

명세서

발명의 명칭: 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법

기술분야

- [1] 본 발명은 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법에 관한 것으로, 보다 상세하게는 매회 변경하여 생성되는 난수데이터를 이용하여 보안 키패드를 통해 입력되는 입력문자에 대한 보안을 강화하는 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법에 관한 것이다.

[2]

배경기술

- [3] 현대 정보화 사회에서는 개인용 컴퓨터, 스마트폰, 태블릿 컴퓨터, 금융자동화 단말기 등 다양한 정보기기들이 존재한다. 이러한 대부분의 정보기기들은 사용자로부터 정보를 입력받기 위한 입력수단을 구비하는데, 최근 입력수단으로서 가상 키패드의 사용이 증가하고 있는 추세이다. 대표적으로, 컴퓨터 또는 스마트폰을 이용한 온라인 뱅킹에서 가상 키패드를 스크린에 표시하고, 마우스 또는 터치스크린을 이용해 계좌비밀번호 또는 보안카드번호 등의 개인 정보를 입력할 수 있게 하고 있다.
- [4] 한편, 최근 지능적이고 지속적으로 위협적인 공격을 하는 악성코드들이 발견되는 등 더욱 정교하고 진화된 보안 위협요소들이 증가하고 있다. 특히, 사용자가 패스워드 입력 시 키보드 입력정보를 요구하는 인터넷 뱅킹 등 금융관련 서비스를 사용할 때, 입력정보를 사용자 몰래 저장 및 유출하는 키로거 공격도 빈번히 발생하고 있다. 그 결과 이를 방지하기 위해 보안이 강화된 가상 키패드에 대한 연구가 활발히 진행되고 있다.
- [5] 이와 같은 가상 키패드와 관련하여, 등록특허 제10-1595794호(발명의 명칭: 보안 기능이 강화된 가상 키패드 생성 장치)가 개시된 바 있다.
- [6] 하지만, 위와 같은 종류의 가상 키패드는 다수의 문자들이 고정적인 위치에 배열되기 때문에 제3자가 사용자의 터치 위치를 엿보거나 해킹하여 사용자가 입력한 정보를 알아낼 수 있었다. 또한, 가상 키패드를 사용할 경우에도 전송되는 터치 좌표 정보를 획득하거나 스마트폰 내에서 터치 이벤트를 로깅할 수도 있으며, 메모리 자체를 해킹할 경우에 입력된 패스워드 등의 개인정보가 유출될 수 있다는 한계가 있었다.

[7]

발명의 상세한 설명

기술적 과제

- [8] 상기와 같은 문제를 해결하기 위한 본 발명의 목적은 매회마다 변경되어 크기가 랜덤하게 생성되는 난수데이터를 이용하여 생성되는 최종 난수데이터로부터

평균 데이터를 추출함에 따라 정형화된 비밀키를 생성하여 관리하는 종래기술보다 보안성을 향상시킬 수 있는 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법을 제공하는 것이다.

[9]

[10] 본 발명이 이루고자 하는 기술적 과제는 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

[11]

과제 해결 수단

[12] 상기와 같은 목적을 달성하기 위한 본 발명의 구성은 (a) 메인 서버가 서버 난수데이터를 랜덤하게 생성하는 단계; (b) 클라이언트가 상기 서버 난수데이터를 이용하여 생성되는 난수데이터로부터 보안 키패드를 통해 입력되는 각각의 입력 문자에 해당하는 클라이언트 난수데이터를 생성하는 단계; 및 (c) 상기 메인 서버가 상기 클라이언트 난수데이터를 이용하여 최종 난수데이터 및 최종 난수데이터를 생성한 후 상기 최종 난수데이터로부터 평균 데이터를 추출하여 생성하는 단계;를 포함하는 것을 특징으로 하는 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법을 제공한다.

[13] 본 발명의 실시예에 있어서, 상기 (a) 단계는, (a1) 상기 메인 서버가 보안 랜덤값인 원타임아이디(OTID: One Time ID)를 생성하는 단계; (a2) 상기 메인 서버가 솔트값(salt value)을 리딩하는 단계; (a3) 상기 메인 서버가 상기 보안 랜덤값과 상기 솔트값을 이용하여 상기 서버 난수데이터의 생성을 위한 기본 해시값(Base HASH value)을 생성하는 단계; (a4) 상기 메인 서버가 상기 보안 키패드에서 사용되는 1개의 문자에 매칭될 랜덤 범위 값(R)을 생성하는 단계; 및 (a5) 상기 메인 서버가 해시함수에 상기 기본 해시값을 적용하여 n차 해시값(HASH value)을 생성하는 단계;를 포함하는 것을 특징으로 할 수 있다.

