

(19)대한민국특허청(KR)

(12) 공개특허공보(A)

(51) Int. Cl.⁸

G06Q 30/00J0 (2006.01)

G06F 15/00 (2006.01)

(11) 공개번호 10-2006-0002000

(43) 공개일자 2006년01월06일

(21) 출원번호 10-2005-0130119(분할)

(22) 출원일자 2005년12월26일

(62) 원출원 특허10-2002-0024895

원출원일자 : 2002년05월07일

심사청구일자

2003년11월17일

(71) 출원인 주식회사 비즈모델라인

서울특별시 강남구 역삼동 830-67 타호비즈니스센터

주식회사 사이버카드

서울특별시 강남구 대치동 999-4 나실빌딩 1층

(72) 발명자

김재형

서울 종로구 구기동 40 동익빌라 4-203

김종률

서울 강남구 삼성동 79 홍실아파트 4동 402호

홍종철

서울 마포구 연남동 260-4

윤종민

인천 남동구 구월3동 1121-18

심사청구 : 있음

(54) 아이씨 카드(스마트 카드 포함)를 이용한 웹사이트 로그인 및 게임 아이템 저장 방법 및 시스템

요약

본 발명은 IC카드(스마트 카드 포함)를 이용한 웹사이트 로그인 및 게임 아이템 저장 방법 및 시스템에 관한 것으로서, 스마트 카드 구동 프로그램을 구비한 클라이언트 시스템(PC 등의 스마트 카드 리더기를 포함한 시스템) 상에서 인터넷을 통해 웹서버(게임서버 포함)로 클라이언트 로그인 요청을 수신하는 단계와, 상기 로그인 요청에 따라, 클라이언트 시스템으로 로그인에 필요한 암호화 데이터를 요구하는 단계와, 클라이언트 시스템 상에서 스마트 카드에 내장된 IC칩 고유번호(Serial Number)를 이용하여 암호화하여 상기 웹서버로 전송하는 단계와, 클라이언트 시스템으로부터 전송된 암호화 데이터를 복호화하여 클라이언트 인증을 확인하는 단계와, 인증이 확인된 클라이언트에게 로그인을 허용하고, 상기 스마트 카드로 게임용 및 아바타 아이템 등의 저장 기능을 유효하게 하는 단계를 포함하여 구성된다.

본 발명에 따르면, 스마트 카드를 이용하여 온라인 게임 등에 안전한 로그인을 실시할 수 있으므로, 타 클라이언트에 의한 아이디 및 패스워드 도용을 미연에 방지할 수 있으며, 클라이언트가 보유한 게임이나 아바타 아이템 등을 안전하게 저장 및 보호할 수 있다.

대표도

도 1

색인어

스마트 카드, 고유번호, 암호화

명세서

도면의 간단한 설명

도1은 본 발명이 구현되는 간단한 구성도이다.

도2는 본 발명이 실시되는 전체적인 과정에 대한 간단한 흐름도이다.

도3은 클라이언트의 시스템에서 암호화된 데이터의 작성과정에서부터 이를 수신한 웹서버가 복호화하는 과정에 대한 간단한 흐름도이다.

도4는 클라이언트가 스마트 카드를 이용하여 로그인 한 후에, 클라이언트가 보유 또는 사용하고 있는 아이템(아바타 또는 게임 등)을 상기 스마트 카드에 저장하는 과정에 대한 간단한 흐름도이다.

<도면의 주요부분에 대한 설명>

100 : 웹서버(게임서버 포함) 105 : 로그인 인증 시스템

110 : 암호화 계산모듈 115 : 인증모듈

120 : 개인정보 데이터 베이스 125 : 아이템 관리 시스템

130 : 업/다운로딩 모듈 135 : 아이템 정보 데이터 베이스

140 : 전송모듈 145 : 클라이언트

150 : 제휴 웹사이트

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 IC카드(스마트 카드 포함)를 이용한 웹사이트 로그인 및 게임 아이템 저장 방법 및 시스템에 관한 것으로써, 스마트 카드 구동 프로그램을 구비한 클라이언트 시스템(PC 등의 스마트 카드 리더기를 포함한 시스템) 상에서 인터넷을 통해 웹서버(게임서버 포함)로 클라이언트 로그인 요청을 수신하여 상기 클라이언트 시스템으로 로그인에 필요한 암호화 데이터를 요구하고, 클라이언트 시스템 상에서 스마트 카드에 내장된 IC칩 고유번호(Serial Number)를 이용하여 암호화되어 전송된 암호 데이터를 복호화하여 클라이언트 인증을 확인한 후, 클라이언트의 로그인을 허용 및 상기 스마트 카드로 게임용 및 아바타 아이템 등의 저장 기능을 제공하는 것이다.

인터넷의 발달로 온라인 상에 많은 웹사이트들이 생겨나게 되었는데, 최근에는 다수의 웹사이트들이 클라이언트의 회원가입을 통해 해당 클라이언트를 식별할 수 있는 로그인 아이디 및 패스워드를 제공하고 있으며, 클라이언트는 상기 부여받은 아이디 및 패스워드를 이용하여 해당 웹사이트에 접속을 실시하고, 상기 웹사이트는 클라이언트가 입력한 아이디 및 패스워드를 통해 각각의 개별 클라이언트를 식별하고 있다.

