JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 11, pp. 139-146, November 2020
https://doi.org/10.9708/jksci.2020.25.11.139

User Authentication Technology Using Multi-Blocks in the Cloud Computing Environment

Eun-Gyeom Jang*

*Professor, Dept. of Internet Communication, Jangan University, Gyeonggi-do, Korea

[Abstract]

Cloud computing technology provides economic and efficient system operation and management features to deal with rapidly changing IT technologies. However, this is less used in institutes and companies due to low security of cloud computing service. It is recognized that storing and managing important information, which is confidential in external systems is vulnerable to security threats. In order to enhance security of this cloud computing service, this paper suggests a system and user authentication reinforcement model. The suggested technology guarantees integrity of user authentication information and provides users with convenience by creating blocks for each cloud service and connecting service blocks with chains. The block chain user authentication model offers integrity assurance technology of block chains and system access convenience for SSO users. Even when a server providing cloud computing is invaded, this prevents chained invasions not to affect other systems.

▸ **Key words**: Cloud Computing, SSO, Block Chain, User Authentication, Integrity

[요 약]

클라우드 컴퓨팅 기술은 급변하는 IT 기술의 경제적이고 효율적인 시스템 운영 및 관리 기능을 제공한다. 하지만, 기관 및 기업에서는 클라우드 컴퓨팅 서비스의 보안성 때문에 활용성이 떨어지고 있다. 외부 시스템에 대외비에 속하는 중요정보를 보관하여 관리하는 것은 보안에 취약하다고 인식되어 있기 때문이다. 이러한 클라우드 컴퓨팅 서비스에 대한 보안성을 강화하기 위해 본 논문에서는 시스템 및 사용자 인증 강화 모델을 연구하였다. 제안 기술은 사용자 인증 정보를 클라우드 서비스별로 블록을 생성하여 서비스 블록을 체인으로 연결하여 정보의 무결성을 보증하고 사용자에게는 편의성을 제공한다. 블록 체인 사용자 인증 모델은 블록 체인의 무결성 보증 기술과 SSO 사용자의 시스템 접근 편의성을 제공한다. 클라우드 컴퓨팅을 제공하는 서버에 침해가 발생하더라도 다른 시스템에 영향이 없도록 연쇄 침해를 방지한다.

▸ **주제어**: 클라우드 컴퓨팅, SSO, 블록 체인, 사용자 인증, 무결성

• First Author: Eun-Gyeom Jang, Corresponding Author: Eun-Gyeom Jang
*Eun-Gyeom Jang (jangeg@jangan.ac.kr), Dept. of Internet Communication, Jangan University
• Received: 2020. 10. 12, Revised: 2020. 11. 03, Accepted: 2020. 11. 03.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

네트워크로 연결된 컴퓨팅 자원을 원격에서 서버 서비스를 이용할 수 있는 패러다임이 클라우드 컴퓨팅이다. 클라우드 컴퓨팅은 소프트웨어와 하드웨어 전반에 걸쳐 서비스를 지원하고 있다. 다양한 소프트웨어 및 IT 자원은 시간과 공간에 구애받지 않고 네트워크가 가능한 단말기기만으로 서비스를 이용할 수 있다.

기존 시스템을 포함한 현재의 로컬 시스템들은 학교 및 기관, 기업 등의 단위 그룹으로 서버를 구축하여 운영하고 있다. 이렇게 구축된 시스템은 급변하는 새로운 IT 기술 환경으로 수년 내에 노후 시스템으로 전락하는 것이 현실이다. 새로운 기술 및 환경의 변화에 시스템을 매번 교환하는 것은 경제성과 활용성에 비효율적이다. 또한, 시스템을 운영, 관리, 장비 설치 장소의 추가적인 공간적인 부분도 고려되어야 한다. 이러한 자원의 낭비를 감소시키기 위한 기술 및 서비스가 클라우드 컴퓨팅이다. 클라우드 컴퓨팅은 일정액을 지불하고 컴퓨팅 자원과 소프트웨어를 활용할 수 있다[1].

클라우드 컴퓨팅의 가장 큰 장점은 시스템 서버 구축과 유지 관리의 비용이 절감되고 시스템 유지 및 관리에 상대적으로 고급 전문 기술을 필요로하지 않는다. 서비스 업체의 클라우드 서버 구축 매뉴얼을 학습하여 클라우드를 컴퓨팅 서비스를 운영할 수 있다. 이렇게 유용한 클라우드 컴퓨팅을 서비스를 활용하는 기관 및 단체가 많아지고는 있지만, 광범위하게 활성화되지 않는 것은 보안적인 측면이 제일 크다. 기업의 기밀정보 및 개인정보를 외부의 서버에 구축하면서 중요정보의 노출이 발생할 수 있다는 것이다. 이러한 클라우드 컴퓨팅의 위험성 내재는 보안적 위험성이 적은 서비스가 많이 활용되고 있는 이유이기도 하다[1,2].

