(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년04월12일
(11) 등록번호 10-1726348
(24) 등록일자 2017년04월06일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
H04L 9/32 (2013.01)
H04L 63/08 (2013.01)
(21) 출원번호 10-2015-7004318
(22) 출원일자(국제) 2013년07월15일
심사청구일자 2015년02월17일
(85) 번역문제출일자 2015년02월17일
(65) 공개번호 10-2015-0038157
(43) 공개일자 2015년04월08일
(86) 국제출원번호 PCT/CN2013/079413
(87) 국제공개번호 WO 2014/012476
국제공개일자 2014년01월23일
(30) 우선권주장
201210249207.3 2012년07월18일 중국(CN)
(56) 선행기술조사문헌
WO2001067219 A1*
EP01919123 A1*
US20120137353 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
텐센트 테크놀로지(센젠) 컴퍼니 리미티드
중국 광동 518044 센젠 푸티안 디스트릭트 젠싱 로드 에스이지 파크 이스트 2 블록 403호
(72) 발명자
허 창
중국 광동 518044 센젠 푸티안 디스트릭트 젠싱 로드 에스이지 파크 이스트 블록 2 403호
(74) 대리인
리앤목특허법인

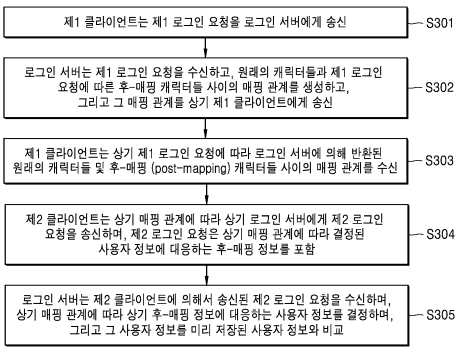
전체 청구항 수 : 총 15 항 심사관 : 정남호

(54) 발명의 명칭 **로그인 인증 방법 및 시스템**

(57) 요 약

로그인 인증을 위한 방법 및 시스템이 개시된다. 상기 방법은: 제1 클라이언트에 의해서 제1 로그인 요청을 로그인 서버로 송신하는 단계, 그리고 원래의 캐릭터들과 상기 제1 로그인 요청에 따라 상기 로그인 서버에 의해서 반환된 후-매핑 캐릭터들 사이의 매핑 관계를 수신하는 단계; 그리고 제2 클라이언트에 의해서 상기 매핑 관계에 따라 상기 로그인 서버로 제2 로그인 요청을 송신하는 단계를 포함하며, 상기 제2 로그인 요청은 상기 매핑 관계에 따라서 결정된 사용자 정보에 대응하는 후-매핑 정보를 포함한다. 본 발명에서의 해결책은 두 클라이언트들에 의한 합동 로그인을 실현하는 것이며, 그래서 심지어 상기 클라이언트들 중 하나가 컴퓨터 바이러스에 감염된다고 하더라도, 어떤 특별한 사용자 정보도 그 감염된 클라이언트를 통해서 얻어질 수 없다. 그래서, 로그인 인증의 보안 그리고 사용자 정보의 보안이 향상될 수 있다.

대 표 도 - 도3



(52) CPC특허분류
H04L 63/0853 (2013.01)

명 세 서

청구범위

청구항 1

로그인 인증을 제공하는 컴퓨터-구현 방법으로서:

하나 이상의 프로세서들 및 메모리를 가진 디바이스에서:

사용자와 연관된 부분적인 사용자 로그인 정보를 포함하는 제1 로그인 요청을 제1 클라이언트 디바이스로부터 수신하는 단계;

상기 제1 로그인 요청에 응답하여:

상기 제1 로그인 요청에 따라 원래의 캐릭터들 및 후-매핑 (post-mapping) 캐릭터들 사이의 매핑 테이블을 생성하고;

상기 매핑 테이블을 상기 제1 클라이언트 디바이스로 제공하며;

상기 각 매핑 테이블을 위한 각 매핑 일련 번호를 생성하고;

그 매핑 일련 번호를 상기 제1 클라이언트 디바이스로 송신하는 단계;

상기 매핑 테이블 및 상기 매핑 일련 번호를 기초로 하여 결정된 후-매핑 정보를 포함하는 제2 로그인 요청을 상기 제1 클라이언트 디바이스와는 상이한 제2 클라이언트 디바이스로부터 수신하는 단계;

상기 제2 클라이언트 디바이스로부터 수신된 제2 로그인 요청 내 매핑 일련 번호를 상기 제1 클라이언트 디바이스로 제공된 상기 매핑 일련 번호에 매칭시킴으로써, 상기 제1 로그인 요청 및 상기 제2 로그인 요청을 연관시키는 단계;

상기 매핑 일련 번호를 기초로 하여, 상기 수신된 제2 로그인 요청에 대응하는 상기 제1 로그인 요청과 연관된 매핑 테이블을 검색하는 단계;

상기 매핑 테이블에 따라 상기 후-매핑 정보에 대응하는 사용자 정보를 결정하는 단계; 그리고

상기 제2 클라이언트 디바이스의 사용자가 로그인을 허용받았는가의 여부를 인증하기 위해 상기 사용자 정보를 미리-저장된 사용자 정보와 비교하는 단계를 포함하는, 로그인 인증 제공 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 사용자와 연관된 상기 부분적인 사용자 로그인 정보는,

상기 제1 클라이언트 디바이스에 의해 상기 사용자를 위해 랜덤으로 생성된 익명의 로그인 ID를 포함하는, 로그인 인증 제공 방법.

청구항 4

제1항에 있어서,

상기 후-매핑 정보는 상기 매핑 테이블에 따라 수정된 사용자 이름 및 패스워드를 포함하는, 로그인 인증 제공 방법.

청구항 5

제1항에 있어서,

상기 후-매핑 정보는 상기 매핑 테이블에 따라 수정된 사용자 이름 또는 패스워드를 포함하는, 로그인 인증 제공 방법.

청구항 6

제1항에 있어서,

상기 후-매핑 정보는 상기 매핑 테이블에 따라 수정된 사용자 이름 또는 패스워드 내에 하나 이상의 캐릭터들을 포함하는, 로그인 인증 제공 방법.

청구항 7

삭제

청구항 8

저장된 명령어들을 구비한 비-일시적 컴퓨터 판독가능 매체로서,

하나 이상의 프로세서들에 의해서 실행될 때에 그 프로세서들로 하여금:

사용자와 연관된 부분적인 사용자 로그인 정보를 포함하는 제1 로그인 요청을 제1 클라이언트 디바이스로부터 수신하고;

상기 제1 로그인 요청에 응답하여:

상기 제1 로그인 요청에 따라 원래의 캐릭터들 및 후-매핑 (post-mapping) 캐릭터들 사이의 매핑 테이블을 생성하고;

상기 매핑 테이블을 상기 제1 클라이언트 디바이스로 제공하며;

상기 각 매핑 테이블을 위한 각 매핑 일련 번호를 생성하고;

그 매핑 일련 번호를 상기 제1 클라이언트 디바이스로 송신하며;

상기 매핑 테이블 및 상기 매핑 일련 번호를 기초로 하여 결정된 후-매핑 정보를 포함하는 제2 로그인 요청을 상기 제1 클라이언트 디바이스와는 상이한 제2 클라이언트 디바이스로부터 수신하고;

상기 제2 클라이언트 디바이스로부터 수신된 제2 로그인 요청 내 매핑 일련 번호를 상기 제1 클라이언트 디바이스로 제공된 상기 매핑 일련 번호에 매칭시킴으로써, 상기 제1 로그인 요청 및 상기 제2 로그인 요청을 연관시키고;

상기 매핑 일련 번호를 기초로 하여, 상기 수신된 제2 로그인 요청에 대응하는 상기 제1 로그인 요청과 연관된 매핑 테이블을 검색하고;

상기 매핑 테이블에 따라 상기 후-매핑 정보에 대응하는 사용자 정보를 결정하고; 그리고

상기 제2 클라이언트 디바이스의 사용자가 로그인을 허용받았는가의 여부를 인증하기 위해 상기 사용자 정보를 미리-저장된 사용자 정보와 비교하는 것을 포함하는,

동작들을 수행하도록 하는, 컴퓨터 판독가능 매체.

청구항 9

삭제

청구항 10

제8항에 있어서,

상기 사용자와 연관된 상기 부분적인 사용자 로그인 정보는,

상기 제1 클라이언트 디바이스에 의해 상기 사용자를 위해 랜덤으로 생성된 익명의 로그인 ID를 포함하는, 컴퓨터 판독가능 매체.

청구항 11

제8항에 있어서,

상기 후-매핑 정보는 상기 매핑 테이블에 따라 수정된 사용자 이름 및 패스워드를 포함하는, 컴퓨터 판독가능 매체.

청구항 12

제8항에 있어서,

상기 후-매핑 정보는 상기 매핑 테이블에 따라 수정된 사용자 이름 또는 패스워드를 포함하는, 컴퓨터 판독가능 매체.

청구항 13

제8항에 있어서,

상기 후-매핑 정보는 상기 매핑 테이블에 따라 수정된 사용자 이름 또는 패스워드 내에 하나 이상의 캐릭터들을 포함하는, 컴퓨터 판독가능 매체.

청구항 14

삭제

청구항 15

하나 이상의 프로세서들; 및

저장된 명령어들을 구비한 메모리를 포함한 시스템으로서,

상기 명령어들은 상기 하나 이상의 프로세서들에 의해서 실행될 때에 그 프로세서들로 하여금:

사용자와 연관된 부분적인 사용자 로그인 정보를 포함하는 제1 로그인 요청을 제1 클라이언트 디바이스로부터 수신하고;

상기 제1 로그인 요청에 응답하여:

상기 제1 로그인 요청에 따라 원래의 캐릭터들 및 후-매핑 (post-mapping) 캐릭터들 사이의 매핑 테이블을 생성하고;

상기 매핑 테이블을 상기 제1 클라이언트 디바이스로 제공하며;

상기 각 매핑 테이블을 위한 각 매핑 일련 번호를 생성하고;

그 매핑 일련 번호를 상기 제1 클라이언트 디바이스로 송신하며;

상기 매핑 테이블 및 상기 매핑 일련 번호를 기초로 하여 결정된 후-매핑 정보를 포함하는 제2 로그인 요청을 상기 제1 클라이언트 디바이스와는 상이한 제2 클라이언트 디바이스로부터 수신하고;

상기 제2 클라이언트 디바이스로부터 수신된 제2 로그인 요청 내 매핑 일련 번호를 상기 제1 클라이언트 디바이스로 제공된 상기 매핑 일련 번호에 매칭시킴으로써, 상기 제1 로그인 요청 및 상기 제2 로그인 요청을 연관시키고;

상기 매핑 일련 번호를 기초로 하여, 상기 수신된 제2 로그인 요청에 대응하는 상기 제1 로그인 요청과 연관된 매핑 테이블을 검색하고;

상기 매핑 테이블에 따라 상기 후-매핑 정보에 대응하는 사용자 정보를 결정하고; 그리고

상기 제2 클라이언트 디바이스의 사용자가 로그인을 허용받았는가의 여부를 인증하기 위해 상기 사용자 정보를 미리-저장된 사용자 정보와 비교하는 것을 포함하는,

동작들을 수행하도록 하는, 시스템.

청구항 16

삭제

청구항 17

제15항에 있어서,

상기 사용자와 연관된 상기 부분적인 사용자 로그인 정보는,

상기 제1 클라이언트 디바이스에 의해 상기 사용자를 위해 랜덤으로 생성된 익명의 로그인 ID를 포함하는, 시스템.

청구항 18

제15항에 있어서,

상기 후-매핑 정보는 상기 매핑 테이블에 따라 수정된 사용자 이름 및 패스워드를 포함하는, 시스템.

청구항 19

제15항에 있어서,

상기 후-매핑 정보는 상기 매핑 테이블에 따라 수정된 사용자 이름 또는 패스워드를 포함하는, 시스템.

청구항 20

제15항에 있어서,

상기 후-매핑 정보는 상기 매핑 테이블에 따라 수정된 사용자 이름 또는 패스워드 내에 하나 이상의 캐릭터들을 포함하는, 시스템.

청구항 21

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 보안의 분야에 관한 것이며, 더 상세하게는 로그인 인증 방법 및 로그인 인증 시스템에 관한 것이다.

배 경 기 술

[0002] 과학 및 기술의 급격한 발전과 함께, 더욱 더 많은 서비스들이 사람들에게 제공될 수 있다. 대응하는 서비스를 효과적으로 그리고 안전하게 활용하기 위해서, 사용자는 관련된 서버에 로그하고 그리고 그 서버에 의해서 인증을 받는 것을 보통 필요로 한다. 그 사용자가 인증을 통과한 이후에, 그 사용자의 보통의 로그인이 실현될 수 있으며, 그리고 그 사용자는 그 대응하는 서비스를 이용할 수 있다. 로그인 인증을 위한 현재의 방법들 중에서 한 가지는 다음과 같다: 사용자가 사용하는 컴퓨터를 통해서 사용자 이름과 패스워드를 사용자가 입력하는 것을 수신하고; 동시에 인증 코드 입력을 수신하며; 그리고 그 입력된 사용자 이름, 패스워드, 및 인증 코드를 서비스-제공 시스템 서버로 보내어 사용자 신원을 인증하도록 한다. 그런 응용 방법에서, 그 사용자의 컴퓨터가 바이러스나 트로이 프로그램에 의해서 침입 당했으며, 그리고 그 바이러스나 트로이 프로그램이 그 사용자의 컴퓨터로의 주요한 로깅을 수행한다면, 그 사용자가 사용자 이름, 패스워드, 인증 코드 등등을 입력할 때에, 그 바이러스나 트로이 프로그램은 그 사용자의 사용자 이름과 패스워드를 쉽게 얻을 것이다. 그래서 보안은 확실하지 않을 수 있다. 심지어 그 사용자의 컴퓨터의 보안을 강화하기 위해서 다양한 보안 수단들이 채택된다고 하더라도, 그 사용자가 사용자 이름과 패스워드를 입력하는 환경은 바이러스나 트로이 프로그램과 동일한 컴퓨터 디바이스이다. 바이러스들이나 트로이 프로그램들이 또한 항상 업그레이드하고 있기 때문에, 이론적으로는, 보안 수단들은 더 높은 기술적인 레벨에서 바이러스나 트로이 프로그램에 의해서 크랙될 수 있을 것이며, 그리고 그 바이러스나 트로이 프로그램은 결국은 사용자의 사용자 이름 및 패스워드를 획득하여, 보안이 손상되는 결과가 된다.

발명의 내용

해결하려는 과제

[0003] 종래 기술에서 존재하는 상기 문제점들을 겨냥하여, 본 발명의 목적은 로그인 인증을 위한 방법 및 로그인 인증을 위한 시스템을 제공하는 것이며, 이것은 로그인 인증의 보안을 효과적으로 향상시킬 수 있으며 그리고 보호받는 사용자에 관한 사용자 정보에 대한 보안을 구비할 수 있다.

과제의 해결 수단

[0004] 위에서 언급된 목적을 달성하기 위해서, 본 발명은 다음과 같은 기술적인 해결책을 사용한다: 로그인 인증 방법은: 제1 클라이언트에 의해서 제1 로그인 요청을 로그인 서버로 송신하는 단계, 그리고 원래의 캐릭터들과 상기 제1 로그인 요청에 따라 상기 로그인 서버에 의해서 반환된 후-매핑 캐릭터들 사이의 매핑 관계를 수신하는 단계, 그리고 제2 클라이언트에 의해서 상기 매핑 관계에 따라 상기 로그인 서버로 제2 로그인 요청을 송신하는 단계를 포함하며, 상기 제2 로그인 요청은 상기 매핑 관계에 따라서 결정된 사용자 정보에 대응하는 후-매핑 정보를 포함한다.

[0005] 로그인 인증 방법은 다음의 단계들을 포함한다: 제1 클라이언트에 의해 송신된 제1 로그인 요청을 로그인 서버에 의해서 수신하는 단계, 원래의 캐릭터들 및 상기 제1 로그인 요청에 따른 후-매핑 캐릭터들 사이의 매핑 관계를 생성하고, 그리고 그 매핑 관계를 상기 제1 클라이언트에게 송신하는 단계; 그리고 제2 클라이언트에 의해 송신된 제2 로그인 요청을 로그인 서버에 의해서 수신하되, 그 제2 로그인 요청은 후-매핑 정보를 포함하는, 수신 단계, 상기 매핑 관계에 따라 상기 후-매핑 정보에 대응하는 사용자 정보를 결정하고, 그 사용자 정보를 미리 저장된 사용자 정보와 비교하는 단계.

[0006] 로그인 인증 시스템은: 제1 로그인 요청을 로그인 서버로 송신하고 그리고 원래의 캐릭터들 및 상기 제1 로그인 요청에 따라 상기 로그인 서버에 의해서 반환된 후-매핑 캐릭터들 사이의 매핑 관계를 수신하는 제1 클라이언트; 그리고 제2 로그인 요청을 상기 매핑 관계에 따라 상기 로그인 서버로 송신하는 제2 클라이언트를 포함하며, 상기 제2 로그인 요청은 상기 매핑 관계에 따라 결정된 사용자 정보에 대응하는 후-매핑 정보를 포함한다.

[0007] 로그인 인증 시스템은: 제1 클라이언트가 송신한 제1 로그인 요청을 수신하고, 원래의 캐릭터들 및 상기 제1 로그인 요청에 따른 후-매핑 캐릭터들 사이의 매핑 관계를 생성하고, 그 매핑 관계를 상기 제1 클라이언트로 송신하고, 제2 클라이언트에 의해 송신된 제2 로그인 요청을 수신하며, 그 제2 로그인 요청은 후-매핑 정보를 포함하며, 상기 매핑 관계에 따라 후-매핑 정보에 대응하는 사용자 정보를 결정하고, 그리고 그 사용자 정보를 미리-저장된 사용자 정보와 비교하는 로그인 서버를 포함한다.

