JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 29 No. 11, pp. 209-216, November 2024
https://doi.org/10.9708/jksci.2024.29.11.209

A Study on Cloud Redundancy for Secure Digital Content Services

Eun-Gyeom Jang*

*Professor, Dept. of Software Convergence, Jangan University, Hwaseong, Korea

[Abstract]

In This paper, we proposed a technology to provide safety and convenience for cloud computing services. The proposed technology strengthens user authentication for the safe service of digital content in a cloud computing environment and proposes a technology to prevent packet infringement on the network. For user authentication, a dual authentication method and an access medium authentication method were applied, and a secure service was provided through session authentication to protect packets on the network. Real-time synchronization between systems as a cloud system's multiplexed service method ensures smooth service is always supported in the event of a system failure. The proposed user authentication technology prevents illegal user access and enables management by access license with the system simultaneous access user management function. Authentication session tickets of authenticated users provide convenience in system access and service use during the validity of the ticket, and packet infringement prevention functions.

▸ **Key words**: User authentication, Packet protection, Multiplexing system, Cloud computing, Routing service

[요　　약]

본 논문은 클라우드 컴퓨팅 서비스를 안전성과 편의성을 제공하기 위한 기술을 제안하였다. 제안 기술은 클라우딩 컴퓨팅 환경에서 디지털콘텐츠의 안전한 서비스를 위해 사용자 인증을 강화하고 네트워크상에서의 패킷 침해 방지를 위한 기술을 제안하였다. 사용자 인증은 이중 인증 방식과 접속 매체 인증 방식을 적용하고 네트워크상에서의 패킷 보호를 위해 세션 인증을 통해 안전한 서비스를 제공하도록 하였다. 클라우드 시스템의 다중화 서비스 방식으로 시스템간의 실시간 동기화로 시스템 장애 발생시, 언제나 원활한 서비스가 지원되도록 하였다. 제안한 사용자 인증 기술은 불법 사용자의 접속을 방지하고 시스템 동시 접속 사용자 관리기능으로 접속 라이선스별로 관리가 가능하도록 하였다. 인증된 사용자의 인증 세션 티켓은 티켓의 유효기간 동안 시스템 접속 및 서비스 이용의 편의성, 패킷 침해 방지 기능을 제공한다.

▸ **주제어**: 사용자 인증, 패킷 보호, 다중화 시스템, 클라우드 컴퓨팅, 라우팅 서비스

• First Author: Eun-Gyeom Jang, Corresponding Author: Eun-Gyeom Jang
*Eun-Gyeom Jang (jangeg@jangan.ac.kr), Dept. of Software Convergence, Jangan University
• Received: 2024. 10. 15, Revised: 2024. 11. 04, Accepted: 2024. 11. 06.

I. Introduction

다양한 문화 콘텐츠가 오프라인 서비스에서 온라인 서비스로 전향되고 있다. 넷플릭스, 티빙, 쿠팡플레이, 디즈니+, 웨이브 등에서 제공하는 영화 및 문화 영상 콘텐츠 서비스가 대표적인 온라인 문화 콘텐츠 서비스라 할 수 있다. 이러한 접근성은 유·무선 네트워크 기반의 정보통신 기술의 발달로 언제나 접근할 수 있는 환경과 편의성을 제공하기 때문이다. 또한 관공서 및 기업의 정보 서비스 시스템은 기관 자체의 로컬 시스템 구축에서 클라우드 컴퓨팅 환경으로 서비스가 변화하고 있다[1].

이러한 시스템 및 서비스 환경의 변화는 빠른 네트워킹 기술과 이동 매체 서비스의 발달로 다양한 분야로 활성화되고 있다. 또한 기술적인 측면과 더불어 시스템 구축 비용에 효율성을 제공한다. 정보시스템은 서버 구축시, 수천에서 수 억원에 달하는 장비이지만 빠른 기술의 발달로 수년이 지나면 속도 및 성능, 새로운 서비스를 제공하지 못하여 주기적으로 고가의 장비를 교체해야 한다.

