(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년07월29일
(11) 등록번호 10-2689195
(24) 등록일자 2024년07월24일

(51) 국제특허분류(Int. Cl.)
*H04L 9/32* (2006.01) *H04L 65/40* (2022.01)
*H04L 9/06* (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
*H04L 9/3231* (2013.01)
*H04L 67/12* (2022.05)
(21) 출원번호 10-2018-7011624
(22) 출원일자(국제) 2016년10월18일
심사청구일자 2021년10월14일
(85) 번역문제출일자 2018년04월24일
(65) 공개번호 10-2018-0075513
(43) 공개일자 2018년07월04일
(86) 국제출원번호 PCT/CN2016/102323
(87) 국제공개번호 WO 2017/071496
국제공개일자 2017년05월04일
(30) 우선권주장
201510702527.3 2015년10월26일 중국(CN)
(56) 선행기술조사문헌
US20060070114 A1
*(뒷면에 계속)*

(73) 특허권자
**알리바바 그룹 홀딩 리미티드**
케이만군도, 그랜드 케이만, 조지 타운, 피.오. 박스 847, 원 캐피탈 플레이스, 플로어 4
(72) 발명자
**팡 키앙**
중국 제지앙 311121 항조우 유 항 디스트릭트 웨스트 웬 위 로드 넘버 969 빌딩 3 5/에프 알리바바 그룹 리갈 디파트먼트
**두안 차오**
중국 제지앙 311121 항조우 유 항 디스트릭트 웨스트 웬 위 로드 넘버 969 빌딩 3 5/에프 알리바바 그룹 리갈 디파트먼트
(74) 대리인
**제일특허법인(유)**

전체 청구항 수 : 총 18 항 심사관 : 나용수

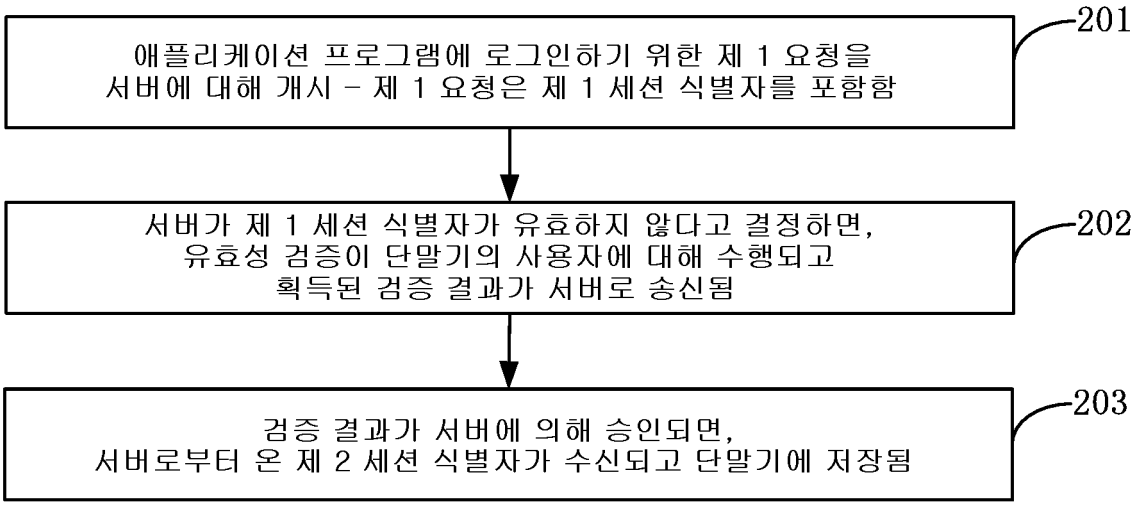
(54) 발명의 명칭 **세션 식별자 동기화를 실현하는 방법 및 장치**

## (57) 요 약

세션 식별자 동기화를 실현하는 방법 및 장치가 본 출원에 제공된다. 이러한 방법은 애플리케이션 프로그램에 로그인하기 위한 제 1 요청을 서버에 개시하는 단계 - 제 1 식별자는 애플리케이션 프로그램의 로그인 계정 및 오리지널 패스워드로부터 생성되고, 오리지널 패스워드는 수정 전의 로그인 계정에 대응하는 로그인 패스워드임-

(뒷면에 계속)

*대 표 도* - 도2



와, 획득된 검증 결과를 서버에 전송하여 제 1 세션 식별자가 서버에 의해 유효하지 않다고 결정되면 서버로 하여금 검증 결과에 대한 확인을 수행하게 하는 단계와, 검증 결과가 서버에 의해 검증되고 승인된 경우, 서버로부터 제 2 세션 식별자를 수신하고 제 2 세션 식별자를 단말기에 저장하는 단계 - 제 2 세션 식별자는 로그인 계정 및 새로운 패스워드로부터 생성되고, 새로운 패스워드는 변경 후의 로그인 계정에 대응하는 로그인운 패스워드임 - 를 포함한다. 본 출원의 기술적 해결책은 단말기의 사용자가 애플리케이션 프로그램에 로그인 하기 위해 새로운 패스워드를 재입력하는 것을 방지할 수 있고 애플리케이션 프로그램에 로그인하는 사용자 경험을 크게 향상시킬 수 있다.

(52) CPC특허분류
***H04L 67/146*** (2022.05)
***H04L 9/0631*** (2013.01)
***H04L 9/0825*** (2013.01)

(56) 선행기술조사문헌
US20140165147 A1
US20090210938 A1
US08973113 B1
CN101594350 A
CN103618604 A

# 명 세 서

## 청구범위

### 청구항 1

단말기에 적용되는 세션 식별자 동기화를 실현하기 위한 방법으로서,

애플리케이션 프로그램에 로그인하기 위한 제 1 요청을 서버에 개시하는 단계 - 상기 제 1 요청은 제 1 세션 식별자를 포함하고, 상기 제 1 세션 식별자는 상기 애플리케이션 프로그램의 로그인 계정 및 오리지널 패스워드로부터 생성되며, 상기 오리지널 패스워드는 수정 이전의 상기 로그인 계정에 대응하는 로그인 패스워드임 - 와,

상기 제 1 세션 식별자가 상기 서버에 의해 유효하지 않은 것으로 결정된 경우 상기 단말기의 사용자에 대한 유효성 검증을 수행하고 획득된 검증 결과를 상기 서버로 송신하여 상기 서버로 하여금 상기 검증 결과에 대한 확인을 수행할 수 있게 하는 단계와,

상기 검증 결과가 상기 서버에 의해 검증되고 승인된 경우 상기 서버로부터 제 2 세션 식별자를 수신하고 상기 제 2 세션 식별자를 상기 단말기에 저장하는 단계 - 상기 제 2 세션 식별자는 상기 로그인 계정 및 새로운 패스워드로부터 생성되고, 상기 새로운 패스워드는 상기 수정 후의 상기 로그인 계정에 대응함 -

를 포함하는

방법.

### 청구항 2

제 1 항에 있어서,

상기 검증 결과에 대응하는 검증 문자열(verification character string)의 난수를 해시 알고리즘을 이용하여 생성하는 단계와,

상기 서버의 대칭 비밀 키를 이용하여 상기 검증 문자열 및 상기 난수를 암호화하여 암호화된 검증 결과를 획득하는 단계

를 더 포함하는

방법.

### 청구항 3

제 2 항에 있어서,

비대칭 암호화 알고리즘에 기초하여 상기 단말기의 공개 키 및 개인 키를 생성하는 단계와,

상기 단말기의 공개 키를 상기 서버에 송신하는 단계와,

상기 서버로부터 상기 단말기의 공개 키를 이용하여 암호화된 상기 서버의 대칭 비밀 키를 수신하는 단계와,

상기 서버의 대칭 비밀 키를 획득하기 위해 상기 단말기의 개인 키를 사용하여 암호화된 상기 대칭 비밀 키를 복호화하는 단계

를 더 포함하는

방법.

### 청구항 4

제 1 항에 있어서,

상기 단말기의 사용자에 대한 유효성 검증을 수행하는 것은,

생체 센서를 이용하여 상기 애플리케이션 프로그램의 로그인 인터페이스 상에서 상기 단말기의 사용자의 생체 특성을 수집하는 것과,

상기 생체 특성에 대한 검증을 수행하는 것과,

상기 생체 특성이 상기 검증을 통과하면, 상기 단말기의 사용자가 정당한 사용자인 것으로 결정하는 것과,

상기 생체 특성이 상기 검증을 통과하지 못하면 상기 로그인 계정 및 상기 로그인 패스워드를 사용하여 상기 애플리케이션 프로그램에 로그인하기 위해 상기 애플리케이션 프로그램의 로그인 인터페이스 상에 프롬프트를 제공하는 것

을 포함하는

방법.

**청구항 5**

제1항 내지 제4항 중 어느 한 항에 있어서,

상기 제 2 세션 식별자가 유효 기간 내에 있는지 여부를 결정하는 단계와,

상기 제 2 세션 식별자가 상기 유효 기간 내에 있는 경우, 상기 제 2 세션 식별자를 사용하여 상기 애플리케이션 프로그램이 로그인되는 것으로 결정하는 단계와,

상기 제 2 세션 식별자가 상기 유효 기간을 벗어난 경우, 상기 로그인 계정 및 상기 로그인 계정의 유효한 로그인 패스워드를 사용하여 상기 애플리케이션 프로그램에 로그인하도록 사용자에게 프롬프트하는 단계

를 더 포함하는

방법.

**청구항 6**

서버에 적용되는 세션 식별자 동기화를 실현하기 위한 방법으로서,

애플리케이션 프로그램에 로그인하기 위한 제 1 요청이 단말기에서 개시될 때 상기 제 1 요청에 포함된 제 1 세션 식별자의 유효성을 검증하는 단계 - 상기 제 1 세션 식별자는 상기 애플리케이션 프로그램의 로그인 계정 및 오리지널 패스워드로부터 생성되며, 상기 오리지널 패스워드는 수정 이전의 상기 로그인 계정에 대응하는 로그인 패스워드임 - 와,

상기 제 1 세션 식별자가 유효하지 않은 것으로 검증되면, 상기 단말기의 사용자에 대한 유효성 검증을 수행하도록 상기 단말기에 지시하는 단계와,

상기 단말기로부터 상기 사용자에 대한 유효성 검증의 검증 결과를 수신하는 단계와,

상기 검증 결과가 상기 서버에 의해 검증되고 승인된 경우, 제 2 세션 식별자를 상기 단말기에 송신하는 단계 - 상기 제 2 세션 식별자는 상기 로그인 계정 및 새로운 패스워드로부터 생성되고 상기 새로운 패스워드는 상기 수정 후의 상기 로그인 계정에 대응하는 로그인 패스워드임 -

를 포함하는

방법.

**청구항 7**

제 6 항에 있어서,

상기 검증 결과가 상기 서버의 대칭 비밀 키를 사용하여 상기 단말기에 의해 암호화되는 경우, 상기 서버의 대칭 비밀 키를 이용하여 암호화된 검증 결과를 복호화하여 상기 검증 결과에 대응하는 검증 문자열 및 난수를 획득하는 단계와,

상기 검증 문자열 및 상기 난수에 대한 검증을 수행하는 단계와,

상기 검증 문자열과 상기 난수가 상기 검증을 통과하면, 상기 제 2 세션 식별자를 상기 단말기에 송신하는 단계

를 더 포함하는

방법.

**청구항 8**

제 7 항에 있어서,

대칭 암호화 알고리즘에 기초하여 상기 서버의 상기 대칭 비밀 키를 생성하는 단계와,

상기 단말기의 공개 키를 이용하여 상기 대칭 비밀 키를 암호화하는 단계와,

상기 암호화된 대칭 비밀 키를 상기 단말기로 송신하여 상기 단말기로 하여금 상기 공개 키에 대응하는 개인 키를 사용하여 상기 암호화된 대칭 비밀 키를 복호화함으로써 상기 서버의 대칭 비밀 키를 획득하도록 하는 단계

를 포함하는

방법.

