

명세서

발명의 명칭: 가상인증코드 기반의 장치 간 인증 방법 및 프로그램 기술분야

- [1] 본 발명은 가상인증코드 기반의 장치 간 인증 방법 및 프로그램에 관한 것이다.

배경기술

- [2] 코드형태 데이터는 많은 영역에서 이용되고 있다. 결제 시에 이용되는 카드번호, 계좌번호뿐만 아니라 사용자 식별을 위한 IPIN번호, 주민등록번호 등이 코드형태 데이터이다.
- [3] 그러나 이러한 코드데이터를 이용하는 과정에서 유출되는 사고가 많이 발생한다. 카드번호의 경우, 카드 표면에 실제카드번호가 그대로 기재되어 있어서 타인에게 시각적으로 유출되며, 마그네틱을 이용한 결제 시에 카드번호가 그대로 POS장치로 전달되면서 유출된다.
- [4] 실제코드가 그대로 유출되지 않도록 하기 위해 가상코드를 이용하고자 하는 시도가 많았으나, 가상코드에 대응되는 실제코드를 탐색하기 위해 사용자를 식별하기 위한 데이터가 필요하였다. 예를 들어, OTP(One Time Password)의 경우, 시간마다 코드가 변경되어 생성되지만, 사용자에게 부여된 알고리즘 판단을 위해 로그인 절차가 필요하여 다양한 영역에 적용되기 어렵다.
- [5] 따라서 실제카드번호, 주민등록번호 등과 같이 사용자나 장치의 식별정보를 제공하지 않으면서 실시간으로 변동되는 가상인증코드를 기반으로 사용자 또는 장치를 인증할 수 있는 발명이 필요하다.
- [6] 최근 많은 웹사이트, 플랫폼 등에서는 이용자들이 해당 웹사이트 상에 사용자 정보를 등록하지 않고, 다른 웹사이트 상의 등록된 사용자 정보에 대한 접근 권한을 부여받는 OAuth 인증 방식이 많이 이용되고 있다. OAuth 인증 방식의 경우 클라이언트 서버가 해당 플랫폼의 사용자 정보에 대한 접근 권한을 부여 받기 위하여, 접근 토큰(Access Token)을 사전에 획득해야만 한다.
- [7] 이때, 접근 토큰은 해당 플랫폼 내 특정 어플리케이션 또는 웹사이트에 대한 특정 정보에 대해서만 유효하다. 예를 들어, 특정 클라이언트 서버가 특정 회원에 대한 구글 캘린더에 대한 접근 토큰을 획득하였다고 하더라도, 구글 드라이브, 구글 스프레드시트 등과 같은 다른 어플리케이션에 대해서는 접근이 허용되지 않는다. 결국, 클라이언트 서버는 특정 회원에 관한 다른 어플리케이션에 대한 접근 토큰을 획득해야만 하고, 이를 위해 인증서버에 접속해야만 한다. 결국, 이러한 상황이 반복된다면, 사용자는 각각의 서버 장치에 대한 접근 토큰, 즉 접근 권한을 부여 받기 위하여 매번 인증서버에 접속해야만 한다. 이는 불필요한 시간을 소요할 뿐만 아니라 궁극적으로 반복적인 인증 절차가 누적되므로, 효율성이 떨어지는 결과를 초래한다.

발명의 상세한 설명

기술적 과제

- [8] 상술한 바와 같은 문제점을 해결하기 위한 본 발명은 가상인증코드 기반의 서버 간 인증 장치 및 방법을 제공하는 것이다.
- [9] 다만 본 발명이 해결하고자 하는 과제들은 이상에서 언급된 과제로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제 해결 수단

- [10] 상술한 과제를 해결하기 위한 가상인증코드 기반의 장치간 인증 방법은, 제1 장치에 의해 수행되는 방법으로서, 클라이언트 장치로부터 수신된 가상인증코드의 생성을 위한 소스 코드인 제1 코드를 송신하되, 상기 제1 코드는, 상기 클라이언트 장치의 식별 정보를 기반으로 생성되며, 검증장치에서 상기 제1 코드의 검증을 통해 상기 클라이언트 장치의 권한 부여에 이용되는, 제1 코드 송신 단계, 상기 검증 장치로부터 상기 제1 코드에 대한 인증 결과가 반영된 제2 코드를 수신하되, 상기 제2 코드는, 상기 제1 코드를 기반으로 상기 검증 장치에 의해 생성된 상기 클라이언트 장치에 관한 해쉬값 및 자격 정보를 포함하는, 제2 코드 수신 단계, 상기 제1 코드 및 상기 제2 코드를 기반으로 상기 가상인증코드인 제3 코드를 생성하는 단계 및 상기 자격 정보와 관련된 적어도 하나의 제2 장치로 상기 제3 코드를 송신하는 단계를 포함한다.
- [11] 또는 상기 제2 코드는, 상기 제2 코드에 관한 유효시간정보를 더 포함하고, 상기 제1 장치는, 상기 제2 장치로부터 만료된 제2 코드의 갱신을 위한 상기 제3 코드를 수신하고, 상기 제1 코드를 상기 검증장치로 송신하여, 상기 검증장치가 상기 제1 코드를 기반으로 상기 클라이언트 장치의 인증이 완료될 경우 상기 제2 코드를 갱신한 후 상기 갱신된 제2 코드를 상기 제1 장치로 송신하도록 요청하고, 상기 제1 코드, 상기 갱신된 제2 코드 및 상기 갱신된 제2 코드가 수신된 시간데이터를 기반으로 제3 코드를 재 생성하여, 제2 장치로 송신하는 단계를 포함한다.
- [12] 또는 상기 제2 코드는, 복수의 세부코드를 포함하고, 상기 복수의 세부코드는, 상기 클라이언트 장치에 의해 단위카운트마다 변경되어 생성되는 것이고, 상기 단위카운트는, 특정한 시간간격으로 설정되어, 상기 시간간격이 경과됨에 따라 변경되는 것이다.
- [13] 또는 상기 세부코드는, 서로 상관관계를 가지는 복수의 제1 세부코드 및 제2 세부코드를 포함하고, 상기 제1 세부코드는, 상기 검증장치에서의 상기 클라이언트 장치의 인증정보에 관한 탐색시작지점을 결정하고, 상기 제2 세부코드는, 상기 탐색시작지점으로부터 상기 인증정보에 관한 탐색경로를 결정한다.
- [14] 상술한 과제를 해결하기 위한 본 발명의 다른 면에 따른, 제2 장치에 의해 수행되는 가상인증코드 기반의 장치 간 인증방법으로서, 제1 장치로부터

가상인증코드인 제3 코드를 수신하는 단계 및 상기 제3 코드를 기반으로, 상기 클라이언트 장치의 권한을 승인하는 단계를 포함하고, 상기 권한 승인 단계는, 상기 제3 코드 내에 포함된 상기 제3 코드의 생성에 사용된 제1 코드(를 기반으로 클라이언트 장치에 관한 해쉬값을 생성하는 단계, 상기 생성된 해쉬값과 상기 제3 코드 내에 해쉬값을 비교하여, 상기 클라이언트 장치를 검증하는 단계 및 상기 제3 코드를 기반으로, 상기 클라이언트 장치에 관한 자격 정보를 판단하여 상기 클라이언트 장치의 권한을 승인하는 단계를 포함한다.

- [15] 또는 상기 권한 승인 단계는 상기 제3 코드를 기반으로, 상기 클라이언트 장치의 접근 가능한 장치에 상기 제2 장치가 포함되는지 여부를 판단하는 단계 및 상기 제3 코드 내에 포함된 시간데이터 및 제2 코드를 기반으로, 상기 제2 장치에 대한 상기 클라이언트 장치의 자격에 해당하는 권한을 승인하는 단계를 포함한다.
- [16] 또는 상기 제2 코드는 상기 제2 코드에 관한 유효시간정보를 더 포함하고, 상기 제2 코드의 유효시간이 만료되면, 상기 제1 장치로 상기 제3 코드를 반환하여, 상기 제2 코드를 갱신할 것을 요청하는 단계를 더 포함한다.
- [17] 또는 상기 제3 코드는 상기 제1 코드 및 상기 제2 코드와, 상기 제2 코드를 수신한 시간 데이터를 기반으로 생성되고, 상기 권한 승인 단계는, 상기 제3 코드를 기반으로, 상기 클라이언트 장치에 관한 자격 정보 및 상기 제2 코드를 수신한 시간을 기반으로, 상기 클라이언트 장치의 권한을 승인한다.
- [18] 또는 상기 클라이언트 장치 검증 성공 및 상기 승인된 권한을 식별하는 정보를 생성하는 단계 및 상기 제3 코드 및 상기 식별 정보를 기반으로 제2 장치에 관한 신규 제3 코드를 생성하는 단계를 포함한다.
- [19] 상술한 과제를 해결하기 위한 본 발명의 다른 면에 따른, 검증 장치에 의해 가상인증코드 기반의 장치 간 인증 방법으로서, 제1 장치를 통해 클라이언트 장치로부터 가상인증코드의 생성을 위한 소스 코드인 제1 코드를 수신하되, 상기 제1 코드는, 상기 클라이언트 장치의 식별 정보를 기반으로 생성된 것인, 제1 코드 수신 단계, 상기 제1 코드를 기반으로, 상기 클라이언트 장치의 식별 정보의 저장위치를 탐색하여 상기 클라이언트 장치의 인증을 수행하는 단계, 상기 클라이언트 장치의 인증이 완료되면, 상기 클라이언트 장치에 관한 자격 정보를 생성하는 단계, 상기 제1 코드를 기반으로 상기 클라이언트 장치에 관한 해쉬값을 생성하는 단계, 상기 생성된 자격 정보 및 해쉬값을 기반으로, 상기 제1 코드에 대한 인증 결과가 반영된 제2 코드를 생성하는 단계 및 상기 제1 장치가 상기 제2 코드를 기반으로 상기 가상인증코드인 제3 코드를 생성하도록 상기 제2 코드를 상기 제1 장치로 송신하는 단계를 포함한다.
- [20] 또는 상기 제2 코드는, 상기 제2 코드에 관한 유효시간정보를 더 포함하고, 상기 검증 장치는, 상기 제1 장치로부터 수신된 제1 코드에 대한 제2 코드의 유효시간이 만료된 상태에서 상기 만료된 제2 코드에 관한 갱신을 요청 받으면, 상기 제1 장치로부터 수신된 제1 코드 및 기 저장된 제1 코드의 동일 여부를

판단하여, 상기 클라이언트 장치의 인증을 수행하는 단계 및 상기 클라이언트 장치의 인증이 완료되면, 상기 제2 코드를 갱신하여, 상기 제1 장치로 송신하는 단계를 더 포함한다.