기관 자체의 로컬 시스템 구축은 외부의 접근성으로부터 내부 정보를 보호한다는 의미로 안전성을 제공한다고 하지만 위험성은 항상 존재한다. 클라우드 컴퓨팅은 외부 관리 업체에 내부 정보를 보관하고 관리한다는 것은 정보보안 측면에서 높은 위험성을 갖는다. 이러한 이유로 클라우드 컴퓨팅 서비스의 장점에 비해 대중화된 서비스 활성화가 부족한 것이 현실이다. 최근 MS사의 클라우드 컴퓨팅 서비스가 장애가 발생하여 항공사 예약시스템이 작동되지 못하는 사례가 발생하였다. MS 클라우드 서비스를 이용하는 몇몇 항공사의 항공 운항에 문제가 발생하여 항공 지연 및 운항 취소, 오프라인 수속 절차로 많은 불편함이 있었다.

이러한 클라우드 서비스 장애로부터 원활한 클라우드 컴퓨팅 서비스를 제공하기 위해 디지털콘텐츠 제공 서비스 기반 환경에서 클라우드 다중화 기법으로 안전한 서비스를 제공하고자 한다. 본 논문의 구성을 2장에서 클라우드 서비스와 디지털콘텐츠 관리 기술을 소개하고 3장에서 클라우드 다중화 기법을 제시한다. 4장에서는 제안 기법을 분석하고 5장에서 결론으로 논문을 마무리한다.

II. Literature Review

1. Cloud Computing

1.1 Cloud Service

클라우드 컴퓨팅 서비스는 네트워크 환경의 이동 매체를 포함한 유·무선 네트워킹 연결 매체에 접근성을 높이고 시·공간에 영향을 받지 않아 서비스 접근의 효율성과 편의성을 제공한다. 클라우드 컴퓨팅 시장은 점진적으로 성장하고 있으며 소프트웨어(SaaS)와 서비스형(IaaS) 인프라를 통해 아마존, 구글, 알리바바, MS 등이 빠르게 성장하고 있으며 빅데이터, 핀테크, 인공지능, IoT 등의 다양한 신기술과 융합된 서비스를 제공하고 있다.

Public 클라우드는 대규모 컴퓨팅 서비스로 구글과 아마존이 대표적이다. 구글 드라이브, Mybox(네이버), Dropbox, 아마존 드라이브, Megacloud는 스토리지 클라우드 서비스를 제공한다[2]. Private 클라우드는 비밀성을 요구하는 서비스에 적합하며 사용자가 컴퓨팅 서비스 인프라 구조로서 관리하고 유지하여 보안성이 높다. 이에 대한 NIST 전문성의 주요 특성은 다음과 같다[1,3].

- (자동 서비스) 자동 서비스 준비
- (범용적 네트워크 접근) 사용자 플랫폼 표준메커니즘
- (리소스 폴링) 권한이 높은 사용자를 위한 리소스 제어
- (탈력적인 서비스) 서비스의 탄력성
- (자원 활용 최적화) 투명한 서비스의 최적화

NIST는 범용적인 환경, 투명한 서비스, 최적화된 정보 및 사용자 접근성, 용이성을 제공하고 정보의 보안 접근성의 특성을 갖는다. 클라우스 컴퓨팅 서비스는 3가지로 분류할 수 있다[4,5]. 첫째, 서비스로 제공되는 소프트웨어(SaaS, Software as a Service)는 가장 일반적인 컴퓨팅 서비스로 플랫폼 기반의 인프라를 제공하고 운영체제 및 웹에서 제공하는 애플리케이션 서비스로서 도롭박스, G-메일 등을 들 수 있다. 웹에서 범용적 서비스를 제공하여 환경 관리 서비스를 제공할 수 있다. 둘째, 서비스로 제공되는 플랫폼(PaaS, Platform as a Service)은 애플리케이션을 실행할 수 있는 플랫폼과 플랫폼에서 실행되는 응용 프로그램이 작동될 수 있도록 언어 및 도구 등의 자원을 제공하여 기관 및 기업에서 큰 비용 없이 개발하고 운영할 수 있도록 한다. 시스템의 운영체제나 스토리지 제어 권한은 없으나 호스팅한 애플리케이션의 환경 구성과 관리 권한을 갖는다. 셋째, 서비스로 제공되는 인프라스트럭처(Iass, Infrastructure as a Service)는 가상의 인프라 서비스를 제공한다. 서버의 자원, IP, 네트워킹, 스토리지 등의 서비스를 제공하여 직접 서버를 구축하지 않고 가상 시스템 환경을 구축할 수 있도록 하여 관리 및 구성 비용을 줄여준다. 추가로 서비스로 제공되는 기능(FaaS, Function as a Service)은 컨테이너에서 실행되는 이벤

트 기반 실행 모델로서 Server less 컴퓨팅을 구현하는 방식의 서비스이다. DaaS(Database as a Service)는 데이터베이스 서비스로 자료 공유 서비스를 제공한다. BaaS(Blockchain as a Service)는 블록체인 기술을 기반으로 정보의 무결성과 불변성 서비스를 제공하는 물류 유통 관리에 적합하다[1,2].