**청구항 9**

제 6 항 내지 제 8 항 중 어느 한 항에 있어서,

상기 제 2 세션 식별자가 유효 기간 내에 있는지 여부를 결정하는 단계와,

상기 제 2 세션 식별자가 상기 유효 기간 내에 있는 경우, 상기 사용자로 하여금 상기 제 2 세션 식별자를 통해 상기 애플리케이션 프로그램에 로그인할 수 있게 하는 단계와,

상기 제 2 세션 식별자가 상기 유효 기간을 벗어난 경우 상기 사용자가 상기 제 2 세션 식별자를 통해 상기 애플리케이션 프로그램에 로그인하는 것을 금지하는 단계

를 더 포함하는

방법.

**청구항 10**

세션 식별자 동기화를 실현하기 위한 장치로서,

애플리케이션 프로그램으로 로그인하기 위한 제 1 요청을 서버에 개시하는 데 사용되는 제 1 송신 모듈 - 상기 제 1 요청은 제 1 세션 식별자를 포함하며, 상기 제 1 세션 식별자는 상기 애플리케이션 프로그램의 로그인 계정 및 오리지널 패스워드로부터 생성되고, 상기 오리지널 패스워드는 수정 전의 상기 로그인 계정에 대응하는 로그인 패스워드임 - 과,

상기 제 1 송신 모듈에 의해 송신된 상기 제 1 세션 식별자가 상기 서버에 의해 유효하지 않은 것으로 결정되면 단말기의 사용자에 대한 유효성 검증을 수행하고 획득된 검증 결과를 상기 서버로 송신하여 상기 서버로 하여금 상기 검증 결과에 대한 확인을 수행할 수 있게 하는 데 사용되는 제 1 검증 모듈과,

상기 제 1 검증 모듈에 의해 획득된 검증 결과가 상기 서버에 의해 검증되고 승인된 경우 상기 서버로부터 제 2

세션 식별자를 수신하고 상기 제 2 세션 식별자를 상기 단말기에 저장하는 데 사용되는 제 1 수신 모듈 - 상기 제 2 세션 식별자는 상기 로그인 계정 및 새로운 패스워드로부터 생성되고, 상기 새로운 패스워드는 수정 후의 상기 로그인 계정에 대응하는 로그인 패스워드임 -

을 포함하는

장치.

**청구항 11**

제 10 항에 있어서,

상기 장치는,

상기 제 1 검증 모듈에 의해 획득된 검증 결과에 대응하는 검증 문자열의 난수를 생성하는 데 사용되는 제 1 생성 모듈과,

상기 제 1 검증 결과에 의해 획득된 검증 문자열과 상기 제 1 생성 모듈에 의해 생성된 난수를 상기 서버의 대칭 비밀 키를 사용하여 암호화하여 암호화된 검증 결과를 획득하는 데 사용되는 제 1 암호화 모듈

을 더 포함하는

장치.

**청구항 12**

제 11 항에 있어서,

상기 장치는,

비대칭 암호화 알고리즘을 이용하여 상기 단말기의 공개 키 및 개인 키를 생성하는 데 사용되는 제 2 생성 모듈과,

상기 제 2 생성 모듈에 의해 생성된 상기 단말기의 공개 키를 상기 서버에 송신하는 데 사용되는 제 2 송신 모듈과,

상기 서버로부터 상기 제 2 송신 모듈에 의해 송신된 상기 단말기의 상기 공개 키를 사용하여 암호화된 상기 서버의 상기 대칭 비밀 키를 수신하는 데 사용되는 제 2 수신 모듈과,

상기 제 2 생성 모듈에 의해 생성된 상기 단말기의 개인 키를 이용하여 상기 암호화된 대칭 비밀 키를 복호화하여 상기 서버의 대칭 비밀 키를 획득하는 데 사용되는 제 1 복호화 모듈

을 더 포함하는

장치.

**청구항 13**

제 10 항에 있어서,

상기 제 1 검증 모듈은,

생체 센서를 통해 상기 애플리케이션 프로그램의 로그인 인터페이스 상에 상기 단말기의 사용자의 생체 특성을 수집하는 데 사용되는 특성 수집 유닛과,

상기 특성 수집 유닛에 의해 수집된 상기 생체 특성에 대한 검증을 수행하는 데 사용되는 검증 유닛과,

상기 생체 특성이 상기 검증 유닛의 검증을 통과하면, 상기 단말기의 사용자가 정당한 사용자인 것으로 결정하는 데 사용되는 제 1 결정 유닛과,

상기 로그인 계정 및 상기 로그인 패스워드를 이용하여 상기 애플리케이션 프로그램에 로그인하기 위해 상기 애플리케이션 프로그램의 로그인 인터페이스 상에 프롬프트를 제공하는 데 사용되는 프롬프트 유닛

을 포함하는

장치.

**청구항 14**

제 10 항 내지 제 13 항 중 어느 한 항에 있어서

상기 장치는,

상기 제 1 수신 모듈에 의해 수신된 상기 제 2 세션 식별자가 유효 기간 내에 있는지 여부를 결정하는 데 사용되는 제 1 결정 모듈과,

상기 제 1 결정 모듈이 상기 제 2 세션 식별자가 상기 유효 기간 내에 있다고 결정하면, 상기 제 2 세션 식별자가 상기 애플리케이션 프로그램에 로그인하는 데 사용되는 것으로 결정하는 데 사용되는 제 2 결정 모듈과,

상기 제 1 결정 모듈(120)이 상기 제 2 세션 식별자가 상기 유효 기간을 벗어났다고 결정하면, 상기 로그인 계정 및 상기 로그인 계정의 유효한 로그인 패스워드를 사용하여 상기 애플리케이션 프로그램에 로그인하도록 상기 사용자에게 프롬프팅하는 데 사용되는 프롬프트 모듈을

더 포함하는

장치.

**청구항 15**

세션 식별자 동기화를 실현하기 위한 장치로서,

단말기에서 제 1 요청이 개시되면 애플리케이션 프로그램에 로그인하기 위한 제 1 요청에 포함된 제 1 세션 식별자의 유효성을 검증하는 데 사용되는 제 2 검증 모듈 - 제 1 세션 식별자는 상기 애플리케이션 프로그램의 로그인 계정 및 오리지널 패스워드로부터 생성되고, 상기 오리지널 패스워드는 수정 전의 상기 로그인 계정에 대응하는 로그인 패스워드임 - 과,

상기 제 1 세션 식별자가 상기 제 2 검증 모듈에 의해 유효하지 않은 것으로 검증되면 상기 단말기의 사용자에 대한 유효성 검증을 수행하도록 상기 단말기에 지시하는 데 사용되는 명령 모듈과,

상기 명령 모듈의 지시에 따라 상기 단말기에 의해 수행되는 상기 사용자의 유효성 검증의 검증 결과를 수신하는 데 사용되는 제 3 수신 모듈과,

상기 제 3 수신 모듈에 의해 수신된 검증 결과가 서버에 의해 검증되고 승인된 경우, 제 2 세션 식별자를 상기 단말기에 송신하는 데 사용되는 제 3 송신 모듈 - 상기 제 2 세션 식별자는 상기 로그인 계정 및 새로운 패스워드로부터 생성되고, 상기 새로운 패스워드는 상기 수정 후의 로그인 계정에 대응하는 로그인 패스워드임 -

을 포함하는

장치.

**청구항 16**

제 15 항에 있어서,

상기 장치는,

상기 제 3 수신 모듈에 의해 획득된 검증 결과가 상기 서버의 대칭 비밀 키를 사용하여 상기 단말기에 의해 암호화된 경우, 상기 서버의 대칭 비밀 키를 이용하여 암호화된 검증 결과를 복호화하여 상기 검증 결과에 대응하

는 검증 문자열 및 난수를 획득하는 데 사용되는 제 2 복호화 모듈과,

상기 제 2 복호화 모듈에 의한 복호화 후에 획득된 상기 검증 문자열 및 상기 난수에 대한 검증을 수행하는 데 사용되는 제 3 검증 모듈

을 더 포함하되,

상기 제 3 송신 모듈은, 상기 검증 문자열과 상기 난수가 검증을 통과한 경우 상기 제 2 세션 식별자를 상기 단말기로 송신하는

장치.

**청구항 17**

제 16 항에 있어서,

상기 장치는,

대칭 암호화 알고리즘에 기초하여 상기 서버의 대칭 비밀 키를 생성하여 상기 제 2 복호화 모듈이 상기 암호화된 검증 결과를 상기 서버의 대칭 비밀 키를 사용하여 복호화할 수 있게 하는 데 사용되는 제 3 생성 모듈과,

상기 제 3 생성 모듈에 의해 생성된 상기 대칭 비밀 키를 상기 단말기의 공개 키를 이용하여 암호화하는 데 사용되는 제 2 암호화 모듈과,

상기 제 2 암호화 모듈에 의해 암호화된 상기 대칭 비밀 키를 상기 단말기에 송신하여, 상기 단말기로 하여금 상기 공개 키에 대응하는 개인 키를 사용하여 암호화된 상기 대칭 비밀 키를 복호화하게 하여 상기 서버의 대칭 키를 획득하는 데 사용되는 제 4 송신 모듈

을 더 포함하는

장치.

**청구항 18**

제 15 항 내지 제 17 항 중 어느 한 항에 있어서,

상기 장치는,

상기 제 3 송신 모듈에 의해 송신된 상기 제 2 세션 식별자가 유효 기간 내에 있는지 여부를 결정하는 데 사용되는 제 3 결정 모듈과,

상기 제 2 세션 식별자가 상기 유효 기간 내에 있다고 상기 제 3 결정 모듈이 결정하면 상기 사용자로 하여금 상기 제 2 세션 식별자를 이용하여 상기 애플리케이션 프로그램에 로그인하게 하는 데 사용되는 제 1 제어 모듈과,

상기 제 3 결정 모듈(140)이 상기 제 2 세션 식별자가 상기 유효 기간을 벗어난 것으로 결정하면, 상기 제 2 세션 식별자를 이용하여 상기 사용자가 상기 애플리케이션 프로그램에 로그인하는 것을 금지하는 데 사용되는 제 2 제어 모듈

을 더 포함하는

장치.

## *발명의 설명*

### *기 술 분 야*

[0001] 관련 특허 출원의 상호 참조

[0002] 본 출원은 2015년 10월 26일자로 출원된 "세션 식별자 동기화를 실현하기 위한 방법 및 장치"라는 명칭의 중국

특허 출원 제 201510702527.3 호에 대한 우선권을 주장하며, 이는 전체로서 본 명세서에 참조로 포함된다.

[0003] 기술 분야

[0004] 본 발명은 네트워크 보안 관련 기술 분야에 관한 것으로, 특히 세션 식별자 동기화를 실현하는 방법 및 장치에 관한 것이다.

## 배 경 기 술

[0005] 임베딩 기술 및 단말기 기술의 지속적인 개발과 함께, 점점 더 많은 수의 단말기 장치가 사람들의 일상생활에 적용되고 있다. 단말기 장치에 설치된 애플리케이션 프로그램은 또한 Windows, Linux, Android, iOS 등 다른 운영 체제에서 사용하기에 적합한 다양한 유형의 버전으로 설계되었다. 사용자가 이들의 계정을 사용하여 상이한 단말기 장치에서 애플리케이션 프로그램에 액세스할 때 그러한 계정의 신원 검증의 문제가 발생한다. 사용자가 신원 검증 정보를 반복적으로 입력하는 것을 방지하기 위해, 많은 애플리케이션 프로그램에는 패스워드 기록 기능이 포함되어 있다. 그러나 사용자가 단말기 장치 중 하나의 단말기 장치의 애플리케이션 프로그램과 관련된 패스워드를 재설정한 후에 사용자가 다른 단말기 장치를 통해 애플리케이션 프로그램에 로그인해야 할 때, 다른 단말기 장치에 이전에 기록된 패스워드는 유효하지 않게 되었으므로 사용자는 그러한 애플리케이션 프로그램에 대해 새로운 패스워드를 입력해야 한다. 일부 시나리오에서는, 다른 단말기 장치를 통해 새로운 패스워드를 입력하는 것이 사용자에게 편리하지 않을 수 있다. 예를 들어, 다른 작업을 하고 있는 사용자의 경우 양손이 사용되고 있을 때 단말기 장치에 새로운 패스워드를 입력하는 것은 특정 보안 위험을 일으킬 수 있다.

