(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0085335
(43) 공개일자 2020년07월14일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *G06F 21/31* (2013.01)
G06Q 20/36 (2012.01)
(52) CPC특허분류
H04L 63/0838 (2013.01)
G06F 21/31 (2013.01)
(21) 출원번호 10-2020-7017685
(22) 출원일자(국제) 2018년10월10일
심사청구일자 2020년06월19일
(85) 번역문제출일자 2020년06월18일
(86) 국제출원번호 PCT/EP2018/077585
(87) 국제공개번호 WO 2019/101420
국제공개일자 2019년05월31일
(30) 우선권주장
17203075.1 2017년11월22일
유럽특허청(EPO)(EP)

(71) 출원인
지멘스 악티엔게젤샤프트
독일 뮌헨 베르너-본-지멘스-슈트라쎄 1 (우: 80333)
(72) 발명자
키르흐너, 미하엘
독일 81737 뮌헨 운터하힝거 슈트라쎄 33아
바모스, 베네딕트
독일 85579 노이비베르크 릴리엔탈슈트라쎄 22
(74) 대리인
특허법인 남앤남

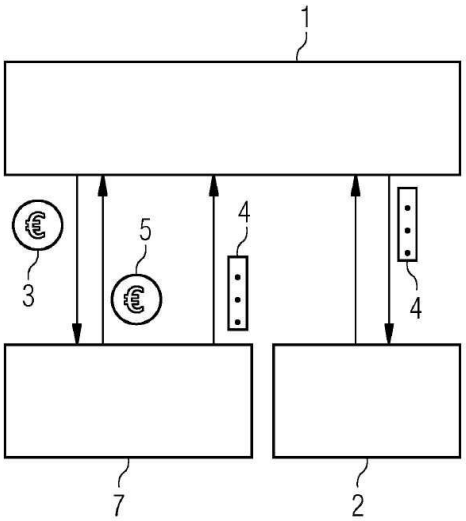
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 **로그인 프로세스들의 보호**

(57) 요 약

본 발명은 로그인 프로세스들의 보호에 관한 것이다. 본 발명은 무차별 대입 공격들에 대비하여 서비스 제공자에 대한 사용자의 로그인 프로세스를 보호하기 위한 방법에 관한 것이다. 금융 값은 임시 로그인 토큰에 대해 사용자로부터 토큰 제공자에게 전달된다. 서비스 제공자에 대한 로그인 시도는 사용자에 의해 수행되고, 로그인 시도는 사용자 특정 로그인 데이터 및 임시 로그인 토큰을 요구한다. 서비스 제공자에 대한 로그인이 미리 정의된 수의 로그인 시도들 내에서 성공하였다면, 금융 값이 다시 사용자에게 전달된다.

대 표 도 - 도2



(52) CPC특허분류
G06Q 20/3674 (2013.01)

명 세 서

청구범위

청구항 1

서비스 제공자(2)에 사용자(1)가 로그인하기 위한 방법으로서,

임시 로그인 토큰(4)에 대한 제1 금융 값(financial value)(3)을 상기 사용자(1)로부터 토큰 제공자(7)에게 전달하는 단계;

상기 서비스 제공자(2)에 대해 로그인 시도를 수행하는 단계 – 상기 로그인 시도는 사용자 특정 로그인 데이터(data) 및 상기 임시 로그인 토큰(4)을 요구함 – ;

상기 서비스 제공자(2)에 대한 상기 로그인이 미리 정의된 수의 로그인 시도들 내에서 성공하였다면, 제2 금융 값(5)을 상기 사용자(1)에게 전달하는 단계를 포함하고,

상기 제2 금융 값(5)은 상기 제1 금융 값(3)과 실질적으로 동일한 값을 갖는,

방법.

청구항 2

제1항에 있어서,

상기 제1 금융 값(3)을 전달한 것에 대한 응답으로, 임시 로그인 토큰(4)이 상기 토큰 제공자(7)로부터 상기 사용자(1)에 의해 수신되는,

방법.

청구항 3

제1항 또는 제2항에 있어서,

상기 서비스 제공자(2)에 대한 로그인이 성공하였다면, 상기 임시 로그인 토큰(4)을 무효화하는 단계를 더 포함하는,

방법.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 서비스 제공자(2)는 상기 토큰 제공자(7)인,

방법.

청구항 5

제1항 내지 제4항 중 어느 한 항에 있어서,

상기 제1 금융 값 및 상기 제2 금융 값의 전달이 완료되면, 상기 로그인 토큰만이 제공되는,

방법.

청구항 6

제1항 내지 제5항 중 어느 한 항에 있어서,

상기 임시 로그인 토큰(4)은 소프트웨어 토큰(software token)인,

방법.

청구항 7

제1항 내지 제6항 중 어느 한 항에 있어서,

상기 제1 금융 값 및 상기 제2 금융 값은 전자 데이터베이스에서 상기 사용자(1)가 소유한 익명의 지갑으로부터 그리고/또는 익명의 지갑으로 전달되는,

방법.

청구항 8

제1항 내지 제7항 중 어느 한 항에 있어서,

상기 제1 금융 값 및 상기 제2 금융 값은 분산형 데이터베이스(6)를 사용하여 전달되고, 상기 데이터는 서로로부터 원격에 위치된 다수의 컴퓨터들 상에 중복으로(redundantly) 저장되는,

방법.

청구항 9

제1항 내지 제8항 중 어느 한 항에 있어서,

상기 제1 금융 값 및 상기 제2 금융 값은 블록체인 기술(blockchain technology)에 기반하여 데이터베이스(6)를 사용하여 전달되는,

방법.