1.2. Cloud Security Threats

CSA(Cloud Security Alliance)에서는 보안 인증 및 사용자 교육 서비스 영역에서의 클라우드 컴퓨팅의 보안 위협을 다음과 같이 분류하고 있다[2,6].

- 위협 1: 클라우드 컴퓨팅의 오용 및 비합리적 사용
- 위협 2: 불안정한 애플리케이션 프로그래밍 인터페이스
- 위협 3: 내부자의 악의성
- 위협 4: 서비스 환경 및 공유 기술
- 위협 5: 자료 손실 및 손상
- 위협 6: 계정 및 서비스 하이재킹
- 위협 7: 알 수 없는 새로운 위험 프로파일

클라우드 서비스는 외부의 보안 위협으로부터 안전하게 애플리케이션 및 시스템 서비스가 제공되어야 하고, 권한이 없는 사용자로부터 시스템 및 서비스 접근이 제어되며 네트워크 기반의 서비스로서 안전한 세션 관리와 원활한 서비스가 제공되어야 한다. 클라우드 서비스에 대한 장애 및 침해 사례로는 스토리지 및 서비스 장애에 의한 정보 유출과 접근성의 문제, 구글의 지메일의 보안 문제, 소니의 개인정보유출을 발생시킨 엔터테인먼트 공격, Capital One, 혼다 자동차의 민간 정보 유출, AWS DNS 및 시스템 장애 등이 있다[5,7].

이러한 시스템 접근성의 사용자 인증을 위해 이중 인증 방식을 활용한다. SMS 문자 인증과 다중 인증(MFA) 방식을 사용하지만, 세션 가로채기 및 로컬 시스템 쿠키로 인한 사용자 접속 정보를 활용한 침해가 발생하기도 한다. 네트워크 환경에서 제공되는 클라우드 컴퓨팅 서비스는 네트워크상에서 발생하는 클라이언트와 서버간의 통신 및 운영체체간의 통신 구성요소 취약점 등 하이퍼바이저 취약점을 갖는다. 이러한 위험성으로부터 시스템 및 서비스를 보호하기 위해 방화벽, 인증, 권한 관리, 세션 관리기능을 활용하여 클라우드 컴퓨팅 서비스를 각 서비스 업체에서 선보이고 있다[7,8].

2. Digital Contents Service

2.1 Digital Rights Management

유•무선 네트워크의 발달은 디지털장비에서 활용되는 디지털콘텐츠 서비스를 공급자와 사용자간에 네트워크 기반 실시간 인증 서비스를 제공하는 환경 변화를 일으켰다. 기존 오프라인 기반의 라이센서 인증은 무단 복제의 불법성이 존재하여 콘텐츠 공급자와 제작자에게 저작권 및 상업적 불이익을 가져오는 결과를 초래하기도 하였다. 하지만 네트워크 기반의 인증 기술을 활용하여 실시간 사용자 및 기기 인증 서비스로 사용자를 식별하고 기기 인증으로 세션을 관리하고 있다. 현재 네플릭스, 쿠팡플레이, 티빙, 웨이브, 디즈니플러스 등에서는 여러 기기에서 동시 접속하여 사용자 인증 및 관리를 실시간으로 감시하여 서비스를 제공한다.

디지털콘텐츠 불법유통은 공급자에게는 사용 인증이 되지 않은 사용자의 불법 사용으로 경제적 손해와 저작자의 저작권을 침해하는 지적재산권의 문제를 발생시킨다. 이러한 디지털콘텐츠의 위험 요소로부터 디지털콘텐츠를 보호하기 위해 워터마킹, 핑거프린팅, CAS(Conditional Access System), DRM(Digital Right Management) 등이 활용된다. CAS는 방송 환경에 적합하게 사용되지만 클라우드 컴퓨팅 서비스에는 환경적인 보완 요소가 존재한다. 또한 기존 DRM 및 워터마킹 기술은 다양한 이동통신 매체에서의 접근성 및 활용성 등의 서비스로 침해 및 보안 위험성이 있다[1,9].