또한, 해당 웹사이트가 클라이언트로부터 특정 IP주소 정보를 획득하여, 다수 클라이언트의 다수 IP주소 정보를 보유하고, 접속을 시도하는 IP주소를 확인하여 접속을 허용하는 방법, 하나의 PC에 접속을 허가하는 인증서와 개인키를 사용하여 클라이언트에게 접속을 허락하는 방법 및 클라이언트 지문, 홍채, 음성인식 및 원타임 패스워드(Onetime Password) 방법들이 존재하고 있다.

그러나, 상기 기술한 클라이언트의 로그인 식별방법에서, 클라이언트에게 아이디 및 패스워드를 제공하는 방식은 클라이언트가 외워야 하는 아이디 및 패스워드 수가 많아지게 되면, 잊어버릴 수 있거나, 해킹 등의 문제가 제기되고 있으며, 서버에서 다수 클라이언트의 접속허용 IP주소를 관리하는 방식은 다수 IP주소 관리에 대한 번거로움이 존재할 수 있으며, 클라이언트가 해당 IP주소에서만 접속이 가능하다는 문제점이 있었다.

각 클라이언트에게 인증서 및 개인키를 제공하여 개인 PC에 저장하도록 하는 방식은 하나의 PC에만 저장하게 되므로, 이동성이나 안전성 등에 문제가 있었고, 지문이나 홍채 등의 생체인식 및 원타임 패스워드 제공 방식은 해당 단말기의 값이 고가이거나 로그인에만 적용이 되고, 동일 세션 내에 연속작업에 적용하기가 힘들다는 단점이 있다.

발명이 이루고자 하는 기술적 과제

상기와 같은 문제점들을 보완하기 위한 본 발명의 목적은 스마트 카드 구동 프로그램을 구비한 클라이언트 시스템(PC 등의 스마트 카드 리더기를 포함한 시스템) 상에서 인터넷을 통해 웹서버(게임서버 포함)로 클라이언트 로그인 요청을 수신하여 상기 클라이언트 시스템으로 로그인에 필요한 암호화 데이터를 요구하고, 클라이언트 시스템 상에서 스마트 카드에 내장된 IC칩 고유번호(Serial Number)를 이용하여 암호화된 암호화 데이터를 수신하여 이를 복호화하여 클라이언트 인증을 확인한 후, 클라이언트의 로그인을 허용 및 상기 스마트 카드로 게임용 및 아바타 아이템 등의 저장 기능을 제공하도록 하는 방법 및 시스템을 제공함에 있다.

발명의 구성 및 작용

본 발명은 IC카드(스마트 카드 포함)를 이용한 웹사이트 로그인 및 게임 아이템 저장 방법 및 시스템에 관한 것으로써, 스마트 카드 구동 프로그램을 구비한 클라이언트 시스템(PC 등의 스마트 카드 리더기를 포함한 시스템) 상에서 인터넷을 통해 웹서버(게임서버 포함)로 클라이언트 로그인 요청을 수신하는 단계와, 상기 로그인 요청에 따라, 클라이언트 시스템으로 로그인에 필요한 암호화 데이터를 요구하는 단계와, 클라이언트 시스템 상에서 스마트 카드에 내장된 IC칩 고유번호(Serial Number)를 이용하여 암호화하여 상기 웹서버로 전송하는 단계와, 클라이언트 시스템으로부터 전송된 암호화된 데이터를 복호화하여 클라이언트 인증을 확인하는 단계와, 인증이 확인된 클라이언트에게 로그인을 허용하고, 상기 스마트 카드로 게임용 및 아바타 아이템 등의 저장 기능을 유효하도록 하는 단계를 포함하여 구성된다.

본 발명의 네트워크 구성요소로는 클라이언트의 스마트 카드 정보를 이용하여 안전하게 로그인 등의 기능을 제공하는 웹서버(게임서버 포함)와, 상기 웹서버에 본인의 스마트 카드를 통해 접속을 실시하고, 또한, 게임이나 아바타 등의 아이템을 상기 스마트 카드에 안전하게 기록하여 보관 등을 하는 적어도 하나 이상의 클라이언트로 구성되는 것을 특징으로 한다.

본 발명에 따르면, 웹서버는 스마트 카드를 가지고 로그인을 요청하는 클라이언트를 인식하고, 상기 클라이언트의 시스템(PC 등의 스마트 카드 리더기를 포함한 시스템)으로부터 전송되는 로그인 요청 암호화 데이터(칩 고유 일련번호, 서버시간, 암호문(Cryptogram) 등)를 해독하여, 클라이언트의 스마트 카드를 이용한 로그인 인증을 실시하고, 로그인이 허락된 클라이언트에게 상기 스마트 카드로의 게임이나 아바타 아이템 등의 업로딩(Up Loading) 또는 다운로드(Down Loading) 기능을 보유하고 있으며, 또한, 스마트 카드에서 웹 상으로 업로딩 되는 데이터들은 임의의 삭제가 가능할 수 있음을 밝힌다.