클라우드 컴퓨팅은 네트워크를 기반으로 온라인 서비스가 이뤄지고 있다. 이러한 환경은 네트워크에 존재하는 위험성을 모두 갖는다. 네트워크상에서의 통신 단절에 의한 서비스 마비, 중앙 집중형 서비스 환경의 네트워크 트래픽과 서버의 부하가 치명적인 문제점이라 할 수 있다.

네트워크 기반 컴퓨팅 서비스는 기밀성, 활용성, 용이성, 접근성, 경제성을 요구한다. 기존 연구에 사용자의 용이성과 편의성, 접근성을 지원하기 위해 SSO를 활용한 보안 서비스가 있으나, 클라우드 컴퓨팅 서비스 환경에서는 보안과 인증 서비스가 미흡하다[3].

본 논문에서는 클라우드 컴퓨팅 서비스를 사용자가 안전하게 활용할 수 있도록 사용자 인증 강화 기술을 제안한다. 제안 모델은 사용자 인증 강화를 위해 사용자 인증 정보를 분산하여 관리하고 각 분산된 블록의 인증 절차를 강화하였다. 논문의 구성은 2장에서 클라우드 컴퓨팅 서비스를 위한 기반 기술들을 분석하고 3장에서는 사용자 인증 정보 관리와 인증 처리 모델을 제안한다. 제안한 모델의 성능 실험 및 분석은 4장에서 논하고 5장에서 연구 결과는 제시한다.

II. Literature Review

1. Cloud Computing

클라우드 컴퓨팅의 인프라는 두 가지로 나눌 수 있다. 대규모 서비스를 제공하는 구글과 아마존은 범용으로 Public Cloud 서비스를 제공하고 있고, 은폐된 서비스를 특정 영역에 제공하는 Private Cloud 형태를 갖는다. 클라우드의 인프라는 Security, App, Solution, IT Management, Server, Storage가 있고, NIST의 클라우드 주요 특성은 다음과 같다[3,4].

- On-demand Self Service: 자동컴퓨팅 서비스 준비
- Broad network access: 플랫폼의 표준 메커니즘
- Resource Pooling: 사용자의 리소스 제어
- Rapid elasticity: 탄력적 특성
- Measured service: 최적화된 투명적 서비스

클라우드 컴퓨팅 서비스 유형으로는 PaaS(Platform as a Service), SaaS(Sofrware as a Service), IaaS(Infrast-ructure as a Service)가 있다[4].

- PaaS(플랫폼 제공): 사용자가 서비스를 개발하여 제공할 수 있다. SaaS보다는 제어 및 관리 권한이 많으며, 제공 시스템의 환경 구성에 대한 관리 권한을 가질 수 있다.
- SaaS(소프트웨어 제공): 네트워크로 연결된 인터넷 서비스를 기반으로 소프트웨어를 임대하여 활용할 수 있도록 서비스를 지원하고 있다. 그러나 제한적인 서비스 제공으로 관리 및 제어가 불가능한 특성을 갖는다.
- IaaS(하드웨어 자원 제공): 하드웨어를 임대하여 서비스를 개발하여 제공할 수 있다. 하드웨어 자원들을 사용자가 관리하고 운영할 수 있다.

클라우드 컴퓨팅 서비스 환경에서의 보안 위협요소를 Gartner, UC Berkely, EINSA에서는 시스템 및 서비스 관리자의 접근 및 통제, 서비스 가용성, 데이터의 기밀성,

시스템 장애, 소프트웨어 라이센싱, 악의적 내부자 등의 사항을 제시하고 있다. 또한 공유 기술의 취약성과 네트워크 서비스 기반에서의 트래픽 하이재킹 등의 IT 전반적인 위협요소가 존재한다.

2. Block Chain

2.1 Block chain introduction

블록체인(block chain security technology)은 데이터를 여러 개의 블록으로 나누어 서로 연결된 형태로 관리하는 기술을 말한다. 블록체인 기술은 중앙집중형 데이터 관리를 분산하여 연계된 데이터를 관리하는 기술로서 데이터의 변조를 방지하고 탈중앙집중 데이터 관리를 추구한다. 이 기술은 중앙집권화된 금융시스템의 위험성을 방지하기 위해 고안된 기술로, 2009년 블록체인 기술을 암호화폐인 비트코인에 적용하여 암호 화폐의 가능성을 보였다. 이러한 블록체인 기술은 택배나 농산물, 부동산, 의료기록 등 다양한 디지털 매체나 물품의 추적 시스템에 활용할 수 있는 기술로서 전 세계적으로 활용 높은 기술로 인정되어 다양한 분야에 적용할 수 있을 것이라는 기대감을 갖는 기술이다[5].