[0008] 본 발명에서의 상기 해결책에 따라서, 제1 클라이언트가 제1 로그인 요청을 로그인 서버에게 송신한 이후에, 상기 로그인 서버는 원래의 캐릭터들 및 상기 제1 로그인 요청에 따른 후-매핑 캐릭터들 사이의 매핑 관계를 생성하며, 그러면 제2 클라이언트는 상기 매핑 관계에 따라 제2 로그인 요청을 상기 로그인 서버에게 송신하며 그리고 상기 제2 로그인 요청은 상기 매핑 관계에 따라서 결정된 사용자 정보에 대응하는 후-매핑 정보를 포함하며, 그리고 이 방법을 기초로 하여, 두 클라이언트 컴퓨터들을 통해서 합동 (joint) 로그인이 실현되며, 이 경우에 상기 제1 클라이언트는 상기 매핑 관계를 단순히 획득하며, 그리고 상기 로그인하는 동안에 상기 제2 클라이언트 내에 포함된 것은 상기 매핑 관계에 따라 결정된 후-매핑 정보이다. 동일한 바이러스나 트로이 프로그램이 두 개의 독립적인 클라이언트들을 동시에 감염시키는 것이 어렵기 때문에, 심지어 컴퓨터 바이러스가 상기 클라이언트들 중 하나를 감염시킨다고 하더라도, 여전히, 어떤 특별한 사용자 정보도 얻어질 수 없다. 그래서, 로그인 인증의 보안은 향상되며 그리고 사용자의 사용자 정보의 보안도 보호된다.

[0009] 몇몇의 실시예들에서, 로그인 서버에 의해서 구현된 로그인 인증을 제공하는 방법은: 하나 이상의 프로세서들 및 메모리를 구비한 디바이스에서: 제1 클라이언트로부터 제1-레벨 로그인 요청을 수신하며, 상기 제1-레벨 로그인 요청은 사용자와 연관된 제1 사용자 로그인 정보를 포함하며; 그리고 상기 제1-레벨 로그인 요청에 응답하여: 상기 제1-레벨 로그인 요청을 위한 각 보안 향상 정보를 생성하고; 상기 보안 향상 정보를 상기 제1 클라이언트 디바이스로 제공하고; 그리고 상기 제1 클라이언트 디바이스와는 상이한 각 클라이언트 기기에 의해서 개시된 제2-레벨 로그인 프로세스를 통해서 상기 사용자를 인증하기 위한 타임 윈도우를 설립하고, 이 경우에 상기 제2-레벨 로그인 프로세스는 사용자가 상기 보안 향상 정보에 따라 제2 사용자 로그인 정보를 제공하도록 요청한다.

[0010] 몇몇의 실시예들에서, 제1 클라이언트 디바이스에 의해서 구현된 로그인 인증을 제공하는 컴퓨터-구현 방법은: 하나 이상의 프로세서들 및 메모리를 가진 디바이스에서: 제1-레벨 로그인 프로세스를 개시하기 위한 사용자 입력을 사용자로부터 수신하는 단계; 부분적인 로그인 정보를 위한 요청을 상기 사용자에게 제시하는 단계; 상기 부분적인 로그인 정보를 상기 사용자로부터 수신하는 단계; 상기 부분적인 로그인 정보를 제1-레벨 로그인 요청에서 로그인 서버에게 송신하는 단계; 상기 제1-레벨 로그인 요청을 위해서 생성된 보안 향상 정보를 상기 로그인 서버로부터 수신하는 단계; 그리고 상기 수신한 보안 향상 정보를 상기 사용자에게 제시하는 단계를 포함한다.

[0011] 몇몇의 실시예들에서, 제2 디바이스에 의해서 구현된 로그인 인증을 제공하는 컴퓨터-구현 방법은: 하나 이상의 프로세서들 및 메모리를 가진 디바이스에서: 제2-레벨 로그인 프로세스를 개시하기 위한 사용자 입력을 사용자로부터 수신하는 단계; 상기 사용자와 연관된 완전한 로그인 정보를 위한 제1 요청, 그리고 상기 디바이스와는 상이한 다른 디바이스로부터 로그인 서버로 이전에 송신되었던 제1-레벨 로그인 요청에 응답하여 상기 로그인 서버에 의해 상기 사용자에게 제공되었던 각 보안 향상 정보를 위한 각 식별 정보용의 제2 요청을 상기 사용자에게 제시하는 단계; 상기 사용자로부터 완전한 로그인 정보를 수신하며 상기 각 보안 향상 정보를 위한 식별 정보를 수신하는 단계로서, 상기 완전한 로그인 정보는 상기 각 보안 향상 정보에 따라 상기 사용자에 의해서 제공되는, 수신 단계; 제2-레벨 로그인 요청을 상기 로그인 서버에게 송신하는 단계로서, 상기 제2-레벨 로그인 요청은 상기 각 보안 향상 정보를 위한 상기 식별 정보 그리고 각 보안 향상 정보에 따라 제공된 상기 완전한 로그인 정보를 포함하는, 송신 단계; 그리고 상기 각 보안 향상 정보 그리고 상기 사용자와 연관된 미리-저장된 원래 로그인 정보를 기초로 하는 검증 프로세스를 상기 완전한 로그인 정보가 통과했는가 또는 실패했는가의 여부를 표시하는 로그인 서버로부터의 로그인 응답을 수신하는 단계를 포함한다.

발명의 효과

[0012] 본 발명의 효과는 본 명세서의 해당되는 부분들에 개별적으로 명시되어 있다.

도면의 간단한 설명

[0013] 도 1은 몇몇의 실시예들에 따른 로그인 인증을 위한 예시적 방법의 흐름도이다.

도 2는 몇몇의 실시예들에 따른 로그인 인증을 위한 예시적 방법의 흐름도이다.

도 3은 몇몇의 실시예들에 따른 로그인 인증을 위한 예시적 방법의 흐름도이다.

도 4는 몇몇의 실시예들에 따른 로그인 인증을 위한 시스템의 개략적인 구조 도면이다.

도 5a 및 도 5b는 몇몇의 실시예들에 따른 로그인 인증을 위한 예시적 방법의 흐름도이다.

도 6a는 몇몇의 실시예들에 따른 로그인 인증을 위한 예시적 방법의 흐름도이다.

도 6b는 몇몇의 실시예들에 따른 로그인 인증을 위한 예시적 방법의 흐름도이다.

도 7은 몇몇의 실시예들에 따른 로그인 인증의 방법을 구현하기 위한 시스템의 블록 도면이다.

발명을 실시하기 위한 구체적인 내용

[0014] 본 발명에서의 해결책은 하나 또는 그 이상의 바람직한 실시예들과 결합하여 이하에서 상세하게 설명될 것이다. 이어지는 설명에서, 본 발명에서 로그인 인증을 위한 방법의 다양한 실시예들이 먼저 설명될 것이며, 그리고 그 후 본 발명에서의 로그인 인증을 위한 시스템의 실시예들이 설명될 것이다.

[0015] 예시적인 실시예 I

[0016] 도 1은 로그인 인증을 위한 방법의 예시적 실시예의 흐름도를 보여준다. 이 예시적인 실시예에서, 예로서 두 클라이언트들의 측에서의 프로세싱 흐름을 취하여 설명한다.

[0017] 도 1에서 보이는 것처럼, 이 예시적인 실시예에서 로그인 인증을 위한 방법은 다음의 단계들을 포함한다:

[0018] 단계 S101: 제1 클라이언트가 제1 로그인 요청을 로그인 서버에게 송신하고 그리고 상기 제1 로그인 요청에 따라 로그인 서버에 의해 반환된 원래의 캐릭터들 및 후-매핑 (post-mapping) 캐릭터들 사이의 매핑 관계를 수신; 그리고

[0019] 단계 S102: 상기 매핑 관계에 따라 결정된 사용자 정보에 대응하는 후-매핑 정보를 포함하는 제2 로그인 요청을

제2 클라이언트에 의해서 상기 매핑 관계에 따라서 상기 로그인 서버에게 송신.

[0020] 이 예시적인 실시예에서의 해결책에 따라, 제1 클라이언트는 제1 로그인 요청을 로그인 서버에게 송신하고 그리고 상기 제1 로그인 요청에 따라 상기 로그인 서버에 의해 생성된 후-매핑 캐릭터들 및 원래의 캐릭터들 사이의 매핑 관계를 얻으며, 그러면 제2 클라이언트는 상기 매핑 관계에 따라 상기 로그인 서버에게 제2 로그인 요청을 송신하며 그리고 상기 제2 로그인 요청은 상기 매핑 관계에 따라 결정된 사용자 정보에 대응하는 후-매핑 정보를 포함한다. 이 로그인 방법을 기초로 하여, 두 클라이언트들의 결합을 통해서 로그인이 실현된다. 동일한 바이러스 또는 트로이 프로그램이 두 개의 독립적인 클라이언트들을 동시에 감염시키는 것이 어렵기 때문에, 혹시 컴퓨터 바이러스가 상기 클라이언트들 중 하나를 감염시킨다고 하더라도, 여전히 어떤 특별한 사용자 정보도 상기 바이러스 또는 트로이 프로그램에 의해서 얻어질 수 없다. 그래서, 로그인 인증의 보안이 향상되고 그리고 그 사용자의 사용자 정보의 보안이 보호받는다.

[0021] 이 경우에, 상기 로그인 서버가 상기 매핑 관계를 생성할 때에, 상기 매핑은 기계-기반의 의사-랜덤 (pseudo-random) 생성기에 따라서 생성될 수 있다. 추가로, 상기 언급된 매핑 관계를 생성할 때에, 상기 로그인 서버는 그 매핑 관계에 대응하는 매핑 관계 일련 번호를 더 생성할 수 있으며 그리고 상기 언급된 매핑 관계를 상기 제1 클라이언트로 송신하면서, 송신하기 이전에 또는 송신한 이후에 그 매핑 관계 일련 번호를 상기 제1 클라이언트로 송신할 수 있다. 상기 제1 클라이언트는 상기 로그인 서버에 의해서 반환된 상기 매핑 관계 일련 번호를 수신하며, 그리고 상기 제2 클라이언트가 제2 로그인 요청을 상기 로그인 서버로 송신할 때에, 그 제2 로그인 요청은 상기 제1 클라이언트가 수신한 상기 언급된 매핑 관계 일련 번호를 더 포함할 수 있다. 상기 제2 로그인 요청을 수신한 이후에, 상기 로그인 서버는 상기 제2 로그인 요청 내 상기 매핑 관계 일련 번호에 따라 대응하는 매핑 관계를 결정하며, 그리고 그 결정된 매핑 관계에 따라 상기 제2 로그인 요청 내 상기 후-매핑 정보에 대응하는 사용자 정보를 결정한다. 로그인 서버는 그 사용자 정보를 미리-저장된 사용자 정보와 비교하여, 상기 제2 클라이언트의 사용자가 로그인이 허용되는가의 여부를 인증하도록 한다.

[0022] 특별한 예들 중 하나의 예에서, 상기 언급된 사용자 정보는 사용자 패스워드를 포함할 수 있으며, 따라서, 상기 후-매핑 정보는 상기 언급된 매핑 관계를 기초로 하여 결정된 상기 사용자 패스워드에 대응하는 후-매핑 패스워드를 포함할 수 있다. 다른 말로 하면, 상기 제2 클라이언트가 상기 제2 로그인 요청을 송신할 때에, 상기 사용자 패스워드는 상기 언급된 매핑 관계에 따라서 암호화될 수 있다.

[0023] 다른 특별한 예에서, 상기 사용자 정보는 사용자 이름을 포함할 수 있으며, 그리고 따라서, 상기 언급된 후-매핑 정보는 상기 매핑 관계를 기초로 하여 결정된 것과 같은 이 사용자 이름에 대응하는 후-매핑 사용자 이름을 포함할 수 있다. 다른 말로 하면, 상기 제2 클라이언트가 상기 제2 로그인 요청을 송신할 때에, 그 사용자 이름은 상기 언급된 매핑 관계에 따라서 암호화될 수 있다.

[0024] 다른 특별한 예에서, 상기 언급된 사용자 정보는 사용자 이름 및 사용자 패스워드를 동시에 포함할 수 있으며, 따라서, 상기 언급된 후-매핑 정보는 상기 언급된 매핑 관계를 기초로 하여 결정된 상기 사용자 이름 및 사용자 패스워드에 대응하는 후-매핑 사용자 이름 및 후-매핑 패스워드를 포함할 수 있다. 다른 말로 하면, 상기 제2 클라이언트가 상기 제2 로그인 요청을 송신할 때에, 그 사용자 이름 및 사용자 패스워드는 상기 언급된 매핑 관계에 따라서 동시에 암호화될 수 있다.

[0025] 물론, 상이한 실제적인 애플리케이션 요구들에 따라서, 상기 언급된 사용자 정보는 다른 유형의 정보를 더 포함할 수 있으며, 그리고 그 특별한 유형들은 적용될 시스템들의 유형에 관련된다. 예를 들면, 학생 관리 시스템에 로그하기 위해서, 사용자 정보는 학생 ID 번호, 이름, 학급 등과 같은 정보를 옵션으로 포함한다. 기업 종업원 정보 관리 시스템에 로그하기 위해서, 사용자 정보는 부서, 종업원 수, 이름, 근속 기간 등과 같은 정보를 옵션으로 포함한다. 상이한 특별한 유형의 애플리케이션 시스템들에 따라서 차이들이 존재하며, 여분의 설명이 여기에서 만들어지지 않을 것이다.

[0026] 예시적인 실시예 II

[0027] 도 2는 본 발명에서 로그인 인증을 위한 방법의 예시적인 실시예의 개략적인 흐름도를 보여준다. 이 예시적인 실시예에서, 예로서 로그인 서버 측에서 프로세싱 흐름을 취하여 설명이 이루어진다.

[0028] 도 2에서 보이는 것처럼, 이 실시예에서 로그인 인증을 위한 방법은 다음의 단계들을 포함한다:

[0029] 단계 S201: 로그인 서버가 상기 제1 클라이언트에 의해 송신된 제1 로그인 요청을 수신한다.

[0030] 단계 S202: 상기 로그인 서버가 원래의 캐릭터들 및 상기 제1 로그인 요청에 따른 후-매핑 캐릭터들 사이의 매

핑 관계를 생성하고, 그리고 그 매핑 관계를 상기 언급된 제1 클라이언트에게 송신한다.

[0031] 단계 S203: 로그인 서버는 제2 클라이언트에 의해 송신된 제2 로그인 요청을 수신하며, 그 제2 로그인 요청은 후-매핑 정보를 포함한다

[0032] 단계 S204: 상기 로그인 서버는 상기 매핑 관계에 따라 상기 후-매핑 정보에 대응하는 사용자 정보를 결정하고 그리고 그 사용자 정보를 미리 저장된 사용자 정보와 비교한다.

[0033] 이 경우에, 상기 로그인 서버가 상기 언급된 매핑 관계를 생성할 때에, 그 매핑은 기계-기반의 의사-랜덤 생성기에 의해서 생성될 수 있다. 추가로, 상기 언급된 매핑 관계를 생성할 때에, 상기 로그인 서버는 상기 매핑 관계에 대응하는 매핑 관계 일련 번호를 더 생성할 수 있으며, 그리고 상기 언급된 매핑 관계를 송신할 때에, 송신하기 이전에, 또는 송신한 이후에 그 매핑 관계 일련 번호를 상기 제1 클라이언트로 송신할 수 있다. 상기 제1 클라이언트가 상기 로그인 서버에 의해서 반환된 상기 매핑 관계 일련 번호를 수신한 이후에, 그리고 상기 제2 클라이언트가 제2 로그인 요청을 상기 로그인 서버에게 송신할 때에, 그 제2 로그인 요청은 상기 제1 클라이언트가 수신한 상기 언급된 매핑 관계 일련 번호를 더 포함할 수 있다. 상기 제2 로그인 요청을 수신한 이후에, 로그인 서버는 상기 제2 로그인 요청 내 매핑 관계 일련 번호에 따라 대응하는 매핑 관계를 결정하며, 그리고 그 결정된 매핑 관계에 따라 상기 제2 로그인 요청 내 상기 후-매핑 정보에 대응하는 사용자 정보를 결정한다. 그러면 상기 로그인 서버는 그 사용자 정보를 미리-저장된 사용자 정보와 비교하여, 상기 제2 클라이언트의 사용자가 로그인이 허용되는지의 여부를 인증하도록 한다.

[0034] 특별한 예들 중 하나의 예에서, 상기 언급된 사용자 정보는 사용자 패스워드를 포함할 수 있으며, 따라서, 상기 언급된 후-매핑 정보는 상기 언급된 매핑 관계를 기초로 하여 결정된 상기 사용자 패스워드에 대응하는 후-매핑 패스워드를 포함할 수 있다. 다른 말로 하면, 상기 제2 클라이언트가 상기 제2 로그인 요청을 송신할 때에, 상기 사용자 패스워드는 상기 언급된 매핑 관계에 따라 암호화될 수 있다.

[0035] 다른 특별한 예에서, 상기 언급된 사용자 정보는 사용자 이름을 포함할 수 있으며, 따라서, 상기 후-매핑 정보는 상기 언급된 매핑 관계를 기초로 하여 결정된 상기 사용자 이름에 대응하는 후-매핑 사용자 이름을 포함할 수 있다. 다른 말로 하면, 상기 제2 클라이언트가 상기 제2 로그인 요청을 송신할 때에, 상기 사용자 이름은 상기 언급된 매핑 관계에 따라서 다만 암호화될 수 있다.

