



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년01월07일
(11) 등록번호 10-1006720
(24) 등록일자 2010년12월31일

(51) Int. Cl.

G06F 21/00 (2006.01) G06F 15/00 (2006.01)

(21) 출원번호 10-2008-0065132
(22) 출원일자 2008년07월04일
심사청구일자 2008년07월04일
(65) 공개번호 10-2010-0004782
(43) 공개일자 2010년01월13일
(56) 선행기술조사문헌
KR100549647 B1*
KR1020010075411 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
킹스정보통신(주)
서울특별시 송파구 송파동 29번지 부영빌딩

(72) 발명자
김진영
전라남도 강진군 작천면 이남리 628번지
허록은
서울특별시 동대문구 휘경1동 78번지 롯데아파트
102동 402호

(74) 대리인
정태훈, 오용수

전체 청구항 수 : 총 8 항

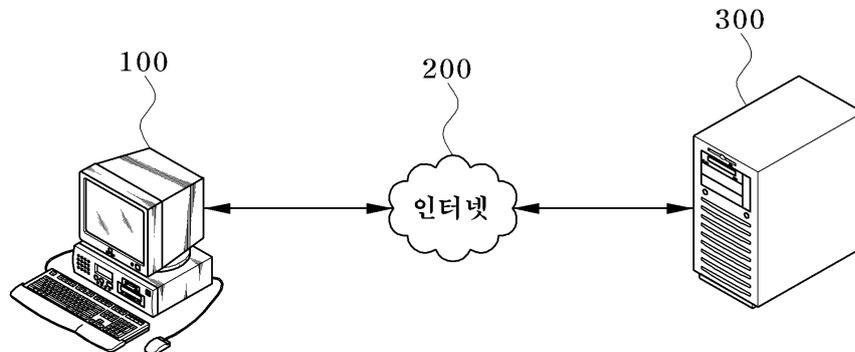
심사관 : 권영학

(54) 웹 페이지에서의 비밀번호 보안방법 및 이를 실행하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체

(57) 요약

본 발명은 웹 페이지에서의 비밀번호 보안방법에 관한 것으로, 사용자 단말의 웹 브라우저를 통해 특정 웹 서버에서 제공되는 웹 페이지에 접속한 후, 해당 사용자 단말의 키보드를 통해 상기 웹 페이지에서 제공되는 비밀번호 입력창에 입력되는 비밀번호 키 값을 보안하기 위한 방법으로서, 상기 비밀번호 입력창에 입력되는 비밀번호 키 값을 암호화한 후, 상기 웹 페이지에서 로그인을 수행하기 위한 이벤트의 발생과 동시에 상기 암호화 된 비밀번호 키 값을 복호화함으로써, 웹 페이지의 비밀번호 입력창에 입력된 비밀번호 키 값을 해당 웹 서버로 전송하기 전까지 악성 프로그램에 의해 외부로 유출되는 사고를 미연에 방지할 수 있는 효과가 있다.

대표도 - 도1



비밀번호 보안모듈(150) 구비

특허청구의 범위

청구항 1

- (a) 사용자 단말의 웹 브라우저를 통해 접속된 현재 웹 페이지에 비밀번호 입력창이 존재하는지를 판단하는 단계;
- (b) 상기 단계(a)에서의 판단 결과, 현재 웹 페이지에 비밀번호 입력창이 존재할 경우, 현재 웹 페이지의 보안 설정 여부를 검사하는 단계;
- (c) 상기 단계(b)에서의 검사 결과, 현재 웹 페이지에 보안이 설정되었을 경우, 해당 사용자 단말의 키보드를 통해 상기 비밀번호 입력창에 입력되는 비밀번호 키 값을 암호화하는 단계; 및
- (d) 현재 웹 페이지에서 로그인을 수행하기 위한 이벤트가 발생할 경우, 상기 암호화 된 비밀번호 키 값을 복호화하는 단계를 포함하는 웹 페이지에서의 비밀번호 보안방법.

