(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2017 년 8 월 24 일 (24.08.2017)

WIPO | PCT

(10) 국제공개번호
WO 2017/142271 A1

(51) 국제특허분류:
G06F 21/46 (2013.01) *H04L 9/32* (2006.01)
G06F 21/31 (2013.01) *G06Q 20/40* (2012.01)

(21) 국제출원번호: PCT/KR2017/001547

(22) 국제출원일: 2017 년 2 월 13 일 (13.02.2017)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2016-0017561 2016 년 2 월 16 일 (16.02.2016) KR
10-2016-0150877 2016 년 11 월 14 일 (14.11.2016) KR

(71) 출원인: **주식회사 프로젝트사공구 (PROJECT 409)** [KR/KR]; 06525 서울시 서초구 나루터로 73,4 층, Seoul (KR).

(72) 발명자: **이명호 (LEE, Myong Ho)**; 14774 경기도 부천시 소사로 78 번길 81, 101 동 1002 호, Gyeonggi-do (KR).

(74) 대리인: **특허법인 동천 (DONGCHEON PATENT FIRM)**; 06178 서울시 강남구 테헤란로 84 길 16, 5 층 (대치동, 세풍빌딩), Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

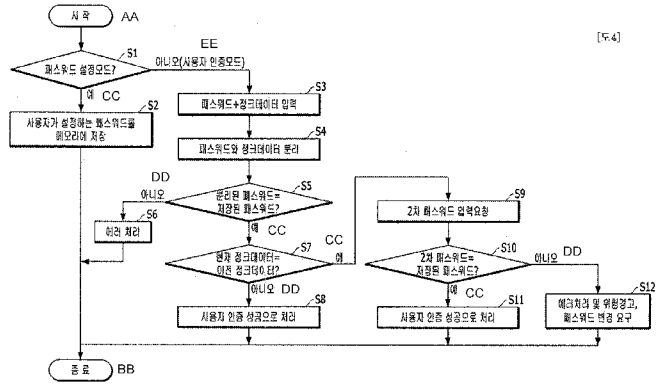
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

(54) **Title**: USER AUTHENTICATION METHOD AND AUTHENTICATION SYSTEM USING MATCH WITH JUNK DATA

(54) **발명의 명칭** : 정크 데이터 일치여부를 이용한 사용자 인증 방법 및 인증 시스템



[도 4]

S1 ... Is it password setting mode?
S2 ... Store password set by user in memory
S3 ... Input password + junk data
S4 ... Separate password and junk data
S5 ... Is separated password same as stored password?
S6 ... Process as error
S7 ... Is current junk data same as previous junk data?
S8, S11 ... Process as success of user authentication
S9 ... Request input of second password
S10 ... Is second password same as stored password?
S12 ... Process as error and warn of risk, and request change of password

AA ... Start
BB ... End
CC ... Yes
DD ... No
EE ... No (user authentication mode)

(57) **Abstract**: The present invention relates to a technique of authenticating a user by using junk data randomly generated when a password is inputted. According to the present invention, a password is received from a user and is stored, and it is determined whether a password matches with an original password stored in a memory among junk data and a password inputted together in a user authentication step. At this time, if a password including the junk data matches, by at least a certain length or more, a password including junk data inputted in a previous authentication step, user authentication fails even if the separately extracted passwords match each other, such that security can be further enhanced.

(57) **요약서**: 본 발명은 패스워드 입력 시 무작위로 발생시킨 정크 데이터(Junk Data)를 이용하여 사용자를 인증하는 기술에 관한 것이다. 이러한 본 발명에 의할 때, 패스워드를 사용자로부터 입력받아 저장해두고, 사용자 인증 단계에서 함께 입력된 정크 데이터 및 패스워드 중에서 메모리에 저장된 원래의 패스워드와 일치하는 패스워드가 존재하는지 판정한다. 이때, 정크 데이터가 포함된 패스워드가 이전의 인증과정에서 입력된 정크 데이터가 포함된 패스워드와 적어도 일정 길이 이상 일치하는 경우 분리 추출된 패스워드가 일치함에도 불구하고 사용자 인증을 실패로 처리함으로써 보안성을 한층 강화할 수 있다.

WO 2017/142271 A1

명세서

발명의 명칭: 정크 데이터 일치여부를 이용한 사용자 인증 방법 및 인증 시스템

기술분야

[1] 본 발명은 정크 데이터(Junk Data)를 이용하여 해킹 예방 및 노출을 방지하는 패스워드 인증 기술에 관한 것이다.

배경기술

[2] 오프라인 및 온라인상의 각종 보안 분야에서 사용자의 인증을 위해 가장 널리 사용되는 것이 패스워드이다. 패스워드란 사용자만이 알고 있는 문자들의 집합으로, 이를 이용해 인증하는 시스템이 패스워드 시스템이다.

[3] 일반적으로, 사용자 인증기술이란 접근이 허가된 적법한 사용자인지를 판단하기 위해 사용되는 기술을 의미한다.

[4] 사용자 인증기술이 적용되는 패스워드 시스템은, 현재 일반적으로 가장 많이 사용되고 있는 현관 도어락, 금고 도어락, 차량 도어락 같은 하드웨어 제품에서부터 노트북 컴퓨터, 개인용 컴퓨터(PC), 태블릿(tablet) PC 및 스마트폰을 포함하는 각종 사용자 단말기의 동작 개시 시의 잠금해제에도 빈번하게 사용되며, 네트워크상의 각 사이트에서 구축한 사용자 인증시스템을 통하여 개인 인증을 하기 위해 자주 사용되고 있다. 이처럼 각종 웹사이트 상의 인증 및 전자상거래, 온라인상의 각종 금융결제, 금융서비스는 물론 현금자동입출금기(ATM: Automated Teller Machine), 민원증명서발급기 등의 자동화기기, 개인 인증을 필요로 하는 금융기관 및 공공기관 등에서 문자를 이용한 패스워드 시스템이 널리 사용되고 있다.

[5] 특히, 정보통신의 발달과 스마트폰의 급속한 보급으로 스마트폰을 통한 전자상거래, 금융거래가 보편화·현실화되면서 개인용 단말기 안에 보관되어 있는 정보의 중요성이 커지게 되었다.

[6] 또한 개인의 건강정보, 활동정보 등을 실시간 측정, 저장, 활용하는 스마트워치, 스마트밴드 등의 웨어러블 기기 및 스마트 홈, 커넥티드 카(Connected car) 기술을 현실화시킨 IoT(Internet of Things)의 등장으로 인한 기기간의 연결은 이를 제어·조정·통제하는 디바이스 역할을 하는 휴대용 개인단말기의 락 해제 및 사용자 인증의 중요성이 커질 수밖에 없고, 이에 따라 패스워드를 이용한 사용자 인증과 이에 따른 안전성 확보 및 보안 강화가 더욱 중요해지고 있다.

[7] 종래 기술에 의한 사용자 인증기술 중에서 가장 널리 사용되는 대표적인 것이 패스워드(암호 숫자 키) 입력방식의 사용자 인증기술이다. 이 패스워드 입력방식의 사용자 인증기술은 암호가 갖추어야 하는 간편성과 일정 수준의 보안성을 함께 갖추었기 때문인데, 간편성이 강조됨(예: 4자리 숫자)으로 인하여 보안성이 취약해지는 결과를 갖게 되었다. 이와 같은 이유로 보다 많은 자릿수의

패스워드(예: 8자리 이상)와 영문 대소문자, 특수문자 사용, 주기적인 패스워드 교체 등을 사용자에게 요구하게 되었다. 이로 인해 보안성은 강화되었지만 동시에 사용의 불편함을 초래하게 되어, 패스워드 분실 및 망각, 입력오류, 입력시간 지연 등 편의성이 떨어지는 역효과를 갖게 되어 사용자의 외면을 받고 있어 오히려 보안상의 문제점을 키우고 있는 실정이다.

[8] 예를 들면, 온라인상에서의 금융 서비스나 상품대금 결제 시, 패스워드 보안에 관련된 패스워드 적정 유효기간(패스워드 수명)으로 알려진 2개월이 지나면 사용자 인증 시에 "패스워드를 교체하라"고 고지하지만, 사용자들 대부분이 이 권고를 무시하고 현재 사용하는 패스워드를 그대로 사용하거나, 어떤 경우에는 두 개의 패스워드를 만들어 놓고 이를 번갈아 교체 사용하고 있는 실정이다. 새로운 신규 패스워드를 2개월에 하나씩 생성해내고, 이를 모두 기억하고, 각기 다른 여러 곳의 인증시스템에서 제각기 다르게 사용해야 한다는 것은 사용자 특성(User Characteristics)이나 사용자 행동 스타일(User Behavior Style)을 무시하거나 도외시한 발상으로 사용자에게의 책임전가나 행정적인 규제를 피해가려는 절차와 의도로 밖에 보이지 않는 것이다. 때문에 다발적으로 발생되는 여러 개의 신규 패스워드를 기록해 두거나, 또다른 곳에 저장을 하게 하거나, 아니면 교체 권고를 무시하게끔 유도하는 것과 다름없는 것이다.

[9] 또한 현재 가장 많이 사용되고 있는 패스워드를 이용한 인증기술의 경우, 가장 큰 문제점으로 개인 단말기 입력 시의 주위 노출은 물론 어깨너머로 훔쳐보는 숄더 서핑(Shoulder surfing)에 의해 주위 사람들에게 패스워드가 그대로 노출된다는 것이며, 현관문의 키패드나 개인용 단말기의 터치스크린 상에 누른 흔적이 남아있거나, 이러한 약간의 노출이나 흔적들을 추적하여 패스워드를 알아내는 추측공격(Guessing attack)이나 은밀하게 설치된 카메라(이하, 몰래 카메라)에 의한 노출 등으로 인하여 보안이 취약해지는 문제점이 있다.

[10] 종래 기술에 의한 또다른 사용자 인증기술로서 스마트폰과 같은 단말기의 터치스크린 상에서 암호 패턴을 그리는 사용자 인증기술이 사용되고 있다. 문자를 찾아 각각 입력하는 것보다 사용이 편하고, 빠른 입력동작이 가능하고, 패스워드 입력키의 숫자가 외부로 보이지 않기 때문에 주위 노출을 효과적으로 막을 수 있다고 여겨졌지만, 사용하는 패턴들이 비교적 단순한 형태여서 이 인증기술의 경우에도 주위의 노출, 숄더 서핑으로부터 안전하지 못하고, 특히 화면에 암호 패턴 자국이 그대로 남아있어 무의식 중에 패스워드가 외부로 노출되는 문제점이 있다.

[11] 이를 극복하기 위한 또다른 사용자 인증기술로서 생체정보(지문, 안면, 홍채, 정맥, 음성 등)를 이용한 생체인식 사용자 인증기술이 제안되고 있지만, 시스템을 구축하는데 비용과 시간이 많이 소요될 뿐만 아니라 사용자 등록과 인증 시 세심한 주의를 필요로 하며, 입력 및 인증 오류 발생 시의 대안으로 패스워드 입력을 또다시 요구하는데 이는 결과적으로 두 번의 인증과정을 거치게 하여 사용자를 번거롭게 만들기도 하지만, 신기술로 인식된 이러한

기술들이 검증 및 사용 단계에서 결국 원론적인 패스워드 입력방식으로 되돌아갔다는 것을 의미하는 것이기도 하다.

[12] 특히 이때 사용되는 패스워드 입력 시스템에는 아무런 보안 조치가 취해지지 않아 주위 노출을 막는 완벽한 보안이라는 생체인식 시스템이 최종에는 노출에 취약한 패스워드 입력 시스템에 의존하는 아이러니와 함께 노출에 대한 보안의 취약점을 그대로 방치하고 있는 셈이다.

[13] 또한, 신기술로 이루어지는 생체인식 사용자 인증기술은 사용자들이 처음 대하는 생소한 기술일 수밖에 없고 이의 적용으로 인한 사용자들의 거부감과 적응기간이 길고, 기기 교체 및 경제적인 문제로 단기간 내의 대중화 및 대량 보급이 어려우며, 보안과 안전성에 또다른 문제를 야기함으로 이에 대한 검증과 대책이 필요하다.

