JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 28 No. 11, pp. 73-80, November 2023
https://doi.org/10.9708/jksci.2023.28.11.073

A Study on Access Control Technique for Provision of Cloud Service in SSO-based Environment

Eun-Gyeom Jang*

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

[Abstract]

In this paper, a technology to protect important information from access in order to revitalize the cloud service market. A technology is proposed to solve the risk of leakage of important confidential and personal information stored in cloud systems, which is one of the various obstacles to the cloud service market. To protect important information, access control rights to cloud resources are granted to cloud service providers and general users. The system administrator has superuser authority to maintain and manage the system. Client computing services are managed by an external cloud service provider, and information is also stored in an external system. To protect important in-house information within the company, all users, it was designed to provide access authority with users including cloud service providers, only after they are authenticated. It is expected that the confidentiality of cloud computing resources and service reliability achieved through the proposed access control technology will contribute to revitalizing the cloud service market.

▸ **Key words**: SSO, Cloud Service, Access Control, User Authentication, Information Security

[요 약]

본 논문은 클라우드 서비스 시장을 활성화하기 위해 중요 정보의 접근을 보호하는 기술을 제안하였다. 클라우드 서비스 시장의 여러가지 저해요소 중에 클라우드 시스템에 저장되는 중요한 대외비 및 개인정보가 유출될 수 있는 문제를 해결하기 위한 기술을 제안하였다. 클라우드 서비스 제공자와 일반 사용자가 클라우드 자원에 대한 접근을 통제하여 중요 정보를 보호 할 수 있도록 하였다. 시스템 관리자는 시스템의 유지 및 관리를 위해 슈퍼유저의 권한을 갖는다. 클라이언트 컴퓨팅 서비스는 외부의 클라우드 서비스 공급자가 관리하고 정보 또한 외부시스템에 저장된다. 이러한 환경으로부터 사내의 중요 정보를 보호하기 위해 클라우드 서비스 공급자를 포함한 모든 사용자가 인증을 받고 자원을 접근할 수 있도록 하였다. 제안한 접근통제 기술을 통해 클라우드 컴퓨팅 자원에 대한 기밀성과 신뢰성 서비스를 제공하여 클라우드 서비스 시장의 활성화를 기대한다.

▸ **주제어**: SSO, 클라우드 서비스, 접근제어, 사용자 인증, 정보 보안

• First Author: Eun-Gyeom Jang, Corresponding Author: Eun-Gyeom Jang
*Eun-Gyeom Jang (jangeg@jangan.ac.kr), Dept. of Software Convergence, Jangan University
• Received: 2023. 10. 12, Revised: 2023. 11. 07, Accepted: 2023. 11. 08.

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

I. Introduction

안정적이고 빠른 유·무선 네트워크 인프라는 현대 사회의 정보 서비스가 가능한 환경을 제공하는 원천적인 기반을 제공한다. 이러한 네트워크 환경은 로컬로 운영되는 정보기술 서비스를 온라인으로 전환할 수 있는 환경을 제공하였다. 공공기관을 비롯한 기업, 학교에서 각각 운영되었던 정보시스템을 클라우드 컴퓨팅 서비스로 안전하고 편리하게 운영할 수 있도록 하였다. 클라우드 컴퓨팅 서비스는 스토리지를 포함한 서버, 소프트웨어 등의 자원을 가상화하여 사용자에게 안정적이고 접근의 용이성을 제공하고, 빠른 정보기술의 발달로 단기 수년 단위로 주기적 시스템 업그레이드의 비용적인 측면에 손실을 줄여준다[1].

클라우드 컴퓨팅 서비스는 사용자에게는 편리성, 관리자에게는 관리의 편리성과 효율성을 제공하고 안정적인 보안 서비스가 보장되어야 한다. 모바일 컴퓨팅 환경의 다양한 매체에 대한 접근과 다양한 서비스가 가능하도록 다변화하는 사회의 정보시스템의 요구사항을 만족시켜야 한다. 각 기관 및 기업에서는 기존 로컬로 운영되던 정보 서비스를 클라우드 서비스의 편의성과 안정적인 환경 제공으로 빠르게 전환하고 있는 추세이다[2].

