(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년04월28일
(11) 등록번호 10-1389682
(24) 등록일자 2014년04월21일

(51) 국제특허분류(Int. Cl.)
G06F 21/00 (2006.01) *G06F 15/16* (2006.01)
(21) 출원번호 10-2011-0085008
(22) 출원일자 2011년08월25일
심사청구일자 2011년10월25일
(65) 공개번호 10-2013-0022189
(43) 공개일자 2013년03월06일
(56) 선행기술조사문헌
KR100794136 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 팬택
서울특별시 마포구 성암로 179 (상암동,팬택계열 알앤디센터빌딩)
(72) 발명자
이세현
서울특별시 마포구 성암로 179, DMC I- 2 팬택빌딩 (상암동)
김보선
서울특별시 마포구 성암로 179, DMC I- 2 팬택빌딩 (상암동)
허수영
서울특별시 마포구 성암로 179, DMC I- 2 팬택빌딩 (상암동)
(74) 대리인
특허법인무한

전체 청구항 수 : 총 14 항 심사관 : 김동성

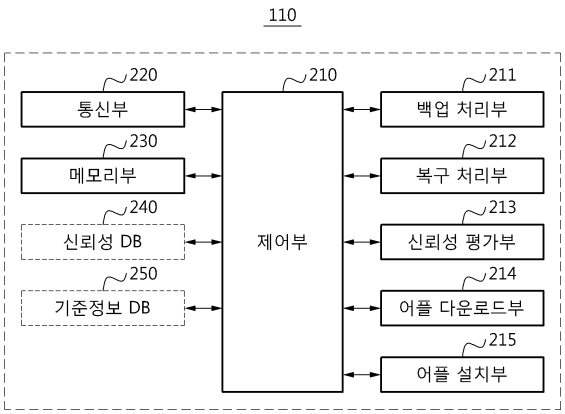
(54) 발명의 명칭 **바이러스 피해를 방지하는 시스템 및 방법**

(57) 요 약

본 발명은 바이러스 피해를 방지하는 시스템 및 방법에 관한 것이다. 단말 장치는 데이터를 클라우드 서버에 백업하고, 클라우드 서버는 단말 장치와 동일한 동작을 수행하는 가상 장치를 생성하고, 단말 장치에 설치하고자 하는 어플을 가상 장치에 먼저 어플을 설치함으로써 단말 장치에 어플을 설치하기 전에 바이러스를 검색한다.

또한, 본 발명의 단말 장치는 백업 데이터를 클라우드 서버에 저장하고, 단말 장치의 이상시 클라우드 서버로부터 저장된 백업 데이터를 수신해서 단말 장치를 복구한다.

대 표 도 - 도2



특허청구의 범위

청구항 1

단말 장치에 있어서,

어플의 신뢰도에 관한 정보 및 상기 어플의 신뢰도를 평가하는 기준이 되는 정보인 기준정보를 이용하여 어플의 신뢰성을 평가하는 신뢰성 평가부;

상기 신뢰성 평가부의 평가결과 상기 어플의 신뢰성이 기설정한 기준 이하이면, 클라우드 서버로 상기 어플의 바이러스 검색을 요청하고, 상기 클라우드 서버로부터 상기 어플에 바이러스가 없다는 검색결과를 수신하면 어플 공급 서버로부터 상기 어플을 다운받는 어플 다운로드부;

상기 어플 다운로드부에서 다운받은 상기 어플을 설치하는 어플 설치부; 및

백업 데이터를 생성해서 상기 클라우드 서버로 송신하는 백업 처리부 - 상기 백업 데이터는, 상기 클라우드 서버에서 상기 단말 장치와 동일한 기능을 수행할 수 있는 가상 장치를 생성할 때 필요로 하는 데이터이고, 상기 가상 장치는, 상기 단말 장치의 운영체제와는 독립된 운영체제를 이용함 -;를 포함하는

바이러스 피해를 방지하는 시스템의 단말 장치.

청구항 2

제1항에 있어서,

상기 어플 다운로드부는,

상기 신뢰성 평가부의 평가결과 상기 어플의 신뢰성이 기설정한 기준 보다 높으면, 상기 어플 공급 서버로부터 상기 어플을 다운받는

바이러스 피해를 방지하는 시스템의 단말 장치.

청구항 3

제1항에 있어서,

상기 신뢰성 평가부는,

상기 클라우드 서버로 상기 어플에 대한 신뢰성 평가를 요청하고 상기 클라우드 서버로부터 상기 어플에 대한 신뢰성 평가결과를 수신해서 상기 어플의 신뢰성을 평가하는,

바이러스 피해를 방지하는 시스템의 단말 장치.

청구항 4

제1항에 있어서,

상기 어플의 신뢰도에 관한 정보를 저장한 신뢰성 데이터베이스를 더 포함하고,

상기 신뢰성 평가부는,

상기 신뢰성 데이터베이스에서 상기 어플을 검색해서 상기 어플의 신뢰성을 평가하는

바이러스 피해를 방지하는 시스템의 단말 장치.

청구항 5

제1항에 있어서,

상기 기준정보를 저장한 기준정보 데이터베이스를 더 포함하고,

상기 신뢰성 평가부는,

상기 어플 공급 서버로부터 상기 어플에 관한 기본정보를 수신하고, 상기 기본정보가 상기 기준정보의 기준을 만족하면 신뢰성이 있다고 판단하는

바이러스 피해를 방지하는 시스템의 단말 장치.

청구항 6

제5항에 있어서,

상기 기준정보는,

신뢰성이 있는 카테고리, 신뢰성이 있는 생산자, 신뢰성이 있는 판매 서버, 신뢰성이 있는 기준 출시일자 및 신뢰성이 있는 권한 중에서 적어도 하나 또는 하나 이상의 조합으로 구성된 정보인

바이러스 피해를 방지하는 시스템의 단말 장치.

청구항 7

삭제

청구항 8

바이러스 검색을 요청 받은 어플을 어플 공급 서버로부터 다운로드하는 어플 다운로드부;

단말 장치와 동일한 기능을 수행할 수 있는 가상 장치를 생성하고 다운로드 받은 상기 어플을 상기 가상 장치에 설치하는 가상 장치 처리부;

어플의 신뢰도에 관한 정보 및 상기 어플의 신뢰도를 평가하는 기준이 되는 정보인 기준정보를 이용하여 어플의 신뢰성을 평가하는 신뢰성 평가부;

상기 가상 장치에 설치된 상기 어플에 바이러스가 존재하는 여부를 검색하고, 검색결과를 상기 단말 장치로 송신하는 바이러스 검색부; 및

상기 단말 장치로부터 백업 데이터를 수신하는 백업 처리부 - 상기 백업 데이터는, 상기 가상 장치를 생성할 때 필요로 하는 데이터임- 를 포함하고,

상기 가상 장치는, 상기 단말 장치의 운영체제와는 독립된 운영체제를 이용하는

바이러스 피해를 방지하는 시스템의 클라우드 서버.

청구항 9

제8항에 있어서,

상기 어플의 신뢰도에 관한 정보들을 저장한 신뢰성 데이터베이스를 더 포함하고,

상기 신뢰성 평가부는,

상기 단말 장치로부터 상기 어플의 신뢰성을 요청 받으면, 상기 신뢰성 데이터베이스에서 상기 어플을 검색해서 상기 어플의 신뢰성을 평가해서 상기 단말 장치로 제공하는

바이러스 피해를 방지하는 시스템의 클라우드 서버.

청구항 10

제8항에 있어서,

상기 바이러스 검색부는

상기 어플에 바이러스가 존재하는 여부를 검색한 결과를 포함하는 상기 어플의 신뢰도에 관한 정보를 상기 신뢰성 데이터베이스에 저장하는

바이러스 피해를 방지하는 시스템의 클라우드 서버.

청구항 11

삭제

청구항 12

제8항에 있어서,

상기 기준정보는,

신뢰성이 있는 카테고리, 신뢰성이 있는 생산자, 신뢰성이 있는 판매 서버, 신뢰성이 있는 기준 출시일자 및 신뢰성이 있는 권한 중에서 적어도 하나 또는 하나 이상의 조합으로 구성된 정보인

바이러스 피해를 방지하는 시스템의 클라우드 서버.

청구항 13

제9항에 있어서,

상기 기준정보를 저장한 기준정보 데이터베이스를 더 포함하고,

상기 신뢰성 평가부는,

상기 어플 공급 서버로부터 상기 어플에 관한 기본정보를 수신하고, 상기 기본정보가 상기 기준정보의 기준을 만족하면 신뢰성이 있다고 판단하는

바이러스 피해를 방지하는 시스템의 클라우드 서버.

청구항 14

제8항에 있어서,

상기 단말 장치로부터 상기 단말 장치와 동일한 기능을 수행할 수 있는 상기 가상 장치를 생성할 때 필요로 하는 데이터인 백업 데이터를 수신하는 백업 처리부를 더 포함하고,

상기 가상 장치 처리부는,

상기 단말 장치의 백업 데이터를 이용해서 상기 가상 장치를 생성하는

바이러스 피해를 방지하는 시스템의 클라우드 서버.