[14] 일례로 최근 상용화된 지문 인증의 경우, 사용자가 만취했을 때나 수면 중에는 타인에 의한 지문 도용이 쉽게 가능한 점, 사용자 손에 땀이나 물, 화장품, 페인트 등 이물질이 묻었거나 상처가 생겼을 경우의 인증 오류 및 실리콘 지문 채취 사용 등 사용상의 또다른 문제점들을 발생시키고 있어 아직은 수많은 검증절차가 필요한 문제점이 있다.

[15] 실제, 이 생체인식 인증 시스템은 사람마다 다 다르고 노출될 염려가 없어 보안성이 높다는 이유와 신기술에 대한 호감과 마케팅 효과로 각광을 받고 있지만, 해킹에 의해 미국의 공공기관에서 수백만 건의 지문정보가 대량 유출되는 사건이 발생하는가 하면, 국내에서도 지문이 탑재된 최신 스마트폰이 불과 출시 2년이 채 안되어 실리콘에 의한 모조 지문의 불법 도용으로 철통같다던 보안이 속속 뚫리고 있다.

[16] 최근 새롭게 제시된 정맥인식이나 홍채인식 인증 시스템도 한번 해킹을 당하면, 개개인의 고유하고 유일한 생체정보는 다른 것으로 바꾸거나 대체할 수가 없으며 이는 평생 바뀌지 않는 개인 신체정보라는 점에서 탈취당할 경우 해킹, 패스워드 불법사용 같은 1차 범죄 외에도 위조여권, 신분세탁 등 다른 범죄에까지 악용될 소지가 있기 때문에 이에 대한 불안감과 개인 생체정보의 보관과 이용문제 에 따른 사회적 논의 부재, 다양한 상황에서 오랜 기간에 걸쳐 철저하게 이루어져야 하는 검증의 부실로 아직은 사용자의 부적응, 불안감과 함께 사용상의 한계를 드러내고 있다.

[17] 이러한 새로운 기술의 검증문제와 편의성 및 사용자 적응문제, 경제적·사회적인 문제점 등으로 인하여, 종래에 거부감 없이 가장 많이 보편적으로 사용되고 있는 문자를 이용하는 패스워드에 보안성을 강화한 사용자 인증기술을 채용하고 있다. 한 예로 종래 기술에 의한 최근의 사용자 인증기술로서 핀테크(Fin-Tech)에 적용되는 일회용 비밀번호 생성기(OTP : One Time Password)와 숫자를 랜덤하게 무작위로 배열하고 이를 가상키보드를 이용해 패스워드를 입력하는 인증방법이 사용되고 있다.

[18] 이 기술은 키로거(Keylogger)를 방지할 수 있기 때문에 다른 사용자 인증기술에

비해 높은 보안등급으로 분류되어, 인터넷과 스마트폰 상의 금융 관련 인증에 널리 사용되고 있다. 이질적인 새로운 기술의 채용보다 사용자 적응 및 편리성, 오랜 기간의 검증, 도입의 간편함, 경제적인 이유 등의 장점 때문에 가장 보편적인 방법인 문자(숫자)를 이용한 패스워드 사용자 인증 방법에 보안성을 강화한 인증기술을 채용하고 있는 것이다.

[19] 하지만, 가상키보드를 이용한 랜덤키보드 방식은 입력키의 위치값 탈취를 막기 위해 사용 시마다 문자가 임의로 새롭게 재배열되기 때문에 사용자의 불편함을 초래하고, 문자 가독성과 직관력을 떨어뜨려 입력시간 지연 등으로 인해 오히려 주위 노출에 더 취약해지는 또다른 문제를 유발하였고, 이를 보완한 패스워드 입력키 사이에 무작위로 빈칸을 삽입하여 가독성과 사용자 편의성을 높이면서도 키로깅을 막는 새로운 랜덤키보드 패스워드 입력 방식이 제시되어 주로 모바일과 인터넷을 이용한 금융거래, 쇼핑 결제 등에 사용되고 있다.

[20] 하지만 이 역시 바뀐 숫자 입력키 위치를 화면 캡쳐하여 입력 패스워드를 탈취할 수 있으며, 이보다 더 큰 문제는 결과적으로 OTP나 랜덤키보드 방식을 채용한 패스워드 시스템 모두 패스워드 입력 시 가장 큰 문제가 되는 주위 노출이나 숄더 서핑을 근본적으로 막을 수 없는 보안성의 한계를 가지고 있다는 것이다.

[21] 이러한 주위의 관찰자에 의한 노출에 의해 보안을 유지할 수 없는 문제점은 이미 익히 알려져, 주위 노출에 의한 범죄가 가장 흔하게 일어나는 현관문 디지털 도어락(잠금장치)의 패스워드 입력 시 손동작을 가릴 수 있는 종이덮개를 서울의 한 경찰서에서 주위 노출 예방책으로 각 가정에 배포하고 있는 실정이며(2016년 2월 5일, 한국일보 신문기사 참조), 이는 수십만원을 호가하는 세련된 디자인의 현관 도어락을 종이박스로 덮어놓고 사용하는 우스꽝스러운 모습을 연출하고 있다. 또한 이와 유사한 범죄가 흔히 발생하는 ATM기에는 “주의, 반드시 비밀번호는 타인이나 카메라 등에 노출되지 않도록 손이나 책 등으로 가린 후 입력하십시오”라는 주의 경고를 띄워 적극적인 해킹방어를 포기한 채 사용자에게 위험을 상기시키는 소극적인 예방 정도로 그치고 있으며, 온라인상의 사용자 인증 시에는 모니터에 패스워드를 가리는 아스트리크(****)를 사용하기도 하지만, 이 모두 패스워드 입력 시 언제든지 발생할 수 있는 주위 노출이나, 숄더 서핑, 손동작 노출은 근본적으로 막을 수 없다는 문제점을 스스로 인정한 예이며, 이로인한 사용자의 피해사실을 알면서도 적극적인 해결책을 제시하지 않는 보안 관계자들의 무책임한 행태이기도 하다.

[22] 또한, 현재 주위에서 흔하게 볼 수 있는 적극적인 숄더 서핑과 주위 노출 방지 사례 중 하나로, 금융기관에서 고객에게 제공하는 비밀번호 입력 키패드에는 비밀번호를 입력하는 버튼과 액정 모니터 주위에 가림판이 설치되어 있는 것을 볼 수 있는데, 이 역시 숫자로 된 짧고 단순한 패스워드의 입력 시 쉽게 발생하는 주위 노출이나 숄더 서핑을 차단하기 위한 것으로, 거의 모든 은행에서는

일상적으로 간편하게 사용하고 있다.

[23] 이처럼 생각만 바꾸면, 간단한 가림판 하나로도 패스워드나 복잡한 암호체계를 특별하거나 어렵게 바꾸지 않더라도 주위 노출을 효과적으로 막는다는 것이 입증되었기 때문에 시중의 모든 은행창구에서 널리 사용되고 있는 것이다. 하지만 이 역시 가림판이 달린 특별한 키패드를 일일이 제공하거나, 이를 사용할 수 있는 장소에 한정되며, ATM기나 핸드폰, 노트북 등 개인용 단말기에는 적용할 수 없고, 온라인상에서도 사용될 수 없는 하드웨어적인 한계와 문제점을 지니고 있다.

[24] 문자(숫자) 입력의 패스워드 인증방식에서 또 한 가지 주목해야 하는 것이, 패스워드 입력 시 발생하는 오류 입력정보의 처리 문제이다. 일반적으로 패스워드 입력 시 누구나 몇 번씩 겪어 본 것이 망각(패스워드 분실)이나 착각 혹은 입력 실수, 입력시간 지연에 의한 패스워드 입력 오류이다.

[25] 이는 패스워드 입력이 필요한 수많은 인증 시스템에서 요구하는 패스워드 키값의 요건이 통일되지 않고 4자리, 6자리, 혹은 여덟 자리 숫자 사용, 문자 혼용 등 제각각 모두 다르기 때문인 것이 1차적인 이유이지만, 근래에 들어서는 보안의 중요성이 부각되면서 잦은 패스워드의 교체와 많은 자릿수(8자리 이상)의 패스워드 사용 요구, 거기에 더불어 영문 대소문자, 특수문자의 사용 등 사용자를 고려하지 않은 일방적인 요구로 사용자의 혼란을 가중시키기 때문이다. 사용(편리성)이 어려워지면 보안성이 높아지는 것은 당연한 이치이므로 이는 패스워드 관련 개발자들이 이를 고민하지 않고 편의주의적으로 도외시하고 사용자에게 그 책임을 전가하고 있는 현상이며, 이로 인한 패스워드 입력 오류가 더욱 빈번히 발생하는 문제점이 있다.

[26] 상기와 같은 사용자 입력 오류 이외에도 불법 해킹 시도에서도 여러번의 패스워드 키값이 입력되지만 쓸모없는 데이터로 오류 처리하고 패스워드 재입력을 요구한다. 즉, 패스워드 입력 시마다 필연적으로 발생할 수 있는 잘못된 데이터, 즉 오류데이터는 정크 데이터로 분류되어 쓸모없는 취급을 하여 왔다. 이처럼 쓸모없이 버려졌던 패스워드 인증 시의 오류데이터 값들인 정크 데이터(Junk data)는 아무 쓸모가 없다는 인식과 관습적인 행태 때문에 이를 저장, 관리하거나 분류 및 분석하고 리스크 데이터로 활용하여 인증기술에 이용하거나 개발하지 못하고 있다.

[27] 현재 부각되고 있는 빅데이터(Big data) 역시 수집의 문제보다는 데이터의 분석과 여기에서 의미 있는 가치 데이터(Value)를 찾아내는 작업이 더 중시되고 있다. IT의 발달로 시시각각 엄청나게 생산되어지는 데이터들은 쓸모없는 것으로 여겨져 대부분 방치되어왔지만, 이 방대한 데이터들은 여러 가지 분석에 의해 구글의 자동번역시스템, 슈퍼컴퓨터 왓슨, 아마존 도서추천시스템 등으로 막강한 위력을 갖춘 혁신 기술로 새로 태어났으며 다양한 마케팅활동에 적용되는 것은 물론 사용자의 생각과 의견까지도 분석하고 예측해내는 단계에까지 와있다.

[28] 빅데이터의 예에서 보듯이, 우리도 모르는 사이에 만들어내고 있는 이 쓸모없다고 여겨왔던 데이터들이 어떻게 분류, 분석되고 어떻게 사용되느냐에 따라 중요한 정보를 가진 핵심 가치데이터로 재탄생하게 되는 것처럼, 하루에도 몇 번씩 사용되는 패스워드 인증 시에 발생하는 오류데이터, 해킹 시도에 사용되었던 오류데이터 등 수많은 패스워드 관련 정크 데이터들을 수집, 분석하거나 혹은 유발시켜, 이를 토대로 위험 데이터(Risk data) 등 가치 데이터를 찾아내지 못하는 것은 물론 해킹 예방이나 보안 강화를 위해 이를 적극적으로 활용하지도 못하고 있는 것이다.

발명의 상세한 설명

기술적 과제

[29] 본 발명의 목적은 사용자가 원래 패스워드로 등록한 패스워드를 입력하기 이전 및 이후 또는 이전, 이후에 랜덤 키(Random Key)값을 이용해 무작위로, 원하는 자릿수만큼 자유롭게 즉흥적으로 정크 데이터를 생성·입력할 수 있도록 하여, 패스워드 입력이 주위에 노출되거나 입력 동작을 타 관찰자가 주시하고 있어도 무작위의 정크 데이터 안에 포함되어 있는 패스워드 키값을 알아보지 못하도록 하여 패스워드의 주위 노출 및 숄더 서핑, 추측공격을 방지하는 사용자 인증시스템을 제공하는 데에 있다.

[30] 특히, 본 발명은 입력받은 정크 데이터가 포함된 패스워드를 과거 입력된 정크 데이터가 포함된 패스워드와 비교하되, 적어도 일정 길이 이상이 일치하는 경우 해킹으로 추단함으로써 보안성을 한층 강화하는 사용자 인증시스템의 제공을 목적으로 한다.

과제 해결 수단

[31] 상기와 같은 목적을 달성하기 위하여 본 발명에 의한 사용자 인증 방법은, 사용자 인증 시스템이, (a) 사용자로부터 정크 데이터가 포함된 패스워드 - 이때, 정크 데이터는 패스워드의 이전, 이후 또는 이전 및 이후에 포함됨 - 를 입력받는 단계;

[32] (b) 입력받은 정크 데이터가 포함된 패스워드로부터 정크 데이터를 제외한 패스워드를 분리 추출하는 단계;

[33] (c) 상기 정크 데이터가 포함된 패스워드가, 과거 입력된 정크 데이터가 포함된 패스워드와 임계길이만큼 일치하는 경우, 상기 분리 추출된 패스워드가 저장수단에 기 저장된 패스워드와 일치함에도 불구하고 사용자 인증을 실패로 처리하는 단계;를 포함할 수 있다.