저작자의 정보를 콘텐츠에 삽입하는 워터마킹과 DOI (Digital Object Identifier)는 저작권을 보호하고 INDECS (Interoper ability of Data in E-Commerce System)은 정형화된 콘텐츠를 제공하여 효율적 콘텐츠 관리를 할 수 있도록 한다[1,7,10]. DRM은 디지털콘텐츠의 안전한 유통 구조를 제공하여 인증된 사용자만이 콘텐츠를 접근할 수 있도록 기술 및 절차, 정책, 알고리즘 등을 포함한다. DRM 기술을 정리하면 표1과 같다.

디지털콘텐츠 보호를 위한 기술을 크게 2개의 영역으로 나눌 수 있다. 콘텐츠 자체에 대한 생성자의 권익 보장을 위한 기술과 유통시 안전한 보급 및 접근 관리이다. 콘텐츠 자체에 대한 위험성은 불법 복제 및 수정의 침해와 유통시 인가되지 않은 사용자의 오용 및 불법 접근이다. 하지만, 콘텐츠 서비스 장애도 침해의 위험성에 포함되어야 한다. 본 논문에서는 클라우드 환경에서 디지털콘텐츠 서비스를 위한 위험 요소를 제거하고 원활한 콘텐츠 서비스가 제공될 수 있도록 서버 관리 및 운영 기법을 제안한다.

Table 1. DRM technology

Item	Description
Contents Encryption	Application of encryption/decryption algorithms and secure key management technology to protect digital content itself
Usage Rule	Application and control of various rights by contents provider
Persistent Protection	Protection of user rights, such as continuous control of the distribution process, change and reproduction of content rights, etc
Trusted Environment	Content authentication and authentication procedures, integrity and reliability authentication of content
Super Distribution	Content management and user accessibility service delivery distribution technology
Value-chain Support	Value-chain Technology for Systemization of Distribution Structure of Content

III. The Proposed Scheme

1. System Configuration and Environment

제안시스템은 디지털콘텐츠를 클라우드 컴퓨팅 기반으로 서비스를 제공하는 환경이다. 클라우드는 다중서버로 운영되어 두 개의 실시간 백업 및 동시 운영 모드로 구성된다. 클라우드 라우팅 시스템은 트래픽 및 시스템 상태(장애) 상태에 따라 라우팅 서비스를 제공한다. 사용자 접근 매체는 모바일 및 유•무선 네트워크의 다양한 환경의 서비스 접근 환경이다. 시스템 구성 환경은 그림1과 같다.

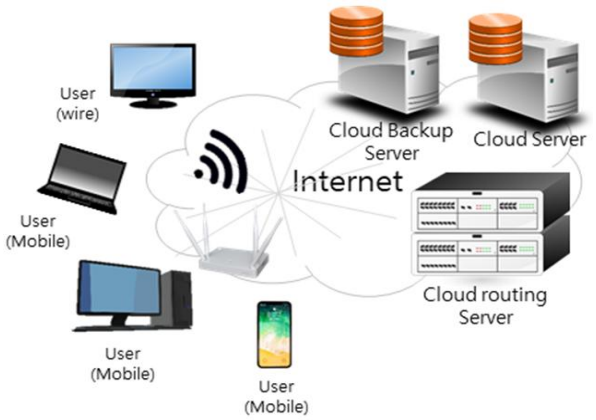

Fig. 1. System Configuration and Environment

2. Digital Contents Management

디지털콘텐츠 관리를 위한 정보로는 소유권자, 제작일, 유효기간, 콘텐츠 등급, 콘텐츠 분류, 콘텐츠 타입, 출처, 핑거프린팅, 서비스 방법, 기타 정보를 갖는다.

- 소유권자: 콘텐츠 저작자로부터 위임 및 저작권(소유권)을 갖는 권한자
- 제작일: 콘텐츠 생산자의 권한 입증을 위한 등록일(유사 콘텐츠 최초 저작권 입증 정보)
- 유효기간: 콘텐츠 공급업체에 유통 기간을 설정, 계약상의 유통기간
- 콘텐츠 등급: 콘텐츠 배포 연령 등급
- 콘텐츠 분류: 액션/애니/SF/드라마/시리즈/공포/애로/환타지/문화 등 콘텐츠 종류
- 콘텐츠 타입: 콘텐츠 종류(이미지, 영상, 텍스트, 음악)
- 출처: 콘텐츠 유효기간의 공급자 정보
- 핑거프린팅: 사용자 로그 기록
- 서비스 방법: 스트링 및 다운로드
- 기타: 서비스 활용 및 추가 정보

3. User Certification Process

클라우드 디지털콘텐츠 서비스는 시스템 및 콘텐츠 접근 제어 기능을 제공한다. 사용자 및 시스템 인증 서비스는 그림2와 같다.