또한, 본 발명에 따르면, 암호화 또는 복호화 데이터는 클라이언트가 보유한 스마트 카드에 장착된 IC칩의 고유 일련번호(Serial Number)가 사용되며, 상기 IC칩의 고유 일련번호는 위조, 변조 및 복제 등이 불가능한 하드웨어적인 유일한 번호이며, 본 발명의 원활한 실시를 위해서 상기 웹서버는 미리 클라이언트로부터 해당 IC칩의 고유 일련번호 정보를 등록 받아서 데이터 베이스에 저장할 수 있음을 명기한다.

또한, 본 발명은 기존의 인터넷 클라이언트 식별방법과 비교하여 보다 보안적인 측면을 강화한 것이며, 상기 기존의 클라이언트 식별방법과 병행하여 사용이 가능하며, 회원이 아닌 경우라도, 일정 시간 동안 접근(접속) 권한 부여 및 회수가 가능할 수 있으며, 본 웹서버와 제휴관계에 있는 타 사이트와 연동해서도 본 발명이 실시될 수 있음을 밝힌다.

이하, 본 발명의 바람직한 실시 예에 대하여 첨부도면을 참조하여 상세히 설명한다. 우선 각 도면의 구성요소들에 대해 참조부호를 부가함에 있어서, 동일한 구성요소들에 한해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호로 표기되었음에 유의하여야 한다. 또한, 하기의 설명에서는 본 발명의 실시 예를 설명하기 위하여 구체적인 구성요소 등과 같은 많은 특정사항들이 도시되어 있는데, 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐 이러한 특정 사

항들 없이도 본 발명이 실시될 수 있음은 이 기술분야에서 통상의 지식을 가진 자에게는 자명하다할 것이다. 그리고, 본 발명을 설명함에 있어서, 관련된 공지 기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

또한, 본 발명에 보다 더 충실하도록 하기 위해서, 본 발명의 취지를 벗어나지 않는 범위 내에서 당업자 수준의 변경이나 변형이 있을 수 있음을 명기하는 바이다.

도1은 본 발명이 구현되는 간단한 구성도이다.

본 도면은 클라이언트(145)가 본인의 스마트 카드를 이용하여 웹서버(게임서버 포함)(100)에 로그인을 실시하면, 상기 웹서버(100)는 상기 클라이언트(145)의 스마트 카드에 장착된 IC칩(Chip) 고유 일련번호를 파악하여 클라이언트(145)를 식별하여, 로그인을 허용하도록 하는 시스템에 대한 간단한 구성도이다.

웹서버(100)는 로그인 인증 시스템(105) 및 아이템 관리 시스템(125) 등으로 구성되어 있으며, 각각의 구체적인 기능은 다음과 같다.

로그인 인증 시스템(105)은 클라이언트(145)의 접속허가 여부를 판단하여, 클라이언트(145)의 본인 인증이 완료되면 상기 클라이언트(145)의 로그인을 허락하도록 하는 기능을 하며, 암호화 계산 모듈(110), 인증처리모듈(115) 및 개인정보 데이터 베이스(120)로 구성되어 있다.

암호화 계산 모듈(110)은 본인의 스마트 카드를 이용하여 로그인을 시도하는 클라이언트(145)를 인지하고, 상기 클라이언트(145)가 접속하고 있는 클라이언트(145) 시스템(PC 등의 스마트 카드 리더기를 포함한 시스템)으로, 로그인을 인증할 수 있는 암호화 데이터를 요청하며, 상기 클라이언트(145) 시스템에서 형성된 로그인 암호화 데이터를 수신하여 이를 복호화하여 상기 클라이언트(145)의 로그인 인증을 확인하고, 상기 클라이언트(145)의 로그인 접속을 허락하는 역할을 한다.

보다 구체적으로 설명하며, 상기 암호화 계산 모듈은 클라이언트(145)의 웹사이트 접속 및 로그인 요청에 따라, 인증을 위한 조회명령 및 서버시간 등이 포함된 전문 데이터를 상기 클라이언트(145)가 스마트 카드로 접속한 클라이언트(145) 시스템(PC 등의 스마트 카드 리더기를 포함한 시스템)으로 전송하고, 클라이언트(145) 시스템으로부터 전송된 로그인 암호화 데이터(칩 고유 일련번호, 서버시간, 암호문(Cryptogram))를 확인하고, 상기 암호화 데이터 내에 포함된 각 요소(Factor)들을 이용하여 클라이언트(145)의 로그인 인증을 위한 복호화를 실시하는 역할을 한다.