## 발명의 내용

[0006] 따라서, 본 출원은 사용자가 새로운 패스워드를 다시 입력할 필요 없이 다른 단말기의 애플리케이션 프로그램에 로그인하게 할 수 있고, 애플리케이션 프로그램의 로그인 보안을 보장할 수 있는 새로운 기술적 해결책을 제공한다.

[0007] 전술한 목적을 달성하기 위해, 본 발명은 다음의 기술적 해결책을 제공한다.

[0008] 본 발명의 제 1 측면에 따라, 패스워드 동기화를 실현하는 방법이 제공되는데, 이러한 방법은 애플리케이션 프로그램에 로그인하기 위한 제 1 요청을 서버에 대해 개시하는 단계 - 제 1 요청은 로그인 계정 및 애플리케이션 프로그램의 오리지널 패스워드로부터 생성되는 제 1 세션 식별자를 포함하고, 오리지널 패스워드는 수정 전의 로그인 계정에 대응하는 로그인 패스워드임 -; 단말기의 사용자에 대한 유효성 증을 수행하고 제 1 세션 식별자가 서버에 의해 유효하지 않은 것으로 결정되면 획득된 검증 결과를 서버로 송신하여 서버로 하여금 검증 결과에 대한 확인을 수행하도록 하는 단계; 서버로부터 제 2 세션 식별자를 수신하고, 검증 결과가 서버에 의해 검증되고 승인된 경우 제 2 세션 식별자를 단말기에 저장하는 단계 - 제 2 세션 식별자는 로그인 계정 및 새로운 패스워드로부터 생성되며, 새로운 패스워드는 수정 후의 로그인 계정에 해당하는 로그인 패스워드임 - 를 포함한다.

[0009] 본 발명의 제 2 측면에 따라, 제 1 요청이 단말기에서 개시될 때 애플리케이션 프로그램에 로그인하기 위한 제 1 요청에 포함된 제 1 세션 식별자의 유효성을 검증하는 단계 - 제 1 세션 식별자는 애플리케이션 프로그램의 로그인 계정 및 오리지널 패스워드로부터 생성되며, 오리지널 패스워드는 수정 이전의 로그인 계정에 대응하는 로그인 패스워드임 -; 제 1 세션 식별자가 유효하지 않은 것으로 확인되면, 단말기로 하여금 단말기의 사용자에 대한 유효성 검증을 수행하도록 단말기에 지시하는 단계; 단말기로부터 유효성 검증의 검증 결과를 수신하는 단계; 및 검증 결과가 서버에 의해 검증되고 승인되는 경우, 단말기에 제 2 세션 식별자를 송신하는 단계 - 상기 제 2 세션 식별자는 로그인 계정 및 새로운 패스워드로부터 생성되고, 상기 새로운 수정 후의 로그인 계정에 대응하는 로그인 패스워드임 - 를 포함한다.

[0010] 본 발명의 제 3 측면에 따라, 패스워드 동기화를 실현하기 위한 장치가 제공되는데, 이러한 장치는 애플리케이션 프로그램에 로그인하기 위한 제 1 요청을 서버에 대해 개시하는 데 사용되는 제 1 송신 모듈 - 제 1 요청은 제 1 세션 식별자를 포함하고, 제 1 세션 식별자는 애플리케이션 프로그램의 로그인 계정 및 오리지널 패스워드로부터 생성되고, 오리지널 패스워드는 수정하기 전의 로그인 계정에 대응하는 로그인 패스워드임 - ; 단말기의 사용자에 대한 유효성 검증을 수행하고 획득된 검증 결과를 서버로 전송하여 제 1 송신 모듈에 의해 송신된 제 1 세션 식별자가 서버에 의해 유효하지 않은 것으로 결정된 경우 서버로 하여금 검증 결과에 대한 확인을 수행하게 하는 제 1 검증 모듈; 및 서버로부터 제 2 세션 식별자를 수신하고, 제 1 검증 모듈에 의해 획득된 검증 결과가 서버에 의해 검증되고 승인된 경우 제 2 세션 식별자를 단말기에 저장하는 제 1 수신 모듈을 포함하며,

제 2 세션 식별자는 수정 후의 로그인 계정에 대응하는 로그인 패스워드인 새로운 패스워드 및 로그인 계정으로부터 생성된다.

[0011] 본 출원의 제 4 측면에 따라, 패스워드 동기화를 실현하기 위한 장치가 제공되며, 이 장치는, 단말기에서 제 1 요청이 개시될 때 애플리케이션 프로그램에 로그인하기 위한 제 1 요청에 포함된 제 1 세션 식별자의 유효성을 검증하기 위해 사용되는 제 2 검증 모듈 - 제 1 세션 식별자는 애플리케이션 프로그램의 로그인 계정 및 오리지널 패스워드로부터 생성되며, 오리지널 패스워드는 수정 이전의 로그인 계정에 대응하는 로그인 패스워드임 - ; 제 1 세션 식별자가 제 2 검증 모듈에 의해 유효하지 않은 것으로 검증되면 단말기의 사용자에 대한 유효성 검증을 수행하도록 단말기에 지시하는 데 사용되는 명령 모듈; 명령 모듈의 지시에 따라 단말기에 의해 수행된 사용자에 대한 유효성 검증의 검증 결과를 수신하는 데 사용되는 제 3 수신 모듈; 및 제 3 수신 모듈에 의해 수신된 검증 결과가 서버에 의해 검증되고 승인된 경우, 로그인 계정 및 새로운 패스워드로부터 생성되는 제 2 세션 식별자를 단말기에 송신하는 데 사용되는 제 3 송신 모듈을 포함하며, 새로운 패스워드는 수정 후의 로그인 계정에 대응하는 로그인 패스워드이다.

[0012] 전술한 기술적 해결책으로부터 알 수 있는 바와 같이, 본 출원은 사용자가 제 2 세션 식별자를 통해 애플리케이션 프로그램에 로그인할 수 있게 함으로써, 단말기를 사용하는 사용자가 애플리케이션 프로그램에 로그인하기 위해 새로운 패스워드를 다시 입력해야 하는 것을 방지하고, 애플리케이션 프로그램에 로그인할 때의 사용자 경험을 크게 향상시킨다. 다수의 사용자가 애플리케이션 프로그램과 관련된 로그인 패스워드를 재설정해야 하는 경우 사용자의 유효성 검증을 수행하여 단말기 정당성을 검증함으로써 사용자 정당성(user legitimacy) 검증과 관련된 서버의 작업 부하를 줄임으로써, 서버의 자원 낭비를 방지할 수 있다.

## *도면의 간단한 설명*

[0013] 도 1은 제 1 단말기를 통해 애플리케이션 프로그램과 관련된 로그인 패스워드를 수정하는 프로세스를 나타내는 흐름도이다.

도 2는 본 발명의 일 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 1 예시적인 방법을 나타내는 흐름도이다.

도 3a는 본 발명의 일 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 2 예시적인 방법을 나타내는 흐름도이다.

도 3b는 도 3a의 단말기와 서버 간에 키를 동기화하는 방식을 나타내는 흐름도이다.

도 4는 본 발명의 일 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 3 예시적인 방법을 나타내는 흐름도이다.

도 5는 본 발명의 일 실시예에 따른 세션 식별자 동기화를 실현하기 위한 제 4 예시적인 방법을 나타내는 흐름도이다.

도 6은 본 발명의 다른 실시예에 따른 세션 식별자 동기화를 실현하기 위한 제 1 예시적인 방법을 나타내는 흐름도이다.

도 7은 본 발명의 다른 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 2 예시적인 방법을 나타내는 흐름도이다.

도 8은 본 발명의 다른 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 3 예시적인 방법을 나타내는 흐름도이다.

도 9는 본 발명의 예시적인 실시예에 따른 단말기의 개략적인 구조도이다.

도 10은 본 발명의 예시적인 실시예에 따른 서버의 개략적인 구조도이다.

도 11은 본 발명의 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 1 예시적인 장치의 개략적인 구조도이다.

도 12는 본 발명의 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 2 예시적인 장치의 개략적인 구조도이다.

도 13은 본 발명의 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 3 예시적인 장치의 개략적인 구조도

이다.

도 14는 본 발명의 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 4 예시적인 장치의 개략적인 구조도이다.

## *발명을 실시하기 위한 구체적인 내용*

[0014] 본 명세서에서는 예시적인 실시예가 첨부된 도면에 나타낸 예와 함께 상세히 설명된다. 첨부된 도면이 다음의 설명과 관련될 때, 상이한 첨부 도면들에서 동일한 도면 부호는 다른 언급이 없는 한 동일하거나 유사한 구성요소를 나타낸다. 다음의 예시적인 실시예에서 설명된 구현예는 본 출원에 부합하는 구현예의 단지 일부만을 나타내고 전부를 나타내는 것은 아니며, 첨부된 청구 범위에 상세하게 기술되는 본 출원의 여러 측면과 부합하는 방법 및 장치의 예이다.

[0015] 본 출원에 사용된 용어는 단지 특정 실시예를 설명하기 위한 목적으로 사용된 것으로서, 본 출원을 한정하려는 것이 아니다. 단수 형태 - 본 출원에서 사용된 "하나의 유형(a type)", "상기(said)" 및 "그(the)"는 다른 의미가 문맥상 명확하게 표현되지 않는 한, 복수 형태를 포함하는 것을 의도한다. 명세서에서 사용된 "및/또는"이라는 용어는 열거된 하나 이상의 관련 아이템의 임의의 또는 모든 가능한 조합을 나타내며 이를 포함한다.

[0016] "제 1", "제 2" 및 "제 3"과 같은 용어는 다양한 유형의 정보를 설명하기 위해 본 출원에서 사용될 수 있음을 이해해야 하며, 정보의 이러한 부분은 이들 용어에 한정되지 않는다. 이러한 용어는 단지 동일한 유형의 정보를 구별하기 위해 사용된다. 예를 들어, 본 출원의 범위를 벗어나지 않는 범위에서, 정보의 제 1 부분은 또한 정보의 제 2 부분으로 지칭될 수 있다. 유사하게, 정보의 제 2 부분은 정보의 제 1 부분으로서 지칭될 수 있다. 문맥에 따라, 본원에서 사용되는 문구 "만약에(if)"는 "~ 경우에", "~ 할 때" 또는 "~에 응답하여"로 해석될 수 있다.

[0017] 도 1은 제 1 단말기를 통해 애플리케이션 프로그램과 관련된 로그인 패스워드를 수정하는 프로세스를 도시하는 흐름도이다. 오리지널 패스워드가 수정되기 전에는, 애플리케이션 프로그램의 패스워드를 기록하는 기능을 통해 제 1 단말기와 제 2 단말기가 로그인할 때마다 로그인 패스워드를 입력할 필요가 없다. 사용자가 제 1 단말기를 통해 애플리케이션 프로그램의 오리지널 패스워드를 수정하면, 로그인 패스워드가 수정되었으므로 제 2 단말기가 애플리케이션 프로그램에 로그인하기 위해 기록된 오리지널 패스워드를 여전히 사용하는 경우 로그인이 실패한다. 도 1에 도시된 바와 같이, 이하의 단계가 포함된다.

[0018] 단계(101)에서, 제 1 단말기는 서버에 패스워드 수정 요청을 전송하고, 서버에 로그인 계정, 오리지널 패스워드 및 새로운 패스워드 등과 같은 패스워드 수정에 필요한 정보를 제공한다.

[0019] 단계(102)에서, 서버는 제공된 정보에 대해 확인을 수행하고 오리지널 패스워드가 정확한지를 검증한다. 단계(101)가 다시 수행되어 오리지널 패스워드가 틀린 경우, 사용자에게 제 1 단말기를 통해 패스워드 수정 요청을 서버에 재송신하도록 지시한다. 단계(103)는 오리지널 패스워드가 정확한 경우 수행된다.

