



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0060814
(43) 공개일자 2018년06월07일

(51) 국제특허분류(Int. Cl.)
G06F 21/51 (2013.01) G06F 21/46 (2013.01)
(52) CPC특허분류
G06F 21/51 (2013.01)
G06F 21/46 (2013.01)
(21) 출원번호 10-2016-0160751
(22) 출원일자 2016년11월29일
심사청구일자 2016년11월29일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
류재철
대전광역시 유성구 어은로 57, 132동 801호
김상후
대전광역시 유성구 도안동로 523, 215동 1102호
(뒷면에 계속)
(74) 대리인
홍성욱, 심경식

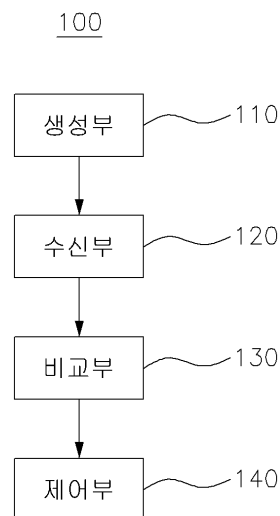
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버 및 그 제어 방법

(57) 요약

본 발명의 일 실시예에 따른 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버 및 그 제어 방법은 모바일 단말기와 연동하여 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버에 있어서, 제1 OTP(One Time Password)를 생성하고, 상기 제1 OTP 및 내부에 저장된 원본 어플리케이션의 제1 메모리코드에 기초하여 기준 검증값을 생성하는 생성부, 상기 모바일 단말기로부터 상기 어플리케이션의 무결성을 검증하기 위한 비교 검증값을 수신하는 수신부, 상기 기준 검증값 및 상기 비교 검증값을 비교하는 비교부, 및 비교 결과에 기초하여 상기 모바일 단말기와의 통신 설정을 제어하는 제어부를 포함한다.

대표도 - 도2



(52) CPC특허분류

H04L 9/3226 (2013.01)

(72) 발명자

허혜지

대전광역시 유성구 문화원로37번길 48, 208호

조제경

대전광역시 유성구 온천북로33번길 22-9, 304호

이 발명을 지원한 국가연구개발사업

과제고유번호 1711035246

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 대학 ICT 연구센터 육성 지원사업

연구과제명 클라우드 환경의 스마트 기기와 서비스 보안 기술 개발 및 연구 인력양성

기 여 율 1/1

주관기관 숭실대학교 산학협력단

연구기간 2016.01.01 ~ 2016.12.31

명세서

청구범위

청구항 1

모바일 단말기와 연동하여 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버에 있어서,
제1 OTP(One Time Password)를 생성하고, 상기 제1 OTP 및 내부에 저장된 원본 어플리케이션의 제1 메모리코드에 기초하여 기준 검증값을 생성하는 생성부;
상기 모바일 단말기로부터 상기 어플리케이션의 무결성을 검증하기 위한 비교 검증값을 수신하는 수신부;
상기 기준 검증값 및 상기 비교 검증값을 비교하는 비교부; 및
비교 결과에 기초하여 상기 모바일 단말기와 통신 설정을 제어하는 제어부
를 포함하는 것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버.

청구항 2

제1항에 있어서,
상기 비교 검증값은
상기 모바일 단말기에서 생성된 제2 OTP(One Time Password)와 실행되기 이전의 어플리케이션의 제2 메모리코드에 기초하여 생성되는 것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버.

청구항 3

제2항에 있어서,
상기 비교 검증값은
상기 제2 메모리코드의 데이터 중 상기 제2 OTP를 이용하여 추출된 소정 크기의 비교 데이터에 대한 해쉬값 및
상기 모바일 단말기의 고유정보에 기초하여 생성되고,
상기 비교 데이터는
상기 제2 OTP를 이용하여 상기 제2 메모리코드의 데이터 내에서 시작 지점과 끝 지점이 설정됨에 따라 추출되는
것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버.

청구항 4

제3항에 있어서,
상기 비교 데이터의 시작 지점은 상기 제2 메모리코드의 시작 주소값으로부터 오프셋값을 더한 주소값을 가지며,
상기 오프셋값은 상기 제2 OTP의 값을 상기 제2 메모리코드의 크기값으로 나눈 몫에 대한 나머지인 제1 나머지값으로 설정되고,
상기 비교 데이터의 끝 지점은 상기 오프셋값으로부터 사이즈값을 더한 주소값을 가지며,
상기 사이즈값은 상기 제2 OTP의 값을 상기 제2 메모리코드의 크기값과 상기 제1 나머지값의 차이로 나눈 몫에 대한 나머지인 제2 나머지값으로 설정되는 것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버.

청구항 5

제2항에 있어서,

상기 수신부는

상기 모바일 단말기로부터 상기 제2 메모리코드를 복호화하기 위한 복호화 키를 요청하는 요청값을 더 수신하고,

상기 제어부는

상기 비교 결과에 기초하여 상기 기준 검증값 및 상기 비교 검증값이 동일하다고 판단되는 경우, 상기 복호화 키의 값을 상기 모바일 단말기로 전송하도록 제어하는 것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버.

청구항 6

제1항에 있어서,

상기 비교 검증값은

상기 모바일 단말기에서 생성된 제2 OTP(One Time Password)와 실행 중인 어플리케이션의 제3 메모리코드에 기초하여 생성되는 것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버.

청구항 7

제6항에 있어서,

상기 비교 검증값은

상기 제3 메모리코드의 데이터 중 상기 제2 OTP를 이용하여 추출된 소정 크기의 비교 데이터에 대한 해쉬값 및 상기 모바일 단말기의 고유정보에 기초하여 생성되고,

상기 비교 데이터는

상기 제2 OTP를 이용하여 상기 제3 메모리코드의 데이터 내에서 시작 지점과 끝 지점이 설정됨에 따라 추출되는 것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버.

청구항 8

제7항에 있어서,

상기 비교 데이터의 시작 지점은 상기 제3 메모리코드의 시작 주소값으로부터 오프셋값을 더한 주소값을 가지며,

상기 오프셋값은 상기 제2 OTP의 값을 상기 제3 메모리코드의 크기값으로 나눈 몫에 대한 나머지인 제1 나머지값으로 설정되고,

상기 비교 데이터의 끝 지점은 상기 오프셋값으로부터 사이즈값을 더한 주소값을 가지며,

상기 사이즈값은 상기 제2 OTP의 값을 상기 제3 메모리코드의 크기값과 상기 제1 나머지값의 차이로 나눈 몫에 대한 나머지인 제2 나머지값으로 설정되는 것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버.

청구항 9

제8항에 있어서,

상기 제어부는

상기 비교 결과에 기초하여 상기 기준 검증값 및 상기 비교 검증값이 동일하다고 판단되는 경우, 상기 모바일 단말기와의 통신이 유지되도록 제어하는 것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버.