[34] 이때, 상기 (c)단계에서, 상기 사용자로부터 입력받은 정크 데이터가 포함된 패스워드가 임계길이 이상인 경우, 상기 정크 데이터가 포함된 패스워드가, 과거 입력된 정크 데이터가 포함된 패스워드와 임계길이만큼 일치하는지 여부를 판정하되,

[35] 상기 사용자로부터 입력받은 정크 데이터가 포함된 패스워드가 임계길이

미만인 경우, 상기 정크 데이터가 포함된 패스워드가, 과거 입력된 정크 데이터가 포함된 패스워드와 임계길이만큼 일치하는지 여부의 판정을 생략하고, 상기 분리 추출된 패스워드가 저장수단에 기 저장된 패스워드와 일치하면 사용자 인증을 성공으로 처리할 수 있다.

[36] 이때, 임계길이는 9자리 또는 그보다 더 긴 길이이며,

[37] 상기 정크 데이터가 포함된 패스워드와 과거 입력되어 기 저장된 정크 데이터가 포함된 패스워드의 일치 여부를 비교하되, 연속적 또는 불연속적으로 임계길이만큼 일치하는 경우, 상기 패스워드가 저장수단에 기 저장된 패스워드가 일치함에도 불구하고 사용자 인증을 실패로 처리할 수 있다.

[38] 이때, 임계길이는 현재 보편적으로 사용되는 4자리 패스워드를 적용할 경우 9자리(패스워드 4자리 + 정크 데이터 5자리)가 바람직하지만, 이 임계길이는 이보다 더 길게 확대 적용할 수 있다. 왜냐하면, 현재 중국에서는 6자리 패스워드 사용이 일반화되었고, 국내에서도 최근 보안성을 높이기 위해 4자리에서 8~10자리로 패스워드 자릿수를 늘리는 것을 감안하면, 패스워드가 8자리일 경우에 임계길이가 9자리이면 패스워드 외에 정크 데이터를 사용하거나 비교 가능한 개수가 1개밖에 되지 않기 때문에 보안성과 사용자 편의성을 고려하면 임계길이를 확대하여 사용할 수 있다.

[39] 한편, 상기 패스워드가 포함된 정크 데이터 패턴은,

[40] 복수 개의 자릿수로 이루어진 정크 데이터 및 4개 이상의 자릿수로 이루어진 패스워드를 포함하는 패턴;

[41] 복수 개의 자릿수로 이루어진 제1 정크 데이터, 4개 이상의 자릿수로 이루어진 패스워드 및 복수 개의 자릿수로 이루어진 제2 정크 데이터를 포함하는 패턴; 및

[42] 3개 이상의 자릿수로 이루어진 제1 패스워드, 복수 개의 자릿수로 이루어진 정크 데이터 및 3개 이상의 자릿수로 이루어진 제2 패스워드를 포함하는 패턴;

[43] 가운데 어느 하나의 패턴을 포함할 수 있다.

[44]

[45] 상기와 같은 목적을 달성하기 위하여 본 발명의 일 실시예에 의한 정크 데이터 일치여부를 이용한 사용자 인증 시스템은, 사용자로부터 패스워드 및 정크 데이터를 입력받는 입력수단;

[46] 프로세서가 실행할 명령어를 적재하는 저장수단;

[47] 상기 저장수단에 적재된 명령어를 순차 실행하는 프로세서;를 구비한다.

[48] 이때, 상기 프로세서는 상기 입력수단을 통해 사용자로부터 정크 데이터가 포함된 패스워드 - 이때, 정크 데이터는 패스워드의 이전, 이후 또는 이전 및 이후에 포함됨 - 를 입력받으면, 입력받은 패스워드로부터 정크 데이터를 분리하고, 상기 정크 데이터가 포함된 패스워드가, 과거 입력된 정크 데이터가 포함된 패스워드와 임계길이만큼 일치하는 경우, 상기 분리 추출된 패스워드가 저장수단에 기 저장된 패스워드와 일치함에도 불구하고 사용자 인증을 실패로 처리할 수 있다.

[49]

[50] 한편, 본 발명의 다른 실시예에 의한 정크 데이터 일치여부를 이용한 사용자 인증 시스템은,

[51] 네트워크를 통해 데이터를 송수신하는 통신 어댑터;

[52] 프로세서가 실행할 명령어를 적재하는 저장수단;

[53] 상기 저장수단에 적재된 명령어를 순차 실행하는 프로세서;를 구비한다.

[54] 이때, 상기 통신 어댑터는 네트워크를 통해 연결된 원격 단말로부터 정크 데이터가 포함된 패스워드 - 이때, 정크 데이터는 패스워드의 이전, 이후 또는 이전 및 이후에 포함됨 - 를 입력받으며,

[55] 상기 프로세서는 원격 단말로부터 입력받은 패스워드에서 정크 데이터를 분리하고, 상기 정크 데이터가 포함된 패스워드가 과거 입력된 정크 데이터가 포함된 패스워드와 임계길이만큼 일치하는 경우, 상기 분리 추출된 패스워드가 저장수단에 기 저장된 패스워드가 일치함에도 불구하고 사용자 인증을 실패로 처리할 수 있다.

[56] 상기 두 실시예에서, 상기 프로세서는 상기 입력받은 정크 데이터가 포함된 패스워드의 길이가 임계길이 이상인 경우, 상기 정크 데이터가 포함된 패스워드가 과거 입력된 정크 데이터가 포함된 패스워드와 임계길이만큼 일치하는지 여부를 비교하되,

[57] 상기 사용자로부터 입력받은 정크 데이터가 포함된 패스워드가 임계길이 미만인 경우 상기 정크 데이터가 포함된 패스워드가, 과거 입력된 정크 데이터가 포함된 패스워드와 임계길이만큼 일치하는지 여부의 비교를 생략하고,

[58] 상기 패스워드가 저장수단에 기 저장된 패스워드가 일치하면 사용자 인증을 성공으로 처리할 수 있다.

[59] 이때, 임계길이는 9자리이거나 또는 그 이상의 길이이며, 연속적 또는 불연속적으로 임계길이만큼 일치하면 상기 패스워드가 저장수단에 기 저장된 패스워드가 일치함에도 불구하고 사용자 인증을 실패로 처리할 수 있다.

발명의 효과

[60] 본 발명은 사용자로부터 입력된 정크 데이터가 포함된 패스워드에서 무작위 자릿수, 무작위 수로 이루어진 하나 이상의 정크 데이터를 제외하고 소정의 자릿수로 이루어진 패스워드를 분리 추출하고, 입력된 정크 데이터가 포함된 패스워드가 과거 입력된 정크 데이터가 포함된 패스워드와 적어도 일정 길이 이상 일치하는 경우, 분리 추출된 패스워드가 미리 저장되어 있는 패스워드와 일치함에도 불구하고 사용자 인증을 실패로 처리함으로써, 보안성과 편리성을 동시에 함께 향상시킬 수 있는 효과가 있다.

[61] 패스워드를 길게 하면 보안성은 높아지는 반면에 간편성은 떨어지기 때문에 보안성을 높이기 위해 무한정 패스워드의 자릿수를 많게 할 수는 없다. 하지만 본 발명은, 사용자는 짧은 패스워드만을 기억하고 사용하지만, 패스워드 입력

시에는 패스워드의 전과 후, 또는 전후에 짧은 패스워드를 타 관찰자가 알아채지 못하도록 정크 데이터를 입력하되, 이 정크 데이터는 소정의 자릿수, 소정의 숫자를 일부러 기억하는 것이 아니라 무의식적이며 즉흥적으로 만들어져 아무런 정보나 의미를 갖지 않는 무작위의 숫자를 임의로 무작위 개수만큼 자유롭게 입력하기 때문에 간편성과 보안성을 동시에 획기적으로 높일 수 있게 된다.

[62] 또한, 현관문의 도어락, 차량 도어의 개폐장치, 금고 도어락과 노트북 컴퓨터, 태블릿 PC 및 스마트폰 등 개인 단말기와 스마트워치 등 웨어러블 기기, IoT와 연동되는 기기의 잠금장치의 잠금 상태를 해제하거나, 유무선의 네트워크를 통해 서버와 연결된 컴퓨터, 스마트폰, 태블릿 PC 및 노트북 컴퓨터, 스마트TV 등의 인터넷 사용자 인증 시스템에서 사용자를 인증하거나, 전자상거래, 금융기관의 온라인 인증이나 금융서비스, 현금자동입출금기(ATM) 및 민원서류발급기 등의 시스템에서 기존의 구조를 변경하거나 기기의 교체 없이 소프트웨어만 업그레이드 하여 간단하게 적용할 수 있는 효과가 있다.

[63] 또한, 사용자 입장에서는 이전부터 사용하고 있던 패스워드를 새로 교체하거나 어렵고 복잡하고 길게 만들지 않고 그대로 사용할 수 있음으로써 패스워드 오류나 패스워드 망각, 분실 등에서 자유롭고, 주위의 노출에 신경 쓸 필요가 없어 장소에 구애 받지 않고 자유로운 사용이 가능해지며, 현재의 익숙한 패스워드(비밀번호) 입력방식을 그대로 사용하게 되어 새로운 기기, 새로운 방법, 새로운 인증 시스템의 적응에 대한 거부감과 작동 오류가 없고 친숙하고 익숙한 이점이 있어 패스워드의 빠른 입력이 가능하여 주위 노출, 숄더 서핑, 추측 공격은 물론 몰래카메라 노출에서도 안전성과 편리성을 함께 확보할 수 있는 효과가 있다.

[64] 특히 OTP나 랜덤 가상키보드는 키로깅을 회피할 수는 있지만 패스워드 입력 시 짧은 패스워드 키값만을 입력하기 때문에 입력 시 필연적으로 발생하는 주위 노출이나 숄더 서핑을 막을 수 없는 보안상의 한계를 지니고 있으나, 본 발명은 패스워드 입력 시마다 패스워드에 무작위 자릿수의 무작위의 즉흥적인 정크 데이터를 함께 입력하여, 일정하지 않고 불규칙하게 생성되는 항상 다른 형태의 숫자 조합 안에 패스워드를 감출 수 있기 때문에, 설령 패스워드 입력 동작이 주위의 사람들에게 노출되더라도 주위 사람들은 패스워드가 포함된 정크 데이터 안에 있는 실제 패스워드를 알아낼 방법이 없고, 항상 바뀌는 긴 패스워드를 기억할 수도 없어 보안성과 편리성이 함께 높아지는 것은 물론, 패스워드 입력 방식에서 현재 기술로는 근본적으로 막을 수 없는 주위 노출과 숄더 서핑, 몰래카메라 해킹에서도 안전성을 함께 확보할 수 있어, 주변 사람들이 함께 있는 장소에서의 패스워드 입력 시 겪는 어색한 분위기와 불안감도 사라지게 된다.

[65] 또한, 정크 데이터를 입력하지 않고 패스워드만으로도 사용자 인증이 가능하기 때문에, 특별한 보안이 필요 없는 자택이나 사무실 등 안전한 상황에서는

간편하고 빠르게 짧은 패스워드만을 그대로 입력하여 사용자 인증을 할 수 있어, 사용자의 선택에 따라 보안성을 높일 수도, 간편성을 높일 수도 있는 선택 사용이 가능한 편리함이 있다.

[66] 또한, 패스워드 입력 시 생성되는 오류 데이터를 활용하지 못하는 OTP나 랜덤 가상키보드를 활용한 인증 방법과 달리, 설령 몰래 카메라나 숄더 서핑, 노출 등에 의해 패스워드가 해킹되었다 하더라도 현재 입력된 정크 데이터와 이전에 입력되어 저장된 정크 데이터와의 비교를 통해 해킹된 패스워드라는 것을 사전에 미리 인식하여 위험 경고 예보를 할 수 있으며, 이후 2차로 정크 데이터가 제외된 실제 패스워드 입력을 요청하여 사용자 인증을 확실하게 다시 하게 되므로, 노출이나 해킹에 의한 불법 사용자 인증을 예방 및 차단할 수 있는 효과가 있다.