인증모듈(115)은 상기 암호화 계산 모듈(110)을 통해 상기 클라이언트(145)가 전송한 로그인 인증 데이터의 분석이 완료되면, 상기 클라이언트(145)의 로그인 인증을 확인하여, 클라이언트(145) 스마트 카드로의 안전한 로그인이 가능하도록 하며, 인증확인정보를 하기에 기술할 아이템 관리 시스템에 전송하여 인증이 확인된 클라이언트(145)가 본인의 게임 및 아바타 아이템 등을 상기 스마트 카드에 저장하도록 돕는 역할을 한다.

개인정보 데이터 베이스(120)는 클라이언트(145)의 개인정보(이름, 아이디, 패스워드, 주소, 핸드폰 번호 등)가 저장되어 있으며, 또한, 본 발명에 따른 클라이언트(145)의 스마트 카드에 탑재된 IC칩의 고유 일련번호(Serial Number)가 저장되어 있다.

아이템 관리 시스템(125)은 본인의 스마트 카드로 안전하게 로그인이 완료된 클라이언트(145)가 본인의 아이템(게임이나 아바타 등) 등을 일부 또는 전부를 선택하여 상기 스마트 카드로 저장하여 관리하도록 하는 역할을 하며, 업/다운(Up/Down) 로딩 모듈(130) 및 아이템 정보 데이터 베이스(135)로 구성되어 있다.

업/다운 로딩 모듈(130)은 로그인 인증이 완료된 클라이언트(145)가 보유한 아이템(게임이나 아바타 아이템 등)을 상기 클라이언트(145)의 스마트 카드의 데이터 영역에 다운로드(Down Loading) 하여 저장하거나, 상기 스마트 카드에 저장되어 있던 아이템들을 업로딩(Up Loading)하는 역할을 한다.

또한, 본 발명에 따르면, 상기 다운로드되는 데이터는 임의 삭제가 불가능하며, 임의 삭제는 업로딩되는 데이터만이 가능하도록 한다.

아이템 정보 데이터 베이스(135)는 클라이언트(145)의 스마트 카드와 웹서버(100)와 상호교환되어 업로딩 또는 다운로드되는 클라이언트(145)의 아이템(게임 또는 아바타 아이템 등) 들에 관한 정보가 기록되어 있는 데이터 베이스이다.

전송모듈(140)은 웹서버(100)에서 처리되어 클라이언트(145)와 주고받는 각종 데이터의 전송 및 수신 기능을 하며, 인터넷을 통한 송·수신 및 개인정보 데이터 베이스(120)와 연동하여 클라이언트(145) 로그인 내역 및 아이템의 업·다운 로딩 내역을 해당 이벤트가 발생할 시에 클라이언트(145)의 요청에 따라 자동으로 전송하여 줌으로써, 보다 안전한 유저 인터페이스(User Interface)를 유지할 수 있도록 돕는 역할을 한다.

클라이언트(145)는 본인의 스마트 카드로 로그인을 실시하려는 인터넷 상의 유저(User)를 의미하며, 기본적으로 스마트 카드의 리드/라이트(Read/Write)가 가능한 카드리더기가 연결된 시스템(인터넷 연결이 가능한 PC 등)을 통해 상기 웹서버(100)에 접근을 하며, 상기 시스템에는 상기 웹서버(100)와 연동이 가능하고 스마트 카드를 관리하는 응용 프로그램이 탑재되어 있다.

웹서버(100)에 로그인하려는 클라이언트(145)는 상기 프로그램 등을 이용하여 스마트 카드에 장착된 IC칩 고유 일련번호 등을 가지고, 암호화 데이터를 작성하여 상기 웹서버(100)로 전송하는 역할을 한다. 상기 암호화 데이터는 클라이언트(145)의 로그인 인증 데이터로써, 상기 웹서버(100)가 이를 해석하여 클라이언트(145)의 로그인 인증을 할 수 있다.

본 발명에 따르면, 스마트 카드에 장착된 칩(Chip)의 고유 일련번호를 이용하여, 클라이언트(145)의 스마트 카드 로그인을 가능하게 함으로써, 보다 안전한 로그인 시스템을 구축하게 될 수 있다.

도2는 본 발명이 실시되는 전체적인 과정에 대한 간단한 흐름도이다.

클라이언트(145)가 본인의 스마트 카드를 이용하여 웹서버(100)에 접속을 시도하면(200), 상기 웹서버(100)는 클라이언트(145)의 접속 요청을 수신하고, 상기 클라이언트(145)에게 인증을 위한 암호화 데이터를 요청하게 된다(205).

클라이언트(145)는 본인이 사용하고 있는 시스템(PC 등의 스마트 카드 리더기를 포함한 시스템)을 통해 상기 스마트 카드에 탑재된 IC칩의 고유 일련번호가 포함된 암호화 데이터를 작성하고, 작성된 암호화 데이터를 웹서버(100)로 전송하게 된다(210).

웹서버(100)는 클라이언트(145)로부터 전송된 암호화 데이터를 수신하고(215), 이를 해석하여 클라이언트(145)의 인증을 확인하게 된다(220). 인증이 확인되면, 상기 클라이언트(145)의 로그인을 허용하고 또한, 보유 아이템의 업/다운 로딩 등도 가능하도록 한다(230). 만약 인증 확인이 이루어지지 않으면, 로그인 거부 메시지를 전송하게 된다(225).

