블록체인을 활용한 다단계 인증 기법 설계

김세민[1] · 홍성혁[2,*]

[1]전주교육대학교 · [2]백석대학교

Design of Multi-Step Authentication Method using Blockchain

Semin Kim[1] · Sunghyuck Hong[2,*]

[1]Jeonju National University of Education · [2]Baekseok University

E-mail : imsil303@hotmail.co.kr / shong@bu.ac.kr

요 약

본 연구에서는 블록체인을 활용하여 인증 데이터를 적재한 후 추후의 인증 데이터와 비교하여 재차 인증을 진행할 수 있는 인증 기법을 설계하였다. 이를 위하여 기존에 많이 활용하던 ID와 패스워드 입력 방법과 널리 활용되고 있는 ARS 인증 방식을 거친 후, 각 사용자의 단말기에 저장되어 있는 생체 데이터를 활용하여 인증을 진행하게 하였다. 이러한 단계를 거친 후 기존에 저장된 체인 데이터와 최근에 인증한 데이터를 비교하여 최종 인증을 진행한 후 인증된 데이터를 다시 체인 데이터에 다시 적재하는 방식을 선택하였다. 본 연구를 통하여 다양한 인증 방식에 대한 방안을 제시할 수 있을 것으로 기대된다.

ABSTRACT

In this study, we designed an authentication method that can perform authentication again by loading authentication data using a blockchain and comparing it with the authentication data in the future. To this end, after passing through the conventional ID and password input method and the widely used ARS authentication method, authentication is performed using biometric data stored in each user's terminal. After going through these steps, we chose a method of comparing the previously stored chain data with the recently authenticated data to perform final authentication and then reloading the authenticated data into the chain data. It is expected that this study will be able to suggest various authentication methods.

키워드

블록체인, 다단계 인증, 생체 인증, 인증 서비스

Ⅰ. 서 론

대한민국에서는 2020년 이후로 공인인증서 제도가 폐지되었다. 따라서 수많은 업체와 기관에서 인증기법을 다양화시키고 있다. 다양한 인증방법은 수요자와 공급자의 선택의 폭을 넓혀주고 편리한 인증방법을 제시하여 줄 수 있지만 기관마다 다르게 제공하는 인증 방법에 따라 너무 여러 가지 방법을 쓰다보면 사용자가 혼란에 빠지는 경우도 있을 수 있다.

이에 본 연구에서는 기본적으로 제공하는 ID와 패스워드 입력방식과 또한 널리 쓰이는 ARS 인증 방식 이후의 인증 단계를 적용하고, 각자의 단말기에 등록된 생체인식 데이터를 포함하여 블록체인에 적재하여 추후 인증에서 비교하여 또 인증하는 기법을 제안하였다.

본 연구의 구성은 다음과 같다. 서론에 이어 2장에서는 이중 인증 및 다단계 인증과 블록체인과 생체 인식을 활용한 인증 기법을 탐구하고, 3장에서는 관련 연구에서 분석한 요소를 융합하여 시스

* corresponding author

템을 설계한 후 4장에서는 결론 및 제언으로 맺는다.

II. 관련 연구

2.1 이중 인증 및 다단계 인증

이중 인증(two-factor authentication)는 사용자가 아는 요소(1단계)와 사용자가 가지고 있는 요소(2단계)를 이용하여 인증하는 방식이다. 서비스에 접근하려면 사용자는 두 가지 요소를 모두 가지고 있어야 한다. 요청/응답 프로세스에서 인증을 할 때 사용자임을 증명할 수 있는 시스템이 요구하는 개인 정보를 가질 때 인증이 완료된다[3].

안전이 요구되는 서비스에서는 이중 인증을 사용하고 있다. 1단계 인증으로 아이디와 패스워드와 같이 자신이 아는 요소를 사용하고, 2단계 인증으로 SMS나 OTP 또는 보안 카드와 같이 가지고 있는 요소를 활용하여 사용자 인증을 사용하고 있다. 안전하지 않는 채널을 통해 1단계의 패스워드가 노출되더라도 사용자가 소지하고 있는 요소를 분실하지 않는 다면 2단계 인증을 해결 할 수 없어 기술적인 측면에서 안전하다[4].

2.2 생체 인증

블록체인에서 생체정보가 저장된 블록을 찾아 해시값과 사용자로부터 받은 정보를 기반으로 생성한 해시값을 비교한다. 해시값이 같으면 인증이 완료된다.

사용자의 생체정보를 측정하기 위해 스마트 폰을 이용하여 홍채나 지문 등을 수집하여 그 정보를 알 수 없도록 해시함수를 통해 사용자의 정보의 내용을 확인할 수 없도록 한다. 이 정보가 노출되더라도 해시함수로 인해 해당 정보를 확인할 수 없고, 오직 서버에서 해당 정보에 대한 식별할 수 있도록 익명성을 보장하는 기법이다.