청구항 10

제1항 내지 제9항 중 어느 한 항에 있어서,

상기 제1 금융 값 및 상기 제2 금융 값은 소액 결제 프로토콜(micropayment protocol) IOTA를 사용하여 전달되는,

방법.

청구항 11

제1항 내지 제10항 중 어느 한 항에 있어서,

상기 임시 로그인 토큰(4)은 미리 정의된 수의 로그인 시도들에 대해 유효한,

방법.

청구항 12

제1항 내지 제11항 중 어느 한 항에 있어서,

상기 임시 로그인 토큰(4)은, 상기 임시 로그인 토큰(4)이 상기 미리 정의된 수의 로그인 시도들에 사용되었다는 것에 대한 응답으로 무효화되는,

방법.

청구항 13

제1항 내지 제12항 중 어느 한 항에 있어서,

상기 임시 로그인 토큰(4)이 상기 미리 정의된 수의 로그인 시도들에 사용된 후에, 상기 임시 로그인 토큰(4)이 무효화되면, 어떠한 금융 값(5)도 상기 사용자(1)에게 전달되지 않는,

방법.

청구항 14

적어도 하나의 프로세싱 유닛에 의해 실행될 수 있는 프로그램 코드를 포함하는 컴퓨터 프로그램으로서,

상기 프로그램 코드를 실행하는 것은, 상기 적어도 하나의 프로세싱 유닛으로 하여금, 제1항 내지 제13항 중 어느 한 항에 따른, 서비스 제공자에 사용자가 로그인하기 위한 방법을 실행하게 하는,

컴퓨터 프로그램.

청구항 15

서비스를 사용자(1)에게 제공하도록 구성된 디바이스로서,

상기 디바이스(2)는 메모리(22) 및 적어도 하나의 프로세싱 유닛(21)을 포함하고, 상기 메모리(22)는 상기 적어도 하나의 프로세싱 유닛(21)에 의해 실행 가능한 명령들을 포함하고,

상기 명령들의 실행은 상기 디바이스(2)로 하여금 제1항 내지 제13항 중 어느 한 항에 따른 방법을 실행하게 하는,

디바이스.

청구항 16

컴퓨팅 네트워크로서,

제15항에 따른 적어도 하나의 컴퓨팅 디바이스를 포함하는,

컴퓨팅 네트워크.

발명의 설명

기 술 분 야

[0001] 본 발명은 서비스 제공자(service provider)에 대한 사용자의 로그인 프로세스(login process)들에 관한 것이며, 특히, 무차별 대입 공격(brute force attack)들에 대비하여 서비스 제공자에 대한 사용자의 로그인 프로세스들을 보호하기 위한 방법에 관한 것이다. 또한, 대응하는 컴퓨팅 디바이스(computing device), 컴퓨팅 네트워크(computing network) 및 컴퓨터 프로그램 제품(computer program product)이 제공된다.

배 경 기 술

[0002] 사용자 이름들 및 사용자 비밀번호들에 기반하는, 서비스 제공자에 대한 일반적인 로그인 프로세스들은 종종 무차별 대입 공격들에 대한 대상이 된다. 특히, 무차별 대입은, 정확한 액세스 데이터(access data)를 추측할 의도로 수많은 사용자 이름들 및 사용자 비밀번호 조합들을 자동으로 테스트(test)하기 위해 스크립트(script)들을 사용하는 공격 방법이다. 예컨대, 단지 몇 글자의 길이이거나 사전(dictionary)에 포함된 단어인 간단한 비밀번호가 선택되었다면, 액세스 데이터가 용이하게 추측될 수 있는 확률이 증가한다.

[0003] 로그인 프로세스들, 예컨대, 웹 애플리케이션(web application)의 로그인 프로세스들에 대한 이러한 무차별 대입 공격들은 다양한 상이한 변형들로 수행될 수 있다. 예컨대, 특정 사용자(예컨대, "관리자")를 선택하고 해당 사용자에 대해 다수의 가능한 비밀번호들을 시도함으로써, 무차별 대입 공격들이 수행된다. 대안적인 변형은 특정 가능한 비밀번호(예컨대, "Password123")를 선택하고 다수의 사용자 계정들을 시도하는 것이다. 특히, 애플리케이션의 사용자 그룹(group)이 더 클수록, 실제로 이 특정 비밀번호를 선택한 개별 사용자를 찾을 가능성이 더 높다.

[0004] 로그인 프로세스들에 대한 무차별 대입 공격들에 대비한 기존의 보호 조치들이 존재하는데, 하나의 보호 조치에 따르면, 사용자들은 비밀번호 복잡성이 높은 비밀번호들을 사용하도록 강제된다. 이는 일반적으로, 비밀번호들이 특정 최소 길이를 갖거나 특수 문자들 및 숫자들을 포함해야 하는 것을 요구한다. 그러나, 실제로, 이는 최종 사용자들이 자신들의 비밀번호들을 기억하기가 더 어렵게 만들고, 따라서 최종 사용자는 종종 "Password123456!"과 같은 간단한 비밀번호들을 선택함으로써 보호 조치를 무시(bypass)한다. 이 간단한 비밀번호들은 비밀번호를 선택하기 위한 가이드라인(guideline)들을 기술적으로 준수하고, 따라서 시스템(system)에 의해 수락되지만, 이들은 여전히 매우 용이하게 추측될 수 있다.