- [21] 상술한 과제를 해결하기 위한 본 발명의 다른 면에 따른, 클라이언트 장치에 의해 수행되는 가상인증코드 기반의 장치 간 인증방법으로서, 상기 클라이언트 장치의 식별 정보를 기반으로, 가상인증코드의 생성을 위한 소스 코드인 제1 코드를 생성하는 단계 및 상기 제1 코드를 제1 장치를 통해 검증 장치로 송신하여, 상기 제1 장치에 대한 상기 클라이언트 장치의 권한 승인을 요청하는 단계를 포함하고, 상기 제1 코드는, 복수의 세부코드를 포함하고, 상기 복수의 세부코드는, 상기 클라이언트 장치에 의해 단위카운트마다 변경되어 생성되는 것이고, 상기 단위카운트는, 특정한 시간간격으로 설정되어, 상기 시간간격이 경과됨에 따라 변경되는 것이다.
- [22] 또는 상기 세부코드는, 서로 상관관계를 가지는 복수의 제1 세부코드 및 제2 세부코드를 포함하고, 상기 제1 세부코드는, 상기 검증장치에서의 상기 클라이언트 장치의 인증정보에 관한 탐색시작지점을 결정하고, 상기 제2 세부코드는, 상기 탐색시작지점으로부터 상기 인증정보에 관한 탐색경로를 결정한다.
- [23] 상술한 과제를 해결하기 위한 본 발명의 다른 면에 가상인증코드를 기반으로 한 서버간 인증 방법을 수행하는 컴퓨터 프로그램은, 저장 매체에 저장될 수 있다.
- [24] 이 외에도, 본 발명을 구현하기 위한 다른 방법, 다른 시스템 및 상기 방법을 실행하기 위한 컴퓨터 프로그램을 기록하는 컴퓨터 판독 가능한 기록 매체가 더 제공될 수 있다.

발명의 효과

- [25] 상기와 같은 본 발명에 따르면, 검증 장치에서의 클라이언트 장치의 단 한번의 인증만으로도, 복수의 서비스 장치에 대한 권한 인증이 가능하다. 이를 통해, 클라이언트 장치가 각각의 서비스 장치에 권한 인증을 위해 검증 장치에 접속한 후 인증 과정을 수행하는데 소요된 시간 및 비용을 절약할 수 있다.
- [26] 한편, 클라이언트 장치에 관한 복수의 서비스 장치에 대한 자격 정보를 포함하는 가상코드를 생성함으로써, 상기 클라이언트 장치의 접근 권한이 인정되는 적어도 하나 이상의 서비스 장치에 대한 정보가 유출되는 것을 방지할 수 있다.
- [27] 또한, 상기 본 발명에 의하면, 가상인증코드생성 및 자격정보저장공간 탐색을 위한 알고리즘이 추가되면 되므로, 기존의 프로세스를 그대로 유지할 수 있다. 이를 통해, 보안성을 높이기 위해 기존 프로세스 내에서 변경되어야 하는 부분을 최소화할 수 있고, 사용자는 보안성 향상을 위한 별도 단계를 수행하지 않아도 된다.

- [28] 본 발명의 효과들은 이상에서 언급된 효과로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

- [29] 도 1은 본 발명의 일 실시예에 따른, 가상인증코드 기반의 서버 간 인증 방법을 개략적으로 나타낸 순서도이다.
- [30] 도 2는 본 발명의 일 실시예에 따른, 클라이언트 장치의 개략적인 구성도이다.
- [31] 도 3은 본 발명의 일 실시예에 따른, 클라이언트 장치의 제1 코드를 기반으로 제1 장치에 대한 권한 승인을 요청하는 방법을 개략적으로 나타낸 순서도이다.
- [32] 도 4는 본 발명의 일 실시예에 따른, 클라이언트 장치의 제1 코드의 개략적인 구성도이다.
- [33] 도 5는 본 발명의 일 실시예에 따른, 검증 장치의 개략적인 구성도이다.
- [34] 도 6은 본 발명의 일 실시예에 따른, 제1 코드를 기반으로 클라이언트 장치를 검증하여, 제2 코드를 생성하는 방법을 개략적으로 나타낸 순서도이다.
- [35] 도 7은 본 발명의 일 실시예에 따라 k각형의 구름이동을 통해 클라이언트 장치의 인증 정보의 저장 위치를 탐색하는 저장위치탐색알고리즘에 대한 예시도이다.
- [36] 도 8는 본 발명의 일 실시예에 따른 검증 장치에 의해 생성된 제2 코드의 개략적인 구성도이다.
- [37] 도 9는 본 발명의 일 실시예에 따른 서비스 장치에 대한 개략적인 구성도이다.
- [38] 도 10은 본 발명의 일 실시예에 따른 제1 장치에 의해 수행되는 제1 코드 및 제2 코드를 기반으로 가상인증코드인 제3 코드를 생성하는 방법을 개략적으로 나타낸 순서도이다.
- [39] 도 11는 본 발명의 일 실시예에 따른 제3 코드의 개략적인 구성도이다.
- [40] 도 12는 본 발명의 일 실시예에 따른, 제3 코드 기반의 서버 간 인증 방법을 개략적으로 나타낸 예시도이다.
- [41] 도 13은 본 발명의 일 실시예에 따른, 제3 코드를 기반으로 한 서버 간 인증 방법을 개략적으로 나타낸 순서도이다.
- [42] 도 14는 본 발명의 일 실시예에 따른, 제3 코드를 기반으로 한 클라이언트 장치에 대한 권한 승인 방법을 개략적으로 나타낸 순서도이다.
- [43] 도 15는 본 발명의 일 실시예에 따른, 제3 코드를 기반으로 클라이언트 장치에 대한 권한을 승인하는 방법을 개략적으로 나타낸 순서도이다.
- [44] 도 16은 본 발명의 제2 장치의 클라이언트 장치의 검증 및 권한 승인 정보를 기반으로, 새로운 제3 코드를 생성하는 것을 개략적으로 나타낸 순서도이다.

발명의 실시를 위한 형태

- [45] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본

발명은 이하에서 개시되는 실시예들에 제한되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술 분야의 통상의 기술자에게 본 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.

- [46] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다. 명세서 전체에 걸쳐 동일한 도면 부호는 동일한 구성 요소를 지칭하며, "및/또는"은 언급된 구성요소들의 각각 및 하나 이상의 모든 조합을 포함한다. 비록 "제1", "제2" 등이 다양한 구성요소들을 서술하기 위해서 사용되나, 이들 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 구성요소를 다른 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 구성요소는 본 발명의 기술적 사상 내에서 제2 구성요소일 수도 있음은 물론이다.
- [47] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술분야의 통상의 기술자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또한, 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.
- [48] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세하게 설명한다.
- [49] 설명에 앞서 본 명세서에서 사용하는 용어의 의미를 간략히 설명한다. 그렇지만 용어의 설명은 본 명세서의 이해를 돕기 위한 것이므로, 명시적으로 본 발명을 한정하는 사항으로 기재하지 않은 경우에 본 발명의 기술적 사상을 한정하는 의미로 사용하는 것이 아님을 주의해야 한다.
- [50] 또한, 명세서에서 사용되는 "부"라는 용어는 소프트웨어, FPGA 또는 ASIC과 같은 하드웨어 엘리먼트를 의미하며, "부"는 어떤 역할들을 수행한다. 그렇지만 "부"는 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. "부"는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 "부"는 소프트웨어 엘리먼트들, 객체지향 소프트웨어 엘리먼트들, 클래스 엘리먼트들 및 태스크 엘리먼트들과 같은 엘리먼트들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다. 엘리먼트들과 "부"들 안에서 제공되는 기능은 더 작은 수의 엘리먼트들 및 "부"들로 결합되거나 추가적인 엘리먼트들과 "부"들로 더

분리될 수 있다.

- [51] 또한, 본 명세서에서 모든 “부”는 적어도 하나의 프로세서에 의해 제어될 수 있으며 본 개시의 “부”가 수행하는 동작을 적어도 하나의 프로세서가 수행할 수도 있다.
- [52] 본 명세서의 실시예들은 기능 또는 기능을 수행하는 블록의 관점에서 설명될 수 있다. 본 개시의 ‘부’ 또는 ‘모듈’ 등으로 지칭될 수 있는 블록은 논리 게이트, 집적 회로, 마이크로 프로세서, 마이크로 컨트롤러, 메모리, 수동 전자 부품, 능동 전자 부품, 광학 컴포넌트, 하드와이어드 회로(hardwired circuits) 등과 같은 아날로그 또는 디지털 회로에 의해 물리적으로 구현되고, 선택적으로 펌웨어 및 소프트웨어에 의해 구동될 수 있다.
- [53] 본 명세서의 실시예는 적어도 하나의 하드웨어 디바이스 상에서 실행되는 적어도 하나의 소프트웨어 프로그램을 사용하여 구현될 수 있고 엘리먼트를 제어하기 위해 네트워크 관리 기능을 수행할 수 있다.
- [54] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술분야의 통상의 기술자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또한, 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.
- [55] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세하게 설명한다.
- [56] 본 명세서에서 “문자”는 코드를 구성하는 구성요소로서, 대문자알파벳, 소문자알파벳, 숫자 및 특수문자 등의 전부 또는 일부를 포함한다.
- [57] 본 명세서에서 “코드”는 문자가 나열된 문자열을 의미한다.
- [58] 본 명세서에서 ‘세부코드’는 가상코드에 포함되는 일부 코드를 의미한다. 즉, 가상코드가 별도로 생성된 복수의 코드를 결합하여 생성되는 경우, 세부코드는 별도로 생성되어 가상코드를 구성하는 개별 코드를 의미한다.
- [59] 본 명세서에서 ‘단위카운트’는 특정한 시간간격으로 설정되어, 상기 시간간격이 경과됨에 따라 변경되는 것으로 정의된 단위이다. 예를 들어, 1카운트는 특정한 시간간격(예를 들어, 1.5초)으로 설정되어 사용될 수 있다.
- [60] 본 명세서에서 “ID(identifier)”는 클라이언트 장치를 식별하기 위해 클라이언트 장치 별로 중복되지 않게 서버 장치에 의해 부여되는 고유한 코드 형태의 값을 의미한다.
- [61] 본 명세서에서 ‘가상코드생성함수’는 가상코드를 생성하는데 이용되는 함수를 의미한다.
- [62] 본 명세서에서 ‘구름이동’은 대상체가 회전하면서 병진운동을 하는 것을 의미한다. 즉, ‘구름이동’은 회전운동과 병진운동을 함께 수행하면서 이동하는 것으로서, 회전하는 대상체의 각 지점이 이동하는 축사에 차례대로 접하면서 이동하는 것을 의미한다.
- [63] 도 1은 본 발명의 일 실시예에 따른, 가상인증코드 기반의 서버 간 인증 방법을

개략적으로 나타낸 예시도이다.