또한, 보다 안전한 로그인 작업을 위해 클라이언트(145)의 로그인이 실시됨과 동시에 클라이언트(145)의 핸드폰으로 로그인 내역을 전송하게 되며(235), 또한, 클라이언트(145)가 보유한 아이템 등의 업/다운 로딩 작업이 요청되면, 그 내역을 상기의 경우와 마찬가지로 클라이언트(145)의 핸드폰으로 전송하게 된다(240).

모든 작업이 완료되어, 클라이언트(145)가 로그 아웃을 요청하면, 상기 웹서버(100)는 클라이언트(145)와 연결된 세션을 종료하고, 클라이언트(145)의 사용 내역을 데이터 베이스에 저장한다(245).

도3은 클라이언트(145)의 시스템에서 암호화된 데이터의 작성과정에서부터 이를 수신한 웹서버(100)가 복호화하는 과정에 대한 간단한 흐름도이다.

웹서버(100)는 클라이언트(145)로부터 스마트 카드를 이용한 로그인 요청을 수신하고(300), 상기 클라이언트(145)가 스마트 카드를 가지고 접속한 클라이언트(145) 시스템으로 로그인 인증을 위해 필요한 암호화 데이터를 요청하고, 암호화 데이터 구성을 위한 서버시간 등을 전송한다(305).

클라이언트(145) 시스템은 웹서버로부터 전송된 서버시간 등을 수신하고(310), 상기 시스템에 연결된 스마트 카드의 칩(Chip) 일련번호를 인식한다(315). 클라이언트(145) 시스템은 칩 일련번호와 수신된 서버시간을 스캔블하여 암호 데이터 작성을 하고(320), 작성된 암호 데이터를 웹서버(100)로 전송하게 된다(325). 상기 암호 데이터에는 칩 일련번호, 서버시간, 암호문(Cryptogram) 등이 포함 가능하다.

웹서버(100)는 클라이언트(145) 시스템으로부터 전송된 로그인 인증에 필요한 암호 데이터를 수신하고(330), 복호화에 앞서 수신된 서버시간과 현재의 서버시간을 비교하여 오차를 확인한다(335). 만약 서버시간 오차가 1분 이내이면, 웹서버(100)는 복호화 과정을 진행하고, 서버시간 오차가 1분이 이상이면 로그인 거부 메시지를 전송한다(340).

웹서버(100)는 암호화되어 전송된 데이터들을 이용하여 복호화 과정을 수행하는데(345), 그 과정은 상기 데이터들에 포함된 서버시간 및 칩 일련번호를 이용하여 암호문(Cryptogram)을 작성하고, 작성된 암호문을 상기 클라이언트(145) 시스템으로부터 수신한 암호문(Cryptogram)과 비교하여 일치하는지를 확인한다.

복호화를 통한 인증의 실시가 완료되면, 웹서버(100)는 데이터 베이스에 저장하고 있었던 클라이언트(145)의 스마트 카드 칩 일련번호를 조회하여 상기 암호 데이터에 포함되어 있던, 칩 일련번호와 일치여부를 비교하여 인증을 확인한다(350). 상기 인증확인 완료되면 클라이언트의 로그인이 가능하게 된다(355).

또한, 상기 암호화 및 복호화에 쓰이는 암호 알고리즘은 16비트 알고리즘(SEED, 3DES) 등을 사용할 수 있음을 명기하는 바이다.

본 도면에서 기술하고자 하는 암호화 및 복호화 과정은 클라이언트(145)가 소지한 스마트 카드에 장착된 IC칩을 이용하는 데, 이는 칩(Chip)이 나타내는 고유 일련번호는 하드웨어적으로 유일한 고유 번호로써, 위조, 변조, 복제 등이 불가능하여, 클라이언트(145)가 보다 안전하게 로그인 절차를 수행할 수 있도록 돕는다.

도4는 클라이언트(145)가 스마트 카드를 이용하여 로그인 한 후에, 클라이언트(145)가 보유 또는 사용하고 있는 아이템(아바타 또는 게임 등)을 상기 스마트 카드에 저장하는 과정에 대한 간단한 흐름도이다.

본 도면은 클라이언트(145)가 소지한 스마트 카드의 데이터 영역에 게임, 아바타 및 기타 아이템들을 저장, 보관, 휴대할 수 있도록 하는 기능을 추가시킴으로써, 클라이언트(145)의 계정에 대한 해킹의 염려를 방지하도록 하는 것으로써, 서로 다른 계정간에도 자유로운 아이템 업로드가 가능할 수 있다.

또한, 상기 데이터 영역에 사용 가능한 데이터의 형식은 웹사이트 코드, 아이템 번호, 인증필드, 다운 또는 업 로딩 시각 및 아이디 등이 포함 가능하며, 상기 인증필드는 사이트 코드, 아이템 번호, 데이터 다운 또는 업 로딩 시각, 칩 고유 일련번호 등을 포함하여 구성 가능하며, 해당 사이트의 암호화 알고리즘으로 스캔블하여 사후 검증이 가능하도록 할 수 있음을 밝힌다.