하지만, 대학 및 기업의 경우, 본 단체의 정보가 외부 시스템에 보관되고 관리된다는 환경이 정보보호에 의문을 갖고 클라우드 컴퓨팅 서비스로 전환하지 않는 부분이 상당히 존재한다. 정보보호 측면에서는 개인의 정보가 외부에 보관되는 부분과 외부 사용자의 접근성에 문제를 제기하고 있다. 로컬 시스템의 경우 내부 정보시스템을 보호하기 위해 내부망과 외부망을 분리하여 운영하도록 권고하고 있다[2,3].

클라우드 컴퓨팅 서비스가 편리하고 효율적이지만, 중요 정보를 외부시스템에서 관리하는 것에 대한 보안문제가 해결되지 못한다면 클라우드 서비스의 시장성에 한계를 가질 것으로 본다. 이에 본 논문에서는 이러한 클라우드 컴퓨팅 서비스에 대한 정보와 접근의 안전성을 강화하여 신뢰성을 제공하는 클라우드 서비스를 위한 연구로 2장에서는 클라우드 컴퓨팅의 시장 동향 및 운영 사례와 서비스를 운영하면서 발생하는 문제점을 분석하고 3장에서는 도출된 문제점을 보완하기 위한 기술과 클라우드 서비스의 활성화를 위한 데이터 관리 및 인증 방안을 제시하고 제안한 기술의 안전성을 분석한다. 4장에서는 연구 결과에 대한 분석과 결론으로 구성하였다.

II. Literature Review

1. Cloud Service

1.1 Cloud service trends

한국클라우드산업협회가 발간한 '2022 국내 클라우드 산업 실태 조사 결과 보고서[1]'에 따르면 2019년에 3조 3,714억이었던 국내 클라우드 시장이 2020년 4조 원을 돌파했고, 2021년에는 9,250억 원이 늘어난 4조 9,250억 원에 달한 것으로 조사되었다. IaaS(Infrastructure as a Service)는 스토리지, 서버, 네트워크를 포함한 인프라 자원을 네트워크를 통해 제공하는 서비스로 2021년 클라우스 시장에서 가장 많은 영역을 차지하였다. 그 뒤를 이어 소프트웨어의 기능을 네트워크로 지원하는 SaaS (Software as a Service)가 두 번째로 많은 활용도를 보였다(Fig. 1). IaaS의 시장이 안정적으로 정착이 되면 점차 SaaS가 활성화될 것으로 예상된다.

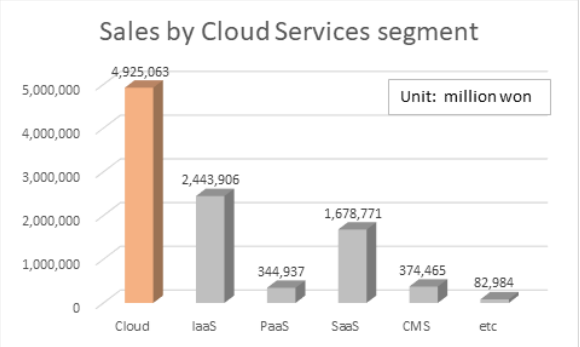


Fig. 1. Sales by Cloud Services segment in 2021 (Source: KACI)

CMS(Cloud Management Service)는 서비스 제공자와 사용자간의 기술과 컨설팅 비즈니스 모델이고, 소프트웨어 개발과 실행 환경을 제공하는 PaaS (Platform as a Service)가 있다.

2021년 IaaS는 전년도에 비해 약 5,500억원이 증가하고 SaaS는 2,400억 원, PaaS는 2020년에 2019년보다 2배의 성장세를 보였으나 소폭 감소한 것으로 조사되었다. 공공기관과 기업에서 온프레미스 인프라를 클라우드로 전환하면서 IaaS가 꾸준하게 증가하고 있다[2,3].