[0005] 또 다른 종래의 보호 조치는, 로그인 시도들이 너무 많이 실패한 경우에 사용자 계정들을 잠그는 것이다. 여기서는, 사용자 계정들은 로그인 시도들이 너무 많이 실패한 후 잠기고, 관리자에 의해 또는 미리 결정된 시간 후

에만 재활성화된다. 그러나, 공격자는, 이 메커니즘(mechanism)을 사용하여, 의도적으로 잘못된 로그인 시도들을 전송함으로써 서비스 거부를 발생시키고, 이로써 특정 사용자들을 잠그고 특정 사용자들이 애플리케이션을 사용하는 것을 방해할 수 있다.

[0006] 또한, 레이트 제한(rate limiting)이 사용될 수 있으며, 이 보호 조치는, 예컨대, 정해진 시간 동안 얼마나 많은 로그인 시도 실패가 발생했는지를 IP 어드레스(address)마다 기록한다. 횟수가 너무 많다면, 추가의 로그인 시도들에 대해 IP 어드레스가 차단될 것이다. 예컨대, 네트워크 어드레스 변환(NAT; Network Address Translation)으로 인해 또는 프록시 서버(proxy server)로 인해, 다수의 합법적인 사용자들이 동일한 IP 어드레스 뒤에 위치되면, 이 보호 조치에 따른 문제들이 발생한다.

[0007] 추가의 방지 조치에 따르면, 예컨대, PIN/TAN 로그인 프로세스들, 모바일 폰(mobile phone)들 상의 텍스트 메시지(text message)들을 사용한 2-단계 인증, 또는 Google 인증자와 같은 시간-기반 OTP 프로세스들에서와 같이, 사용자가 서비스 제공자에 싸인(sign)하기 위해 소위 일회성 토큰(One-Time-Token)들이 요구될 수 있다. 그러나, 이러한 보호 조치들은 서비스 제공자와의 개개의 보안 토큰의 사용자에 의한 선행 등록 단계(preceding registration step)들, 다시 말해서, 바인딩 단계(binding step)들을 요구하며, 이는 시간을 소비하고 사용자에 대한 부가적인 노력을 요구한다. 또한, 이 일회용 토큰들은 로그인 프로세스에서 임의의 새로운 사용자가 즉석에서 그리고 익명으로 이용할 수 없다.

[0008] 특정 사용 경우에서 위에서 언급된 보호 조치들 및 그들 개개의 단점들이 수용될 수 없다면, 로그인 프로세스에서 무차별 대입 공격들이 수행될 수 있다는 것이 또한 수용될 수 있다.

발명의 내용

[0009] 따라서, 무차별 대입 공격들에 대비하여 서비스 제공자들의 로그인 프로세스들에 대한 개선된 보호 조치들에 대한 필요성이 있고, 이는 위에 언급된 단점들을 극복한다. 따라서, 본 발명의 목적은, 서비스 제공자의 로그인 프로세스에 대한 무차별 대입 공격들에 대비하여 개선된 보호를 제공하는 그러한 개선된 방법, 개개의 디바이스, 컴퓨터 프로그램 제품 및 컴퓨팅 네트워크를 제공하는 것이다.

[0010] 이러한 목적은 독립항들의 청구대상에 의해 해결된다. 추가의 유리한 특징들은 종속항들의 청구대상이다.

[0011] 본 발명의 제1 양상에 따르면, 서비스 제공자에 사용자가 로그인하기 위한 방법이 제공된다. 제1 단계에서, 제1 금융 값(financial value)은 사용자로부터 임시 로그인 토큰을 위한 토큰 제공자에게 전달되고, 이에 대한 응답으로, 임시 로그인 토큰은 토큰 제공자로부터 사용자에 의해 수신된다. 추가의 단계에서, 로그인 시도는 사용자 특정 로그인 데이터 및 임시 로그인 토큰을 사용하여 사용자에 의해 서비스 제공자에 대해 수행되며, 로그인 시도는 사용자 특정 로그인 데이터 및 임시 로그인 토큰을 요구한다. 다른 단계에서, 서비스 제공자에 대한 로그인이 미리 정의된 수의 로그인 시도들 내에서 성공하였다면, 제2 금융 값은 사용자에게 전달되며, 제2 금융 값은 제1 금융 값과 실질적으로 동일한 값을 갖는다.

[0012] 이로써, 무차별 대입 공격들에 대비하여 로그인 프로세스를 보호하기 위한 개선된 방법이 제공되고, 이는 부가적인 트랜잭션(transaction) 단계들에 의해 로그인 프로세스를 확장시키고, 이로써 금융 팩터(financial factor)를 포함하는 부가적인 트랜잭션 단계들을 포함함으로써 공격자에 대한 기술 복잡성뿐만 아니라 비용을 증가시킨다. 여기서는, 부가적인 트랜잭션 단계들은 백그라운드(background)에서 그리고 최종 사용자에 대해 투명하게 실행되고, 무차별 대입 공격들이 노력 및 금융 면에서 비용이 많이 들게 하고, 따라서 이 공격자에게 매력을 잃게 한다.