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

단말 장치에서 바이러스 피해를 방지하는 방법에 있어서,

신뢰성 평가부가 어플의 신뢰도에 관한 정보 및 상기 어플의 신뢰도를 평가하는 기준이 되는 정보인 기준정보를 이용하여 어플의 신뢰성을 평가하는 단계;

상기 신뢰성 평가부의 평가결과 상기 어플의 신뢰성이 기설정한 기준 이하이면, 클라우드 서버로 상기 어플의 바이러스 검색을 요청하는 단계;

상기 클라우드 서버로부터 상기 어플에 바이러스가 없다는 검색결과를 수신하면, 어플 다운로드부가 어플 공급 서버로부터 상기 어플을 다운받는 단계;

상기 어플 다운로드부에서 다운받은 상기 어플을 설치하는 단계;

상기 클라우드 서버에서 상기 단말 장치와 동일한 기능을 수행할 수 있는 가상 장치를 생성할 때 필요로 하는 데이터인 백업 데이터를 생성하는 단계; 및

상기 백업 데이터를 상기 클라우드 서버로 송신하는 단계- 상기 백업 데이터는, 상기 클라우드 서버에서 상기 단말 장치와 동일한 기능을 수행할 수 있는 가상 장치를 생성할 때 필요로 하는 데이터이고, 상기 가상 장치는, 상기 단말 장치의 운영체제와는 독립된 운영체제를 이용함 -

를 포함하는 방법.

청구항 22

삭제

청구항 23

삭제

청구항 24

제1항에 있어서,

상기 어플 다운로드부는,

상기 어플에 바이러스가 존재한다는 검색결과를 수신하면, 다운받은 상기 어플을 삭제하는

바이러스 피해를 방지하는 시스템의 단말 장치.

명 세 서

기 술 분 야

[0001] 본 발명은 단말 장치를 클라우드 서버에 백업하고, 클라우드 서버를 통해 설치하고자 하는 어플의 바이러스를 검색함으로 해서 단말 장치에 바이러스 피해를 방지하는 시스템에 관한 것이다.

배 경 기 술

[0002] 휴대용 단말기의 급격한 발달에 따라 특히 무선 음성 통화 및 정보 교환이 가능한 휴대폰은 필수품이 되었다. 휴대용 단말기 초기에는 단순히 휴대할 수 있고, 무선 통화가 가능한 것으로 인식되었으나, 그 기술이 발달함과 무선 인터넷의 도입에 따라 휴대용 단말기는 통화뿐 아니라 단순한 전화 통화 또는 일정 관리 등의 목적뿐만 아니라 장착된 디지털 카메라에 의한 이미지 촬영하거나, 위성 방송의 시청, 게임, 무선 인터넷을 통한 웹서핑, 블루투스를 이용한 무선 장치와의 연결 서비스, 음악청취 및, 이메일 서비스 등 그 활용범위가 갈수록 커지고 있다.

[0003] 또한, 휴대용 단말기는 제조사에서 제공하는 응용 프로그램 외에도 사용자의 선택에 의한 다양한 응용 프로그램이 설치될 수 있다. 하지만, 응용 프로그램을 설치하기 전에는 악성코드가 포함되어 있는 여부를 확인하기 어려워서 악성코드가 삽입된 응용 프로그램이 설치되는 문제가 발생할 수 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명의 실시예는 단말 장치와 동일하게 동작할 수 있는 가상 장치를 생성할 수 있는 데이터들을 백업 데이터로 생성해서 클라우드 서버에 저장 함으로써 단말 장치에 문제 발생시 클라우드 서버에 저장한 백업 데이터를 이용해서 단말 장치를 복구하는 방법을 제공한다.

[0005] 본 발명의 실시예는 단말 장치에서 메모리부에 저장된 데이터들을 백업 데이터로 송신하고, 클라우드 서버는 백업 데이터를 이용해서 단말 장치와 동일하게 동작하는 가상 장치를 생성하고, 가상 장치에 단말 장치에 설치될 응용 프로그램을 미리 설치해서 바이러스 검사를 수행함으로써 바이러스 피해를 방지하는 시스템 및 방법을 제공한다.

과제의 해결 수단

[0006] 본 발명의 실시예에 따른 바이러스 피해를 방지하는 시스템의 단말 장치는, 어플의 신뢰성을 평가하는 신뢰성 평가부; 상기 신뢰성 평가부의 평가결과 상기 어플의 신뢰성이 기설정한 기준 이하이면, 클라우드 서버로 상기 어플의 바이러스 검색을 요청하고, 상기 클라우드 서버로부터 상기 어플에 바이러스가 없다는 검색결과를 수신하면 어플 공급 서버로부터 상기 어플을 다운받는 어플 다운로드부; 및 상기 어플 다운로드부에서 다운받은 상기 어플을 설치하는 어플 설치부를 포함한다.

[0007] 본 발명의 실시예에 따른 바이러스 피해를 방지하는 시스템의 클라우드 서버는, 바이러스 검색을 요청 받은 어플을 어플 공급 서버로부터 다운로드하는 어플 다운로드부; 단말 장치와 동일한 기능을 수행할 수 있는 가상 장치를 생성하고 다운로드 받은 상기 어플을 상기 가상 장치에 설치하는 가상 장치 처리부; 및 상기 가장 장치에 설치된 상기 어플에 바이러스가 존재하는 여부를 검색하고, 검색결과를 상기 단말 장치로 송신하는 바이러스 검색부를 포함한다.

[0008] 본 발명의 실시예에 따른 바이러스 피해를 방지하는 시스템에서 데이터를 백업하는 단말 장치는, 설치된 어플, 상기 어플의 변경이력 정보, 사용자 데이터 및 시스템 데이터 중에서 적어도 하나를 저장하는 메모리부; 및 상기 메모리부에 저장된 데이터를 백업 데이터로 생성해서 클라우드 서버로 송신하는 백업 처리부를 포함한다.

[0009] 본 발명의 실시예에 따른 단말 장치에서 바이러스 피해를 방지하는 방법은, 어플의 신뢰성을 평가하는 단계; 평가결과 상기 어플의 신뢰성이 기설정한 기준 이하이면, 클라우드 서버로 상기 어플의 바이러스 검색을 요청하는 단계; 상기 클라우드 서버로부터 상기 어플에 바이러스가 없다는 검색결과를 수신하면 어플 공급 서버부터 상기

어플을 다운받는 단계; 및 다운받은 상기 어플을 설치하는 단계를 포함한다.

[0010] 본 발명의 실시예에 따른 클라우드 서버에서 바이러스 피해를 방지하는 방법은, 단말 장치와 동일한 기능을 수행할 수 있는 가상 장치를 생성하는 단계; 상기 단말 장치로부터 어플의 바이러스 검색을 요청 받으면, 상기 어플을 어플 공급 서버로부터 다운로드하는 단계; 다운로드 받은 상기 어플을 상기 가상 장치에 설치하는 단계; 및 상기 가장 장치에 설치된 상기 어플에 바이러스가 존재하는 여부를 검색하고, 검색결과를 상기 단말 장치로 송신하는 단계를 포함한다.

발명의 효과

[0011] 본 발명은 단말 장치를 클라우드 서버에 백업하고, 클라우드 서버를 통해 설치하고자 하는 어플의 바이러스를 검색하는 시스템에 관한 것으로, 단말 장치에 신뢰성이 없는 어플을 설치하지 않음으로써 단말 장치에 바이러스를 포함한 어플이 설치됨으로 발생할 수 있는 피해를 사전에 방지할 수 있다.

도면의 간단한 설명

[0012] 도 1은 바이러스 피해를 방지하는 시스템의 개략적인 구성을 도시한 도면이다.

도 2는 바이러스 피해를 방지하는 시스템에서 단말 장치의 구성을 도시한 도면이다.

도 3은 바이러스 피해를 방지하는 시스템에서 클라우드 서버의 구성을 도시한 도면이다.

도 4는 신뢰성 데이터베이스의 예를 도시한 도면이다.

도 5는 바이러스 피해를 방지한 단말 장치에서 어플을 설치하는 과정을 도시한 흐름도이다.

도 6은 바이러스 피해를 방지한 클라우드 서버에서 어플의 바이러스 여부를 검색하는 과정을 도시한 흐름도이다.

도 7은 단말 장치에서 데이터를 백업하고 복구하는 과정을 도시한 흐름도이다.

도 8은 클라우드 서버에서 신뢰성을 판단하는 기준정보 생성하는 과정을 도시한 흐름도이다.

도 9는 바이러스 피해를 방지하는 시스템에서 단말 장치의 다른 구성 예를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0013] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0014] 본 발명의 설명에 앞서 이하의 설명에서 응용 프로그램, 어플리케이션(application) 및 펌웨어(firmware)를 어플로 칭한다.

[0015] 도 1은 바이러스 피해를 방지하는 시스템의 개략적인 구성을 도시한 도면이다.