청구항 2

제1 항에 있어서,

상기 단계(b)에서의 검사 결과, 현재 웹 페이지에 보안이 설정되어 있지 않으면, 현재 웹 페이지에서 로그인을 수행하기 위한 이벤트의 발생 시 보안설정을 위한 윈도우를 해당 사용자 단말의 화면에 디스플레이하는 단계를 더 포함하는 것을 특징으로 하는 웹 페이지에서의 비밀번호 보안방법.

청구항 3

제1 항에 있어서,

상기 단계(c)에서, 상기 비밀번호 입력창에 입력되는 비밀번호 키 값을 암호화한 후, 상기 암호화 된 비밀번호 키 값을 상기 비밀번호 입력창에 디스플레이하는 단계를 더 포함하는 것을 특징으로 하는 웹 페이지에서의 비밀번호 보안방법.

청구항 4

제1 항에 있어서,

상기 단계(d)에서, 상기 암호화된 비밀번호 키 값을 복호화한 후, 상기 복호화 된 비밀번호 키 값을 상기 비밀번호 입력창에 저장하는 단계를 더 포함하는 것을 특징으로 하는 웹 페이지에서의 비밀번호 보안방법.

청구항 5

사용자 단말의 웹 브라우저를 통해 특정 웹 서버에서 제공되는 웹 페이지에 접속한 후, 해당 사용자 단말의 키보드를 통해 상기 웹 페이지에서 제공되는 비밀번호 입력창에 입력되는 비밀번호 키 값을 보안하기 위한 방법으로서,

상기 비밀번호 입력창에 입력되는 비밀번호 키 값을 암호화한 후, 상기 웹 페이지에서 로그인을 수행하기 위한 이벤트의 발생과 동시에 상기 암호화 된 비밀번호 키 값을 복호화하는 것을 특징으로 하는 웹 페이지에서의 비밀번호 보안방법.

청구항 6

제5 항에 있어서,

상기 비밀번호 입력창에 입력되는 비밀번호 키 값을 암호화한 후, 상기 암호화 된 비밀번호 키 값을 상기 비밀번호 입력창에 디스플레이하는 것을 특징으로 하는 웹 페이지에서의 비밀번호 보안방법.

청구항 7

제5 항에 있어서,

상기 암호화된 비밀번호 키 값을 복호화한 후, 상기 복호화 된 비밀번호 키 값을 상기 비밀번호 입력창에 저장하는 것을 특징으로 하는 웹 페이지에서의 비밀번호 보안방법.

청구항 8

제1 항 내지 제7 항 중 어느 한 항의 방법을 컴퓨터로 실행시킬 수 있는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명세서

발명의 상세한 설명

기술분야

[0001] 본 발명은 웹 페이지에서의 비밀번호 보안방법에 관한 것으로, 보다 상세하게는 특정 웹 서버에서 제공하는 웹 페이지의 비밀번호 입력창에 입력된 비밀번호 키 값을 해당 웹 서버로 전송하기 전까지 악성 프로그램에 의해 외부로 유출되는 사고를 미연에 효과적으로 방지할 수 있도록 한 웹 페이지에서의 비밀번호 보안방법 및 이를 실행하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

배경기술

[0002] 최근, 개인이나 기업 및 공공기관에서는 인터넷 상에서 인터넷 뱅킹 등의 금융거래, 전자상거래, 이메일(E-mail) 전송, 채팅 및 게임 등을 사용하는 경우가 더욱 증대되고 있는 실정이다.

[0003] 이중에서도, 인터넷 뱅킹 등의 금융거래나 전자상거래에 있어서는 해당 사용자의 정당한 거래인지를 확인하기 위하여 인터넷 사용자의 아이디(ID), 비밀번호(Password), 인증서 및 이체 비밀번호, 신용카드번호 및 주민등록번호 등을 입력하도록 되어 있다.

[0004] 그러나, 이러한 사용자 정보들은 개방형 네트워크인 인터넷을 통해 전송되기 때문에 해커들의 해킹에 의해 신종 범죄의 대상이 되고 있다.

