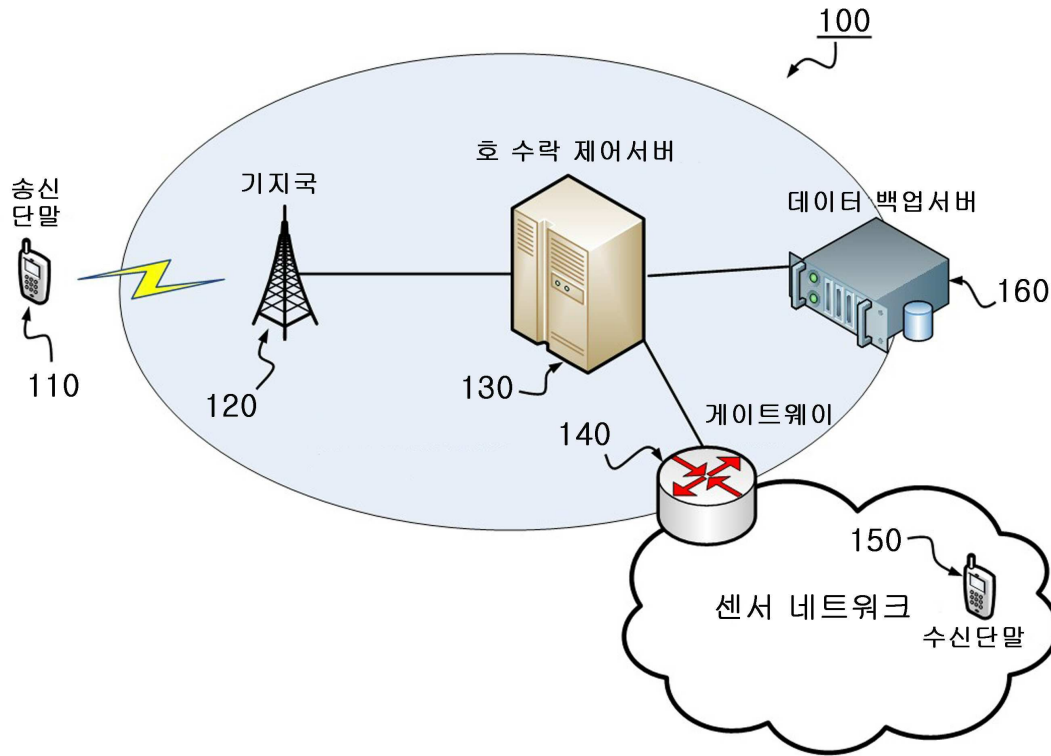
부호의 설명

- [0049] S210: 복수 개의 단말간 호 접속정보를 송수신함
- S220: 단말의 외부 환경조건에 대한 센싱정보를 획득함
- S230: 획득한 센싱정보가 기설정된 사용자 정의 정책에 따른 정상범위를 이탈하였는지 여부를 판단함
- S240: 센싱정보가 사용자 정의 정책에 따른 정상범위를 이탈하였는지 여부를 비교함

S250: 센싱정보의 사용자 정의 정책에 따른 정상 범위에 대한 이탈정도를 판단함

도면

도면1



도면2