[0020] 단계(103)에서, 서버는 새로운 패스워드를 백엔드 데이터베이스에 저장하고, 로그인 계정 및 새로운 패스워드에 기초하여 새로운 세션 식별자를 생성하며, 로그인 계정 및 오리지널 패스워드에 기초하여 생성된 오리지널 세션 식별자를 유효하지 않은 것으로 설정한다.

[0021] 단계(104)에서, 새로운 세션 식별자가 제 1 단말기에 리턴된다.

[0022] 단계(105)에서, 제 1 단말기는 서버가 리턴한 새로운 세션 식별자를 수신하여 제 1 단말기의 로컬 보안 공간에 저장하고 제 1 단말기의 애플리케이션 프로그램의 패스워드를 수정하는 프로세스를 완료한다.

[0023] 단계(106)에서, 서버가 패스워드를 수정한 후, 제 2 단말기는 오리지널 세션 식별자를 사용하여 서버에 로그인 요청을 개시하고, 제 2 단말기는 애플리케이션 프로그램이 제 2 단말기에서 처음 로그인된 후에 패스워드 기록 방식을 통해 제 2 단말기에 오리지널 세션 식별자를 기록한다.

[0024] 단계(107)에서, 서버는 제 2 단말기의 오리지널 세션 식별자에 대한 검증을 수행하고, 사용된 오리지널 세션 식별자가 유효하지 않은 것으로 결정하고, 제 2 단말기로 패스워드를 재입력하라는 요청을 리턴한다. 이러한 경우에 제 2 단말기는 다시 수정된 새로운 패스워드를 입력해야 한다. 사용자의 양손이 사용 중일 때, 제 2 단말기를 통해 새로운 패스워드를 입력하는 것은 소정의 보안 위험을 초래할 수 있다.

[0025] 따라서, 본 발명은 제 1 단말기에서 로그인 패스워드가 수정된 후에 새로운 패스워드를 입력할 필요 없이 제 2 단말기가 서버에 로그인할 수 있게 하는 다음과 같은 실시예를 사용함으로써, 사용자가 제 2 단말기를 통해 애

플리케이션 프로그램에 로그인할 필요가 있을 때 애플리케이션 프로그램을 제공하는 서버에 로그인하기 위해 새로운 패스워드가 입력되어야 하는 기존 기술의 문제점을 해결한다.

[0026] 다음의 실시예는 본 출원 내용을 보다 상세하게 설명하기 위해 제공된다.

[0027] 도 2는 본 발명의 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 1 예시적인 방법을 도시하는 흐름도이다. 방법이 적용되는 단말기는 도 1에 도시된 제 2 단말기이다. 도 2에 도시된 바와 같이, 다음의 단계가 포함된다.

[0028] 단계(201)에서, 애플리케이션 프로그램에 로그인하기 위한 제 1 요청이 서버에 개시되고, 제 1 요청은 로그인 계정 및 애플리케이션 프로그램의 오리지널 패스워드로부터 생성되는 제 1 세션 식별자를 포함하고, 오리지널 패스워드는 수정 전의 로그인 계정에 대응하는 로그인 패스워드이다.

[0029] 일부 실시예에서, 애플리케이션 프로그램이 처음으로 로그인되면, 단말기는 패스워드 기록 방식을 통해 제 1 세션 식별자에 대응하는 문자열(character string)을 서버에 송신할 수 있고, 제 1 세션 식별자를 제 1 단말기에 로컬로 기록할 수 있다. 애플리케이션 프로그램이 다시 로그인되면, 단말기는 기록된 제 1 세션 식별자를 사용하여 애플리케이션 프로그램에 로그인할 수 있으므로 사용자는 로그인 패스워드를 다시 입력하는 작업을 피할 수 있다. 일부 실시예에서, 제 1 세션 식별자를 생성하는 방법은 서버에 의해 결정될 수 있다. 제 1 세션 식별자는 md5 또는 sha1 등과 같은 해시 알고리즘을 사용하여 사용자의 로그인 계정 및 오리지널 패스워드에 기초하여 생성될 수 있다. 예를 들어, 로그인 계정 및 zhangxiao 및 zx098와 같은 오리지널 패스워드 및 20151026와 같은 로그인 타임 스탬프에 기초하여, 제 1 세션 식별자(3EC3ED381B9CF4359F4C1CB02CDF64)는 로그인 계정, 오리지널 패스워드 및 타임 스탬프에 대한 md5 알고리즘의 해시 계산을 수행함으로써 md5 알고리즘을 통해 얻어진다.

[0030] 단계(202)에서, 서버가 제 1 세션 식별자가 유효하지 않다고 결정한 경우, 단말기의 사용자에 대하여 유효성 검증을 수행하고, 취득한 검증 결과를 서버에 송신하여, 서버로 하여금 검증 결과에 대한 확인을 수행하게 한다.

[0031] 일부 실시예에서, 유효성 검증은 단말기 사용자의 생체 특성을 이용하여 수행될 수 있다. 예를 들어, 사용자의 지문, 홍채, 사람 얼굴 등과 같은 생체 특성을 이용하여 단말기에 대해 로컬로 유효성 검증을 사용자에 대해 수행할 수 있다. 일부 실시예에서, 단말기가 검증 결과를 서버에 보내기 전에, 검증 결과 및 검증 결과에 대응하는 난수가 서버의 대칭 비밀 키를 사용하여 암호화될 수 있다. 암호화된 검증 결과를 서버에 송신함으로써, 송신 처리 중에 검증 결과가 불법적으로 가로채기 되거나 조작되지 않도록 보증하고, 단말기와 서버간에 송신된 검증 결과의 보안을 보증한다.

[0032] 단계(203)에서, 검증 결과가 서버에 의해 승인되면, 서버로부터 제 2 세션 식별자가 수신되어 단말기에 저장되고, 제 2 세션 식별자는 로그인 계정 및 새로운 패스워드로부터 생성되며, 새로운 패스워드는 수정 후의 로그인 계정에 대응하는 로그인 패스워드이다.

[0033] 일부 실시예에서, 제 2 세션 식별자가 전송 프로세스 동안 불법적으로 가로채기되고 조작되는 것을 방지하기 위해, 제 2 세션 식별자는 단말기의 공개 키를 사용하여 암호화될 수 있다. 암호화된 제 2 세션 식별자를 수신한 후, 단말기는 암호화된 제 2 세션 식별자를 단말기의 개인 키를 사용하여 복호화하여 제 2 세션 식별자를 획득한다. 일부 실시예에서, 제 2 세션 식별자를 생성하는 방법은 제 1 세션 식별자를 생성하는 전술한 방법을 반영할 수 있다. 예를 들어, 사용자가 도 1에 도시된 실시예에서 제 1 단말기를 사용하여 로그인 패스워드를 zhangxiao로 변경한 후에, 제 1 세션 식별자에 대해 동일한 해시 계산을 사용하여 제 2 세션 식별자(2EF430338DF56A6FE40819CBF75982A9)가 획득된다.

[0034] 단계(201 - 203)를 통해, 사용자는 제 2 세션 식별자를 이용하여 애플리케이션 프로그램에 로그인할 수 있고, 단말기를 사용하는 사용자는 애플리케이션 프로그램에 로그인하기 위해 새로운 패스워드를 다시 입력할 필요가 없어 사용자의 애플리케이션 프로그램에 대한 로그인 경험이 크게 향상된다.

[0035] 도 3a는 본 발명의 일 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 2 예시적인 방법을 나타내는 흐름도이다. 도 3b는 도 3a의 단말기와 서버 간의 키를 동기화하는 방식을 나타내는 흐름도이다. 도 3a에 도시된 바와 같이, 다음의 단계가 포함된다.

[0036] 단계(301)에서, 검증 결과에 대응하는 검증 문자열의 난수가 해시 계산을 이용하여 생성된다.

[0037] 일부 실시예에서, 단말기 및 서버는 해시 알고리즘에 기초하여 동일한 난수를 생성할 수 있도록 동일한 해시 알고리즘에 대해 합의(agree on)할 수 있다. 일부 실시예에서, 검증 결과의 검증 문자열(verification

character string)은 예를 들어 "001" 및 "000"일 수 있는데, 여기서 "001"은 검증을 통과했음을 나타내고, "000"은 검증이 실패한 것을 나타낸다.

[0038] 단계(302)에서, 검증 문자열과 난수를 서버의 대칭 비밀 키를 사용하여 암호화하여 암호화된 검증 결과를 얻는다.

[0039] 일부 실시예에서, 단말기가 서버의 대칭 비밀 키를 획득하는 방식은 도 3b에 도시된 프로세스를 반영할 수 있다. 도 3b에 도시된 바와 같이, 서버와 단말기 간의 키 동기화는 다음의 단계를 포함한다.

[0040] 단계(311)에서, 비대칭 암호화 알고리즘에 기초하여 단말기의 공개 키 및 개인 키가 생성된다.

[0041] 일부 실시예에서, 비대칭 암호화 알고리즘은 예를 들어, RSA, 배낭 알고리즘(knapsack algorithm), Elgamal, D-H, 타원 곡선 암호화 알고리즘(ECC) 등일 수 있다. 본 실시예는 비대칭 암호화 알고리즘에 기초하여 공개 키 및 개인 키를 생성할 수 있다는 전제하에 비대칭 암호화 알고리즘에 대해 어떠한 제한도 가하지 않는다.

[0042] 단계(312)에서, 단말기의 공개 키를 서버에 송신한다.

[0043] 단계(313)에서, 단말기의 공개 키를 사용하여 암호화된 서버의 대칭 비밀 키가 수신된다.

[0044] 일부 실시예에서, 서버는 자신의 대칭 비밀 키를 생성하고, 단말기의 공개 키를 사용하여 대칭 비밀 키를 암호화하고, 암호화된 대칭 비밀 키를 단말기에 송신한다. 또한, 서버는 대칭 비밀 키를 사용하여 수정된 새로운 패스워드를 암호화 및 저장할 수 있어, 도 1에 도시된 제 1 단말기를 통해 사용자에 의해 수정된 새로운 패스워드가 누설되어 발생하는 위험을 회피할 수 있다.

[0045] 단계(314)에서, 암호화된 대칭 비밀 키가 단말기의 개인 키를 사용하여 복호화되어 서버의 대칭 비밀 키를 획득한다.

[0046] 단계(311) 내지 단계(314)를 통해 서버는 단말기의 공개 키를 얻을 수 있고, 단말기는 서버의 대칭 키를 얻을 수 있으므로 서버의 대칭 비밀 키와 단말기의 개인 키 사이의 키 동기화 과정을 실현할 수 있다.

[0047] 본 실시예에서는 대칭 암호화 기술을 통해 검증 결과의 비밀성을 보장할 수 있으며, 부정한 사용자에 의한 검증 결과의 변조를 방지할 수 있다. 난수를 사용하는 것은 암호화된 데이터가 재사용되는 것을 방지할 수 있다.

[0048] 도 4는 본 발명의 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 3 예시적인 방법을 나타내는 흐름도이다. 본 실시예는 설명을 위해 사용자가 로컬에서 유효성 검증을 어떻게 수행하는지에 대한 일례를 사용한다. 도 4에 도시된 바와 같이, 다음의 단계가 포함된다.

[0049] 단계(401)에서, 단말기 사용자의 생체 특성을 생체 센서를 통해 애플리케이션 프로그램의 로그인 인터페이스에서 수집한다.

[0050] 일부 실시예에서, 생체 특성은 사용자의 지문, 홍채 또는 사람의 얼굴과 같은 생체 특성일 수 있다. 생체 특성이 지문이면, 애플리케이션 프로그램의 현재 로그인 인터페이스는 사용자의 지문을 획득할 수 있고, 이에 따라 사용자가 애플리케이션 프로그램에 의해 현재 디스플레이되는 로그인 인터페이스를 벗어나는 것을 방지한다. 이를 통해 로그인 인터페이스에서 직접 지문 인식 동작을 수행할 수 있으며 사용자에 대한 유효성 검증을 로컬로 수행하는 절차를 간소화할 수 있다.