[14] 본 발명의 실시예에 있어서, 상기 (a) 단계는, (a6) 상기 메인 서버가 상기 n차 해시값을 저장하는 단계; 및 (a7) 상기 메인 서버가 상기 서버 난수데이터의 생성이 완료되었는지를 판단하는 단계;를 더 포함하고, 상기 (a7) 단계는, 상기 서버 난수데이터의 생성이 미완료된 경우, (a71) 상기 메인 서버가 상기 해시함수에 상기 n차 해시값을 적용하여 (n+1)차 해시값을 생성하는 단계; 및 (a72) 상기 (a6) 단계로 복귀하는 단계;를 포함하며, 상기 (a72) 단계 이후, 상기 (a6) 단계에서는 상기 메인 서버가 상기 (n+1)차 해시값을 저장하는 것을 특징으로 할 수 있다.

[15] 본 발명의 실시예에 있어서, 상기 (a) 단계는, (a8) 상기 서버 난수데이터의 생성이 완료되는 단계; (a9) 상기 메인 서버가 상기 클라이언트로 상기 서버 난수데이터를 전송하는 단계; 및 (a10) 상기 메인 서버가 상기 서버 난수데이터를 삭제하는 단계;를 포함하는 것을 특징으로 할 수 있다.

- [16] 본 발명의 실시예에 있어서, 상기 (b) 단계는, (b1) 상기 클라이언트가 상기 메인 서버로부터 전송되는 상기 서버 난수데이터를 수신한 후 상기 서버 난수데이터가 기설정된 형식에 맞는지 검증하는 단계; (b2) 상기 클라이언트가 상기 서버 난수데이터와 상기 입력문자를 매칭시키기 위한 난수데이터를 생성하는 단계; (b3) 사용자에게 의한 상기 보안 키패드를 통해 상기 각각의 입력문자가 입력되는 단계; (b4) 상기 클라이언트가 상기 난수데이터에서 상기 각각의 입력문자에 해당하는 클라이언트 난수데이터를 리딩하여 저장하는 단계; 및 (b5) 상기 클라이언트가 상기 각각의 입력문자의 입력이 완료되었는지 판단하는 단계;를 포함하고, 상기 (b5) 단계는, 상기 각각의 입력문자의 입력이 미완료된 경우, (b51) 상기 (b3) 단계로 복귀하는 단계를 포함하는 것을 특징으로 할 수 있다.
- [17] 본 발명의 실시예에 있어서, 상기 (b) 단계는, (b6) 상기 클라이언트 난수데이터의 생성이 완료되는 단계; 및 (b7) 상기 클라이언트가 상기 메인 서버로 상기 클라이언트 난수데이터를 전송하는 단계;를 더 포함하는 것을 특징으로 할 수 있다.
- [18] 본 발명의 실시예에 있어서, 상기 (c) 단계는, (c1) 상기 메인 서버가 상기 클라이언트로부터 전송되는 상기 클라이언트 난수데이터를 수신한 후 상기 클라이언트 난수데이터의 변조 여부를 검증하는 단계; (c2) 상기 메인 서버가 상기 클라이언트 난수데이터를 이용하여 상기 최종 난수데이터를 생성하는 단계; (c3) 상기 메인 서버가 상기 최종 난수데이터를 이용하여 상기 최종 난수데이터를 생성하는 단계; (c4) 상기 메인 서버가 상기 최종 난수데이터를 통한 상기 평문데이터를 추출하는 단계; 및 (c5) 상기 메인 서버가 상기 평문데이터의 추출이 완료되었는지 판단하는 단계;를 포함하고, 상기 (c5) 단계는, 상기 평문데이터의 추출이 미완료된 경우, (c51) 상기 (c4) 단계로 복귀하는 단계;를 포함하는 것을 특징으로 할 수 있다.
- [19] 본 발명의 실시예에 있어서, 상기 (c) 단계는, (c6) 상기 평문데이터의 생성이 완료되는 단계;를 더 포함하는 것을 특징으로 할 수 있다.
- [20] 본 발명의 실시예에 있어서, 상기 (c2) 단계는, (c21) 상기 메인 서버가 최종 보안 랜덤값인 최종 원타임아이디(OTID: One Time ID)를 상기 클라이언트 난수데이터에서 추출하여 생성하는 단계; (c22) 상기 메인 서버가 상기 솔트값(salt value)을 리딩하는 단계; (c23) 상기 메인 서버가 상기 최종 보안 랜덤값과 상기 솔트값을 이용하여 상기 최종 난수데이터의 생성을 위한 최종 기본 해시값(Base HASH value)를 생성하는 단계; (c24) 상기 메인 서버가 상기 보안 키패드에서 사용되는 1개의 문자에 매칭될 최종 랜덤 범위 값(R)을 생성하는 단계; (c25) 상기 메인 서버가 해시함수에 상기 최종 기본 해시값을 적용하여 n차 최종 해시값(Final HASH value)을 생성하는 단계; (c26) 상기 메인 서버가 상기 n차 최종 해시값을 저장하는 단계; 및 (c27) 상기 메인 서버가 상기 최종 난수데이터의 생성이 완료되었는지를 판단하는 단계;를 포함하는 것을 특징으로 할 수 있다.
- [21] 본 발명의 실시예에 있어서, 상기 (c27) 단계는, 상기 최종 난수데이터의 생성이 미완료된 경우, (c271) 상기 메인 서버가 상기 해시함수에 상기 최종 해시값을 적