[0016] 도 1을 참조하면 바이러스 피해를 방지하는 시스템은 크게 단말 장치(110), 클라우드 서버(120) 및 어플 공급 서버(130)를 포함한다.

[0017] 단말 장치(110)는 단말 장치(110)에 포함된 모든 데이터 또는 일부 데이터를 백업 데이터로 생성해서 네트워크(100)를 통해 클라우드 서버(120)로 송신한다.

[0018] 그리고, 단말 장치(110)는 시스템 오류 내지 바이러스 발견 등의 문제가 발생하면 클라우드 서버(120)에 저장한 백업 데이터를 이용해서 단말 장치(110)를 복구 할 수 있다.

[0019] 또한, 단말 장치(110)는 어플 공급 서버(130)로부터 어플을 다운받아 설치하기 이전에 클라우드 서버(120)로 설치하고자 하는 어플의 바이러스 검색을 요청할 수 있다.

[0020] 클라우드 서버(120)는 단말 장치(110)로부터 수신한 백업 데이터를 이용해서 단말 장치(110)와 동일하게 동작하는 가상 장치를 생성하고, 단말 장치(110)로부터 어플의 바이러스 검색을 요청 받으면, 어플 공급 서버(130)로부터 어플을 다운받아 가상 장치에 설치하고, 바이러스 검색해서 검색결과를 단말 장치(110)로 제공 한다.

[0021] 그러면, 단말 장치(110)와 클라우드 서버(120)의 구체적인 설명이 이하 도 2와 도 3을 참조해서 후술한다.

[0022] 도 2는 바이러스 피해를 방지하는 시스템에서 단말 장치의 구성을 도시한 도면이다.

[0023] 도 2를 참조하면 단말 장치(110)는 제어부(210), 백업 처리부(211), 복구 처리부(212), 신뢰성 평가부(213), 어플 다운로드부(214), 어플 설치부(215), 통신부(220), 메모리부(230)를 포함한다. 또한, 단말 장치(110)는 추가로 신뢰성 데이터베이스(240)과 기준정보 데이터베이스(250) 중 하나 내지는 모두를 더 포함할 수도 있다.

[0024] 통신부(220)는 유/무선으로 네트워크를 통해 클라우드 서버(120) 또는 어플 공급 서버(130)와 데이터를 송수신한다. 통신부(220)는 FDMA(Frequency Division Multiple Access), TDMA(Time Division Multiple Access), SDMA(Space-Division Multiple Access), CDMA(Code Division Multiple Access), WCDMA(Wideband Code Division Multiple Access), OFDM, Wifi, 와이브로(Wibro), 블루투스, 적외선 통신 등을 기반으로 하는 무선 통신 기법을 통해 무선으로 데이터를 송수신할 수 있다. 무선으로 통신하는 통신부(220)는 안테나를 통해 입출력되는 데이터의 무선신호를 송수신 처리하는 기능을 수행할 수 있다. 예를 들어, 송신인 경우, 송신할 데이터를 채널 코딩(Channel coding) 및 확산(Spreading)한 후, RF처리하여 송신하는 기능을 수행하고, 수신인 경우, 수신된 RF신호를 기저대역신호로 변환하고 상기 기저대역신호를 역 확산(De-spreading) 및 채널 복호(Channel decoding)하여 데이터를 복원하는 기능을 수행한다. 단말 장치(110)의 구성요소가 클라우드 서버(120) 또는 어플 공급 서버(130)와 데이터를 송수신함은 모두 통신부(220)를 통해 이루어 지는 것임으로 이하의 설명에서 통신부(220)를 통한다는 내용은 생략한다.

[0025] 메모리부(230)는 단말 장치(110)의 전반적인 동작을 제어하기 위한 운영체제에 속하는 시스템 데이터, 설치된 어플, 어플의 변경이력 정보 및 사용자 데이터(전화번호, SMS 메시지, 압축된 이미지 파일, 동영상 등) 등을 저장한다. 그리고, 메모리부(230)는 백업 처리부(211)에서 생성한 백업 데이터 또는 클라우드 서버(120)로부터 수신하는 백업 데이터를 저장할 수도 있다.

[0026] 신뢰성 데이터베이스(240)는 어플들 각각에 대한 신뢰도에 관한 정보들을 저장한다. 이때, 신뢰성 데이터베이스(240)에 저장된 어플들 각각에 대한 신뢰도에 관한 정보들은 클라우드 서버(120) 또는 신뢰성을 평가하는 별도의 서버로부터 제공받을 수 있다.

[0027] 기준정보 데이터베이스(250)는 어플의 신뢰도를 평가하는 기준이 되는 정보인 기준정보를 저장한다. 이때, 기준정보 데이터베이스(250)에 저장된 기준정보는 클라우드 서버(120) 또는 기준정보를 생성하는 별도의 서버로부터 제공받을 수 있다. 여기서, 기준정보는 신뢰성이 있는 카테고리, 신뢰성이 있는 생산자, 신뢰성이 있는 판매 서버, 신뢰성이 있는 기준 출시일자 및 신뢰성이 있는 권한 중에서 적어도 하나 또는 하나 이상의 조합으로 구성된 정보일 수 있다.

[0028] 예를 들어, 기준정보가 판매 서버 P인 경우, 판매 서버 P를 통해 판매되는 어플들은 신뢰할 수 있다. 다른 예로 기준정보가 생산자 A인 경우, 생산자 A가 생성한 어플은 신뢰할 수 있다. 또 다른 예로 기준정보가 판매 서버 P와 생산자 A의 조합인 경우, 판매 서버 P를 통해 판매되는 생산자 A가 생성하는 어플은 신뢰할 수 있다.

[0029] 백업 처리부(211)는 메모리부(230)에 저장된 모든 데이터 또는 일부 데이터를 백업 데이터로 생성해서 클라우드 서버로 송신한다. 이때, 백업 데이터는 생성시점을 나타내는 타임 스템프(Time stamp)를 포함할 수 있다.

[0030] 백업 처리부(211)는 초기에 메모리부(230)에 저장된 모든 데이터를 백업 데이터를 생성해서 클라우드 서버로 송신하고, 이후, 변경 또는 추가된 데이터를 압축해서 업데이트 데이터를 생성해서 클라우드 서버로 송신할 수 있다.

[0031] 백업 처리부(211)는 클라우드 서버(120)에서 단말 장치(110)와 동일한 기능을 수행할 수 있는 가상 장치를 생성할 때 필요로 하는 데이터를 포함하는 백업 데이터를 생성한다. 이때, 가상 장치를 생성할 때 필요로 하는 데이터는 시스템 데이터, 설치된 어플 및 어플의 변경이력 정보를 포함하고, 추가로 사용자 데이터(전화번호, SMS 메시지, 압축된 이미지 파일, 동영상 등)를 더 포함할 수도 있다.

[0032] 백업 처리부(211)는 백업 데이터를 생성할 때, 메모리부(230)에 저장된 데이터를 블록 단위로 읽고(read), 압축해서 백업 데이터를 생성할 수 있다.

[0033] 또한, 백업 처리부(211)는 업데이트 이벤트의 발생을 감지하면 업데이트 데이터를 생성해서 클라우드 서버(120)로 송신한다. 업데이트 데이터는 생성시점을 나타내는 타임 스템프(Time stamp)를 포함할 수 있다.

[0034] 백업 처리부(211)는 변경 또는 추가된 데이터를 압축해서 업데이트 데이터를 생성할 수도 있고, 메모리부(230)

의 변경된 블록을 블록 단위로 압축해서 업데이트 데이터를 생성할 수도 있다. 블록 단위로 업데이트 데이터를 생성하는 경우, 하나의 블록 내에는 변경된 데이터와 변경되지 않은 데이터가 포함될 수 있다. 이 경우 변경되지 않은 데이터도 같이 압축하기 때문에 자원의 낭비가 발생할 수 있지만, 클라우드 서버(120) 측에서 백업 데이터를 최신 데이터로 관리하기 용이한 장점이 있다.

[0035] 백업 처리부(211)는 업데이트 이벤트의 발생을 아래의 경우에 감지할 수 있다. 백업 처리부(211)는 메모리부에 저장된 데이터의 내용이 변경 또는 추가된 경우, 메모리부에 저장된 데이터의 내용이 변경 또는 추가된 횟수가 기설정된 횟수 이상인 경우, 메모리부에 저장된 데이터의 내용이 변경 또는 추가된 데이터의 양이 기설정된 데이터양을 초과한 경우, 메모리부의 블록이 변경된 경우, 메모리부의 블록이 변경되는 횟수가 기설정된 횟수 이상인 경우, 메모리부의 블록들 중에서 변경된 블록이 기설정된 개수 이상인 경우, 기설정된 업데이트 시간간격을 초과한 경우 및 사용자의 요청을 감지한 경우 중에서 적어도 하나의 경우에 업데이트 이벤트의 발생으로 감지한다.