[0051] 단계(402)에서, 생체 특성에 대해 검증을 수행하여 검증이 통과되었는지를 결정한다. 생체 특성이 검증을 통과하면, 단계(403)가 수행된다. 생체 특성이 검증을 통과하지 못하면, 단계(404)가 수행된다.

[0052] 단계(403)에서, 생체 특성이 검증을 통과하면, 단말기의 사용자는 부정한 사용자인 것으로 확인된다.

[0053] 일부 실시예에서, 생체 특성의 검증은 현존 기술의 관련 설명을 참조할 수 있으며, 본 실시예에서는 상세한 설명이 제공되지 않는다.

[0054] 단계(404)에서, 생체 특성이 검증을 통과하지 못하면, 애플리케이션 프로그램의 로그인 인터페이스는 애플리케이션 프로그램에 로그인하기 위한 로그인 계정 및 로그인 패스워드를 사용하라는 프롬프트를 표시한다.

[0055] 본 실시예에서, 동일한 애플리케이션 프로그램이 다수의 단말기 중 하나를 통해 로그인 패스워드를 재설정하고 다른 단말기를 통해 애플리케이션 프로그램에 로그인하는 다수의 사용자를 갖는 경우, 본 실시예는 로컬 ID 검증 메커니즘을 통해 서버의 작업 부하를 최적화할 수 있고, 서버가 공격자로부터 DDoS 공격을 겪지 않도록 한다.

[0056] 도 5는 본 발명의 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 4 예시적인 방법을 나타내는 흐름도이다. 단말기가 전술한 실시예를 통해 제 2 세션 식별자를 획득하고 저장한 후에, 서버는 사용자 로그인의 보안을 보장하기 위해 제 2 세션 식별자에 대한 유효 기간을 설정할 수 있다. 따라서 사용자가 애플리케이션 프로그램에 로그인하는 데 할당된 시간은 제 2 세션 식별자의 유효 기간을 통해 제한된다. 도 5에 도시된 바와 같이, 다음의 단계가 포함된다.

[0057] 단계(501)에서, 제 2 세션 식별자가 유효 기간 내에 있는지를 결정하고, 제 2 세션 식별자가 유효 기간 내에 있으면 단계(502)가 수행되고, 제 2 세션 식별자가 유효 기간을 벗어나면 단계(503)가 수행된다.

[0058] 단계(502)에서, 제 2 세션 식별자가 유효 기간 내에 있는 경우, 애플리케이션 프로그램은 제 2 세션 식별자를 사용하여 로그인된다.

[0059] 단계(503)에서, 제 2 세션 식별자가 유효 기간을 벗어난 경우, 사용자는 로그인 계정 및 로그인 계정의 유효한 패스워드를 사용하여 애플리케이션 프로그램에 로그인하라는 프롬프트가 표시된다.

[0060] 일부 실시예에서, 유효 기간은 서버로부터 획득될 수 있다. 예를 들어, 사용자는 제 1 단말기를 통해 새로운 패스워드를 다시 설정한다. 서버가 새로운 패스워드에서 제 2 세션 식별자를 생성하는 시간은 2015 년 10 월 10 일 12시 12 분이며 유효 기간은 1 개월이다. 단말기는 서버로부터 제 2 세션 식별자의 생성 시간 및 유효 기간을 획득할 수 있다. 이와 같이, 사용자가 제 2 세션 식별자에 기초하여 제 2 세션 식별자를 사용하여 애플리케이션 프로그램에 직접 로그인할 수 있는지 여부에 대한 결정이 이루어질 수 있다. 제 2 세션 식별자가 1 개월을 경과한 경우, 애플리케이션 프로그램의 로그인 인터페이스는 애플리케이션 프로그램에 로그인하는 데 로그인 계정 및 로그인 계정의 유효한 로그인 패스워드가 필요하다는 것을 사용자에게 프롬프트할 수 있다.

[0061] 본 실시예에서는 사용자의 로그인 활동을 제 2 세션 식별자의 유효 기간을 통해 제한함으로써 제 2 세션 식별자를 획득한 후 부정 사용자가 애플리케이션 프로그램에 불법적으로 로그인하는 것을 방지하고 애플리케이션 프로그램의 사용자의 로그인에 대한 보안을 보장한다.

[0062] 도 6은 본 발명의 다른 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 1 예시적인 방법(600)을 도시하는 흐름도이다. 도 1에 도시된 실시예와 일치하도록, 방법을 서버에 적용한 예가 설명을 위해 사용된다. 도 6에 도시된 바와 같이, 이하의 단계가 포함된다.

[0063] 단계(601)에서, 애플리케이션 프로그램에 로그인하기 위한 제 1 요청이 단말기에 의해 개시될 때, 제 1 요청에 포함된 제 1 세션 식별자에 대한 검증이 수행되고, 제 1 세션 식별자는 로그인 계정 및 애플리케이션 프로그램과 연관된 오리지널 패스워드로부터 생성되며, 오리지널 패스워드는 수정 전의 로그인 계정에 대응하는 로그인 패스워드이다.

[0064] 일부 실시예에서, 제 1 세션 식별자는 서버에 저장된 유효한 세션 식별자와 비교될 수 있다. 제 1 세션 식별자가 저장된 유효한 세션 식별자와 동일한 경우, 제 1 세션 식별자는 유효한 것으로 결정된다. 제 1 세션 식별자가 저장된 유효한 세션 식별자와 동일하지 않으면, 제 1 세션 식별자는 유효하지 않은 것으로 결정된다.

[0065] 단계(602)에서, 제 1 세션 식별자가 유효하지 않은 것으로 검증된 경우, 단말기의 사용자에 대한 유효성 검증을 수행하도록 단말기에 지시한다.

[0066] 일부 실시예에서, 단말기 사용자의 유효성 검증을 수행하는 방법은 전술한 실시예의 관련 설명이 반영될 수 있으며, 본 명세서에서 반복적으로 설명하지 않는다.

[0067] 단계(603)에서, 사용자의 유효성 검증의 검증 결과를 단말기로부터 수신한다.

[0068] 일부 실시예에서, 단말기가 검증 결과를 서버로 송신하기 전에, 검증 결과 및 검증 결과에 대응하는 난수가 서버의 대칭 비밀 키를 이용하여 암호화되면, 암호화 검증 결과는 서버로 송신된다. 이 경우, 서버는 추가로 대칭 비밀 키를 사용하여 암호화된 검증 결과를 복호화할 필요가 있다.

[0069] 단계(604)에서, 검증 결과가 서버에 의해 검증되고 승인되면, 제 2 세션 식별자가 단말기로 전송되며, 제 2 세션 식별자는 로그인 계정 및 새로운 패스워드로부터 생성되고, 새로운 패스워드는 수정 후의 로그인 계정에 대응한다.

[0070] 단계(601) 내지 단계(604)를 통해 정당한 사용자가 서버에 로그인하도록 허용될 수 있다. 또한, 정당한 사용자는 제 2 세션 식별자를 획득할 수 있다. 이는 정당한 사용자가 단말기를 사용할 때 애플리케이션 프로그램에 로그인하기 위해 새로운 패스워드를 다시 입력하는 것을 방지하여, 애플리케이션 프로그램의 사용자 로그인 경

험을 크게 향상시킨다. 다수의 사용자가 애플리케이션 프로그램의 로그인 패스워드를 재설정해야 하는 경우, 단말기 측에서 유효성 검증을 수행함으로써, 사용자에 대한 유효성 검증과 관련된 서버의 작업 부하를 줄일 수 있으므로 서버의 자원 낭비를 피할 수 있다.

[0071] 도 7은 본 발명의 다른 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 2 예시적인 방법을 나타내는 흐름도이다. 도 7에 도시된 바와 같이, 이하의 동작이 포함된다.

[0072] 단계(701)에서, 서버의 대칭 비밀 키를 이용하여 단말기에 의해 검증 결과가 암호화된 경우, 암호화된 검증 결과는 서버의 대칭 비밀 키를 이용하여 복호화되어 검증 결과에 대응하는 검증 문자열과 난수를 획득한다.

[0073] 단계(702)에서, 검증 문자열과 난수에 대한 검증을 수행하고, 검증 문자열과 난수가 검증을 통과하면 제 2 세션 식별자를 단말기로 송신한다.

[0074] 일부 실시예에서, 단말기 및 서버는 해시 알고리즘에 기초하여 동일한 난수를 생성할 수 있도록 하기 위해 해시 알고리즘에 대해 합의할 수 있고, 이로써 난수를 사용하여 이중 검증을 수행할 수 있다. 일부 실시예에서, 검증 결과의 검증 문자열은 예를 들어 "001" 및 "000"일 수 있으며, "001"은 검증을 통과한 것을 나타내고, "000"은 검증이 실패한 것을 나타낸다. 일부 실시예에서, 제 2 세션 식별자는 단말기의 공개 키를 사용하여 암호화될 수 있으며, 이로써 송신 프로세스 동안 제 2 세션 식별자의 보안을 보장한다.

[0075] 단말기가 서버의 대칭 키를 획득하는 방식 및 서버가 단말기의 공개 키를 획득하는 방식에 관한 세부 사항은 도 3b에 대해 전술한 설명을 반영할 수 있으며, 본 명세서에서 반복적으로 설명하지 않는다.

[0076] 본 실시예에서는 대칭 암호화 기술을 통해 검증 결과의 비밀성을 보장할 수 있으며, 부정한 사용자에 의한 검증 결과의 변조를 방지할 수 있다. 난수를 사용하는 것은 암호화된 데이터가 재사용되는 것을 방지할 수 있다.

[0077] 도 8은 본 발명의 다른 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 3 예시적인 방법을 나타내는 흐름도이다. 서버가 전술한 실시예를 사용하여 제 2 세션 식별자를 생성한 후에, 서버는 사용자 로그인의 보안을 보증하기 위해 제 2 세션 식별자에 대한 유효 기간을 설정할 수 있다. 따라서, 사용자가 애플리케이션 프로그램에 로그인하는 데 할당된 시간은 제 2 세션 식별자의 유효 기간으로 제한된다. 도 8에 도시된 바와 같이, 이하의 단계가 포함된다.

[0078] 단계(801)에서, 제 2 세션 식별자가 유효 기간 내에 있는지 여부가 결정되고, 제 2 세션 식별자가 유효 기간 내에 있는 경우 단계(802)가 수행되고, 제 2 세션 식별자가 유효 기간을 벗어난 경우에는 단계(803)가 수행된다.

[0079] 단계(802)에서, 제 2 세션 식별자가 유효 기간 내에 있으면, 사용자는 제 2 세션 식별자를 사용하여 애플리케이션 프로그램에 로그인하도록 허용된다.

[0080] 단계(803)에서, 제 2 세션 식별자가 유효 기간을 벗어난 경우 사용자는 제 2 세션 식별자를 사용하여 애플리케이션 프로그램에 로그인하는 것이 허용되지 않는다.

[0081] 일부 실시예에서, 서버는 사용자에 의해 설정된 할당 시간에 기초하여 제 2 세션 식별자의 유효 기간을 결정할 수 있다. 예를 들어, 사용자는 제 1 단말기를 통해 새로운 패스워드를 다시 설정하고 유효 기간은 1 개월이다. 서버가 새로운 패스워드에서 제 2 세션 식별자를 생성하는 시간은 2015 년 10 월 10 일, 12 시 12 분이며 서버는 제 2 세션 식별자의 만료 시간이 2015 년 11 월 10 일, 12 시 12 분이라고 결정할 수 있다. 사용자는 이러한 할당된 시간 내에 제 2 세션 식별자를 사용하여 애플리케이션 프로그램에 직접 로그인할 수 있다. 할당된 시간이 지난 후에는, 사용자가 제 2 세션 식별자를 사용하여 애플리케이션 프로그램에 로그인하는 것이 허용되지 않는다.