청구항 10

제1항에 있어서,

상기 수신부는

상기 모바일 단말기로부터 상기 모바일 단말기의 고유정보를 더 수신하고,

상기 생성부는

상기 제1 OTP를 이용하여 상기 제1 메모리코드의 데이터 내에서 시작 지점과 끝 지점을 설정하여 소정 크기의 기준 데이터를 추출하고, 상기 기준 데이터에 대한 해쉬값 및 상기 모바일 단말기의 고유정보에 기초하여 상기 기준 검증값을 생성하는 것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버.

청구항 11

제10항에 있어서,

상기 기준 데이터의 시작 지점은 상기 제1 메모리코드의 시작 주소값으로부터 오프셋값을 더한 주소값을 가지며,

상기 오프셋값은 상기 제1 OTP의 값을 상기 제1 메모리코드의 크기값으로 나눈 몫에 대한 나머지인 제1 나머지값으로 설정되고,

상기 비교 데이터의 끝 지점은 상기 오프셋값으로부터 사이즈값을 더한 주소값을 가지며,

상기 사이즈값은 상기 제1 OTP의 값을 상기 제1 메모리코드의 크기값과 상기 제1 나머지값의 차이로 나눈 몫에 대한 나머지인 제2 나머지값으로 설정되는 것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버.

청구항 12

모바일 단말기와 연동하여 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버에 있어서,

제1 OTP(One Time Password)를 생성하는 단계;

상기 제1 OTP 및 내부에 저장된 원본 어플리케이션의 제1 메모리코드에 기초하여 기준 검증값을 생성하는 단계;

상기 모바일 단말기로부터 상기 어플리케이션의 무결성을 검증하기 위한 비교 검증값을 수신하는 단계;

상기 기준 검증값 및 상기 비교 검증값을 비교하는 단계; 및

비교 결과에 기초하여 상기 모바일 단말기와의 통신 설정을 제어하는 단계

를 포함하는 것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버의 제어 방법.

청구항 13

제12항에 있어서,

상기 수신하는 단계는

상기 모바일 단말기로부터 상기 모바일 단말기의 고유정보를 더 수신하고,

상기 기준 검증값을 생성하는 단계는

상기 제1 OTP를 이용하여 상기 제1 메모리코드의 데이터 내에서 시작 지점과 끝 지점을 설정하여 소정 크기의 기준 데이터를 추출하는 단계; 및

상기 기준 데이터에 대한 해쉬값 및 상기 모바일 단말기의 고유정보에 기초하여 상기 기준 검증값을 생성하는 단계

를 포함하는 것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버의 제어 방법.

청구항 14

제13항에 있어서,

상기 기준 데이터를 추출하는 단계는

상기 제1 메모리코드의 시작 주소값으로부터 오프셋값을 더한 주소값을 상기 기준 데이터의 시작 지점으로 설정하는 단계; 및

상기 오프셋값으로부터 사이즈값을 더한 주소값을 상기 기준 데이터의 끝 지점으로 설정하는 단계를 포함하고,

상기 오프셋값은 상기 제1 OTP의 값을 상기 제1 메모리코드의 크기값으로 나눈 몫에 대한 나머지인 제1 나머지값으로 설정되고,

상기 사이즈값은 상기 제1 OTP의 값을 상기 제1 메모리코드의 크기값과 상기 제1 나머지값의 차이로 나눈 몫에 대한 나머지인 제2 나머지값으로 설정되는 것을 특징으로 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버의 제어 방법.

발명의 설명

기술 분야

[0001] 본 발명은 OTP를 이용하여 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버 및 그 제어 방법에 관한 것이다.

배경 기술

[0002] 최근 스마트폰의 급속한 보급 확대로 "앱"이라는 스마트폰 응용프로그램 시장 또한 거대한 시장으로 부각되는 추세이다. 2010년 미국방언협회(American Dialect Society)는 올해의 단어로 "앱"을 선정할 정도로 스마트폰과 앱은 우리 생활 깊숙이 자리잡아 가고 있다.

[0003] 전세계적으로 2012년 3월 기준 750,000개(유효앱 580,000개)의 앱이 등록되고 있으며, 국내는 2012년 3월 기준 스마트폰 이용자가 30,000,000명을 돌파할 것으로 추정되고 있다. 2012년 10월 안드로이드 기반 앱 마켓에서 사용한 앱 개수는 700,000개로 아이폰 앱스토어의 사용 가능한 앱의 수를 따라잡았다. 앱을 불법 복제하여 임의로 변조한 뒤 마켓에 등록한 불법 복제 앱의 수도 지난 2012년 9월말 약 170,000건으로 2012년 6월말에 비교하여 6배 증가하였다.

[0004] 앱 불법 복제 문제는 iOS보다 특히 안드로이드 운영체제의 경우가 더 심각하며, 이로 인해 앱에 대한 지적재산권 문제가 심각하게 발생하고 있다. 안드로이드가 최고 인기 스마트폰용 플랫폼인 동시에 해킹 공격도 가장 많이 받는 것으로 나타나고 있다.

[0005] 특히, 해킹 또는 루팅된 스마트폰은 보안 문제에 매우 취약하여 타인에게 개인정보가 유출될 수 있다. 그러나, 개개인의 단말기에 대해 해킹 또는 루팅이 이루어지지 못하게 하는 것은 거의 불가능하며, 위변조된 앱의 무분별한 배포를 차단하는 것 또한 한계가 있어 스마트폰을 통한 보안 범죄는 점차 진화될 것으로 예상된다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 한국 공개특허공보 제10-2013-0153655호(2015.06.19)

발명의 내용

해결하려는 과제

[0007] 본 발명의 일 실시예는 OTP를 이용하여 무결성을 검증하고자 하는 어플리케이션의 메모리코드의 데이터 중 일부의 데이터만을 추출하여 검증값을 생성하고, 생성된 검증값을 통해 해당 어플리케이션의 위변조를 방지하도록 하는 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버 및 그 제어 방법을 제공한다.

[0009] 본 발명이 해결하고자 하는 과제는 이상에서 언급한 과제(들)로 제한되지 않으며, 언급되지 않은 또 다른 과제(들)는 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0010] 본 발명의 일 실시예에 따른 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버는 모바일 단말기와 연동하여 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버에 있어서, 제1 OTP(One Time Password)를 생성하고, 상기 제1 OTP 및 내부에 저장된 원본 어플리케이션의 제1 메모리코드에 기초하여 기준 검증값을 생성하는 생성부, 상기 모바일 단말기로부터 상기 어플리케이션의 무결성을 검증하기 위한 비교 검증값을 수신하는 수신부, 상기 기준 검증값 및 상기 비교 검증값을 비교하는 비교부, 및 비교 결과에 기초하여 상기 모바일 단말기와의 통신 설정을 제어하는 제어부를 포함한다.

[0011] 또한, 본 발명의 일 실시예에 따른 상기 비교 검증값은 상기 모바일 단말기에서 생성된 제2 OTP(One Time Password)와 실행되기 이전의 어플리케이션의 제2 메모리코드에 기초하여 생성될 수 있다.