[0005] 따라서, 이러한 해커들의 해킹을 방지하기 위하여 네트워크 상에서 전송되는 데이터에 대한 보안방법으로서 각종 보안 프로그램(예컨대, 안티 스파이웨어 또는 안티 바이러스, 방화벽 등)을 사용자 컴퓨터에 설치하는 방법이 제안되어 사용되고 있다.

[0006] 그러나, 각종 보안 프로그램을 사용자 컴퓨터에 설치하는 방법을 사용하더라도, 사용자가 키보드를 이용하여 키 값을 입력할 때마다 각각의 키 값에 해당하는 고유 코드가 키보드 드라이버를 통해 사용자 컴퓨터에 입력되기 때문에, 해커들에 의해 키보드 드라이버가 해킹을 당하면 키보드를 통해 입력되는 사용자의 신용카드번호 및 주민등록번호 등의 사용자 개인정보 및 사용자가 가입한 해당 웹 사이트의 비밀번호 등이 해커들에게 해킹되는 문제점이 있다.

[0007] 또한, 사용자 컴퓨터의 키보드를 통해 웹 페이지의 비밀번호 입력창에 입력되는 비밀번호 키 값은 윈도우로 전달되는 과정에서 후킹(hooking)이나 서브클래싱(subclassing)을 이용하여 읽을 수 있다. 이를 통해 악성 프로그램은 사용자의 아이디(ID)와 비밀번호와 같은 정보를 가로챈다.

[0008] 이를 방지하기 위하여 종래에는 키보드 보안 프로그램을 사용자 단말에 설치하여, 키보드 보안이 동작하면 키 값이 암호화되어, 마지막 윈도우에 전달되기 직전에 복호화 된다.

[0009] 이때, 윈도우로 전달되는 과정에서는 입력된 키 값을 알 수 없지만, 키보드를 통해 입력이 완료된 값은 윈도우 핸들로 접근하여 읽을 수 있으며, 비밀번호의 경우에도 웹 페이지의 비밀번호 입력창에 "*****"표시되어 사용자의 눈에는 보이지 않지만 실제 비밀번호 키 값을 읽어 올 수 있다.

[0010] 상기와 같이 종래 기술의 키보드 보안 프로그램을 이용한 키보드 보안방법은 키보드로부터 입력되는 비밀번호 키 값이 전달되는 과정에서는 그 비밀번호 키 값을 보호할 수 있지만, 이미 쓰고 난 후의 비밀번호 키 값은 보호할 수 없는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

[0011] 본 발명은 전술한 문제점을 해결하기 위하여 안출된 것으로서, 본 발명의 목적은 특정 웹 서버에서 제공하는 웹 페이지의 비밀번호 입력창에 입력된 비밀번호 키 값을 해당 웹 서버로 전송하기 전까지 악성 프로그램에 의해 외부로 유출되는 사고를 미연에 효과적으로 방지할 수 있도록 한 웹 페이지에서의 비밀번호 보안방법 및 이를 실행하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는데 있다.

과제 해결수단

[0012] 전술한 목적을 달성하기 위하여 본 발명의 제1 측면은, (a) 사용자 단말의 웹 브라우저를 통해 접속된 현재 웹 페이지에 비밀번호 입력창이 존재하는지를 판단하는 단계; (b) 상기 단계(a)에서의 판단 결과, 현재 웹 페이지에 비밀번호 입력창이 존재할 경우, 현재 웹 페이지의 보안설정 여부를 검사하는 단계; (c) 상기 단계(b)에서의 검사 결과, 현재 웹 페이지에 보안이 설정되었을 경우, 해당 사용자 단말의 키보드를 통해 상기 비밀번호 입력창에 입력되는 비밀번호 키 값을 암호화하는 단계; 및 (d) 현재 웹 페이지에서 로그인을 수행하기 위한 이벤트가 발생할 경우, 상기 암호화 된 비밀번호 키 값을 복호화하는 단계를 포함하는 웹 페이지에서의 비밀번호 보안 방법을 제공하는 것이다.