2.2 Block chain technology

블록체인은 세 가지 유형으로 나눌 수 있다. 첫 번째는 개방형으로 누구나 참여할 수 있는 인프라 환경에서 운영되는 Public 블록체인 형태가 있다[5,6].

Public 블록체인은 탈 중앙식 구조로 암호화폐에서 적용되고 있는 기술이다. 네트워크에 참여하고 있는 모든 노드는 모든 거래 정보를 확인할 수 있다. 또한 Pos, PoW 알고리즘에 따라 거래 증명자가 결정되고 거래 속도가 느리고 서비스 확장이 어렵다는 특성을 갖는다. 활용사례는 Open Bazaar DASH, Bitcoin, Ripple, Litecoin, 등이다.

두 번째는 제한된 환경의 인프라를 구축하여 참여자를 제안하는 형태의 폐쇄형 인프라를 제공하는 Private 블록체인이다. Private 블록체인은 Public 블록체인과 반대로 중앙 집중식 구조로서 중앙에서 블록을 관리하고 제어할 수 있는 구조를 갖는다. 그러나 이것은 블록체인의 가장 큰 특징인 탈중앙화의 특징을 갖지 못한다. 서비스 처리 속도가 빠르고 확장성이 용이하다. 활용사례로는 NAS-DAQ, Overstock, Chain 등이 있다.

컨소시엄 블록체인은 Private 블록체인과 Public 블록체인의 중간 형태로 블록 관리 및 제어, 검증을 일부 피어들만 할 수 있다는 것인 특징이다. 장점으로는 거래 속도가 빠르고 서비스 확장이 용이하다. 활용사례는 R3 CEV, HSBC, Citi Barclays, Goldman Sachs, BoA 가 있다. Public 블록 체인, Private 블록체인, 컨소시엄 블록체인은 각각의 특성에 따라 운영환경 및 요구 조건에 맞게 적절하게 적용되어 운용되어야 한다.

그림 1은 블록체인 구조이다. 각 블록은 해쉬값을 활용하여 블록간에 체인으로 연결되어 관리 된다[7].

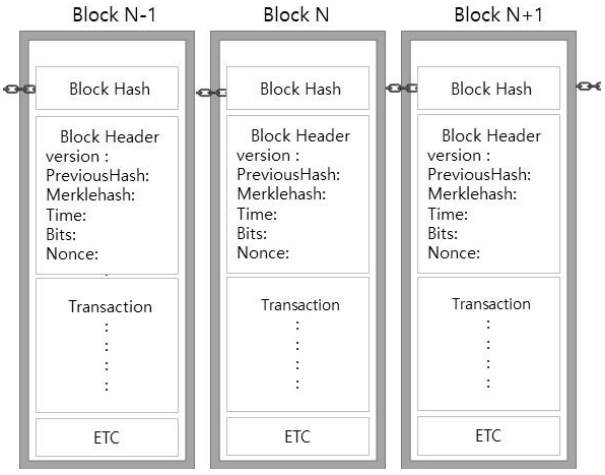


Fig. 1. Blockchain Structure

블록은 블록의 고유 Number(block N), 이전 블록의 Block Hash(block hash N-1), 블록 헤더, 거래 정보(transaction), 기타 정보를 갖는다.

블록 헤더(block header)는 소프트웨어 및 프로토콜의 버전(version), 이전 블록의 해쉬값(previoushash, 첫 번째 블록은 디폴트 값), Tree root에 위치하는 해쉬(merklehash), 블록 생성시간(time), 난이도(bits), 해쉬 검색 계산값(nonce)로 구성된다. 거래 정보는 입금과 출금에 관한 정보를 갖는다. 기타 정보(etc)는 블록의 거래 및 헤더 정보 이외의 정보를 말하며 블록의 해쉬값에 포함되지 않는다. 해쉬 함수 SHA256을 2라운드 운영하여 32byte의 결과값을 갖는다.

분산형 구조의 블록체인은 거래 내역을 모든 참여자가 확인할 수 있어 투명성을 제공하고 분산 DOS(Denial of Service attack) 공격이 불가능하고, 중앙 집중형 보다는 시스템을 구축하고 유지하는데 적은 비용이 든다. 그러나 상대적으로 서비스 속도가 느리고 인증 및 관리를 위한 상호 인터페이스 제어 구조가 복잡하다.