[0012] 또한, 본 발명의 일 실시예에 따른 상기 비교 검증값은 상기 제2 메모리코드의 데이터 중 상기 제2 OTP를 이용하여 추출된 소정 크기의 비교 데이터에 대한 해쉬값 및 상기 모바일 단말기의 고유정보에 기초하여 생성되고, 상기 비교 데이터는 상기 제2 OTP를 이용하여 상기 제2 메모리코드의 데이터 내에서 시작 지점과 끝 지점이 설정됨에 따라 추출될 수 있다.

[0013] 또한, 본 발명의 일 실시예에 따른 상기 비교 데이터의 시작 지점은 상기 제2 메모리코드의 시작 주소값으로부터 오프셋값을 더한 주소값을 가지며, 상기 오프셋값은 상기 제2 OTP의 값을 상기 제2 메모리코드의 크기값으로 나눈 몫에 대한 나머지로 제1 나머지로 설정되고, 상기 비교 데이터의 끝 지점은 상기 오프셋값으로부터 사이즈값을 더한 주소값을 가지며, 상기 사이즈값은 상기 제2 OTP의 값을 상기 제2 메모리코드의 크기값과 상기 제1 나머지의 차이로 나눈 몫에 대한 나머지로 설정될 수 있다.

[0014] 또한, 본 발명의 일 실시예에 따른 상기 수신부는 상기 모바일 단말기로부터 상기 제2 메모리코드를 복호화하기 위한 복호화 키를 요청하는 요청값을 더 수신하고, 상기 제어부는 상기 비교 결과에 기초하여 상기 기준 검증값 및 상기 비교 검증값이 동일하다고 판단되는 경우, 상기 복호화 키의 값을 상기 모바일 단말기로 전송하도록 제어할 수 있다.

[0015] 또한, 본 발명의 일 실시예에 따른 상기 비교 검증값은 상기 모바일 단말기에서 생성된 제2 OTP(One Time Password)와 실행 중인 어플리케이션의 제3 메모리코드에 기초하여 생성될 수 있다.

[0016] 또한, 본 발명의 일 실시예에 따른 상기 비교 검증값은 상기 제3 메모리코드의 데이터 중 상기 제2 OTP를 이용하여 추출된 소정 크기의 비교 데이터에 대한 해쉬값 및 상기 모바일 단말기의 고유정보에 기초하여 생성되고, 상기 비교 데이터는 상기 제2 OTP를 이용하여 상기 제3 메모리코드의 데이터 내에서 시작 지점과 끝 지점이 설정됨에 따라 추출될 수 있다.

[0017] 또한, 본 발명의 일 실시예에 따른 상기 비교 데이터의 시작 지점은 상기 제3 메모리코드의 시작 주소값으로부터 오프셋값을 더한 주소값을 가지며, 상기 오프셋값은 상기 제2 OTP의 값을 상기 제3 메모리코드의 크기값으로

나는 뭇에 대한 나머지인 제1 나머지값으로 설정되고, 상기 비교 데이터의 끝 지점은 상기 오프셋값으로부터 사이즈값을 더한 주소값을 가지며, 상기 사이즈값은 상기 제2 OTP의 값을 상기 제3 메모리코드의 크기값과 상기 제1 나머지값의 차이로 나는 뭇에 대한 나머지인 제2 나머지값으로 설정될 수 있다.

[0018] 또한, 본 발명의 일 실시예에 따른 상기 제어부는 상기 비교 결과에 기초하여 상기 기준 검증값 및 상기 비교 검증값이 동일하다고 판단되는 경우, 상기 모바일 단말기와의 통신이 유지되도록 제어할 수 있다.

[0019] 또한, 본 발명의 일 실시예에 따른 상기 수신부는 상기 모바일 단말기로부터 상기 모바일 단말기의 고유정보를 더 수신하고, 상기 생성부는 상기 제1 OTP를 이용하여 상기 제1 메모리코드의 데이터 내에서 시작 지점과 끝 지점을 설정하여 소정 크기의 기준 데이터를 추출하고, 상기 기준 데이터에 대한 해쉬값 및 상기 모바일 단말기의 고유정보에 기초하여 상기 기준 검증값을 생성할 수 있다.

[0020] 또한, 본 발명의 일 실시예에 따른 상기 기준 데이터의 시작 지점은 상기 제1 메모리코드의 시작 주소값으로부터 오프셋값을 더한 주소값을 가지며, 상기 오프셋값은 상기 제1 OTP의 값을 상기 제1 메모리코드의 크기값으로 나는 뭇에 대한 나머지인 제1 나머지값으로 설정되고, 상기 비교 데이터의 끝 지점은 상기 오프셋값으로부터 사이즈값을 더한 주소값을 가지며, 상기 사이즈값은 상기 제1 OTP의 값을 상기 제1 메모리코드의 크기값과 상기 제1 나머지값의 차이로 나는 뭇에 대한 나머지인 제2 나머지값으로 설정될 수 있다.

[0021] 또한, 본 발명의 일 실시예에 따른 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버의 제어 방법은 모바일 단말기와 연동하여 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버에 있어서, 제1 OTP(One Time Password)를 생성하는 단계, 상기 제1 OTP 및 내부에 저장된 원본 어플리케이션의 제1 메모리코드에 기초하여 기준 검증값을 생성하는 단계, 상기 모바일 단말기로부터 상기 어플리케이션의 무결성을 검증하기 위한 비교 검증값을 수신하는 단계, 상기 기준 검증값 및 상기 비교 검증값을 비교하는 단계, 및 비교 결과에 기초하여 상기 모바일 단말기와의 통신 설정을 제어하는 단계를 포함한다.

[0022] 또한, 본 발명의 일 실시예에 따른 상기 수신하는 단계는 상기 모바일 단말기로부터 상기 모바일 단말기의 고유정보를 더 수신하고, 상기 기준 검증값을 생성하는 단계는 상기 제1 OTP를 이용하여 상기 제1 메모리코드의 데이터 내에서 시작 지점과 끝 지점을 설정하여 소정 크기의 기준 데이터를 추출하는 단계, 및 상기 기준 데이터에 대한 해쉬값 및 상기 모바일 단말기의 고유정보에 기초하여 상기 기준 검증값을 생성하는 단계를 포함할 수 있다.

[0023] 또한, 본 발명의 일 실시예에 따른 상기 기준 데이터를 추출하는 단계는 상기 제1 메모리코드의 시작 주소값으로부터 오프셋값을 더한 주소값을 상기 기준 데이터의 시작 지점으로 설정하는 단계, 및 상기 오프셋값으로부터 사이즈값을 더한 주소값을 상기 기준 데이터의 끝 지점으로 설정하는 단계를 포함하고, 상기 오프셋값은 상기 제1 OTP의 값을 상기 제1 메모리코드의 크기값으로 나는 뭇에 대한 나머지인 제1 나머지값으로 설정되고, 상기 사이즈값은 상기 제1 OTP의 값을 상기 제1 메모리코드의 크기값과 상기 제1 나머지값의 차이로 나는 뭇에 대한 나머지인 제2 나머지값으로 설정될 수 있다.