[0013] 바람직하게는, 상기 단계(b)에서의 검사 결과, 현재 웹 페이지에 보안이 설정되어 있지 않으면, 현재 웹 페이지에서 로그인을 수행하기 위한 이벤트의 발생 시 보안설정을 위한 윈도우를 해당 사용자 단말의 화면에 디스플레이하는 단계를 더 포함할 수 있다.

[0014] 바람직하게는, 상기 단계(c)에서, 상기 비밀번호 입력창에 입력되는 비밀번호 키 값을 암호화한 후, 상기 암호화 된 비밀번호 키 값을 상기 비밀번호 입력창에 디스플레이하는 단계를 더 포함할 수 있다.

[0015] 바람직하게는, 상기 단계(d)에서, 상기 암호화 된 비밀번호 키 값을 복호화한 후, 상기 복호화 된 비밀번호 키 값을 상기 비밀번호 입력창에 저장하는 단계를 더 포함할 수 있다.

[0016] 본 발명의 제2 측면은, 사용자 단말의 웹 브라우저를 통해 특정 웹 서버에서 제공되는 웹 페이지에 접속한 후, 해당 사용자 단말의 키보드를 통해 상기 웹 페이지에서 제공되는 비밀번호 입력창에 입력되는 비밀번호 키 값을 보안하기 위한 방법으로서, 상기 비밀번호 입력창에 입력되는 비밀번호 키 값을 암호화한 후, 상기 웹 페이지에서 로그인을 수행하기 위한 이벤트의 발생과 동시에 상기 암호화 된 비밀번호 키 값을 복호화하는 것을 특징으로 하는 웹 페이지에서의 비밀번호 보안방법을 제공하는 것이다.

[0017] 바람직하게는, 상기 비밀번호 입력창에 입력되는 비밀번호 키 값을 암호화한 후, 상기 암호화 된 비밀번호 키 값을 상기 비밀번호 입력창에 디스플레이할 수 있다.

[0018] 바람직하게는, 상기 암호화 된 비밀번호 키 값을 복호화한 후, 상기 복호화 된 비밀번호 키 값을 상기 비밀번호 입력창에 저장할 수 있다.

[0019] 본 발명의 제3 측면은, 상술한 웹 페이지에서의 비밀번호 보안방법을 실행시키기 위한 프로그램을 기록한 기록매체를 제공한다.

효 과

[0020] 이상에서 설명한 바와 같은 본 발명의 웹 페이지에서의 비밀번호 보안방법 및 이를 실행하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 따르면, 특정의 웹 서버에서 제공하는 웹 페이지의 비밀번호 입력창에 입력된 비밀번호 키 값을 해당 웹 서버로 전송하기 전까지 악성 프로그램에 의해 외부로 유출되는 사고를 미연에 효과적으로 방지할 수 있는 이점이 있다.

발명의 실시를 위한 구체적인 내용

[0021] 이하, 첨부 도면을 참조하여 본 발명의 실시예를 상세하게 설명한다. 그러나, 다음에 예시하는 본 발명의 실시예는 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 다음에 상술하는 실시예에 한정되는 것은 아니다. 본 발명의 실시예는 당업계에서 통상의 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위하여 제공되어지는 것이다.

[0022] 도 1은 본 발명의 일 실시예에 따른 웹 페이지에서의 비밀번호 보안방법을 구현하기 위한 시스템을 나타낸 개략적인 블록 구성도이다.

[0023] 도 1을 참조하면, 본 발명의 일 실시예에 따른 웹 페이지에서의 비밀번호 보안방법을 구현하기 위한 시스템은, 인터넷(200)을 통해 서로 접속된 사용자 단말(100) 및 특정의 웹 서버(Web Server)(300)를 포함한다.

[0024] 여기서, 사용자 단말(100)은 웹 서버(300)에서 제공되는 다양한 HTML(Hyper Text Markup Language) 문서 등의 웹 페이지(Web Page)를 가져와 화면에 디스플레이될 수 있도록 통상의 웹 브라우저(Web Browser)가 구비되어 있다.