[0036] 다른 특별한 예에서, 상기 언급된 사용자 정보는 사용자 이름과 사용자 패스워드를 동시에 포함할 수 있으며, 따라서, 상기 언급된 후-매핑 정보는 상기 매핑 관계를 기초로 하여 결정된 사용자 이름 및 사용자 패스워드에 대응하는 후-매핑 사용자 이름 및 후-매핑 패스워드를 포함할 수 있다. 다른 말로 하면, 상기 제2 클라이언트가 상기 제2 로그인 요청을 송신할 때에, 사용자 이름 및 사용자 패스워드는 상기 언급된 매핑 관계에 따라서 동시에 암호화될 수 있다.

[0037] 물론, 상이한 실제적인 애플리케이션 요구들에 따라서, 상기 언급된 사용자 정보는 다른 유형의 정보를 더 포함할 수 있으며, 그리고 그 특별한 유형들은 적용될 시스템들의 유형에 관련된다. 예를 들면, 학생 관리 시스템에 로그하기 위해서, 사용자 정보는 학생 ID 번호, 이름, 학급 등과 같은 정보를 옵션으로 포함한다. 기업 종업원 정보 관리 시스템에 로그하기 위해서, 사용자 정보는 부서, 종업원 인원수, 이름, 근속 기간 등과 같은 정보를 포함할 수 있으며, 그리고 상이한 특별한 유형의 애플리케이션 시스템들에 따라서 차이들이 존재할 수 있을 것이며, 그리고 여분의 설명이 여기에서 만들어지지 않을 것이다.

[0038] 예시적인 실시예 3

[0039] 도 3은 본 발명에서 로그인 인증을 위한 방법의 예시적인 실시예의 개략적인 흐름도를 보여준다. 이 예시적인 실시예에서, 예로서 두 개의 클라이언트들 및 하나의 로그인 서버의 상호작용 프로세스를 취하여 설명이 이루어진다.

[0040] 도 3에서 보이는 것처럼, 이 실시예에서 로그인 인증을 위한 방법은 다음의 단계들을 포함한다:

[0041] 단계 S301: 제1 클라이언트는 제1 로그인 요청을 로그인 서버에게 송신한다.

[0042] 단계 S302: 상기 로그인 서버는 상기 제1 클라이언트에 의해 송신된 상기 제1 로그인 요청을 수신하고, 원래의 캐릭터들과 제1 로그인 요청에 따른 후-매핑 캐릭터들 사이의 매핑 관계를 생성하고, 그리고 그 매핑 관계를 상기 제1 클라이언트에게 송신한다.

[0043] 단계 S303: 상기 제1 클라이언트는 상기 제1 로그인 요청에 따라 로그인 서버에 의해 반환된 원래의 캐릭터들

및 후-매핑 (post-mapping) 캐릭터들 사이의 매핑 관계를 수신한다.

[0044] 단계 S304: 제2 클라이언트는 상기 매핑 관계에 따라 상기 로그인 서버에게 제2 로그인 요청을 송신하며, 제2 로그인 요청은 상기 매핑 관계에 따라 결정된 사용자 정보에 대응하는 후-매핑 정보를 포함한다.

[0045] 단계 S305: 상기 로그인 서버는 상기 제2 클라이언트에 의해서 송신된 제2 로그인 요청을 수신하며, 상기 매핑 관계에 따라 상기 후-매핑 정보에 대응하는 사용자 정보를 결정하며, 그리고 그 사용자 정보를 미리 저장된 사용자 정보와 비교한다.

[0046] 이 경우에, 상기 로그인 서버가 상기 언급된 매핑 정보를 생성할 때에, 상기 매핑 관계는 기계-기반의 의사-랜덤 생성기에 의해서 생성될 수 있다. 상기 언급된 매핑 관계를 생성할 때에, 상기 로그인 서버는 상기 매핑 관계에 대응하는 매핑 관계 일련 번호를 더 생성할 수 있으며, 그리고 상기 언급된 매핑 관계를 상기 제1 클라이언트에게 송신하는 것과 동시에 또는 그 이전에 또는 그 이후에 상기 매핑 관계 일련 번호를 상기 제1 클라이언트로 송신할 수 있다.

[0047] 특별한 예들 중 하나의 예에서, 상기 언급된 매핑 관계는 캐릭터 매핑 테이블 방식으로 구체화될 수 있으며, 따라서, 상기 언급된 매핑 관계 일련 번호는 패스워드 테이블 일련 번호로서 언급될 수 있으며, 그리고 그 패스워드 테이블 일련 번호 및 캐릭터 매핑 테이블은 패스워드 테이블을 같이 형성할 수 있다. 패스워드 테이블의 특별한 예는 다음의 표 1의 테이블에서 보여진다.

표 1

[0048]

패스워드 테이블 일련 번호	2012000001	
캐릭터 매핑 테이블	원래 캐릭터	후-매핑 캐릭터
	0	7
	1	3
	2	8
	3	2
	4	5
	5	1
	6	9
	7	4
	8	0
	9	6

[0049] 위의 표에서 보이는 것처럼, 상기 패스워드 테이블 일련 번호는 현재의 로그인 동안에 사용된 패스워드 테이블을 식별하는데 있어서 사용된다. 일반적으로, 동일한 패스워드 테이블 번호가 단 한번만 사용될 것이며 그리고 다른 로그인 프로세스들에서는 다시 사용되지 않을 것이다. 채택된 패스워드 테이블을 식별하기 위해서 상기 패스워드 테이블 일련 번호가 주로 사용되기 때문에, 그 패스워드 테이블 일련 번호는 동작하는 번호 시스템을 기초로 하여 생성될 수 있다.

[0050] 상기 언급된 캐릭터 매핑 테이블은 원래의 캐릭터들과 후-매핑 캐릭터들 사이의 매핑 관계를 설명하는데 있어서 사용된다. 그 테이블은 암호화된 캐릭터를 대응하는 실제의 또는 비-암호화된 캐릭터로 변환하기 위한 매핑 테이블이다. 간단한 설명을 위해서, 상기 테이블은 원래의 캐릭터 및 후-매핑 캐릭터를 위한 예로서 숫자들만을 사용한다. 캐릭터 매핑 테이블을 실제로 생성할 때에, 상기 원래의 캐릭터들 및 후-매핑 캐릭터들은 알파벳들, 숫자들, 특수한 심볼들, 중국어 캐릭터들 등을 포함하는 임의 유형의 정보일 수 있다.

[0051] 캐릭터 매핑 테이블은 기계-기반의 의사-랜덤 생성기에 따라서 생성될 수 있다. 예를 들면, 상기 방법들 중 하나의 방법에서, 원래의 캐릭터들을 결정하고 그것들을 연속하게 배치한 이후에, 그 연속으로 배치된 원래의 캐릭터들의 시퀀스 순서는 랜덤으로 또는 의사-랜덤으로 재배치될 수 있으며, 그리고 그 재배치된 시퀀스 내의 캐릭터들은 원래의 시퀀스 순서로 배치된 캐릭터들과 1 대 1 대응으로 놓여져서, 상기 원래의 캐릭터들 그리고 상기 후-매핑 캐릭터들 사이의 매핑 관계를 실현하도록 한다.

[0052] 다른 예시적인 방법에서, 상기 모든 원래의 캐릭터들 중 하나의 사본은 백업 캐릭터들로서 만들어진다. 매핑되지 않은 캐릭터는 원래의 캐릭터들로부터 하나씩 연속하여 선택된다. 각 선택된 매핑되지 않은 캐릭터에 대해서, 백업 캐릭터들 내에서 선택되지 않은 캐릭터들로부터 한 캐릭터가 상기 선택되지 않은 캐릭터의 후-매핑 캐릭터로서 랜덤으로 선택된다. 예를 들어, 원래의 캐릭터들이 "A, B, C, D ……"로 라벨이 붙여진다고 가정

하면,, 그러면 상기 백업 캐릭터들은 "A', B', C', D' ……"로 라벨이 붙여진다. 모든 원래의 캐릭터들을 결정한 이후에, (A와 같은) 어떤 캐릭터를 선택할 때에, 캐릭터 A의 후-매핑 캐릭터로서 사용되도록 (C'와 같은) 캐릭터가 모든 백업 캐릭터들로부터 랜덤으로 선택된다. 그 후 (B와 같은) 다른 캐릭터가 원래의 캐릭터들로부터 선택되며, 그리고 상기 백업 캐릭터들로부터 캐릭터 C'를 제거한 이후에 모든 남아있는 캐릭터들로부터 (A'와 같은) 캐릭터가 캐릭터 B의 후-매핑 캐릭터로서 사용되도록 랜덤으로 선택된다. 상기 프로세스는 원래의 캐릭터들 모두를 매핑하는 것이 완료될 때까지 계속된다. 물론, 실제의 요구 사항들에 따라서, 하나의 원래 캐릭터가 하나의 후-매핑 캐릭터에 유일하게 대응하고, 그리고 하나의 후-매핑 캐릭터가 하나의 원래 캐릭터에 유일하게 대응하는 한은, 캐릭터 매핑 테이블을 생성하기 위해서 다른 방법들 또한 채택될 수 있다

[0053] 상기 제2 클라이언트에 의해서 송신된 상기 제2 로그인 요청에서 상기 후-매핑 캐릭터들로 채워질 사용자 패스워드를 상기 서버가 필요로 한다고 가정한다. 위의 테이블에서 보이는 것처럼, 상기 제2 로그인 요청에서의 사용자 패스워드가 "7"이라고 가정하면, 그러면 사용자 패스워드 "7"이 실제로 암호화된 패스워드, 즉, 후-매핑 캐릭터이며, 그리고 그것의 대응하는 원래의 캐릭터는 "0"이어야 한다. 상기 제2 로그인 요청 내의 패스워드가 "965328"이라고 가정하면, 그러면 이 "965328"은 또한 후-매핑 캐릭터들을 포함하는 암호화된 패스워드이며, 그리고 그것의 대응하는 실제 패스워드는 "694132"이어야 한다.

[0054] 다음은 몇몇의 실시예들에 따라 상기 패스워드 테이블 번호를 생성하기 위한 예시적인 코드 세그먼트 그리고 C++ 언어로 된 캐릭터 매핑 테이블이다.

[0055] #include <map>

[0056] #include <string>

[0057] #include <list>

[0058] using namespace std;

[0059] class PasswordCode

[0060] {public:

[0061] int m_nID; //패스워드 테이블 번호

[0062] map<char,char> m_mapCode; //캐릭터 매핑 테이블

[0063] void Init()

[0064] { static int nPasswordId = 0; //동작 번호로 사용된다

[0065] m_nID = nPasswordId++; //패스워드 테이블 번호를 얻는다, 여기에서 증가하는 동작 번호가 사용된다

[0066] //캐릭터 매핑 테이블 생성

[0067] list<char> listSource; //보조 캐릭터 추출 목록

[0068] //패스워드 캐릭터 세트 준비

[0069] for(char i='0' ; i <= '9' ; ++i)

[0070] { listSource.push_back(i);

[0071] }

[0072] for(char j='0' ; j <= '9' ; ++j)

[0073] { //캐릭터 세트 시퀀스를 랜덤으로 순서를 흩트린다

[0074] if(listSource.size() > 1)

[0075] { int nIndex = rand() % listSource.size();

[0076] list<char>::iterator itor = listSource.begin();

[0077]
```
                for( int k = 0 ; k < nIndex ;k++)
```
[0078]
```
                { itor++;
```
[0079]
```
                }
```
[0080]
```
                m_mapCode[*itor]=j;
```
[0081]
```
                listSource.erase(itor);
```
[0082]
```
            }
```
[0083]
```
            else
```
[0084]
```
            {m_mapCode[listSource.front()] = j;
```
[0085]
```
            }
```
[0086]
```
        }
```
[0087]
```
    //완료됨, 순서가 흩트러진 캐릭터 세트가 데이터 구조 맵 내에 저장된다, 즉, m_mapCode 멤버
```
[0088]
```
    }
```
[0089]
```
    string Decode(string strOld)
```
[0090]
```
    {  string strDecode;
```
[0091]
```
       string::iterator itor;
```
[0092]
```
         for(itor = strOld.begin();itor!=strOld.end();++itor)
```
[0093]
```
         {  strDecode += m_mapCode[*itor];
```
[0094]
```
         }
```
[0095]
```
         return strDecode;
```
[0096]
```
      }
```
[0097]
```
    };
```
[0098]
```
    //새로운 패스워드 테이블을 얻기 위한 방법
```
[0099]
```
    PasswordCode myPassword;
```
[0100]
```
    myPassword.Init();
```

[0101] 상기 제1 클라이언트가 상기 로그인 서버에 의해서 반환된 패스워드 테이블을 얻은 이후에, 상기 제2 클라이언트는 이 패스워드 테이블에 따라서 관련된 로그인 정보를 입력하고 그리고 제2 로그인 요청을 상기 로그인 서버에게 송신한다. 이 제2 로그인 요청은 상기 언급된 패스워드 테이블에 의해서 결정된 후-매핑 정보를 포함한다. 몇몇의 실시예들에서, 필요에 따라, 이 제2 로그인 요청은 상기 로그인 서버가 필요로 하는 특별한 유형들을 위한 대응 후-매핑 정보만을 포함할 수 있다. 예를 들면, 상기 로그인 서버가 사용자 패스워드에 대응하는 후-매핑 패스워드만을 필요로 하는 경우에, 상기 로그인 서버로 송신된 제2 로그인 요청에 포함된 패스워드는 상기 언급된 패스워드 테이블을 기초로 하는 상기 원래의 사용자 패스워드에 대응하는 후-매핑 패스워드이다. 그런 사용자 이름 등과 같은 다른 정보를 위해서, 상기 제2 로그인 요청 내에 포함된 정보는 상기 언급된 패스워드 테이블을 기초로 하여 매핑되지 않은 원래의 정보를 포함한다.

[0102] 보관-관련된 요소들을 고려할 때에, 보안을 추가로 향상시키기 위해서, 상기 제2 클라이언트가 상기 로그인 서버로 송신한 상기 제2 로그인 요청은 상기 언급된 패스워드 테이블을 기초로 하는 후-매핑 정보를 모든 사용자 정보용으로 포함할 것을 필요로 할 수 있다. 예를 들면, 상기 사용자 정보가 사용자 이름 및 사용자 패스워드를 포함한다면, 상기 제2 로그인 요청 내에 포함된 사용자 이름은 상기 언급된 패스워드 테이블을 기초로 하는 상기 원래의 사용자 이름에 대응하는 후-매핑 사용자 이름이며, 그리고 상기 제2 로그인 요청 내에 포함된 상기 사용자 패스워드는 상기 언급된 패스워드 테이블을 기초로 하는 상기 원래의 사용자 패스워드에 대응하는 후-매핑 패스워드이다. 상기 제2 로그인 요청이 패스워드 테이블 일련 번호를 포함하는 경우에, 제2 로그인 요청 내

그 패스워드 테이블 일련 번호는 상기 로그인 서버가 상기 제1 클라이언트로 송신한 원래의 패스워드 테이블 일련 번호일 것이다.

[0103] 표 1에서 보이는 패스워드 테이블을 감안하여, 어떤 사용자의 계정 번호가 2300223이고 패스워드는 123456이라고 가정한다. 그러면, 표 1에서 보이는 매핑 규칙들을 기초로 하여, 상기 사용자 계정 번호 2300223의 후-매핑 계정 번호는 8277882 이며, 그리고 상기 패스워드 123456의 후-매핑 패스워드는 382519 이다.

[0104] 사용자 계정 번호만이 암호화될 필요가 있는 예시적인 실시예에서, 상기 제2 로그인 요청이 상기 로그인 서버로 송신되기 이전에 관련된 사용자 정보가 제공될 때에, 사용자에 의해서 입력된 사용자 계정 번호는 후-매핑 계정 번호 8277882이며, 그리고 입력 사용자 패스워드는 상기 원래의 패스워드 123456 이다. 동시에, 사용자는 패스워드 테이블 일련 번호 2012000001를 또한 입력한다. 그런 관련된 정보를 입력한 이후에, 상기 제2 클라이언트가 로그인 서버로 송신한 상기 제2 로그인 요청 내에 포함된 패스워드 테이블 일련 번호는 2012000001 이며, 포함된 사용자 계정 번호는 후-매핑 계정 번호 8277882 이며, 그리고 상기 포함된 사용자 패스워드는 원래의 사용자 패스워드 123456 이다. 로그인 서버가 상기 제2 로그인 요청을 수신하고 패스워드 테이블 번호 2012000001에 따른 대응하는 패스워드 테이블을 얻은 이후에, 로그인 서버는 이 패스워드 테이블을 기초로 하는 후-매핑 계정 8277882 에 대응하는 원래의 사용자 계정 번호 2300223 을 결정할 필요가 있으며, 그리고 이 사용자 계정 번호 2300223 및 사용자 패스워드 123456를 상기 로그인 서버에 저장된 계정 번호 및 패스워드와 비교하여, 이 사용자가 로그인을 허용 받는지의 여부를 인증하고 결정하도록 한다.

[0105] 유사하게, 사용자 패스워드만이 암호화될 필요가 있는 예시적인 실시예에서, 상기 제2 로그인 요청이 송신되기 이전에 관련된 사용자 정보가 제공될 때에, 사용자에 의해서 입력된 사용자 계정 번호는 원래의 계정 번호 2300223 이며, 그리고 입력 사용자 패스워드는 후-매핑 패스워드 382519 이다. 동시에, 사용자는 패스워드 테이블 일련 번호 2012000001 을 입력할 수 있다. 그런 관련 정보를 입력한 이후에, 제2 클라이언트가 로그인 서버에게 송신한 제2 로그인 요청 내에 포함된 패스워드 테이블 일련 번호는 2300223 이며, 그리고 포함된 사용자 패스워드는 후-매핑 패스워드 382519 이다. 로그인 서버가 제2 로그인 요청을 수신하고 상기 패스워드 테이블 일련 번호 2012000001 에 따른 대응하는 패스워드 테이블을 얻은 이후에, 로그인 서버는 이 패스워드 테이블을 기초로 하여 후-매핑 패스워드 382519 에 대응하는 원래의 패스워드 123456 을 결정할 필요만이 있을 뿐이며, 그리고 이 사용자 패스워드 123456 및 사용자 계정 번호 2300223 을 상기 로그인 서버에 저장된 계정 번호 및 패스워드와 비교하여, 이 사용자가 로그인이 허용되었는가의 여부를 인증하고 결정하도록 한다.