발명의 효과

[0024] 본 발명의 일 실시예에 따르면, OTP를 이용하여 무결성을 검증하고자 하는 어플리케이션의 메모리코드의 데이터 중 일부의 데이터만을 추출하여 검증값을 생성하고, 생성된 검증값을 통해 해당 어플리케이션의 위변조를 방지할 수 있다.

[0025] 본 발명의 일 실시예에 따르면, 해당 어플리케이션의 무결성을 검증하기 위한 검증값을 생성하는데 있어서 어플리케이션의 특정 위치부터 특정 길이만큼의 데이터를 추출하여 활용함으로써, 검증과정에 소요되는 시간을 최소화할 수 있고 검증과정의 절차를 보다 간소화할 수 있다.

도면의 간단한 설명

[0026] 도 1은 본 발명의 일 실시예에 따른 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버가 적용되는 환경을 설명하기 위해 도시한 도면이다.

도 2는 본 발명의 일 실시예에 있어서, 어플리케이션 서버를 설명하기 위해 도시한 블록도이다.

도 3은 본 발명의 일 실시예에 있어서, 비교 검증값의 생성 과정을 설명하기 위해 도시한 도면이다.

도 4는 본 발명의 일 실시예에 따른 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버의 제어 방법을

설명하기 위해 도시한 흐름도이다.

도 5a는 도 4의 제어 방법에 있어서, 실행되기 이전의 어플리케이션의 무결성을 검증하기 위한 모바일 단말기 및 어플리케이션 서버 간의 통신과정을 설명하기 위해 도시한 도면이다.

도 5b는 도 4의 제어 방법에 있어서, 실행 중인 어플리케이션의 무결성을 검증하기 위한 모바일 단말기 및 어플리케이션 서버 간의 통신과정을 설명하기 위해 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0027] 본 발명의 이점 및/또는 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성요소를 지칭한다.
- [0029] 이하에서는 첨부된 도면을 참조하여 본 발명의 실시예들을 상세히 설명하기로 한다.
- [0030] 도 1은 본 발명의 일 실시예에 따른 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버(100)가 적용되는 환경을 설명하기 위해 도시한 도면이다.
- [0031] 도 1을 참고하면, 발명의 일 실시예에 따른 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버(100)가 적용되는 환경에는 어플리케이션 서버(100) 및 적어도 하나의 모바일 단말기(200)를 포함하는데, 어플리케이션 서버(100) 및 모바일 단말기(200)가 서로 연동하여 동작할 수 있다.
- [0032] 어플리케이션 서버(100)는 개발자에 의해 개발된 어플리케이션이 저장되는 서버로서, 실행되기 이전의 어플리케이션이 압축 및 암호화된 상태로 저장되거나 실행 중인 어플리케이션이 복호화된 상태로 저장될 수 있다.
- [0033] 모바일 단말기(200)는 어플리케이션 서버(100)로부터 사용자들의 필요에 따라 다운로드 된 어플리케이션을 설치 및 실행할 수 있다. 참고로, 모바일 단말기(200)는 휴대전화기 이외에 개인용 노트북, PDA와 같은 휴대용 디바이스를 모두 포함할 수 있다.
- [0034] 도 2는 본 발명의 일 실시예에 있어서, 어플리케이션 서버(100)를 설명하기 위해 도시한 블록도이다.
- [0035] 도 2를 참조하면, 본 발명의 일 실시예에 따른 어플리케이션 서버(100)는 생성부(110), 수신부(120), 비교부(130), 및 제어부(140)를 포함한다.
- [0036] 생성부(110)는 OTP 생성부(미도시)와 기준 검증값 생성부(미도시)를 포함할 수 있다.
- [0037] OTP 생성부는 일회용 패스워드인 OTP(One Time Password)를 생성하는데, 일반적으로 OTP란 고정된 패스워드 대신 무작위로 생성되는 난수의 일회용 패스워드를 의미한다. OTP는 주로 동일한 패스워드가 반복 사용됨에 따라 발생하는 보안상의 취약점을 극복하기 위해 사용된다.
- [0038] 본 실시예에서, OTP 생성부는 후술하고자 하는 모바일 단말기(200)에서 생성된 OTP(제2 OTP)와 구분하기 위하여 편의상 제1 OTP를 생성하는 것으로 설명하기로 한다. 참고로, 제1 OTP 및 제2 OTP는 서로 동일한 시간에 동시 생성된다.
- [0039] 기준 검증값 생성부는 해당 어플리케이션의 무결성을 검증하기 위한 비교 작업을 위해 기준 대상이 되는 값인 기준 검증값을 생성한다. 이를 위해, 기준 검증값 생성부는 제1 OTP 및 내부에 저장된 원본 어플리케이션의 제1 메모리코드에 기초하여 기준 검증값을 생성한다. 여기서, 원본 어플리케이션의 제1 메모리코드는 어플리케이션이 복호화되기 이전의 압축 및 암호화된 상태일 수 있고, 복호화된 상태일 수도 있다.
- [0040] 이때, 기준 검증값 생성부는 제1 OTP를 이용하여 제1 메모리코드의 데이터 내에서 시작 지점과 끝 지점을 설정하여 소정 크기의 기준 데이터를 추출할 수 있다. 즉, 기준 검증값 생성부는 제1 OTP를 통해 압축 및 암호화된 상태 또는 복호화된 상태의 제1 메모리코드의 특정 부분을 추출함으로써 기준 데이터를 추출할 수 있다.
- [0041] 구체적으로, 기준 데이터의 시작 지점은 제1 메모리코드의 시작 주소값으로부터 오프셋값(offset)을 더한 주소값을 가질 수 있다. 여기서, 오프셋값은 제1 OTP의 값을 제1 메모리코드의 크기값으로 나눈 몫에 대한 나머지

인 제1 나머지값으로 설정될 수 있다. 한편, 기준 데이터의 끝 지점은 오프셋값으로부터 사이즈값을 더한 주소값을 가질 수 있다. 여기서, 사이즈값은 제1 OTP의 값을 제1 메모리코드의 크기값과 제1 나머지값의 차이로 나눈 몫에 대한 나머지인 제2 나머지값으로 설정될 수 있다. 참고로, 제1 메모리코드의 크기값은 모바일 단말기(200)로부터 검증을 요청해오는 어플리케이션이 실행되기 이전의 어플리케이션에 관한 검증 요청인지, 실행 중인 어플리케이션에 관한 검증 요청인지에 따라 달라질 수 있으며, 이에 따라 추출되는 기준 데이터의 크기 또한 달라질 수 있다.