[0036] 복구 처리부(212)는 단말 장치(110)의 시스템 오류, 바이러스 발견 또는 사용자의 요청에 따라 클라우드 서버(120)로 백업 데이터를 요청하고, 클라우드 서버(120)로부터 백업 데이터를 수신해서 단말 장치(110)를 복구한다. 이때, 수신하는 백업 데이터는 마지막 업데이트 데이터가 적용된 가장 최근의 백업 데이터이다. 하지만, 복구 처리부(212)는 사용자의 요청에 따라 특정 시점에 저장된 백업 데이터를 수신해서 특정 시점으로 복구할 수도 있다.

[0037] 신뢰성 평가부(213)는 사용자가 설치하고자 하는 어플의 신뢰성을 평가한다. 신뢰성 평가부(213)는 여러가지 방법을 통해 신뢰성을 평가할 수 있다. 신뢰성 평가부(213)가 신뢰성을 평가하는 예는 다음과 같다.

[0038] 신뢰성 평가부(213)는 클라우드 서버(120)로 어플에 대한 신뢰성 평가를 요청하고 클라우드 서버(120)로부터 어플에 대한 신뢰성 평가결과를 수신해서 어플의 신뢰성을 평가할 수 있다.

[0039] 신뢰성 평가부(213)는 신뢰성 데이터베이스(240)에서 어플을 검색해서 어플의 신뢰성을 평가할 수도 있다.

[0040] 신뢰성 평가부(213)는 어플 공급 서버(130)로부터 어플에 관한 기본정보를 수신하고, 기본정보가 기준정보 데이터베이스(250)에 저장되어 있는 기준을 만족하는지 여부를 판단해서 신뢰성을 평가할 수 있다.

[0041] 여기서, 기본정보는 어플의 카테고리, 어플의 생산자, 어플의 판매 서버, 어플의 출시일자 및 어플의 권한 등을 포함할 수 있다. 그리고, 기준정보는 신뢰성이 있는 카테고리, 신뢰성이 있는 생산자, 신뢰성이 있는 판매 서버, 신뢰성이 있는 기준 출시일자 및 신뢰성이 있는 권한 중에서 적어도 하나 또는 하나 이상의 조합으로 구성된 정보일 수 있다. 기준정보의 예를 들면, 특정 생산자가 생성한 어플은 모두 신뢰할 수 있다, 특정 판매 서버를 통해 판매되는 특정 생산자의 특정 출시일자 이전에 생성된 어플은 모두 신뢰할 수 있다. 특정 판매 서버를 통해 판매되는 특정 카테고리의 어플들은 모두 신뢰할 수 있다. 특정 판매 서버를 통해 판매되는 어플들 중에서 특정 권한만을 가진 어플들은 모두 신뢰 할 수 있다. 등등이 될 수 있다.

[0042] 예를 들어, 기준정보가 판매 서버 P인 경우, 판매 서버 P를 통해 판매되는 어플들은 신뢰할 수 있다. 다른 예로 기준정보가 생산자 A인 경우, 생산자 A가 생성한 어플은 신뢰할 수 있다. 또 다른 예로 기준정보가 판매 서버 P와 생산자 A의 조합인 경우, 판매 서버 P를 통해 판매되는 생산자 A가 생성하는 어플은 신뢰할 수 있다.

[0043] 어플 다운로드부(214)는 신뢰성 평가부(213)의 평가결과 어플의 신뢰성이 기설정한 기준 보다 높으면, 어플 공급 서버(130)로부터 어플을 다운받는다.

[0044] 또한, 어플 다운로드부(214)는 신뢰성 평가부(213)의 평가결과 어플의 신뢰성이 기설정한 기준 이하이면, 클라우드 서버(120)로 어플의 바이러스 검색을 요청하고, 클라우드 서버(120)로부터 어플에 바이러스가 없다는 검색결과를 수신하면 어플 공급 서버(130)로부터 어플을 다운받는다.

[0045] 어플 설치부(215)는 어플 다운로드부(214)에서 다운받은 어플을 설치한다.

[0046] 제어부(210)는 단말 장치(110)의 전반적인 동작을 제어할 수 있다. 그리고, 제어부(210)는 백업 처리부(211), 복구 처리부(212), 신뢰성 평가부(213), 어플 다운로드부(214) 및 어플 설치부(215)의 기능을 수행할 수 있다. 제어부(210), 백업 처리부(211), 복구 처리부(212), 신뢰성 평가부(213), 어플 다운로드부(214) 및 어플 설치부(215)를 구분하여 도시한 것은 각 기능들을 구별하여 설명하기 위함이다. 따라서 제어부(210)는 백업 처리부(211), 복구 처리부(212), 신뢰성 평가부(213), 어플 다운로드부(214) 및 어플 설치부(215) 각각의 기능을 수행하도록 구성된(configured) 적어도 하나의 프로세서를 포함할 수 있다. 또한, 제어부(210)는 백업 처리부(211), 복구 처리부(212), 신뢰성 평가부(213), 어플 다운로드부(214) 및 어플 설치부(215) 각각의 기능 중 일

부를 수행하도록 구성된(configured) 적어도 하나의 프로세서를 포함할 수 있다.

[0047] 도 3은 바이러스 피해를 방지하는 시스템에서 클라우드 서버의 구성을 도시한 도면이다.

[0048] 도 3을 참조하면 클라우드 서버(120)는 제어부(310), 백업 처리부(311), 복구 처리부(312), 가상 장치 처리부(313), 신뢰성 평가부(314), 어플 다운로드부(315), 바이러스 검색부(316), 통신부(320), 백업 데이터 저장부(330), 신뢰성 데이터베이스(340)를 포함한다. 또한, 클라우드 서버(120)는 추가로 기준정보 생성부(317)과 기준정보 데이터베이스(350)를 더 포함할 수도 있다.

[0049] 통신부(320)는 네트워크를 통해 단말 장치(110) 또는 어플 공급 서버(130)와 데이터를 송수신한다. 클라우드 서버(120)가 단말 장치(110) 또는 어플 공급 서버(130)와 데이터를 송수신함은 모두 통신부(320)를 통해 이루어지는 것임으로 이하의 설명에서 통신부(320)를 통한다는 내용은 생략한다.

[0050] 백업 데이터 저장부(330)는 단말 장치(110)로부터 수신한 백업 데이터와 업데이트 데이터를 저장한다. 백업 데이터 저장부(330)는 백업 데이터와 업데이트 데이터가 수신된 시점 또는 생성된 시점을 나타내는 타임 스탬프를 함께 저장한다. 즉, 백업 데이터 저장부(330)는 백업 데이터와 업데이트 데이터를 수신된 시간 또는 생성된 시간에 따라 관리한다.

[0051] 신뢰성 데이터베이스(340)는 어플들 각각에 대한 신뢰도에 관한 정보들을 저장한다. 신뢰성 데이터베이스(340)는 아래 도 4와 같이 구성될 수 도 있다.

[0052] 도 4는 신뢰성 데이터베이스의 예를 도시한 도면이다.

[0053] 도 4를 참조하면, 신뢰성 데이터베이스는 각 어플별로 다운로드 받은 시간, 설치 시각, 공급자 정보, 출시일자, 권한, 신뢰성 여부, 사용한 바이러스 검색 엔진정보 및 사용자 리뷰정보 등을 포함할 수 있다.

[0054] 기준정보 데이터베이스(350)는 어플의 신뢰도를 평가하는 기준이 되는 정보인 기준정보를 저장한다. 여기서, 기준정보는 신뢰성이 있는 카테고리, 신뢰성이 있는 생산자, 신뢰성이 있는 판매 서버, 신뢰성이 있는 기준 출시일자 및 신뢰성이 있는 권한 중에서 적어도 하나 또는 하나 이상의 조합으로 구성된 정보일 수 있다.

[0055] 백업 처리부(311)는 단말 장치(110)의 메모리부에 저장된 모든 데이터 또는 일부 데이터를 이용해서 생성된 백업 데이터를 수신하면, 백업 데이터를 백업 데이터 저장부(330)에 저장한다. 클라우드 서버(120)에서 어플의 바이러스를 선 검색을 하는 경우, 백업 데이터는 단말 장치(110)와 동일한 기능을 수행할 수 있는 가상 장치를 생성할 때 필요로 하는 데이터를 포함한다. 이때, 가상 장치를 생성할 때 필요로 하는 데이터는 단말 장치(110)의 시스템 데이터, 설치된 어플 및 어플의 변경이력 정보를 포함하고, 추가로 사용자 데이터(전화번호, SMS 메시지, 압축된 이미지 파일, 동영상 등)를 더 포함할 수도 있다.

[0056] 또한, 백업 처리부(311)는 단말 장치(110)로부터 업데이트 데이터를 수신하면 수신한 업데이트 데이터를 백업 데이터 저장부(330)에 저장한다. 이때, 백업 처리부(311)는 백업 데이터와 업데이트 데이터의 각각에 포함된 타임 스탬프를 이용해서 백업 데이터와 업데이트 데이터를 관리한다.