클라우드는 퍼블릭 클라우드(public cloud), 프라이빗 클라우드(private cloud), 하이브리드 클라우드(hybrid cloud) 모델로 분류할 수 있다. 퍼블릭 클라우드는 개방형 서비스로 클라우드 제공자가 운영하고 관리한다. 운영되고 있는 서비스를 개인 또는 기업이 비용을 지불하고 공동으로 이용하는 형태이다. 퍼블릭 클라우드는 개방형 서비스

환경이라면 프라이빗 클라우드는 폐쇄적인 서비스 환경으로 특정 기업이나 조직 자체적으로 구축한 서비스 환경에서 이용된다. 하이브리드 클라우드는 퍼블릭 클라우드와 프라이빗 클라우드를 연계한 서비스 형태로 정보의 보안이나 자원의 접근제어가 필요한 서비스에는 프라이빗 서비스를 제공하고 그렇지 않을 경우에는 퍼블릭 클라우드 서비스를 제공하는 서비스 형태이다[2,4].

클라우드 제공 모델별 매출 비중으로 퍼블릭 클라우드 모델이 38.1%, 프라이빗 클라우드 모델 17.1%, 하이브리드 클라우드 모델 중 하이브리드-퍼블릭 클라우드 25.3%, 하이브리드-프라이빗 클라우드 19.5%의 비중으로 조사되었다(Fig. 2).

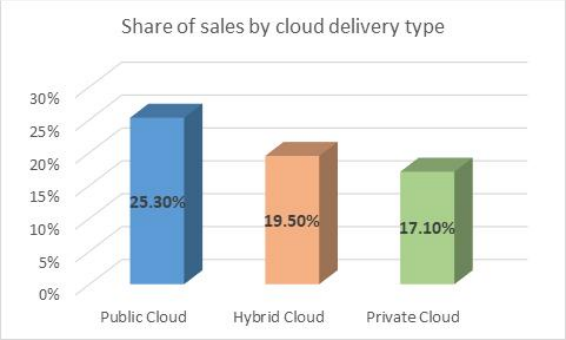


Fig. 2. Share of revenue by cloud delivery type(출처:KACI)

종사자가 적은 소규모 기업 및 단체에서는 퍼블릭 클라우드, 대기업은 하이브리드 클라우드, 서비스 모델은 퍼블릭 클라우드 상대적으로 많은 것으로 나타났다. 그리고 SaaS 개발시, 국산 IaaS를 이용하는 이유는 서비스의 안정성을 뽑았고, 외산 IaaS를 선호하는 경우에는 해외 진출시 유연한 서비스 제공의 이유로 조사되었다[1].

1.2 Cloud Service Types

클라우드 컴퓨팅을 NIST에서는 On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured service로 5가지 특성으로 정리하고 있다. 네트워크 스토리지 접근과 같이 필요시에 자동으로 연결하여 활용(On-demand self-service), 단말기를 통한 표준 메커니즘 접근 제공(Broad network access), 권한이 높은 관리자나 사용자의 접근 관리(Resource Pooling), 확대 및 축소의 탄력적인 서비스(Rapid elasticity), 서비스 유형에 따른 자원 활용의 최적화(Measured service)를 통해 사용자에게 투명성을 제공한다[5].

최근 클라우드 서비스 유형에서 IaaS가 가장 많은 비중을 차지하고 있다. IaaS는 컴퓨팅 자원들을 가상화 서비스를 제공하여 소프트웨어를 개발하거나 동작시키는 프로세스, 네트워크, 스토리지를 지원하는 서비스이다. SaaS는 클라우드 서비스 제공자가 지원하는 제한적인 애플리케이션 서비스로서 다양한 서비스가 부족하고 클라우드 인프라 등에 제어 및 관리가 어렵다. 클라우드 서비스가 대중화 되지 않은 상황에서 PasS(프로그래밍 개발부터 인프라, 스토리지, 서버, 운영체제 관리 및 제어)는 현재 다른 클라우드 서비스에 비해 시장성이 적다. 하지만, 클라우드 서비스 정착성에 비래하여 많은 기업 및 공공영역에서 활용될 것으로 본다[5,6].