[67] 특히 개인정보가 실시간 저장·공유되는 웨어러블 제품이나 IoT 기기의 경우, 주변을 의식하지 못하고 개방된 불안전한 공간에서도 자주 사용하게 되는 것은 물론 IoT 기술의 발달로 텍스트 입력 외에도 음성, 그래픽, 영상 등을 사용하게 됨으로써, 컨트롤러나 디바이스의 락 해제나 사용자 인증 시 주변에 패스워드가 노출될 가능성이 더욱 높아지지만, 본 발명은 무작위의 랜덤키값을 입력하여 생성한 정크 데이터 안에 패스워드를 숨겨 사용하기 때문에 패스워드를 입력하는 화면, 음성, 동작 등이 주위에 노출되어도 타인은 패스워드를 알아챌 수가 없어 웨어러블 제품이나 IoT 기기를 여러 사람 앞에서도 어색하지 않게 사용하게 되고, 보안관련 사용자 불안감 1위가 "디바이스 사용 시의 주위 노출"이라는 불안감을 없애줌으로써 제품의 신뢰도 향상은 물론 편리성과 보안성을 함께 높이는 효과가 있다.

도면의 간단한 설명

[68] 도 1은 본 발명에 의한 사용자 인증 시스템의 하드웨어 구성을 예시한 블록도이며,

[69] 도 2는 본 발명에 의한 사용자 인증 시스템과 원격단말의 연결관계를 도시한 망구성도이며,

[70] 도 3은 사용자가 입력수단 또는 원격단말을 이용하여 입력하는 모습을 예시하는 도면이며,

[71] 도 4는 본 발명에 의한 정크 데이터 일치여부를 이용한 사용자 인증 방법의 처리과정을 도시한 플로우차트이며,

[72] 도 5는 본 발명에 의해 실제 패스워드에 랜덤키값이 추가되어 생성된 정크 데이터의 패턴 예시를 나타낸 도면이며,

[73] 도 6은 본 발명에 의해 패스워드와 정크 데이터를 입력하여 사용자 인증에 사용된 3가지 패턴과 불법 노출이나 해킹에 의해 사용된 예시를 나타낸 도면이다.

[74] - 도면 부호의 설명 -

[75] 100 : 사용자 인증 시스템

[76] 110 : 프로세서

[77] 120 : 입력수단

[78] 130 : 표시수단

[79] 140 : 저장수단

[80] 150 : 통신수단

[81] 200 : 원격단말

발명의 실시를 위한 최선의 형태

[82] 본 명세서에서 사용되는 용어에 대해 간략히 설명하고, 본 발명에 대해 구체적으로 설명하기로 한다.

[83] 본 발명에서 사용되는 용어는 본 발명에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들을 선택하였으나, 이는 당 분야에 종사하는 기술자의 의도 또는 판례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 발명의 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서 본 발명에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 발명의 전반에 걸친 내용을 토대로 정의되어야 한다.

[84] 명세서 전체에서 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있음을 의미한다. 또한, 명세서에 기재된 "...수단", "...부", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어 또는 소프트웨어로 구현되거나 하드웨어와 소프트웨어의 결합으로 구현될 수 있다.

[85] 아래에서는 첨부한 도면을 참고하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[86] 도 1은 본 발명에 의한 사용자 인증 시스템의 하드웨어 구성을 예시한 블록도이다.

[87] 도 1에 도시된 사용자 인증 시스템(100)은 프로세서(110), 입력수단(120), 표시수단(130), 저장수단(140) 및 통신수단(150)을 구비한다.

[88] 프로세서(110)는 저장수단(140)에 저장된 명령어를 실행한다. 한편, 프로세서(110)는 입력수단(120)을 통해 입력되는 패스워드 및 정크 데이터를 표시수단(130)에 표시함과 함께, 저장수단(140)에 미리 저장되어 있는 패스워드 및 정크 데이터들을 비교하여 후술하는 사용자 인증방법으로 사용자 인증을

실시하는 역할을 한다.

[89] 입력수단(120)은 사용자 인증 시스템(100)에 구비된 주변기기로서 사용자로부터 패스워드 및 정크 데이터를 입력받기 위한 장치로서, 그 형태에는 제한을 두지 아니한다.

[90] 예컨대, 키보드나 마우스, 터치스크린 등일 수 있다.

[91] 또는, 입력수단(120)은 마이크일 수 있다. 사용자의 음성을 입력받아 이를 텍스트 데이터로 변환하여 입력값으로 사용할 수 있다.

[92] 이외에도, 현관문의 디지털 도어락, 차량 도어나 금고에 설치된 키패드, 리모콘, 현금자동입출금기(ATM) 및 민원서류발급기 등 자동화기기의 키패드 등 다양한 형태로 구현될 수 있다.

[93] 표시수단(130)은 프로세서(110)의 제어를 받아 사용자에게 알려주고자 하는정보를 시각적, 청각적, 촉각적인 방식에 의해 표시하기 위한 장치로서, 액정표시장치(LCD), 스피커, 기타 알려진 다양한 형태의 출력장치일 수 있다.

[94] 저장수단(140)은 프로세서(110)가 실행할 명령어가 포함된 프로그램을 적재할 수 있다. 한편, 저장수단(140)은 사전에 사용자에 의해 상기 입력수단(120)을 통해 입력된 패스워드 및 패스워드와 함께 입력되어 사용된 정크 데이터를 저장한다.

[95] 이러한 저장수단(140)은 하드 디스크나, 플래쉬 메모리 등 휘발성 또는 비휘발성의 로컬 스토리지이거나, 또는 클라우드나 원격지 서버나 NAS(Network Attached Storage)일 수 있다.

[96] 통신 어댑터(150)는 네트워크를 통해 연결되는 원격단말(200)과 소정의 통신규약에 따라 통신하기 위한 장치이다.

[97] 이때, 네트워크는 인터넷 망이나, 인트라넷, 이동통신망 등 알려진 다양한 형태의 유무선 통신망일 수 있다.

[98] 이러한 사용자 인증 시스템(100)은 상기와 같은 요소를 구비하는 것이라면 하드웨어의 형태에는 특별한 제한을 두지 아니한다.

[99] 예컨대, 개인용 컴퓨터나 랩탑, 스마트폰, 타블렛 컴퓨터의 형태일 수도 있으며, 스마트 워치나 기타 웨어러블 디바이스, 네트웍을 통해 다수의 원격 단말과 연결되는 서버의 형태일 수 있다.

[100] 도 2는 본 발명에 의한 사용자 인증 시스템과 원격단말의 연결관계를 도시한 망구성도이다.

[101] 도 2에 예시된 사용자 인증 시스템(100)은 다수의 원격단말(200)과 네트워크를 통해 연결된다.

[102] 사용자는 사용자 인증 시스템(100)에 구비된 입력수단(120)을 이용하여 직접 입력을 할 수도 있으나, 네트워크를 통해 연결된 원격단말(200)을 이용하여 입력할 수도 있다.

[103] 원격단말(200)은 원격지에서 사용자 인증 시스템(100)과 통신하며, 사용자 인증 시스템(100)으로 패스워드 및 패스워드와 함께 정크 데이터를 입력하기

위한 수단으로, 사용자 인증 시스템(100)과 물리적으로 분리된 스마트폰, 개인용 컴퓨터, 유무선 통신이 가능한 현관문의 디지털 도어락, 차량 도어나 금고, 네트워크에 연결된 현금자동입출금기(ATM) 및 민원서류발급기 등 자동화기기일 수 있다.

[104] 이외에도, 원격단말(200)은 유무선 통신이 가능한 가스보일러, 전구, 전원스위치, 스피커와 같은 IoT(Internet of Things) 제품일 수 있다.

[105] 또는, 원격단말(200)은 무선 통신망에 연결되며, 지그비(Zigbee)나 블루투스(Bluetooth)와 같은 근거리 무선 통신 방식에 의해 각종 IoT 제품을 콘트롤하는 IoT 콘트롤러일 수도 있다.

[106] 그 외에도, 이와 같은 다양한 IoT 제품과 연동되는 스마트폰이나 타블렛 컴퓨터 등의 모바일 디바이스의 형태일 수도 있다.

[107] 이외에도, 상기의 정의를 만족하는 것이라면 하드웨어의 형태에 제약을 두지 아니한다.

[108] 도 3은 사용자가 입력수단 또는 원격단말을 이용하여 입력하는 모습을 예시하는 도면이며, 도 4는 본 발명에 의한 정크 데이터 일치여부를 이용한 사용자 인증 방법의 처리과정을 도시한 플로우차트이다.

[109] 사용자는 도 3에 예시된 바와 같이, 입력수단(120) 또는 원격단말(200)을 통해 패스워드 또는 정크 데이터를 입력할 수 있다.

[110] 도 3의 예에서는 숫자를 터치하여 입력하는 것으로 도시하였으나, 이는 예시적인 것으로 패스워드와 정크 데이터는 숫자는 물론, 문자 및 특수문자, 기호가 사용될 수 있다.

[111] 입력수단(120)이 마이크인 경우, 사용자는 음성으로 입력할 수도 있다.

[112] 프로세서(110)는 입력받은 데이터를 분절화하여 텍스트 데이터로 변환한 다음 이를 입력값으로 사용할 수 있다. 음성 데이터를 텍스트로 변환하는 알고리즘은 공지의 것을 사용할 수 있다.

[113] 도 5는 본 발명에 의해 실제 패스워드에 랜덤키값이 추가되어 생성된 정크 데이터의 패턴 예시를 나타낸 도면이며, 도 6은 본 발명에 의해 패스워드와 정크 데이터를 입력하여 사용자 인증에 사용된 3가지 패턴과 불법 노출이나 해킹에 의해 사용된 예시를 나타낸 도면이다.

[114] 이하, 도 3 내지 도 6을 참조하여 본 발명에 의한 정크 데이터 일치여부를 이용한 사용자 인증 방법에 대하여 살펴보기로 한다.

[115] 사용자가 이전에 패스워드 설정모드를 수행하지 않아 최초로 패스워드 설정을 요청하거나 이미 설정된 패스워드의 변경을 요청하는 경우 프로세서(110)는 패스워드 설정모드를 실행한다(S1).

[116] 이어서, 프로세서(110)는 사용자가 설정하는 패스워드의 키(Key)값을 입력받아 저장수단(140)에 저장한다(S2).

[117] 본 발명에 사용되는 패스워드는 사용자가 설정하고자 한 소정의 자릿수를 가진 패스워드(PW, Password)로 이루어지지만, 사용자 인증단계에서의 패스워드

입력 시에는 상기 패스워드를 감추기 위한 하나 이상의 정크 데이터(JD, Junk Data)와 함께 입력이 이루어진다.

[118] 상기 정크 데이터는 사용자가 항시 기억해야 하는 일정한 형식과 요건을 갖춘 패스워드와는 달리, 사용자의 무의식적이고 즉흥적인 입력 동작에 의해 생성되기 때문에 필요한 정보가 없는 무의미하고 엉터리인 '정크 데이터(Junk data)'란 말 그대로 아무 쓸데없는 데이터로, 사용자가 원래 패스워드로 등록한 패스워드(PW)를 입력하기 이전 및 이후 또는 이전, 이후에 사용자에 의해 무작위로, 원하는 자릿수만큼 즉흥적으로 자유롭게 입력되어 생성, 사용된다.

[119] 도 5의 (a) 내지 (d)는 사용자 인증단계에서 사용자에 의해 입력되는 패스워드와 함께 입력되는 정크 데이터(JD)에 의해 만들어지는 패턴을 예로 들어 나타낸 것이다. 여기서, (a)는 4자리 수의 정크 데이터(JD)와 상기 정크 데이터(JD)의 다음에 위치하는 4자리 수의 패스워드로 이루어진 패턴의 예를 나타낸 것이다. (b)는 4자리 수의 패스워드와 상기 패스워드의 다음에 위치하는 8자리 수의 정크 데이터(JD)로 이루어진 패턴의 예를 나타낸 것이다. (c)는 3자리 수의 제1 정크 데이터(JD1), 상기 제1 정크 데이터(JD1)의 다음에 위치하는 4자리 수의 패스워드 및 상기 패스워드의 다음에 위치하는 5자리 수의 제2 정크 데이터(JD2)로 이루어진 패턴의 예를 나타낸 것이다. (d)는 4자리 수의 제1 패스워드(PW1), 상기 패스워드(PW1)의 다음에 위치하는 5자리 수의 정크 데이터(JD) 및 상기 정크 데이터(JD)의 다음에 위치하는 3자리 수의 제2 패스워드(PW2)로 이루어진 패턴의 예를 나타낸 것이다.