[0057] 복구 처리부(312)는 단말 장치(110)로부터 백업 데이터를 요청 받으면, 해당 단말 장치(110)의 백업 데이터를 백업 데이터 저장부(330)에서 검색해서 단말 장치(110)로 송신한다. 이때, 송신하는 백업 데이터는 마지막 업데이트 데이터가 적용된 가장 최근의 백업 데이터이다. 하지만, 복구 처리부(312)는 단말 장치(110)로부터 특정 시점에 저장된 백업 데이터를 요청받는 경우, 백업 데이터 저장부(330)에 저장된 백업 데이터와 업데이트 데이터의 타임 스탬프를 이용해서 특정 시점의 백업 데이터를 송신한다.

[0058] 신뢰성 평가부(314)는 단말 장치(110)로부터 어플의 신뢰성을 요청 받으면, 어플의 신뢰성을 평가하고 평가결과를 단말 장치(110)로 제공한다. 이때, 신뢰성 평가부(314)는 아래 방법으로 통해 어플의 신뢰성을 평가할 수 있다.

[0059] 신뢰성 평가부(314)는 신뢰성 데이터베이스(340)에서 신뢰성을 요청 받은 어플을 검색해서 어플의 신뢰성을 평가할 수 있다.

[0060] 다른 방법으로, 신뢰성 평가부(314)는 어플 공급 서버(130)로부터 어플에 관한 기본정보를 수신하고, 기본정보가 기준정보 데이터베이스(350)에 저장된 기준정보의 기준을 만족하는지 여부를 판단해서 신뢰성을 평가할 수 있다. 여기서, 기준정보는 어플의 신뢰도를 평가하는 기준이 되는 정보이다.

[0061] 어플 다운로드부(315)는 바이러스 검색을 요청 받은 어플을 어플 공급 서버(130)에 요청해서 다운로드 받는다.

[0062] 가상 장치 처리부(313)는 단말 장치(110)의 백업 데이터를 이용해서 단말 장치(110)와 동일한 동작을 수행하는 가상 장치(318)를 생성한다. 이때, 가상 장치(318)는 클라우드 서버(120)의 프레임워크(framework)나 운영체제를 이용해서 단말 장치(110)의 프레임워크(framework)나 운영체제를 이용하는 것과 같은 동작을 하는 클라우드 서버(120)에 존재하는 가상의 장치이다. 가상 장치 처리부(313)는 가상 장치(318)를 생성하면, 생성한 가상장치에 어플 다운로드부(315)를 통해 다운로드 받은 어플을 설치한다. 즉, 가상 장치 처리부(313)는 사용자가 단말 장치(110)에 설치하고자 하는 어플을 바이러스 검사를 위해 클라우드 서버(120)에 존재하는 가상 장치(318)에 먼저 설치한다.

[0063] 바이러스 검색부(316)는 가장 장치(318)에 설치된 어플에 바이러스가 존재하는 여부를 검색하고, 검색결과를 단말 장치(110)로 송신한다. 또한, 바이러스 검색부(316)는 어플에 바이러스가 존재하는 여부를 검색한 결과를 어플에 관한 신뢰성 정보로서 활용하기 위해 신뢰성 데이터베이스(340)에 저장할 수 있다.

[0064] 가상 장치 처리부(313)는 가상 장치(318)에 바이러스가 검색되면, 백업 데이터 저장부(330)에 저장된 백업 데이터와 업데이트 데이터를 이용해서 가상 장치(318)를 어플을 설치하기 전 상태로 복구한다.

[0065] 가상 장치 처리부(313)는 가상 장치(318)에 바이러스가 검색되면, 단말 장치(110)로부터 백업 데이터를 수신해서 가상 장치(318)를 어플을 설치하기 전 상태로 복구할 수도 있다.

[0066] 한편, 바이러스 검색부(316)의 바이러스 검색결과 바이러스가 존재하지 않더라도, 사용자의 변심 또는 시스템의 오류로 인해 어플이 단말 장치(110)에 설치되지 않을 수 있다. 따라서, 가상 장치 처리부(313)는 가상 장치(318)에 바이러스가 검색되지 않아도 어플이 단말 장치(110)에 설치되지 않으면, 백업 데이터 저장부(330)에 저장된 백업 데이터와 업데이트 데이터를 이용하거나, 단말 장치(110)로부터 백업 데이터를 수신해서 가상 장치(318)를 어플을 설치하기 전 상태로 복구한다.

[0067] 기준정보 생성부(317)는 신뢰성 데이터베이스(340)에 저장된 신뢰도 정보를 이용해서 어플의 신뢰도를 평가하는 기준이 되는 정보인 기준정보를 생성해서 기준정보 데이터베이스(350)에 저장하고, 기준정보를 단말 장치(110)로 송신한다.

[0068] 예를 들어, 기준정보 생성부(317)는 판매 서버 P를 통해 판매되는 생산자 A가 이전에 생성한 어플의 수가 50개(기설정 기준 개수)를 초과하고, 판매 서버 P를 통해 판매되는 생산자 A가 이전에 생성한 모든 어플에 바이러스가 존재하지 않은 경우, 판매 서버 P를 통해 판매되는 생산자 A가 생성하는 어플이 기준정보로 생성 될 수 있다. 이 경우, 추후 설치하고자 하는 어플이 판매 서버 P를 통해 판매되는 생산자 A가 생성하는 어플에 부합되면 설치하고자 하는 어플은 신뢰성이 있다고 판단될 수 있다.

[0069] 제어부(310)는 클라우드 서버(120)의 전반적인 동작을 제어할 수 있다. 그리고, 제어부(310)는 백업 처리부(311), 복구 처리부(312), 가상 장치 처리부(313), 신뢰성 평가부(314), 어플 다운로드부(315), 바이러스 검색부(316) 및 기준정보 생성부(317)의 기능을 수행할 수 있다. 제어부(310), 백업 처리부(311), 복구 처리부(312), 가상 장치 처리부(313), 신뢰성 평가부(314), 어플 다운로드부(315), 바이러스 검색부(316) 및 기준정보 생성부(317)를 구분하여 도시한 것은 각 기능들을 구별하여 설명하기 위함이다. 따라서 제어부(310)는 백업 처리부(311), 복구 처리부(312), 가상 장치 처리부(313), 신뢰성 평가부(314), 어플 다운로드부(315), 바이러스 검색부(316) 및 기준정보 생성부(317) 각각의 기능을 수행하도록 구성된(configured) 적어도 하나의 프로세서를 포함할 수 있다. 또한, 제어부(310)는 백업 처리부(311), 복구 처리부(312), 가상 장치 처리부(313), 신뢰성 평가부(314), 어플 다운로드부(315), 바이러스 검색부(316) 및 기준정보 생성부(317) 각각의 기능 중 일부를 수행하도록 구성된(configured) 적어도 하나의 프로세서를 포함할 수 있다.

[0070] 이하, 상기와 같이 구성된 본 발명에 따른 바이러스 피해를 방지하는 방법을 아래에서 도면을 참조하여 설명한다.

[0071] 도 5는 바이러스 피해를 방지한 단말 장치에서 어플을 설치하는 과정을 도시한 흐름도이다.

[0072] 도 5를 참조하면, 단말 장치(110)는 510단계에서 클라우드 서버(120)에서 상기 단말 장치와 동일한 기능을 수행할 수 있는 가상 장치를 생성할 때 필요로 하는 데이터를 포함하는 백업 데이터를 생성해서 클라우드 서버로 송신한다.

[0073] 그리고, 단말 장치(110)는 512단계에서 어플을 설치하는 이벤트의 발생을 감지하면, 514단계에서 설치하고자 하는 어플의 신뢰성을 평가한다. 이때, 단말 장치(110)는 클라우드 서버(120)로 어플에 대한 신뢰성 평가를 요청하는 메시지를 송신해서 어플의 신뢰성을 평가할 수도 있고, 신뢰성 데이터베이스(240) 또는 기준정보 데이터베이스(250)에 저장된 정보들을 이용해서 어플의 신뢰성을 평가 할 수도 있다. 이때, 신뢰성 평가를 요청하는 메시지는 어플에 대한 기본정보를 포함할 수 있다.

[0074] 514단계의 평가결과 신뢰할 수 있는 어플이면, 단말 장치(110)는 524단계에서 어플을 설치한다.

[0075] 514단계의 평가결과 신뢰할 수 없는 어플이면, 단말 장치(110)는 516단계에서 클라우드 서버(120)로 바이러스 검색을 요청한다. 단말 장치(110)는 어플의 기본정보를 포함하는 바이러스 검색 요청 메시지를 클라우드 서버(120)로 송신해서 바이러스 검색을 요청할 수 있다.

[0076] 그리고, 단말 장치(110)는 518단계에서 클라우드 서버(120)로부터 바이러스를 검색한 검색결과를 수신한다.

[0077] 그리고, 단말 장치(110)는 520단계에서 수신한 검색결과를 분석해서 어플에 바이러스가 포함되어 있는 여부를 확인한다.

[0078] 520단계의 확인결과 바이러스가 검색되면, 단말 장치(110)는 522단계에서 바이러스가 발견되었음을 단말 장치(110)의 사용자에게 공지한다.