- [64] 도 1을 참조하면, 클라이언트 장치(100)는 복수의 서비스 장치(200) 중 특정 장치에 대한 접근 또는 이용 권한을 승인 받고자 할 때, 검증 장치(300)에 인증 및 검증을 받아야 한다. 클라이언트 장치(100)를 검증하기 위해서는, 검증 장치(300)에 저장된 해당 클라이언트 장치(100)의 인증 정보를 활용해야 하기 때문이다. 도 1을 참조하면, 클라이언트 장치는, 제1 장치에 관한 권한을 승인 받고자 제1 코드를 생성한 후 제1 장치를 통해 검증 장치에 송신하였다. 이때 검증 장치(300)는, 수신한 제1 코드를 기반으로 클라이언트 장치에 대한 검증을 수행하게 될 것이다. 만약, 클라이언트 장치(100)가 서비스 장치(200) 중 제1 장치(200_1)가 아닌 제2 장치(200_2)에 대한 권한을 승인 받고자 한다면, 클라이언트 장치(100)를 인증하기 위한 또 다른 제1 코드를 생성한 후 검증 장치(300)로 송신하여, 검증 과정을 다시 수행하여야 한다. 즉, 클라이언트 장치(100)는 각각의 서비스 장치(200)에 대한 권한 승인을 위하여, 매번 검증 장치(300)에 권한 승인을 요청해야 한다. 이는 시간적으로 비효율적이며, 반복되는 과정으로 인하여, 효율성이 떨어진다. 따라서, 본 발명은 이러한 문제점을 해결하고, 검증 장치(300)에서의 클라이언트 장치(100)에 대한 한번의 인증 후 해당 인증 정보를 포함하는, 가상인증코드를 생성하도록 하여, 클라이언트 장치(100)의 검증 장치(300)에 대한 반복적인 권한 승인 없이도 서비스 장치(200) 간의 클라이언트 장치(100)의 검증이 가능하도록 한다.
- [65] 도 1을 참조하면, 상술한 본 발명의 과제 해결 원리는, 검증 장치(300)에 의해 생성되는 제2 코드를 기반으로 제1 장치(200_1)에서 생성되는 제3 코드를 통해 발휘될 수 있다. 이하, 이에 대한 본 발명의 실시예에 대하여 자세히 설명하도록 한다.
- [66] 도 2는 본 발명의 일 실시예에 따른, 클라이언트 장치의 개략적인 구성도이다. 도 3은 본 발명의 일 실시예에 따른, 클라이언트 장치의 제1 코드를 기반으로 제1 장치에 대한 권한 승인을 요청하는 방법을 개략적으로 나타낸 순서도이다. 도 4는 본 발명의 일 실시예에 따른, 클라이언트 장치의 제1 코드의 개략적인 구성도이다.
- [67] 먼저, 제1 코드는 상술한 가상인증코드 중 하나로서, 클라이언트 장치에 대한 인증을 위해 생성된 가상코드를 의미한다. 발명의 이해를 돕기 위하여, 클라이언트 장치에 관한 가상인증코드를 본 명세서에서는 상기 제1 코드로 설명하도록 한다.
- [68] 한편, 제1 코드는 검증 장치(300)에서 상기 클라이언트 장치를 인증하는데 이용된다. 구체적으로, 제1 코드에 포함된 클라이언트 장치(100)의 식별정보와 상응하여 검증 장치 내 저장된, 클라이언트 장치(100)의 인증정보의 저장위치를 탐색하여, 상기 클라이언트 장치를 인증한다.
- [69] 도 2 및 도 3을 참조하여, 클라이언트 장치(100) 및 클라이언트 장치(100)의 제1 코드 생성 방법에 대하여 설명하도록 한다.

- [70] 도 2를 참조하면, 클라이언트 장치(100)는 세부코드생성부(110), 제1코드생성부(120) 및 통신부(130)를 포함한다. 한편, 클라이언트 장치(100)는 리소스 서버(Resource Server)에 대한 접근 권한 및 데이터 이용 권한을 검증 서버(Authentication Server)에 요청하는 클라이언트 서버(Client Server)에 해당할 수 있다. 그러나 이에 한정하는 것은 아니다.
- [71] 세부코드생성부(110)는, 상기 제1코드 내 포함된 복수의 세부코드를 생성한다. 이때, 제1코드생성부(120)는 하나 이상의 세부코드를 조합하여 제1코드로 생성하는 역할을 수행한다. 일 실시예로, 상기 제1코드는 복수의 세부코드를 특정한 규칙에 따라 결합하여 생성되는 것이다.
- [72] 한편, 세부코드는, 클라이언트 장치(100)에 의해 단위카운트마다 변경되어 생성되는 것으로, 이때 단위카운트는, 특정한 시간간격으로 설정되어 시간간격에 따라 변경되는 것을 의미한다. 예를 들어, 시간간격이 2초라고 가정한다면, 각각의 2초가 경과될 때마다 상기 단위카운트가 누적되어 산출되게 될 것이다.
- [73] 도 3을 참조하면, 클라이언트 장치(100)는 식별 정보를 기반으로, 가상인증코드의 생성을 위한 소스 코드인 제1 코드를 생성한다(S410).
- [74] 구체적으로, 클라이언트 장치(100)의 제1코드생성부(120)는 클라이언트 장치의 식별 정보를 기반으로 제1 코드를 생성한다. 이때, 클라이언트 장치(100)는 특정 서비스 장치에 대한 접근 권한 승인을 위하여, 제1코드생성함수에 따라 제1 코드를 생성한다. 클라이언트 장치(100)의 식별 정보란, 검증 장치에 설정된 해당 클라이언트 장치의 ID(Identifier) 및 비밀값(Secret)일 수 있다. 그러나 이에 제한되는 것은 아니다.
- [75] 도 4를 참조하면, 제1 코드의 개략적인 구성을 알 수 있다. 제1코드 생성부(120)는 해당 클라이언트 장치의 검증장치에 대한 ID(Identifier) 및 해쉬값이 포함된 제1코드를 생성하였다. 그러나 이에 제한되는 것은 아니다.
- [76] 예를 들어, 도면에 명확히 도시되지는 않았으나, 본 발명의 일 실시예로, 클라이언트 장치의 ID를 상기 제1코드생성함수에 적용하여 가상인증코드를 생성한 후 상기 클라이언트 장치(100)의 검증 장치에 대한 비밀값(SECRET)을 해쉬함수(Hash Function)에 적용하여 해쉬값을 산출한다. 그리고 상기 가상인증코드와 상기 해쉬값을 결합하여 최종적으로 제1 코드를 생성할 수도 있을 것이다.
- [77] 또한, 도면에 명확히 도시되지는 않았으나, 제1 코드를 생성함에 있어서, 시간 데이터를 활용할 수도 있을 것이다. 여기서 시간 데이터란, 클라이언트 장치(100)의 제1 장치에 대한 권한 승인 요청 시간일 수 있다. 그러나 이에 제한되는 것은 아니다. 시간 데이터를 활용한 경우, 클라이언트 장치(100)의 식별 정보, 예를 들어 ID 및 상기 시간 데이터를 상기 제1코드생성함수에 적용하여 가상인증코드를 생성한다. 그리고 상기 시간 데이터 및 클라이언트 장치(100)의 비밀값을 해쉬함수(Hash Function)에 적용하여 해쉬값을 산출한다.

가상인증코드 및 해쉬값을 결합하여 제1 코드를 생성할 수도 있을 것이다.

- [78] 한편, 도 3을 참조하면, 클라이언트 장치(100)는 제1 코드를 제1 장치로 송신하여, 상기 제1 장치에 대한 상기 클라이언트 장치의 권한 승인을 요청한다(S420). 보다 상세하게는, 클라이언트 장치(100)는 제1 장치를 통해 검증 장치로 제1 코드를 송신하여, 제1 장치에 대한 클라이언트 장치의 권한 승인을 요청한다.
- [79] 한편, 본 발명의 일 실시예로는, 클라이언트 장치(100)가 검증 장치(300)에 등록된 복수의 서비스 장치(200)에 대한 권한 승인을 위하여, 검증 장치(300)로 직접 제1코드를 송신하여, 복수의 서비스 장치(200)에 대한 권한 승인을 요청할 수 있을 것이다. 이때, 검증 장치(300)에 의해 해당 클라이언트 장치(100)에 대한 인증이 완료되면, 검증 장치(300)는 제1 코드를 기반으로 생성된 제2 코드를 서비스 장치(200)가 아닌 클라이언트 장치(100)로 직접 송신한다.
- [80] 상술한 바와 같이, 클라이언트 장치(100)가 접근 권한 승인을 받고자 하는 제1 장치로 제1 코드를 송신한다. 이때, 제1 장치는 상술한 바와 같이, 복수의 서비스 장치(200) 중 클라이언트 장치(100)의 최초 접근 권한 승인을 요청한 장치로 결정될 수 있다. 즉, 제1 장치는 클라이언트 장치(100)가 접근 권한 승인을 요청하기 위하여 제1 코드를 송신함으로써, 결정될 수 있다. 그러나 이에 제한되는 것은 아니다.
- [81] 예를 들어, 복수의 서비스 장치(200)가 순서를 가지고 연동하는 경우, 즉 클라이언트 장치(100)가 최초 서비스 장치(200)에 대한 접근 및/또는 해당 장치의 이용 권한 승인을 받아야만, 나머지 서비스 장치(200)에 대한 접근 및/또는 나머지 서비스 장치(200)에 대한 이용 권한 승인이 가능하다면, 제1 장치는 사전에 설정될 수도 있을 것이다. 또한, 제1 장치를 비롯한 서비스 장치(200) 내 나머지 장치에 대해서도 순서에 기반하여, 명칭이 결정될 수 있다.
- [82] 통신부(130)는 제1코드를 검증장치(300)로 송신하는 역할을 수행한다. 통신부(130)는 제1코드를 외부로 제공할 수 있는 다양한 구성을 포함할 수 있다.
- [83] 도면에 명확히 도시되지는 않았으나, 무선통신모듈; 근거리통신모듈; IC칩; 자장발생부; 디스플레이부 등의 전부 또는일부를 포함한다.
- [84] 무선 인터넷 모듈은 무선 인터넷 접속을 위한 모듈을 말하는 것으로, 이동 단말기(100)에 내장되거나 외장될 수 있다. 무선 인터넷 기술로는 WLAN(Wireless LAN)(Wi-Fi), Wibro(Wireless broadband), Wimax(World Interoperability for Microwave Access), HSDPA(High Speed Downlink Packet Access), LTE(long term evolution), LTE-A(Long Term Evolution-Advanced) 등이이용될 수 있다.
- [85] 근거리 통신 모듈은 근거리 통신을 위한 모듈을 말한다. 근거리 통신(short range communication) 기술로 블루투스(Bluetooth), BLE(Bluetooth Low Energy), 비콘(Beacon), RFID(Radio Frequency Identification), NFC(Near Field Communication), 적외선 통신(Infrared Data Association; IrDA), UWB(Ultra

Wideband), ZigBee 등이 이용될 수 있다.