[120] 상기와 같이 이루어지는 패스워드와 정크 데이터에 사용되는 숫자의 개수는 특별하게 한정되지 않는다. 단지, 패스워드를 구성하는 숫자의 개수는 사용자의 편의성을 감안할 때 짧을수록 좋겠지만, 패스워드 구성의 최소단위인 4자릿수 이상이 바람직하고, 정크 데이터를 구성하는 개수는 1개부터 n개까지 자유롭게 무작위로 즉흥적으로 사용할 수 있지만, 사용자의 편의성과 입력시간을 고려하고, 타인에 의한 추측공격을 가정할 경우 현실적인 실제 입력 개수는 10자릿수 이하로 한정하는 것이 좋다.

[121] 즉, 사용자가 기억해야 하는 실제 패스워드는 짧고 간편하게 4개의 숫자 조합으로 사용하지만, 패스워드의 전과 후 또는 전 후에 추가하는 정크 데이터의 개수(자릿수)는 사용자가 임의로 무작위하게 자유롭게 마음대로 생성해 추가할 수 있다.

[122] 단, 사용자의 편의성을 고려한다면 10자리 미만의 개수가 편리하지만, 도 5의 (b), (c), (d)에서와 같이 패스워드가 포함된 정크 데이터 전체의 숫자 개수는 보안성을 높이기 위해서는 적어도 10자리 이상의 충분히 긴 길이인 것이 바람직하다. (b), (c)의 경우, 사용한 정크 데이터 8자리를 제외하면 사용자가 기억해야 하는 실제 패스워드의 키값은 4개밖에 되지 않는다. 참고로, 1956년 발표된 조지 밀러(George A. Miller)의 연구논문 "The Magic number seven, plus or minus Two"에 의하면, 사람이 외울 수 있는 숫자의 일반적인 개수는 평균 7자리

수로 보고되고 있다. 이를 감안할 때, 도 5의 (b)와 (c)같은 패스워드는 편의성과 보안성을 모두 만족하는 패스워드이다.

[123] 왜냐하면, 패스워드를 포함한 정크 데이터를 이루는 숫자가 모두 12자리이므로 주위 노출이나 타인의 기억 등에서 보안성이 매우 우수하고, 이 12자리 중에서 사용자는 정크 데이터를 제외한 실제 패스워드에 해당하는 4자리 숫자 '2016'만 기억하면 되므로 편리성 또한 우수하다고 할 수 있다.

[124] 이는 조지 밀러의 연구논문에 따르면, 7자리 숫자를 기준으로, 여기서 2자리가 작은 5자리 숫자는 누구든지 쉽게 외울 수 있는 반면, 2자리가 큰 9자리 숫자는 외울 수 없는 숫자조합이 된다. 즉, 사용자에게는 암기하기 쉬운 패스워드이지만, 정크 데이터로 위장된 패스워드는 노출되어도 곁에서 이를 보고 외울 수가 없게 된다.

[125] 도 6의 (c)와 (n)의 경우처럼, 주변에 관찰자들이 많아 부득이 긴 숫자인 16자리 숫자나 19자리 숫자가 입력될 경우, 패스워드로 사용하기에는 매우 긴 숫자이지만 사용자는 4자리의 패스워드만 기억하기 때문에 아무런 부담 없이 이 긴 숫자조합을 편하게 입력하게 되고, 패스워드 입력 시 고의로 주위 노출을 유발한다 해도 주위 관찰자들은 이 긴 숫자 조합 중에서 실제 패스워드 4개를 알아낼 수도 없고, 또한 인간의 기억범위와 능력으로는 이 긴 숫자 조합을 기억할 방법이 없어 주위 노출이나 숄더 서핑에서 확실한 안전을 보장하게 된다.

[126] 이하, 설명에서는 사용자에 의해 입력되는 패스워드를 포함한 정크 데이터가 도 5의 (c)와 같은 패턴인 것을 예로 하여 설명한다.

[127] 사용자 인증모드에서 제어부(120)는 키 입력부(110)를 통해 사용자로부터 패스워드(PW)와 상기 패스워드의 이전에 입력되는 제1 정크 데이터(JD1) 및 상기 패스워드의 이후에 입력되는 제2 정크 데이터(JD)를 입력받는다(S3).

[128] 이때 사용자가 항상 상기와 같이 패스워드와 함께 정크 데이터(JD)를 입력하는 것은 아니다. 예를 들어, 사용자가 현재 상황이 패스워드와 정크 데이터(JD)를 함께 사용하지 않아도 되는 자택이나 사무실 등 보안이 필요 없는 안전한 상황이라고 판단될 때, 도 6의 (e), (k), (m)과 같이 간단한 실제 패스워드만을 빠르고 간편하게 입력할 수 있다.

[129] 도 6에서 제시한, 수집된 정크 데이터 사용 예시를 자세히 비교·분석해보면, 상기의 예시와 같이 (e), (k), (m)은 실제 패스워드만을 사용해 인증한 경우로 안전한 장소에서 사용된 것임을 알 수 있고, 4자리 패스워드와 6자리 이상의 정크 데이터, 즉 10자릿수 이상을 입력하여 사용한 (a), (c), (f), (g), (h), (j), (n), (o)의 경우 주위가 불안전하거나 불안한 상태에서 입력된 패스워드라는 것을 알 수 있다.

[130] 특히 이 중 (h)와 (o)의 경우, 패스워드와 함께 입력된 정크 데이터 12자릿수가 동일하고, 먼저 입력된 (h)가 불안전한 곳에서 불안한 상태로 입력된 것이 확실하고, 이후 입력된 (o)가 (h)와 동일하므로, (h)가 주위 노출, 몰래 카메라 등에 의해 해킹되어 사용된 것이 (o)라는 판단을 하게 된다. 이렇게 정크

데이터를 이용해 해킹에 의한 불법 사용을 예측하여 사용자 인증을 에러 처리하고 "해킹 위험"경고를 게시할 수 있다.(S7, S9)

[131] 상기 예시에서 알 수 있듯이 패스워드 입력 시 수시로 발생, 생성되지만 쓸모없다고 여겨왔던 패스워드 오류값들인 정크 데이터의 수집 및 정크 데이터 생성을 유도하고 이를 저장, 분류, 분석하여 가치 데이터를 찾아내고 이를 이용해 해킹이나 불법 노출 사용 등을 사전 예측할 수 있게 된다.

[132] 프로세서(110)는 상기와 같은 패턴으로 입력된 패스워드가 포함된 정크 데이터 중에서 제1 정크 데이터(JD1)와 제2 정크 데이터(JD2)를 제외한 실제 패스워드를 추출하게 되는데, 이를 위해 Finite-state automaton based search, Brute Force Algorithm, Knuth-Morris-Pratt Algorithm, Rabin-Karp string algorithm 등의 문자열 검색 알고리즘이나 패턴 매칭 알고리즘, 패턴 인식 알고리즘 등을 사용할 수 있다(S4).

[133] 만약, 상기와 같이 사용자가 정크 데이터(JD)를 입력하지 않고 실제 패스워드만을 입력한 경우(도 6의 (e), (k), (m)), 상기 패스워드 추출단계(S4)에서 정크 데이터(JD)는 검출되지 않고 패스워드만 검출된다.

[134] 프로세서(110)는 상기 추출된 패스워드가 저장수단(140)에 저장되어 있는 패스워드와 일치하는지의 여부를 확인하여 일치하지 않는 것으로 판명되면, 이는 올바르지 않은 패스워드이므로 에러 처리하고, 그 사실을 표시수단(130)에 표시한다(S5, S6).

[135] 만약, 상기와 같이 사용자가 정크 데이터(JD)를 입력하지 않고 실제 패스워드만을 입력한 경우에도 프로세서(110)는 상기 추출된 패스워드가 저장수단(140)에 저장되어 있는 패스워드와 일치하는지의 여부를 확인하여 일치하지 않는 것으로 판명되면, 이는 올바르지 않은 패스워드이므로 에러 처리하고, 그 사실을 표시수단(130)에 표시한다.

[136] 그러나, 상기 확인 결과 상기 추출된 패스워드가 저장수단(140)에 저장되어 있는 패스워드와 일치하는 것으로 판명되면, 프로세서(110)는 상기 정크 데이터(JD)가 포함된 패스워드가 이전의 인증과정에서 사용자가 입력한 정크 데이터(JD)가 포함된 패스워드로서 저장수단(140)에 저장된 것과 일치하는지 여부를 확인하고, 상기 확인 결과 서로 일치하지 않는 것으로 판명되면 사용자 인증을 성공으로 처리한다(S7, S8).

[137] 이와 같이 현재 입력된 정크 데이터(JD)가 포함된 패스워드가 이전의 인증과정에서 사용자가 입력하여 저장수단(140)에 저장된 정크 데이터(JD)가 포함된 패스워드와 일치하는지의 여부를 확인하는 이유는, 사용자가 이전에 사용한 패스워드가 노출이나 숄더 서핑, 몰래 카메라나 다른 수단에 의해 불법 사용자에게 노출된 경우 그 불법 사용자는 사용자가 입력한 제1 정크 데이터(JD1), 패스워드(PW) 및 제2 정크 데이터(JD2)로 이루어진 정크 데이터가 포함된 패스워드 전체를 하나의 패스워드로 인식하여 '325 2016 11234'를 그대로 입력하기 때문이다(도 6의 (o)). 이를 감안하여 사용자는 제1 정크 데이터(JD1)와

제2 정크 데이터(JD2)를 이루는 랜덤의 숫자(또는 문자, 특수문자, 기호) 중에서 적어도 하나 이상의 숫자나 자릿수가 이전에 입력한 것과 달라야 한다.

[138] 상기 입력된 정크 데이터(JD)가 포함된 패스워드를 과거의 인증과정에서 사용자가 입력하여 메모리(140)에 저장된 정크 데이터(JD)가 포함된 패스워드들과 일치 여부를 판정할 때에, 과거에 입력되었던 모든 정크 데이터(JD)가 포함된 패스워드들과의 일치 여부를 판정해야만 하는 것은 아니며, 바로 직전을 포함하여 미리 정해진 회수만큼 또는 미리 정해진 시간만큼 이전에 입력된 정크 데이터(JD)가 포함된 패스워드와 일치 여부를 비교 판정할 수도 있다.

[139] 따라서, 상기 확인 결과 상기 정크 데이터(JD)가 포함된 패스워드가 저장수단(140)에 저장되어 있는 정크 데이터(JD)가 포함된 패스워드와 각각 일치하는 것으로 판명되면, 프로세서(110는 현재 입력된 패스워드가 불법 사용자에 의해 입력된 것이거나 혹은 사용자의 실수에 의한 입력으로 판단하여, 2차 패스워드 입력을 요청할 수 있다(S9), (도 6 (p)).

[140] 한편, 사용자에 의해 현재 입력된 정크 데이터가 포함된 패스워드의 자릿수가 임계길이 이상이고, 메모리(140)에 저장되어 있는 과거에 사용된 패스워드와 일치하는 자릿수가 임계길이에 해당하는 경우 - 예컨대, 입력된 정크 데이터가 포함된 패스워드가 14자리(도 6 (j))이고, 이 중 일치하는 자릿수가 9자리 이상일 경우, 두 패스워드가 상기와 같이 완전히 똑같이 일치하지 않더라도 과거에 사용되었던 패스워드와 동일한 것으로 판단하여, 현재 입력된 패스워드가 불법 사용자에 의해 입력된 것이거나 혹은 사용자의 실수(우연)에 의한 입력이므로 2차 패스워드 입력을 요청할 수 있다(S9), (도 6 (p)).

[141] 사용자에 의해 현재 입력된 정크 데이터가 포함된 패스워드의 길이가 임계길이 이하로 짧거나(도 6의(b), (i), (l)) 정크 데이터 입력 없이 패스워드만 사용한 경우(도 6의(e), (k), (m)) 안전한 장소에서 사용된 것이고, 정크 데이터가 포함된 패스워드의 입력된 자릿수가 임계길이 이상으로 긴 경우, 주위가 불안한 상태에서 입력되었다는 것으로 판단하는 것이다.