[0082] 본 실시예에서, 사용자의 로그인 활동을 제 2 세션 식별자의 유효 기간을 통해 제한함으로써 제 2 세션 식별자를 획득한 후 부정 사용자가 애플리케이션 프로그램에 불법적으로 로그인하는 것을 방지하고, 애플리케이션 프로그램에 대한 사용자의 로그인에 대한 보안을 보장한다.

[0083] 예시적인 시나리오로서, 사용자가 휴대 전화를 이용하여 애플리케이션 프로그램의 로그인 패스워드를 리셋한 후에 차량 탑재 단말기를 통해 애플리케이션 프로그램에 로그인하면, 차량 탑재 단말기는 사용자가 로그인 패스워드를 재설정하기 전의 유효하지 않은 제 1 세션 식별자를 기록한다. 서버가 제 1 세션 식별자를 유효하지 않은 것으로 설정했기 때문에, 사용자는 차량 탑재 단말기를 통해 애플리케이션 프로그램에 로그인할 수 없다. 사용자가 운전 중이기 때문에 사용자는 새로운 비밀번호를 입력하는 것이 용이하지 않다. 사용자의 생체 인증을 수

행하기 위한 전술한 실시예를 이용하여, 사용자가 차량 탑재 단말기의 정당한 사용자라고 결정되면, 차량 탑재 단말기를 통해 서버로부터 제 2 세션 식별자를 획득할 수 있다. 따라서, 애플리케이션 프로그램은 제 2 세션 식별자를 이용하여 로그인되므로 사용자가 운전할 중일 때의 위험을 줄일 수 있다.

[0084] 세션 식별자 동기화를 실현하는 전술한 방법에 대해, 본 발명은 도 9에 도시된 바와 같은 본 출원의 예시적인 실시예에 따른 단말기의 개략적인 구조도를 더 개시한다. 도 9를 참조하면, 단말기는 하드웨어 레벨의 프로세서, 내부 버스, 네트워크 인터페이스, 메모리 및 비 휘발성 저장 장치를 포함한다. 또한, 다른 서비스에 의해 요구되는 하드웨어가 포함될 수 있다는 점은 명백하다. 프로세서는 대응하는 컴퓨터 명령어를 실행하기 위해 비 휘발성 저장 장치로부터 메모리로 판독하여 로직 레벨에서 세션 식별자 동기화를 실현하기 위한 장치를 형성한다. 소프트웨어 구현예를 제외하고, 본 출원이 로직 컴포넌트 또는 소프트웨어와 하드웨어의 조합 등과 같은 다른 구현예를 배제하지 않는다는 점은 명백하다. 달리 설명하면, 다음의 처리 절차의 실행 엔티티(들)는 여러 로직 유닛에 제한되지 않으며, 하드웨어나 로직 컴포넌트일 수도 있다.

[0085] 세션 식별자 동기화를 실현하는 전술한 방법에 대해, 본 발명은 도 10에 도시된 본 출원의 예시적인 실시예에 따른 서버의 개략적인 구조도를 더 개시한다. 도 10을 참조하면, 서버는 프로세서, 내부 버스, 네트워크 인터페이스, 메모리 및 비 휘발성 메모리 저장 장치를 하드웨어 레벨에서 유지한다. 다른 서비스에 의해 요구되는 하드웨어가 포함될 수도 있다는 점이 명백하다. 프로세서는 실행을 위해 비 휘발성 저장 장치(1010)로부터 대응하는 컴퓨터 명령어를 메모리로 판독하여, 로직 레벨에서 세션 식별자 동기화를 실현하기 위한 장치를 형성한다. 소프트웨어 구현예를 제외하고, 본 출원은 로직 컴포넌트 또는 소프트웨어와 하드웨어의 조합 등과 같은 다른 구현예를 배제하지 않는다는 점은 명백하다. 달리 설명하면, 후속 처리 절차의 실행 엔티티(들)는 여러 로직 유닛으로 제한되지 않으며, 하드웨어 또는 로직 컴포넌트일 수도 있다.

[0086] 도 11은 본 발명의 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 1 예시적인 장치에 대한 개략적인 구조도를 도시한다. 도 11에 도시된 바와 같이, 세션 식별자 동기화를 실현하기 위한 장치는 제 1 송신 모듈(111), 제 1 검증 모듈(112) 및 제 1 수신 모듈(113)을 포함할 수 있다.

[0087] 제 1 송신 모듈(111)은 애플리케이션 프로그램에 로그인하기 위한 제 1 요청을 개시하는 데 사용되고, 제 1 요청은 제 1 세션 식별자를 포함하며, 제 1 세션 식별자는 애플리케이션 프로그램의 로그인 계정 및 오리지널 패스워드로부터 생성되고, 오리지널 패스워드는 수정 전의 로그인 계정에 대응하는 로그인 패스워드이다.

[0088] 제 1 검증 모듈(112)은 단말기의 사용자에 대한 유효성 검증을 수행하고, 획득된 검증 결과를 서버에 송신하여 제 1 송신 모듈(111)에 의해 송신된 제 1 세션 식별자가 서버에 의해 유효하지 않은 것으로 결정되면, 서버로 하여금 검증 결과에 대한 확인을 수행하게 하는 데 사용된다.

[0089] 제 1 수신 모듈(113)은 서버로부터 제 2 세션 식별자를 수신하고, 제 1 검증 모듈(112)에 의해 획득된 검증 결과가 서버에 의해 검증되고 승인된 경우 제 2 세션 식별자를 단말기에 저장하는 데 사용되며, 제 2 세션 식별자는 로그인 계정과 새로운 패스워드로부터 생성되고, 새로운 패스워드는 수정 후의 로그인 계정에 대응하는 로그인 패스워드이다.

[0090] 도 12는 본 발명의 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 2 예시적인 장치의 개략적인 구조도를 도시한다. 일 실시예에서, 도 11에 도시된 실시예에 기초하여, 도 12에 도시된 장치는 제 1 검증 모듈(112)에 의해 획득된 검증 결과에 대응하는 검증 문자열의 난수를 생성하는 제 1 생성 모듈(114)과, 제 1 검증 결과에 의해 획득된 검증 문자열과 제 1 생성 모듈(114)에 의해 생성된 난수를 서버의 대칭 비밀 키를 사용하여 암호화하여 암호화된 검증 결과를 획득하는 데 사용되는 제 1 암호화 모듈(1204)을 포함한다.

[0091] 일 실시예에서, 장치는 비대칭 암호화 알고리즘을 사용하여 단말기의 공개 키 및 개인 키를 생성하는 데 사용되는 제 2 생성 모듈(116)과, 제 2 생성 모듈(116)에 의해 생성된 단말기의 공개 키를 서버에 송신하기 데 사용되는 제 2 송신 모듈(117)과, 제 2 송신 모듈(117)에 의해 송신된 단말기의 공개 키를 사용하여 암호화된 서버의 대칭 비밀 키를 서버로부터 수신하는 데 사용되는 제 2 수신 모듈(118)과, 제 2 생성 모듈(118)에 의해 생성된 단말기의 개인 키를 이용하여 암호화된 대칭 비밀 키를 복호화하여 서버의 대칭 비밀 키를 획득하는 데 사용되는 제 1 복호화 모듈(119)을 포함한다.

[0092] 일부 실시예에서, 제 1 검증 모듈(112)은 생체 센서를 통해 애플리케이션 프로그램의 로그인 인터페이스 상에 단말기의 사용자의 생체 특성을 수집하는 데 사용되는 특성 수집 유닛(1121)과, 특성 수집 유닛(1121)에 의해 수집된 생체 특성에 대한 검증을 수행하는 데 사용되는 검증 유닛(1122)과, 생체 특성이 검증 유닛(1122)의 검증을 통과한 경우, 단말기의 사용자가 정당한 사용자인지를 결정하는 데 사용되는 제 1 결정 유닛과, 로그인 계

정 및 로그인 패스워드를 이용하여 애플리케이션 프로그램에 로그인하기 위한 애플리케이션 프로그램의 로그인 인터페이스 상에 프롬프트를 제공하는 데 사용되는 프롬프트 유닛(prompting unit)(1123)을 포함할 수 있다.

[0093] 일부 실시예에서, 장치는 제 1 수신 모듈(113)에 의해 수신된 제 2 세션 식별자가 유효 기간 내인지를 결정하는 데 사용되는 제 1 결정 모듈(120)과, 제 1 결정 모듈(120)이 제 2 세션 식별자가 유효 기간 내에 있다고 결정하면 애플리케이션 프로그램에 로그인하기 위해 제 2 세션 식별자가 사용되는 것으로 결정하는 데 사용되는 제 2 결정 모듈(121)과, 제 1 결정 모듈(120)이 제 2 세션 식별자가 유효 기간을 경과한 것으로 결정하면, 로그인 계정 및 로그인 계정의 유효한 로그인 패스워드를 사용하여 애플리케이션 프로그램에 로그인하도록 사용자에게 프롬프트하는 데 사용되는 프롬프트 모듈(122)을 포함한다.

[0094] 도 13은 본 발명의 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 3 예시적인 장치의 개략적인 구조도를 도시한다. 도 13에 도시된 바와 같이, 세션 식별자 동기화를 실현하기 위한 장치는 제 2 검증 모듈(131), 명령 모듈(132), 제 3 수신 모듈(133) 및 제 3 송신 모듈(134)을 포함할 수 있다.

[0095] 제 2 검증 모듈(131)은 제 1 요청이 단말기에서 시작될 때 애플리케이션 프로그램에 로그인하기 위한 제 1 요청에 포함된 제 1 세션 식별자의 유효성을 검증하는 데 사용되며, 제 1 세션 식별자는 애플리케이션 프로그램의 로그인 계정 및 오리지널 패스워드로부터 생성되고, 오리지널 패스워드는 수정 전의 로그인 계정에 대응하는 로그인 패스워드이다.

[0096] 명령 모듈(132)은, 제 1 세션 식별자가 제 2 검증 모듈(131)에 의해 유효하지 않다고 검증된 경우, 단말기의 사용자에 대한 유효성 검증을 수행하도록 단말기에 지시하는 데 사용된다.

[0097] 제 3 수신 모듈(133)은 명령 모듈(132)의 지시에 따라 단말기가 수행하는 사용자의 유효성 검증의 검증 결과를 수신하는 데 사용된다.

[0098] 제 3 송신 모듈(134)은 제 3 수신 모듈(134)에 의해 수신된 검증 결과가 서버에 의해 확인되고 승인되는 경우 제 2 세션 식별자를 단말기에 송신하는 데 사용되며, 제 2 세션 식별자는 로그인 계정 및 새로운 패스워드로부터 생성되고, 새로운 패스워드는 수정 후의 로그인 계정에 대응하는 로그인 패스워드이다.

[0099] 도 14는 본 발명의 실시예에 따라 세션 식별자 동기화를 실현하기 위한 제 4 예시적인 장치의 개략적인 구조도를 도시한다. 일 실시예에서, 도 13에 도시된 실시예에 기초하여, 도 14에 도시된 장치는, 제 3 수신 모듈(133)에 의해 획득된 검증 결과가 서버의 대칭 비밀 키를 이용하여 단말기에 의해 암호화된 경우 난수 및 검증 결과에 대응하는 검증 문자열을 획득하기 위해 서버의 대칭 비밀 키를 사용하여 암호화된 검증 결과를 복호화하는 데 사용되는 제 2 복호화 모듈(135); 및 제 2 복호화 모듈(135)에 의한 복호화 후에 얻어진 검증 문자열과 난수에 대한 검증을 행하기 위한 제 3 검증 모듈(136)을 더 포함할 수 있다. 검증 문자열과 난수가 검증을 통과하면, 제 3 송신 모듈(134)은 제 2 세션 식별자를 단말기에 송신하는 단계를 수행한다.