[0106] 유사하게, 사용자 계정 번호 및 사용자 패스워드 둘 모두가 동시에 암호화될 필요가 있는 예시적인 실시예에서, 상기 제2 로그인 요청이 송신되기 이전에 관련된 사용자 정보가 입력될 때에, 사용자가 입력한 사용자 계정 번호는 후-매핑 계정 번호 8277882 이며, 그리고 입력된 사용자 패스워드는 후-매핑 패스워드 382519 이다. 동시에, 사용자는 패스워드 테이블 일련 번호 2012000001 을 입력할 수 있다. 그런 관련 정보를 입력한 이후에, 상기 제2 클라이언트가 로그인 서버로 송신한 제2 로그인 요청 내에 포함된 패스워드 테이블 일련 번호는 2012000001 이며, 포함된 사용자 계정 번호는 후-매핑 계정 번호 8277882 이며, 그리고 포함된 사용자 패스워드는 후-매핑 패스워드 382519 이다. 로그인 서버가 제2 로그인 요청을 수신하고 패스워드 테이블 번호 2012000001에 따른 대응 패스워드 테이블을 획득한 이후에, 후-매핑 계정 번호 8277882 에 대응하는 원래의 계정 번호 2300223 그리고 이 패스워드 테이블에 기초한 후-매핑 패스워드 382519 에 대응하는 원래의 패스워드 123456 을 결정하고, 그리고 그 사용자 패스워드 123456 및 사용자 계정 번호 2300223 을 자체적으로 저장하는 계정 번호 및 패스워드와 비교하여, 이 사용자가 로그인이 허용될 것인가의 여부를 인증하고 결정하도록 할 것을 필요로 한다.

[0107] 물론, 간단한 설명을 위해서, 상기 언급된 설명은 사용자 계정 번호 및 사용자 패스워드만을 예로서 취하여 기술되었다. 다양한 상이한 애플리케이션 시스템들에서의 실제의 요구 사항들에 따라서, 상기 포함된 사용자 정보는 또한 상이할 수 있다. 예를 들면, 학생 관리 시스템에 로그인하기 위해서, 상기 사용자 정보는 학생 ID 번호, 이름, 학급 등과 같은 정보를 포함할 수 있을 것이다. 기업 종업원 정보 관리 시스템에 로그인하기 위해서, 상기 사용자 정보는 부서, 종업원 인원수, 이름, 종업원 근속 기간 등과 같은 정보를 포함할 수 있을 것이다. 상이한 특별한 유형의 애플리케이션 시스템들에 따라 차이가 존재할 수 있다. 사용자 정보에 관하여, 그 사용자 정보 중의 어느 부분이 후-매핑 모습으로 로그인 서버에 제공되어야만 하는가는 특별한 애플리케이션들의 실제의 요구 사항들을 기초로 하여 결정될 수 있으며, 그리고 그것의 특별한 구현의 나머지 설명은 여기에서 기술되지 않을 것이다.

[0108] 제2 클라이언트가 제출한 제2 로그인 요청을 수신한 이후에, 로그인 서버는 패스워드 테이블 일련 번호에 따른

대응 패스워드 테이블을 발견하고, 그리고 그 후 원래의 실제의 사용자 계정 번호 및 사용자 패스워드를 찾기 위해서 대응 패스워드 테이블을 기초로 하여 후-매핑 계정 번호 및 후-매핑 패스워드에 관한 매핑 및 암호해독을 수행한다. 그러면, 상기 로그인 서버는 부합하는 사용자 계정 번호 및 사용자 패스워드에 관한 기록들이 존재하는가의 여부를 찾기 위해서 데이터베이스를 검색한다. 찾는다면, 그 로그인 서버는 이 사용자의 신원이 유효하며 그리고 그 사용자는 로그인이 허용된다고 표시하며; 그리고 찾지 못한다면, 그러면 그 로그인 서버는 현재의 로그인이 정당하지 않으며 그리고 그 로그인은 거절되었다는 것을 표시한다.

[0109] 다음은 몇몇의 실시예들에 따라서, 로그인 서버의 프로세싱 흐름을 실현하기 위해서 C++ 프로그래밍 언어로 구현된 예시적인 코드 세그먼트이다.

[0110] map<int,PasswordCode*> mapPasswordTable;

[0111] PasswordCode myPassword;

[0112] myPassword.Init();

[0113] mapPasswordTable[myPassword.m_nID] = &myPassword;

[0114] //사용자는 패스워드 테이블 번호 (nTableId), 암호화된 계정 번호 (strName) 및 암호화된 패스워드 (strPass)를 제출한다

[0115] PasswordCode* pCode = mapPasswordTable[nTableId]; //상기 번호에 따라 패스워드 테이블 획득

[0116] string strTrueName = pCode->Decode(strName); //계정 번호 디코딩

[0117] string strTruePass = pCode->Decode(strPass); //패스워드 디코딩

[0118] 상기 언급된 코드에 의해서, 디코드된 계정 번호 (변수 strTrueName 내에 저장된다)및 디코드된 패스워드 (변수 strTruePass 내에 저장된다)가 얻어질 수 있다.

[0119] 디코드된 계정 번호 및 패스워드를 획득한 이후에, 이 계정 번호가 유효한가의 여부는 상기 데이터베이스에 질의함으로써 더 체크될 수 있다. 몇몇의 실시예들에서, 이 계정 번호가 유효한가의 여부를 체크하기 위한 데이터베이스 SQL 문장은다음과 같을 수 있다: "string strSQL = "select * from USER_INFO where name=\'" + strTrueName + "\' and password = \'" + strTruePass + "\'"".

[0120] 다양한 실시예들에서, 상기 언급된 제1 클라이언트 및 제2 클라이언트는 컴퓨터, 스마트폰, 테블릿 PC 또는 다른 인텔리전트 단말 디바이스들 등과 같은 어떤 가능한 디바이스들을 사용하여 구현될 수 있다. 두 개의 독립적인 클라이언트들을 결합하여 로그인이 실현될 수 있고, 그리고 동일한 바이러스 또는 트로이 프로그램이 두 개의 기계들을 동시에 감염시키고 그리고 이 두 기계들을 연관시키도록 할 가능성이 극도로 작기 때문에, 사용자 로그인이 보안이 크게 향상된다.

[0121] 상기 제1 클라이언트 및 상기 제2 클라이언트가 서로에게 독립적이기 때문에, 상기 제1 클라이언트에 의해 수신된 패스워드 테이블이 상기 제2 클라이언트로 운반되도록 하는 방법 또는 상기 제1 클라이언트에 의해서 수신된 패스워드 테이블을 획득하기 위해서 상기 제2 클라이언트나 상기 제2 클라이언트를 이용하는 사용자를 위한 방법은 다양한 가능한 방식들로 수행될 수 있다.

[0122] 가장 간단한 방식들 중 하나는 상기 두 클라이언트들이 위치한 곳인 컴퓨터들, 모바일 단말들 등이 물리적으로 같이 위치하도록 하여, 사용자가 그 두 디바이스들의 디스플레이들을 직접 보고 동작을 직접적으로 수행할 수 있도록 하는 것이다. 이 경우는 복수의 컴퓨터들을 구비한 사무실, 학교, 가정 등과 같이 복수의 컴퓨터들을 동시에 이용할 수 있는 경우인 애플리케이션 시나리오들을 위해서 적합하다. 이 애플리케이션 시나리오들에서는 상대적으로 많은 대수의 컴퓨터들이 존재하며, 그래서 인접한 컴퓨터들 상에서 디스플레이된 정보를 보는 것은 직접적으로 실현될 수 있다. 예를 들면, 보안 로그인을 실현하기 위해서 복수의 컴퓨터들이 직접적으로 사용될 수 있는 장소에서, 사용자가 로그인하기 위해서 제2 컴퓨터 내 제2 클라이언트를 이용할 때에, 제1 클라이언트가 위치한 곳인 제1 컴퓨터가 수신한 패스워드 테이블은 그 사용자들이 쉽게 볼 수 있다.

[0123] 그러나, 상기 두 클라이언트들이 위치한 곳인 컴퓨터들이 물리적으로 같이 위치하지 않으며 그리고 직접적으로 같이 볼 수 없는 경우에 관하여, 상기 제1 클라이언트가 수신한 패스워드 테이블은 로그인하기 위해서 제2 클라

이언트를 이용하는 사용자나 오퍼레이터에게 송신될 수 있다. 예를 들면, 취해진 상기 패스워드는 제1 클라이언트가 위치한 컴퓨터의 사용자 또는 그 사용자의 조수에 의해, 전화기, 카메라, 이메일, 멀티미디어 메시지 및/또는 다른 통신 방법들을 통해서 송신될 수 있다. 이 패스워드 테이블에 따라 매핑되고 암호화될 것을 필요로 하는 사용자 정보에 관한 매핑 및 암호화를 수행할 수 있도록 하기 위해서, 로그인하기 위해 상기 제2 클라이언트를 이용하는 사용자가 이 패스워드 테이블을 획득할 수 있는 한 상기 특별한 통신 방법들 또는 통신 유형들은 제한되지 않는다.

[0124] 추가로, 다른 실시예에서, 보안을 더 확실하게 하기 위해서, 상기 패스워드 테이블을 생성할 때에, 상기 로그인 서버는 이 패스워드 테이블을 위한 대응하는 유효한 기간, 또는 이 패스워드 테이블을 이용하기 위한 미리 설정된 시간 기간을 생성할 수 있다; 그리고 상기 제2 클라이언트는 이 미리 설정된 시간 기간 내에 이 패스워드 테이블의 패스워드 테이블 일련 번호를 포함하는 제2 로그인 요청을 상기 로그인 서버에게 송신할 것이다. 다른 말로 하면, 로그인 서버는 이 미리 설정된 시간 기간 내에 이 패스워드의 패스워드 테이블 일련 번호를 포함하는 제2 로그인 요청을 수신할 것이다. 이 미리 설정된 시간 기간이 초과된다면, 그러면 상기 로그인 서버는 악의를 가진 사용자들에 의한 이후의 악의적 사용을 피하기 위해서 이 패스워드 테이블을 옵션으로 제거한다. 몇몇의 실시예들에서, 이 미리 설정된 시간 구간이 초과된 이후에 상기 로그인 서버가 이 패스워드 테이블의 패스워드 테이블 번호를 포함하는 제2 로그인 요청을 수신한다면, 그러면 이 패스워드 테이블이 존재하지 않는다는 것, 또는 상기 패스워드가 잘못되었다는 것 등을 표시하는 정보와 같은 촉구 정보가 상기 제2 클라이언트에게 반환될 수 있다. 동시에, 상기 패스워드를 다시 획득하는 것에 관한 촉구 정보가 상기 제2 클라이언트에게 반환될 것이다.

[0125] 본 발명의 상기 언급된 해결책에 의해서, 두 클라이언트들의 조합을 통해서 로그인이 실현되며, 이것은 두 클라이언트들을 결합하여 로그인을 실현하는 것과 동등하며, 이는 보안을 크게 향상시킨다.

[0126] 클라이언트가 위치한 곳인 단말이 컴퓨터인 예시적인 실시예에서, 그 컴퓨터들 중 하나가 트로이 프로그램이나 바이러스에 의해서 감염되는지에 관계없이, 사용자의 패스워드는 추측되거나 알려질 수 없다. 트로이 프로그램이나 바이러스가 제1 클라이언트가 위치한 곳인 컴퓨터의 제1 레벨 로그인을 모니터할 때에 단 하나의 패스워드 테이블만이 얻어지고, 그리고 사용자가 상기 제1 클라이언트가 위치한 곳인 컴퓨터 상에서 입력 동작을 수행하지 않기 때문에, 트로이 프로그램이나 바이러스는 실제의 패스워드를 얻을 수 없다. 제2 클라이언트가 위치한 곳인 컴퓨터의 제2 레벨 로그인을 트로이 프로그램이나 바이러스가 모니터할 때에, 심지어 그것이 사용자에 의한 사용자 정보 입력을 가로챌 수 있다고 하더라도, 이 가로채어진 사용자 정보는 암호화되고 사용 후 버려질 수 있으며, 이는 일단 사용된 이후에는 유효하지 않을 것이다. 패스워드 테이블이 없으면, 트로이 프로그램이나 바이러스는 올바른 원래의 패스워드를 얻을 수 없다.

[0127] 반면에, 사용자에 의해서 동작되는 두 개의 컴퓨터들을 트로이 프로그램이나 바이러스가 동시에 감염시키는 것은 매우 힘들다. 트로이 프로그램의 감염이 랜덤이기 때문에, 그것은 사용자에 의해서 동작되는 두 개의 특정 컴퓨터들이 바로 그 동일한 트로이 프로그램이나 바이러스에 의해서 동시에 감염되도록 하는 상황을 제어할 수 없다. 더욱이, 두 컴퓨터들은 상이한 운영 시스템들을 채택할 수 있을 것이며, 그리고 트로이 프로그램이 그 시스템들의 호환성을 깨닫는 것 그리고 동시에 그것들을 동시적으로 모니터링하는 것을 또한 실현하는 것은 매우 어려우며, 이는 막대한 양의 백그라운드 계산을 필요로 한다. 그러므로, 동일한 트로이 프로그램이나 바이러스가 사용자에 의해서 동작되는 두 컴퓨터들을 동시에 감염시키는 것은 거의 발생할 것 같지 않다. 일반적으로 말하면, 두 개의 컴퓨터들을 이용하여 로그인하기 위한 보안 기준의 레벨은 단일의 컴퓨터를 이용하여 로그인하기 위한 보안 기준에 비교하면 크게 향상된다. 필요하다면, 제1 클라이언트가 위치한 곳인 컴퓨터는 패스워드 테이블을 획득하기 위해서만 사용될 수 있으며, 다른 소프트웨어는 설치되지 않을 것이다. 몇몇의 실시예들에서, 상기 제1 클라이언트는 다른 관련성이 없는 웹사이트들로의 액세스 또는 로그인이 거절될 수 있으며, 그래서 어떤 트로이 프로그램이나 바이러스로 인해서 감염될 것 같은 가능성이 크게 줄어들도록 한다. 그래서 보안 문제가 덜 발생할 것 같다.

[0128] 추가로, 두 개의 컴퓨터들 상에서 합동 로그인이 사용되기 때문에, 따라서 동시에 로그인하기 위해서 두 명의 오퍼레이터들이 필요할 수 있으며, 그리고 몇몇의 특별한 시스템들이 개별적으로 상기 오퍼레이터들 중 어느 하나를 신뢰할 수 없는 경우에, 두 오퍼레이터들의 합동 로그인은 시스템 보안의 신뢰성을 더 향상시킬 수 있다.

[0129] 로그인 인증을 위한 상기 언급된 방법에 따라서, 본 발명은 로그인 인증을 위한 시스템을 더 제공하며, 그리고 본 발명에서 제공된 로그인 인증을 위한 시스템은 상기 언급된 제1 클라이언트 및 제2 클라이언트만을 포함할 수 있으며 그리고 상기 언급된 로그인 서버만을 또한 포함할 수 있으며, 그리고 상기 언급된 제1 클라이언트,

제2 클라이언트 및 로그인 서버를 동시에 또한 포함할 수 있다.

[0130] 도 4는 본 발명에서 로그인 인증을 위한 시스템의 예시적인 실시예의 개략적인 블록 도면을 보여준다. 이 예시적인 실시예에서, 간단한 설명을 위해서, 예로서 제1 클라이언트, 제2 클라이언트 및 로그인 서버를 동시에 포함하는 것을 취하여 설명을 할 수 있다.

[0131] 도 4에서 보이는 것처럼, 이 예시적인 실시예에서, 제1 클라이언트 (401), 제2 클라이언트 (402) 및 로그인 서버 (403)가 포함된다.

[0132] 상기 제1 클라이언트 (401)는 제1 로그인 요청을 상기 로그인 서버 (403)에게 송신하고 그리고 원래의 캐릭터들 및 상기 제1 로그인 요청에 따라 상기 로그인 서버 (403)에 의해서 반환된 후-매핑 캐릭터들 사이의 매핑 관계를 수신하기 위해서 사용된다.

[0133] 상기 제2 클라이언트 (402)는 상기 언급된 매핑 관계에 따라 로그인 서버 (403)로 제2 로그인 요청을 송신하기 위해서 사용되며, 상기 제2 로그인 요청은 상기 언급된 매핑 관계에 따라 결정된 사용자 정보에 대응하는 후-매핑 정보를 포함한다.

[0134] 상기 로그인 서버 (403)는 상기 제1 클라이언트 (401)에 의해 송신된 제1 로그인 요청을 수신하고, 상기 원래의 캐릭터들 및 상기 제1 로그인 요청에 따른 후-매핑 캐릭터 사이의 매핑 관계를 생성하고, 그리고 그 매핑 관계를 상기 언급된 제1 클라이언트 (401)로 송신하고, 그리고 상기 제2 클라이언트 (402)에 의해 송신된 상기 언급된 제2 로그인 요청 - 이는 후-매핑 정보를 포함한다 - 을 수신하며, 상기 언급된 매핑 관계에 따라 상기 언급된 후-매핑 정보에 대응하는 사용자 정보를 결정하며, 그리고 상기 사용자 정보를 미리-저장된 사용자 정보를 비교하기 위해서 사용된다.

[0135] 도 4에서 보이는 것처럼, 이 로그인 서버 (403)는 특히 다음을 포함한다: 메시지 송수신 모듈 (4031), 매핑 관계 생성 모듈 (4032), 그리고 로그인 인증 모듈 (4033).