[0025] 또한, 사용자 단말(100)은 웹 서버(300)에서 제공되는 웹 페이지에서의 비밀번호 보안을 위한 비밀번호 보안모듈(150)이 탑재되어 있다.

[0026] 특히, 비밀번호 보안모듈(150)은 웹 페이지의 비밀번호 입력창에 입력된 비밀번호 키 값을 해당 웹 서버(300)로 전송하기 전까지 악성 프로그램에 의해 외부로 유출되는 것을 효과적으로 방지하는 기능을 수행한다.

[0027] 이러한 비밀번호 보안모듈(150)은 소프트웨어로 구현됨이 바람직하지만, 이에 국한하지 않으며, 하드웨어 형태로 구현할 수도 있다.

[0028] 한편, 상기와 같은 사용자 단말(100)은 예컨대, 데스크탑 PC, 노트북 PC 등 컴퓨터인 것이 일반적이지만, 이에 한정되는 것은 아니며 인터넷(200)을 통하여 특정의 웹 서버(300)에 접속하여 다양한 웹 서비스를 이용할 수 있는 모든 종류의 유무선 통신 장치일 수 있다.

[0029] 예를 들어, 사용자 단말(100)은 무선 인터넷 또는 휴대 인터넷을 통하여 통신하는 셀룰러폰(Cellular phone), 피씨에스폰(PCS phone: Personal Communications Services phone), 동기식/비동기식 IMT-2000(International Mobile Telecommunication-2000) 등 이동 단말을 포함하고, 이외에도 팜 PC(Palm Personal Computer), 개인용 디지털 보조기(PDA: Personal Digital Assistant), 스마트폰(Smart phone), 왓폰(WAP phone: Wireless application protocol phone), 모바일 게임기(mobile play-station) 등 웹 서버(300)에 접속하기 위한 사용자 인터페이스를 갖는 모든 유무선 가전/통신 장치를 포괄적으로 의미할 수 있다.

[0030] 인터넷(200)은 TCP/IP 프로토콜 및 그 상위계층에 존재하는 여러 서비스, 즉 HTTP(Hyper Text Transfer Protocol), Telnet, FTP(File Transfer Protocol), DNS(Domain Name System), SMTP(Simple Mail Transfer Protocol), SNMP(Simple Network Management Protocol), NFS(Network File Service), NIS(Network Information Service) 등을 제공하는 전 세계적인 개방형 컴퓨터 네트워크 구조를 의미하며, 사용자 단말(100)의 임의의 사용자가 웹 서버(300)에 접속될 수 있게 하는 환경을 제공한다.

[0031] 한편, 인터넷(200)은 유선 또는 무선 인터넷일 수도 있고, 이외에도 유선 공중망, 무선 이동 통신망, 또는 휴대 인터넷 등과 통합된 코어망 일 수도 있다.

[0032] 그리고, 웹 서버(300)는 통상적으로 웹 브라우저(Web Browser)를 구비한 사용자 단말(100)로부터 HTTP(Hyper Text Transfer Protocol) 요청을 받아들이고, HTML(Hyper Text Markup Language) 문서와 같은 웹 페이지에서

흔히 찾아볼 수 있는 자료 콘텐츠에 따라 HTTP에 반응하는 기능을 수행한다.