[0079] 520단계의 확인결과 바이러스가 검색되지 않으면, 단말 장치(110)는 524단계에서 어플을 설치한다.

[0080] 도 6은 바이러스 피해를 방지한 클라우드 서버에서 어플의 바이러스 여부를 검색하는 과정을 도시한 흐름도이다.

[0081] 도 6을 참조하면, 클라우드 서버(120)는 610단계에서 단말 장치(110)로부터 백업 데이터를 수신하면, 612단계에서 수신한 백업 데이터를 이용해서 단말 장치(110)와 동일한 동작을 수행하는 가상 장치를 생성한다.

[0082] 그리고, 클라우드 서버(120)는 614단계에서 단말 장치(110)로부터 어플의 신뢰성을 요청 받으면, 614단계에서 어플의 신뢰성을 확인해서 단말 장치(110)로 송신한다. 이때, 클라우드 서버(120)는 신뢰성 데이터베이스(340)에서 신뢰성을 요청 받은 어플을 검색해서 어플의 신뢰성을 평가 할 수 있다. 또한, 클라우드 서버(120)는 어플 공급 서버(130)로부터 어플에 관한 기본정보를 수신하고, 기본정보가 기준정보의 기준을 만족하는지 여부를 판단해서 신뢰성을 평가할 수 있다. 614단계의 확인결과 단말 장치(110)로부터 어플의 신뢰성을 요청 받지 않으면, 클라우드 서버(120)는 616단계를 생략하고 618단계로 진행한다.

[0083] 그리고, 클라우드 서버(120)는 618단계에서 단말 장치(110)로부터 어플의 바이러스 검색을 요청 받으면, 620단계에서 어플 공급 서버(130)로부터 어플을 다운받아 가상 장치에 설치한다. 그리고, 클라우드 서버(120)는 622단계에서 가상 장치에 바이러스가 존재하는지 검색하고, 624단계에서 바이러스 검색결과를 단말장치(110)로 송신한다. 그리고, 클라우드 서버(120)는 626단계에서 바이러스 검색결과를 신뢰도 데이터베이스에 갱신하고, 628단계에서 가상 장치를 어플을 설치하기 전 상태로 복구한다. 이때, 클라우드 서버(120)는 단말 장치(110)에 어플이 설치됨을 확인하는 경우 628단계를 생략할 수 있다.

[0084] 도 7은 단말 장치에서 데이터를 백업하고 복구하는 과정을 도시한 흐름도이다.

[0085] 도 7을 참조하면, 단말 장치(110)는 710단계에서 백업 이벤트의 발생을 감지하면, 712단계에서 메모리부에 저장된 모든 데이터 또는 일부 데이터를 백업 데이터로 생성해서 클라우드 서버로 송신한다. 이때, 백업 데이터는 생성시점을 나타내는 타임 스템프(Time stamp)를 포함할 수 있다.

[0086] 그리고, 단말 장치(110)는 714단계에서 업데이트 이벤트의 발생을 감지하면, 716단계에서 업데이트 데이터를 생성해서 클라우드 서버(120)로 송신한다. 업데이트 데이터는 생성시점을 나타내는 타임 스템프(Time stamp)를 포함할 수 있다. 이때, 업데이트 이벤트는 메모리부에 저장된 데이터의 내용이 변경 또는 추가된 경우, 메모리부에 저장된 데이터의 내용이 변경 또는 추가된 횟수가 기설정된 횟수 이상인 경우, 메모리부에 저장된 데이터의 내용이 변경 또는 추가된 데이터의 양이 기설정된 데이터양을 초과한 경우, 메모리부의 블록이 변경된 경우, 메모리부의 블록이 변경되는 횟수가 기설정된 횟수 이상인 경우, 메모리부의 블록들 중에서 변경된 블록이 기설정된 개수 이상인 경우, 기설정된 업데이트 시간간격을 초과한 경우 및 사용자의 요청을 감지한 경우 중에서 적어

도 하나의 경우를 포함하는 경우에 해당한다.

[0087] 그리고, 단말 장치(110)는 718단계에서 단말 장치(110)의 시스템 오류, 바이러스 발견 또는 사용자의 요청에 따른 복구 이벤트의 발생을 감지하면, 720단계에서 클라우드 서버(120)로 백업 데이터를 요청한다. 이때 요청하는 백업 데이터는 마지막 업데이트 데이터가 적용된 가장 최근의 백업 데이터이거나, 사용자의 요청에 따라 특정 시점에 저장된 백업 데이터이다. 그리고, 단말 장치(110)는 722단계에서 클라우드 서버(120)로부터 백업 데이터를 수신해서 단말 장치(110)를 복구한다.

[0088] 도 8은 클라우드 서버에서 신뢰성을 판단하는 기준정보 생성하는 과정을 도시한 흐름도이다.

[0089] 도 8을 참조하면 클라우드 서버(120)는 810단계에서 신뢰성 정보 제공 이벤트의 발생을 확인한다. 이때, 신뢰성 정보 제공 이벤트는 클라우드 서버(120)의 운영자의 요청, 단말 장치(110)의 요청, 기설정된 시간 간격, 신뢰성 데이터베이스(340)에 어플의 수가 기설정된 개수를 초과할 때마다 또는 신뢰성 데이터베이스(340)에 저장된 데이터가 기설정한 비율 이상 갱신된 경우 발생할 수 있다.

[0090] 810단계의 확인결과 신뢰성 정보 제공 이벤트가 발생하면, 812단계에서 기준정보 생성부(317)는 신뢰성 데이터베이스(340)에 저장된 각 어플들의 신뢰도 정보를 분석해서 어플의 신뢰도를 평가하는 기준이 되는 정보인 기준정보를 생성한다. 예를 들어 클라우드 서버(120)는 신뢰성 데이터베이스(340)를 분석한 결과 특정 판매 서버를 통해 판매되는 특정 생산자의 특정 출시일자 이전에 생성된 어플이 모두 신뢰성이 있으면 이를 기준정보로 설정할 수 있다.

[0091] 그리고, 클라우드 서버(120)는 814단계에서 생성한 기준정보를 단말 장치(110)로 송신한다.

[0092] 한편, 바이러스 피해를 방지하는 시스템에서 단말 장치(110)는 도 2의 구성 외에도 다르게 구성될 수 있다.

[0093] 도 9는 바이러스 피해를 방지하는 시스템에서 단말 장치의 다른 구성 예를 도시한 도면이다.

[0094] 도 9를 참조하면 단말 장치(110)는 제어부(910), 백업 처리부(911), 복구 처리부(912), 어플 다운로드부(913), 신뢰성 평가부(914), 바이러스 검색 요청부(915), 바이러스 검색결과 수신부(916) 어플 설치부(917), 통신부(920), 메모리부(930)를 포함한다. 또한, 단말 장치(110)는 추가로 신뢰성 데이터베이스(940)과 기준정보 데이터베이스(950) 중 하나 내지는 모두를 더 포함할 수도 있다.

[0095] 도 9에서 백업 처리부(911), 복구 처리부(912), 통신부(920), 메모리부(930), 신뢰성 데이터베이스(940) 및 기준정보 데이터베이스(950)는 도 2의 설명과 동일함으로 그 상세한 설명은 생략한다.

[0096] 어플 다운로드부(913)는 사용자로부터 요청받은 어플을 어플 공급 서버(130)로부터 다운로드 받는다.

[0097] 신뢰성 평가부(914)는 다운로드 받은 상기 어플을 설치하기 전에 다운로드 받은 어플에 포함된 어플의 기본정보 또는 어플 공급 서버(130)로부터 어플에 관한 기본정보를 수신해서 기본정보를 이용해서 신뢰성을 평가한다. 이때, 기본정보는 어플의 카테고리, 어플의 생산자, 어플의 판매 서버, 어플의 출시일자 및 어플의 권한 등을 포함할 수 있다. 신뢰성을 평가하는 방법은 도 2의 신뢰성 평가부(213)의 방법과 동일하다.

[0098] 바이러스 검색 요청부(915)는 신뢰성 평가부(914)의 평가결과 어플의 신뢰성이 기설정한 기준 이하이면, 클라우드 서버(120)로 어플의 바이러스 검색을 요청한다.

[0099] 바이러스 검색결과 수신부(916)는 클라우드 서버(120)로부터 어플에 대한 바이러스 검색결과를 수신한다.

[0100] 어플 설치부(917)는 신뢰성 평가부(914)의 평가결과 어플의 신뢰성이 기설정한 기준 보다 높거나 또는 어플에 바이러스가 없다는 검색결과를 수신하면, 어플 다운로드부(913)에서 다운받은 어플을 단말 장치(110)에 설치한다.

[0101] 한편, 어플 다운로드부(913)는 어플에 바이러스가 존재한다는 검색결과를 수신하면, 다운받은 어플을 삭제한다.