[0013] 본 발명의 방법에 따르면, 로그인 프로세스는 직접적으로 실행되는 트랜잭션들에 의해 유리하게 보안되는데, 이는 소액 금융 값 트랜잭션들, 이를테면, 분산형 데이터베이스 시스템(distributed database system)들 또는 IOTA, PIVX와 같은 블록체인-기반 시스템(blockchain-based system)들, 또는 동의(consent) 및 확인(validation) 메커니즘들을 갖는 대응하는 공공 지불 프로토콜(public payment protocol)들에 의해 가능하게 되는 트랜잭션들일 수 있다. 특히, 서비스 제공자에 등록하기 원하는 사용자는, 금융 값을 예치함으로써, 예컨대, 10 번의 시도들 내에서 사용자가 등록을 성공적으로 완료할 수 있다는 것을 보장하는 반면에, 무차별 대입 공격의 맥락에서 수천 번의 로그인 동작들을 수행하기 원하는 공격자들에 대해, 예컨대, 절차는 비용이 너무 많이 든다. 따라서, 사용자 계정들을 잠그거나 IP 어드레스들에 대한 레이트 제한들을 설정하는 것과 같은 대안적인 보안 메커니즘들이 더 이상 필요하지 않다. 또한, 서비스 제공자는, 실제로 수행된 무차별 대입 공격들로부터 재정적으로 큰 이득을 볼 수 있다. 부가적으로, 사용자와 자신의 블록체인 지갑(wallet) 사이에 할당, 즉 사용자가 특정 지갑을 소유하고 있다는 확인을 설정할 필요가 없다. 유리하게도, 사용자는 로그인 프로세스를

위해 임의의 전자 지불 지갑을 사용하고, 다른 로그인 프로세스를 위해 시간이 지남에 따라 이를 변경하고, 가능하게는, 익명의 금융 값 서비스들을 제공하는 상이한 블록체인 기술들의 지갑들을 사용할 수 있다.

[0014] 본 발명의 제2 양상에 따르면, 특히 서비스 제공자, 또는 사용자에게 서비스를 제공하도록 구성된 컴퓨팅 디바이스일 수 있는, 사용자에게 서비스를 제공하도록 구성된 디바이스가 제공되며, 디바이스는 메모리(memory), 및 적어도 하나의 프로세싱 유닛(processing unit)을 포함하고, 메모리는 적어도 하나의 프로세싱 유닛에 의해 실행 가능한 명령들을 포함하고, 명령들의 실행은 디바이스로 하여금 본 발명의 제1 양상에 대해 위에 설명된 바와 같은 방법의 단계들을 실행하게 한다.

[0015] 제2 양상에서 설명된 서비스 제공자에 사용자가 로그인하기 위한 디바이스는 제1 양상에서 위에 설명된 방법들 중 어느 하나 또는 임의의 조합을 수행하도록 구성될 수 있다. 이러한 디바이스들에 대해, 제1 양상에 따른, 서비스 제공자에 사용자가 로그인하기 위한 방법에 대해 설명된 기술적 효과들에 대응하는 기술적 효과들이 달성될 수 있다.

[0016] 본 발명의 제3 양상에 따르면, 컴퓨팅 네트워크가 제공되며, 컴퓨팅 네트워크는 본 발명의 제2 양상에 대해 위에 설명된 바와 같은 적어도 하나의 컴퓨팅 디바이스를 포함한다.

[0017] 본 발명의 제4 양상에 따르면, 컴퓨터 프로그램 제품은 프로그램 코드(program code)를 포함한다. 프로그램 코드는 적어도 하나의 프로세서(processor)에 의해 실행 가능하다. 프로그램 코드를 실행하는 것은 적어도 하나의 프로세서로 하여금 본 발명의 제1 양상에 따른, 서비스 제공자에 사용자가 로그인하기 위한 방법들 중 하나를 수행하게 한다.

[0018] 서비스 제공자에 사용자가 로그인하기 위한 이러한 디바이스, 컴퓨팅 네트워크 및 컴퓨터 프로그램 제품에 대해, 본 발명의 제1 양상에 대해 설명된 기술적 효과들에 대응하는 기술적 효과들이 달성될 수 있다.

[0019] 위의 요약 및 하기의 상세한 설명에서 설명된 특정 특징들이 본 발명의 특정 실시예들 및 양상들과 관련하여 설명되지만, 예시적인 실시예들 및 양상들의 특징들이, 달리 구체적으로 언급되지 않는 한, 서로 결합될 수 있고, 서로 상관될 수 있음이 이해되어야 한다.

[0020] 따라서, 위의 요약은, 단지 일부 실시예들 및 구현들의 일부 특징들에 대한 짧은 개요를 제공하도록 의도되며, 제한하는 것으로 해석되지 않아야 한다. 다른 실시예들은, 위에서 설명된 특징들 이외의 다른 특징들을 포함할 수 있다.

도면의 간단한 설명

[0021] 본 개시내용의 전술한 그리고 다른 엘리먼트(element)들, 특징들, 단계들 및 특성들은 다음의 도면들을 참조하여 실시예들의 다음의 상세한 설명으로부터 자명해질 것이다.

도 1은 본 발명의 실시예들에 따른, 서비스 제공자에 사용자가 로그인하기 위한 단계들을 갖는 흐름도를 예시한다.

도 2는 본 발명의 실시예들에 따른, 서비스를 사용자에게 제공하기 위한 디바이스의 개략도를 예시한다.

도 3은 본 발명의 실시예들에 따른, 분산형 데이터베이스를 사용하여 서비스를 사용자에게 제공하기 위한 추가의 디바이스의 개략도를 예시한다.

도 4는 본 발명의 실시예에 따른, 서비스를 사용자에게 제공하기 위한 추가의 디바이스의 개략도를 예시한다.

발명을 실시하기 위한 구체적인 내용

[0022] 다음에서, 본 발명의 실시예들은 첨부 도면들을 참조하여 상세하게 설명될 것이다. 실시예들의 다음의 설명은 제한적인 의미로 간주되지 않아야 한다는 것이 이해되어야 한다. 본 발명의 범위는, 단지 예시적인 것으로 간주되는 도면들 또는 아래에서 설명되는 실시예들에 의해 제한되는 것으로 의도되지 않는다.