3. Distributed user authentication technology

3.1 DID

DID(Decentralized Identity)는 블록체인 기반 인증서비스이다. 서버 모델들은 사용자 관리를 위해 각 서비스 시

스템마다 개인 식별정보를 기록하고 관리하고 있다[6,7]. 이렇게 등록된 사용자의 개인정보는 사용자 입장에서, 10개의 서비스를 받기 위해 10개의 서버 시스템에 같은 내용의 사용자 개인정보가 저장되어 관리된다. 서비스를 제공하는 서버는 보안이 강화된 시스템도 있고, 그렇지 못한 시스템도 존재할 것이다. 이러한 환경에서 10개의 서버 시스템 중에 하나의 시스템이 악의적인 사용자에 의해 침해를 당했을 때, 침해를 당한 서버뿐만 아니라 다른 9개의 서버에도 침해를 발생시키는 연쇄적인 침해가 발생한다. 이러한 침해 문제를 보완하고자 제시된 모델이 DID이다[8,9].

DID는 사용자의 식별 및 인증 정보를 인증 기관에 등록하고 등록된 사용자에게는 티켓을 발급한다. 발급된 티켓은 블록체인 기술을 활용하여 블록으로 개인 인증 정보를 분산하여 관리한다. 사용자는 서비스를 받기 위한 서버에 접속하여 티켓을 서비스 시스템에 제출하고 서비스 제공 서버는 사용자의 티켓을 블록체인 인증 정보를 조합하여 사용자를 식별하고 무결성을 인증하여 사용자를 인증한다. DID 모델 인터페이스 구조는 그림2와 같다.

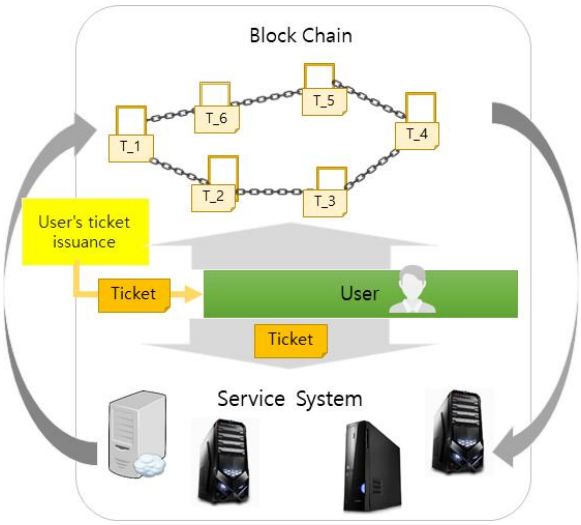


Fig. 2. DID Interface Structure

서비스 제공 서버는 사용자로부터 받은 티켓을 블록체인 서비스 서버에 전송하여 인증하는 방법은 각각의 서비스 서버에 사용자 인증 정보를 저장하고 있지 않아 안전한 서비스 환경을 제공한다. 하지만, 티켓 자체에 대한 공격에 대한 부분은 여전히 안전을 보증하지 못한다.

3.2 Distributed SSO Authentication Technology

분산 SSO(Single Sign On) 인증 기술은 인증 정보를 여러 개의 블록으로 나누어 관리하는 기술이다. SSO는 한 번의 인증으로 여러 시스템 서비스를 활용할 수 있는 기술로서 사용자의 편의성을 제공하는 것이 목적이다. 한 번의 인증으로 여러 시스템을 활용할 수 있다는 것은 보안 입장에서는 위험성이 매우 크다. 침해가 일어났을 경우 여러 시스템이 모두 침해를 당할 수 있는 구조이기 때문이다. 이러한 위험성으로부터 시스템을 보호하기 위해 사용자 인증 정보를 분산하여 관리하고 해쉬값을 활용하여 인증 정보의 무결성을 검증한다. 그림 3은 사용자 인증 정보를 분산 관리하는 SSO 모델이다[3,4].