2. Cloud Security Threats

클라우드 컴퓨팅 서비스와 보안 인증, 사용자 교육 등을 목적으로한 CSA(Cloud Security Alliance)에서는 클라우드 컴퓨팅 보안 위협(Table 1)을 구성 요소별로 정의하고 있다[6].

Table 1. CSA Cloud Computing Security Threats

Threat1	Misuse and irrational use of cloud computing
Threat2	Insecure application programming interface
Threat3	Maliciousness of insider
Threat4	Share of service and construction technology
Threat5	Data leakage or loss
Threat6	Hijacking of service or account
Threat7	Unknown new risk profile

클라우드 서비스 도입은 데이터 유출 및 접근제어의 보안 위협과 서비스의 안정성과 가용성, 내부 구축 어플리케이션과 클라우드 서비스와의 연동, 법 규제, 서비스 제공 시스템의 안정성, 서비스 비용 사항 등을 종합적으로 고려되어야 한다. 이러한 사항은 유지·관리에 비용적인 측면과 서비스의 안정성·편의성 측면, 정보의 안전성의 3가지 측면으로 요약될 수 있다. 예민한 정보를 다루는 시스템의 경우에는 현재 클라우드 컴퓨팅 서비스로 전환하지 못하는 가장 큰 이유로 작용되고 있다.

클라우드 보안사고로 스토리지 설정 오류로 인한 데이터 유출, 사용자나 관리자의 계정 관리(탈취) 문제로 인한 시스템 오작동 및 업무 방해, 클라우드 인프라 및 컨테이너 취약점을 이용한 침해 유형을 볼 수 있다.

클라우드 컴퓨팅 서비스에서 발생한 보안 문제로 구글의 G-메일 시스템의 장애를 들 수 있다. G-메일 사용자들의 데이터가 사라지는 경우가 발생하였고, 소니의 엔터테

인먼트 공격은 2천 명이 넘는 사용자의 개인 정보가 유출되기도 하였다. 미국의 은행 Capital One의 개인 정보 유출, 인도 혼다 자동차의 민감정보 유출, AWS DNS Server 설정 오류로 인한 서비스 접속 불가, 클라우드 시스템 장애 발생, 고객사 데이터 및 백업파일 삭제 등의 사례가 있다[6,7].

클라우드 컴퓨팅 환경에서 발생하는 보안 문제로 계정을 보호하기 위해 SMS 문자 인증 또는 다중 인증(MFA)를 사용하지만, SMS의 해킹과 MFA를 제공하지 않는 경우가 있다. 또한 많은 사용자가 클라우드를 빠르고 쉽게 관리하기 위해 관리자를 다수 생성 또는 아이디와 패스워드를 공유하여 사용하면서 보편적인 권한 상승 공격에 대한 감지가 어려운 실정이다.

한국인터넷진흥원에서는 다양한 보안 위협 중에 가상머신 제어권을 상실하는 보안 위협을 가장 큰 이슈로 보고 있다. 그 중 하이퍼바이저의 취약점 공격으로 제어권을 획득하여 개인 정보가 유출되는 것이다. 하이퍼바이저 취약점으로 Guest-Host OS간 통신 구성요소 취약성, Integer signedness error, 하이퍼바이저 권한 명령 디코딩 등이 있다.

이러한 가상화 기술에 대한 보안 위협으로부터 시스템을 보호하기 위해 EMC, HP, IBM, CA 등의 클라우드 컴퓨팅 기업들은 가상머신 보안 제품과 방화벽 보안 기술을 개발하고 있다. IBM은 클라우드의 가상화 환경에서 이기종의 하이퍼바이저에 대한 공격을 탐지하고 방어하여 데이터의 무결성을 보장하는 하이퍼센트리(Hyper Sentry)을 선보였다[6,7,8].

III. Proposed System

1. System configuration

클라우드 컴퓨팅 환경에서의 시스템 구성은 Fig. 3과 같다. 유무선 네트워크 기반으로 다양한 장치들과의 인터페이스를 통해 이기종 시스템 및 애플리케이션 소프트웨어 서비스를 제공한다. 본 연구의 기본 환경은 SSO(Single Sign On) 시스템 환경에서 클라우드 서비스를 제공한다.