[142] 한편, 이 중 9자리가 예전에 입력되었던 패스워드와 동일하다는 것은 앞서 제시한 밀러의 논문에 의하면 9자리 수는 사람이 외울 수 있는 범위를 넘어가는 자릿수이기 때문에, 이 정도 길이의 수가 일치한다면 해킹으로 판단할 수 있다.

[143] 좀 더 상세히 예를 들어 설명하자면, 현재 사용자가 입력한 패스워드가 제1 정크 데이터(JD1)와 패스워드(PW)와 제2 정크 데이터((JD2)의 조합으로 이루어진 '325 2016 11238'이고, 메모리(140)에 저장되어 있는 과거에 사용된 패스워드가 '325 2016 11234'일 경우(도 6의 (h)), 현재 입력된 패스워드는 과거에 사용된 패스워드와 11자리 수가 동일하고 1자리 수가 다르지만 과거와 동일한 패스워드를 입력했다고 판단하여 해킹 등으로 예측하여 인증을 거부한다. 왜냐하면, 몰래카메라 등으로 패스워드를 촬영한 후 전체 패스워드를 동일하게 그대로 사용할 수도 있지만(도 6의 (o)), 의도적으로 전체 패스워드 중 일부를

변경하거나 누락하여 사용할 수도 있기 때문이다.

[144] 이 경우를 자세히 살펴보면, 1자리를 제외한 11자리 수인 '32520161123'이나 2자리를 제외한 10자리 수 '3252016112'를 인간의 머리로는 암기하여 재현할 수 없기 때문에 이 긴 숫자의 조합이 과거에 사용된 것과 동일하다면, 해킹이 아니고서는 기억해서 사용할 수 있는 숫자의 조합이 아닌 것이다.

[145] 같은 관점에서, 사용자가 15자리 수의 정크 데이터가 포함된 패스워드를 입력할 경우, 입력한 패스워드 15자리 수가 과거의 패스워드와 모두 일치하거나, 15자리 수 중 1자리가 다르고 14자리 수가 일치하거나, 2자리가 다르고 13자리 수가 일치하거나....15자리 수 중 6자리가 다르고 9자리 수가 일치하는 패스워드라면 각각 모두 해킹으로 판단하여 2차 패스워드 입력을 요청한다(S9).

[146] 반드시 연속적으로 일치하지 않더라도 도합하여 9자리 이상이 순차 일치하는 경우에도 해킹으로 판단하여 2차 패스워드 입력을 요청할 수 있다(S9).

[147] 상기 2차 패스워드란 상기 제1 정크 데이터(JD1) 및 패스워드(PW), 제2 정크 데이터(JD2) 중에서 정크 데이터를 모두 제외한 패스워드(PW)만을 의미하는 것으로, 사용자는 이 사실을 인지하고 실제 패스워드인 4자리의 숫자 '2016'을 입력할 것이다. 이에 반하여, 불법 사용자인 경우 패스워드가 포함되어 있는 정크 데이터의 전체 숫자는 알고 있지만 그 안에 들어있는 실제 패스워드만을 알 수는 없으므로 제1 정크 데이터(JD1) 및 패스워드(PW), 제2 정크 데이터(JD2)를 포함하는 12자리의 숫자를 입력할 것이다. 아니면, 이 전체 12자리 숫자들 중에서 패스워드 키값을 임의로 선택하여 입력할 수밖에 없게 된다.

[148] 프로세서(110)는 이때 입력된 2차 패스워드를 메모리(140)에 저장되어 있는 패스워드와 비교하여 일치하는 것으로 판명되면 사용자 인증에 대해 성공으로 처리하고, 일치하지 않는 것으로 판단되면 에러 처리한다(S10-S12).

[149] 이때, 입력된 2차 패스워드가 저장수단(140)에 저장되어 있는 패스워드와 일치하지 않는 경우, 상기 프로세서(110)는 패스워드가 불법 유출된 것으로 판단하여 표시수단(130)을 통해 사용자에게 패스워드 변경을 요청할 수 있어, 불법 해킹에 대한 사전 예측 및 고지가 가능하여 예방과 보안을 강화할 수 있게 된다.

[150] 단, 상기와 같이 입력된 2차 패스워드가 저장수단(140)에 저장되어 있는 패스워드와 일치하지 않는 경우, 해킹일 수도 있지만 혹은 사용자의 실수에 의한 것일 수도 있으므로, 미리 설정된 횟수(예: 3회)에 걸쳐 2차 패스워드 입력을 요청하여 계속해서 입력된 2차 패스워드가 저장수단(140)에 저장되어 있는 패스워드와 일치하지 않는 경우, 상기 프로세서(110)는 바로 이전에 입력된 패스워드가 불법 유출(해킹)에 의한 패스워드로 판단하여 에러 처리함과 아울러 표시수단(130)을 통해 사용자에게 불법 유출의 가능성을 알리고 패스워드 변경을 요청하는 것이 바람직하다.

발명의 실시를 위한 형태

[151] 본 발명의 일 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[152] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속한다.

[153]

청구범위

[청구항 1] 사용자 인증 시스템에 의한 사용자 인증 방법에 있어서,
(a) 사용자로부터 정크 데이터가 포함된 패스워드 - 이때, 정크 데이터는 패스워드의 이전, 이후 또는 이전 및 이후에 포함됨 - 를 입력받는 단계;
(b) 입력받은 정크 데이터가 포함된 패스워드로부터 정크 데이터를 제외한 패스워드를 분리 추출하는 단계;
(c) 상기 정크 데이터가 포함된 패스워드가 과거 입력되어 기 저장된 정크 데이터가 포함된 패스워드와 임계길이만큼 일치하는 경우, 상기 분리 추출된 패스워드가 기 저장된 패스워드와 일치함에도 불구하고 사용자 인증을 실패로 처리하는 단계;를 포함하는 것을 특징으로 하는 정크 데이터 일치여부를 이용한 사용자 인증 방법.

[청구항 2] 제1항에 있어서,
상기 (c)단계에서, 상기 사용자로부터 입력받은 정크 데이터가 포함된 패스워드의 길이가 임계길이 이상인 경우, 상기 정크 데이터가 포함된 패스워드와 과거 입력되어 기 저장된 정크 데이터가 포함된 패스워드의 일치 여부를 비교하되,
상기 사용자로부터 입력받은 정크 데이터가 포함된 패스워드의 길이가 임계길이 미만인 경우, 상기 정크 데이터가 포함된 패스워드와 과거 입력되어 기 저장된 정크 데이터가 포함된 패스워드의 일치 여부의 비교를 생략하고, 상기 분리 추출된 패스워드가 저장수단에 기 저장된 패스워드가 일치하면 사용자 인증을 성공으로 처리하는 것을 특징으로 하는 정크 데이터 일치여부를 이용한 사용자 인증 방법.

[청구항 3] 제1항에 있어서,
상기 (c)단계에서, 상기 임계길이는 9자리 또는 그보다 더 긴 길이이며,
상기 정크 데이터가 포함된 패스워드와 과거 입력되어 기 저장된 정크 데이터가 포함된 패스워드의 일치 여부를 비교하되, 연속적 또는 불연속적으로 임계길이만큼 일치하는 경우,
상기 패스워드가 저장수단에 기 저장된 패스워드가 일치함에도 불구하고 사용자 인증을 실패로 처리하는 것을 특징으로 하는 정크 데이터 일치여부를 이용한 사용자 인증 방법.

[청구항 4] 제1항에 있어서,
상기 패스워드가 포함된 정크 데이터 패턴은,
복수 개의 자릿수로 이루어진 정크 데이터 및 4개 이상의 자릿수로 이루어진 패스워드를 포함하는 패턴;
복수 개의 자릿수로 이루어진 제1 정크 데이터, 4개 이상의 자릿수로 이루어진 패스워드 및 복수 개의 자릿수로 이루어진 제2 정크 데이터를 포함하는 패턴; 및

3개 이상의 자릿수로 이루어진 제1 패스워드, 복수 개의 자릿수로 이루어진 정크 데이터 및 3개 이상의 자릿수로 이루어진 제2 패스워드를 포함하는 패턴;

가운데 어느 하나의 패턴을 포함하는 것을 특징으로 하는 정크 데이터 일치여부를 이용한 사용자 인증 방법.

[청구항 5] 제1항에 있어서,

상기 (b) 단계에서, 문자열 검색 알고리즘, 패턴 매칭 알고리즘 및 패턴 인식 알고리즘 가운데 어느 하나를 이용하는 것을 특징으로 하는 정크 데이터 일치여부를 이용한 사용자 인증 방법.

[청구항 6] 제1항에 있어서,

상기 (c) 단계 이후,

(d) 정크 데이터를 제외한 패스워드만을 입력하라는 메시지를 표시하는 단계; 및

(e) 사용자로부터 재차 패스워드가 입력되면 저장수단에 기 저장된 패스워드와 일치여부를 판정하여, 일치하는 경우 사용자 인증을 성공으로 처리하는 단계;를 더 포함하는 것을 특징으로 하는 정크 데이터 일치여부를 이용한 사용자 인증 방법.

[청구항 7] 제6항에 있어서,

상기 (e) 단계에서, 사용자로부터 재차 입력된 패스워드가 저장수단에 기 저장된 패스워드와 일치하지 않는 경우, 해킹위험 경고처리를 수행하는 것을 특징으로 하는 정크 데이터 일치여부를 이용한 사용자 인증 방법.

[청구항 8] 사용자로부터 패스워드 및 정크 데이터를 입력받는 입력수단;

프로세서가 실행할 명령어를 적재하는 저장수단;

상기 저장수단에 적재된 명령어를 순차 실행하는 프로세서;를 구비하되,

상기 프로세서는 상기 입력수단을 통해 사용자로부터 정크 데이터가 포함된 패스워드 - 이때, 정크 데이터는 패스워드의 이전, 이후 또는 이전 및 이후에 포함됨 - 를 입력받으면, 입력받은 패스워드로부터 정크 데이터를 제외한 패스워드를 분리 추출하고, 상기 정크 데이터가 포함된 패스워드와 과거 입력되어 기 저장된 정크 데이터가 포함된 패스워드가 임계길이만큼 일치하는 경우, 상기 분리 추출된 패스워드가 저장수단에 기 저장된 패스워드와 일치함에도 불구하고 사용자 인증을 실패로 처리하는 것을 특징으로 하는 정크 데이터 일치여부를 이용한 사용자 인증 시스템.

[청구항 9] 네트워크를 통해 데이터를 송수신하는 통신 어댑터;

프로세서가 실행할 명령어를 적재하는 저장수단;

상기 저장수단에 적재된 명령어를 순차 실행하는 프로세서;를 구비하되,

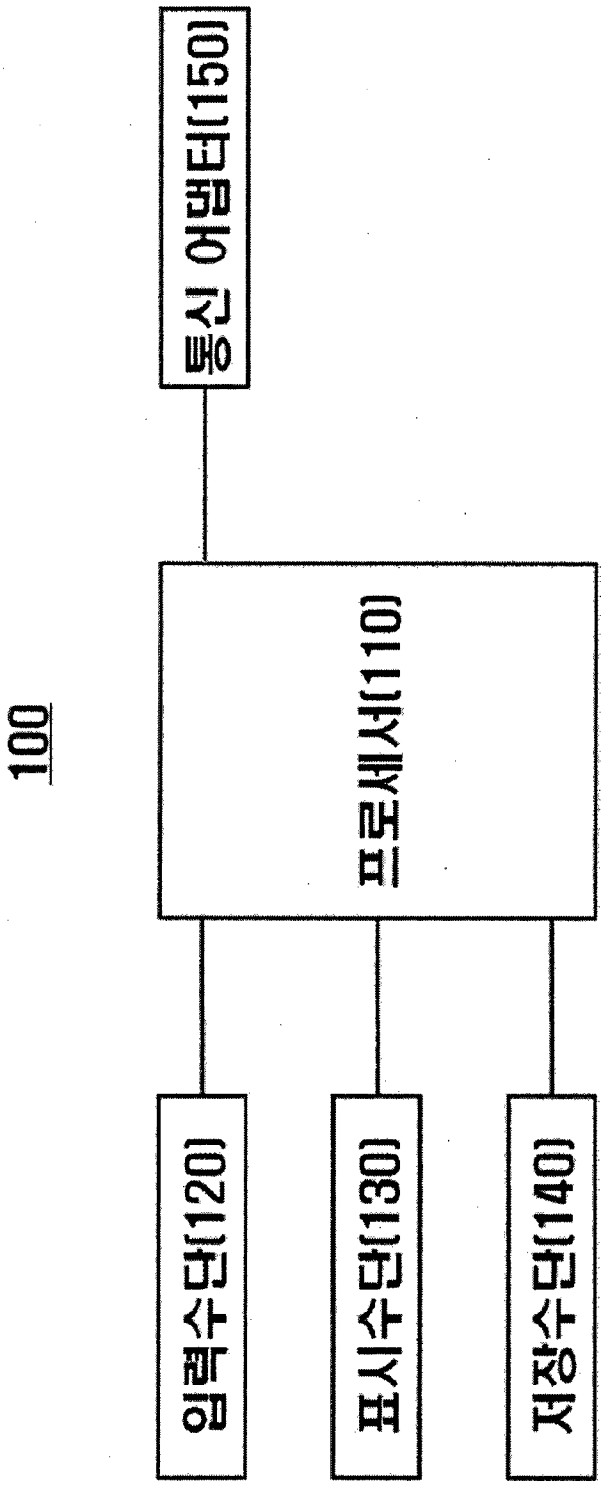
상기 통신 어댑터는 네트워크를 통해 연결된 원격 단말로부터 정크 데이터가 포함된 패스워드 - 이때, 정크 데이터는 패스워드의 이전, 이후