- [86] 이하에서는, 세부코드를 기반으로 클라이언트장치(100)가 제1코드를 생성하는 방법에 대하여 설명한다.
- [87] 도면에 명확히 도시되지는 않았으나, 제1코드생성부(120)는 하나 이상의 세부코드를 조합하여 제1코드로 생성하는 역할을 수행한다. 일 실시예로, 상기 제1코드는 복수의 세부코드를 특정한 규칙에 따라 결합하여 생성되는 것이다. 제1코드생성함수는 복수의 세부코드를 조합하는 규칙(즉, 세부코드결합함수)을 포함한다.
- [88] 복수의 세부코드를 결합하여 하나의 가상코드를 생성하는 방식으로는 다양한 방식이 적용될 수 있다.
- [89] 클라이언트 장치(100)는, 일 실시예로, 클라이언트 장치의 인증을 위한 가상인증코드, 즉 제1코드를 생성하는 프로그램(즉, 애플리케이션)을 포함할 수 있다.
- [90] 이때 세부코드생성부(110)는 클라이언트의 식별 정보(Identifier, Secret 등)를 기반으로 하나 이상의 세부코드를 생성하는 역할을 수행한다. 제1코드생성함수는 하나 이상의 세부코드생성함수를 포함한다. 예를 들어, 제1코드가 복수의 세부코드를 포함하는 경우, 제1코드생성함수는 복수의 세부코드생성함수를 이용하여 복수의 세부코드를 생성하고, 복수의 세부코드를 결합하는 세부코드결합함수를 이용하여 제1코드를 생성한다.
- [91] 이때, 제1코드는 클라이언트 장치(100)에 내장 또는 설치된 전용프로그램에 의해 단위카운트마다 생성한다.
- [92] 본 발명의 일 실시예로, 클라이언트 장치(100)는 클라이언트 장치의 식별 정보, 예를 들어 클라이언트 장치의 ID(Identifier)를 제1코드생성함수의 시드데이터 중 하나로 이용할 수 있다. 구체적인 예로, 세부코드생성부(110)는 하나의 세부코드생성함수를 이용하여 클라이언트 장치의 ID(Identifier)와 클라이언트 장치(100)에 내장 또는 설치된 전용프로그램의 시리얼번호를 조합한 조합시리얼번호를 각 세부코드생성함수의 시드데이터로 이용하여 각각의 세부코드를 생성한다..
- [93] 일 실시예로, 세부코드생성부(110)는 세부코드생성함수로 제1세부코드생성함수와 제2세부코드생성함수를 포함하여, 제1세부코드 및 제2세부코드를 생성할 수 있다. 이때, 클라이언트 장치(100)는 보안성을 높이기 위해 제1세부코드를 생성하는 제1세부코드생성함수와 제2세부코드를 생성하는 제2세부코드생성함수를 세부코드생성함수로 포함할 뿐, 제1세부코드와 제2세부코드의 상관관계에 대한 데이터는 포함하지 않을 수 있다.
- [94] 제1코드생성부(120)는 제1코드생성함수를 이용하여 하나 이상의 세부코드를 조합하여 제1코드로 생성하는 역할을 수행한다. 일 실시예로, 제1코드는 복수의 세부코드를 특정한 규칙에 따라 결합하여 생성된다. 제1코드생성함수는 복수의 세부코드를 조합하는 규칙(즉, 세부코드결합함수)을 포함한다. 즉,

제1코드생성부(120)는 하나 이상의 세부코드를 제1코드생성함수에 포함된 세부코드결합함수를 이용하여 조합할 수 있다.

- [95] 이때, 본 발명의 일 실시예로, 제1코드가 제1세부코드 및 제2세부코드의 특정한 규칙에 따른 조합으로 생성되는 경우, 제1세부코드와 제2세부코드는 클라이언트 정보가 저장된 저장위치탐색알고리즘 내의 클라이언트 인증 정보의 저장위치를 탐색하기 위한 각각의 역할을 수행할 수 있다. 예를 들어, 제1세부코드는 저장위치탐색의 시작지점을 설정하고, 제2세부코드는 특정한 탐색방식에 따라 상기 시작지점으로부터 상기 클라이언트 장치의 인증 정보의 저장위치로의 탐색경로를 설정한다. 즉, 클라이언트장치(100)에서 단위카운트마다 정상적으로 생성된 제1코드가 제공되면, 검증장치(200)는 제1코드에 포함된, 제1세부코드에 대응하는 탐색시작지점으로부터 제2세부코드에 대응하는 탐색경로에 따라 이동한 지점을 클라이언트 장치의 인증 정보가 저장된 지점(즉, 클라이언트 장치의 인증정보의 저장위치)으로 판단한다. 제1코드를 구성하는 제1세부코드와 제2세부코드를 기반으로 클라이언트 장치의 인증 정보의 저장위치를 탐색하는 구체적인 방식은 후술한다.
- [96] 세부코드생성부(110)가 세부코드를 생성하는 방식의 일 실시예로, 세부코드생성부(110)는 단위카운트마다 새로운 세부코드를 생성하고, 이에 따라 클라이언트 장치(100)는 단위카운트마다 새로운 제1코드를 생성한다. 단위카운트마다 신규로 생성되는 제1코드는 중복되어 생성되지 않는다. 구체적으로, 세부코드생성부(110)는, 단위카운트마다 신규 생성되는 제1코드가 특정한 클라이언트장치(100)에게 정해진 기간 동안 중복 생성되지 않도록 설정될 수 있다.
- [97] 또한, 본 발명의 일 실시예로, 상술한 제1 코드 생성에 이용되는, 클라이언트 장치(100)의 식별 정보를 기반으로 복수의 세부코드를 생성하여, 궁극적으로 제1 코드를 생성하는 방법과 관련하여, 클라이언트 장치(100)의 검증 장치(300)에 대한 ID를 기반으로 제1 세부코드를 생성하고, 상술한 시간데이터를 기반으로 제2 세부코드를 생성하여, 상기 제1 세부코드 및 제2 세부코드를 결합한 제1 코드를 생성할 수도 있다. 그러나 이에 한정하는 것은 아니다.
- [98] 이하에서는, 검증장치(300)의 제1코드를 기반으로 클라이언트장치(100)를 검증하고, 궁극적으로 클라이언트장치(100)의 적어도 하나의 서비스장치(200)에 대한 자격 정보를 추출하고, 상기 자격 정보를 기반으로 제2코드를 생성하는 방법에 대하여 구체적으로 서술하도록 한다.
- [99] 도 5는 본 발명의 일 실시예에 따른, 검증 장치의 개략적인 구성도이고, 도 6은 본 발명의 일 실시예에 따른, 제1 코드를 기반으로 클라이언트 장치를 검증하여, 제2 코드를 생성하는 방법을 개략적으로 나타낸 순서도이고, 도 7은 본 발명의 일 실시예에 따라 k각형의 구름이동을 통해 클라이언트 장치의 인증 정보의 저장 위치를 탐색하는 저장위치탐색알고리즘에 대한 예시도이다. 도 8은 본

발명의 일 실시예에 따른 검증 장치에 의해 생성된 제2 코드의 개략적인 구성도이다.

- [100] 도 5를 참조하면, 검증 장치(300)는, 통신부(310), 세부코드추출부(320), 인증정보탐색부(330) 및 제2코드생성부(340)를 포함한다. 검증 장치(300)는, 서버 장치일 수 있으며, 예를 들어, 클라이언트 장치(100)가 OAuth 인증 방식을 이용하는 클라이언트 서버인 경우, 리소스 서버(Resource Server)에 대한 클라이언트 장치(100)의 접근 권한을 부여 및 관리하는 검증 서버일 수 있다. 그러나 이에 한정하는 것은 아니다.
- [101] 먼저 도 6을 참조하면, 검증 장치(300)는 제1 장치를 통해 클라이언트 장치로부터 가상인증코드의 생성을 위한 소스 코드인 제1 코드를 수신한다(S430). 이때, 상술한 바와 같이 제1 코드는, 클라이언트 장치의 식별 정보를 기반으로 생성된 것이다.
- [102] 구체적으로, 검증 장치(300)는 제1 장치(200_1)의 클라이언트 장치(100)에 대한 인증 요청을 수신한다. 그리고 검증 장치(300)는 해당 클라이언트 장치(100)가 검증 장치(300)에 등록된, 신뢰할 수 있는 장치에 해당하는지 여부를 검증한다. 즉, 제1 코드를 기반으로 검증 장치(300)내 저장된 클라이언트 장치(100)의 인증 정보를 추출하여, 상기 제1 코드 내 포함된 클라이언트 장치(100)의 식별 정보와 비교한다. 그리고 인증 정보 및 식별 정보가 일치하거나 또는 적합하게 매칭된다면, 클라이언트 장치(100)의 인증을 완료할 것이다.
- [103] 한편, 클라이언트 장치(100)가 인증되었음이 곧 클라이언트 장치(100)의 제1 장치에 대한 권한 승인을 의미하는 것은 아니다. 왜냐하면, 클라이언트 장치(100)는 전체 서비스 장치(200) 중에서 접근 권한이 인정되지 않는 장치가 존재할 수 있기 때문이다. 예를 들어, OAuth 인증 방식을 가정한다면, 검증 서버로부터 Access Token을 획득하지 못한 서버에 대해서는, 클라이언트 서버의 클라이언트 ID 및 비밀번호가 인증되었다 하더라도, 해당 서버에 대한 권한을 인정할 수 없기 때문이다. 이하, 이에 대한 검증 장치(300)의 인증 수행 및 자격 정보 생성에 관한 과정을 상세히 설명한다.
- [104] 도 6을 참조하면, 검증 장치(300)는 제1 장치로부터 수신한 제1 코드를 기반으로, 클라이언트 장치(100)의 인증 정보의 저장위치를 탐색하여 상기 클라이언트 장치의 인증을 수행한다(S440).
- [105] 여기서, 클라이언트 장치(100)의 인증 정보라, 클라이언트 장치(100)가 검증 장치(300)에 등록할 때, 제공된 정보로 특정 클라이언트 장치임을 식별할 수 있는 식별 정보와 대응되는 것을 의미한다. 예를 들어, 클라이언트 장치(100) 자체의 시리얼 번호, 발급된 ID(예를 들어, Client ID), 해당 ID(Identifier)와 관련한 비밀값(예를 들어, Client Secret) 등이 이에 해당할 수 있다.
- [106] 보다 구체적으로, 다시 도 4를 참조하면, 제1 코드는 클라이언트 장치(100)의 식별정보를 기반으로 생성된 가상인증코드이다. 제1 코드 내에는 클라이언트 장치(100)의 검증 장치(300)에 대한 ID(Identifier) 및 비밀값(Secret)이 포함될 수

있다. 이때, 검증 장치(300) 내 저장된 상기 클라이언트 장치(100)에 대한 인증 정보, 예를 들어 저장된 ID ID(Identifier) 및 비밀값(Secret)의 저장위치를 탐색한다. 그리고 상기 제1 코드 내 포함된, 식별값과 저장위치 내 저장된 식별값을 비교하여 클라이언트 장치(100)에 대한 인증을 수행할 수 있을 것이다.

- [107] 또 다른 실시예로, 검증 장치(300)의 인증정보탐색부(330)는 클라이언트 장치(100)의 제1코드생성함수와 동일한 함수를 포함할 수도 있다. 이때, 검증 장치(300)는 수신한 제1코드를 상기 제1코드생성함수에 적용하여, 클라이언트 장치(100)의 식별 정보를 추출할 수 있을 것이다. 예를 들어 클라이언트 장치(100)의 ID(Identifier)가 이에 해당할 것이다. 이때, 인증정보탐색부(330)는 상기 ID(Identifier)에 매칭되는 상기 클라이언트 장치(100)의 인증 정보 저장위치를 탐색한다. 그리고 인증 정보 저장위치로부터 상기 클라이언트 장치(100)의 비밀값을 추출한다. 추출된 비밀값을 해쉬함수에 적용하여 해쉬값을 산출한다. 그리고 산출된 해쉬값을 제1코드 내 해쉬값과 비교하여, 클라이언트 장치(100)의 인증을 완료할 수 있을 것이다.
- [108] 한편, 제1 코드 생성 과정에서, 시간 데이터를 활용할 수 있다고 상술하여 설명한 바 있다. 시간 데이터를 활용하여 생성된 제1 코드를 기반으로, 클라이언트 장치(100)의 인증을 수행할 경우에는, 시간 데이터(클라이언트 장치(100)가 제1 장치에 대한 권한 승인을 요청한 시점) 및 저장위치로부터 추출된 비밀값을 해쉬함수에 적용하여 해쉬값을 산출한 후 제1 코드 내 해쉬값과 비교하여, 클라이언트 장치(100)의 인증을 완료할 수 있다.
- [109] 이때 상술한 인증 수행을 위해, 클라이언트 장치(100)와 검증 장치(300)의 해쉬 함수는 동일한 함수에 해당할 수 있다.
- [110] 이하에서는, 검증 장치(300)의 클라이언트 장치(100)의 세부코드 기반의 식별 정보의 저장위치를 탐색하는 구체적인 방법에 대하여 설명한다.
- [111] 세부코드추출부(320)는 상기 제1코드에 포함된 복수의 세부코드를 추출한다. 상기 제1 코드는 복수의 세부코드를 특정한 규칙에 따라 결합하여 생성
- [112] 되는 것이다. 검증장치(300)의 세부코드추출부(320)는 클라이언트 장치(100)와 동일한 세부코드결합함수를 포함하여, 세부코드추출부(320)는 세부코드결합함수를 적용하여 제1코드에서 복수의 세부코드를 추출할 수 있다. 예를 들어, 클라이언트 장치(100)에서 두 개의 세부코드(즉, 제1세부코드 및 제2세부코드)가 결합된 제1 코드를 생성하는 경우, 세부코드추출부(220)는 제1코드의 문자배열에서 세부코드결합함수를 적용하여 제1세부코드 및 제2세부코드를 분리해낼 수 있다.
- [113] 그리고 인증정보탐색부(230)는 복수의 세부코드를 기반으로 클라이언트 장치(100)의 저장위치를 탐색한다. 인증정보탐색부(230)가 각각의 세부코드를 기반으로 인증정보의 저장위치를 탐색하는 방식으로는 다양한 방식이 적용될 수 있다. 인증정보탐색부(230)가 복수의 세부코드를 기반으로 저장위치를 탐색하기 위해 세부코드 간에는 상관관계를 포함할 수 있다.