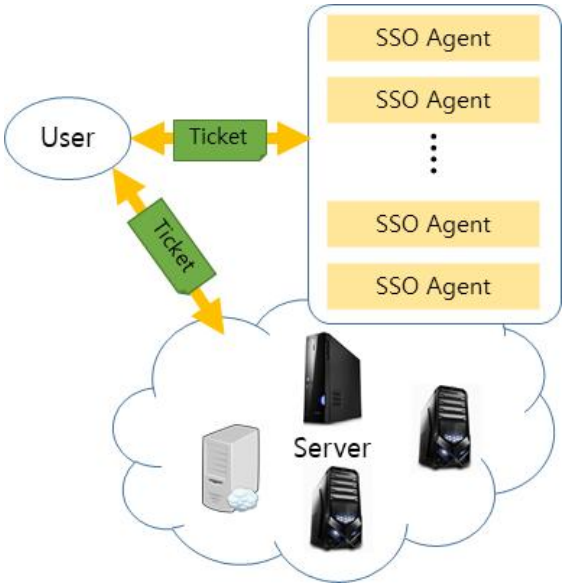


Fig. 3. Distributed SSO Authentication Model

사용자 식별을 위한 인증 정보는 Agent 관리 시스템에 의해 분산하여 SSO Agent에 저장한다. 이렇게 생성된 인증 정보는 티켓으로 생성되어 사용자의 인증 정보로 활용된다. 또한 사용자 인증은 시스템별로 리소스 접근권한에 따른 보안 등급으로 접근을 허용한다. 이러한 서비스는 티켓 레벨에 따라 사용자 시스템 접근허용과 리소스의 접근을 이중으로 제어하여 시스템의 안전하게 보호하고 있다. 분산 SSO 인증 모델의 인증 티켓은 여러 개의 SSO Agent에서 분산하여 관리하고 있다. 분산된 인증 티켓에 대한 보호 및 무결성 인증에 대한 문제가 발생할 수 있다.

III Block chain user authentication technology

1. System Configuration and Introduce

클라우드 컴퓨팅 서비스 환경은 그림 4와 같다.

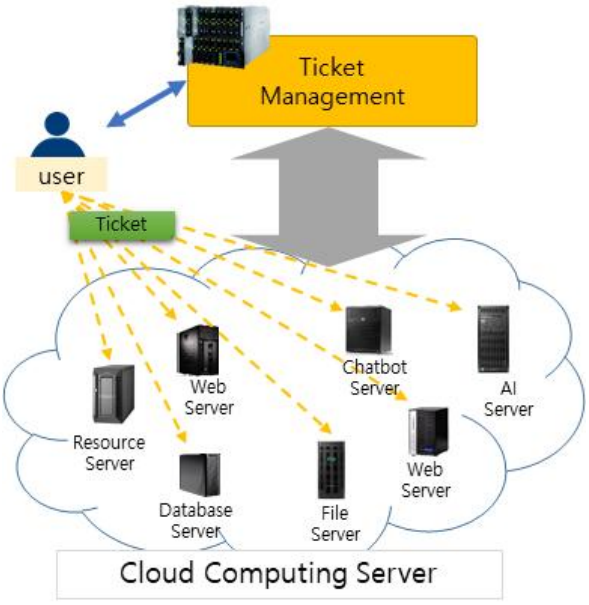


Fig. 4. System Configuration

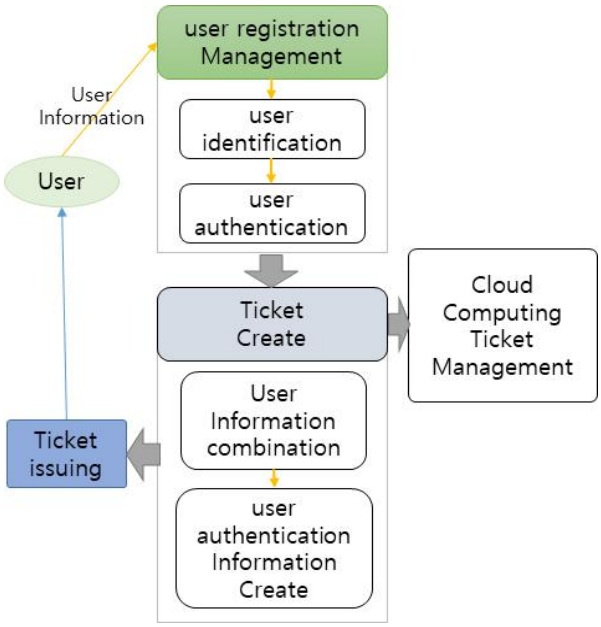


Fig. 5. Ticket Management

사용자는 티켓 관리 서버로부터 사용자 식별 및 인증을 위한 정보를 등록하고 티켓을 발급받는다. 발급받은 티켓은 클라우드 컴퓨팅 서버의 각 서비스에 제출하여 사용자 인증을 받는 구조이다.

- User: 클라우드 컴퓨팅 서비스 사용자
- Ticket Management: 클라우드 컴퓨팅 사용자를 식별하고 인증하는 정보를 관리하는 시스템으로 사용자별 고유 티켓 발급
- Ticket: 사용자의 식별 및 인증을 위한 고유 정보
- Cloud Computing Server: 네트워크 환경에서 클라우드 컴퓨팅 서비스를 제공하는 서버

2. Ticket Management System

티켓 관리 시스템은 클라우드 컴퓨팅 서비스를 사용할 수 있는 티켓을 관리한다. 클라우드 컴퓨팅 서비스를 활용하고자 하는 사용자는 티켓 발급을 신청하여 유효한 티켓을 발급받는다. 관리 시스템은 사용자 식별을 위한 개인정보를 등록하고 관리한다. 등록된 사용자의 정보를 활용하여 사용자별 고유 티켓을 생성한다. 티켓 생성 및 관리는 그림 5와 같다.