사용자는 시스템 로그인으로 시스템에 접근한다. 사용자의 인증 정보는 사용자 인증 서버(user authentication server)에서 인증하고 인증된 사용자는 사용자 권한 관리(user rights management)에서 사용자 등급별 인증 세션을 발급한다. 발급된 인증 세션(certification section) 티켓은 유효성을 갖고 콘텐츠 서버에 접근을 허용한다. 접근이 허용된 사용자는 트래픽 및 장애 등의 네크워크 및 시스템 상황에 따라 사용자가 연결할 클라우스 시스템을 선택하여 서비스를 제공한다.

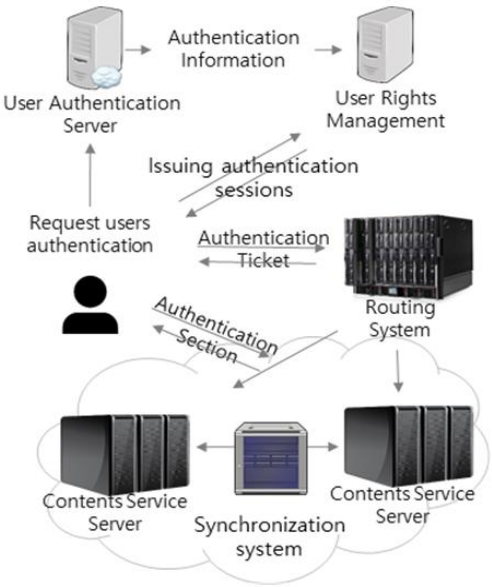

Fig. 2. Users and System Certification

3.1 User Authentication

사용자는 클라우드 시스템에 접속하기 위해 사용자 인증 절차를 갖는다. 사용자는 사용자 고유 인증 정보를 사전에 등록하고 등록된 정보로 자동 세션 연결 및 인증 강화 정책을 적용한다. 고유 인증 정보는 사용자의 고유 ID와 패스워드가 기본정보이다. 추가 이중 인증을 위한 이메일과 SMS 인증 절차로 보안을 강화한다. 또한 접근의 편의성과 사용자 인증을 보완하기 위해 시스템 인증 정보를 추가한다. 사용자 인증 정보를 정리하면 다음과 같다.

{User ID||Password||E-Mail/Phone Number ||System Information List|| etc}

- User ID/Password - 기본 사용자 식별 및 인증 정보
- E-Mail/Phone Number - 사용자 인증 이중화를 위한 E-Mail 인증, Phone SMS 인증
- System Information List - 클라우드 시스템 접속 장치 관리

초기 사용자 인증은 사용자 고유 정보를 인증하고 인증된 사용자는 이중 인증(E-Mail/SMS)으로 사용자를 인증한다. 사용자의 접속 매체 인증인 System Information (System Mac Address)는 기기의 고유 네트워크 장치 식별정보로서 사전에 등록한 기기임을 인증한다.

3.2 User Rights Management

인증된 사용자는 사용자 라이선스 권한 영역을 확인하여 정당한 접속 여부를 확인하고 클라우드 시스템에 접속할 수 있도록 인증 세션을 발급한다. 사용자 권한 관리 시스템은 클라우드 시스템에 접속할 수 있도록 사용자의 라이선스 계약 및 등급을 확인하고 인증 세션을 발급한다. 사용자 라이선스 등급은 사용자 등급에 따란 동시 무한 접속 허용 및 동시 접속 허용 개수 등의 동시 접속 및 접속 매체 관리기능을 제공한다. 사용자 권한 인증 처리 절차는 그림 3과 같다.