용하여 (n+1)차 최종 해시값을 생성하는 단계; 및 (c272) 상기 (c26) 단계로 복귀하는 단계;를 포함하며, 상기 (c272) 단계 이후, 상기 (c26) 단계에서는 상기 메인 서버가 상기 (n+1)차 최종 해시값을 저장하는 것을 특징으로 할 수 있다.

[22]

발명의 효과

[23] 상기와 같은 구성에 따르는 본 발명의 효과는, 매회마다 크기가 변경되어 랜덤하게 생성되는 난수데이터를 이용하여 생성되는 최종 난수데이터로부터 평균 데이터를 추출함에 따라 노출 시에도 해킹될 위험성이 없어 정형화된 비밀키를 생성하여 관리하는 종래기술보다 보안을 강화시킬 수 있다.

[24]

[25] 본 발명의 효과는 상기한 효과로 한정되는 것은 아니며, 본 발명의 상세한 설명 또는 특허청구범위에 기재된 발명의 구성으로부터 추론 가능한 모든 효과를 포함하는 것으로 이해되어야 한다.

[26]

도면의 간단한 설명

[27] 도 1은 본 발명의 일실시예에 따른 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법을 나타낸 순서도이다.

[28] 도 2는 본 발명의 일실시예에 따른 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법의 세부단계(S100)를 구체화한 순서도이다.

[29] 도 3은 본 발명의 일실시예에 따른 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법의 세부단계(S200)를 구체화한 순서도이다.

[30] 도 4는 본 발명의 일실시예에 따른 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법의 세부단계(S300)를 구체화한 순서도이다.

[31]

발명의 실시를 위한 형태

[32] 이하에서는 첨부한 도면을 참조하여 본 발명을 설명하기로 한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 따라서 여기에서 설명하는 실시예로 한정되는 것은 아니다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[33] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결(접속, 접촉, 결합)"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 부재를 사이에 두고 "간접적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 구비할 수 있다는 것을 의미한다.

- [34] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [35] 이하 첨부된 도면을 참고하여 본 발명의 실시예를 상세히 설명하기로 한다.
- [36]
- [37] 명세서 전반에 걸쳐 사용되는 “클라이언트”는 네트워크를 통하여 서버라는 다른 컴퓨터 시스템 상의 원격 서비스에 접속할 수 있는 응용 프로그램이나 서비스를 의미한다.
- [38] 구체적으로 “클라이언트”는 클라이언트-서버 구조에서 서버에서 그 서버가 제공하는 서비스를 요청하고, 또는 서비스 요청을 위해 필요 인자를 서버가 원하는 방식에 맞게 제공하며, 서버로부터 반환되는 응답에 사용자에게 적절한 방식으로 표현하는 기능을 가진 프로그램이나 시스템이다.
- [39]
- [40] 도 1은 본 발명의 일실시예에 따른 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법을 나타낸 순서도이다.
- [41] 도 1을 참조하면, 본 발명의 일실시예에 따른 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법은 (a) 메인 서버가 서버 난수데이터를 랜덤하게 생성하는 단계(S100), (b) 클라이언트가 서버 난수데이터를 이용하여 생성되는 난수데이터로부터 보안 키패드를 통해 입력되는 각각의 입력문자에 해당하는 클라이언트 난수데이터를 생성하는 단계(S200) 및 (c) 메인 서버가 클라이언트 난수데이터를 이용하여 최종 난수데이터 및 최종 난수데이터를 생성한 후 최종 난수데이터로부터 평문 데이터를 추출하여 생성하는 단계(S300)를 포함한다.
- [42] 도 2는 본 발명의 일실시예에 따른 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법의 세부단계(S100)를 구체화한 순서도이다.
- [43] 도 2를 참조하면, 상기 (a) 단계는, (a1) 메인 서버가 보안 랜덤값인 원타임아이디(OTID: One Time ID)를 생성하는 단계(S110), (a2) 메인 서버가 솔트값(salt value)을 리딩하는 단계(S120), (a3) 메인 서버가 보안 랜덤값과 솔트값을 이용하여 서버 난수데이터의 생성을 위한 기본 해시값(Base HASH value)를 생성하는 단계(S130), (a4) 메인 서버가 보안 키패드에서 사용되는 1개의 문자에 매칭될 랜덤 범위 값(R)을 생성하는 단계(S140) 및 (a5) 메인 서버가 해시함수에 기본 해시값을 적용하여 N차 해시값(HASH value)(여기서, N은 자연수)을 생성하는 단계(S150)를 포함한다.