또는 이전 및 이후에 포함됨 - 를 입력받으며,
상기 프로세서는 입력받은 패스워드로부터 정크 데이터를 제외한 패스워드를 분리하고, 상기 정크 데이터가 포함된 패스워드와 과거 입력되어 기 저장된 정크 데이터가 포함된 패스워드가 임계길이만큼 일치하는 경우, 상기 패스워드가 저장수단에 기 저장된 패스워드가 일치함에도 불구하고 사용자 인증을 실패로 처리하는 것을 특징으로 하는 정크 데이터 일치여부를 이용한 사용자 인증 시스템.

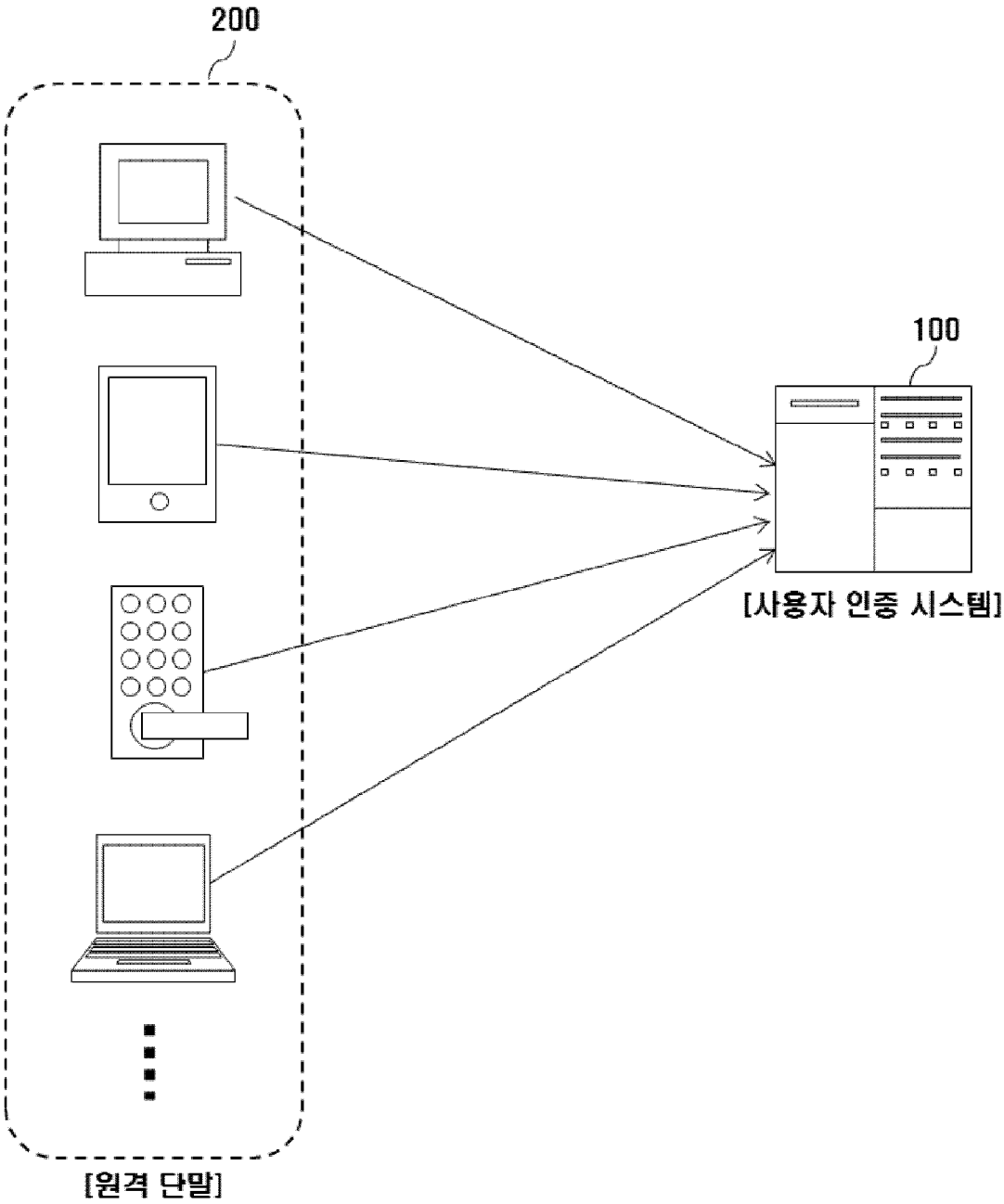
[청구항 10] 제8항 및 제9항 가운데 어느 한 항에 있어서,
상기 프로세서는 상기 입력받은 정크 데이터가 포함된 패스워드의 길이가 임계길이 이상인 경우, 상기 정크 데이터가 포함된 패스워드와 과거 입력되어 기 저장된 정크 데이터가 포함된 패스워드의 일치 여부를 비교하되,
상기 사용자로부터 입력받은 정크 데이터가 포함된 패스워드의 길이가 임계길이 미만인 경우, 상기 정크 데이터가 포함된 패스워드와 과거 입력되어 기 저장된 정크 데이터가 포함된 패스워드의 일치 여부의 비교를 생략하고,
상기 분리 추출된 패스워드가 저장수단에 기 저장된 패스워드와 일치하면 사용자 인증을 성공으로 처리하는 것을 특징으로 하는 정크 데이터 일치여부를 이용한 사용자 인증 시스템.

[청구항 11] 제10항에 있어서,
상기 프로세서는, 상기 정크 데이터가 포함된 패스워드와 과거 입력되어 기 저장된 정크 데이터가 포함된 패스워드의 일치 여부를 비교하며,
연속적 또는 불연속적으로 임계길이만큼 일치하면 상기 분리 추출된 패스워드가 저장수단에 기 저장된 패스워드가 일치함에도 불구하고 사용자 인증을 실패로 처리하되,
상기 임계길이는 9자리 또는 그보다 더 긴 길이인 것을 특징으로 하는 정크 데이터 일치여부를 이용한 사용자 인증 시스템.

[도1]

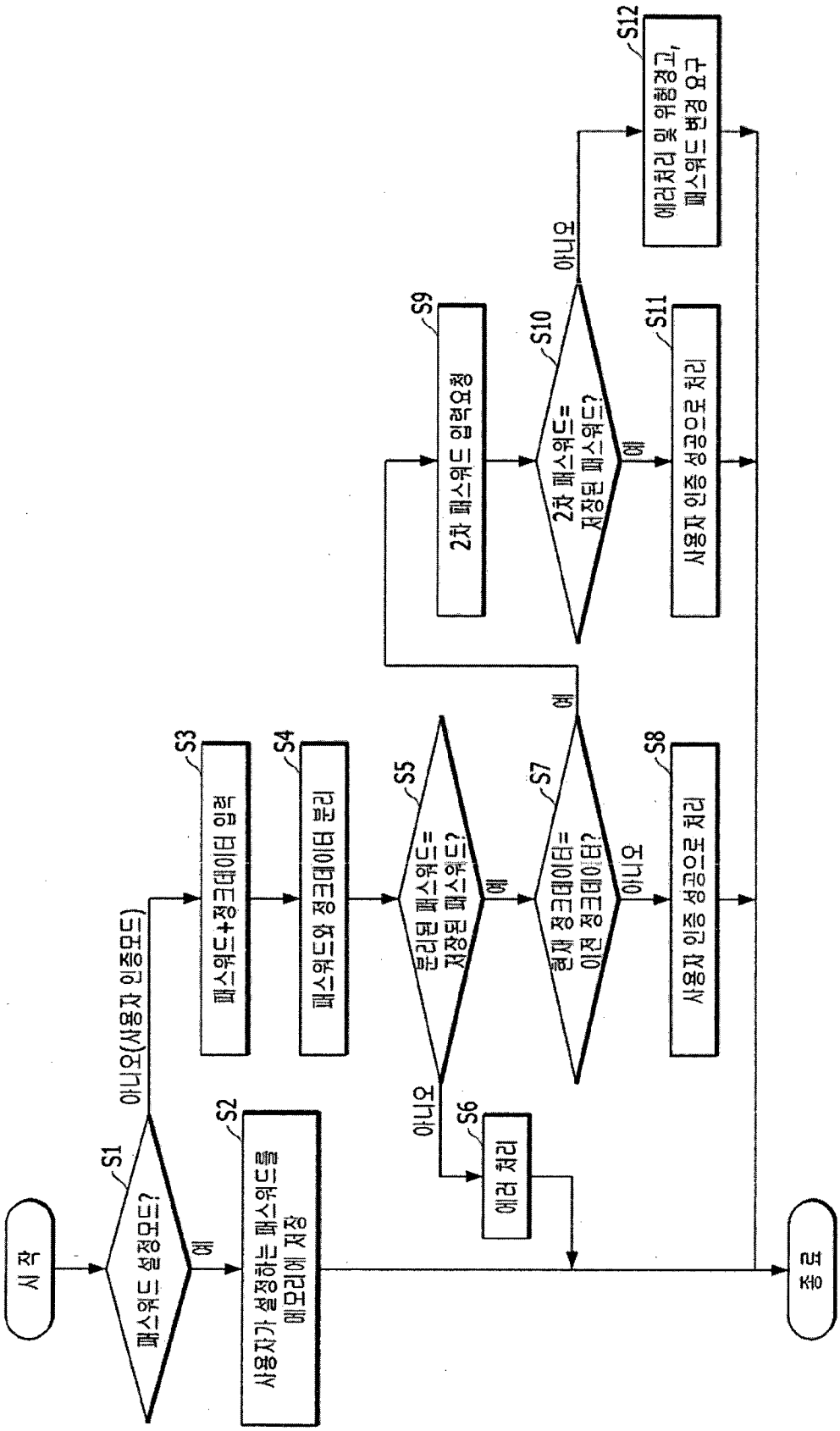


[도2]