[0102] 본 발명의 실시 예에 따른 방법들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위

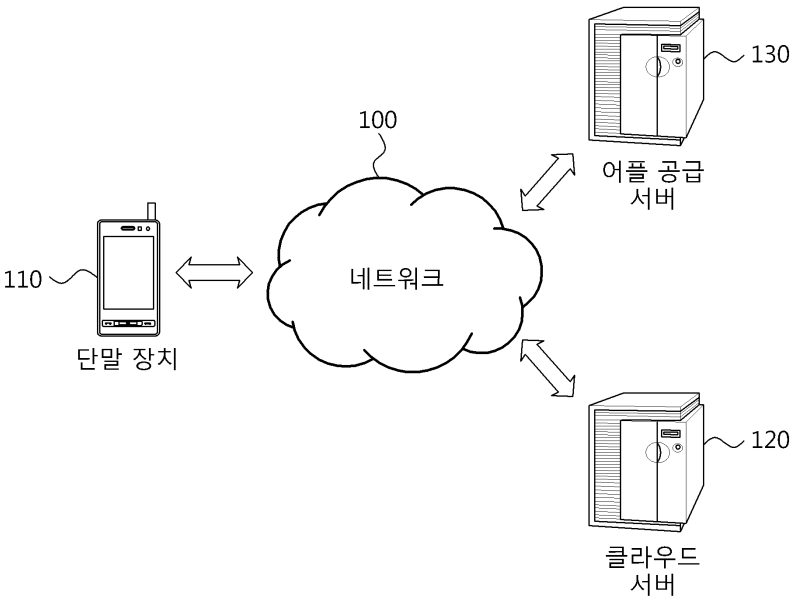
하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[0103] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

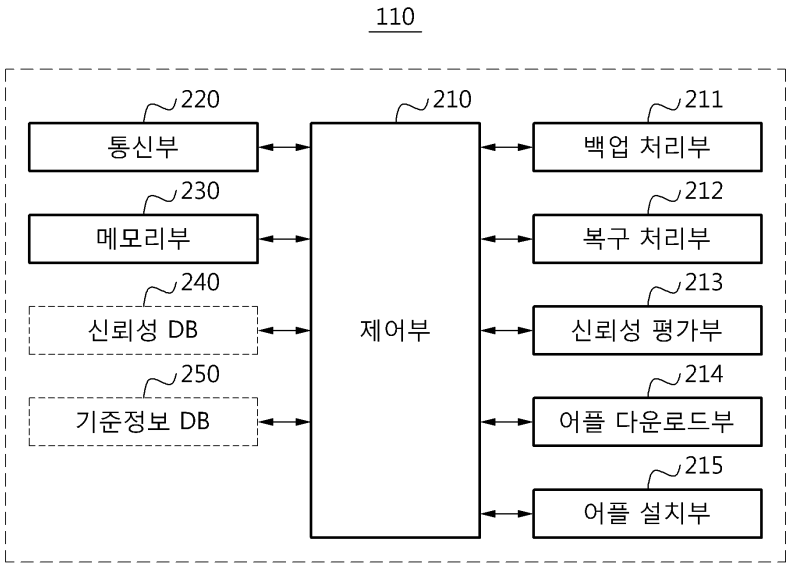
[0104] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

도면

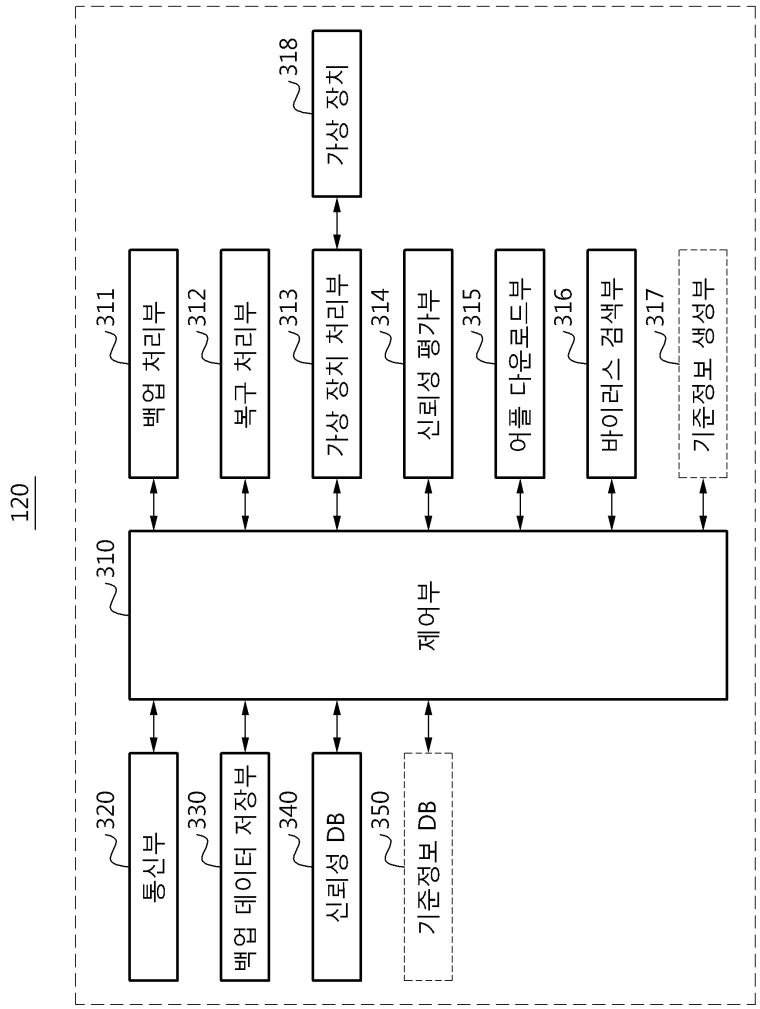
도면1



도면2



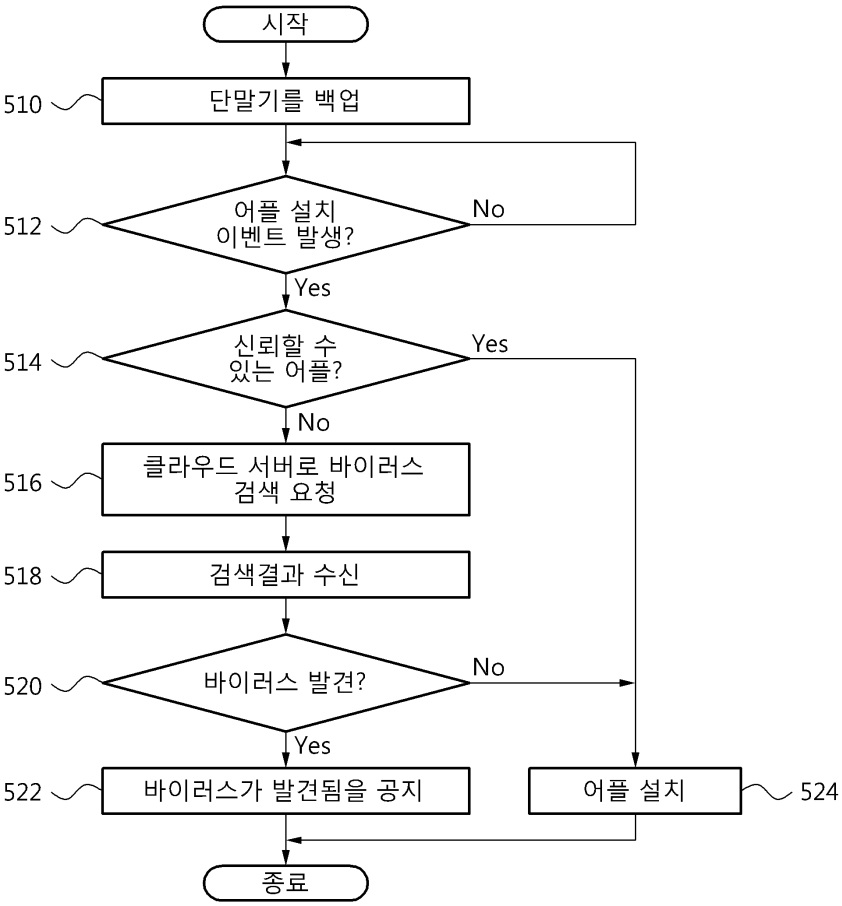
도면3


120
310
제어부
311
백업 처리부
312
복구 처리부
313
가상 장치 처리부
314
신뢰성 평가부
315
어플 다운로드부
316
바이러스 검색부
317
기준정보 생성부
318
가상 장치
320
통신부
330
백업 데이터 저장부
340
신뢰성 DB
350
기준정보 DB