- [44] 상기 (a1) 단계에서, 메인 서버는 난수데이터의 생성이 요청될 경우, 난수 발생기를 통해 난수값을 생성하고, 생성된 난수값을 해쉬함수에 적용하여 해쉬값을 생성하여 원타임아이디(OTID: One Time ID)로 사용한다.
- [45] 다음, 상기 (a2) 단계에서, 메인 서버는 고객사(=클라이언트)에 발급된 라이선스 파일에서 솔트값(salt value)을 읽어 들인다.
- [46] 다음, 상기 (a3) 단계에서, 메인 서버는 보안 랜덤값과 솔트값을 해시함수에 적용하여 생성된 해시값을 기본 해시값으로 사용한다.
- [47] 다음, 상기 (a4) 단계에서, 메인 서버는 보안 키패드(=가상 키패드)에서 사용되는 1개의 문자에 매칭될 랜덤 범위 값(R)을 생성한다.
- [48] 여기서, 서버 난수데이터는 444개의 문자 내지 1776개의 문자가 조합된 범위 내에서 랜덤하게 생성될 수 있다.
- [49] 종래기술에서는 정형화된 비밀키를 생성하여 암호화하고 관리하는 방식을 취함에 따라 노출 시 해킹될 위험성이 커서 보안에 취약한 반면, 본 발명에서는 난수데이터를 생성하고, 생성된 난수데이터는 크기가 랜덤하게 변경되어 생성됨에 따라 노출 시에도 해킹될 위험성이 없는 장점이 있다.
- [50] 다음, 상기 (a5) 단계에서, 메인 서버는 기본 해시값을 해시함수에 적용하여 N차 해시값을 생성한다.
- [51] 도 2를 참조하면, 추가적으로 상기 (a) 단계는, (a6) 메인 서버가 N차 해시값을 저장하는 단계(S160) 및 (a7) 메인 서버가 서버 난수데이터의 생성이 완료되었는지를 판단하는 단계(S170)를 더 포함한다.
- [52] 구체적으로 도 2를 참조하면, 상기 (a7) 단계는, 서버 난수데이터의 생성이 미완료된 경우, (a71) 메인 서버가 해시함수에 N차 해시값을 적용하여 (n+1)차 해시값을 생성하는 단계(S175) 및 (a72) 상기 (a6) 단계로 복귀하는 단계를 포함하고, 상기 (a72) 단계 이후, 상기 (a6) 단계에서는 메인 서버가 (n+1)차 해시값을 저장한다.
- [53] 예를 들어, 상기 (a5) 단계에서 생성된 기본 해시값을 해시함수에 적용하여 1차 해시값(N=1 일 때)을 생성한 후 상기 (a6) 단계에서 메인 서버가 1차 해시값을 저장한다.
- [54] 다음, 상기 (a7) 단계에서 메인 서버가 서버 난수데이터의 생성이 완료되었는지를 판단하는데, 서버 난수데이터의 생성이 미완료된 경우, 상기 (a71) 단계에서 메인 서버가 해시함수에 1차 해시값을 적용하여 2차 해시값을 생성하고, 상기 (a72) 단계에서 (a6) 단계로 복귀하는데, 이때 상기 (a6) 단계에서는 메인 서버가 2차 해시값을 저장하고, 상기 (a6) 단계부터 상기 (a72) 단계를 거쳐 상기 (a6) 단계로 복귀하는 과정이 1차 사이클(사이클 순서: (a6) 단계=>(a7) 단계=>(a71) 단계=>(a72) 단계=>(a6) 단계)이다(단, (a5) 단계는 최초 1회만 실행됨).
- [55] 다음, 2차 사이클에서도 상기 (a7) 단계에서 메인 서버가 서버 난수데이터의 생성이 완료되었는지를 판단하는데, 서버 난수데이터의 생성이 미완료된 경우, 상기 (a71) 단계에서 메인 서버가 해시함수에 2차 해시값을 적용하여 3차 해시값을

생성하고, 상기 (a72) 단계에서 (a6) 단계로 복귀하는데, 이때 상기 (a6) 단계에서는 메인 서버가 3차 해시값을 저장하고, 상기 (a6) 단계부터 상기 (a72) 단계를 거쳐 상기 (a6) 단계로 복귀하는 과정이 2차 사이클이다.