[0100] 일부 실시예에서, 장치는 대칭 암호화 알고리즘에 기초하여 서버의 대칭 비밀 키를 생성하여 제 2 복호화 모듈(135)이 서버의 대칭 비밀 키를 사용하여 암호화된 검증 결과를 복호화할 수 있게 하는 제 3 생성 모듈(137); 단말기의 공개 키를 사용하여 제 3 생성 모듈(137)이 생성한 대칭 비밀 키를 암호화하는 제 2 암호화 모듈(138); 및 제 2 암호화 모듈(138)에 의해 암호화된 대칭 비밀 키를 단말기로 송신하여 단말기가 공개 키에 대응하는 개인 키를 사용하여 암호화된 대칭 비밀 키를 복호화함으로써 서버의 대칭 키를 획득하게 하는 제 4 송신 모듈(138)을 더 포함할 수 있다.

[0101] 일부 실시예에서, 장치는 제 3 송신 모듈(134)에 의해 송신된 제 2 세션 식별자가 유효 기간 내에 있는지 여부를 결정하기 위해 사용되는 제 3 결정 모듈(140); 제 3 결정 모듈(140)이 제 2 세션 식별자가 유효 기간 내에 있다고 결정하면 사용자로 하여금 제 2 세션 식별자를 이용하여 애플리케이션 프로그램에 로그인하게 하는 데 사용되는 제 1 제어 모듈(141); 제 2 세션 식별자가 유효 기간을 벗어난 것으로 제 3 결정 모듈(140)이 결정하면 사용자가 제 2 세션 식별자를 이용하여 애플리케이션 프로그램에 로그인하는 것을 금지하는 제 2 제어 모듈(142)을 포함한다.

[0102] 전술한 실시예에서 알 수 있듯이, 사용자가 제 1 단말기에서 애플리케이션 프로그램의 로그인 패스워드를 수정한 후에 제 2 단말기를 통해 애플리케이션 프로그램에 로그인하는 경우, 이러한 동일한 사용자는 제 1 단말기와 상이한 제 2 단말기에서 애플리케이션 프로그램에 로그인하는 것이 허용되고, 이에 따라 애플리케이션 프로그램에 로그인하기 위해 수정된 로그인 패스워드를 입력하는 방식을 피할 수 있다. 따라서, 사용자 경험이 향상되고, 로그인의 보안이 보장된다.

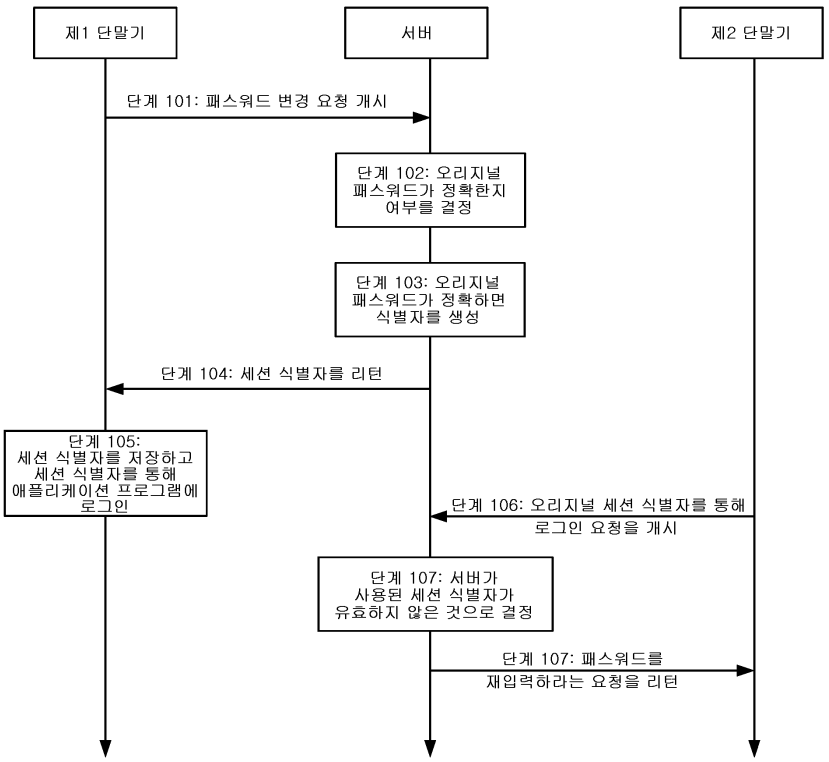
[0103] 당업자는 명세서를 고려하고 본 명세서에 개시된 발명을 실시한 후에 본 출원의 다른 구현예를 쉽게 생각해 낼 수 있다. 본 발명은 임의의 수정, 사용 또는 적응적 수정을 포함하고자 한다. 이러한 변경, 사용 또는 적응적 수정은 본 출원의 공통 원리를 따르며, 본 출원에 기술되어 있거나 기술되지 않은 현재의 기술 분야에서의 잘 알려진 지식 또는 공통의 기술적 수치(technical measure)를 포함한다. 명세서 및 실시예는 단지 예시적인 것이다. 본 출원의 실제 범주 및 사상은 첨부된 청구 범위에 의해 표시된다.

[0104] 또한, "포함하는", "함유하는" 또는 임의의 다른 변형어는 비 배타적인 포함 사항을 포괄하려는 것이다. 따라서 일련의 구성 요소를 포함하는 프로세스, 방법, 제품 또는 장치는 이들 구성 요소를 포함할 뿐만 아니라 명시적으로 나열되지 않은 다른 구성 요소를 포함하거나, 프로세스, 방법, 제품 또는 장치에 내재된 구성 요소를 더 포함할 수 있다. 추가 제한 없이, "... 을 포함하는"이라는 문구에 의해 정의된 구성 요소는 이러한 구성 요소를 포함하는 프로세스, 방법, 제품 또는 디바이스에서 동일한 구성 요소를 더 추가하는 것을 배제하지 않는다.

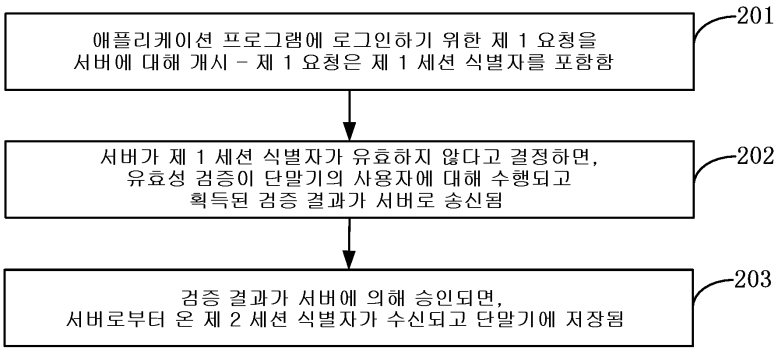
[0105] 전술한 설명은 단지 본 발명의 바람직한 실시예를 나타내고, 본 출원에 대한 제한으로서 사용되지는 않는다. 본 출원의 사상 및 원리에 대해 이루어진 임의의 수정, 등가의 치환, 개선 등은 모두 본 출원의 보호 범위에 포함될 것이다.

## 도면

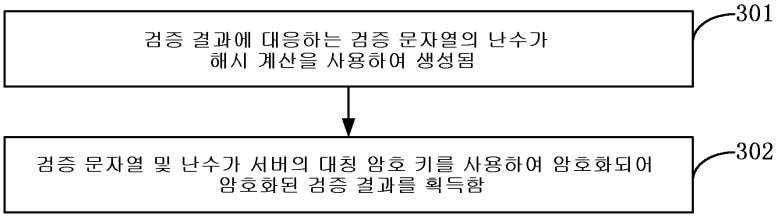
### 도면1



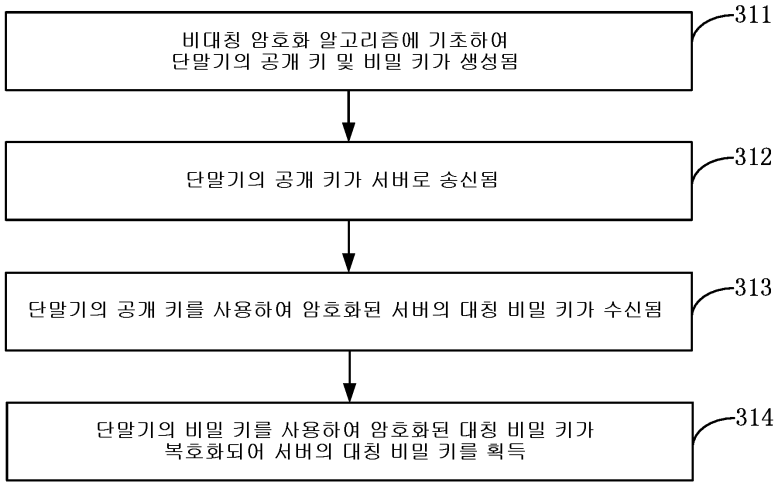
도면2



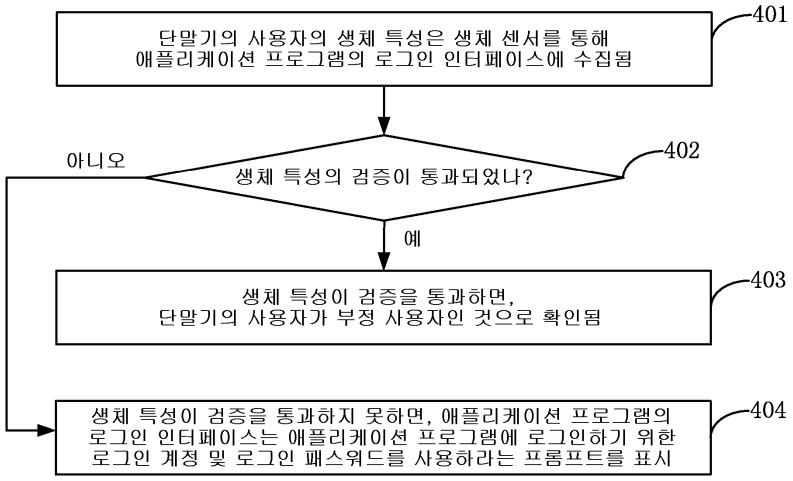

도면3a



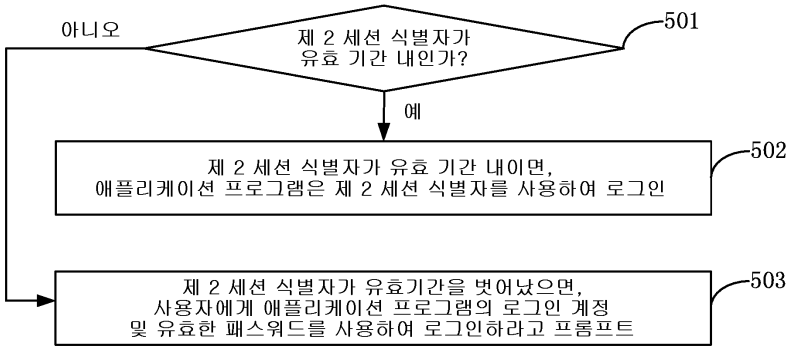

도면3b



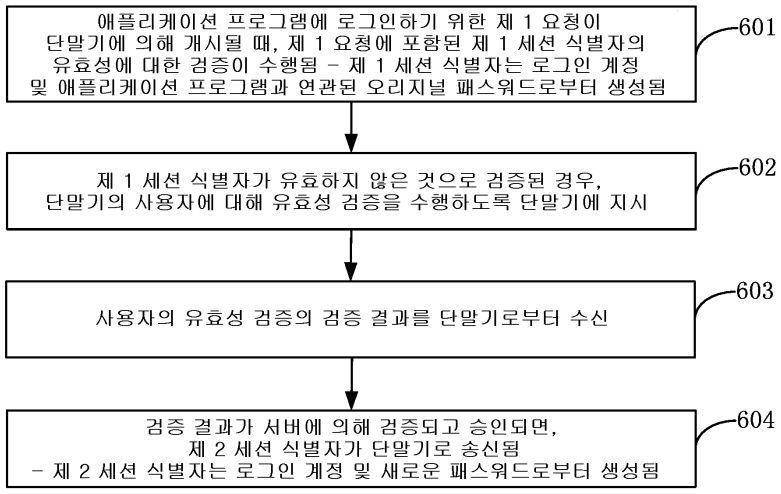
도면4


단말기의 사용자의 생체 특성은 생체 센서를 통해
애플리케이션 프로그램의 로그인 인터페이스에 수집됨
401
생체 특성의 검증이 통과되었나?
402
아니오
예
생체 특성이 검증을 통과하면,
단말기의 사용자가 부정 사용자인 것으로 확인됨
403
생체 특성이 검증을 통과하지 못하면, 애플리케이션 프로그램의
로그인 인터페이스는 애플리케이션 프로그램에 로그인하기 위한
로그인 계정 및 로그인 패스워드를 사용하라는 프롬프트를 표시
404