[0023] 도면들은 개략적인 표현들인 것으로서 간주되어야 하며, 도면들에서 예시되는 엘리먼트들은 반드시 실척대로 예시되지는 않는다. 오히려, 다양한 엘리먼트들은, 그 다양한 엘리먼트들의 기능 및 일반적인 목적이 당업자에게 명백해지도록 표현된다. 도면들에서 도시되는 또는 본원에서 설명되는 기능 블록(functional block)들, 디바이스들, 컴포넌트(component)들, 모듈(module)들 또는 다른 물리적인 또는 기능적인 유닛들 사이의 임의의 연결

또는 커플링(coupling)은 또한, 직접적인 또는 간접적인 연결 또는 커플링에 의해 구현될 수 있다. 컴포넌트들 사이의 커플링은 유선 또는 무선 연결을 통해 확립될 수 있다. 기능 블록들, 컴퓨팅 디바이스들, 노드(node)들 또는 엔티티(entity)들은 하드웨어(hardware), 펌웨어(firmware), 소프트웨어(software), 또는 이들의 결합으로 구현될 수 있다.

[0024] 이후에, 서비스 제공자에 사용자가 로그인하기 위한 방법 및 컴퓨팅 디바이스를 사용하는 것과 관련하여 다양한 기법들이 설명된다.

[0025] 본 개시내용의 의미 내에서 사용자(1)는 서비스 제공자(2)에 로그온(log on)하기 원하는 자연인 또는 기술 사용자를 지칭할 수 있으며, 사용자(1)에게 서비스를 제공하기 위한 서비스 제공자(2) 또는 디바이스(2)는, 예컨대, 사용자 이름 및 비밀번호에 의해 로그인 또는 로그온을 수락하고, 그런 다음 사용자에게 특정 서비스를 제공하는 엔티티이다.

[0026] 본 개시내용의 의미 내에서 서비스는 컴퓨팅 인프라구조(infrastructure)에서 구현된 임의의 기술적 개념들을 지칭할 수 있다. 이로써, 데이터 액세스 메커니즘들을 더 효율적이고 신뢰할 수 있게 하기 위해, 개인 소유 클라우드(cloud)에 또는 데이터 센터(data center)에 위치된 제3자 서버에 데이터를 저장하고 프로세싱하는 컴퓨팅 능력들이 가능하게 될 수 있다.

[0027] 본 개시내용의 의미 내에서 네트워크는, 복수의 참가자들이 서로 데이터 통신을 수행할 수 있게 하는 임의의 노드들의 세트를 지칭할 수 있다. 네트워크는 공공 네트워크 또는 개인 네트워크일 수 있다. 네트워크는 블록체인 플랫폼(blockchain platform)에 기반할 수 있거나 기반하지 않을 수 있다. 네트워크는 적어도 하나의 추가의 네트워크에 연결될 수 있다. 네트워크는 블록체인 기법들에 기반하여 데이터를 비가역적으로(irreversibly) 프로세싱할 수 있다.

[0028] 본 개시내용의 의미 내에서 분산형 네트워크는 네트워크에서 구현된 임의의 데이터베이스를 지칭할 수 있으며, 이 데이터베이스는 서로 원격에 있는 몇몇의 네트워크 노드들 상에 적어도 부분적으로 중복으로 저장된다. 블록체인 기술은 트랜잭션들 및/또는 스마트 계약(Smart Contract)들에 관련된 데이터를 포함하는 복수의 블록들을 포함할 수 있다. 상이한 블록들의 체인화(chaining)는 각각의 블록에 저장된 암호화 해시 값(cryptographic hash value)들에 의해 구현될 수 있으며, 각각의 해시 값은 이전 블록의 데이터를 나타낼 수 있다.

[0029] 도 1은 본 발명의 실시예들에 따른, 서비스 제공자에 사용자가 로그인하기 위한 단계들을 갖는 흐름도를 예시한다.

[0030] 방법은 단계(S10)에서 시작한다. 단계(S20)에서, 제1 금융 값(3)은 사용자로부터 임시 로그인 토큰(4)을 위해 토큰 제공자(7)에 전달된다. 단계(S30)에서, 로그인 시도는 서비스 제공자(2) 상에서 수행되며, 로그인 시도는 사용자 특정 로그인 데이터 및 임시 로그인 토큰(4)을 필요로 한다. 단계(S40)에서, 미리 정의된 수의 로그인 시도들 내에서 서비스 제공자(2)에 대한 로그인이 성공하였다면, 제2 금융 값(5)이 사용자(1)에게 전달되고, 제2 금융 값(5)은 제1 금융 값(3)과 실질적으로 동일한 값을 갖는다. 방법은 단계(S50)에서 종료된다.

[0031] 도 2는 본 발명의 실시예에 따른, 사용자(1)에게 서비스를 제공하기 위한 디바이스(2)의 개략도를 예시한다.

[0032] 도 2에서 볼 수 있듯이, 사용자(1)는, 디바이스(2)에 로그인하기 위해, 사용자(1)에게 서비스를 제공하기 위한 디바이스(2) 및 로그인 토큰 제공자(7)와의 트랜잭션들을 수행한다.

[0033] 로그인 시도에서, 사용자(1)는 사용자 이름 및 대응하는 사용자 특정 비밀번호를 포함하는 특정 로그인 데이터를 서비스 제공자(2)에 제공한다.

[0034] 서비스 제공자(2)는 사용자가 로그인할 때 다음 3개의 데이터 블록들을 요구한다.