- [56] 위와 같이 메인 서버는 서버 난수데이터의 생성이 완료될 때까지 상기한 과정을 반복한다.
- [57] 구체적으로 메인 서버는 기본 해시값을 해시함수에 넣고 해시문자열(64문자)을 생성한다(예를 들어, 생성된 해시문자열을 A라고 할 경우 A를 다시 해시함수에 넣고 해시문자열을 생성하고, 생성된 해시문자열을 B라고 할 경우 B를 다시 해시함수에 넣고 해시문자열을 생성).
- [58] 위와 같이 예를 들어 설명한 과정을 반복하여 해시문자열을 생성하는데, 반복 횟수는 (상기 (a4)에서 생성한 랜덤 범위 값(R) X 키패드 문자열 최대값(N))/ 해시함수를 돌려서 나오는 해시값(예를 들어, 64)보다 클 때로 결정된다.
- [59] 이에 따라 상기 (a5) 단계에서, 1차 해시값만 생성한다.
- [60] 상기 (a6) 단계에서, 서버 난수데이터는 444개의 문자 내지 1776개의 문자가 조합된 범위 내에서 랜덤하게 생성될 수 있다.
- [61] 이에 따라 상기 (a7) 단계에서, 메인 서버는 보안 키패드(=가상 키패드)에서 사용할 서버 난수데이터의 생성이 완료될 때까지 키패드 문자열 최대 값(N)만큼 반복하여 R×N 크기의 서버 난수데이터를 생성한다.
- [62] 다음, 상기 (a) 단계는, (a8) 서버 난수데이터의 생성이 완료되는 단계, (a9) 메인 서버가 클라이언트로 서버 난수데이터를 전송하는 단계 및 (a10) 메인 서버가 서버 난수데이터를 삭제하는 단계를 포함한다.
- [63] 특히, 상기 (a10) 단계에서는 서버 난수데이터를 삭제하는데, 이는 상기 (b) 단계가 수행된 후 획득되는 클라이언트 난수데이터를 기반으로 상기 (c) 단계를 수행하기 위함이다.
- [64] 도 3은 본 발명의 일실시예에 따른 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법의 세부단계(S200)를 구체화한 순서도이다.
- [65] 도 3을 참조하면, 상기 (b) 단계는, (b1) 클라이언트가 메인 서버로부터 전송되는 서버 난수데이터를 수신한 후 서버 난수데이터가 기설정된 형식에 맞는지 검증하는 단계(S210), (b2) 클라이언트가 서버 난수데이터와 입력문자를 매칭시키기 위한 난수테이블을 생성하는 단계(S220), (b3) 사용자에게 의한 보안 키패드를 통해 각각의 입력문자가 입력되는 단계(S230), (b4) 클라이언트가 난수테이블에서 각각의 입력문자에 해당하는 클라이언트 난수데이터를 리딩하여 저장하는 단계(S240) 및 (b5) 클라이언트가 각각의 입력문자의 입력이 완료되었는지 판단하는 단계를 포함한다.
- [66] 상기 (b1) 단계에서, 클라이언트는 서버 난수데이터의 형식, 길이, 패턴 등을 포함하는 기설정된 형식이 기저장되어 있고, 서버 난수데이터가 기설정된 형식에 부합하는지 검증하는 프로그램이 내장되어 있다.