[0136] 상기 메시지 송수신 모듈 (4031)은 상기 제1 클라이언트에 의해서 송신된 제1 로그인 요청 및 상기 제2 클라이언트에 의해서 송신된 제2 로그인 요청을 수신하고, 매핑 관계 생성 모듈 (4032)에 의해서 생성된 매핑 관계를 상기 언급된 제1 클라이언트에게 송신하도록 구성되며, 상기 언급된 제2 로그인 요청은 후-매핑 정보를 포함한다.

[0137] 상기 매핑 관계 생성 모듈 (4032)은 상기 원래의 캐릭터들 및 상기 언급된 제1 로그인 요청에 따른 상기 후-매핑 캐릭터들 사이의 매핑 관계를 생성하도록 구성된다.

[0138] 상기 로그인 인증 모듈 (4033)은 상기 언급된 매핑 관계에 따라 상기 언급된 후-매핑 정보에 대응하는 사용자 정보를 결정하고 그리고 그 사용자 정보를 미리-저장된 사용자 정보와 비교하도록 구성된다.

[0139] 상기 실시예들 중 하나의 실시예에서, 상기 언급된 매핑 관계 생성 모듈 (4032)은 상기 언급된 제1 로그인 요청에 따라 상기 언급된 매핑 관계에 대응하는 매핑 관계 일련 번호를 생성하도록 더 구성된다. 상기 메시지 송수신 모듈 (4031)은 상기 매핑 관계 일련 번호를 상기 언급된 제1 클라이언트 (401)로 송신하도록 더 구성되며, 그리고 동시에, 상기 언급된 제2 로그인 요청은 상기 매핑 관계 일련 번호를 더 포함한다. 따라서, 상기 언급된 제1 클라이언트 (401)는 상기 제1 로그인 요청에 따라 상기 로그인 서버 (403)에 의해서 반환된 상기 언급된 매핑 관계에 대응하는 상기 매핑 관계 일련 번호를 수신하도록 더 구성되며, 그리고 제2 클라이언트 (402)에 의해서 송신된 상기 언급된 제2 로그인 요청은 상기 매핑 관계 일련 번호를 더 포함한다.

[0140] 몇몇의 실시예들에서, 매핑 관계 생성 모듈 (4032)이 상기 언급된 매핑 관계를 생성할 때에, 그 매핑 관계는 기계-기반의 의사-랜덤 생성기를 이용하여 생성될 수 있다.

[0141] 따라서, 상기의 설명들을 기초로 하여, 로그인 서버 (예를 들면, 도 4에서의 로그인 서버 (403))는 도 5에서 설명된 것과 같은 사용자 로그인을 인증하는 예시적인 방법을 구현할 수 있다. 위에서 설명된 것처럼, 상기 로그인 서버는 개별 시각들에 (예를 들면, 주어진 인증 타임 윈도우 내에서 두 개의 상이한 시각들에) 수행된 제1-레벨 로그인 프로세스 및 제2-레벨 로그인 프로세스를, 두 개의 상이한 클라이언트 디바이스들 (예를 들면, 제1 클라이언트 디바이스 및 제2 클라이언트 디바이스)과 함께 제안한다. 상기 로그인-서버는 대응하는 제1-레벨 로그인 요청 및 제2-레벨 로그인 요청을, 제1-레벨 로그인 요청 내에 포함된 부분적인 사용자 로그인 정보 (예를 들면, 제1-레벨 로그인 요청 내에 제공된 사용자 이름)를 기초로 하여, 또는 상기 제1-레벨 로그인 요청에 응답하여 상기 제1 클라이언트 디바이스에게 제공된 보안 향상 정보 (예를 들면, 각 매핑 테이블)를 위한 각 레퍼런스 번호 (예를 들면, 각 매핑 테이블 일련 번호)를 기초로 하여 상관시킨다. 일단 상기 로그인 서버가 제1-레벨

로그인 요청 및 제2-레벨 로그인 요청 사이의 연관을 설립하면, 그 로그인 서버는 사용자의 미리-저장된 원래의 로그인 정보 및 상기 사용자에게 제공된 각 보안 향상 정보에 따라 상기 제2-레벨 로그인 요청 내에 포함된 완전한 로그인-정보를 검증한다. 몇몇의 실시예들에서, 상기 로그인-서버는 정규적인 로그인 인증 및 상기 2-레벨 로그인 인증 둘 모두를 옵션으로 제안한다. 사용자는 그 사용자가 두 개의 상이한 클라이언트 디바이스들에 동시에 액세스하는가의 여부, 그리고 그 사용자가 상기 정규적인 단일-레벨 로그인에 의해서 강제된 보안 위험을 감내할 수 있는가의 여부에 종속하여 상기 정규적인 로그인 또는 상기 2-레벨 로그인 중 어느 하나를 불러낼 수 있을 것이다. 몇몇의 실시예들에서, 사용자가 상기 로그인 서버와의 통신을 설립하기 위해서 클라이언트 디바이스 상에서 단일-레벨 로그인 프로세스를 초기에 선택할 때에, 상기 로그인 서버는 상기 보안 위험들에 관하여 상기 사용자에게 교육하는 통지를 옵션으로 돌려보내며 그리고 상기 단일-레벨 로그인으로 계속하는가의 여부를 상기 사용자에게 확인시킨다. 몇몇의 실시예들에서, 상기 로그인 서버는 고-민감도 서비스들 또는 데이터의 특정 유형들을 위한 강제적인 2-레벨 로그인을 옵션으로 구현하며, 사용자가 상기 2-레벨 로그인 프로세스를 통해서만 상기 서비스들 또는 데이터에 액세스할 것을 필요로 한다.

[0142] 몇몇의 실시예들에서, 도 5에서 보이는 것처럼, 상기 로그인 서버는 제1 클라이언트 디바이스로부터 제1-레벨 로그인 요청을 수신하며 (S502), 그 제1-레벨 로그인 요청은 사용자와 연관된 제1 사용자 로그인 정보를 포함한다. 예를 들면, 상기 사용자는 상기 제1-레벨 로그인 프로세스를 시작하기 위해서 제1 클라이언트 디바이스 상에 제공된 옵션을 선택할 수 있을 것이다. 몇몇의 실시예들에서, 상기 제1 클라이언트 디바이스는 상기 로그인-서버의 웹페이지를 제시할 수 있으며, 그리고 상기 웹페이지는 제1-레벨 로그인 프로세스를 시작하기 위한 링크 및 제2-레벨 로그인 프로세스를 시작하기 위한 다른 링크를 구비한다. 몇몇의 실시예들에서, 상기 사용자가 상기 제1-레벨 로그인 옵션을 선택했을 때에, 상기 로그인-서버는 사용자로부터 제1 사용자 로그인 정보를 수집하기 위해서 상기 제1 클라이언트 디바이스 상에 인터페이스를 (예를 들면, 하나 또는 그 이상의 입력 필드들을) 제공한다. 몇몇의 실시예들에서, 상기 제1 사용자 로그인 정보는 상기 로그인 서버에서 사용자 로그인 세션을 설립하기 위해서 사용될 수 있는 정보이지만, 그러나 상기 사용자를 완전하게 인증하기에 충분하지 않으며 그리고 사용자가 상기 로그인 서버에 의해서 제공된 서비스로의 완전한 액세스를 얻는 것을 가능하게 한다. 몇몇의 실시예들에서, 상기 제1 사용자 로그인 정보는 그 사용자와 연관된 부분적인 사용자 로그인 정보만을 포함한다. 몇몇의 실시예들에서, 상기 부분적인 사용자 로그인 정보는 그 사용자의 계정 번호, 또는 다른 사용자 식별자들을 옵션으로 포함하지만, 그 사용자의 계정을 위한 사용자의 패스워드는 포함하지 않는다. 몇몇의 실시예들에서, 상기 제1 사용자 로그인 정보는 상기 제1 클라이언트 디바이스에 의해서 상기 사용자를 위해서 랜덤으로 생성된 익명의 로그인 ID를 포함한다.

[0143] 몇몇의 실시예들에서, 상기 제1-레벨 로그인 요청에 응답하여 (S504), 상기 로그인 서버는 상기 사용자를 위하여 제1-레벨 로그인 프로세스를 시작한다. 이 제1-레벨 로그인 프로세스 동안에, 상기 로그인 서버는 상기 제1-레벨 로그인 요청을 위해 각 보안 향상 정보를 생성한다 (S506). 상기 로그인 서버는 그러면 상기 보안 향상 정보를 제1 클라이언트 디바이스에게 제공하며 (S520), 그리고 제2-레벨 로그인 프로세스를 통해서 상기 사용자를 인증하기 위한 타임 윈도우를 설립한다 (S522). 위에서 설명된 것처럼, 상기 제2-레벨 로그인 프로세스는 상기 제1 클라이언트 디바이스와는 상이한 각 클라이언트 디바이스에 의해서 개시될 것이며, 그리고 상기 제2-레벨 로그인 프로세스는 상기 사용자가 상기 보안 향상 정보에 따라 제2 사용자 로그인 정보를 제공할 것을 필요로 한다.

[0144] 위에서 설명될 것처럼, 몇몇의 실시예들에서, 상기 수신된 제1-레벨 로그인 요청을 위해 향상된 보안 정보를 생성하기 위해서, 상기 로그인 서버는 복수의 원래의 캐릭터들을 복수의 후-매핑 캐릭터들로 변환하기 위해서 각 매핑 테이블을 생성한다 (S506). 예를 들면, 표 1에서 보이는 것처럼, 상기 원래의 사용자 로그인 정보가 적어도 부분적으로 숫자들로 표현된다면, 상기 매핑 테이블은 숫자 캐릭터들 (예를 들면, 숫자들 1, 2, 3)로부터 다른 캐릭터들 (예를 들면, 4, 5, 3과 같은 다른 숫자들; 또는 a, T, e와 같은 다른 문자들; 또는 ㄷ, %, *와 같은 다른 심볼들; 또는 #, 5, a와 같은 상이한 다른 유형의 캐릭터들의 혼합)로의 매핑을 포함한다. 제1 클라이언트 디바이스 상에서 제1-레벨 로그인 프로세스 동안에 상기 사용자가 부분적인 개인적인 로그인 정보 또는 어떤 개인적인 로그인 정보를 제공할 것을 요청하는 목적은 바이러스 또는 트로이 프로그램이 상기 제1 클라이언트 디바이스 상에서 상기 사용자의 완전한 개인적인 로그인 정보를 얻는 것을 방지하는 것이다. 원래의 캐릭터들로부터 후-매핑 캐릭터들로의 매핑을 이용함으로써, 상기 사용자는 자신의 개인적인 로그인 정보의 적어도 일부를 원래의 모습 (예를 들면, 개인적인 로그인 정보에서 원래의 캐릭터들을 이용하여 표현된 개인적인 로그인 정보)으로부터 다른 모습 (예를 들면, 개인적인 로그인 정보에서 원래의 캐릭터들에 대응하는 후-매핑 캐릭터들을 이용하여 표현된 개인적인 로그인 정보)으로 고쳐 쓸 수 있다. 상기 매핑이 제2 클라이언트 디바이스에서 이용 가능하지 않기 때문에, 상기 후-매핑 캐릭터들로 표현된 상기 개인적인 로그인 정보는 상기 개인적인 로그인

정보의 원래의 모습을 해독하기 위해서 사용될 수 없다. 그래서, 상기 제2 클라이언트 디바이스가 바이러스 또는 트로이 프로그램에 의해서 또한 감염된다고 하더라도, 그 바이러스 또는 트로이 프로그램은 그 사용자의 원래의 개인적인 로그인 정보를 여전히 획득할 수 없다.

[0145] 몇몇의 실시예들에서, 각 매핑 테이블을 생성할 때에, 상기 로그인 서버는 상기 사용자의 로그인 정보 내에 포함된 복수의 원래 캐릭터들을 제1 랜덤 시퀀스에 배치한다 (S508). 상기 로그인 서버는 상기 사용자의 로그인 정보 내에 포함된 복수의 원래 캐릭터들을 제2 랜덤 시퀀스에 또한 배치하다 (S510). 그 후, 상기 로그인 서버는 상기 제1 랜덤 시퀀스 및 제2 랜덤 시퀀스 사이의 1-대-1 매핑을 생성하며 (S512), 이 경우에 제1 랜덤 시퀀스 내의 캐릭터들은 각 매핑 테이블의 원래의 캐릭터들로서 사용되며, 그리고 상기 제2 랜덤 시퀀스 내의 캐릭터들은 각 매핑 테이블의 후-매핑 캐릭터들로서 사용된다. 예를 들면, 표 1에서, 상기 원래의 캐릭터들은 10개의 숫자들 모두를 포함하며, 그리고 상기 후-매핑 캐릭터들 10개 숫자들 모두를 또한 포함하며, 그리고 원래의 시퀀스 내의 10개의 숫자들과 후-매핑 시퀀스 내 상기 10개의 숫자들 사이의 대응은 기계-기반의 랜덤 또는 의사-랜덤 (pseudo-random) 생성기에 따라서 생성된다. 문자들, 심볼들, 한자 캐릭터들 등과 같은 다른 유형의 캐릭터들이 상기 원래의 시퀀스 및 상기 후-매핑 시퀀스 내에 포함될 수 있다. 몇몇의 실시예들에서, 상기 원래의 시퀀스 및 상기 후-매핑 시퀀스는 계정 보유자들의 개인적인 로그인 정보에서 사용되지 않은 캐릭터들 또는 캐릭터들의 유형들을 포함할 수 있다. 이것은 계정 보유자들의 개인적인 로그인 정보를 추측하는 것에 대한 추가적인 장벽일 수 있다. 몇몇의 실시예들에서, 간략함을 위해서, 매핑 테이블 내 원래의 시퀀스는 사용자의 개인적인 로그인 정보에서 실제로 사용되는 캐릭터들만을 랜덤화된 순서로 포함한다. 예를 들면, 사용자의 원래의 패스워드가 "3724A"이라면, 원래의 시퀀스는 "273A4"일 수 있으며, 후-매핑 시퀀스는 "F$G2P"일 수 있다. 이 매핑을 기초로 하여, 사용자는 제2 클라이언트 디바이스에 자신의 후-매핑 패스워드를 "G$FP2"로 제공할 수 있다. 상기 매핑 내에 필수적인 캐릭터들만을 포함시킴으로써, 디스플레이 공간 및 계산 능력의 어느 정도의 효율성이 달성될 수 있다.

[0146] 몇몇의 실시예들에서, 상기 제1-레벨 로그인 요청을 위해 상기 보안 향상 정보를 생성할 때에, 상기 로그인 서버는 상기 각 매핑 테이블을 위해 각 매핑 일련 번호를 생성한다 (S516). 위에서 설명된 것처럼, 상기 각 매핑 테이블을 위한 상기 각 매핑 일련 번호는 상기 로그인 서버에서 상기 각 매핑 테이블과 함께 저장될 수 있다. 추가로, 각 매핑 일련 번호는 각 매핑 테이블과 함께 상기 제1 클라이언트에서 사용자에게 제공된다. 사용자가 제2 클라이언트 디바이스에서 대응하는 제2-레벨 로그인 프로세스를 시작할 때에, 그 사용자는 상기 매핑 일련 번호를 로그인 서버에게 제공하며, 그리고 상기 각 매핑 테이블에 따라서 수정된 자신의 개인적인 로그인 정보를 제공한다. 위에서 설명된 것처럼, 몇몇의 실시예들에서, 상기 로그인 서버에 의해서 요청된 것처럼, 모든 개인적인 로그인 정보는 자신들의 후-매핑 모습으로 상기 제2 클라이언트 디바이스에서 상기 로그인 서버에게 옵션으로 제공된다. 몇몇의 실시예들에서, 상기 로그인 서버에 의해서 요청된 것처럼, 사용자 이름만이 후-매핑 모습으로 제공되며, 패스워드는 자신의 원래의 모습으로 제시된다. 몇몇의 실시예들에서, 상기 로그인 서버에 의해서 요청된 것처럼, 패스워드만이 후-매핑 모습으로 제공되며, 사용자 이름은 원래의 모습으로 제시된다.

[0147] 몇몇의 실시예들에서, 제1-레벨 로그인 프로세스 동안에 사용자가 원래의 모습으로 사용자 이름을 제공했다면, 매핑 일련 번호는 상기 제1-레벨 로그인 요청 및 상기 대응하는 제2-레벨 로그인 요청을 상관시키기 위해서 필요하지 않을 수 있을 것이다. 그런 실시예들에서, 상기 로그인 서버는 원래의 모습으로 표현된 사용자 이름을 기초로 하여 상기 제1-레벨 로그인 요청을 그것의 대응하는 제2-레벨 로그인 요청에 옵션으로 연관시킬 수 있을 것이다. 몇몇의 실시예들에서, 사용자 이름이 제1-레벨 로그인 프로세스 및 제2-레벨 로그인 프로세스 둘 모두를 위해 원래의 모습으로 표현된다면, 희망했던 보안 향상을 달성하기 위해서 상기 패스워드는 상기 제2-레벨 로그인 프로세스 동안에 후-매핑 모습으로 표현될 필요가 있다.