[0035] 사용자 이름 + 사용자 특정 비밀번호 + 로그인 토큰(4)

[0036] 이상적인 구현에서, 본원에 언급된 부가적인 "로그인 토큰" 팩터는 사용자(1)의 백그라운드에서 투명하게 취급되어, 사용자는 평소처럼 사용자 이름 및 비밀번호만을 계속 입력한다. 예컨대, 로그인 토큰(4)은 길고 무작위로 보이는 스트링(string)으로 표현되거나, 임시 로그인 토큰은 문자 스트링, 데이터 세트, 데이터 블록, 개인/공개 키 쌍(private/public key pair), 식별자, 또는 제3자가 용이하게 추측할 수 없는 임의의 다른 비밀 정보와 같은 소프트웨어 토큰일 수 있다.

[0037] 사용자(1)와 토큰 제공자(7) 사이의 다른 트랜잭션에서, 임시 로그인 토큰(4)이 구매된다. 사용자(1)는 특정 값(3), 예로서 금융 값(3)을 서비스 제공자(2)에게 전달한다. 이에 대한 응답으로, 사용자는 유효한 임시 로그

인 토큰(4) 및 로그인 절차가 성공하자마자 금융 값(3)이 즉시 사용자(1)에게 다시 전달된다는 보장을 수신한다. 로그인 토큰(4)은 자신의 유효성이 예컨대, 최대 10 번의 로그인 시도들로 제한된다.

[0038] 금융 값들의 전달은 트랜잭션들을 즉시(몇 분 또는 몇 시간의 지연 없이) 실행하는 방법에 기반해야 한다. 이상적으로, 사용자에 대한 트랜잭션 수수료들을 생성하지 않는 절차가 사용된다. 따라서, 이는 유리하게는 분산형 데이터베이스, 우선적으로는, 소액 지불 프로토콜들 IOTA, PIVX, ETHEREUM, DASH 및 BITCOIN CASH 중 하나와 같은 블록체인 기술에 기반한 데이터베이스에 기반한다. 당업자에게 알려진 바와 같이, 임의의 다른 소액 결제 프로토콜이 사용될 수 있다.

[0039] 추가의 트랜잭션에서, 서비스 제공자(2)가 정확한 사용자 이름 및 비밀번호로 로그인 시도를 프로세싱하면, 로그인 토큰이 무효화되고, 금융 값(5)은 토큰 제공자(7)로부터 전송자의 어드레스로 반환된다. 다른 실시예에서, 금융 값(5)은 서비스 제공자(2)로부터 사용자(1)에게 반환될 수 있다.

[0040] 서비스 제공자(2)가 부정확한 사용자 이름 및 비밀번호를 이용한 로그인 시도를 프로세싱하면, 이 임시 로그인 토큰(4)으로 허용되는 시도들의 수는 1씩 감소된다. 허용된 시도들의 횟수가 0에 도달하면, 임시 로그인 토큰은 무효화되고, 로그인 토큰(4)과 연관된 금융 값(3)은 로그인 토큰 제공자(7)에 의해 또는 다른 실시예에서 서비스 제공자(2)에 의해 유지된다. 일 실시예에서, 서비스 제공자(2) 및 로그인 토큰 제공자(7)는 동일한 엔티티일 수 있다.

[0041] 도 3은 본 발명의 실시예들에 따른, 분산형 데이터베이스를 사용하여 서비스를 사용자(1)에게 제공하기 위한 추가의 디바이스(2)의 개략도를 예시한다.

[0042] 도 3으로부터 도출될 수 있듯이, 사용자(1)는 분산형 데이터베이스(6)를 통해 서비스 제공자(2)와, 그리고 직접적으로 서비스 제공자(2)와 트랜잭션을 수행한다. 수행된 트랜잭션들은 도 2에 대해 설명된 트랜잭션들에 대응하며, 금융 값들(3, 5)의 전달들은 분산형 데이터베이스(6)를 사용하여 수행되며, 더욱이 서비스 제공자(2)는 또한 사용자(1)에 대한 로그인 토큰 제공자(7)이다.

[0043] 도 4는 본 발명의 실시예에 따른, 서비스를 사용자(1)에게 제공하기 위한 추가의 디바이스(2)의 개략도를 예시한다.

[0044] 도 4에 도시된 디바이스(2)는, 위에 설명된 바와 같이, 사용자(1)를 로그인하기 위한 방법들 중 하나를 수행할 수 있으며, 디바이스(2)는 인터페이스(interface)(20)를 더 포함하고, 인터페이스(20)는 분산형 데이터베이스(6)의 서버들과 같은 다른 엔티티들에 사용자 데이터 또는 제어 메시지들을 송신하도록 구성되고, 분산형 데이터베이스(6)의 서버들 또는 컴퓨팅 네트워크에 위치된 임의의 다른 노드들과 같은 다른 엔티티들로부터 사용자 데이터 또는 제어 메시지들을 수신하기 위해 제공된다. 인터페이스(20)는 특히, 본 발명의 제1 양상에 대해 설명된 바와 같이, 사용자(1)로부터 사용자 이름, 사용자 특정 비밀번호 및 임시 로그인 토큰과 같은 로그인 데이터를 수신하도록 자격이 주어진다. 디바이스(2)는 또한, 디바이스(2)의 동작을 담당하는 프로세싱 유닛(21)을 포함한다. 프로세싱 유닛(21)은 하나 이상의 프로세서들을 포함하고, 메모리(22)에 저장된 명령들을 수행할 수 있으며, 메모리(22)는 판독 전용 메모리, 랜덤 액세스 메모리(random access memory), 대용량 저장소, 하드 디스크(hard disk) 등을 포함할 수 있다. 메모리는 또한, 디바이스(2)가 수반된 위에 설명된 기능들을 구현하기 위해 프로세싱 유닛(21)에 의해 실행되기에 적합한 프로그램 코드를 포함할 수 있다.