- [67] 다음, 상기 (b2) 단계에서, 클라이언트는 서버 난수데이터로부터 1개의 문자에 매칭될 랜덤 범위 값(R)을 추출하고, 보안 키패드(=가상 키패드)에서 사용되는 모든 문자(=각각의 입력문자)를 담아둔 배열에서 R값을 이용하여 1개의 문자를 가져오며, 1개의 문자와 R길이 만큼의 서버 난수데이터를 매칭하여 난수테이블에 저장한다.
- [68] 이에 따라 클라이언트는 상기한 과정을 키패드 문자열 최대 값(N)만큼 반복하여 난수데이터를 생성한다.
- [69] 다음, 상기 (b3) 단계에서는 사용자에게 의해 입력되는 보안 키패드(=가상 키패드)를 통해 각각의 입력문자가 입력된다.
- [70] 다음, 상기 (b4) 단계에서, 클라이언트는 입력된 각각의 입력문자 중 1개의 문자에 해당하는 클라이언트 난수데이터를 난수테이블에서 매칭하여 저장한다.
- [71] 상기 (b5) 단계에서, 클라이언트는 각각의 입력문자의 입력이 완료되었는지 판단하고, 판단된 결과에 따라 다음과 같은 단계를 수행한다.
- [72] 구체적으로 상기 (b5) 단계는, 각각의 입력문자의 입력이 미완료된 경우, (b51) 상기 (b3) 단계로 복귀하는 단계를 포함한다.
- [73] 도 3을 참조하면, 추가적으로 상기 (b) 단계는, (b6) 클라이언트 난수데이터의 생성이 완료되는 단계(S260) 및 (b7) 클라이언트가 메인 서버로 클라이언트 난수데이터를 전송하는 단계(S270)를 더 포함한다.
- [74] 상기 (b6) 단계 및 상기 (b7) 단계는 사용자의 입력이 완료된 상태이고, 상기 (b6) 단계 및 상기 (b7) 단계에서 획득된 클라이언트 난수데이터는 변조되지 않은 데이터이다.
- [75] 도 4는 본 발명의 일실시예에 따른 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법의 세부단계(S300)를 구체화한 순서도이다.
- [76] 도 4를 참조하면, 상기 (c) 단계는, (c1) 메인 서버가 클라이언트로부터 전송되는 클라이언트 난수데이터를 수신한 후 클라이언트 난수데이터의 변조 여부를 검증하는 단계(S310), (c2) 메인 서버가 클라이언트 난수데이터를 이용하여 최종 난수데이터를 생성하는 단계(S320), (c3) 메인 서버가 최종 난수데이터를 이용하여 최종 난수테이블을 생성하는 단계(S330), (c4) 메인 서버가 최종 난수테이블을 통한 평문데이터를 추출하는 단계, (c5) 메인 서버가 평문데이터의 추출이 완료되었는지 판단하는 단계를 포함한다.
- [77] 상기 (c1) 단계에서, 메인 서버는 전술한 상기 (a10) 단계에서 이미 서버 난수데이터가 삭제된 상태에서 클라이언트로부터 전송되는 클라이언트 난수데이터를 수신한 후 클라이언트 난수데이터의 변조 여부를 검증한다.
- [78] 이때, 메인 서버에는 클라이언트 난수데이터가 변조되었는지를 판단하기 위한 프로그램이 내장되어 있다.
- [79] 다음, 상기 (c2) 단계는, (c21) 메인 서버가 최종 보안 랜덤값인 최종 원타임아이디(OTID: One Time ID)를 클라이언트 난수데이터에서 추출하여 생성하는 단계, (c22) 메인 서버가 솔트값(salt value)을 리딩하는 단계, (c23) 메인 서버가 최종

보안 랜덤값과 솔트값을 이용하여 최종 난수데이터의 생성을 위한 최종 기본 해시값(Base HASH value)를 생성하는 단계, (c24) 메인 서버가 보안 키패드에서 사용되는 1개의 문자에 매칭될 최종 랜덤 범위 값(R)을 생성하는 단계, (c25) 메인 서버가 해시함수에 최종 기본 해시값을 적용하여 N차 최종 해시값(Final HASH value)을 생성하는 단계, (c26) 메인 서버가 N차 최종 해시값을 저장하는 단계 및 (c27) 메인 서버가 최종 난수데이터의 생성이 완료되었는지를 판단하는 단계를 포함한다.

- [80] 상기 (c21) 단계에서, 메인 서버는 클라이언트 난수데이터로부터 최종 원타임 아이디(OTID: One Time ID)를 추출하여 생성한다.
- [81] 다음, 상기 (c22) 단계에서, 메인 서버는 고객사(=클라이언트)에서 발급된 라이선스 파일에서 솔트값을 읽어들인다.
- [82] 다음, 상기 (c23) 단계에서, 메인 서버는 최종 보안 랜덤값과 솔트값을 해시함수에 적용하여 생성된 해시값을 최종 기본 해시값으로 사용한다.
- [83] 다음, 상기 (c24) 단계에서, 메인 서버는 보안 키패드(=가상 키패드)에서 사용되는 1개의 문자에 매칭될 랜덤 범위 값(R)을 생성한다.
- [84] 여기서, 최종 난수데이터는 상기 (a6) 단계와 유사하게 444개의 문자 내지 1776개의 문자가 조합된 범위 내에서 크기가 랜덤하게 생성될 수 있다.
- [85] 다음, 상기 (c25) 단계에서, 메인 서버는 기본 해시값을 해시함수에 적용하여 N차 해시값을 생성한다.
- [86] 다음, 상기 (c26) 단계에서, 메인 서버는 N차 해시값을 저장한다.
- [87] 다음, 상기 (c27) 단계는, 최종 난수데이터의 생성이 미완료된 경우, (c271) 메인 서버가 해시함수에 N차 최종 해시값을 적용하여 (n+1)차 최종 해시값을 생성하는 단계 및 (c272) 상기 (c26) 단계로 복귀하는 단계를 포함하고, 상기 (c272) 단계 이후, 상기 (c26) 단계에서는 메인 서버가 (n+1)차 최종 해시값을 저장한다.
- [88] 여기서, 최종 난수데이터는 444개의 문자 내지 1776개의 문자가 조합된 범위 내에서 크기가 랜덤하게 생성될 수 있다.
- [89] 상기 (c27) 단계에서, 메인 서버는 최종 난수데이터의 생성이 완료될 때까지 키패드 문자열 최대 값(N)만큼 반복하여 R×N 크기의 최종 난수데이터를 생성한다.
- [90] 이와 같은 상기 (c2) 단계의 세부단계는 전술한 (a) 단계와 유사하게 진행된다.
- [91] 다음, 상기 (c3) 단계에서, 메인 서버는 클라이언트 난수데이터로부터 1개의 문자에 매칭될 랜덤 범위 값(R)을 추출하고, 보안 키패드(=가상 키패드)에서 사용되는 모든 문자를 담아둔 배열에서 R값을 이용하여 1개의 문자를 가져오며, 1개의 문자와 R길이 만큼의 최종 난수데이터를 매칭하여 최종 난수데이터에 저장한다.
- [92] 이와 같은 상기 (c3) 단계는 전술한 (b) 단계와 유사하게 진행된다.
- [93] 다음, 상기 (c4) 단계에서, 메인 서버는 최종 난수데이터로부터 클라이언트 난수데이터에 대한 평문데이터를 추출하여 생성한다.