[0042] 기준 검증값 생성부는 상기 과정을 거쳐 추출된 기준 데이터에 대한 해쉬값 및 모바일 단말기(200)의 고유정보에 기초하여 기준 검증값을 생성할 수 있다. 즉, 기준 검증값 생성부는 해쉬 함수(Hash Function)를 이용하여 추출된 기준 데이터의 해쉬값을 생성하고, 생성된 해쉬값과 모바일 단말기(200)의 고유정보를 연결하여 기준 검증값을 최종 생성할 수 있다. 여기서, 모바일 단말기(200)의 고유정보는 단말기 ID, MAC 주소, 단말기 규격정보 등을 포함할 수 있다. 본 실시예에서, SHA-256 함수인 해쉬 함수를 사용하는 것이 바람직하나, 이에 한정되지 않고 다양한 종류의 해쉬 함수를 사용할 수 있다.

[0043] 본 실시예에서는, 기준 검증값을 생성하는데 있어서, 후술하고자 하는 수신부(120)가 모바일 단말기(200)의 고유정보를 따로 수신하여 해쉬값에 모바일 단말기(200)의 고유정보를 연결하여 최종 기준 검증값을 생성할 수 있다. 또는, 모바일 단말기(200)의 고유정보를 따로 수신하지 않고 모바일 단말기(200)의 접속이 확인되면 후술하고자 하는 비교 검증값의 해쉬값만을 수신하여 기준 검증값의 해쉬값과 비교함으로써 해당 어플리케이션의 무결성을 검증할 수도 있다.

[0044] 수신부(120)는 모바일 단말기(200)로부터 상기 어플리케이션의 무결성을 검증하기 위한 비교 검증값을 수신한다.

[0045] 비교 검증값은 해당 어플리케이션의 무결성을 검증하기 위한 비교 작업을 위해 비교 대상이 되는 값으로서, 도 3을 참조하여 그 생성 과정을 더 자세히 설명하고자 한다. 도 3은 본 발명의 일 실시예에 있어서, 비교 검증값의 생성 과정을 설명하기 위해 도시한 도면이다.

[0046] 이하에서는, 비교 검증값의 생성 과정을 실행되기 이전의 어플리케이션에 대한 무결성을 검증하기 위한 경우와 실행 중인 어플리케이션에 대한 무결성을 검증하기 위한 경우로 나누어 설명하고자 한다.

[0047] 먼저, 실행되기 이전의 어플리케이션에 대한 무결성을 검증하기 위한 경우, 비교 검증값은 모바일 단말기(200)에서 생성된 제2 OTP와 실행되기 이전의 어플리케이션의 제2 메모리코드에 기초하여 생성될 수 있다. 여기서, 제2 메모리코드는 모바일 단말기(200)가 어플리케이션 서버(100)로부터 전달받은 어플리케이션이 설치되기 이전의 압축 및 암호화된 상태의 메모리코드이다.

[0048] 이때, 비교 검증값은 제2 메모리코드의 데이터 중 제2 OTP를 이용하여 추출된 소정 크기의 비교 데이터에 의해 생성될 수 있다. 이때, 비교 데이터는 제2 OTP를 이용하여 제2 메모리코드의 데이터 내에서 시작 지점과 끝 지점이 설정됨에 따라 추출될 수 있다. 다시 말해, 비교 데이터는 제2 OTP를 통해 압축 및 암호화된 제2 메모리코드의 특정 부분이 추출됨으로써 생성될 수 있다.

[0049] 구체적으로, 비교 데이터의 시작 지점은 제2 메모리코드의 시작 주소값으로부터 오프셋값(offset)을 더한 주소값을 가질 수 있다. 여기서, 오프셋값은 제2 OTP의 값을 제2 메모리코드의 크기값으로 나눈 몫에 대한 나머지인 제1 나머지값으로 설정될 수 있다.

[0050] 예컨대, 모바일 단말기(200)에서 생성된 제2 OTP의 값이 100100이고 제2 메모리코드의 크기값이 50000 byte인 경우, 오프셋값은 제2 OTP의 값인 100100에서 제2 메모리코드의 크기값인 50000을 나눈 몫 2에 대한 나머지인 100으로 설정될 수 있다. 이에 따라, 비교 데이터의 시작 지점은 제2 메모리코드의 시작 주소값으로부터 100번째 위치에 해당하는 주소값을 가질 수 있다.

[0051] 한편, 비교 데이터의 끝 지점은 오프셋값으로부터 사이즈값을 더한 주소값을 가질 수 있다. 여기서, 사이즈값은 제2 OTP의 값을 제2 메모리코드의 크기값과 제1 나머지값의 차이로 나눈 몫에 대한 나머지인 제2 나머지값으로 설정될 수 있다.

[0052] 예컨대, 전술한 예시에서와 같이, 모바일 단말기(200)에서 생성된 제2 OTP의 값이 100100이고 제2 메모리코드의 크기값이 50000 byte인 경우, 사이즈값은 제2 OTP의 값인 100100에서 제2 메모리코드의 크기값과 제1 나머지값의 차이값인 49900을 나눈 몫 2에 대한 나머지 300으로 설정될 수 있다. 이에 따라, 비교 데이터의 끝 지점은 제2 메모리코드의 시작 주소값에 오프셋값을 더한 주소값으로부터 300번째 위치에 해당하는 주소값을 가질 수

있다.