[0148] 몇몇의 실시예들에서, 제1-레벨 로그인 프로세스 동안에, 예를 들면, 상기 사용자가 랜덤으로 생성된 그리고 익명인 사용자 이름을 이용하여 제1-레벨 로그인 프로세스를 개시했을 때에, 상기 사용자가 사용자 이름을 원래의 모습으로 제공하지 않았다면, 상기 로그인 서버는 각 매핑 일련 번호를 제1 클라이언트 디바이스에서 상기 사용자에게 제공한다. 제2-레벨 로그인 프로세스 동안에, 사용자는 적어도 부분적으로 후-매핑 모습으로 표현된 그 사용자의 개인적인 로그인 정보와 함께 (예를 들면, 상기 로그인 서버에 의해서 지시된 것과 같은 후-매핑 모습으로 표현된 사용자 이름 및/또는 패스워드와 함께) 상기 매핑 일련 번호를 제2 클라이언트 디바이스에서 상기 로그인 서버에게 제공한다. 상기 로그인 서버는, 상기 제2 클라이언트 디바이스로부터 수신된 제2-레벨 로그인 요청 내 매핑 일련 번호를 상기 제1-레벨 로그인 프로세스 동안에 상기 제1 클라이언트 디바이스로 이전에 제공된 매핑 일련 번호에 매칭시킴으로써, 상기 제1 로그인 요청 및 상기 제2 로그인 요청을 연관시킬 수 있다

[0149] 몇몇의 실시예들에서, 상기 제1 기계 및 제2 기계 상에 존재하는 바이러스들 또는 트로이 프로그램들이 백엔드

서버에 의해서 연결될 수 있을 것이며, 그리고 상기 제1-레벨 로그인 요청, 매핑 테이블, 그리고 제2-레벨 로그인 요청 사이의 연관을 합동으로 발견할 수 있을 것이라는 작은 가능성이 여전히 존재한다. 더욱 양호한 보안을 제공하기 위해서, 몇몇의 실시예들에서, 상기 제1-레벨 로그인 요청을 위한 보안 향상 정보를 생성할 때에, 로그인 서버는 보안 향상 정보의 적어도 일부를 CAPTCHA 로서 생성한다. CAPTCHA 는 컴퓨터들과 사람들을 구분할 수 있는 튜링 (Turing) 테스트의 유형이다. 예를 들면, 일그러진 캐릭터는 인간 사용자에 의해서 쉽게 인식될 수 있을 것이지만, 기계가 인식하기에는 매우 어려울 수 있다. 다른 예를 위해서, 제시된 이미지가 역전되었는가 또는 역전되지 않았는가의 여부를 인간 사용자가 아는 것은 매우 쉬울 수 있을 것이지만, 컴퓨터가 아는 것은 매우 어려울 수 있다. 원래의 캐릭터를 후-매핑 캐릭터로 매핑하도록 설계될 수 있는 많은 CAPTCHA들 또는 튜링 테스트들이 존재하여, 인간 사용자만이 매핑이 어떤 것인지를 쉽게 결정할 수 있도록 하며, 심지어는 상기 매핑을 운반하는 콘텐트 (예를 들면, 이미지)를 기계가 소유한다고 하더라도 그 기계는 상기 매핑이 어떤 것이지를 판별할 수 없다. 예를 들면, 상기 매핑이 원래의 캐릭터 "1"로부터 후-매핑 캐릭터 "X"로의 매핑이라면, 상기 매핑 관계는 비스듬한 캐릭터 "1"을 상이한 폰트 또는 색상인 비스듬한 캐릭터 "X"를 가리키는 화살표와 함께 보여주는 이미지로서 상기 사용자에게 제시될 수 있다. 이 이미지는 인간 사용자가 상기 매핑을 판별하는 것에는 어떤 어려움도 제시하지 않을 것이지만, 상기 매핑을 해독하기 위한 기계 (예를 들면, 상기 제1 클라이언트 디바이스 및 제2 클라이언트 디바이스 상에 존재하는 바이러스들이나 트로이 프로그램들을 연결시키는 백엔드 기계)의 능력을 심각하게 방해할 것이다. 몇몇의 실시예들에서, 상기 매핑이 CAPTCHA 모습으로 제시될 때에, 모든 가능한 원래의 캐릭터들의 세트가 아니라 원래 캐릭터들의 더 작은 세트 (예를 들면, 상기 사용자의 원래의 로그인 정보를 표현하기 위해서 사용된 원래의 캐릭터들의 세트로부터 랜덤으로 선택된 하나 또는 두 개의 캐릭터들)를 위한 매핑이 생성될 수 있다. 그런 실시예들에서, 사용자가 제2-레벨 로그인 프로세스에 참여할 때에, 그 사용자는 원래의 로그인 정보의 일부 (예를 들면, 사용자 이름 및 패스워드 중 하나 또는 두 개의 캐릭터들)만을 후-매핑 모습으로 제공할 필요가 있을 뿐이다. 그런 실시예들에서, 상기 로그인 서버는 상기 매핑을 비-CAPTCHA 모습으로 저장하며, 그리고 상기 후-매핑 사용자 로그인 정보가 올바른 사용자 로그인 정보인가를 쉽게 판별할 수 있다.

[0150] 몇몇의 실시예들에서, 위에서 설명된 것처럼, 상기 제1-레벨 로그인 요청은 사용자와 연관된 불완전한 로그인 정보를 포함한다. 이 방식에서 완전한 개인적인 로그인 정보는 상기 제1 클라이언트 디바이스 상에 존재할 수 있을 바이러스 및 트로이 프로그램에게는 노출되지 않는다. 몇몇의 실시예들에서, 상기 제2 사용자 로그인 정보는 상기 보안 향상 정보에 따라서 수정된 완전한 사용자 로그인 정보를 포함한다. 이 방식에서, 심지어 상기 제2 클라이언트 디바이스가 바이러스 또는 트로이 프로그램에 의해서 감염되었다고 하더라도, 상기 보안 향상 정보의 콘텐트 (예를 들면, 매핑 테이블 및/또는 매핑 일련 번호)를 알지 못하기 때문에, 상기 바이러스 또는 트로이 프로그램은 상기 보안 향상 정보에 따라서 수정된 완전한 로그인 정보로부터 상기 사용자의 원래의 개인적인 로그인 정보를 여전히 해독할 수 없다. 추가로, 상기 바이러스 또는 트로이 프로그램은 상기 사용자의 계정이나 로그인-서버의 서비스로의 액세스를 얻기 위해, 미래에 상기 보안 향상 정보에 따라서 수정된 완전한 로그인 정보를 다시 사용할 수 없다. 몇몇의 실시예들에서, 상기 로그인 인터페이스는 후속된 제2-레벨 로그인 프로세스 동안에 모든 로그인 정보가 후-매핑 캐릭터 내에 제공될 것인지 또는 상기 로그인 정보의 일부만이 후-매핑 캐릭터들 내에 제공되어야만 하는지의 여부를 동적으로 판별한다.

[0151] 몇몇의 실시예들에서, 로그인 서버는 제2-레벨 로그인 요청을 위해서 사용될 완전한 로그인 정보의 모습을 동적으로 결정한다. 몇몇의 실시예들에서, 로그인 서버는 이어지는 제2-레벨 로그인 프로세스 동안에 로그인 정보 중의 어느 부분 (예를 들면, 사용자 이름만, 또는 패스워드만, 또는 사용자 이름 및 패스워드 중 특별한 캐릭터들만)이 후-매핑 캐릭터들에서 제공되는가를 동적으로 결정한다. 몇몇의 실시예들에서, 로그인 서버는 상기 제2-레벨 로그인 프로세스에서 사용될 로그인 정보를 위해서 동적으로 결정된 포맷에 관한 명령을 다른 보안 향상 정보와 함께 상기 제1 클라이언트 디바이스로 제공한다. 그런 실시예들에서, 상기 로그인 서버는 상기 포맷 정보를, 제1-레벨 로그인 요청을 위해서 생성된 향상된 보안 정보와 함께 저장한다. 추가로, 그런 실시예들에서, 상기 제1 클라이언트 디바이스는 상기 명령을 사용자에게 디스플레이한다. 몇몇의 실시예들에서, 제2 클라이언트 디바이스가 상기 매핑 일련 번호를 상기 제2 클라이언트 디바이스에서 상기 로그인 서버에게 제공한 이후에, 로그인 서버는 상기 명령을 상기 제2 클라이언트 디바이스에서 사용자에게 송신한다. 그런 실시예들에서, 제2 클라이언트 디바이스에서 상기 명령이 사용자에게 디스플레이된 이후에, 그 사용자는 상기 명령에 따라 완전한 로그인 정보를 제공할 수 있다.

[0152] 몇몇의 실시예들에서, 위에서 설명된 것처럼, 상기 로그인 서버는 상기 제1-레벨 로그인 요청에 대응하는 제2-레벨 로그인 요청을 기초로 하여 인증이 수행될 수 있는 타임 윈도우를 설립한다. 몇몇의 실시예들에서, 상기 타임 윈도우는 각 보안 향상 정보가 제1 클라이언트 디바이스에서 사용자에게 제공될 때에 시작하는 10분 타임

윈도우일 수 있다. 몇몇의 실시예들에서, 로그인 서버는 상기 타임 윈도우의 시작 시각 및 종료 시각을 각 보안 향상 정보 (예를 들면, 매핑 테이블) 및 각 매핑 일련 번호 (예를 들면, 매핑 테이블 일련 번호)와 함께 데이터베이스 (예를 들면, 매핑 테이블 데이터베이스)에 저장한다. 몇몇의 실시예들에서, 어떤 대응하는 제2-레벨 로그인 요청도 제2 클라이언트 디바이스로부터 수신되지 않는다면, 로그인 서버는 저장된 매핑 테이블 그리고 그 매핑 테이블과 연관된 다른 정보 (예를 들면, 시간 정보 및 일련 번호 정보)를 폐기한다. 몇몇의 실시예들에서, 상기 로그인 서버가 동일한 제1 클라이언트 디바이스로부터 제2-레벨 로그인 요청을 수신한다면, 그 로그인 서버는 대응하는 제2-레벨 로그인 프로세스를 수행하기 위해서 사용자가 상이한 클라이언트 디바이스를 찾을 것을 요청하는 통지를 옵션으로 사용자에게 제공한다. 몇몇의 실시예들에서, 로그인 서버가 정규적인 단일-레벨 로그인을 마찬가지로 허용한다면, 그 로그인 서버는 정규의 단일-레벨 로그인과 연관된 보안 위험을 사용자에게 옵션으로 경고하고, 그리고 그 사용자가 그래도 단일-레벨 로그인 프로세스로 진행하기를 원하는가의 여부를 그 사용자에게 확인한다. 몇몇 실시예들에서, 보안 위험에도 불구하고 사용자가 단일-레벨 로그인을 수행하기를 원한다는 것을 그 사용자가 확인한다면 (예를 들어, 어떤 다른 클라이언트 기계들이 근처에서 이용가능하지 않을 때에), 상기 로그인 서버는 저장된 매핑 테이블 및 다른 연관된 정보를 폐기하고, 그리고 정규적인 로그인 프로세스를 진행시킨다.

[0153] 몇몇의 실시예들에서, 위에서 설명된 것처럼, 상기 제2-레벨 로그인 프로세스를 통해서 사용자를 인증하기 위한 타임 윈도우 동안에, 로그인 서버는 제2 클라이언트 디바이스로부터 제2-레벨 로그인 요청을 수신하며 (S524), 상기 제2-레벨 로그인 요청은 상기 제2 클라이언트 디바이스에서 상기 사용자에 의해서 제공된 완전한 로그인 정보 및 보안 향상 정보를 위한 각 식별 정보를 포함한다. 예를 들면, 몇몇의 실시예들에서, 사용자는 사용자 이름과 패스워드를 제공하며, 그리고 그 사용자 이름이나 패스워드 중 적어도 하나, 또는 그 사용자 이름 및/또는 패스워드 내의 적어도 몇몇의 캐릭터들은 상기 제1 클라이언트 디바이스에서 수신된 매핑 테이블에 따라서 수정되었다. 몇몇의 실시예들에서, 위에서 설명된 것처럼, 보안 향상 정보를 위한 식별 정보는 원래의 모습인 사용자 이름이다. 몇몇의 실시예들에서, 상기 보안 향상 정보를 위한 식별 정보는 제1 클라이언트 디바이스에서 사용자가 수신한 매핑 일련 번호이다. 몇몇의 실시예들에서, 상기 제2 디바이스는 두 개의 옵션들을 디스플레이하며, 한 옵션은 제1-레벨 로그인 프로세스를 개시하기 위한 것이며, 그리고 제2 옵션은 제2-레벨 로그인 프로세스를 개시하기 위한 것이다. 몇몇의 실시예들에서, 제2 클라이언트 디바이스는 상기 두 옵션들을 제공하는 로그인 서버에 의해서 제공된 웹페이지를 디스플레이한다. 몇몇의 실시예들에서, 사용자는 제2-레벨 로그인 프로세스를 불러내기 위해 상기 옵션을 선택하며, 그리고 응답으로, 제2 클라이언트 디바이스 상에 사용자 인터페이스가 디스플레이되어 완전한 로그인 정보를 요청하며, 이 완전한 로그인 정보는 보안 향상 정보, 그리고 그 보안 향상 정보를 위한 식별 정보에 따라서 수정된 것이다.

[0154] 몇몇의 실시예들에서, 로그인 서버는 제2 클라이언트 디바이스로부터 수신된 제2-레벨 로그인 요청에 포함된 각 식별 정보를 기초로 하여 보안 향상 정보를 검색한다 (S526). 예를 들면, 매핑 일련 번호를 기초로 하여, 로그인 서버는 현재 수신된 제2-레벨 로그인 요청에 대응하는 제1-레벨 로그인 요청과 연관된 각 매핑 테이블을 검색할 수 있다. 몇몇의 실시예들에서, 일단 올바른 매핑 테이블이 식별되면, 로그인 서버는 제2-레벨 로그인 요청이 상기 제1-레벨 로그인 요청 및 매핑 테이블과 연관된 타임 윈도우 내에 수신되었다는 것을 또한 검증한다.

[0155] 몇몇의 실시예들에서, 로그인 서버는 상기 검색된 보안 향상 정보 그리고 상기 사용자와 연관된 미리-저장된 원래의 로그인 정보를 기초로 하여 제2 로그인 요청에 포함된 완전한 로그인 정보를 검증한다 (S528). 예를 들면, 몇몇의 실시예들에서, 상기 검색된 매핑 테이블 내에서 특정된 캐릭터 대응을 기초로 하여, 상기 로그인 서버는 상기 제2-레벨 로그인 요청 내에 포함된 완전한 로그인 정보 (예를 들면, 사용자 이름 및 패스워드)로부터 원래의 완전한 개인적인 로그인 정보를 복구한다. 상기 복구된 완전한 로그인 정보가 사용자와 연관된 원래의 로그인 정보 (이것은 로그인 서버에서 사용자 로그인 정보 데이터베이스 내에 저장된 것임)에 부합한다면, 로그인 서버는 상기 제2-레벨 로그인 요청이 검증을 통과했다고 판별한다. 상기 복구된 완전한 로그인 정보가 사용자와 연관된 원래의 로그인 정보에 부합하지 않는다면, 로그인 서버는 상기 제2-레벨 로그인 요청이 검증에 실패했다고 판별한다. 몇몇의 실시예들에서, 로그인 서버는 검증을 통과한 제2 로그인 요청에 따른 각 서비스로의 사용자 액세스를 허용한다 (S530). 몇몇의 실시예들에서, 로그인 서버는 검증에 실패한 제2 로그인 요청에 따른 각 서비스로의 사용자 액세스를 거절한다 (S532).

[0156] 도 5a - 도 5b는 로그인 서버에 의해서 수행된 프로세스들의 예시일 뿐이다. 다른 상세한 내용들 및 변형들은 각각 도 1 - 도 4 및 첨부된 도면들과 함께 제공된다.

[0157] 추가로, 비록 제1 클라이언트 디바이스 및 제2 클라이언트 디바이스의 행동들이 위의 도면들에서는 언급되지 않았지만, 본 발명이 속한 기술 분야에서의 통상의 지식을 가진 자는 상기 제1 클라이언트 디바이스 및 상기 제2

클라이언트 디바이스 각각이 사용자 및 로그인 서버와의 상호작용 (interaction) 동안에 수행할 단계들을 인지할 것이다. 예시적인 목적을 위해서, 도 6a 및 도 6b는 제1 클라이언트 디바이스 및 제2 클라이언트 디바이스에 의해서 수행되는 예시적인 프로세스들을 제공한다. 몇몇의 실시예들에서, 특별한 클라이언트 디바이스는 한 사용자를 위한 제1 클라이언트 디바이스로서 서빙할 수 있으며 그리고 상이한 사용자를 위한 제2 클라이언트 디바이스로서 서빙할 수 있다. 추가로, 그 특별한 클라이언트 디바이스는 어떤 사용자를 위해서 한 때에는 제1 클라이언트 디바이스로서 또한 서빙하며, 그리고 다른 시각 (예를 들면, 이전 타임을 위해서 설립된 인증 타임 윈도우의 바깥쪽)에서는 그 동일한 사용자를 위한 제2 클라이언트 디바이스로서 서빙할 수 있다.

[0158] 몇몇의 실시예들에서, 도 6a는 제1-레벨 로그인 프로세스가 수행되는 제1 클라이언트 디바이스에 의해서 구현된 예시적인 프로세스를 도시한다.

[0159] 도 6a에서 보이는 것처럼, 상기 제1 클라이언트 디바이스는 제1-레벨 로그인 프로세스를 개시하기 위한 사용자 입력을 사용자로부터 수신한다 (S602). 예를 들면, 상기 사용자 입력은 상기 제1 클라이언트 디바이스 상에 현재 제시된 로그인 서버의 웹페이지 상에 제공된 제1-레벨 로그인 프로세스를 불러내기 위한 링크 또는 사용자 인터페이스 요소로 향한 선택 입력이다.

[0160] 몇몇의 실시예들에서, 제1 클라이언트 디바이스는 부분적인 로그인 정보를 위한 요청을 사용자에게 제시한다 (S604). 예를 들면, 사용자 인터페이스에, 상기 제1 클라이언트 디바이스는 사용자로부터 사용자 이름만을 요청하는 텍스트 입력 필드를 옵션으로 제공한다. 다른 예를 들면, 상기 제1 클라이언트 디바이스는 상기 로그인 서버 또는 상기 제1 클라이언트 디바이스에 의해서 랜덤으로 생성된 익명의 사용자 이름을 이용하여 상기 제1-레벨을 수행하기 위한 옵션을 선택으로 제공한다.