클라이언트(145)가 본인의 스마트 카드를 이용하여 웹서버(100)에 접속을 실시하면(400), 상기 도3의 과정을 통해 클라이언트(145)의 로그인 인증을 완료하게 된다. 스마트 카드를 이용한 클라이언트(145)의 로그인이 완료되면(405), 상기 클라이언트(145)는 본 웹사이트 상에서 게임이나 기타 인터넷 작업을 수행하게 되고, 또한, 아바타 등이 관리도 가능하게 된다(410).

클라이언트(145)가 스마트 카드에 저장되어 있던 게임이나 기타 아바타 아이템의 사용을 위해 업로딩을 요청하고(415), 스마트 카드에 저장되어 있던 클라이언트(145) 아이템의 업로딩이 진행되면(420) 웹서버(100)는 업로딩의 내역을 상기 클라이언트(145) 핸드폰이나 이메일 등으로 전송하여 타인에 의한 도용 등을 실시간적으로 방지할 수 있도록 한다(425).

웹사이트 내에서 클라이언트(145)의 해당 작업이 완료되어 클라이언트(145)가 로그 아웃을 요청하면(430), 상기 웹서버(100)는 사용중인 아이템에 대한 스마트 카드로의 다운로드 여부를 확인하고(435), 클라이언트(145)의 요청에 따라, 사용중이거나 선택된 아이템들을 스마트 카드로 다운로드를 실시하게 된다(440).

상기 업로딩과 마찬가지로, 아이템의 다운로드 작업과 동시에 다운로드 내역은 클라이언트(145) 핸드폰으로 전송되어 클라이언트(145)로 하여금 실시간 확인이 가능하도록 한다(445). 상기 과정이 완료되면, 클라이언트(145)의 로그아웃 과정은 완료된다(450).

스마트 카드를 이용한 아이템의 업로딩 또는 다운로드에는 본 발명이 구현되는 웹사이트와 제휴 등의 관계를 가진 타 사이트와도 연동이 가능할 수 있음을 명기한다.

발명의 효과

본 발명에 따르면, 클라이언트가 소유한 스마트 카드를 이용하여 인터넷 상의 웹사이트에 로그인이 가능하도록 하고, 아바타 또는 게임 아이템들을 저장할 수 있도록 하는 방법 및 시스템을 제공함으로써, 스마트 카드 칩의 고유 일련번호를 통해 아이디 및 패스워드의 위조, 변조 및 복제 등이 불가능하도록 하여, 보다 안전한 로그인 절차를 수행할 수 있다는 장점이 있다.

제 3자에게 일정시간 동안의 접근 권한을 제공 및 회수할 수 있고, 중요한 게임 아이템, 포인트, 마일리지, 상품권 및 아바타 아이템 등을 스마트 카드에 기록하여 업로딩 또는 다운로드가 가능하다는 장점이 있다.

(57) 청구의 범위

청구항 1.

클라이언트 단말 접속시, 상기 클라이언트를 인증처리하는 인증수단; 및

상기 인증결과를 근거로 하여, 상기 클라이언트 단말로 게임을 제공하고, 상기 게임 진행에 따라 상기 클라이언트가 보유하게 되는 게임 아이템 정보가 상기 클라이언트 소유 IC카드에 저장되도록 상기 클라이언트 단말로 상기 게임 아이템 정보를 전송하는 게임 아이템 관리수단;을 구비하여 이루어지는 것을 특징으로 하는 게임서버.