- [94] 다음, 상기 (c5) 단계는, 평문데이터의 추출이 완료된 경우, (c51) 상기 (c4) 단계로 복귀하는 단계(S350)를 포함한다.
- [95] 추가적으로 상기 (c) 단계는, (c6) 평문데이터의 생성이 완료되는 단계(S360)를 더 포함한다.
- [96] 이와 같이 최종적으로 도출된 평문데이터는 고객사로 전달되어 고객사에 의해 활용된다.
- [97]
- [98] 상기한 바에 따른 본 발명은 종래기술에서 정형화된 비밀키를 사용함에 따라 노출 시 보안에 취약한 것과 달리 크기가 다른 난수데이터를 랜덤하게 변경시켜 생성함으로써 별도의 비밀키에 대한 생성 및 관리가 필요없고 보안을 강화시킬 수 있다.
- [99]
- [100] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.
- [101] 본 발명의 범위는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

청구범위

- [청구항 1] (a) 메인 서버가 서버 난수데이터를 랜덤하게 생성하는 단계;
 (b) 클라이언트가 상기 서버 난수데이터를 이용하여 생성되는 난수데이터로부터 보안 키패드를 통해 입력되는 각각의 입력문자에 해당하는 클라이언트 난수데이터를 생성하는 단계; 및
 (c) 상기 메인 서버가 상기 클라이언트 난수데이터를 이용하여 최종 난수데이터 및 최종 난수데이터를 생성한 후 상기 최종 난수데이터로부터 평문 데이터를 추출하여 생성하는 단계;를 포함하는 것을 특징으로 하는 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법.
- [청구항 2] 제1 항에 있어서,
 상기 (a) 단계는,
 (a1) 상기 메인 서버가 보안 랜덤값인 원타임아이디(OTID: One Time ID)를 생성하는 단계;
 (a2) 상기 메인 서버가 솔트값(salt value)을 리딩하는 단계;
 (a3) 상기 메인 서버가 상기 보안 랜덤값과 상기 솔트값을 이용하여 상기 서버 난수데이터의 생성을 위한 기본 해시값(Base HASH value)을 생성하는 단계;
 (a4) 상기 메인 서버가 상기 보안 키패드에서 사용되는 1개의 문자에 매칭될 랜덤 범위 값(R)을 생성하는 단계; 및
 (a5) 상기 메인 서버가 해시함수에 상기 기본 해시값을 적용하여 N차 해시값(HASH value)을 생성하는 단계;를 포함하는 것을 특징으로 하는 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법.
- [청구항 3] 제2 항에 있어서,
 상기 (a) 단계는,
 (a6) 상기 메인 서버가 상기 N차 해시값을 저장하는 단계; 및
 (a7) 상기 메인 서버가 상기 서버 난수데이터의 생성이 완료되었는지를 판단하는 단계;를 더 포함하고,
 상기 (a7) 단계는,
 상기 서버 난수데이터의 생성이 미완료된 경우,
 (a71) 상기 메인 서버가 상기 해시함수에 상기 N차 해시값을 적용하여 (n+1)차 해시값을 생성하는 단계; 및
 (a72) 상기 (a6) 단계로 복귀하는 단계;를 포함하며,
 상기 (a72) 단계 이후, 상기 (a6) 단계에서는 상기 메인 서버가 상기 (n+1)차 해시값을 저장하는 것을 특징으로 하는 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법.
- [청구항 4] 제3 항에 있어서,
 상기 (a) 단계는,

- (a8) 상기 서버 난수데이터의 생성이 완료되는 단계;
- (a9) 상기 메인 서버가 상기 클라이언트로 상기 서버 난수데이터를 전송하는 단계; 및
- (a10) 상기 메인 서버가 상기 서버 난수데이터를 삭제하는 단계;를 포함하는 것을 특징으로 하는 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법.