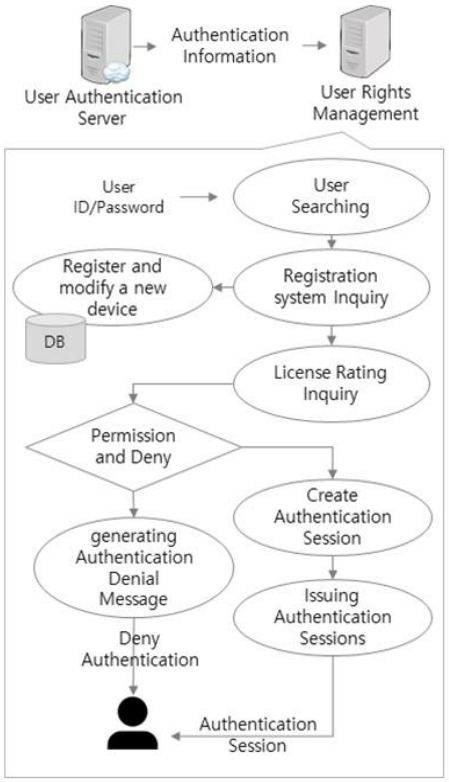

Fig. 3. User Rights Authentication Procedure

사용자가 정당한 사용자임을 인증하고 라이선스 권한 영역에서의 접근 허용 인증은 그림 3과 같이 처리된다.

(1) (*User Searching*) 정당한 사용자를 식별(추출)한다.
(2) (*Registration system Inquiry*) 사용자가 클라우드 시스템에 접속할 매체(MAC)를 조회하여 등록된 매체인지를 확인한다.
(3) (*Register and modify a new device*) 등록된 매체가 아닐 경우, 매체 등록 허용범위 개수내에서 등록할 수 있도록 하고, 초과시 기존 매체를 수정할 수 있도록 한다.
(4) (*License Rating Inquiry*) 라이선스 허용 범위를 조회한다.
(5) (*Permission and Deny*) 사용자 세션 인증 허용 및

거부를 판단한다.

(6) (*Create Authentication Session*) 인증 세션을 생성한다.

(7) (*Issuing Authentication Sessions*) 인증 세션을 사용자에게 발급한다.

(8) (*Generating Authentication Denial Message*) 세션 인증 거부 메시지를 생성하여 사용자에게 전송한다.

3.3 Cloud Computing Processing

인증된 사용자는 클라우드 서비스 시스템 접근을 허용한다. 라우팅 시스템은 사용자를 식별하고 사용자에게 원활한 클라우드 컴퓨팅 서비스를 제공하기 위해 최적의 클라우드 서비스 시스템을 제공한다. 그림 4는 최적의 클라우드 서비스를 제공하기 위한 시스템 프로세스이다.

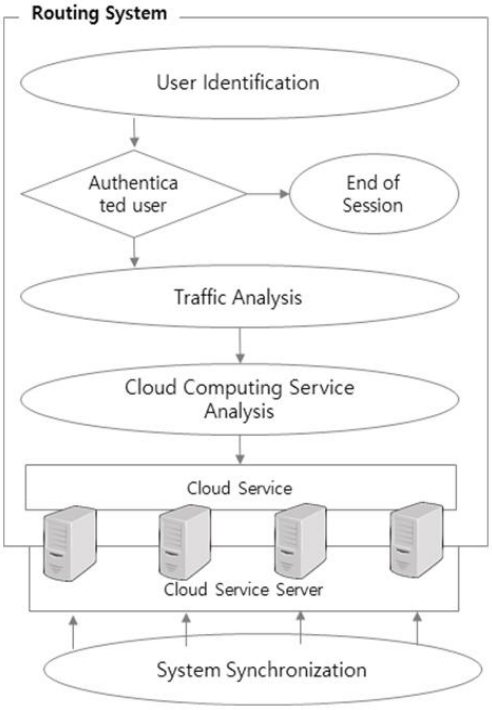

Fig. 4. Cloud Computing Processing

(1) (User Identification) 사용자를 식별한다.

(2) (Authenticated user) 인증된 사용자를 식별한다.

(3) (Traffic Analysis) 접속 매체의 종류 및 접속 정보, 네트워크 트래픽을 분석한다.

(4) (Cloud Computing Service Analysis) 클라우드 컴퓨팅 서버의 상태 정보를 분석하고 트래픽 및 장애 상태를 체크하여 최적의 라우팅 경로를 제공한다.

(5) (Cloud Service) 요청 클라우드 서비스에 적절한 서비스를 제공한다.