- [0033] 한편, 사용자 단말(100)의 웹 브라우저와 웹 서버(300)간의 전송경로를 살펴보면, 사용자 단말(100)의 웹 브라우저는 HTTP(HyperText Transfer Protocol)프로토콜을 사용하여 웹 서버(300)에게 URL(Uniform Resource Locator)에 지정되어 있는 장소의 HTML 문서를 요구(request)하며, 웹 서버(300)는 요구받은 HTML 문서를 찾아 사용자 단말(100)의 웹 브라우저에게 제공한다.
- [0034] 그리고, 상기 웹 브라우저는 제공받은 HTML 문서를 그 형식에 맞게 사용자 단말(100)의 화면을 통해 해당 사용자에게 보여준다.
- [0035] 이하에는 본 발명의 일 실시예에 따른 웹 페이지에서의 비밀번호 보안방법을 상세하게 설명하기로 한다.
- [0036] 도 2는 본 발명의 일 실시예에 따른 웹 페이지에서의 비밀번호 보안방법을 설명하기 위한 전체적인 흐름도로서, 별다른 설명이 없는 한 비밀번호 보안모듈(150)이 주체가 되어 수행함을 밝혀둔다.
- [0037] 도 1 및 도 2를 참조하면, 본 발명의 일 실시예에 따른 웹 페이지에서의 비밀번호 보안방법은, 먼저, 사용자 단말(100)은 통상의 웹 브라우저를 통해 특정의 웹 서버(300)에 접속하여 특정의 웹 사이트를 열어 임의의 웹 페이지를 제공받으면, 사용자 단말(100)에 탑재된 비밀번호 보안모듈(150)은 현재 접속된 웹 페이지에 비밀번호 입력창이 존재하는지를 판단한다(S100).
- [0038] 만약, 상기 단계S100에서의 판단 결과, 현재 웹 페이지에 비밀번호 입력창이 존재할 경우, 현재 웹 페이지에 본 발명에 따른 비밀번호 보안이 설정되어 있는지를 검사한다(S110).
- [0039] 상기 단계S110에서의 검사 결과, 현재 웹 페이지에 비밀번호 보안이 설정되어 있을 경우, 해당 사용자 단말(100)의 키보드를 통해 현재 웹 페이지에 존재하는 비밀번호 입력창에 특정의 비밀번호 키 값이 입력되는지 확인하여, 상기 비밀번호 입력창에 특정의 비밀번호 키 값이 입력되면, 상기 비밀번호 입력창에 입력되는 특정의 비밀번호 키 값을 암호화 한다(S120).
- [0040] 그런 다음, 현재 웹 페이지에서 로그인(Login)을 수행하기 위한 이벤트(Event) 예컨대, 클릭(Click) 또는 키다운(KeyDown) 이벤트 등이 발생할 경우, 상기 단계S120에서 암호화 된 비밀번호 키 값을 복호화한다(S130). 상기 단계S130에서 복호화 된 비밀번호 키 값은 사용자 단말(100)의 웹 브라우저를 통해 현재 웹 페이지를 제공한 웹 서버(300)로 전송한다.
- [0041] 즉, 상기 비밀번호 입력창에 입력되는 특정의 비밀번호 키 값이 해당 웹 서버(300)로 전송되기 전까지 암호화 되어 있으며, 웹 서버(300)로 전송되기 직전에 상기 암호화 된 비밀번호 키 값을 복호화 함으로써, 악성 프로그램으로부터 비밀번호 타입의 정보를 안전하게 보호할 수 있다.
- [0042] 한편, 상기 단계S110에서의 검사 결과, 현재 웹 페이지에 본 발명에 따른 비밀번호 보안이 설정되어 있지 않으면, 현재 웹 페이지가 복호화가 가능한지 검사한다(S140).
- [0043] 상기의 단계S140은, 사용자가 키보드를 통해 현재 웹 페이지의 비밀번호 입력창에 특정의 비밀번호 키 값을 입력한 후, 전송 버튼(즉, 로그인 버튼)을 눌렀을 때 수행함이 바람직하다.
- [0044] 이 후에, 상기 단계S140에서, 현재 웹 페이지에서 로그인을 수행하기 위한 이벤트가 발생할 경우, 본 발명에 따른 비밀번호 보안설정을 위한 보호설정 윈도우를 해당 사용자 단말(100)의 화면에 예컨대, 팝업 형태로 디스플레이 하거나 현재 열려진 웹 브라우저 상에 디스플레이 한다(S150).
- [0045] 그리고, 상기 단계S150에서 사용자에게 의해 보호 설정된 웹 페이지는 다음에 방문했을 때부터 실제로 본 발명에 따른 비밀번호 보안을 수행하게 된다. 즉, 상기 보호 설정된 웹 페이지의 비밀번호 입력창에 입력되는 비밀번호 키 값은 암호화 된 값이 입력되며, 이렇게 암호화 된 비밀번호 키 값은 해당 웹 서버(300)로 전송하기 전에 복호화 되어 해당 웹 서버(300)로 전달된다.
- [0046] 추가적으로, 상기 단계S120에서, 상기 비밀번호 입력창에 입력되는 비밀번호 키 값을 암호화한 후, 상기 암호화 된 비밀번호 키 값을 상기 비밀번호 입력창에 디스플레이하는 단계를 더 포함함이 바람직하다.
- [0047] 한편, 상기 단계S120에서, 동 출원인에 의해 기 출원된 특허출원 제2006-0100366호(유에스비 키보드 보안장치 및 그 방법)를 비롯한 통상의 키보드 보안과의 연동을 통해 상기 비밀번호 입력창에 입력되는 비밀번호 키 값을 보다 안전하게 전달받아 암호화할 수도 있다.