사용자는 사용자 식별을 위한 정보를 티켓 관리시스템에 전송한다. 관리 시스템은 두 개의 영역으로 사용자 인증 및 티켓발급 과정을 처리한다.

- User registration management
  - User identification: 사용자 개인정보를 식별
  - User authentication: 사용자의 식별정보를 통해 사용자를 인증
- Ticket Create
  - User information combination: 티켓 생성을 위한 사용자 정보 조합
  - User authentication information create: 사용자의 고유 티켓 생성

전송된 정보는 사용자 등록을 위해 사용자 식별정보를 통해 인증하고 인증된 사용자에게는 사용자의 고유 티켓을 발급한다.

3. Ticket Create

티켓은 사용자의 식별을 위한 고유 정보와 클라우드 서비스 서버에서 발급하는 일련번호로 생성된다(그림 6). 사용자 식별정보는 사용자의 비밀키와 개인정보를 활용한다. 클라우드 서버에서 생성한 일련번호는 각 클라우드 서비스를 제공하는 서버에서 사용자 식별을 위한 고유 일련번호를 생성하여 티켓 관리 시스템에 전송한다. 전송된 고유 일련번호는 클라우드 서비스마다 고유 정책으로 중복성이 없는 식별 코드이다.

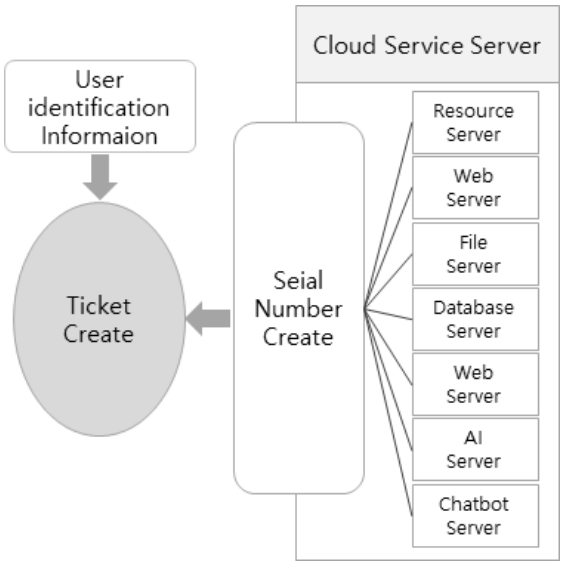


Fig. 6. Ticket Create

사용자의 정보와 클라우드 서비스 제공 서버에서 생성된 고유 번호는 해쉬 함수(SHA256)로 체인을 형성한다. 그림 7과 같이 사용자가 활용하는 클라우드 서비스 목록에 따라 각 클라우드 서버는 고유 일련번호를 생성하여 티켓 관리 서버에 전송한다. 이렇게 전송된 정보는 사용자 정보와 함께 티켓을 생성한다.

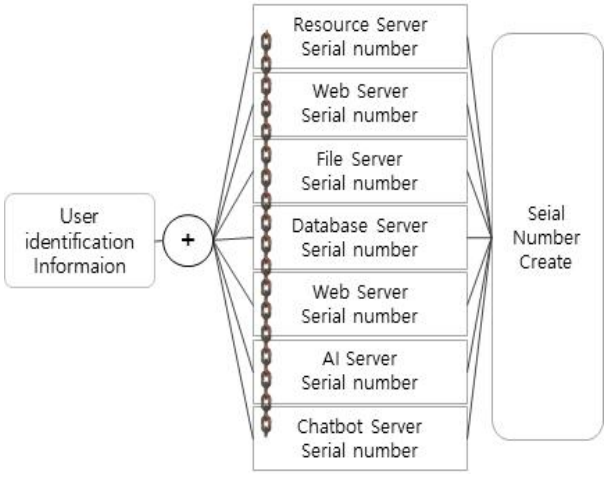


Fig. 7. Ticket creation process

티켓은 일련번호, 사용자의 기본 정보, 해쉬값, 클라우드 서비스 번호, 접근 및 기타 정보를 포함한다. 티켓의 구조는 그림 8과 같다.

Ticket #N	Ticket #N+1	Ticket #N+2
User Information	User Information	User Information
32Byte Hash(N-1)	32Byte Hash(N)	32Byte Hash(N+1)
Cloud Service Resource Service Name	Cloud Service Web Service Name	Cloud Service File Service Name
Access and etc Information	Access and etc Information	Access and etc Information

Fig. 8. Ticket Structure

티켓은 사용자가 클라우드 서비스 활용 가능한 목록에 따라 서비스 티켓이 생성된다. 생성된 클라우드 서비스별 블록은 해쉬 함수에 의해 해쉬값을 생성하고 이전에 생성한 블록의 해쉬값을 포함한다. 즉, “Ticket #N”은 이전에 생성된 “Ticket #N-1”의 해쉬값을 포함하고 블록 “Ticket #N+1”은 “Ticket #N”의 해쉬값을 포함하여 체인을 형성하고, 첫 번째 블록의 티켓 해쉬값은 마지막에 생성된 블록의 해쉬값을 갖는다. 이렇게 만들어진 블록체인은 사용자의 티켓으로 발행된다.