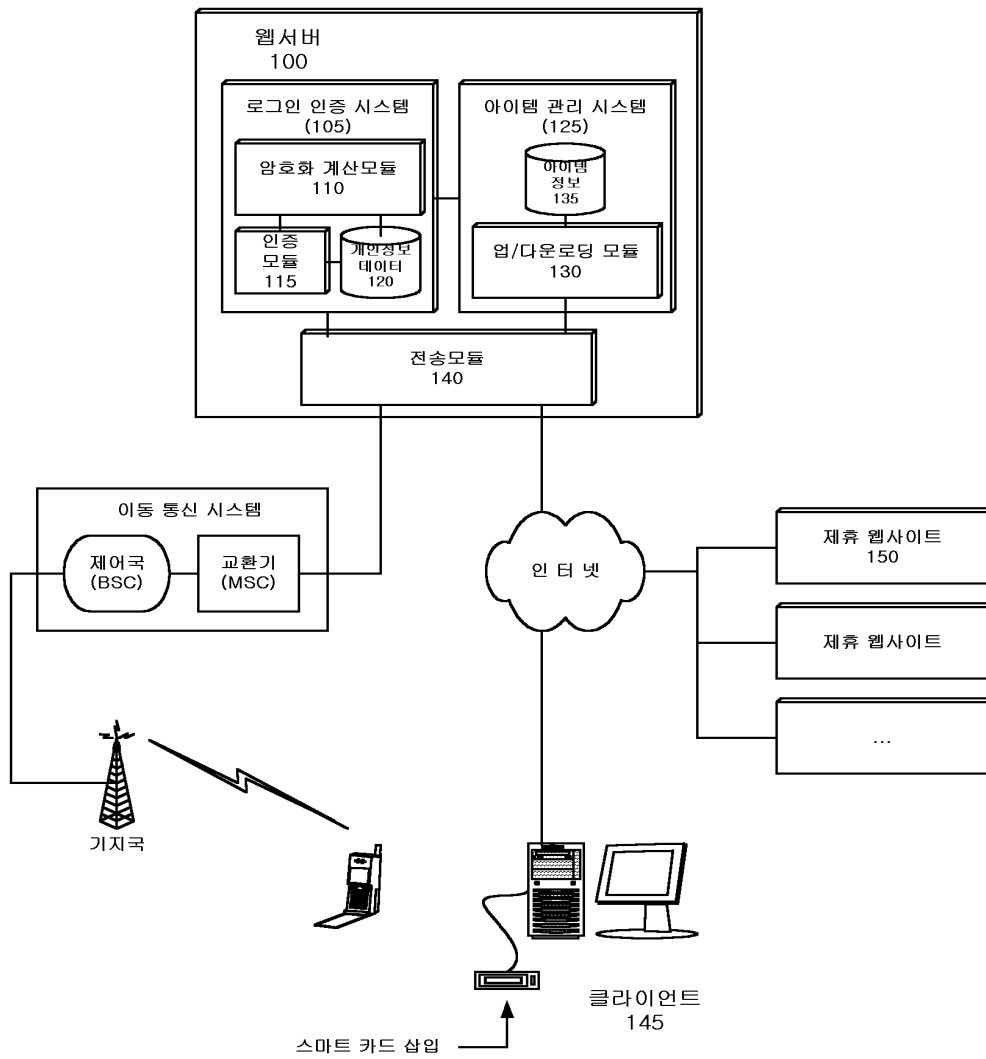
청구항 2.

제 1항에 있어서, 상기 인증수단은,

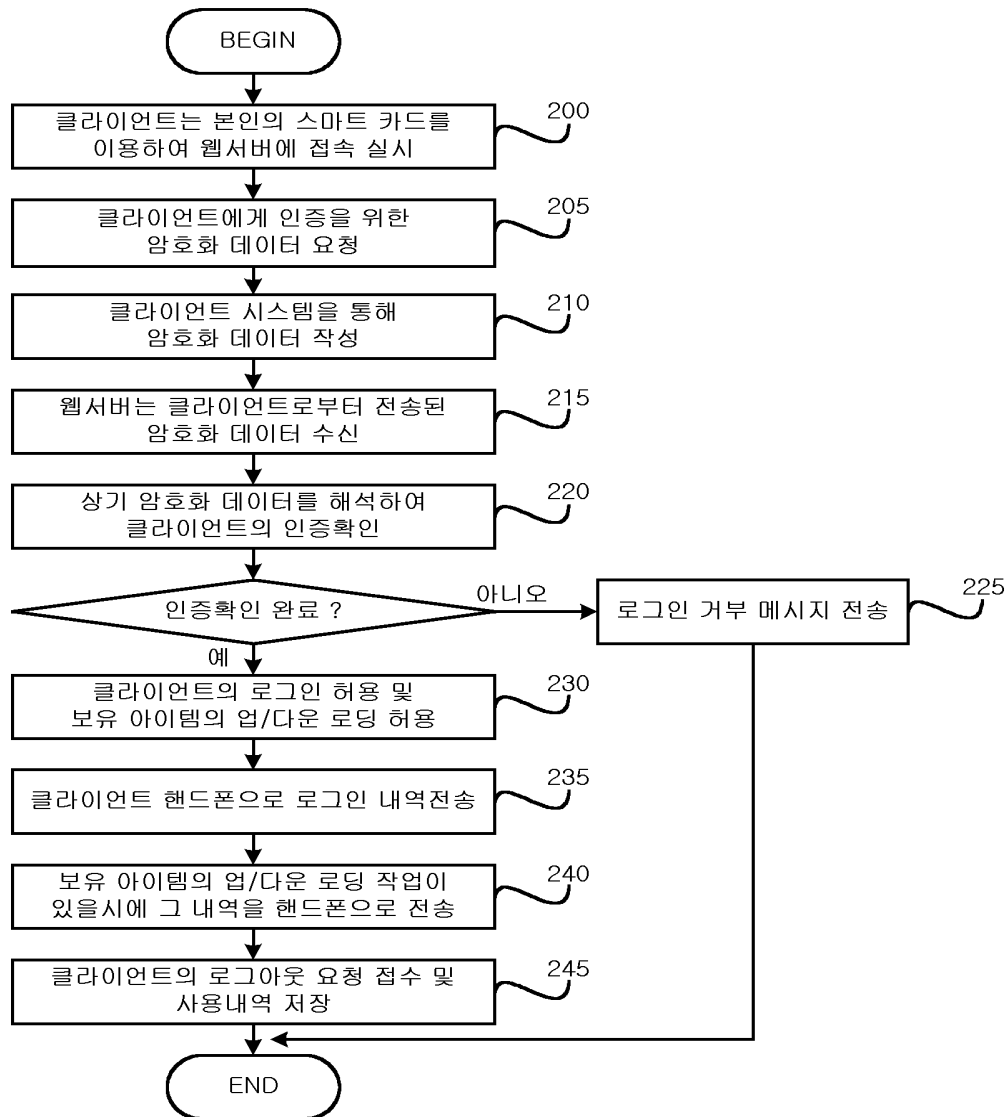
상기 클라이언트 소유 IC카드에 기 저장된 고유코드를 저장하는 저장매체와 연계하여, 상기 클라이언트 단말에서 상기 IC카드에 기 저장된 고유코드를 전송시, 상기 클라이언트 단말에서 전송한 고유코드와 상기 저장매체에 기 저장된 고유코드를 비교하여 상기 클라이언트를 인증처리하는 것을 특징으로 하는 게임서버.