- [청구항 5] 제1 항에 있어서,
상기 (b) 단계는,
(b1) 상기 클라이언트가 상기 메인 서버로부터 전송되는 상기 서버 난수데이터를 수신한 후 상기 서버 난수데이터가 기설정된 형식에 맞는지 검증하는 단계;
(b2) 상기 클라이언트가 상기 서버 난수데이터와 상기 입력문자를 매칭시키기 위한 난수테이블을 생성하는 단계;
(b3) 사용자에게 의한 상기 보안 키패드를 통해 상기 각각의 입력문자가 입력되는 단계;
(b4) 상기 클라이언트가 상기 난수테이블에서 상기 각각의 입력문자에 해당하는 클라이언트 난수데이터를 리딩하여 저장하는 단계; 및
(b5) 상기 클라이언트가 상기 각각의 입력문자의 입력이 완료되었는지 판단하는 단계;를 포함하고,
상기 (b5) 단계는,
상기 각각의 입력문자의 입력이 미완료된 경우,
(b51) 상기 (b3) 단계로 복귀하는 단계를 포함하는 것을 특징으로 하는 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법.

- [청구항 6] 제5 항에 있어서,
상기 (b) 단계는,
(b6) 상기 클라이언트 난수데이터의 생성이 완료되는 단계; 및
(b7) 상기 클라이언트가 상기 메인 서버로 상기 클라이언트 난수데이터를 전송하는 단계;를 더 포함하는 것을 특징으로 하는 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법.

- [청구항 7] 제1 항에 있어서,
상기 (c) 단계는,
(c1) 상기 메인 서버가 상기 클라이언트로부터 전송되는 상기 클라이언트 난수데이터를 수신한 후 상기 클라이언트 난수데이터의 변조 여부를 검증하는 단계;
(c2) 상기 메인 서버가 상기 클라이언트 난수데이터를 이용하여 상기 최종 난수데이터를 생성하는 단계;
(c3) 상기 메인 서버가 상기 최종 난수데이터를 이용하여 상기 최종 난수테이블을 생성하는 단계;

- (c4) 상기 메인 서버가 상기 최종 난수데이터를 통한 상기 평문데이터를 추출하는 단계; 및
- (c5) 상기 메인 서버가 상기 평문데이터의 추출이 완료되었는지 판단하는 단계;를 포함하고,
- 상기 (c5) 단계는,
- 상기 평문데이터의 추출이 미완료된 경우,
- (c51) 상기 (c4) 단계로 복귀하는 단계;를 포함하는 것을 특징으로 하는 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법.
- [청구항 8] 제7 항에 있어서,
- 상기 (c) 단계는,
- (c6) 상기 평문데이터의 생성이 완료되는 단계;를 더 포함하는 것을 특징으로 하는 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법.
- [청구항 9] 제7 항에 있어서,
- 상기 (c2) 단계는,
- (c21) 상기 메인 서버가 최종 보안 랜덤값인 최종 원타임아이디(OTID: One Time ID)를 상기 클라이언트 난수데이터에서 추출하여 생성하는 단계;
- (c22) 상기 메인 서버가 상기 솔트값(salt value)을 리딩하는 단계;
- (c23) 상기 메인 서버가 상기 최종 보안 랜덤값과 상기 솔트값을 이용하여 상기 최종 난수데이터의 생성을 위한 최종 기본 해시값(Base HASH value)을 생성하는 단계;
- (c24) 상기 메인 서버가 상기 보안 키패드에서 사용되는 1개의 문자에 매칭될 최종 랜덤 범위 값(R)을 생성하는 단계;
- (c25) 상기 메인 서버가 해시함수에 상기 최종 기본 해시값을 적용하여 N차 최종 해시값(Final HASH value)을 생성하는 단계;
- (c26) 상기 메인 서버가 상기 N차 최종 해시값을 저장하는 단계; 및
- (c27) 상기 메인 서버가 상기 최종 난수데이터의 생성이 완료되었는지를 판단하는 단계;를 포함하는 것을 특징으로 하는 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법.
- [청구항 10] 제9 항에 있어서,
- 상기 (c27) 단계는,
- 상기 최종 난수데이터의 생성이 미완료된 경우,
- (c271) 상기 메인 서버가 상기 해시함수에 상기 최종 해시값을 적용하여 (n+1)차 최종 해시값을 생성하는 단계; 및
- (c272) 상기 (c26) 단계로 복귀하는 단계;를 포함하며,
- 상기 (c272) 단계 이후, 상기 (c26) 단계에서는 상기 메인 서버가 상기 (n+1)차 최종 해시값을 저장하는 것을 특징으로 하는 보안 키패드용 난수데이터를 이용한 입력데이터의 보안 방법.