- [114] 제1 코드가 제1세부코드 및 제2세부코드로 구성되는 경우, 세부코드 간에 상관관계를 가지는 일 실시예로, 인증정보탐색부(230)는 제1세부코드에 대응하는 탐색시작 지점을 결정하고, 상기 탐색시작지점으로부터 제2세부코드에 대응하는 탐색경로에 따라 이동한 지점을 실제코드의 인증정보의 저장위치로 찾을 수 있다. 즉, 상기 세부코드는, 저장위치탐색의 시작지점을 설정하는 제1세부코드 및 특정한 탐색방식에 따라, 상기 시작지점으로부터 상기 저장위치로의 탐색경로를 설정하는 제2세부코드를 포함할 수 있다.
- [115] 또한, 다른 일 실시예로, 클라이언트 장치(100)가 단위카운트마다 신규 제1코드를 제공함에 따라, 검증장치(300)는 저장위치 탐색을 위한 제1세부코드와 제2세부코드가 단위카운트의 경과 시마다 변경된다. 검증장치(300)는 각 카운트마다 변경되는 제1세부코드 및 제2세부코드를 기반으로 탐색시작지점과 탐색경로를 설정하여 클라이언트 장치(100)의 인증정보의 저장위치를 탐색할 수 있다.
- [116] 또한, 다른 일 실시예로, 인증정보탐색부(230)는 상관관계를 가지는 복수의 세부코드를 이용하여 인증정보의 저장위치를 찾기 위해, 저장위치탐색알고리즘을 포함할 수 있다. 저장위치탐색알고리즘은 제1코드에 포함되는 각각의 세부코드 적용 시에 인증정보의 저장위치 탐색이 가능하도록 하는 알고리즘이다.
- [117] 예를 들어, 제1코드로부터 인증정보의 저장위치의 탐색시작지점을 결정하는 제1세부코드와 탐색시작지점으로부터의 저장위치 방향을 제시하는 제2세부코드를 포함하는 경우, 저장위치탐색알고리즘은 제1세부코드에 대응되는 지점에서 제2세부코드에 대응되는 방향을 지시할 때, 해당 위치에 클라이언트 장치(100)의 인증정보가 매칭되는 저장위치가 배치되도록 조절하는 알고리즘이다. 저장위치탐색알고리즘을 이용함에 따라, 검증장치(200)는 제1코드에 포함된 제1세부코드와 제2세부코드가 변경되어도, 해당 클라이언트 장치(100)의 인증정보의 저장위치 또는 저장위치에 매칭된 지점을 찾을 수 있다. 저장위치탐색알고리즘은 다양한 방식이 적용될 수 있으며, 구체적인 예시는 후술한다. 다만, 저장위치탐색알고리즘은 후술되는 예시에 한정되지 않는다.
- [118] 도 7을 참조하면, 저장위치탐색알고리즘이 제1세부코드에 해당하는 M^N 개의 코드가 나열된 트랙을 따라 구름 이동하는 k 각형(k 는 M^N)이며, k 각형의 꼭지점이 제1세부코드 트랙 상에 코드가 배치되는 지점에 대응되면서 이동하는 경우, k 각형의 각 꼭지점이 클라이언트의 인증정보의 저장위치와 매칭되고, 제1세부코드 트랙(즉, 제1트랙)과 k 각형이 대응되는 지점이 제1세부코드에 대응하는 저장위치 탐색시작지점이 될 수 있다. 이 때, 인증정보탐색부(230)는 세부코드추출부(220)에서 추출된 제1세부코드에 대응되는 지점에 k 각형의 꼭지점이 접하도록 k 각형을 구름이동을 적용할 수 있다. 이를 통해, 인증정보탐색부(230)는 k 각형이 접한 제1트랙 상의 위치에서 제2세부코드에

상응하는 각도(예를 들어, k각형의 꼭지점을 향하도록 180도를 M^N 개로 분할한 특정한 각도)로 지시함에 따라, 제1코드에 대응하는 클라이언트 장치(100)의 인증정보가 저장된 저장위치인 k각형의 꼭지점을 탐색할 수 있다.

- [119] 구체적으로, 도 7에서와 같이, 검증장치(300)는 제1세부코드에 대응하는 지점으로 k각형을 구름이동(즉, k각형의 각 꼭지점과 트랙 상의 각 지점이 차례대로 접하도록 하면서 이동)시킨다. 그 후, 검증장치(200)는 제2세부코드에 상응하는 각도 방향을 지시하여 클라이언트 장치(100)의 인증정보의 저장위치에 상응하는 꼭지점을 탐색한다. 예를 들어, 클라이언트 장치B는 상기 검증장치(200) 내 등록하여, ID(Identifier) 및 비밀값을 발급받은 후 2카운트가 경과하였으므로 클라이언트 장치B는 2카운트를 함수값으로 적용한 제2세부코드를 생성하여 검증장치(200)로 제공한다. 검증장치(200)는 k각형과 트랙이 접하는 지점에서 각 꼭지점을 향하는 각도에 각 카운트마다 제2세부코드생성함수에 의해 생성되는 제2세부코드를 매칭하여 저장(즉, n카운트가 적용된 제2세부코드를 k각형의 n카운트만큼 구름이동함에 따라 구름이동된 n번째 꼭지점을 향하는 각도로 매칭하여 저장)하므로, 검증장치(300)는 제2세부코드에 상응하는 각도를 제1세부코드 대응지점에 적용하여 실제코드 저장위치에 대응하는 k각형의 꼭지점을 탐색할 수 있다.
- [120] 한편, 본 발명의 다른 일 실시예로, 제1세부코드 및 제2세부코드는 클라이언트 장치(100)의 인증 정보가 등록된 시점 또는 클라이언트 장치(100)의 인증이 요청된 시점(예를 들어, 클라이언트 장치가 제1코드를 생성한 시점)으로부터 랜덤으로 생성되는 가상보안코드(예를 들어, OTP코드)만큼 부가된 기준 카운트에 대한 코드일 수 있다.
- [121] 구체적인 실시예로, 클라이언트 장치(100)는 가상보안코드를 외부로 출력하지 않고 제1세부코드 및 제2세부코드에 반영하여 생성한다. 검증 장치(300)는 클라이언트 장치(100) 내 시리얼번호(즉, 고유값) 및 클라이언트 장치(100)의 식별정보 중 일부 또는 클라이언트 장치(100)와 클라이언트 장치(100) 내 프로그램의 시리얼번호의 조합을 기반으로 가상보안코드값(예를 들어, OTP코드)를 생성하고, 클라이언트 장치의 인증 정보 등록시점에 상보안코드값을 더한 카운트의 제1세부코드를 생성하고, 가상보안코드값에 대응되는 카운트의 제2세부코드 생성(즉, 가상보안코드 자체를 제2코드로 생성)한다.
- [122] 즉, 제1세부코드 및 제2세부코드는 클라이언트 장치(100)에 의해 클라이언트 장치의 인증 정보가 검증 장치(300)에 등록된 A시점(또는, 검증 장치에 의해 클라이언트 장치에 대한 ID(Identifier)가 발급된 시점)으로부터 가상보안코드값만큼 이동(shifting)된 카운트를 기반으로 생성된다. A시점으로부터 가상보안코드값만큼 이동(Shifting)된 카운트는 생성되는 가상보안코드 값에 따라 현재시점에 대응하는 카운트보다 이전 카운트가 될 수도 있고, 이후 카운트가 될 수도 있다.

- [123] 검증 장치(300)는 수신된 제1코드에 포함된 제1세부코드와 제2세부코드를 저장위치탐색알고리즘에 적용하여 클라이언트 장치(100)의 인증 정보 저장위치(또는 등록위치)를 탐색할 수 있다.
- [124] 또한, 다른 일 실시예로, 검증 장치(300)는 가상보안코드를 기반으로 생성된 제2세부코드에서 가상보안코드를 추출한 후, 가상보안코드생성함수(즉, OTP함수)를 제1코드를 수신한 카운트로부터 특정범위 내의 카운트를 입력하여 산출된 OTP번호 중에 가상보안코드와 일치하는 값이 있는지 여부를 확인한다. 그리고 검증 장치(300)는 제2코드에 제2함수의 역함수를 적용하여 제2코드 생성에 이용된 가상보안코드값(즉, OTP함수값)을 획득하고, 가상보안코드값과 동일한 값을 산출하는 카운트를 찾아낸다.
- [125] 제1코드의 전송시간이나 딜레이에 의해 클라이언트 장치(100)에서 가상보안코드가 생성된 시점과 검증 장치(300)가 가상보안코드를 수신한 시점(정확하게는 가상보안코드를 포함하는 제1코드를 수신한 시점)의 차이가 존재함에 따라 검증 장치(300)가 제1코드를 수신한 카운트와 가상보안코드에 해당하는 OTP번호를 생성한 카운트가 일치하지 않을 수도 있다.
- [126] 그렇기 때문에 검증 장치(300)는 제1코드를 수신한 카운트로부터 오차범위를 허용한다. 이를 통해, 검증 장치(300)는 현시점에 생성된 제1코드가 아닌 이전에 생성된 제1코드로 클라이언트 장치의 인증을 수행하려는 것을 막을 수 있어서, 보안성이 향상될 수 있다.
- [127] 또한, 다른 일 실시예로, 클라이언트 장치(100)는 클라이언트 장치의 인증이 요청된 또는 권한 승인을 요청한 시점에 클라이언트 장치(100) 또는 전용프로그램 내의 시리얼번호(즉, 고유값) 및 클라이언트 장치(100)의 식별 정보 중 일부 또는 양자의 조합을 시드데이터로 사용하여 생성된 가상보안코드값을 더한 카운트에 대응하는 제1세부코드를 생성할 수 있다. 이때, 클라이언트 장치의 식별 정보가 등록된 시점(A시점)과 권한 승인을 요청한 시점(B시점) 간의 카운트 차이와 가상보안코드값을 더한 카운트에 대응하는 제2세부코드를 생성한다. 즉, 제1코드를 생성하는 클라이언트 장치(100) 내 전용프로그램이 제1세부코드와 제2세부코드를 생성하는 수식은 다음과 같다.
- [128]
- [129] 제1세부코드 = $f1(\text{B시점 카운트} + \text{가상보안코드})$
- [130] 제2세부코드 = $f2(\text{B시점 카운트} - \text{A시점 카운트} + \text{가상보안코드})$
- [131] (A시점: 클라이언트 장치의 인증 정보 등록시점, B시점: 클라이언트 장치의 권한 승인 요청 시점의 카운트, 가상보안코드: OTP번호)
- [132]
- [133] 검증 장치(300)는 수신한 제1코드 내의 제1세부코드 및 제2세부코드를 기반으로 클라이언트 장치의 정보가 저장된 위치를 탐색하고, 해당 위치에 함께 저장된 시드데이터(즉, 제1코드생성 전용프로그램 또는 클라이언트 장치의 시리얼번호, 클라이언트 장치 정보, 제1코드생성 전용프로그램 시리얼번호 및

클라이언트 장치 정보 시리얼번호를 조합한 조합시리얼번호 중 제1코드 생성 시에 이용되는 것)을 추출한다. 검증 장치(300)는 시드 데이터를 기반으로 권한 승인 요청 수신시점으로부터 특정카운트 범위 내의 가상보안코드(즉, OTP번호)를 생성한다.