[0161] 몇몇의 실시예들에서, 사용자는 요청된 부분적인 로그인 정보를 제공하며, 그리고 상기 제1 클라이언트는 사용자로부터의 이 부분적인 로그인 정보를 수신한다 (S606). 일부 실시예들에서, 일단 제1 클라이언트 디바이스가 상기 부분적인 로그인 정보를 수신하면, 그 제1 클라이언트 디바이스는 제1-레벨 로그인 요청에서 상기 부분적인 로그인 정보를 로그인 서버에게 송신한다 (S608). 몇몇의 실시예들에서, 제1 클라이언트 디바이스는 제1-레벨 로그인 요청을 위해서 생성된 보안 향상 정보를 상기 로그인 서버로부터 수신한다 (S610). 위에서 설명된 것처럼, 다양한 실시예들에 따라, 상기 로그인 서버로부터 수신된 보안 향상 정보는 상이한 모습들일 수 있으며 그리고 상이한 정보를 포함한다. 몇몇의 실시예들에서, 상기 제1 클라이언트 디바이스는 상이한 클라이언트 디바이스 상에서 어떻게 제2-레벨 로그인 프로세스를 진행하는가에 관한 지시들을 상기 사용자에게 디스플레이한다. 몇몇의 실시예들에서, 상기 제1 클라이언트 디바이스는 상기 수신한 보안 향상 정보를, 예를 들면, 캐릭터 매핑 테이블로서, 또는 CAPTCHA 모습인 캐릭터 매핑 정보로 사용자에게 제시한다 (S612). 상기 제1 클라이언트 디바이스의 행동들의 더욱 상세한 내용들은 위에서 제시되었으며, 그래서 도 6a에 관련하여 여기에서 반복되지 않는다.

[0162] 몇몇의 실시예들에서, 도 6b는 제2-레벨 로그인 프로세스가 수행되는 제2 클라이언트 디바이스에 의해서 구현된 예시적인 프로세스를 도시한다.

[0163] 도 6b에서 보이는 것처럼, 상기 제2 클라이언트 디바이스는 제2-레벨 로그인 프로세스를 개시하기 위한 사용자 입력을 사용자로부터 수신한다 (S614). 상기 제2 클라이언트 디바이스는 상기 사용자와 연관된 완전한 로그인 정보를 위한 제1 요청 그리고 상기 디바이스와는 상이한 다른 디바이스로부터 로그인 서버로 이전에 송신되었던 제1-레벨 로그인 요청에 응답하여 상기 로그인 서버에 의해 상기 사용자에게 제공되었던 각 보안 향상 정보를 위한 각 식별 정보용의 제2 요청을 상기 사용자에게 제시한다 (S616). 예를 들면, 몇몇의 실시예들에서, 상기 제2 클라이언트 디바이스는 사용자 이름 입력 필드, 패스워드 입력 필드, 및 매핑 테이블 일련 번호 입력 필드를 보여주는 로그인 인터페이스를 디스플레이한다. 몇몇의 실시예들에서, 로그인 인터페이스는 완전한 로그인 정보 중 어느 부분이 후-매핑 캐릭터들과 함께 제공되어야만 하는지에 관한 지시를 또한 제공한다. 몇몇의 실시예들에서, 로그인 서버는 완전한 로그인 정보의 포맷을 동적으로 결정하고, 그리고 제2 클라이언트 디바이스를 통해서 사용자에게 지시를 제공한다.

[0164] 몇몇의 실시예들에서, 제2 클라이언트 디바이스는 상기 사용자로부터의 완전한 로그인 정보 그리고 상기 각 보안 향상 정보를 위한 식별 정보를 수신하며 (S618), 상기 완전한 로그인 정보는 상기 각 보안 향상 정보에 따라, 그리고 이용 가능한 경우에는 옵션으로 로그인 서버로부터의 지시에 따라 상기 사용자에 의해서 제공된다.

[0165] 몇몇의 실시예들에서, 사용자가 요청된 정보를 제2 클라이언트 디바이스에게 제공한 이후에, 상기 제2 클라이언

트 디바이스는 제2-레벨 로그인 요청을 상기 로그인 서버에게 송신하며 (S620), 상기 제2-레벨 로그인 요청은 상기 각 보안 향상 정보를 위한 상기 식별 정보 및 각 보안 향상 정보에 따라 제공된 상기 완전한 로그인 정보를 포함한다.

[0166] 몇몇의 실시예들에서, 요청된 정보가 상기 로그인 서버로 송신된 이후에, 상기 제2 클라이언트 디바이스는 상기 각 보안 향상 정보 및 상기 사용자와 연관된 미리-저장된 원래 로그인 정보를 기초로 하여 검증 프로세스를 상기 완전한 로그인 정보가 통과했는가 또는 실패했는가의 여부를 표시하는 로그인 서버로부터의 로그인 응답을 수신한다 (S622). 상기 제1 클라이언트 디바이스의 행동들에 관한 더 상세한 내용들은 위에서 제공되었으며, 도 6b에 관련하여 여기에서는 반복되지 않는다.

[0167] 도 7은 몇몇의 실시예들에 따라, 위에서 설명된 것과 같은 로그 서버로서 서빙할 수 있는 시스템 (700)의 블록도면이다.

[0168] 도 7에서 보이는 것처럼, 상기 시스템 (700)은 하나 또는 그 이상의 프로세싱 유닛들 (또는 "프로세서들") (702), 메모리 (704), 입력/출력 (I/O) 인터페이스 (706), 및 네트워크 통신 인터페이스 (708)를 포함한다. 이 컴포넌트들은 하나 또는 그 이상의 통신 버스들 또는 신호 라인들 (710)을 통해서 서로 통신한다. 몇몇의 실시예들에서, 상기 메모리 (704) 또는 상기 메모리 (704)의 컴퓨터 판독가능 저장 매체는 프로그램들, 모듈들, 명령어들, 그리고 운영 시스템 (712), I/O 모듈 (714), 통신 모듈 (716), 및 동작 제어 모듈 (718) 모두 또는 서브세트를 포함하는 데이터 구조들을 저장한다. 상기 하나 또는 그 이상의 프로세서들 (702)은 상기 메모리 (704)에 연결되며 그리고 이 프로그램들, 모듈들, 및 명령어들을 실행하고, 그리고 상기 데이터 구조들로부터 읽고/상기 데이터 구조들에 쓰도록 동작할 수 있다.

[0169] 몇몇의 실시예들에서, 상기 프로세싱 유닛 (702)은 단일 코어 또는 멀티-코어 마이크로프로세서와 같은 하나 또는 그 이상의 마이크로프로세서들을 포함한다. 몇몇의 실시예들에서, 상기 프로세싱 유닛들 (702)은 하나 또는 그 이상의 범용 프로세서들을 포함한다. 몇몇의 실시예들에서, 상기 프로세싱 유닛들 (702)은 하나 또는 그 이상의 특수 목적 프로세서들을 포함한다. 몇몇의 실시예들에서, 상기 프로세싱 유닛들 (702)은 하나 또는 그 이상의 개인용 컴퓨터들, 모바일 디바이스들, 핸드헬드 컴퓨터들, 테블릿 컴퓨터들, 또는 하나 또는 그 이상의 프로세싱 유닛들을 포함하며 다양한 운영 시스템들 상에서 동작하는 아주 다양한 하드웨어 플랫폼들 중 하나의 하드웨어 플랫폼을 포함한다.

[0170] 몇몇의 실시예들에서, 상기 메모리 (704)는 DRAM, SRAM, DDR RAM 또는 다른 랜덤 액세스 솔리드 스테이트 메모리 디바이스들과 같은 고속의 랜덤 액세스 메모리를 포함한다. 몇몇의 실시예들에서 상기 메모리 (704)는 하나 또는 그 이상의 자기 디스크 저장 디바이스들, 광학 디시크 저장 디바이스들, 플래시 메모리 디바이스들, 또는 다른 비-휘발성 솔리드 스테이트 저장 디바이스들과 같은 비-휘발성 메모리를 포함한다. 몇몇의 실시예들에서, 상기 메모리 (704)는 상기 프로세싱 유닛들 (702)과는 먼 거리에 위치한 하나 또는 그 이상의 저장 디바이스들을 포함한다. 상기 메모리 (704) 또는 대안으로 상기 메모리 (704) 내의 비-휘발성 메모리 디바이스(들)는 컴퓨터 판독가능 저장 매체를 포함한다.

[0171] 몇몇의 실시예들에서, 상기 I/O 인터페이스 (706)는 디스플레이들, 키보드들, 터치 스크린들, 스피커들, 및 마이크로폰들과 같은 입력/출력 디바이스들을 상기 시스템 (700)의 I/O 모듈 (714)로 연결시킨다. 상기 I/O 인터페이스 (706)는 상기 I/O 모듈 (714)과 연결하여 사용자 입력들 (예를 들면, 음성 입력, 키보드 입력, 터치 입력 등)을 수신하고 그리고 그것들을 적절하게 처리한다. 상기 I/O 인터페이스 (706) 그리고 사용자 인터페이스 (714)는 출력들 (예를 들면, 사운드들, 이미지들, 텍스트 등)을 상기 시스템 (700) 상에 구현된 다양한 프로그램 명령어들에 따라 사용자에게 또한 제시한다

[0172] 몇몇의 실시예들에서, 네트워크 통신 인터페이스 (708)는 유선 통신 포트(들) 그리고/또는 무선 전송 및 수신 회로를 포함한다. 유선 통신 포트(들)는 하나 또는 그 이상의 유선 인터페이스들, 예를 들면, 이더넷, USB (Universal Serial Bus), 파이어와이어 (FIREWIRE) 등을 경유하여 통신 신호들을 수신하고 송신한다. 상기 무선 회로는 RF 신호들 및/또는 광 신호들을 통신 네트워크들 및 다른 통신 디바이스들로부터/에게 수신하고/송신한다. 상기 무선 통신은 GSM, EDGE, CDMA, TDMA, Bluetooth, Wi Fi, VoIP, Wi-MAX, 또는 어떤 다른 적합한 통신 프로토콜과 같은 복수의 통신 표준들, 프로토콜들 및 기술들 중 어느 것을 이용할 수 있을 것이다.

[0173] 상기 통신 네트워크 (708)는 인터넷, 인트라넷 및/또는 셀룰러 전화 네트워크, 무선 로컬 영역 네트워크 (LAN) 및/또는 대도시 영역 네트워크 (MAN)와 같은 무선 네트워크 등의 네트워크들을 구비한 시스템 (700)과 다른 디바이스들 사이의 통신을 가능하게 한다. 통신 모듈 (716)은 네트워크 통신 인터페이스 (708)를 통한 상기 시스

템 (700)과 다른 디바이스들 (예를 들면, 상기 제1 클라이언트 디바이스 및 상기 제2 클라이언트 디바이스) 사이의 통신들을 용이하게 한다.

[0174] 몇몇의 실시예들에서, 상기 운영 시스템 (702) (예를 들면, Darwin, RTXC, LINUX, UNIX, OS X, WINDOWS, 또는 VxWorks처럼 내장된 운영 시스템)은 일반적인 시스템 태스크들 (예를 들면, 메모리 관리, 저장 디바이스 제어, 전력 관리 등)을 제어하기 위한 다양한 소프트웨어 컴포넌트들 및/또는 드라이버들을 포함하며 그리고 다양한 하드웨어, 펌웨어, 및 소프트웨어 컴포넌트들 사이의 통신들을 용이하게 한다.

[0175] 몇몇의 실시예들에서, 상기 시스템 (700)은 단독의 컴퓨터 시스템 상에서 구현된다. 몇몇의 실시예들에서, 상기 시스템 (700)은 여러 컴퓨터들을 가로질러 분포된다. 몇몇의 실시예들에서, 상기 시스템 (700)의 모듈들 및 기능들 중 몇몇은 서버 부분과 클라이언트 부분으로 분할되며, 이 경우에 상기 클라이언트 부분은 사용자 디바이스 (예를 들면, 상기 제1 클라이언트 디바이스 및 상기 제2 클라이언트 디바이스) 상에 존재하며 그리고 서버 디바이스 상에 존재하는 상기 서버 부분과 하나 또는 그 이상의 네트워크를 통해서 통신한다. 상기 시스템 (700)은 운영 서버 시스템의 한 예일 뿐이며, 그리고 그 시스템 (700)은 도시된 것보다 더 많은 또는 더 작은 개수의 컴포넌트들을 구비할 수 있을 것이며, 둘 또는 그 이상의 컴포넌트들을 결합할 수 있을 것이며, 또는 상이한 구성의 컴포넌트들 또는 컴포넌트들의 배치를 가질 수 있을 것이라는 것에 유의해야 한다. 도 7에서 보이는 다양한 컴포넌트들은 하나 또는 그 이상의 신호 프로세싱 및/또는 애플리케이션 특정 집적 회로들, 또는 그것들의 결합을 포함하는 하드웨어, 소프트웨어, 펌웨어로 구현될 수 있을 것이다.

[0176] 도 7에서 보이는 것처럼, 상기 시스템 (700)은 메모리 (704) 내에 동작 제어 모듈 (718)을 저장한다. 몇몇의 실시예들에서, 상기 동작 제어 모듈 (718)은 다음의 서브-모듈들, 또는 그것들의 서브세트나 슈퍼세트 (superset)를 더 포함한다: 제1-레벨 로그인 모듈 (720), 제2-레벨 로그인 모듈 (722). 몇몇의 실시예들에서, 상기 제1-레벨 로그인 모듈 (720)은 보안 정보 생성 모듈 (724)을 더 포함한다. 몇몇의 실시예들에서, 상기 제2-레벨 로그인 모듈 (722)은 보안 정보 검증 모듈 (726)을 더 포함한다. 추가로, 이 서브-모듈들 각각은 동작 제어 모듈 (718)의 다음의 데이터 구조들 그리고 데이터 소스들 중 하나 또는 그 이상 , 또는 그것들의 서브세트 또는 슈퍼세트에 대한 액세스를 구비한다: 인증 윈도우가 기간 만료되지 않은 각 제1-레벨 로그인 요청을 위해서 생성된 매핑 테이블들을 포함하는 매핑 테이블 데이터베이스 (728) 그리고 다양한 사용자들과 연관된 개인적인 로그인 정보의 원래의 모습들을 포함하는 로그인 정보 데이터베이스 (730). 몇몇의 실시예들에서, 상기 동작 제어 모듈은 여기에서 설명된 다른 관련된 기능성들을 제공하기 위해서 하나 또는 그 이상의 다른 모듈들 (732) (예를 들면, 로그인-레벨 선택 모듈)을 옵션으로 포함한다. 상기 동작 제어 모듈 (718)의 데이터 구조들 그리고 서브-모듈들의 구조들, 기능들, 및 상호작용들에 관한 더욱 상세한 내용들은 도 1 내지 도 6b 및 첨부된 설명들에 관하여 제공된다.

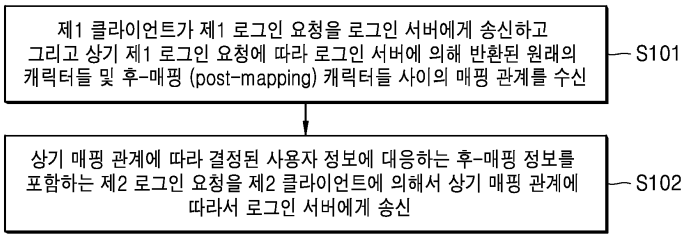
[0177] 본 발명이 속한 기술 분야에서의 통상의 지식을 가진 자가 인지할 것처럼, 상기 제1 클라이언트 디바이스 및 상기 제2 클라이언트 디바이스는 상기 예시적인 시스템 (700)의 일부 (예를 들면, 상기 클라이언트 부분들)로서 구현될 수 있다. 몇몇의 실시예들에서, 상기 예시적인 시스템 (700)고 유사한 시스템이 상기 제1 클라이언트 디바이스 및 상기 제2 클라이언트 디바이스를 구현하기 위해서 사용될 수 있다. 상기 클라이언트 디바이스들의 대응하는 모듈들 및 기능들은 클라이언트 디바이스들로서 서빙하는 시스템들의 동작 제어 모듈 (718) 내에 제공될 수 있다.

[0178] 상기 매핑 관계를 생성하기 위한 방법, 사용자 정보 내에 특별하게 포함된 콘텐트 및 상기 매핑 관계 일련 번호를 생성하기 위한 방법 등과 같이 본 발명에서 로그인 인증을 위한 시스템에서의 다양한 모듈들 등의 특별한 구현 방법들은 본 발명에서 로그인 인증을 위한 상기 언급된 방법에서의 방법들과 동일할 수 있으며, 그래서 그것들의 나머지 설명은 여기에서 하지 않을 것이다.

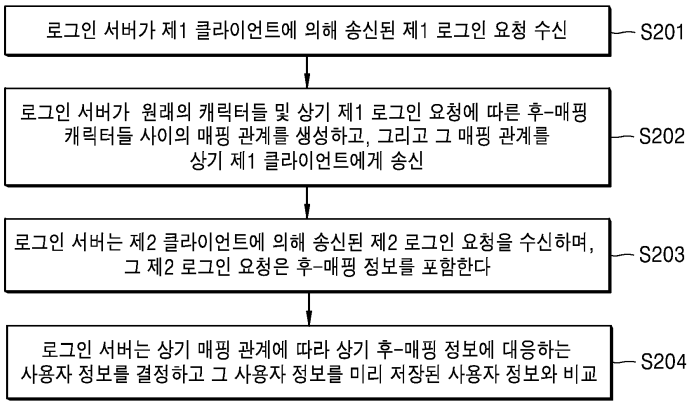
[0179] 상기 언급된 실시예들은 본 발명의 여러 구현 방법들을 설명할 뿐이다. 그 구현 방법들의 상기 설명은 상대적으로 특정되며 상세하지만, 그것은 본 발명의 범위에 대한 제한들로서 이해될 수는 없다. 본 발명의 개념을 벗어나지 않으면서도 여러 변형들 및 개선들이 만들어질 수 있으며, 그리고 그것들은 본 발명의 보호 범위 내에 속한다는 것을, 본 발명이 속한 기술 분야에서의 통상의 지식을 가진 자들은 유의해야 한다. 그러므로, 본 발명 특허의 보호 범위는 첨부된 청구항들을 기초로 해야만 한다.