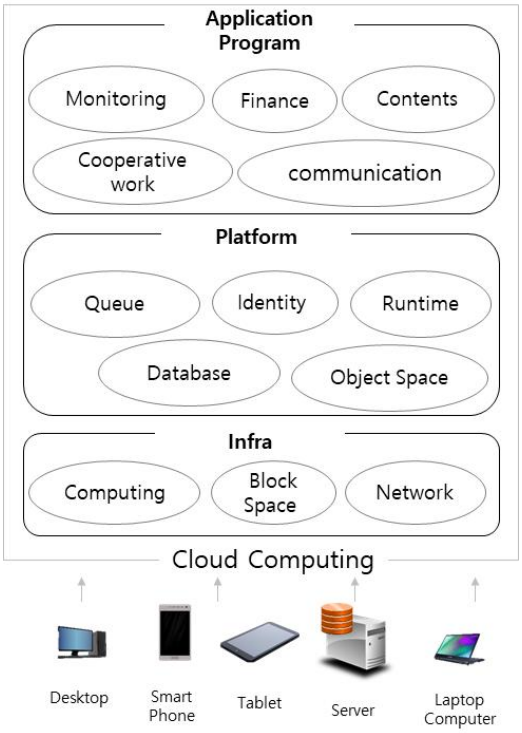


Fig. 3. Cloud service environment

제안 시스템은 데스크탑, 모바일 폰, 태블릿, 서버, 랩톱 컴퓨터 등의 다양한 클라이언트가 인프라(컴퓨팅, 블록 공간, 네트워크), 플랫폼(큐, 신원, 런타임, 데이터베이스, 오브젝트 공간), 응용 프로그래밍(모니터링, 금융, 콘텐츠, 협업, 통신)의 클라우드 서비스를 활용할 수 있는 환경을 갖는다.

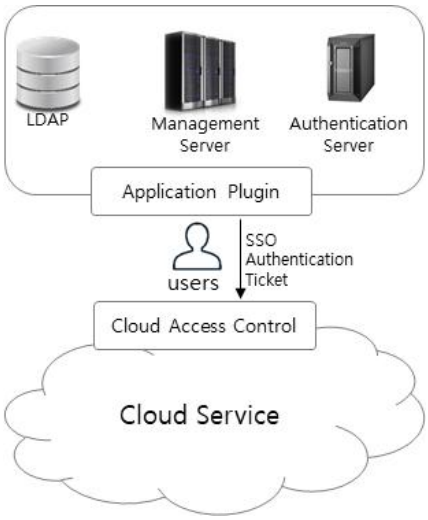


Fig. 4. User authentication structure

사용자의 클라우드 서비스 접근을 위한 사용자 인증 체계는 Fig. 4와 같다. 사용자 인증 정보는 사용자 관리 시스템에 등록되고 등록된 사용자는 인증 시스템으로부터 티켓을 발급받아 클라우드 서비스에 접근할 수 있다.

2. Configuring a Ticket Issuance System

클라우드 컴퓨팅 서비스 접근은 인증 티켓으로 접근할 수 있다. 티켓은 사용자 권한별로 발급하여 접근권한내에서 서비스를 제공받는다. 일반적인 티켓을 Fig. 5와 같이 사용자의 정보와 시스템 정보를 인증 데이터로 활용하여 사용자 인증 서버에서 관리한다. 사용자가 인증되면 티켓 관리 서버에서 인증된 사용자임을 증명하는 티켓을 발급하여 사용자가 클라우드 서비스를 사용할 수 있도록 한다.