- [0053] 결과적으로, 제2 메모리코드가 50000 byte의 크기를 가지고 제2 OTP가 100100의 값을 가지면 오프셋값은 100으로, 사이즈값은 300으로 설정됨으로써, 제2 메모리코드의 100번째 위치부터 300 byte만큼의 크기를 가지는 데이터가 비교 데이터로 추출될 수 있다.
- [0054] 비교 검증값은 상기 과정을 거쳐 추출된 비교 데이터에 대한 해쉬값 및 모바일 단말기(200)의 고유정보에 기초하여 생성될 수 있다. 즉, 비교 검증값은 해쉬 함수(Hash Function)를 이용하여 추출된 비교 데이터의 해쉬값을 생성하고, 생성된 해쉬값과 모바일 단말기(200)의 고유정보를 연결하여 최종 생성될 수 있다.
- [0055] 다음으로, 실행 중인 어플리케이션에 대한 무결성을 검증하기 위한 경우, 비교 검증값은 모바일 단말기(200)에서 생성된 제2 OTP와 실행 중인 어플리케이션의 제3 메모리코드에 기초하여 생성될 수 있다. 여기서, 제3 메모리코드는 모바일 단말기(200)에서 실제로 실행 중인 어플리케이션에 대한 복호화된 상태의 메모리코드이다.
- [0056] 이때, 비교 검증값은 제3 메모리코드의 데이터 중 제2 OTP를 이용하여 추출된 소정 크기의 비교 데이터에 의해 생성될 수 있다. 이때, 비교 데이터는 제2 OTP를 이용하여 제3 메모리코드의 데이터 내에서 시작 지점과 끝 지점이 설정됨에 따라 추출될 수 있다. 다시 말해, 비교 데이터는 제2 OTP를 통해 복호화된 제3 메모리코드의 특정 부분이 추출됨으로써 생성될 수 있다.
- [0057] 구체적으로, 비교 데이터의 시작 지점은 제3 메모리코드의 시작 주소값으로부터 오프셋값(offset)을 더한 주소값을 가질 수 있다. 여기서, 오프셋값은 제2 OTP의 값을 제3 메모리코드의 크기값으로 나눈 몫에 대한 나머진 제1 나머지값으로 설정될 수 있다.
- [0058] 예컨대, 모바일 단말기(200)에서 생성된 제2 OTP의 값이 500200이고 제3 메모리코드의 크기값이 100000 byte인 경우, 오프셋값은 제2 OTP의 값인 500200에서 제2 메모리코드의 크기값인 100000을 나눈 몫 5에 대한 나머진 200으로 설정될 수 있다. 이에 따라, 비교 데이터의 시작 지점은 제3 메모리코드의 시작 주소값으로부터 200번째 위치에 해당하는 주소값을 가질 수 있다.
- [0059] 한편, 비교 데이터의 끝 지점은 오프셋값으로부터 사이즈값을 더한 주소값을 가질 수 있다. 여기서, 사이즈값은 제2 OTP의 값을 제3 메모리코드의 크기값과 제1 나머지값의 차이로 나눈 몫에 대한 나머진 제2 나머지값으로 설정될 수 있다.
- [0060] 예컨대, 전술한 예시에서와 같이, 모바일 단말기(200)에서 생성된 제2 OTP의 값이 500200이고 제3 메모리코드의 크기값이 100000 byte인 경우, 사이즈값은 제2 OTP의 값인 500200에서 제3 메모리코드의 크기값과 제1 나머지값의 차이값인 99800을 나눈 몫 5에 대한 나머지 1200으로 설정될 수 있다. 이에 따라, 비교 데이터의 끝 지점은 제2 메모리코드의 시작 주소값에 오프셋값을 더한 주소값으로부터 1200번째 위치에 해당하는 주소값을 가질 수 있다.
- [0061] 결과적으로, 제3 메모리코드가 100000 byte의 크기를 가지고 제2 OTP가 500200의 값을 가지면 오프셋값은 200으로, 사이즈값은 1200으로 설정됨으로써, 제3 메모리코드의 200번째 위치부터 1200 byte만큼의 크기를 가지는 데이터가 비교 데이터로 추출될 수 있다.
- [0062] 비교 검증값은 상기 과정을 거쳐 추출된 비교 데이터에 대한 해쉬값 및 모바일 단말기(200)의 고유정보에 기초하여 생성될 수 있다. 즉, 비교 검증값은 해쉬 함수(Hash Function)를 이용하여 추출된 비교 데이터의 해쉬값을 생성하고, 생성된 해쉬값과 모바일 단말기(200)의 고유정보를 연결하여 최종 생성될 수 있다.
- [0063] 참고로, 전술한 비교 검증값의 생성 과정에서 언급된 예시는 기준 검증값을 생성하는데 있어서 동일 및 유사하게 적용될 수 있다.
- [0064] 다시 도 2를 참조하면, 수신부(120)는 전술한 바와 같이 모바일 단말기(200)로부터 비교 검증값을 수신할 수 있는데, 실행되기 이전의 어플리케이션에 대한 비교 검증값을 수신하는 경우, 제2 메모리코드를 복호화하기 위한 복호화 키를 요청하는 요청값을 더 수신할 수 있다. 즉, 실행되기 이전의 어플리케이션의 제2 메모리코드는 암호화된 상태의 메모리코드이기 때문에 복호화 키를 통해 암호화를 해제한 후 어플리케이션을 실행시킬 수 있다.
- [0065] 비교부(130)는 기준 검증값 및 비교 검증값을 비교한다. 또한, 비교부(130)는 기준 검증값 및 비교 검증값을 비교하여 두 검증값의 일치 여부를 판단할 수 있다.
- [0066] 제어부(140)는 비교 결과에 기초하여 상기 모바일 단말기(200)와의 통신 설정을 제어한다.

- [0067] 구체적으로, 실행되기 이전의 어플리케이션의 제2 메모리코드에 기초하여 생성된 비교 검증값과 기준 검증값을 비교하는 경우에 비교부(130)는 비교 결과에 따라 두 검증값이 동일하다고 판단되면, 제2 메모리코드를 복호화할 수 있는 복호화 키의 값을 모바일 단말기(200)로 전송하도록 통신 설정을 제어할 수 있다. 반면에, 실행 중인 어플리케이션의 제3 메모리코드에 기초하여 생성된 비교 검증값과 기준 검증값을 비교하는 경우에 비교부(130)는 비교 결과에 따라 두 검증값이 동일하다고 판단되면 모바일 단말기(200)와의 통신이 유지되도록 통신 설정을 제어할 수 있다.
- [0068] 이로써, 본 발명의 일 실시예에 따르면, 해당 어플리케이션의 무결성을 검증하기 위한 검증값을 생성하는데 있어서 어플리케이션의 특정 위치부터 특정 길이만큼의 데이터를 추출하여 활용함으로써, 검증과정에 소요되는 시간을 최소화할 수 있고 검증과정의 절차를 보다 간소화할 수 있다.
- [0070] 도 4는 본 발명의 일 실시예에 따른 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버(100)의 제어 방법을 설명하기 위해 도시한 흐름도이다.
- [0071] 도 2 및 도 4를 참조하면, 단계(410)에서, 본 발명의 일 실시예에 따른 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버(100)의 생성부(110, OTP 생성부)는 제1 OTP를 생성한다.
- [0072] 다음으로, 단계(420)에서, 본 발명의 일 실시예에 따른 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버(100)의 생성부(110, 기준 검증값 생성부)는 제1 OTP 및 내부에 저장된 원본 어플리케이션의 제1 메모리코드에 기초하여 기준 검증값을 생성한다. 이때, 생성부(110)는 제1 OTP를 이용하여 제1 메모리코드의 데이터 내에서 시작 지점과 끝 지점을 설정하여 소정 크기의 기준 데이터를 추출할 수 있다.
- [0073] 여기서, 생성부(110)는 제1 메모리코드의 시작 주소값으로부터 오프셋값을 더한 주소값을 상기 기준 데이터의 시작 지점으로 설정하고, 오프셋값으로부터 사이즈값을 더한 주소값을 상기 기준 데이터의 끝 지점으로 설정할 수 있다. 구체적으로, 오프셋값은 상기 제1 OTP의 값을 상기 제1 메모리코드의 크기값으로 나눈 몫에 대한 나머지인 제1 나머지값으로 설정되고, 사이즈값은 상기 제1 OTP의 값을 상기 제1 메모리코드의 크기값과 상기 제1 나머지값의 차이로 나눈 몫에 대한 나머지인 제2 나머지값으로 설정될 수 있다.
- [0074] 이후에, 생성부(110)는 기준 데이터에 대한 해쉬값 및 모바일 단말기(200)의 고유정보에 기초하여 기준 검증값을 생성할 수 있다.
- [0075] 다음으로, 단계(430)에서, 본 발명의 일 실시예에 따른 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버(100)의 수신부(120)는 모바일 단말기(200)로부터 어플리케이션의 무결성을 검증하기 위한 비교 검증값을 수신한다. 이때, 수신부(120)는 모바일 단말기(200)로부터 모바일 단말기(200)의 고유정보를 더 수신할 수 있다.
- [0076] 다음으로, 단계(440)에서, 본 발명의 일 실시예에 따른 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버(100)의 비교부(130)는 기준 검증값 및 비교 검증값을 비교한다.
- [0077] 다음으로, 단계(450)에서, 본 발명의 일 실시예에 따른 어플리케이션의 무결성을 검증하기 위한 어플리케이션 서버(100)의 제어부(140)는 비교 결과에 기초하여 모바일 단말기(200)와의 통신 설정을 제어한다.
- [0078] 이하에서는, 도 5a 및 도 5b를 참조하여 어플리케이션의 무결성을 검증하기 위한 모바일 단말기(200) 및 어플리케이션 서버(100) 간의 통신과정을 보다 구체적으로 설명하고자 한다. 참고로, 도 5a는 도 4의 제어 방법에 있어서, 실행되기 이전의 어플리케이션의 무결성을 검증하기 위한 모바일 단말기(200) 및 어플리케이션 서버(100) 간의 통신과정을 설명하기 위해 도시한 도면이고, 도 5b는 도 4의 제어 방법에 있어서, 실행 중인 어플리케이션의 무결성을 검증하기 위한 모바일 단말기(200) 및 어플리케이션 서버(100) 간의 통신과정을 설명하기 위해 도시한 도면이다.
- [0079] 먼저, 실행되기 이전의 어플리케이션의 무결성을 검증하기 위한 방법이 적용되는 환경에는 도 5a에 도시된 바와 같이, 모바일 단말기(200) 및 어플리케이션 서버(100)를 포함할 수 있다.
- [0080] 1단계로, 어플리케이션 서버(100) 및 모바일 단말기(200)는 각각 OTP를 생성할 수 있다. 즉, 어플리케이션 서버(100)는 제1 OTP를 생성하고 모바일 단말기(200)는 제2 OTP를 생성할 수 있다. 여기서, 제1 OTP 및 제2 OTP는 서로 동시간에 생성될 수 있다.
- [0081] 2단계로, 어플리케이션 서버(100) 및 모바일 단말기(200)는 각각 해당 어플리케이션의 무결성을 검증하기 위한