- [134] 그 후, 검증 장치(300)는 제1세부코드 및 제2세부코드를 기반으로 클라이언트 장치의 정보가 저장된 지점을 탐색함에 따라 클라이언트 장치 인증 또는 식별 정보의 등록시점(A시점)을 파악한다. 검증 장치(300)는 클라이언트 장치의 인증 정보 등록시점(A시점)으로부터 권한 승인 요청 수신시점을 기준으로 특정카운트범위 내의 각각의 카운트까지의 카운트 개수와 가상보안코드(즉, OTP번호)의 합에 해당하는 계산값을 각각 산출하고, 상기 각각의 계산값 중에 제2세부코드에 대응하는 카운트수(즉, 제2코드에 제2함수의 역함수를 적용한 값)와 같은 카운트가 존재하는지 확인한다. 이를 통해, 검증 장치(300)는 제1코드가 정상적으로 제공된 것인지 확인할 수 있다.
- [135] 한편, 검증 장치(300)는 클라이언트 장치(100)에 대한 인증이 완료되면, 후술할 제3 코드 생성에 이용되는 제2 코드를 생성한다(S450).
- [136] 도 6을 참조하면, 먼저 검증 장치(300)는 클라이언트 장치의 인증이 완료되면, 상기 클라이언트 장치에 관한 자격 정보를 생성한다(S451). 이때, 자격 정보는 상기 클라이언트 장치(100)의 식별정보에 매칭되어 저장될 수 있다. 예를 들어, 검증 장치(300)에 저장된 클라이언트 장치(100)의 ID(Identifier) 또는 비밀값에 연결되어 저장될 수 있다. 그렇기 때문에, 검증 장치(300)는 클라이언트 장치(100)의 인증이 완료되면, 해당 인증 정보에 매칭 또는 연결되어 저장된 자격 정보를 추출한다.
- [137] 이때, 자격 정보는 클라이언트 장치(100)의 서비스 장치(200)에 대한 권한 정보를 포함한다. 권한 정보란, 클라이언트 장치(100)가 접근 또는 이용 권한을 갖는 서비스 장치(200)에 대한 정보(예를 들어, 서비스 장치 리스트)뿐만 아니라, 권한과 관련하여, 해당 서비스 장치(200)에서 상기 클라이언트 장치(100)가 접근 또는 이용할 수 있는 범위(Scope)에 대한 정보를 포함한다.
- [138] 한편, 자격 정보의 경우, 해당 자격 정보에 대응되는 자격 ID(Role Identifier) 및 자격 비밀값(Role Secret)이 설정될 수 있다. 상기 자격 ID(Role Identifier) 및 자격 비밀값(Role Secert)은 각각의 클라이언트 장치(100)에 대하여 설정된다. 본 발명의 일 실시예로, 각각의 클라이언트 장치(100)의 자격 ID(Role Identifier) 및 자격 비밀값(Role Secert)은 각각의 클라이언트 장치(100)의 인증 정보의 저장위치에 저장될 수도 있으며, 또는 각각의 클라이언트 장치(100)의 ID에 매칭되어 저장될 수도 있을 것이다. 그러나 이에 제한되는 것은 아니다.
- [139] 다시 도 6을 참조하면, 검증 장치(300)는 인증이 완료된 클라이언트 장치에 관한 자격 정보를 추출한 후, 제1 코드를 기반으로 상기 클라이언트 장치에 관한 해쉬값을 생성한다(S452).
- [140] 즉, 각 검증 장치(300)가 제1 코드를 해쉬함수에 적용하여 해쉬값을 산출한다.

이때, 본 발명의 일 실시예로, 서비스 장치(200)는 검증 장치의 해쉬함수와 동일한 해쉬함수를 포함할 수 있다. 한편, 해쉬값은 제1코드를 기반으로 생성되므로, 클라이언트 장치(100)에 대하여 매칭된다. 상술한 바와 같이, 제1 코드는 각각의 클라이언트 장치(100)의 식별 정보에 기반하여 생성되므로, 각각의 클라이언트 장치(100)의 제1 코드는 상이할 수 밖에 없으며, 따라서 제1 코드를 기반으로 생성된 해쉬값 또는 클라이언트 장치(100)마다 상이하다.

- [141] 한편, 해쉬값을 생성한 후 검증 장치(300)의 제2코드생성부(340)는 생성된 자격 정보 및 해쉬값을 기반으로, 제1 코드에 대한 인증 결과가 반영된 제2 코드를 생성한다. 즉 검증 장치(300)는 제2코드생성함수를 기반으로, 제2 코드를 생성할 수 있다(S453).
- [142] 도 8을 참조하면, 제2 코드는 제1 코드를 해쉬함수에 적용하여 산출된 제2 해쉬값과 해당 클라이언트에 대한 자격 정보(예를 들어, 자격 ID) 및 자격 정보에 관한 비밀(예를 들어, 자격 비밀값)을 해쉬함수에 적용하여 산출된 제3 해쉬값을 포함할 수 있다.
- [143] 제1코드를 기반으로 생성된 해쉬값은 이후 서비스 장치(300)에서 클라이언트 장치(100)에 대한 검증 및 권한을 승인하는데 이용된다. 구체적으로, 서비스 장치(300)는 제3 코드에 포함된 제1코드를 추출하고 해쉬값을 생성한다. 그리고 검증장치(300)에서 클라이언트 장치(100)로부터 수신한 제1코드를 기반으로 생성된 해쉬값과 비교하여, 클라이언트 장치(100)에 대한 인증 및 검증을 수행할 수 있다. 이에 대해서는 자세히 후술하도록 한다.
- [144] 본 발명의 일 실시예로, 클라이언트에 대한 자격 정보를 상기 제2코드생성함수에 적용하여 가상인증코드를 생성한 후 상기 제2 해쉬값과 제3 해쉬값을 결합하여 최종적으로 제2코드를 생성할 수 있다.
- [145] 한편, 도면에 명확히 도시되지는 않았으나, 제2 코드는, 복수의 세부코드를 포함할 수 있다. 이때, 복수의 세부코드는, 상기 검증 장치에 의해 단위 카운트마다 변경되어 생성되는 것이고, 상기 단위카운트는, 특정한 시간간격으로 설정되어, 상기 시간 간격이 경과됨에 따라 변경되는 것일 수 있다. 즉, 클라이언트 장치(100)의 세부코드에 기반하여 제1 코드를 생성하는 것과 마찬가지로, 검증 장치(300)에 의해 생성되는 제2 코드 또한 복수의 세부코드를 포함할 수 있다. 일 실시예로, 상기 제1코드는 복수의 세부코드를 특정한 규칙에 따라 결합하여 생성되는 것이다. 이를 위해, 도면에 명확히 도시되지는 않았으나, 제2코드생성함수는 복수의 세부코드를 조합하는 규칙(즉, 세부코드결합함수)을 포함할 수 있다. 세부코드를 조합하여 가상인증코드를 생성하는 방법에 대해서는, 상술하였는바 생략하도록 한다.
- [146] 한편, 본 발명의 일 실시예로, 제2 코드에 포함된 세부코드는, 서로 상관관계를 가지는 복수의 제1 세부코드 및 제2 세부코드를 포함하고, 상기 제1 세부코드는, 상기 검증장치에서의 상기 클라이언트 장치의 자격 정보에 관한 탐색시작지점을 결정하고, 상기 제2 세부코드는, 상기 탐색시작지점으로부터

상기 자격정보에 관한 탐색경로를 결정할 수 있다. 제1 코드에 포함된 제1 세부코드 및 제2 세부코드가 클라이언트 장치(100)의 인증 정보를 탐색하는데 이용되었다면, 제2 코드에 포함된 제1 세부코드 및 제2 세부코드는, 상기 클라이언트 장치(100)의 자격정보를 탐색하는데 이용될 수 있다.

- [147] 한편, 클라이언트 장치의 자격 정보는 클라이언트 장치의 인증 정보의 저장위치에 저장될 수도 있으며, 또는 실시예에 따라서는 인증 정보의 저장위치에 매칭되거나 또는 연결되어 저장될 수 있다.
- [148] 다시 도 6을 참조하면, 검증 장치(300)는 제1 장치(200_1)가 제2 코드를 기반으로 가상인증코드인 제3 코드를 생성하도록 상기 제2 코드를 제1 장치로 송신한다(S460).
- [149] 한편, 제2 코드는, 제2 코드에 관한 유효시간정보를 더 포함할 수 있다. 이때, 검증 장치(300)는, 제1 장치(200_1)로부터 수신된 제1 코드에 대한 제2 코드의 유효시간이 만료된 경우, 만료된 제2 코드에 관한 갱신을 요청 받으면, 제1 장치로부터 수신된 제1 코드 및 기 저장된 제1 코드의 동일 여부를 판단하여, 상기 클라이언트 장치의 인증을 수행할 수 있다. 이때, 클라이언트 장치의 인증(100)이 완료되면, 제2 코드를 갱신하여, 제1 장치로 송신한다. 이에 대해서는 자세히 후술하도록 한다.
- [150] 도 9는, 서비스 장치(200)에 대한 개략적인 구성도이고, 도 10은, 제1 장치에 의해 수행되는 제1 코드 및 제2 코드를 기반으로 가상인증코드인 제3 코드를 생성하는 방법을 개략적으로 나타낸 순서도이고, 도 11는 제3 코드의 개략적인 구성도이다.
- [151] 도 9를 참조하면, 서비스 장치(200)는, 통신부(210), 제3코드생성부(220), 제1코드추출부(230) 및 자격정보검증부(240)를 포함한다. 한편, 본 명세서에서는, 서비스 장치(200)의 클라이언트 장치(100)의 권한 승인 요청에 따라서 제1 장치 및 제2 장치로 구분되어 설명되나, 이는 발명의 이해를 위해 구분되는 것이다. 즉, 제1 장치(200_1) 및 제2 장치(200_2)는 검증 장치(300)와 연동하는 서비스를 제공하는 장치로, 예를 들어 OAuth 인증 방식에 의할 경우, 각각의 리소스 서버(Resource Server)가 이에 해당할 수 있을 것이다. 한편, 리소스 서버는 동일한 플랫폼에서 제공되는 각각의 서버일 수도 있으나, 서로 다른 플랫폼에서 제공되는 각각의 리소스 서버일 수도 있다. 그러나 이에 제한되는 것은 아니다.
- [152] 도 10을 참조하면, 클라이언트 장치(100)로부터 수신된 가상인증코드의 생성을 위한 소스 코드인 제1 코드를 통신부(210)를 통해 검증 장치(300)로 송신한다(S430).
- [153] 이때 제1 코드는, 클라이언트 장치의 식별 정보를 기반으로 생성되며, 검증 장치(300)에서 제1 코드의 검증을 통해 클라이언트 장치(100)의 권한 부여에 이용된다. 한편, 도면에 명확히 도시되지는 않았으나, 제1 장치는 제3 코드 생성을 위하여, 상기 제1 코드를 메모리(미도시)에 저장할 수 있다.