III. 다단계 인증 시스템 구현

본 연구에서 구현한 다단계 인증 시스템에서는 아이디와 패스워드가 첫 번째 기본 인증 항목이고 ARS는 두 번째 인증 항목이며 세 번째 인증 항목은 Face ID나 지문을 활용한 생체 인식이다.

다단계 인증은 사용자가 이미 가지고 있는 속성들을 활용하여 인증하는 방식이다. 시스템이 요청하여 사용자가 응답하는 프로세스에서는 인증을 통하여 사용자가 맞음을 증명할 수 있을 때 인증이 완료된다. 단계별로 인증이 진행되면서 보안 안정성이 요구되는 서비스에서 활용할 수 있다. 그림 1은 다단계 인증 단계를 나타낸 것이다.

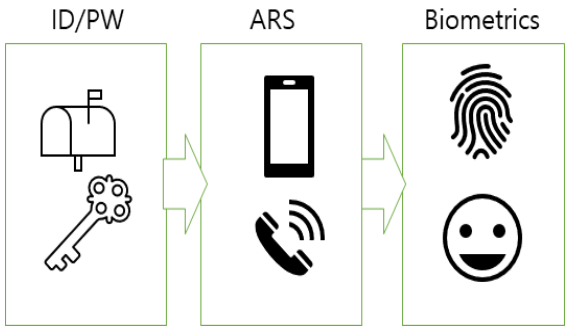

그림 1. 다단계 인증 구성도

인증된 후에 최근 인증 데이터는 기존의 체인데이터에 적재되어 포함된다. 추후 재차 인증이 진행될 시에는 그림 2에서 묘사한 바와 같이 기존의 체인 데이터와 최근 인증 데이터를 비교한 후 최종 인증이 진행되고, 최근 인증 데이터가 다시 체인 데이터에 적재된 후 서비스를 진행할 수 있다.

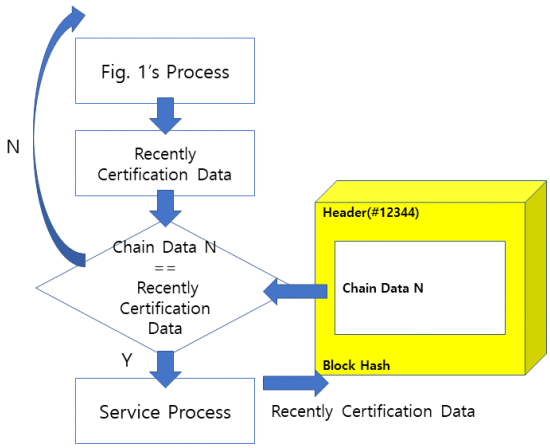

그림 2. 인증 진행 절차

IV. 결론 및 제언

본 연구에서는 블록체인을 활용하여 다단계 인증 기법을 구현하였다. 제안된 기법에서는 기존에 블록체인에 적재되어있는 데이터와 최근에 인증 절차를 거친 데이터가 비교되어 인증을 최종 진행한다. 인증을 거치는 초기 단계로는 ID와 패스워드 입력-ARS 인증 단계-생체 인식 단계 등을 거친 후 기존의 블록체인에 적재된 데이터와 비교하는 것이다.

본 연구에서 제안한 기법을 통하여 2020년 대한민국에서 공인인증서 제도가 없어진 후 보안과 인증에 불안함을 느끼는 많은 사람들에게 안전한 인증의 방법 중 하나로 제시할 수 있다.

연구의 한계점으로는 사용성 평가를 거친 후 평

가 점수에 따른 서비스 만족도를 측정하지 못하였다는 점이다.

향후 연구과제에서는 인증 과정 전반에 걸쳐서 설계한 시스템을 구축하는 것이다.

Acknowledgement

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2020R1F1A1048684).

References

[1] S. R. Lee, H. Berry, O. Temam, and M. Lipasti, “Performance improvement of WDM channels using inline dispersion management in transmission links with OPC placed at various position,” *The Journal of Korea Navigation Institute*, Vol. 14, No. 5, pp. 668-676, Oct. 2010.

[2] A. Hashmi, H. Berry, O. Temam, and M. Lipasti, “Automatic abstraction and fault tolerance in cortical microachitectures,” in *Proceeding of the 38th Annual International Symposium on Computer Architecture*, New York: NY, pp. 1-10, 2011.

[3] J. G. Proakis, *Digital Communications,* 4th ed. New York, NY: McGraw-Hill, 1993.

[4] Malardalen Real-Time Research Center. The worst-case execution time (WCET) analysis project [Internet]. Available : http://www.mrtc.mdh.se/projects/wcet/.