검증값을 생성할 수 있다. 즉, 어플리케이션 서버(100)는 해당 어플리케이션의 무결성을 검증하기 위한 비교 작업을 위해 기준 대상이 되는 값인 기준 검증값을 생성하고, 모바일 단말기(200)는 해당 어플리케이션의 무결성을 검증하기 위한 비교 작업을 위해 비교 대상이 되는 값인 비교 검증값을 생성할 수 있다. 기준 검증값 및 비교 검증값을 생성하는 구체적인 과정은 도 2 및 도 3을 참조하여 기술한 내용에 기초한다.

[0082] 3단계로, 모바일 단말기(200)는 비교 검증값을 복호화 키 요청값과 함께 어플리케이션 서버(100)로 전송할 수 있다. 이때, 복호화 키 요청값은 해당 어플리케이션이 압축 및 암호화된 상태의 메모리코드로 구성됨에 따라, 메모리코드의 암호화를 해제하기 위한 복호화 키의 요청을 의미한다.

[0083] 4단계로, 어플리케이션 서버(100)는 모바일 단말기(200)로부터 수신한 비교 검증값을 기준 검증값과 비교할 수 있다. 이에 따라, 어플리케이션 서버(100)는 기준 검증값과 비교 검증값이 동일한지 여부를 판단할 수 있다.

[0084] 5단계로, 어플리케이션 서버(100)는 비교 결과에 기초하여, 기준 검증값과 비교 검증값이 동일하다고 판단되는 경우, 모바일 단말기(200)로 암호화된 메모리코드에 대한 복호화 키의 값을 전송할 수 있다. 반면에, 기준 검증값과 비교 검증값이 동일하지 않다고 판단되는 경우, 모바일 단말기(200)와의 통신을 종료할 수 있다.

[0085] 한편, 기준 검증값과 비교 검증값이 동일하다고 판단되어 어플리케이션 서버(100)로부터 모바일 단말기(200)로 복호화 키의 값이 전송되는 경우, 6단계로, 모바일 단말기(200)는 어플리케이션 서버(100)로부터 수신한 복호화 키의 값을 이용하여 암호화된 메모리코드를 복호화하여 해당 어플리케이션을 실행시킬 수 있다.

[0086] 다음으로, 실행되기 이전의 어플리케이션의 무결성을 검증하기 위한 방법이 적용되는 환경에는 도 5b에 도시된 바와 같이, 모바일 단말기(200) 및 어플리케이션 서버(100)를 포함할 수 있다.

[0087] 1단계로, 어플리케이션 서버(100) 및 모바일 단말기(200)는 각각 OTP를 생성할 수 있다. 즉, 어플리케이션 서버(100)는 제1 OTP를 생성하고 모바일 단말기(200)는 제2 OTP를 생성할 수 있다. 여기서, 제1 OTP 및 제2 OTP는 서로 동시간에 생성될 수 있다.

[0088] 2단계로, 어플리케이션 서버(100) 및 모바일 단말기(200)는 각각 해당 어플리케이션의 무결성을 검증하기 위한 검증값을 생성할 수 있다. 즉, 어플리케이션 서버(100)는 해당 어플리케이션의 무결성을 검증하기 위한 비교 작업을 위해 기준 대상이 되는 값인 기준 검증값을 생성하고, 모바일 단말기(200)는 해당 어플리케이션의 무결성을 검증하기 위한 비교 작업을 위해 비교 대상이 되는 값인 비교 검증값을 생성할 수 있다. 기준 검증값 및 비교 검증값을 생성하는 구체적인 과정은 도 2 및 도 3을 참조하여 기술한 내용에 기초한다.

[0089] 3단계로, 모바일 단말기(200)는 비교 검증값을 어플리케이션 서버(100)로 전송할 수 있다.

[0090] 4단계로, 어플리케이션 서버(100)는 모바일 단말기(200)로부터 수신한 비교 검증값을 기준 검증값과 비교할 수 있다. 이에 따라, 어플리케이션 서버(100)는 기준 검증값과 비교 검증값이 동일한지 여부를 판단할 수 있다.

[0091] 5단계로, 어플리케이션 서버(100)는 비교 결과에 기초하여, 기준 검증값과 비교 검증값이 동일하다고 판단되는 경우, 모바일 단말기(200)와의 통신을 유지할 수 있다. 반면에, 기준 검증값과 비교 검증값이 동일하지 않다고 판단되는 경우, 모바일 단말기(200)와의 통신을 종료할 수 있다.