4. Ticket Processing

티켓 관리 시스템에 티켓 발급을 요청한 사용자는 사용자 등록 정보를 전송하고 클라우드 서비스 활용을 위한 보안 패킷 요청한다. 패킷은 다음과 같다.

• User_Ticket Request

{User_information, Section_Key, Authentication_Key, TS}

- Uer_information(사용자 정보), Section_Key(보안 통신을 위한 세션 키), Authentication_Key(사용자 고유 인증 키), TS(Time Stamp)

티켓 관리 시스템에서 생성한 티켓은 사용자 요청에 따라 다음과 같이 패킷을 생성하여 사용자에게 전송한다.

• User_Ticket Response

{Service Number || EA(KA||Section_Key||TS || TicketSK) || Ticket}

- EA/KA(User Encryption Key), Section_Key(보안 통신을 위한 세션 키), TS(Time Stamp), TicketSK(Ticket Access Key), Ticket(User Authentication Ticket)

이렇게 전송된 패킷을 클라우드 컴퓨팅 서비스를 제공하는 서버에 전송되고 클라우드 서버는 티켓을 확인하고 체인으로 연결된 블록을 확인하고 클라우드 서비스를 제공한다.

IV. Proposal system analysis

제안 기술 분석을 위해 일반적으로 활용되고 있는 사용자 ID와 패스워드를 활용한 시스템 접근과 SSO 기술을 활용한 영역으로 기술을 비교 분석한다.

첫 번째로 ID와 Password를 활용한 시스템 접근 방법이다. 사용자의 ID와 패스워드 관리는 사용자 영역과 클라우드 서버 영역으로 나눌 수 있다. 사용자 영역에서 사용자의 미비한 보안 관리로 발생할 수 있는 패스워드 누출의 위험성을 가지고 있고, 서버 또한 외부의 침입으로 정보가 침해당할 수 있는 환경을 제공한다. 사용자의 미숙한 패스워드 관리는 클라우드 서버의 전체적인 위협을 발생시키기도 한다. 그러나 티켓을 활용한 기술은 티켓 자체에서 패킷 보호 기술을 제공하여 사용자의 미숙한 관리에도 안전성을 제공한다. 또한 클라우드 서버에서도 침해가 발생해도 사용자 정보의 변형을 막을 수 있는 블록 체인 기술을 활용하여 무결성을 보증할 수 있다.

두 번째로 SSO 서비스 환경과 비교한다. SSO는 한 번의 인증으로 여러 시스템을 활용할 수 있는 기술이다. 한 번의 인증된 사용자는 인증 세션을 활용하여 다중의 클라우드 서비스를 활용할 수 있다. 이것은 사용자의 인증 정보가 유출되었을 때, 다중의 클라우드 서버가 침해를 당할 수 있는 환경을 의미한다. 블록 체인을 활용한 제안 기술은 티켓별 클라우드 인증 영역의 정보를 따로 구분하여 인증 서비스를 제공한다. 그림 9와 같이 클라우드 웹 서비스를 제공하는 서버의 사용자 정보가 유출되었을 때, 침해된 정보로 데이터베이스 클라우드 서버를 공격할 수는 없다. 즉, 웹 서버에서 사용되는 사용자의 인증 데이터와 데이터베이스에서 사용되는 인증 데이터는 다르기 때문이다. 이것은 사용자가 웹서버에 접근할 때, 사용자의 모든 티켓 정보를 웹서버에 제시하는 것이 아니라, 웹서버에서 인증받을 수 있는 “Ticket #1”만 제시하기 때문에 가능하다. 또한, 클라우드 웹 서버는 티켓 인증을 위해 사용자의 식별정보와 티켓 정보를 티켓 관리 시스템에 전송하여 티켓의 유효성을 인증하여 서비스를 제공한다.

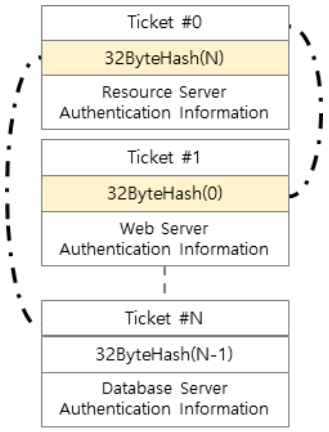


Fig. 9. Block Chain

제안 기술과 기존 기술을 비교 분석을 정리하면 표 1과 같다.