[0045] 위에서 말했듯이, 일부 일반적인 결론들이 도출될 수 있다.

[0046] 제1 금융 값을 전달하는 것에 대한 응답으로, 임시 로그인 토큰은 토큰 제공자로부터 사용자에 의해 수신될 수 있다. 서비스 제공자는, 임시 로그인 토큰이 미리 결정된 수의 로그인 시도들에 사용될 수 있고, 로그인 시도들 중 하나가 미리 정의된 수의 로그인 시도들 내에서 성공하면, 금융 값이 사용자에게 다시 전달될 것이라는 임시 로그인 토큰에 대한 보증을 추가로 제공할 수 있다. 이로써, 서비스 제공자에 대해 로그인하기 원하는 사용자가 임시 로그인 토큰 – 이는 서비스 제공자에 대해 로그인을 시도하기 위해 필요함 -을 수신하기 전에, 사용자가 우선 먼저 금융 값을 예치해야 한다는 것이 보장된다.

[0047] 서비스 공급자에 대한 로그인에 성공하였다면, 임시 로그인 토큰이 무효화될 수 있다. 성공적인 로그인 시도 후에 임시 로그인 토큰을 무효화하는 것은 임시 로그인 토큰의 추가의 사용을 방지하고, 따라서 공격자가 임시 로그인 토큰으로 추가의 로그인을 시도하는 것을 방지하는데 기여한다.

[0048] 서비스 제공자는 토큰 제공자일 수 있거나, 서비스 제공자는 토큰 제공자를 포함할 수 있다. 서비스 제공자 및 토큰 제공자의 통합(unity)은 빠르고 효율적인 통신, 및 따라서 로그인 프로세스의 개선된 성능을 가능하게 한

다.

[0049] 제1 및 제2 금융 값들의 전달이 완료되었고 사용자가 그 자신의 액션(action)에 의해 금융 값의 전달을 취소하거나 무효화할 가능성이 없는 경우에만, 로그인 토큰이 제공될 수 있다. 이로써, 서비스 제공자에 대해 로그인하기 원하는 사용자가 임시 로그인 토큰 – 이는 서비스 제공자에 대해 로그인을 시도하기 위해 필요함 -을 수신하기 전에, 사용자가 우선 먼저 금융 값을 예치해야 한다는 것이 추가로 보장된다.

[0050] 서비스 제공자에 대한 사용자의 로그인이 성공한 경우에만, 금융 값이 다시 전달될 수 있고, 서비스 제공자에 대한 로그인이 성공한 것에 대한 응답으로, 금융 값은 토큰 제공자 또는 서비스 제공자로부터 사용자에게 전달된다.

[0051] 임시 로그인 토큰은 문자 스트링, 데이터 세트, 데이터 블록, 개인/공개 키 쌍, 식별자, 또는 제3자가 용이하게 추측할 수 없는 임의의 다른 비밀 정보와 같은 소프트웨어 토큰일 수 있다. 이로써, 임시 로그인 토큰은 안전하고, 토큰 제공자로부터 사용자에 의해 용이하게 수신될 수 있다.

[0052] 제1 및 제2 금융 값들은 전자 데이터베이스에서 사용자가 소유한 익명의 지갑들로부터 그리고/또는 익명의 지갑들에 전달될 수 있다. 이로써, 각각 사용자가 소유한 보안 피처(feature)인, 토큰 제공자와의 사용자의 이전 바인딩 및 등록없이, 로그인 프로세스가 보안될 수 있다. 따라서, 임의의 사용자는 본 발명에 따른 로그인 프로세스를 수행할 수 있으며, 사용자에 대한 유일한 요건은 사용자가 지갑을 소유하는 것이고, 사용자는 지갑을 사용하여 금융 값을 서비스 제공자에게 전달할 수 있다.

[0053] 제1 및 제2 금융 값들은 분산형 데이터베이스를 사용하여 전달될 수 있으며, 데이터는 서로 원격에 위치된 다수의 컴퓨터들 상에 중복으로 저장된다. 분산형 데이터베이스를 사용하는 것은 금융 값들 및 임시 로그인 토큰의 전달을 더 안전하고 더 빠르게 만들고, 익명성이 요구되는 경우, 즉, 로그인 프로세스 전에, 사용자의 어떠한 사전 등록도 이루어질 필요가 없다.

[0054] 제1 및 제2 금융 값들은 블록체인 기술에 기반하여 데이터베이스를 사용하여 전달될 수 있다. 또한, 스마트 계약들은 임시 로그인 토큰의 전달과 결합된 금융 값의 전달을 위한 기반으로서 사용될 수 있다. 특히, 제1 및 제2 금융 값들은 IOTA, PIVX, ETHEREUM, DASH 및 BITCOIN CASH를 포함하는 그룹으로부터 선택된 소액 지불 프로토콜을 사용하여 전달될 수 있다. 위에서 언급된 기술들은 독점 솔루션들(proprietary solutions)보다 더욱 신뢰할 수 있는 로그인 프로세스를 가능하게 하고, 이는 또한 더 안전하고 더 빠르고, 익명성이 요구되는 경우, 즉, 로그인 프로세스 전에, 사용자의 어떠한 사전-등록도 이루어질 필요가 없다.