[0093] 지금까지 본 발명에 따른 구체적인 실시예에 관하여 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서는 여러 가지 변형이 가능함은 물론이다. 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허 청구의 범위뿐 아니라 이 특허 청구의 범위와 균등한 것들에 의해 정해져야 한다.

[0094] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 이는 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명 사상은 아래에 기재된 특허청구범위에 의해서만 파악되어야 하고, 이의 균등 또는 등가적 변형 모두는 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0095] 100 : 어플리케이션 서버

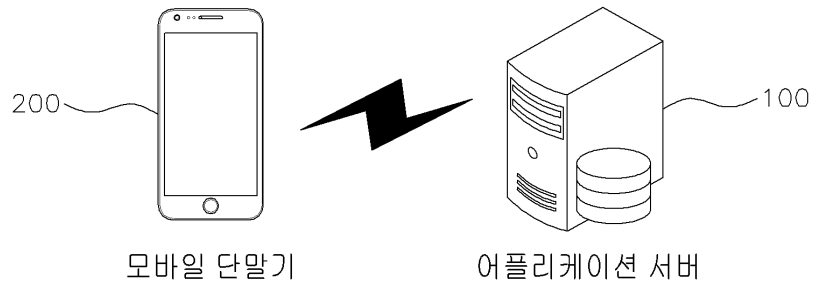
110 : 생성부

120 : 수신부

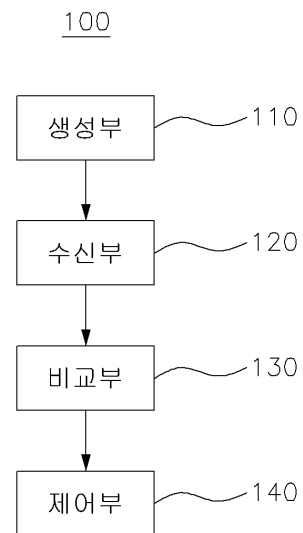
130 : 비교부
 140 : 제어부
 200 : 모바일 단말기

도면

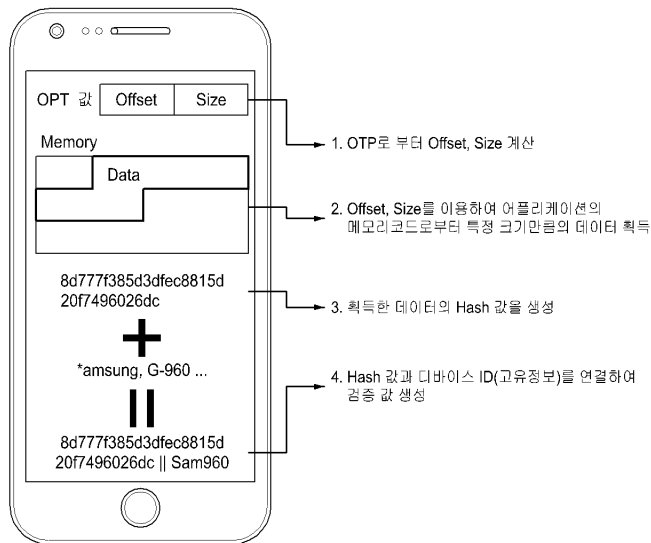
도면1



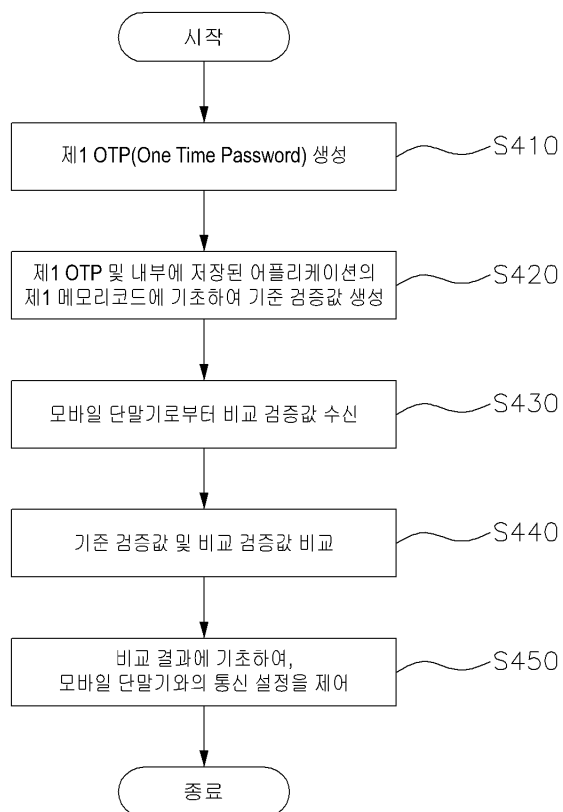
도면2



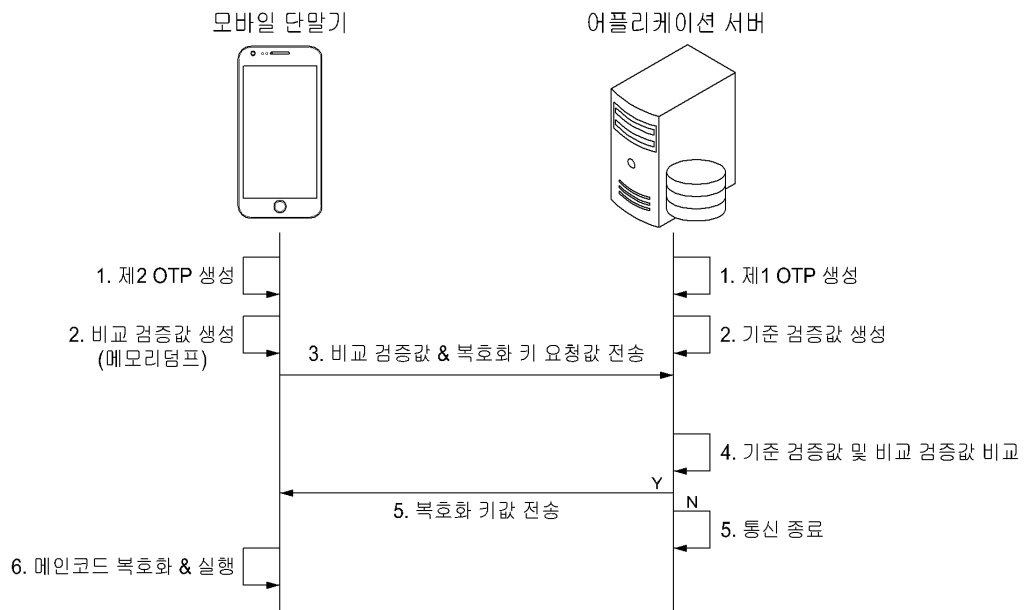
도면3



도면4



도면5



도면6