(6) (System Synchronization) 사용자 정보 및 서비스 관리 정보의 변화에 다중의 클라우드 컴퓨팅 서버에 데이터 동기화를 실행한다.

4. Analyzing the Proposition Technology

4.1 User Authentication and Convenience Service

사용자 인증을 위한 요소로는 사용자 식별 ID(UserID), 사용자 인증 Password(*PWD*), 접속 매체(*ConMD*), 시스템 Mac Address(*MacAD*), 이중 인증 방법(*DualAMed*) 및 매체 정보(*Mname*)를 포함한다.

[User Authentication]
{UserID||PWD||ConMD||MacAD||DualAMed||Mname}

이중 인증 방식으로 사용자의 ID와 패스워드로 1차 인증하고 인증된 사용자의 이메일 및 SMS를 통한 2차 인증 기능을 제공한다. 3차 인증으로 접속 매체의 종류를 식별하고 매체의 Mac Address를 통해 접속 장치 식별 및 인증 서비스를 제공한다. 즉 소프트웨어적 접근과 하드웨어 정보를 활용한 인증 방식을 지원한다. 하지만, 인증 이후 세션 하이재킹 공격으로부터 여전히 자유롭지 못하다.

사용자 인증 이후 클라우드에 접속할 수 있는 인증 세션을 발급받는다. 발급받은 인증 세션(티켓)은 유효성과 보안성 기능을 제공한다. 인증 세션은 다음과 같다.

[Authentication Session Ticket]
[Serial Number||E{UserID+MacAD
+Creation Date+Expiration data
+Verification Value}]

Serial Number는 인증 서버에서 생성한 인증 세션의 고유 번호로서 티켓을 식별하는 기능을 제공하고, 사용자에게 발급한 세션키로 티켓의 유효 정보를 암호화한다. 암호화로 보호된 정보는 사용자 식별을 위한 식별값(ID)와 티켓의 유효성 정보(*Creation Date/Expiration Date*), 인증 서버가 인증할 수 있는 검증값(*Verification Value*), 접속 매체의 하드웨어 정보(*MacAD*)이다.

인증된 사용자는 인증세션 티켓을 발급받아 클라우드 컴퓨팅 시스템에 접속하여 권한내에서의 기능을 수행할 수 있다. 네트워크 상에서의 패킷 침해 공격에 패킷이 노출되어도 사용자와 서버간의 비밀키로부터 패킷을 보호받을 수 있다. 또한 비밀키가 노출되어 패킷이 Decryption 되어도 접속 매체의 하드웨어 정보가 동일하지 않아서 정

상적인 접근을 어렵게 한다. 또한 티켓으로 사용자 유효성을 관리하여 사용자의 로그인 및 사용자 관리의 편의성을 제공한다.

4.2 Service Management

(1) Traffic Management

사용자의 인증 티켓을 클라우드 서비스 시스템에 접속하여 권한 영역내의 콘텐츠를 접근할 수 있다. (1)사용자의 인증 티켓을 식별하고 티켓을 해독하여 등록된 접속 매체 및 티켓의 유효성을 검사한다. (2)라우팅 시스템은 접속 매체의 특성 및 접속 환경에 적합한 클라우드 시스템에 라우팅한다. (3)라우팅 시스템은 무선 및 유선형 매체의 특성과 트래픽을 분석하여 사용자의 위치 및 접속 환경에 적합한 클라우드 시스템에 세션을 라우팅한다.

(2) Digital Contents Management

콘텐츠는 소유권자 정보, 유통 및 공급 권한자 정보를 기본정보로 갖는다. 위의 권한을 보증받기 위해서 콘텐츠 서비스에 핑거프린팅 기법을 적용한다. 콘텐츠 서비스는 스트리밍 및 다운로드 서비스를 지원한다. 스트리밍 및 다운로드 서비스는 사용자 인증과 매체 인증 서비스가 적용되어 사용자와 매체 인증을 동시에 수행한다. 로그 정보는 콘텐츠에 접근한 사용자와 매체 정보를 콘텐츠 자체에 인덱스 정보로 저장하고 사용자 관리 서버에 로그 정보를 저장한다.

(3) System Synchronize

사용자 정보 및 콘텐츠 관리 정보는 접속한 클라우드 컴퓨팅 시스템에 저장되어 최신 정보를 유지한다. 클라우드 서비스 사용자 및 시스템 정보, 콘텐츠 활용 정보는 실시간으로 저장되며, 클라우드 컴퓨팅 서버간에 동기화를 통해 실시간 동일한 정보를 갖도록 시스템 동기화 서비스를 제공한다.