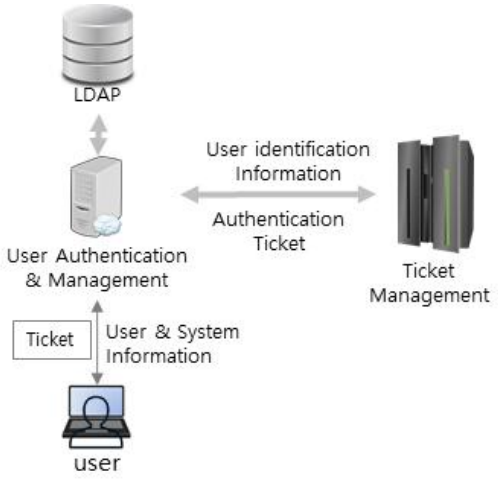


Fig. 5. Manage user tickets

클라우드 서비스 제공자 영역에 관리자는 고객에게 안전한 클라우스 서비스를 제공하기 위해 클라우드 시스템 관리가 필요하다. 클라우드 서비스 관리를 위해 공급자도 인증 티켓을 발급받아야 한다. 즉, 시스템을 접근하는 사용자는 고객 입장(서비스 사용자)에서의 사용자와 관리자가 있으며, 클라우드 서비스를 제공하는 공급자로 구분하여 관리된다.

클라우드 서비스 공급자 영역의 접근 관리자는 Fig. 6과 같이 각 클라우드 서비스 영역별 접근 티켓이 구분되어 제공된다. 클라우드 서비스 공급자라 할지라도 서비스 사용자(관리자)의 접근 제어에 의해 접근이 허용되어 관리된다. 클라우드 서비스 제공 관리자는 클라우드 시스템의 안전한 관리를 위해 클라우드 서비스 사용자(관리자)에게 접근권한을 받아 시스템에 접근할 수 있다.

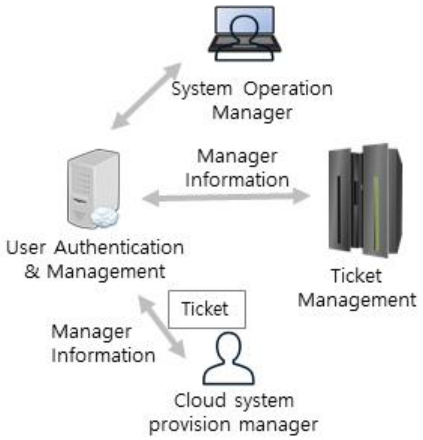


Fig. 6. Manage Service Provider Tickets

3. Issuing a Certification

3.1 Issue service user tickets

서비스 이용자는 사용자의 고유 및 기본 식별 정보를 등록하고 서비스 접근 매체인 클라이언트를 추가 등록한 후 서비스 접근이 가능하다. 사용자 등록은 다음과 같다.

■ 사용자 등록

U : 사용자, I : 기본 정보, SI : 고유 보안 정보,
AC : 클라우드 서비스 접근 매체(클라이언트 에이전트 시스템 고유 기기 번호)

$$U\left\{I+SI+\left\{\sum_{i=1}^{n}CA_i\right\}\right\} \Rightarrow U_{ID}\| U_{P/W}\| CA_n$$

사용자의 기본 정보와 식별정보(주민/여권번호/Pin번호, 스마트폰 인증 등 사용자 식별 고유정보)가 기본 요구사항이다. 또한 클라우드 서비스 접근에 사용할 기기 정보가 필요하다. $\sum_{i=1}^{n}CA_i$은 여러 대의 접근 기기를 등록하여 접근을 허용하고, 동시 접근 및 티켓 관리의 유효성 서비스에 활용된다. 이렇게 등록된 사용자가 시스템 접근에 필요한 정보는 사용자 ID와 P/W, 클라우드 서비스 접근 매체($U_{ID}\| U_{P/W}\| CA_n$) 정보로 시스템 접근 정책에 의해 통제된다.