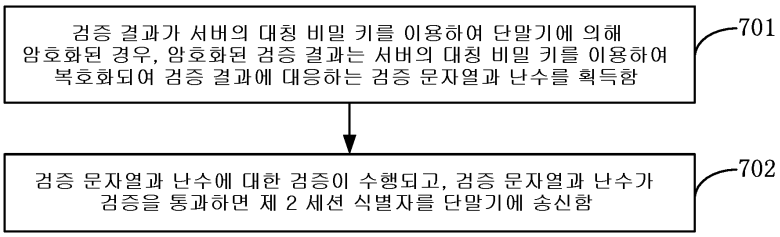
도면5


제 2 세션 식별자가
유효 기간 내인가?
501
아니오
예
제 2 세션 식별자가 유효 기간 내이면,
애플리케이션 프로그램은 제 2 세션 식별자를 사용하여 로그인
502
제 2 세션 식별자가 유효기간을 벗어났으면,
사용자에게 애플리케이션 프로그램의 로그인 계정
및 유효한 패스워드를 사용하여 로그인하라고 프롬프트
503

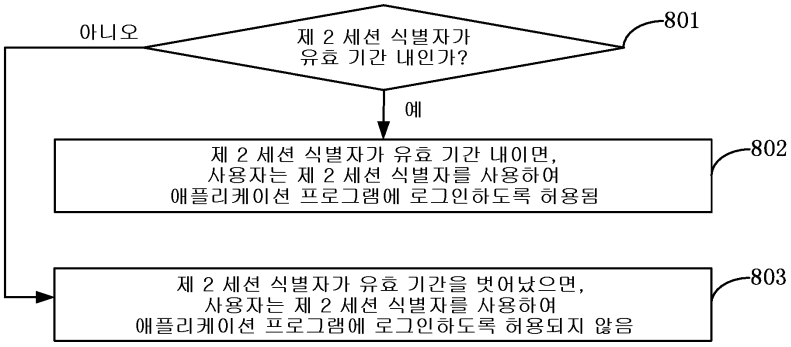
도면6


애플리케이션 프로그램에 로그인하기 위한 제 1 요청이
단말기에 의해 개시될 때, 제 1 요청에 포함된 제 1 세션 식별자의
유효성에 대한 검증이 수행됨 - 제 1 세션 식별자는 로그인 계정
및 애플리케이션 프로그램과 연관된 오리지널 패스워드로부터 생성됨
601
제 1 세션 식별자가 유효하지 않은 것으로 검증된 경우,
단말기의 사용자에 대해 유효성 검증을 수행하도록 단말기에 지시
602
사용자의 유효성 검증의 검증 결과를 단말기로부터 수신
603
검증 결과가 서버에 의해 검증되고 승인되면,
제 2 세션 식별자가 단말기로 송신됨
- 제 2 세션 식별자는 로그인 계정 및 새로운 패스워드로부터 생성됨
604

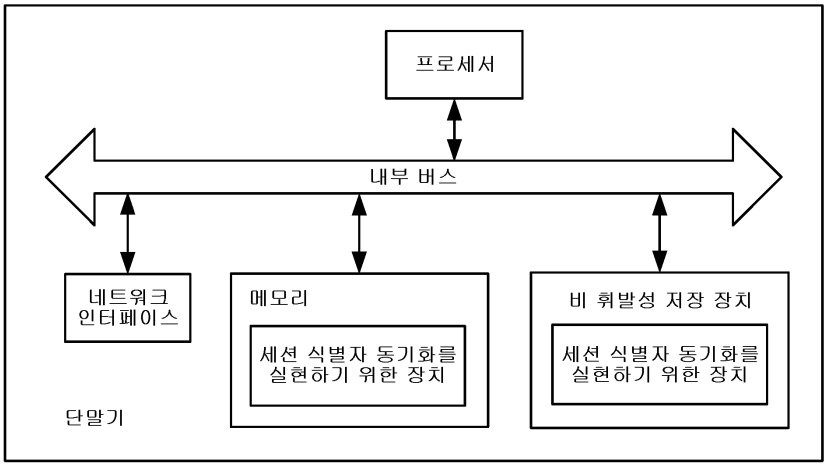
도면7


검증 결과가 서버의 대칭 비밀 키를 이용하여 단말기에 의해
암호화된 경우, 암호화된 검증 결과는 서버의 대칭 비밀 키를 이용하여
복호화되어 검증 결과에 대응하는 검증 문자열과 난수를 획득함
701
검증 문자열과 난수에 대한 검증이 수행되고, 검증 문자열과 난수가
검증을 통과하면 제 2 세션 식별자를 단말기에 송신함
702

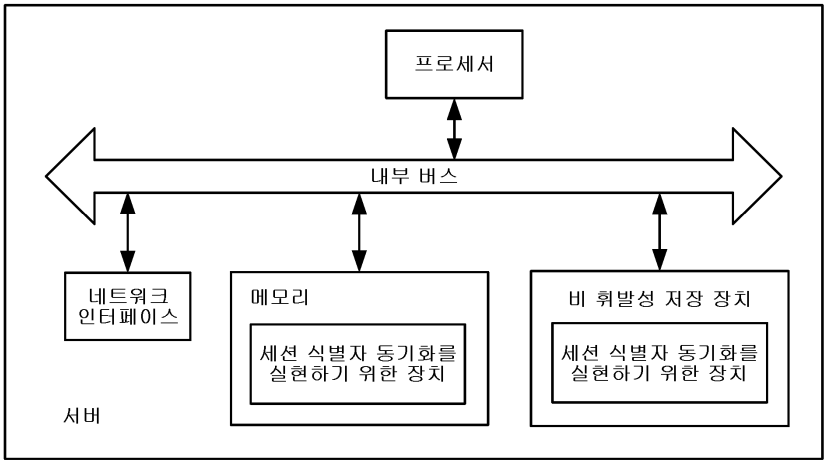
도면8


아니오
제 2 세션 식별자가
유효 기간 내인가?
801
예
제 2 세션 식별자가 유효 기간 내이면,
사용자는 제 2 세션 식별자를 사용하여
애플리케이션 프로그램에 로그인하도록 허용됨
802
제 2 세션 식별자가 유효 기간을 벗어났으면,
사용자는 제 2 세션 식별자를 사용하여
애플리케이션 프로그램에 로그인하도록 허용되지 않음
803

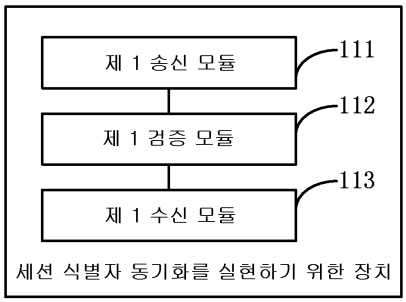
도면9


프로세서
내부 버스
네트워크
인터페이스
메모리
세션 식별자 동기화를
실현하기 위한 장치
비 휘발성 저장 장치
세션 식별자 동기화를
실현하기 위한 장치
단말기

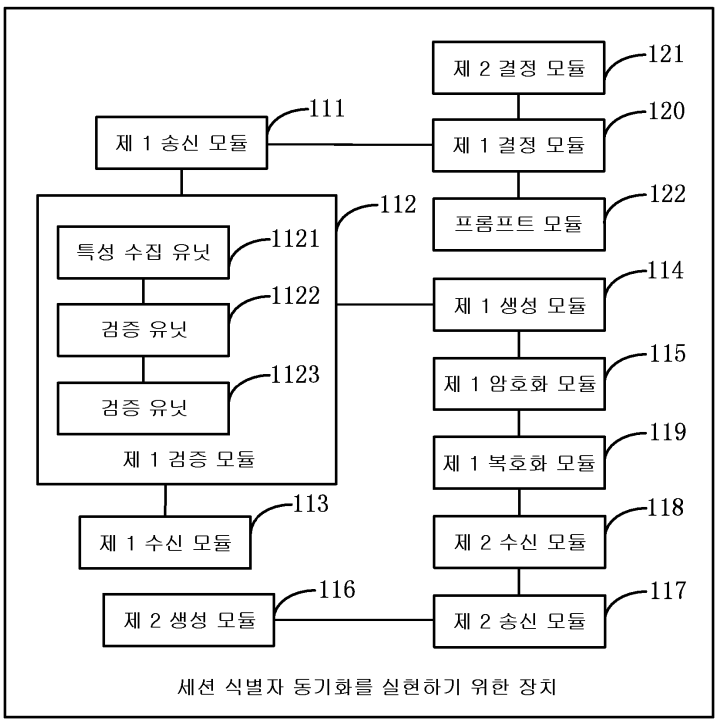
도면10



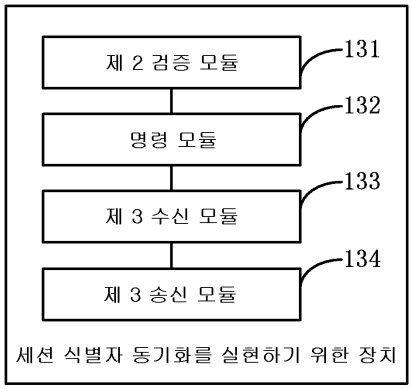

도면11



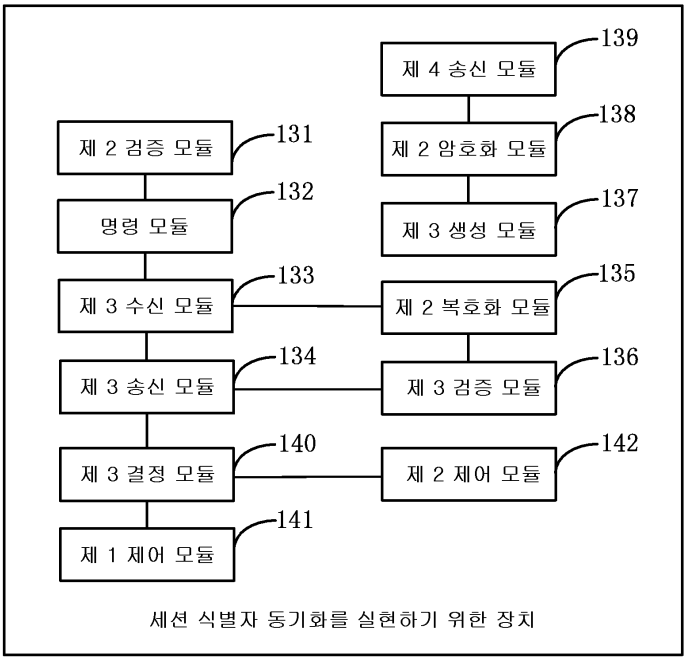

도면12



도면13


제 2 검증 모듈
131
명령 모듈
132
제 3 수신 모듈
133
제 3 송신 모듈
134
세션 식별자 동기화를 실현하기 위한 장치

도면14


제 4 송신 모듈
139
제 2 암호화 모듈
138
제 3 생성 모듈
137
제 2 복호화 모듈
135
제 3 검증 모듈
136
제 2 제어 모듈
142
제 2 검증 모듈
131
명령 모듈
132
제 3 수신 모듈
133
제 3 송신 모듈
134
제 3 결정 모듈
140
제 1 제어 모듈
141
세션 식별자 동기화를 실현하기 위한 장치