- [154] 한편, 제1 장치(100_1)는 검증 장치(300)로부터 상기 제1 코드에 대한 인증 결과가 반영된 제2 코드를 수신한다(S460). 이때 제2 코드는, 상기 제1 코드를 기반으로 검증 장치(300)에 의해 생성된 클라이언트 장치(100)에 관한 해쉬값 및 자격 정보를 포함한다.
- [155] 상술한 바와 같이, 클라이언트 장치(100)에 의해 생성된 제1 코드를 기반으로 생성된 해쉬값 및 검증 장치(300)에서 클라이언트 장치(100)의 인증을 완료한 후 추출된 자격 정보가 제2 코드에 포함된다. 이와 관련하여 상술한 바 상세한 설명은 생략한다.
- [156] 구체적으로, 제1 장치(200_1)는 검증 장치(300)로부터 제1 코드에 대한 인증 결과가 반영된 제2 코드를 수신하면, 클라이언트 장치(100)의 해당 제1 장치에 대한 권한을 승인한다. 이때, 제1 장치(200_1)는 자격정보검증부(240)를 통해, 제2 코드 내 클라이언트 장치(100)에 대한 해당 제1 장치에 대한 자격 정보를 검증할 수도 있을 것이다. 보다 상세하게, 자격 정보에 포함된, 클라이언트 장치(100)의 접근 및/또는 이용 권한이 있는 서비스 장치(200)에 해당 제1 장치가 포함되는지를 판단할 것이다. 그리고, 자격 정보를 기반으로, 클라이언트 장치(100)의 해당 제1 장치에 대한 접근 및/또는 이용 권한에 대한 범위(Scope)를 검증할 수도 있을 것이다. 그리고, 자격 검증이 완료되면, 클라이언트 장치(100)의 제1 장치에 대한 권한을 승인할 것이다.
- [157] 도 10을 참조하면, 상기 제1 코드 및 상기 제2 코드를 기반으로 상기 가상인증코드인 제3 코드를 생성한다(S470). 제3 코드는, 서버 간 인증과정에서 이용되는 가상인증코드를 의미한다.
- [158] 한편, 도 11를 참조하면, 본 발명의 일 실시예로, 상기 제3 코드는 상술한 제1 코드 및 제2 코드와 함께 검증 장치(300)로부터 제2 코드를 수신한 시간(Time Stamp) 또는 검증 장치에서의 제2 코드 생성 시간(Time Stamp)를 기반으로 생성될 수 있다.
- [159] 예를 들어, 도 11을 참조하면 제3코드는 검증 장치(300)의 클라이언트 장치(100)에 대한 인증이 완료된 시간(Time Stamp) 또는 검증이 완료된 후 제2코드를 생성한 시간(Time Stamp) 정보를 더 포함할 수 있다.
- [160] 이는, 클라이언트 장치(100)에 대한 검증과 검증 결과를 기반으로 최종적으로 생성된 제3 코드를 통해 각각의 서비스 장치(200)에 대한 클라이언트 장치(100)의 권한 승인이 단위 카운트 또는 기 설정된 카운트 내 완료되지 않는 경우에 클라이언트 장치(100)에 대한 권한을 승인하기 위함이다. 각각의 서비스 장치(200)는 제3 코드 내 인증 완료 시간(Time Stamp) 또는 제2코드의 생성 시간(Time Stamp)를 기반으로, 해당 제3 코드 및 제3코드에 포함된 제2 코드가 권한 승인을 위해 정상적으로 생성된 것인지 여부를 판단할 수 있다. 보다 구체적으로는, 클라이언트 장치(100)의 권한 승인 요청에 상응하여 생성된 제3코드 및 제2코드에 대한 것인지를 판단하기 위함이다. 복수의 서비스 장치(200)에서 클라이언트 장치(100)에 대한 인증 및 권한 승인을 수행하기

위해서는, 검증 장치(300)에서의 클라이언트 장치(100)에 대한 인증 결과가 반영된 제2 코드가 유효한지를 판단해야 한다. 이를 위해 제3 코드에 포함된 생성 시점(Time Stamp)을 기반으로 판단하기 위함이다.

- [161] 도 12은 본 발명의 일 실시예에 따른, 제3 코드 기반의 서버 간 인증 방법을 개략적으로 나타낸 예시도이다.
- [162] 클라이언트 장치(100)가 최초 권한 승인을 요청한 제1 장치의 경우, 검증 장치(200)에 의하여, 해당 클라이언트 장치(100)를 인증하고, 권한을 부여할 수 있었다. 그러나, 도 12를 참조하면, 제1 장치(200_1)에 의해 생성되는 제3 코드의 경우, 클라이언트 장치(100)의 인증 정보와 관련되는 제1 코드 및 자격 정보와 관련되는 제2 코드를 포함하므로, 제1 장치(200_1) 이외의 서비스 장치(200)는 검증 장치(300)의 개입 없이도 클라이언트 장치(100)에 대한 인증 및 권한 승인이 가능하다. 이에 대하여 자세히 후술하도록 한다.
- [163] 또한 본 발명의 다른 실시예로, 도면에 명확히 도시되지는 않았으나, 상기 제3 코드는 클라이언트 장치에 의해 생성될 수도 있다. 이를 위해, 제1 장치(200_1)는 검증 장치(300)로부터 수신한 제2 코드를 클라이언트 장치(100)로 송신할 수 있다. 이때, 제3 코드 생성 방법에 따라서, 제1 장치(200_1)는 검증 장치로부터 제2 코드를 수신한 시간 정보 또는 검증 장치에서의 제2 코드 생성 시간 정보를 제2 코드와 함께 클라이언트 장치(100)로 송신할 수도 있을 것이다. 한편, 클라이언트 장치(100)의 제3 코드 생성방법에 대해서는, 상술한 제1 장치에 의한 제3 코드 생성방법과 생성 주체의 차이점만을 가지므로, 상세한 설명은 생략하도록 한다.
- [164] 한편, 제1 장치는 자격 정보와 관련된 적어도 하나의 제2 장치(200_2)로 제3 코드를 송신한다(S480).
- [165] 본 발명의 일 실시예로, 제1 장치(200_1)는 제3 코드에 포함된 제2 코드의 자격 정보를 기반으로, 클라이언트 장치(100)의 권한 인증이 가능한 적어도 하나의 제2 장치(200_2)를 식별한 후 제2 장치(200_2)로 제3 코드를 송신할 수 있다. 그러나 이에 제한되는 것은 아니다.
- [166] 한편 도 12를 참조하면, 제1 장치(200_1)가 제3 코드를 하나의 제2 장치에 대하여 송신한 것으로 나타나 있지만, 클라이언트 장치(100)의 자격 정보에 근거하여, 서비스 장치 중 복수의 제2 장치(200_2)에 대하여 제3 코드를 송신할 수도 있을 것이다. 이를 통해, 클라이언트 장치(100)는 각각의 서비스 장치(200)의 권한 인증을 위하여, 검증 장치(300)에 접속하지 않아도, 접근 권한을 부여 받을 수 있다.
- [167] 도 13은 본 발명의 일 실시예에 따른, 제3 코드를 기반으로 한 서버 간 인증 방법을 개략적으로 나타낸 순서도이다. 도 14는 본 발명의 일 실시예에 따른, 제3 코드를 기반으로 한 클라이언트 장치에 대한 권한 승인 방법을 개략적으로 나타낸 순서도이고, 도 15는 제3 코드를 기반으로 클라이언트 장치에 대한 권한을 승인하는 방법을 개략적으로 나타낸 순서도이다.

- [168] 도 13을 참조하면, 제2 장치(200_2)는 제1 장치로부터 가상인증코드인 제3 코드를 수신한다(S480). 그리고 제3 코드를 기반으로, 클라이언트 장치(100)의 상기 제2 장치(200_2)에 대한 권한을 승인한다(S490).
- [169] 이때, 도 14를 참조하면, S490 단계는, 상기 제3 코드 내에 포함된 상기 제3 코드의 생성에 사용된 제1 코드를 기반으로 클라이언트 장치에 관한 해쉬값을 생성하고(S491), 상기 생성된 해쉬값과 상기 제3 코드 내에 해쉬값을 비교하여, 상기 클라이언트 장치를 검증한다(S492). 그리고 상기 제3 코드를 기반으로, 상기 클라이언트 장치에 관한 자격 정보를 판단하여 상기 클라이언트 장치의 권한을 승인한다(S493).
- [170] 구체적으로, 제2 장치(200_2)는 제3 코드에 포함된 제1 코드를 추출한다. 그리고 제1 코드를 해쉬함수에 적용하여 해쉬값을 산출한다. 이를 위해, 제2 장치를 비롯한 모든 서비스 장치(200)는 검증 장치(300)와 동일한 해쉬함수를 포함한다. 한편, 해쉬값을 추출한 후 제3 코드 내 제2 코드를 추출하고, 상기 제2 코드에 포함되는 해쉬값을, 제2 장치(200_2)에서의 해쉬함수를 적용하여 산출된 해쉬값과 비교한다. 이때, 두 해쉬값이 일치하면, 클라이언트 장치를 인증하고, 해당 클라이언트 장치에 관한 자격 정보를 판단한다. 상술한 바와 같이, 제2 코드는 자격 정보(예를 들어, 자격 ID 및 자격 비밀번호)를 포함하므로, 상기 자격 정보를 기반으로, 클라이언트 장치(100)의 제2 장치에 대한 권한을 승인한다.
- [171] 한편, 본 발명의 일 실시예로, 제3 코드는, 제1 코드 및 상기 제2 코드와, 제2 코드를 수신한 시간 데이터를 기반으로 생성될 수 있다. 이때, 권한 승인 단계는, 제3 코드를 기반으로, 상기 클라이언트 장치(100)에 관한 자격 정보 및 상기 제2 코드를 수신한 시간을 기반으로, 클라이언트 장치의 권한을 승인할 수 있을 것이다. 즉, 제2 장치(100_2)는, 제2 코드를 수신한 시간 데이터를 기반으로, 제2 코드에 대한 유효성을 검증한 후 제2 코드에 포함된 자격 정보를 기반으로 클라이언트 장치(100)에 대한 권한을 승인할 수 있을 것이다.
- [172] 한편, 도 15를 참조하면, 본 발명의 일 실시예로, 상기 권한 승인 단계(S493)는, 제3 코드를 기반으로, 상기 클라이언트 장치의 접근 가능한 장치에 상기 제2 장치가 포함되는지 여부를 판단하고(S493_a), 제3 코드 내에 포함된 시간데이터 및 제2 코드를 기반으로, 상기 제2 장치에 대한 상기 클라이언트 장치의 자격에 해당하는 권한을 승인할 수 있다(S493_b)
- [173] 보다 상세하게, 자격 정보에 포함된, 클라이언트 장치(100)의 접근 및/또는 이용 권한이 있는 서비스 장치(200)에 해당 제2 장치가 포함되는지를 판단할 것이다. 그리고, 자격 정보를 기반으로, 클라이언트 장치(100)의 해당 제2 장치에 대한 접근 및/또는 이용 권한에 대한 범위(Scope)를 검증할 수도 있을 것이다. 그리고, 자격 검증이 완료되면, 클라이언트 장치(100)의 제2 장치에 대한 권한을 승인할 것이다.
- [174] 한편, 도면에 명확히 도시되지는 않았으나, 서비스 장치(200)는 세부코드추출부(미도시)를 더 포함할 수도 있을 것이다.