■ *인증 티켓 발급*

등록된 사용자는 사용자의 $U_{ID}\|U_{P/W}\|CA_n$ 정보를 세션키로 암호화($S_{CKey}\{U_{ID}\| U_{P/W}\| CA_n\}$)하여 사용자 인증 정보를 서버에 전송한다.

$$User\ Client : \left(S_{Ckey}\{U_{ID}\|U_{P/W}\|CA_n\}\right) \Rightarrow Authentication\ Server$$

인증 서버는 세션 복호화키로 암호화된 정보를 복호화 한다.

$$Authentication\ Server\ :\ S_{Dkey}\{U_{ID}\|U_{P/W}\|CA_n\} \Rightarrow U_{ID}\|U_{P/W}\|CA_n$$

사용자 인증 절차에 의해 인증된 사용자는 요청한 클라우드 서비스 접근을 위한 티켓은 티켓 관리 시스템에서 생성한다. 생성된 티켓은 다음과 같다.

$$\begin{aligned} Ticket\ :\ & Ticket_{Num} \\ & \|Seed_{user/doud}\{User_{ID}+CA_n+A_{Issuer}\} \\ & \|Ticket_{Issuer}\|Ticket_{\mathrm{Expiration}} \\ & \|Ticket_{Verification\ Value} \\ & \|Hash_{SHA}\left\{\begin{array}{l} Ticket_{Num}\|CA_n\|User_{ID} \\ \|Seed_{user/doud}\{User_{ID}+CA_n+A_{Issuer}\} \\ \|Ticket_{Issuer}\|Ticket_{\mathrm{Expiration}} \\ \|Ticket_{Verification\ Value} \end{array}\right\} \end{aligned}$$

- $Ticket_{Nm}$: *티켓 발행 번호*
- $Seed_{user/doud}$: *사용자 대칭 암호화 키*
- A_{Issuer} : *티켓 발급자 번호*
- $Hash_{SHA}$: *해쉬함수*
- $Ticket_{Issuer}$: *티켓 발생 시간*
- $Ticket_{\mathrm{Expiration}}$: *티켓 유효기간*
- $Ticket_{Virification\ Value}$: *티켓 검증 잉여비트*

티켓에는 사용자의 식별 정보($User_{ID}$)와 사전 등록된 클라이언트, 티켓 번호를 기본 정보로 갖는다. 사용자의 고유 정보를 보호하기 위해 접속 요청 클라이언트와 티켓 발행자, 사용자 정보는 암호화하여 보호한다. 티켓의 유효성을 검증하기 위해서 티켓 생성시간($Ticket_{Issuer}$), 티켓 유효기간($Ticket_{\mathrm{Expiration}}$), 티켓 검증 정보($Ticket_{Verification\ Value}$)가 포함된다. 이러한 티켓의 무결성 서비스를 위해 티켓의 블록을 해쉬함수($Hash_{SHA}$)로 보호하여 검증한다.

3.2 Issue system provider tickets

클라우드 시스템 공급자의 티켓은 일반 사용자의 기본 티켓 발급 절차와 같으나, 추가적인 인증 세션(Fig. 7)을 갖는다. 클라우드 시스템의 안전한 서비스 제공을 위해 클라우드 제공자의 시스템 접근은 임의적인 접근에서 발생하는 정보 보안의 신뢰성을 감소시킨다. 본 연구에서는 관리적 또는 유지 보수를 위한 시스템 접근제어에 클라우드를 사용하는 사용자(관리자)로부터 접근 허용 토큰을 인증받고 클라우드 시스템에 접근할 수 있다.

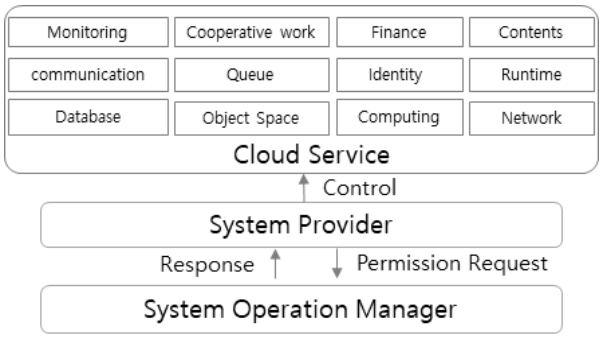


Fig. 7. System Provider Cloud Access

클라우드 관리자가 클라우드 접근을 위해 해당 서비스 운영 관리자에게 다음과 같은 접근 허용 토큰을 요청한다.