도면

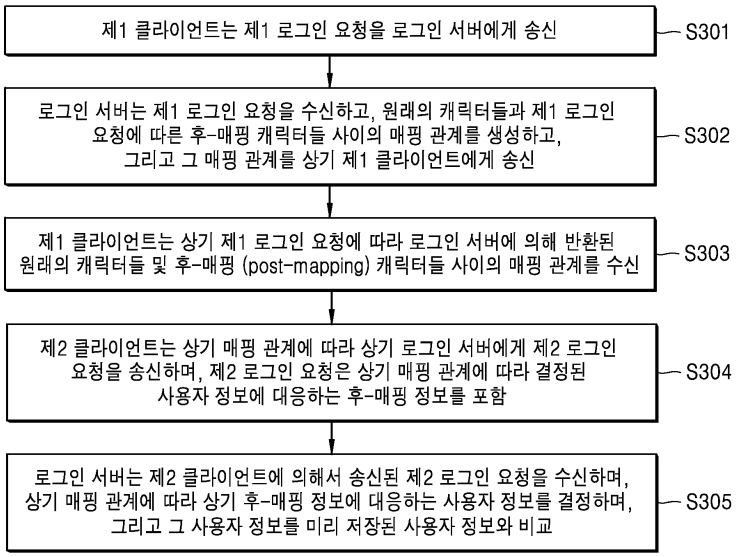
도면1



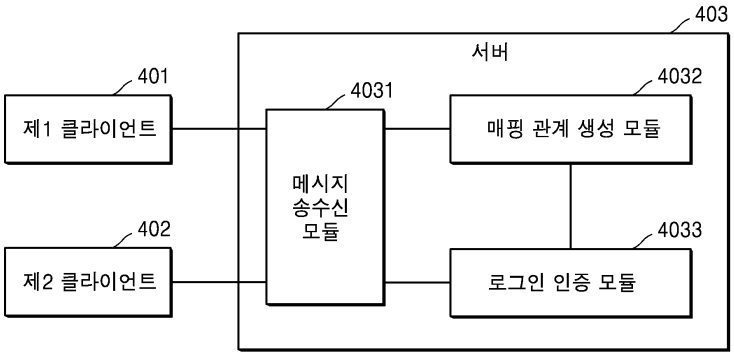
도면2



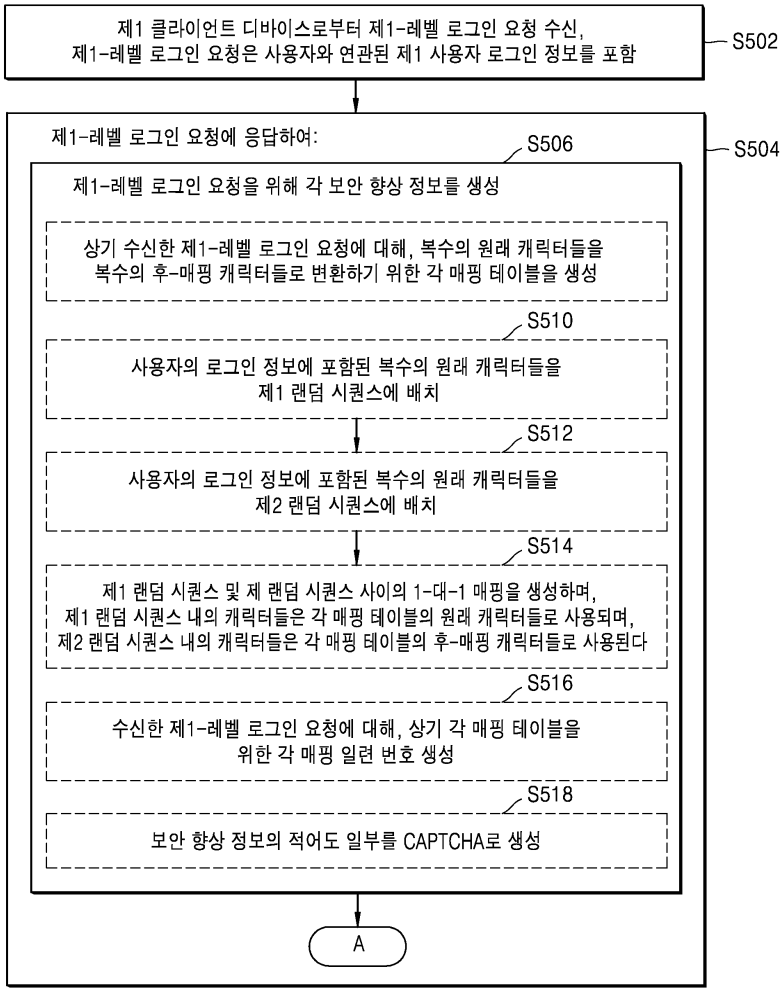
도면3



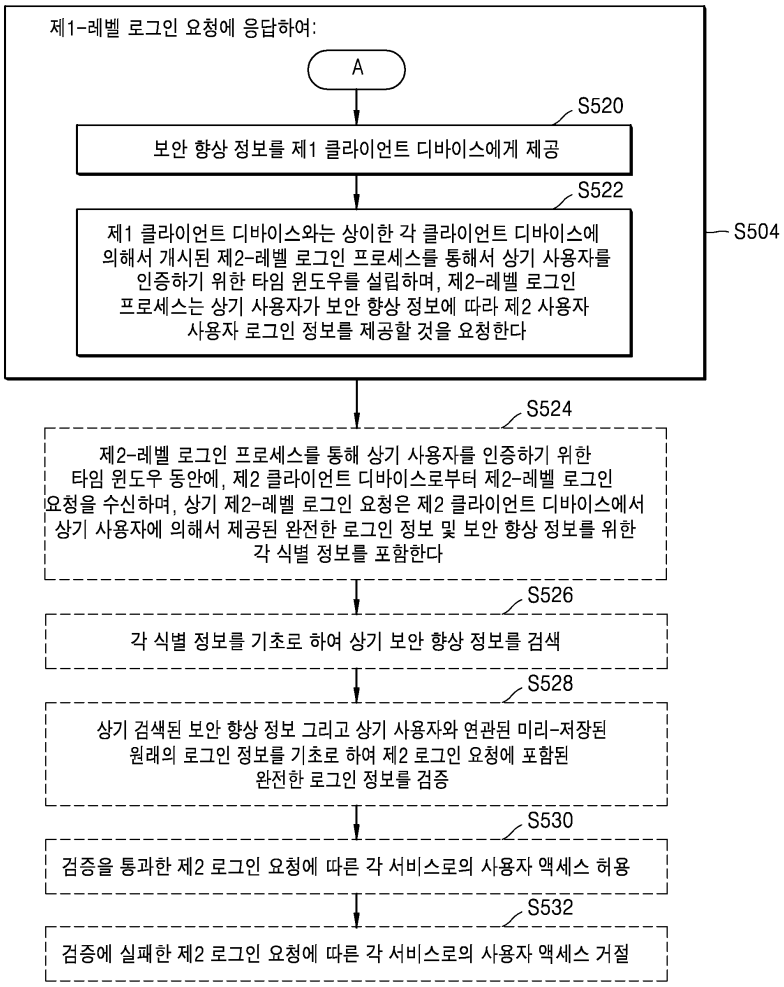
도면4


403
서버
401
제1 클라이언트
402
제2 클라이언트
4031
메시지
송수신
모듈
4032
매핑 관계 생성 모듈
4033
로그인 인증 모듈

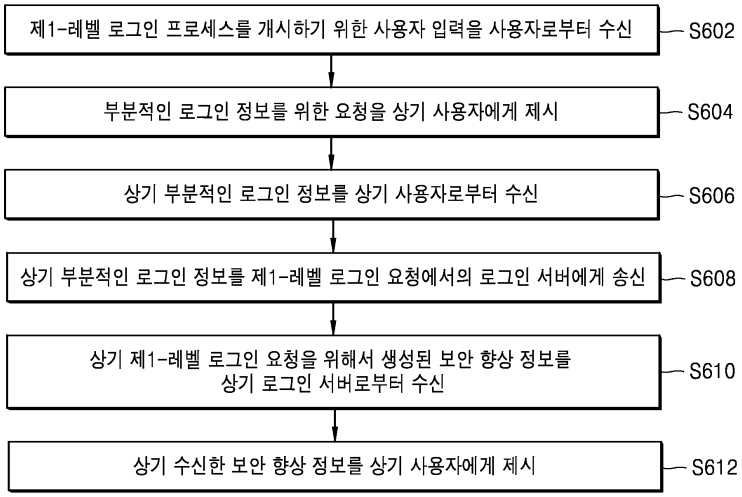
도면5a


제1 클라이언트 디바이스로부터 제1-레벨 로그인 요청 수신,
제1-레벨 로그인 요청은 사용자와 연관된 제1 사용자 로그인 정보를 포함
S502
제1-레벨 로그인 요청에 응답하여:
S504
S506
제1-레벨 로그인 요청을 위해 각 보안 향상 정보를 생성
상기 수신한 제1-레벨 로그인 요청에 대해, 복수의 원래 캐릭터들을
복수의 후-매핑 캐릭터들로 변환하기 위한 각 매핑 테이블을 생성
S510
사용자의 로그인 정보에 포함된 복수의 원래 캐릭터들을
제1 랜덤 시퀀스에 배치
S512
사용자의 로그인 정보에 포함된 복수의 원래 캐릭터들을
제2 랜덤 시퀀스에 배치
S514
제1 랜덤 시퀀스 및 제 랜덤 시퀀스 사이의 1-대-1 매핑을 생성하며,
제1 랜덤 시퀀스 내의 캐릭터들은 각 매핑 테이블의 원래 캐릭터들로 사용되며,
제2 랜덤 시퀀스 내의 캐릭터들은 각 매핑 테이블의 후-매핑 캐릭터들로 사용된다
S516
수신한 제1-레벨 로그인 요청에 대해, 상기 각 매핑 테이블을
위한 각 매핑 일련 번호 생성
S518
보안 향상 정보의 적어도 일부를 CAPTCHA로 생성
A

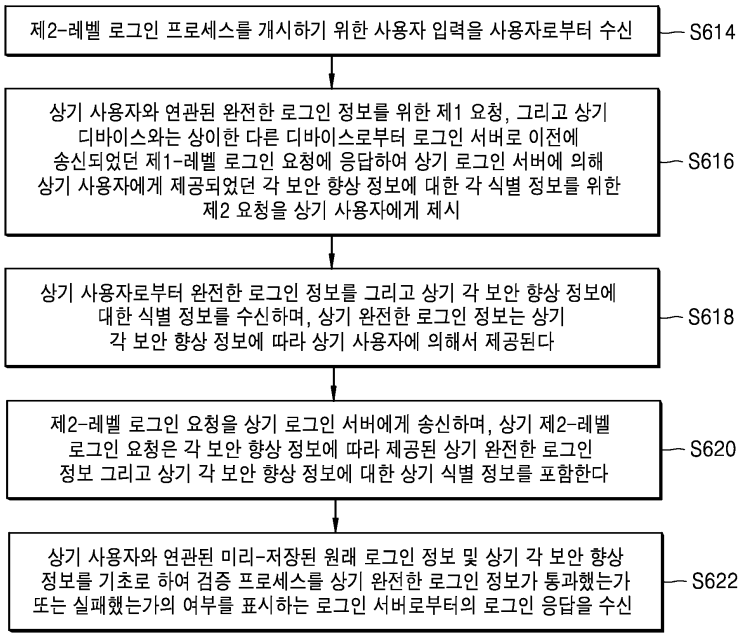
도면5b


제1-레벨 로그인 요청에 응답하여:
A
S520
보안 향상 정보를 제1 클라이언트 디바이스에게 제공
S522
제1 클라이언트 디바이스와는 상이한 각 클라이언트 디바이스에 의해서 개시된 제2-레벨 로그인 프로세스를 통해서 상기 사용자를 인증하기 위한 타임 윈도우를 설립하며, 제2-레벨 로그인 프로세스는 상기 사용자가 보안 향상 정보에 따라 제2 사용자 사용자 로그인 정보를 제공할 것을 요청한다
S504
S524
제2-레벨 로그인 프로세스를 통해 상기 사용자를 인증하기 위한 타임 윈도우 동안에, 제2 클라이언트 디바이스로부터 제2-레벨 로그인 요청을 수신하며, 상기 제2-레벨 로그인 요청은 제2 클라이언트 디바이스에서 상기 사용자에 의해서 제공된 완전한 로그인 정보 및 보안 향상 정보를 위한 각 식별 정보를 포함한다
S526
각 식별 정보를 기초로 하여 상기 보안 향상 정보를 검색
S528
상기 검색된 보안 향상 정보 그리고 상기 사용자와 연관된 미리-저장된 원래의 로그인 정보를 기초로 하여 제2 로그인 요청에 포함된 완전한 로그인 정보를 검증
S530
검증을 통과한 제2 로그인 요청에 따른 각 서비스로의 사용자 액세스 허용
S532
검증에 실패한 제2 로그인 요청에 따른 각 서비스로의 사용자 액세스 거절

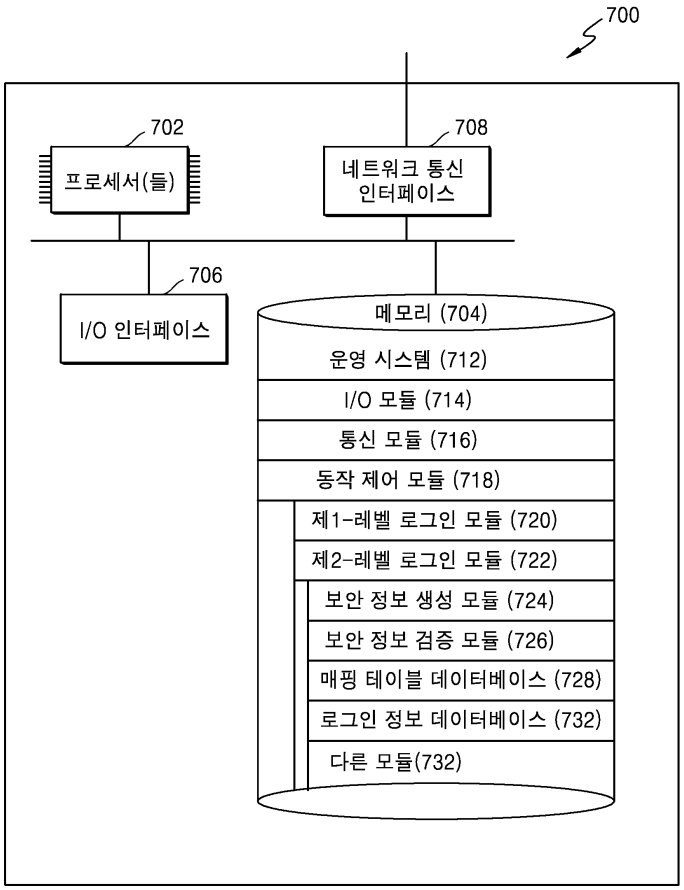
도면6a


제1-레벨 로그인 프로세스를 개시하기 위한 사용자 입력을 사용자로부터 수신
S602
부분적인 로그인 정보를 위한 요청을 상기 사용자에게 제시
S604
상기 부분적인 로그인 정보를 상기 사용자로부터 수신
S606
상기 부분적인 로그인 정보를 제1-레벨 로그인 요청에서의 로그인 서버에게 송신
S608
상기 제1-레벨 로그인 요청을 위해서 생성된 보안 향상 정보를 상기 로그인 서버로부터 수신
S610
상기 수신한 보안 향상 정보를 상기 사용자에게 제시
S612

도면6b


제2-레벨 로그인 프로세스를 개시하기 위한 사용자 입력을 사용자로부터 수신
S614
상기 사용자와 연관된 완전한 로그인 정보를 위한 제1 요청, 그리고 상기 디바이스와는 상이한 다른 디바이스로부터 로그인 서버로 이전에 송신되었던 제1-레벨 로그인 요청에 응답하여 상기 로그인 서버에 의해 상기 사용자에게 제공되었던 각 보안 향상 정보에 대한 각 식별 정보를 위한 제2 요청을 상기 사용자에게 제시
S616
상기 사용자로부터 완전한 로그인 정보를 그리고 상기 각 보안 향상 정보에 대한 식별 정보를 수신하며, 상기 완전한 로그인 정보는 상기 각 보안 향상 정보에 따라 상기 사용자에 의해서 제공된다
S618
제2-레벨 로그인 요청을 상기 로그인 서버에게 송신하며, 상기 제2-레벨 로그인 요청은 각 보안 향상 정보에 따라 제공된 상기 완전한 로그인 정보 그리고 상기 각 보안 향상 정보에 대한 상기 식별 정보를 포함한다
S620
상기 사용자와 연관된 미리-저장된 원래 로그인 정보 및 상기 각 보안 향상 정보를 기초로 하여 검증 프로세스를 상기 완전한 로그인 정보가 통과했는가 또는 실패했는가의 여부를 표시하는 로그인 서버로부터의 로그인 응답을 수신
S622

도면7


700
702
프로세서(들)
708
네트워크 통신 인터페이스
706
I/O 인터페이스
메모리 (704)
운영 시스템 (712)
I/O 모듈 (714)
통신 모듈 (716)
동작 제어 모듈 (718)
제1-레벨 로그인 모듈 (720)
제2-레벨 로그인 모듈 (722)
보안 정보 생성 모듈 (724)
보안 정보 검증 모듈 (726)
매핑 테이블 데이터베이스 (728)
로그인 정보 데이터베이스 (732)
다른 모듈(732)