- [175] 즉, 검증 장치(300)에 의해 생성된 제2 코드가 복수의 세부코드를 포함하는 경우, 서비스 장치(200)는 상기 세부코드를 추출하여, 자격 정보의 저장위치를 탐색할 수도 있을 것이다. 이는, 제1 코드가 복수의 세부코드를 포함하는 경우, 검증 장치(300)에서의 세부코드를 추출하여, 클라이언트 장치(100)의 인증 정보의 저장위치를 탐색하는 방법과 방식이 유사하므로, 상세한 설명은 생략하도록 한다.
- [176] 한편, 본 발명의 일 실시예로, 제2 코드는, 제2 코드에 관한 유효시간정보를 더 포함할 수 있다. 즉, 도면에 명확히 도시되지는 않았으나, 검증 장치(300)는 제2 코드를 생성할 때, 상기 제2 코드의 유효시간정보를 더 포함할 수도 있다. 이때, 제2 장치(200_2)는 제1 장치(200_1)로부터 수신한 제3 코드 내 제2 코드의 유효시간이 만료되면, 제1 장치(200_1)로 수신한 제3 코드를 반환하여, 상기 제2 코드를 갱신할 것을 요청한다.
- [177] 그리고 제1 장치(200_1)는, 제2 장치(200_2)로부터 만료된 제2 코드의 갱신을 위한 상기 제3 코드를 수신하고, 제3 코드에 포함된 제1 코드를 상기 검증장치(300)로 송신한다. 검증장치(300)는 제1 코드를 기반으로 클라이언트 장치(100)의 인증을 다시 수행한다. 그리고 상기 클라이언트 장치(100)의 인증이 완료되면, 제2 코드를 갱신한 후 상기 갱신된 제2 코드를 상기 제1 장치로 송신하도록 요청할 수 있다. 제2 코드의 갱신 방법은, 제2 코드의 생성 방법과 동일한 바 자세한 설명은 생략하도록 한다.
- [178] 한편, 검증 장치(300)는, 제1 장치(200_1)로 제1 코드를 수신한 경우, 상기 제1 코드를 저장한 후, 상기 제2 장치(200_2)의 제1 장치(200_1)를 통한 제2 코드의 갱신 요청을 수신하면, 저장된 제1 코드와 제1 장치(200_1)로부터 수신한 제1 코드의 직접 비교를 통해 유효성 여부를 확인할 수 있다.
- [179] 한편, 검증 장치(300)에 의한, 제2 코드의 갱신 과정이 중지되거나, 갱신을 허용하지 않으면, 제2 장치(200_2)에서의 클라이언트 장치(100)에 대한 검증 및 권한 부여 과정이 중지된다.
- [180] 한편, 제1 장치(100_1)는 검증 장치(300)로부터 갱신된 제2 코드를 수신하면, 제1 코드, 제2코드 및 상기 갱신된 제2 코드가 수신된 시간데이터를 기반으로 제3 코드를 재생성하여, 제2 장치(100_2)로 다시 송신한다. 이를 통해, 제2 장치(100_2)는 클라이언트 장치(100)에 관한 인증 및 권한 승인 과정을 다시 수행할 수 있을 것이다.
- [181] 도 16은 본 발명의 제2 장치의 클라이언트 장치의 검증 및 권한 승인 정보를 기반으로, 새로운 제3 코드를 생성하는 것을 개략적으로 나타낸 순서도이다.
- [182] 클라이언트 장치(100)에 대한 검증 및 권한 승인이 완료된 제2 장치(200_2)는 해당 클라이언트 장치(100)의 서비스 장치(200)내 또 다른 장치에 대한 인증을 위한 새로운 제3 코드를 생성할 수 있다. 예를 들어, 제1 장치(200_1)의 제3 코드를 기반으로 클라이언트 장치(100)에 제2 장치(200_2)에 대한 인증이 완료되어야만, 클라이언트 장치(300)에 대한 권한을 승인할 수 있는 제3

장치(미도시)가 존재할 수 있다. 이때, 제2 장치(200_2)는 제1 장치(200_1)로부터 수신한 제3 코드를 기반으로, 제2 장치(200_2)에 대한 클라이언트 장치(100)의 검증 및 권한 승인이 완료되었음을 나타내는 정보와 함께 새로운 제3 코드를 생성할 수 있을 것이다.

- [183] 도 16을 참조하면, 클라이언트 장치 검증 성공 및 상기 승인된 권한을 식별하는 정보를 생성하고, 상기 제3 코드 및 상기 식별 정보를 기반으로 제2 장치에 관한 신규 제3 코드를 생성한다.
- [184] 구체적으로, 제2 장치(200_2)는 클라이언트 장치(100)에 대한 제2 장치(200_2)의 검증이 완료된 후 해당 제2 장치(200_2)에 대한 권한 승인이 완료되었음을 인증하는 정보를 생성한다. 그리고 해당 정보를 포함한, 새로운 제3 코드를 생성하여, 서비스 장치(200) 내 클라이언트 장치(100)의 인증이 필요한 또 다른 장치(예를 들어, 제3 장치)로 새로운 제3 코드를 송신한다.
- [185] 이는, 복수의 서비스 장치(300)가 순차적으로 클라이언트 장치(100)에 대한 인증을 필요로 하는 경우, N번째(N은 2이상의 자연수)서비스 장치가 N-1번째 서비스 장치로부터 수신한 제3코드를 기반으로 클라이언트 장치(100)에 대해 N번째 서비스 장치에서의 검증을 완료하고 권한을 승인하였음을 식별하였음을 N+1번째 장치가 인지할 수 있도록 하기 위함이다. 이를 위해 권한 승인이 완료되었음을 인증하는 정보 및 N-1번째 장치로부터 수신한 제3코드를 기반으로 새로운 제3코드를 생성하여 N+1번째 장치로 송신할 수 있다.
- [186] 한편, 위 실시예에서는 복수의 서비스 장치(200)의 클라이언트 장치(100)에 대한 순차적 인증 및 검증 상황을 예시로 설명하였으나, A 서비스 장치(200_A)가 또 다른 B 서비스 장치(200_B)에 대한 클라이언트 장치(100)의 선 검증 및 선 권한 부여를 필요로 하는 경우에도, B 서비스 장치는 새로운 제3 코드를 생성하여, A 서비스 장치로 송신할 수 있다.
- [187] 이상에서 기술한 본 발명의 일 실시예에 가상인증코드 기반의 장치간 인증방법은, 하드웨어인 서버와 결합되어 실행되기 위해 프로그램(또는 어플리케이션)으로 구현되어 매체에 저장될 수 있다.
- [188] 상기 기술한 프로그램은, 상기 컴퓨터가 프로그램을 읽어 들여 프로그램으로 구현된 상기 방법들을 실행시키기 위하여, 상기 컴퓨터의 프로세서(CPU)가 상기 컴퓨터의 장치 인터페이스를 통해 읽힐 수 있는 C, C++, JAVA, 기계어 등의 컴퓨터 언어로 코드화된 코드(Code)를 포함할 수 있다. 이러한 코드는 상기 방법들을 실행하는 필요한 기능들을 정의한 함수 등과 관련된 기능적인 코드(Functional Code)를 포함할 수 있고, 상기 기능들을 상기 컴퓨터의 프로세서가 소정의 절차대로 실행시키는데 필요한 실행 절차 관련 제어 코드를 포함할 수 있다. 또한, 이러한 코드는 상기 기능들을 상기 컴퓨터의 프로세서가 실행시키는데 필요한 추가 정보나 미디어가 상기 컴퓨터의 내부 또는 외부 메모리의 어느 위치(주소 번지)에서 참조되어야 하는지에 대한 메모리 참조관련 코드를 더 포함할 수 있다. 또한, 상기 컴퓨터의 프로세서가 상기 기능들을

실행시키기 위하여 원격(Remote)에 있는 어떠한 다른 컴퓨터나 서버 등과 통신이 필요한 경우, 코드는 상기 컴퓨터의 통신 모듈을 이용하여 원격에 있는 어떠한 다른 컴퓨터나 서버 등과 어떻게 통신해야 하는지, 통신 시 어떠한 정보나 미디어를 송수신해야 하는지 등에 대한 통신 관련 코드를 더 포함할 수 있다.

- [189] 상기 저장되는 매체는, 레지스터, 캐쉬, 메모리 등과 같이 짧은 순간 동안 데이터를 저장하는 매체가 아니라 반영구적으로 데이터를 저장하며, 기기에 의해 판독(reading)이 가능한 매체를 의미한다. 구체적으로는, 상기 저장되는 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있지만, 이에 제한되지 않는다. 즉, 상기 프로그램은 상기 컴퓨터가 접속할 수 있는 다양한 서버 상의 다양한 기록매체 또는 사용자의 상기 컴퓨터상의 다양한 기록매체에 저장될 수 있다. 또한, 상기 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장될 수 있다.
- [190] 본 발명의 실시예와 관련하여 설명된 방법 또는 알고리즘의 단계들은 하드웨어로 직접 구현되거나, 하드웨어에 의해 실행되는 소프트웨어 모듈로 구현되거나, 또는 이들의 결합에 의해 구현될 수 있다. 소프트웨어 모듈은 RAM(Random Access Memory), ROM(Read Only Memory), EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM), 플래시 메모리(Flash Memory), 하드 디스크, 착탈형 디스크, CD-ROM, 또는 본 발명이 속하는 기술 분야에서 잘 알려진 임의의 형태의 컴퓨터 판독가능 기록매체에 상주할 수도 있다.
- [191] 이상, 첨부된 도면을 참조로 하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야의 통상의 기술자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며, 제한적이 아닌 것으로 이해해야만 한다.
- [192] [부호의 설명]
- [193] 100 : 클라이언트 장치
- [194] 110 : 세부코드 생성부
- [195] 120 : 제1코드 생성부
- [196] 130 : 통신부
- [197] 200 : 서비스 장치
- [198] 200_1 : 제1 장치
- [199] 200_2 : 제2 장치
- [200] 210 : 통신부
- [201] 220 : 제3코드 생성부
- [202] 230 : 제1코드 추출부

- [203] 240 : 자격정보검증부
- [204] 300 : 검증 장치
- [205] 310 : 통신부
- [206] 320 : 세부코드추출부
- [207] 330 : 인증정보탐색부
- [208] 340 : 제2코드생성부