4.3 System Analysis Results

사용자 인증 및 네트워크 패킷의 안전성, 콘텐츠 관리, 시스템 장애 및 오류 발생시 서비스 영역으로 구분하여 분석한다.

Table 2. Comparative Analysis of Proposed Technologies

Service	Existing Technology	Proposed Technology
User authentication and network security	• User identification and password based user authentication • Management of access media for user access control	• Provides user identification and password user authentication services • Provides dual authentication with and SMS • Provides access media authentication
Tracking contents Logs	Stream and download support	Stream and Download Support Help manage user content logs
Service in case of system failure and error	Multiple hours of delay to a single server	Synchronization across systems during multiple cloud services ensures no recovery time in case of failure

IV. Conclusions

본 논문에서는 클라우드 컴퓨팅 서비스의 보안 및 서비스 장애를 발생시키는 위험 요소로부터 안전한 서비스와 편의성을 제공하기 위한 기술은 제안하였다. 사용자 인증 기술을 소프트웨어적 보안 기술과 하드웨어 인증 기술을 적용하였으며 네트워크상에서 발생하는 침해를 방지하기 위해 패킷 암호화 기능을 적용하였다. 또한 콘텐츠 유통의 지적재산권을 보호하기 위해 로그 추적 기능을 제공한다. 특히, 클라우드 시스템간의 실시간 동기화 서비스로 시스템 장애 및 오류시 원활한 서비스를 제공하고 있다.

본 제안 기술의 클라우드 컴퓨팅 서비스의 동기화 기술은 단순한 정보 공유로서 추후 블록체인 기술의 데이터 무결성 및 인증 기술을 접목하면 시스템 운영과 관리에 매우 적합한 서비스를 제공할 것으로 본다.

ACKNOWLEDGEMENT

The Work was supported by Jangan University Research Grant in 2024.

REFERENCES

[1] Eun-Gyeom Jang, A Study on the Authentication of Digital Content in Cloud Computing Environment. Journal of the Korea Society of Computer and Information, 27(11), 99-106, November 2022. DOI:10.9708/jksci.2022.27.11.099.

[2] KSCI, "2022 Cloud Industry Survey Report", Korea Association of Cloud Industry, Approval number 127010, 2022.

[3] Eun-Gyeom Jang, Study on Access Control Technique for Provision of Cloud Service in SSO-based Environment. Journal of the Korea Society of Computer and Information, 28(11), 73-80, November 2023, DOI: 10.9708/jksci.2023. 28.11.073.

[4] Sooyoung Kim, Byoungseob Kim, Seokho Son, Jihoon Seo, Yunkon Kim, & Dongjae Kang (2021), Design and Implementation of Multi-Cloud Service Common Platform. Journal of Korea Multimedia Society, 24(1), 75-94. January 2021.

[5] Eun-Gyeom Jang, "Digital Content Certification and Management Technology Based on Blockchain Technology", Journal of the Korea Society of Computer and Information, 26(11), 121-128. November 2021. DOI:10.9708/ jksci.2021. 26.11.121

[6] Dongyoung Koo, "Cloud Computing Security Technology Trends", REVIEW OF KIISC, 30(6), 101-106. December 2020. DOI:10. 3745/PKIPS.y2012m11a.1111

[7] Sung-Soo Son, Jung-Ae Park, Kyungyong Lee, "Technology Trend to Enable Cloud Computing Services in HPC Environments", Communications of the Korean Institute of Information Scientists and Engineers, 37(10), 17-24, October 2019.

[8] Sang-Yong Choi, Kimoon Jeong, "The Security Architecture for Secure Cloud Computing Environment", Journal of the Korea Society of Computer and Information, 23(12), 81-87. December 2018. DOI:10.9708/jksci.2018.23.12.081

[9] Jinl-OH Jeon, & Byeong Min Seo (2021). Design and implementation of improved authentication mechanism base on mobile DRM using blockchain. Digital Convergence Research, 19(4), 133-139.

[10] Dueckyoun Cho, Seogchan Hwang, & Gunho Jeong (2017). DRM Market System for Cloud-based Media Service Platform. Journal of Korea Multimedia Society, 20(6), 918-926.

Authors

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