[0048] 또한, 상기 단계S130에서, 상기 암호화 된 비밀번호 키 값을 복호화한 후, 상기 복호화 된 비밀번호 키 값을 상기 비밀번호 입력창에 저장하는 단계를 더 포함함이 바람직하다.

[0049] 한편, 본 발명의 일 실시예에 따른 웹 페이지에서의 비밀번호 보안방법은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현되는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다.

[0050] 예컨대, 컴퓨터가 읽을 수 있는 기록매체로는 롬(ROM), 램(RAM), 시디-롬(CD-ROM), 자기 테이프, 하드디스크, 플로피디스크, 이동식 저장장치, 비휘발성 메모리(Flash Memory), 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)의 형태로 구현되는 것도 포함된다.

[0051] 또한, 컴퓨터로 읽을 수 있는 기록매체는 컴퓨터 통신망으로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 읽을 수 있는 코드로서 저장되고 실행될 수 있다.

[0052] 전술한 본 발명에 따른 웹 페이지에서의 비밀번호 보안방법 및 이를 실행하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 대한 바람직한 실시예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 특허청구범위와 발명의 상세한 설명 및 첨부한 도면의 범위 안에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 본 발명에 속한다.

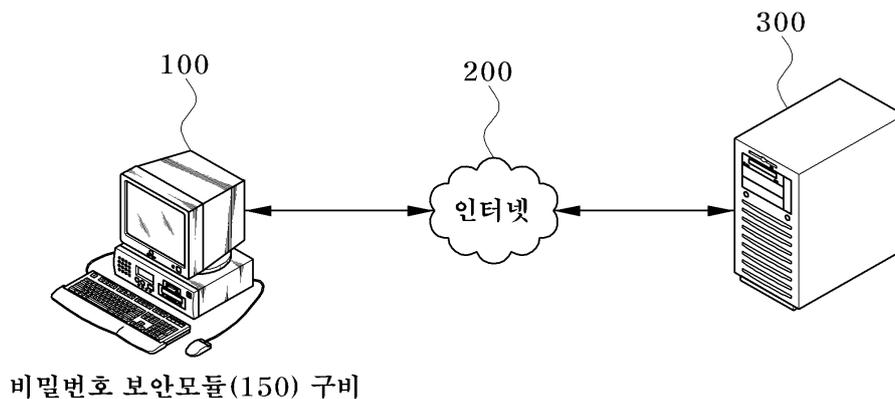
도면의 간단한 설명

[0053] 도 1은 본 발명의 일 실시예에 따른 웹 페이지에서의 비밀번호 보안방법을 구현하기 위한 시스템을 나타낸 개략적인 블록 구성도이다.

[0054] 도 2는 본 발명의 일 실시예에 따른 웹 페이지에서의 비밀번호 보안방법을 설명하기 위한 전체적인 흐름도이다.

도면

도면1



도면2