Table 1. Comparison analysis

Access / Field	ID /Password	SSO	Proposal Model
Information leakage	Impact on users and cloud service servers	Affects all servers associated with the user	Only compromised cloud servers are affected
Forgery of information	○	○	Immutable by connecting to the service blockchain
Convenience	Multiple services require login every time	Multiple services can be used with one authentication	Multiple services can be used with one authentication
User management on the server	○	○	X
Safety in case of ticket leakage	X	X	△

V. Conclusions

본 논문은 클라우드 서비스를 안전하고 효율적으로 활용할 수 있도록 사용자 인증 정보를 블록 체인으로 연결하여 관리하는 기술을 제안하였다. SSO처럼 한 번의 인증으로 다중의 서비스를 활용할 수 있는 환경에 유용하도록 각

서비스별 블록을 생성하고 서비스 블록을 체인으로 연결하여 사용자의 인증 정보를 보호하였다.

제안 기술은 블록 체인 기술의 인증 정보의 무결성을 보증하고 Private 블록 체인과 같이 사용자의 정보를 보호하여 무결성 서비스를 제공하였다. 티켓 발생시에만 중앙집중식 시스템 운영으로 시스템 부하를 줄이고 티켓의 안전한 관리를 위해 보안 서비스를 운영하였다. 블록 체인을 활용한 사용자 인증 모델은 사용자에게는 편의성을 제공하고 클라우드 서버측면에서는 효율적인 사용자 인증 관리를 하여 안전한 네트워크 클라우드 컴퓨팅 서비스를 제공하도록 하였다.

그러나 티켓 자체에 대한 유출은 표면적으로 기존 사용자 인증 영역에서 발생하는 시스템 침해에 문제를 가지고 있으나, 네트워크 보안 세션 운영으로 보호하여 시스템 안전성을 유지할 수 있을 것으로 본다.

ACKNOWLEDGEMENT

The Work was supported by Jangan University Research Grant in 2020.

REFERENCES

[1] Jae-Young Moon, Cloud Computing Trend and Future Directions, The Korea Contents Association Review, Vol. 17, No. 1, pp. 23-26, Mar. 2019.

[2] Un SungKyong, Cloud Computing Security Technology Trend, Korea Institute Of Information Security And Cryptology, Vol. 20, No. 20, pp.27-31, April. 2010. DOI:10.9708/jksci.2015.20.7.049

[3] Min-Hee Cho, Eun-Gyeom Jang, Yong-Rak Choi, User Authentication Technology using Multiple SSO in the Cloud Computing Environment, Journal of the Korea Society of Computer and Information, Vol 21 No. 4, pp. 31-38, April. 2016. DOI:10.9708/jksci.2016.21.4.031

[4] Eun-Gyeom Jang, A Enhanced Security Model for Cloud Computing in SSO Environment, Journal of the Korea Society of Computer and Information. Vol. 22, No. 8, pp. 55-61, Aug. 2017. DOI:10.9708/jksci.2017.22.08.055

[5] Ye-Ryoung Suh, Sung-Hwan Park, Dong-Jun Choi, Jae-Woo Lee, Blockchain security issues and the latest robust blockchain technology, Communications of the Korean Institute of Information Scientists and Engineers, Vol. 38, No. 7, pp. 14- 18, July. 2020.

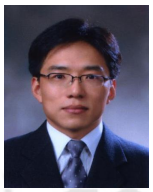
[6] HAN Ho Hyeorn, Authentication for Blockchain Service Communications of the Korean Institute of Information Scientists and Engineers Vol. 38 No. 7, pp. 19-24, July. 2020.

[7] Jinho Yoo, A study on Applying Privacy by Design in Blockchain Services, Communications of the Korean Institute of Information Scientists and Engineers, Vol. 38, No. 7, pp. 32-39, July. 2020.

[8] Ju Min Cha, Jeong Gyu Kim, Yong Yook Kim, Moo Hyun Lim, Woosaeng Kim, Blockchain-Based Pet Trade Service DApp, Journal of Information Technology Applications & Management, Vol. 26, No. 6, pp.79-87, Dec. 2019. DOI:10.21219/jitam.2019.26.6.079

[9] Baek, YeongTae, Min Youn A, A study on DID self-sovereign identity for digital content management, Proceedings of the Korean Society of Computer Information Conference. Vol. 28, No. 2, pp 395-396, July. 2020.

Authors



Eun-Gyeom Jang received a Ph.D in Daejeon University in 2007. He is currently a Professor in the Department of Internet Communication Jangan University. It has an interest in mobile communications, system security and Computer Forensics.