도면

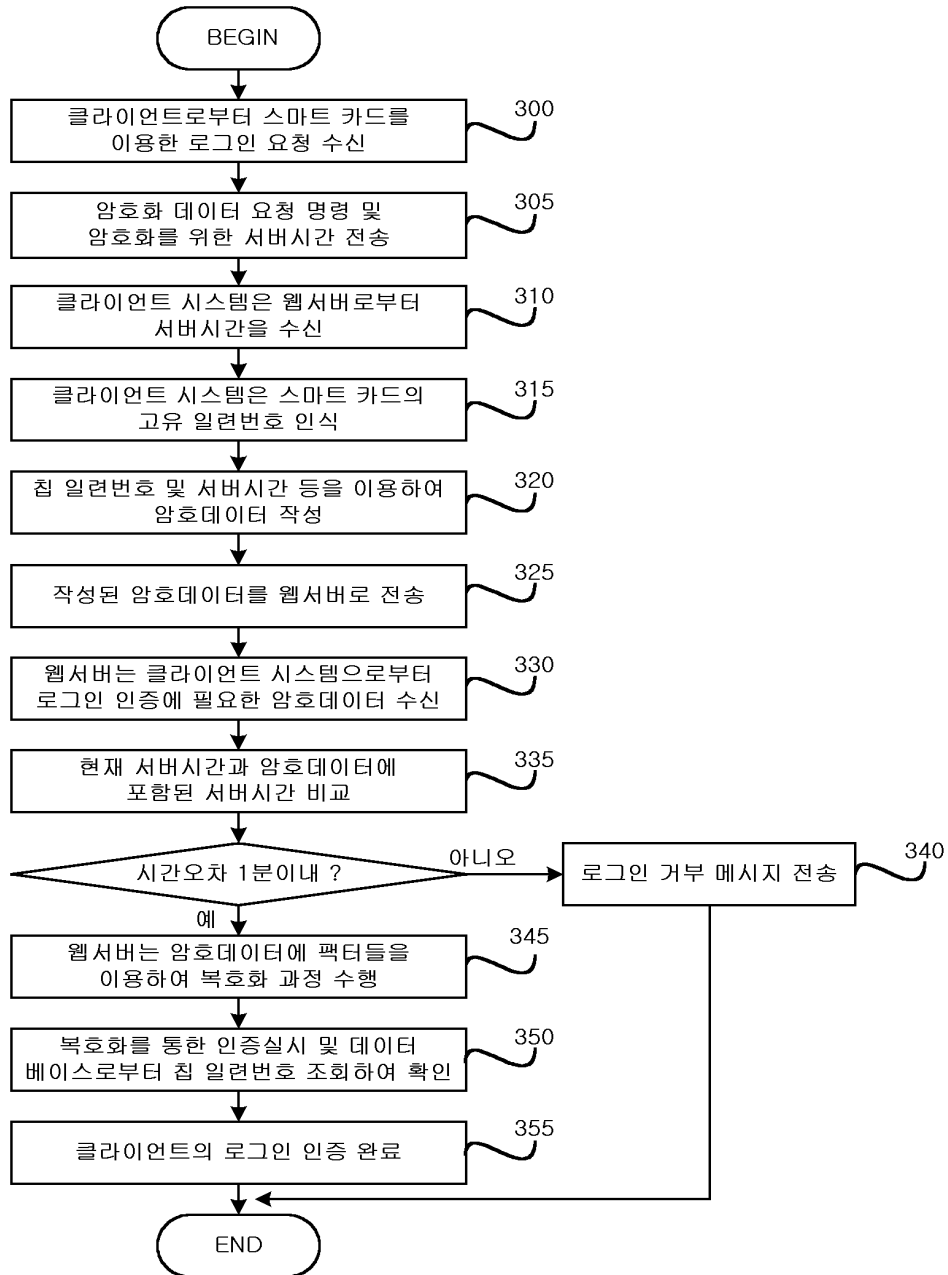
도면1



도면2



도면3



도면4