[0055] 임시 로그인 토큰은 미리 정의된 수의 로그인 시도들에 대해 유효할 수 있으며, 이로써 사용자는 첫번째 시도에서 서비스 제공자에 몇 번 로그인을 시도하여, 로그인 프로세스에서 일부 에러(error)들은 임시 로그인 토큰의 손실로 이어지지 않는다. 따라서, 인증된 사용자가 예치한 금융 값을 잃을 위험이 감소된다.

[0056] 임시 로그인 토큰은, 미리 정의된 수의 로그인 시도에 대해 임시 로그인 토큰이 사용되었다는 것에 대한 응답으로 무효화된다. 미리 정의된 수의 로그인 시도들에 대해 임시 로그인 토큰이 사용되었다는 것에 대한 응답으로 임시 로그인 토큰을 무효화하는 것은, 새로운 임시 로그인 토큰에 대한 금융 값의 새로운 전달이 필요하기 전에, 미리 정의된 수보다 더 많은 로그인 시도들이 수행될 수 있는 것을 방지한다.

[0057] 임시 로그인 토큰이 미리 정의된 수의 로그인 시도들에 대해 사용된 후에, 임시 로그인 토큰이 무효화되면, 어떠한 금융 값도 사용자에게 전달되지 않을 수 있고, 이로써 비인가된 사용자 또는 공격자에 대한 미리 정의된 수의 성공하지 않은 로그인 시도들 후에 금융 값의 손실 및 증가된 트랜잭션 노력을 제공하여, 증가된 노력 및 비용으로 인해 무차별 대입 공격은 매력을 잃게 된다.

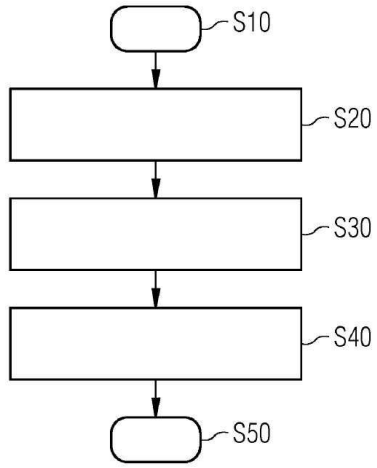
[0058] 요약하면, 서비스 제공자에 사용자가 로그인하기 위한 방법이 제공되며, 금융 값은 임시 로그인 토큰에 대해 사용자로부터 토큰 제공자에게 전달되며, 사용자 특정 로그인 데이터 및 임시 로그인 토큰을 요구하는 로그인 시도가 수행된다. 서비스 제공자에 대한 로그인이 미리 정의된 수의 로그인 시도들 내에서 성공하였다면, 금융 값이 사용자에게 다시 전달된다.

[0059] 이로써, 로그인 프로세스는 부가적인 트랜잭션들에 의해 유리하게 보안되며, 이는 공격자에 대한 노력, 복잡성 및 비용을 증가시키며, 부가적인 트랜잭션 단계들은 인가된 최종 사용자에 대해 백그라운드에서 그리고 투명하게 실행되고, 공격자에게 무차별 대입 공격이 매력을 잃게 만들 수 있다. 부가적으로, 사용자와 사용자의 블록체인 지갑과 토큰 제공자 사이에 할당 또는 등록을 설정할 필요가 없고, 즉, 사용자가 특정 지갑을 소유하고 있다는 것을 확인할 필요가 없어서, 사용자는 로그인 프로세스에서 임의의 지갑을 사용하고, 시간이 지남에 따라

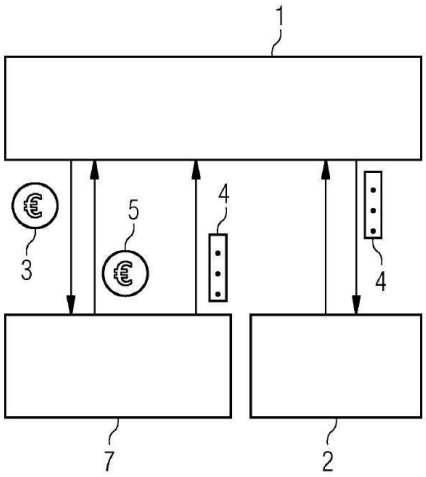
임의의 지갑을 변경하고, 가능하게는, 상이한 블록체인 기술들 또는 유사한 익명의 금융 프로토콜들의 지갑들을 사용할 수 있다.

도면

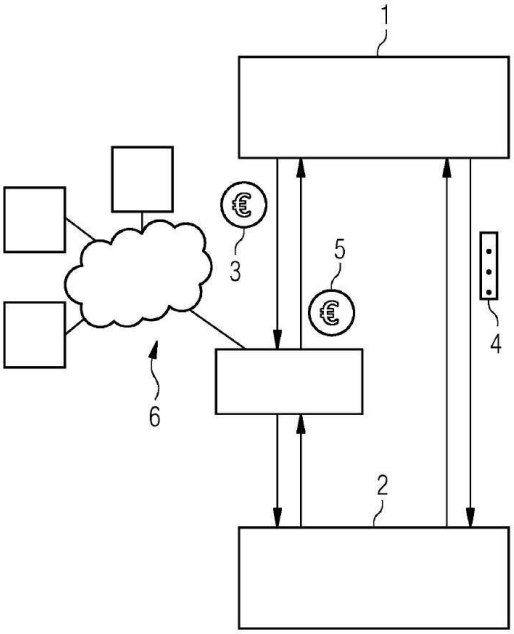
도면1



도면2



도면3



도면4