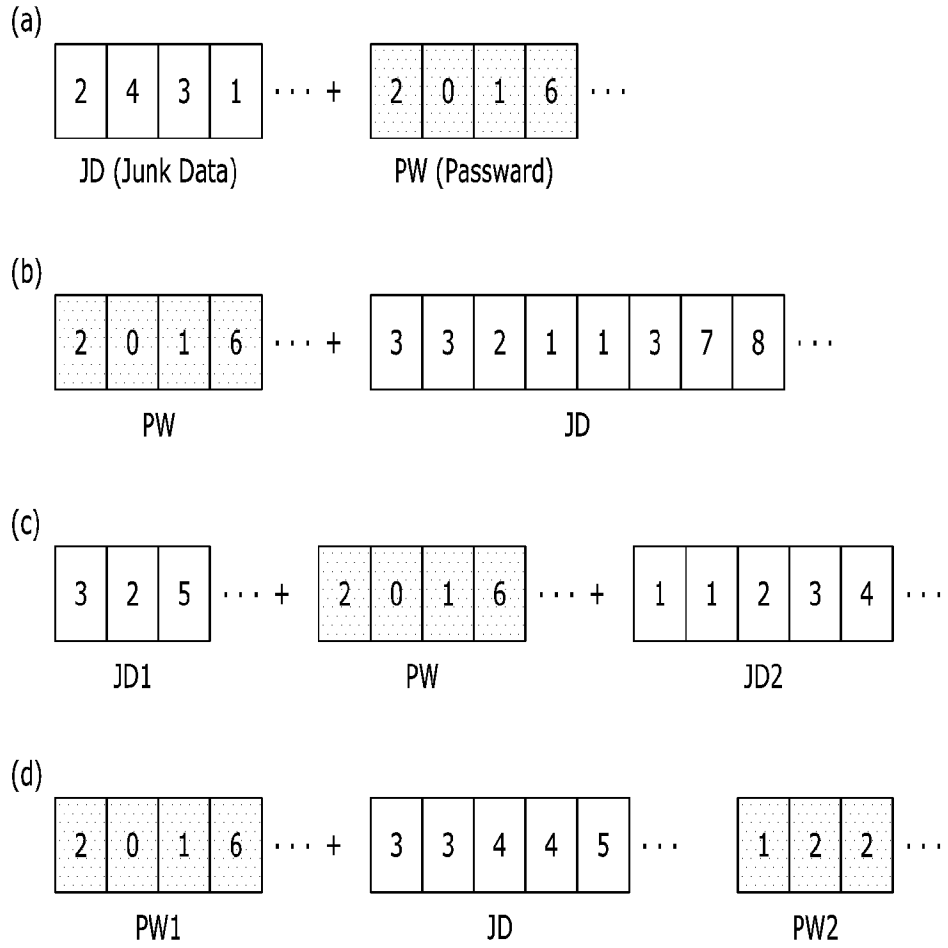


[도3]

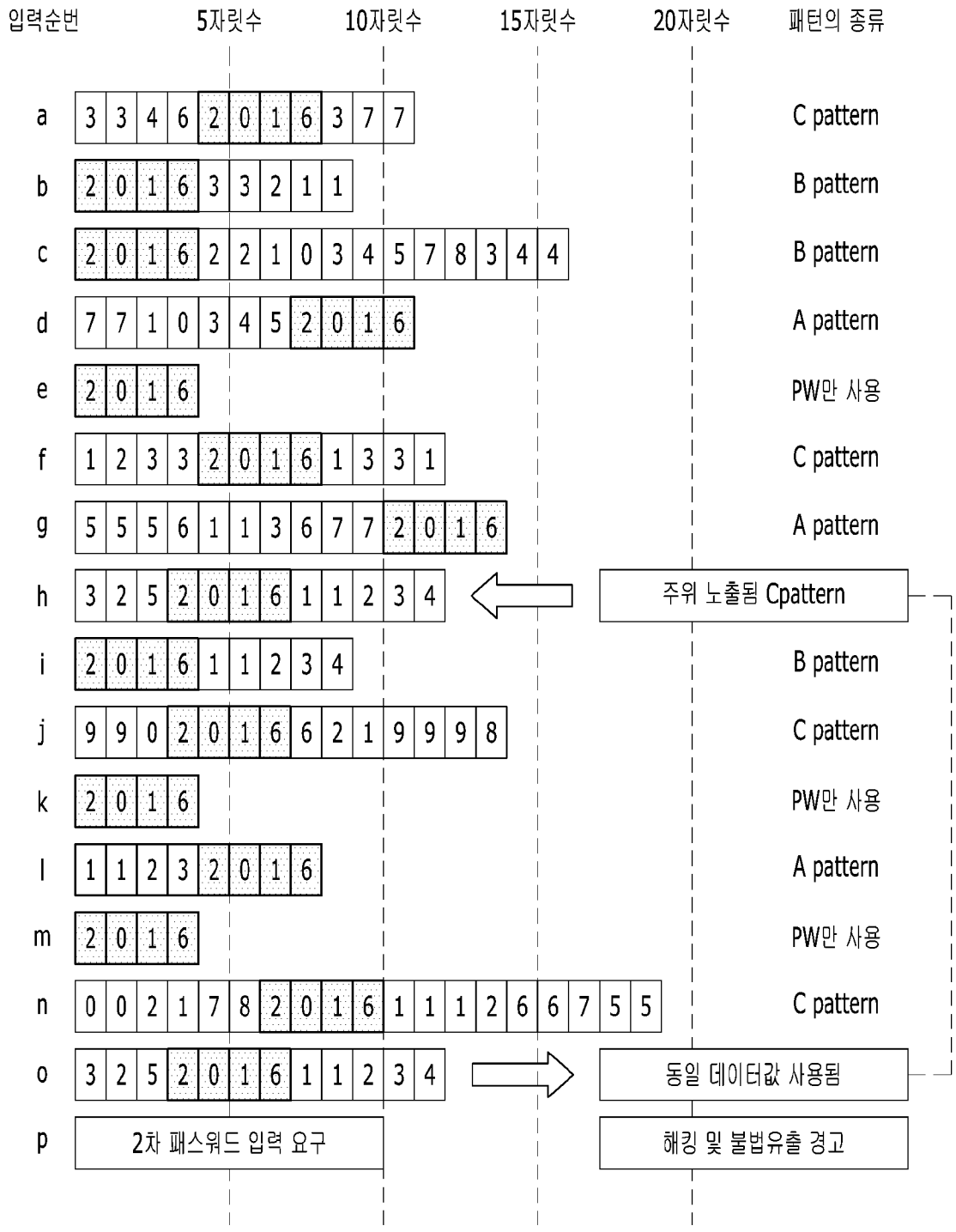
[도4]


시작
S1
패스워드 설정모드?
예
아니오(사용자 인증모드)
S2
사용자가 설정하는 패스워드를 메모리에 저장
S3
패스워드+정크데이터 입력
S4
패스워드와 정크데이터 분리
S5
분리된 패스워드= 저장된 패스워드?
예
아니오
S6
에러 처리
S7
현재 정크데이터= 이전 정크데이터?
아니오
예
S8
사용자 인증 성공으로 처리
S9
2차 패스워드 입력요청
S10
2차 패스워드= 저장된 패스워드?
예
아니오
S11
사용자 인증 성공으로 처리
S12
에러처리 및 위험경고, 패스워드 변경 요구
종료

[도5]


(a)
2 4 3 1 · · · + 2 0 1 6 · · ·
JD (Junk Data)
PW (Passward)
(b)
2 0 1 6 · · · + 3 3 2 1 1 3 7 8 · · ·
PW
JD
(c)
3 2 5 · · · + 2 0 1 6 · · · + 1 1 2 3 4 · · ·
JD1
PW
JD2
(d)
2 0 1 6 · · · + 3 3 4 4 5 · · · 1 2 2 · · ·
PW1
JD
PW2

[도6]


입력순번
5자릿수
10자릿수
15자릿수
20자릿수
패턴의 종류
a 3 3 4 6 2 0 1 6 3 7 7 C pattern
b 2 0 1 6 3 3 2 1 1 B pattern
c 2 0 1 6 2 2 1 0 3 4 5 7 8 3 4 4 B pattern
d 7 7 1 0 3 4 5 2 0 1 6 A pattern
e 2 0 1 6 PW만 사용
f 1 2 3 3 2 0 1 6 1 3 3 1 C pattern
g 5 5 5 6 1 1 3 6 7 7 2 0 1 6 A pattern
h 3 2 5 2 0 1 6 1 1 2 3 4
주위 노출됨 Cpattern
i 2 0 1 6 1 1 2 3 4 B pattern
j 9 9 0 2 0 1 6 6 2 1 9 9 9 8 C pattern
k 2 0 1 6 PW만 사용
l 1 1 2 3 2 0 1 6 A pattern
m 2 0 1 6 PW만 사용
n 0 0 2 1 7 8 2 0 1 6 1 1 1 2 6 6 7 5 5 C pattern
o 3 2 5 2 0 1 6 1 1 2 3 4
동일 데이터값 사용됨
p
2차 패스워드 입력 요구
해킹 및 불법유출 경고

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2017/001547

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/46(2013.01)i, G06F 21/31(2013.01)i, H04L 9/32(2006.01)i, G06Q 20/40(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/46; G06F 21/20; H04L 9/32; H04W 48/02; H04W 12/06; G06F 21/31; H04B 1/40; G06Q 20/40

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: identification, junk data, password, threshold length, failure

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2011-113523 A (KYOCERA MITA CORP.) 09 June 2011 See paragraphs [0010], [0015]-[0023]; claim 1; and figures 1-3.	1-11
A	KR 10-2015-0113366 A (SHIN, Won-Kug) 08 October 2015 See paragraphs [0058]-[0075]; and figures 3-4.	1-11
A	KR 10-2011-0051174 A (KT CORPORATION) 17 May 2011 See paragraphs [0042]-[0084]; and figures 2-4.	1-11
A	KR 10-2012-0010602 A (KOREA MOBILE CERTIFICATION INC.) 06 February 2012 See paragraphs [0018]-[0042]; and figures 1-2.	1-11
A	US 2015-0205942 A1 (ROWEM INC.) 23 July 2015 See paragraphs [0031]-[0059]; and figures 1-3.	1-11

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 MAY 2017 (16.05.2017)	**16 MAY 2017 (16.05.2017)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea	
Facsimile No. +82-42-481-8578	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2017/001547

Patent document cited in search report	Publication date	Patent family member	Publication date
JP 2011-113523 A	09/06/2011	NONE	
KR 10-2015-0113366 A	08/10/2015	KR 10-1669770 B1	27/10/2016
KR 10-2011-0051174 A	17/05/2011	CA 2755142 A1	16/09/2010
		CA 2755142 C	12/04/2016
		KR 10-2010-0102026 A	20/09/2010
		US 2012-0005727 A1	05/01/2012
		WO 2010-104283 A2	16/09/2010
		WO 2010-104283 A3	16/12/2010
KR 10-2012-0010602 A	06/02/2012	KR 10-1122655 B1	09/03/2012
US 2015-0205942 A1	23/07/2015	CN 104620249 A	13/05/2015
		KR 10-1416540 B1	09/07/2014
		KR 10-2014-0009038 A	22/01/2014
		WO 2014-011001 A1	16/01/2014

국 제 조 사 보 고 서

국제출원번호
PCT/KR2017/001547

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/46(2013.01)i, G06F 21/31(2013.01)i, H04L 9/32(2006.01)i, G06Q 20/40(2012.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/46; G06F 21/20; H04L 9/32; H04W 48/02; H04W 12/06; G06F 21/31; H04B 1/40; G06Q 20/40

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 인증, 정크 데이터, 패스워드, 임계길이, 실패

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	JP 2011-113523 A (KYOCERA MITA CORP.) 2011.06.09 단락 [0010], [0015]-[0023]; 청구항 1; 및 도면 1-3 참조.	1-11
A	KR 10-2015-0113366 A (신원국) 2015.10.08 단락 [0058]-[0075]; 및 도면 3-4 참조.	1-11
A	KR 10-2011-0051174 A (주식회사 케이티) 2011.05.17 단락 [0042]-[0084]; 및 도면 2-4 참조.	1-11
A	KR 10-2012-0010602 A (한국모바일인증 주식회사) 2012.02.06 단락 [0018]-[0042]; 및 도면 1-2 참조.	1-11
A	US 2015-0205942 A1 (ROWEM INC.) 2015.07.23 단락 [0031]-[0059]; 및 도면 1-3 참조.	1-11

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2017년 05월 16일 (16.05.2017)	2017년 05월 16일 (16.05.2017)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
진상범
전화번호 +82-42-481-8398

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2017/001547

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
JP 2011-113523 A	2011/06/09	없음	
KR 10-2015-0113366 A	2015/10/08	KR 10-1669770 B1	2016/10/27
KR 10-2011-0051174 A	2011/05/17	CA 2755142 A1	2010/09/16
		CA 2755142 C	2016/04/12
		KR 10-2010-0102026 A	2010/09/20
		US 2012-0005727 A1	2012/01/05
		WO 2010-104283 A2	2010/09/16
		WO 2010-104283 A3	2010/12/16
KR 10-2012-0010602 A	2012/02/06	KR 10-1122655 B1	2012/03/09
US 2015-0205942 A1	2015/07/23	CN 104620249 A	2015/05/13
		KR 10-1416540 B1	2014/07/09
		KR 10-2014-0009038 A	2014/01/22
		WO 2014-011001 A1	2014/01/16