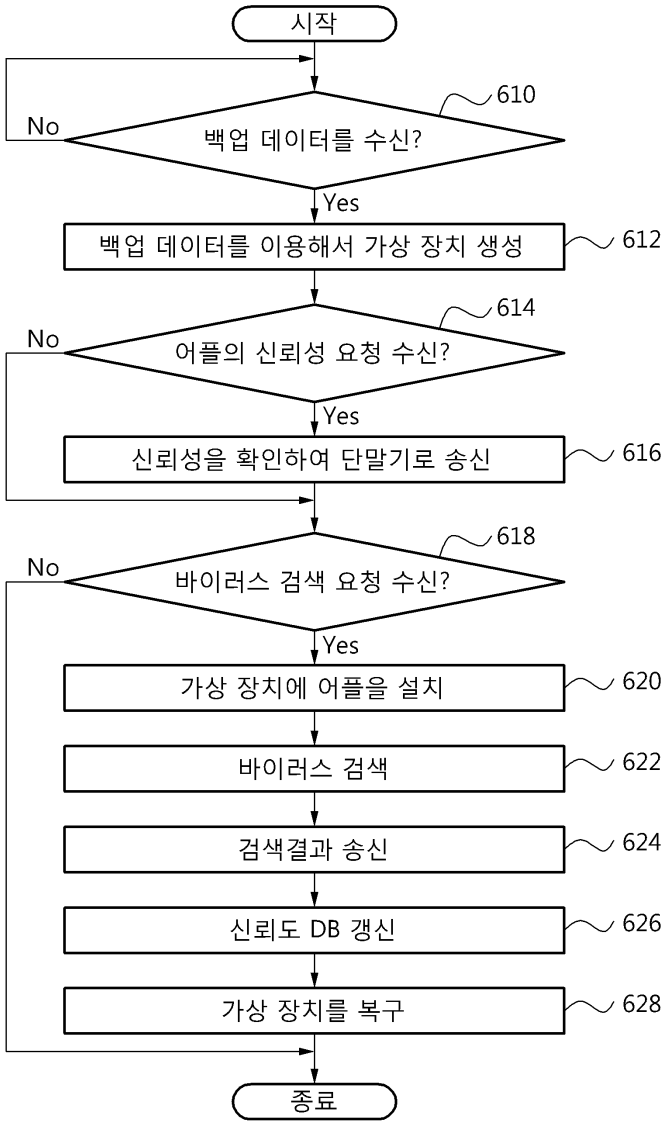
도면4

다운로드 받은 시간	설치 시각	공급자 정보	출시 일자	권한 (permission)	신뢰성 여부	사용한 검색 엔진 정보	사용자 review
2011/05/09: 13:14	2011/05/09: 13:15	Pantech	2011/05/08	Wi-Fi, Contact	OK	V3 (Ver 011.05.09.00)	Good.

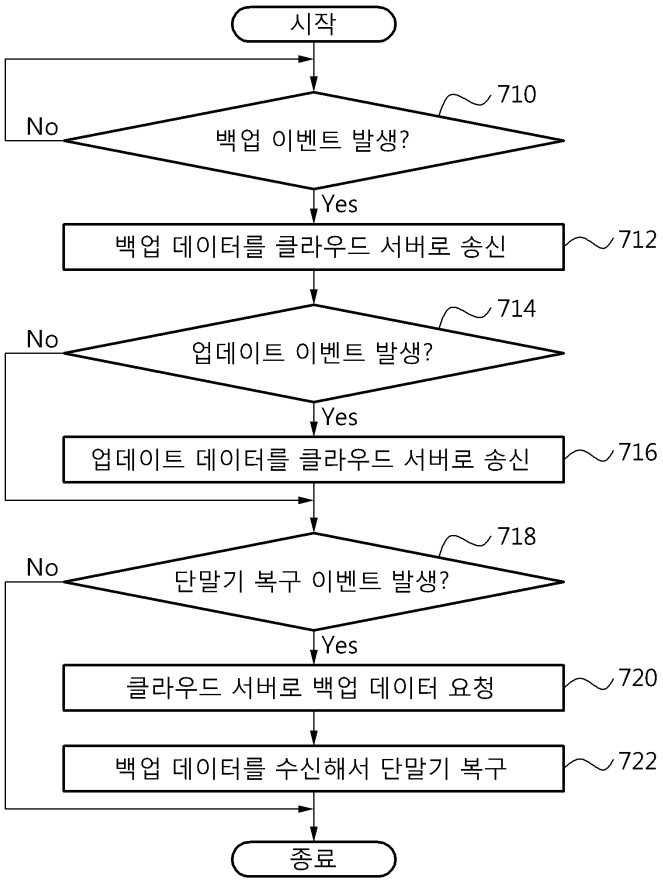
도면5


시작
510
단말기를 백업
512
어플 설치
이벤트 발생?
No
Yes
514
신뢰할 수
있는 어플?
Yes
No
516
클라우드 서버로 바이러스
검색 요청
518
검색결과 수신
520
바이러스 발견?
No
Yes
522
바이러스가 발견됨을 공지
어플 설치
524
종료

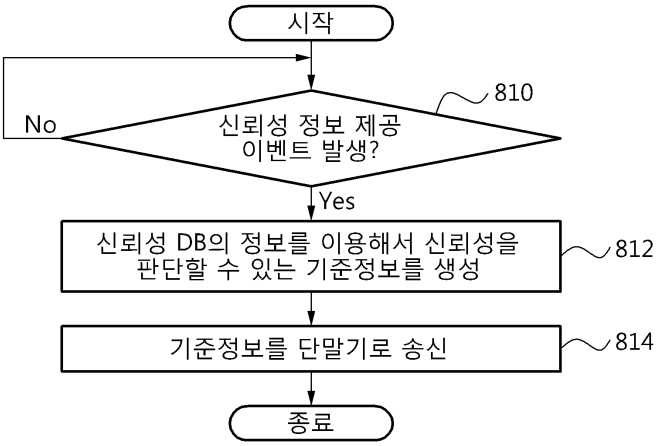
도면6


시작
610
No
백업 데이터를 수신?
Yes
백업 데이터를 이용해서 가상 장치 생성
612
614
No
어플의 신뢰성 요청 수신?
Yes
신뢰성을 확인하여 단말기로 송신
616
618
No
바이러스 검색 요청 수신?
Yes
가상 장치에 어플을 설치
620
바이러스 검색
622
검색결과 송신
624
신뢰도 DB 갱신
626
가상 장치를 복구
628
종료

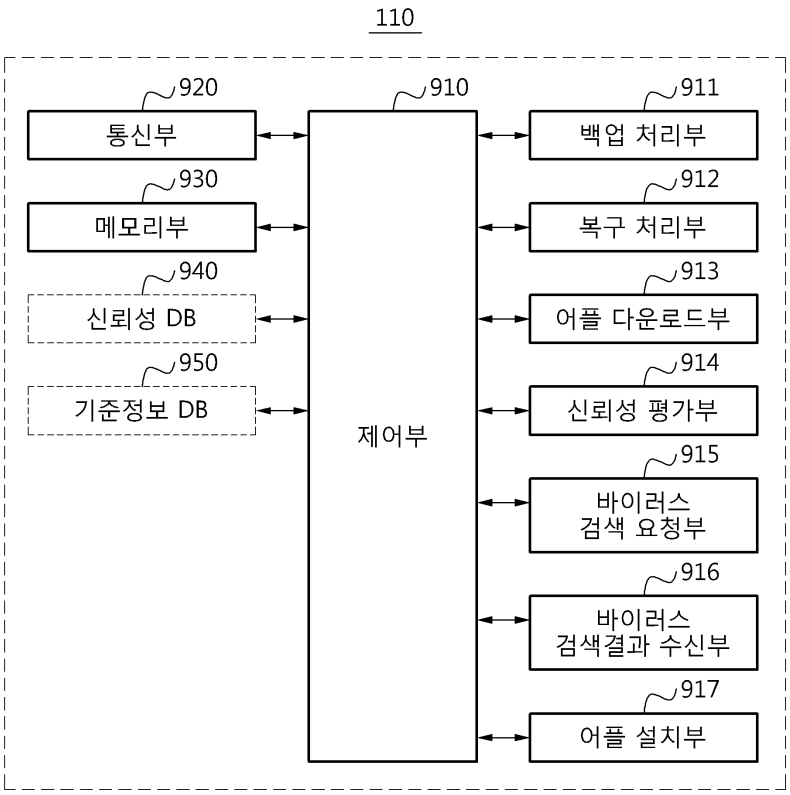
도면7


시작
710
No
백업 이벤트 발생?
Yes
백업 데이터를 클라우드 서버로 송신
712
714
No
업데이트 이벤트 발생?
Yes
업데이트 데이터를 클라우드 서버로 송신
716
718
No
단말기 복구 이벤트 발생?
Yes
클라우드 서버로 백업 데이터 요청
720
백업 데이터를 수신해서 단말기 복구
722
종료

도면8


시작
810
No
신뢰성 정보 제공
이벤트 발생?
Yes
신뢰성 DB의 정보를 이용해서 신뢰성을
판단할 수 있는 기준정보를 생성
812
기준정보를 단말기로 송신
814
종료

도면9


110
920
통신부
930
메모리부
940
신뢰성 DB
950
기준정보 DB
910
제어부
911
백업 처리부
912
복구 처리부
913
어플 다운로드부
914
신뢰성 평가부
915
바이러스
검색 요청부
916
바이러스
검색결과 수신부
917
어플 설치부