$$\begin{aligned} & Request\ Token\ : \\ & Serial\ Nmber\| \\ & SM_{pu}\left\{Sec_{Key}\left\{CM_{ID}+CM_{A_{Num}}+Cood_{Service}\right\}\right\} \\ & \|Hash\left\{SM_{pu}\left\{Sec_{Key}\left\{CM_{ID}+CM_{A_{Num}}+Cood_{Service}\right\}\right\}\right\} \end{aligned}$$

- $Serial\ Nmber$: *토큰 일련번호*
- SM_{pu} : *클라우드 서비스 운영 관리자 공개키*
- Sec_{key} : *세션키*
- CM_{ID} : *클라우드 서비스 제공 관리자 식별자(ID)*
- $CM_{A_{Nm}}$: *클라우드 서비스 제공 관리자 인증값*
- $Cood_{Service}$: *요청 서비스 코드*

클라우드 제공 관리자를 식별하고 인증받기 위해 고유값(CM_{ID}, $CM_{A_{Nm}}$)을 암호화하여 전송한다. 클라우드 서비스 운영 관리자는 클라우드 제공 관리자의 인증하고 요청 서비스 코드($Cood_{Service}$)에 대한 접근 권한 확인 후 클라우드 서비스 제공 관리자에게 인증 티켓을 전송한다.

$$\begin{aligned} & Serial\ Nmber\|Cood_{Service}\| \\ & SM_{pr}\left\{\begin{array}{l} SA_{Code_{Num}}+CM_{ID}+Ticket_{Issuer}+Ticket_{\mathrm{Expiration}} \\ +Ticket_{Verification} \end{array}\right\}\| \\ & Hash\left\{\begin{array}{l} Serial\ Nmber\|Cood_{Service}\| \\ SM_{pr}\left\{\begin{array}{l} SA_{Code_{Nm}}+CM_{ID}+Ticket_{Issuer}+ \\ Ticket_{\mathrm{Expiration}}+Ticket_{Verification} \end{array}\right\} \end{array}\right\} \end{aligned}$$

- $SA_{Cood_{Nm}}$: 서비스 요청 인증 코드

인증 티켓은 티켓 생성시간($Ticket_{Issuer}$), 티켓 유효기간($Ticket_{\mathrm{Expiration}}$), 티켓 검증 정보($Ticket_{Verification\ Value}$)를 포함한다.

4. Proposed Technical Analysis

4.1 User authentication

다양한 클라우드 서비스를 한 번의 인증으로 접근이 가능하도록 사용자 인증 티켓이라는 SSO 서비스를 기반으로 운영된다. 사용자 인증은 사용자 식별 코드 및 인증 코드로 정상적인 사용자임을 인증받는다.

$$S_{key}\{U_{ID}\| U_{P/W}\| CA_n\}$$

▪ *티켓 인증 서비스*

사용자 인증을 강화하기 위해 사용자의 접근 장치(클라이언트(CA_n))를 등록하고 관리한다. CA_n는 접근 장치의 고유 장치 번호를 추가 등록하여 동시 접근통제 기능을 수행할 수 있다. 또한 발급 티켓에 생성시간($Ticket_{Issuer}$), 티켓의 유효기간($Ticket_{\text{Expiration}}$)으로 인증 시간을 제한하였다. 티켓 자체에 대한 보호를 위해 티켓 검증 잉여비트($Ticket_{Virification\,Value}$)와 검증정보($Ticket_{Verification\,Value}$)를 활용하여 티켓을 보호하였다.

▪ *티켓의 무결성 서비스*

티켓의 외부 접근에 의한 손상 및 변형에 대한 무결성 서비스를 위해 해쉬 함수($Hash_{SHA}$)를 활용하여 티켓의 해쉬값을 활용하여 티켓이 변형되지 않았다는 무결성 서비스를 제공한다.

$$Hash_{SHA}\begin{Bmatrix} Ticket_{Num}\|CA_n\|User_{ID} \\ \|Seed_{user/cloud}\{User_{ID}+CA_n+A_{Issuer}\} \\ \|Ticket_{Issuer}\|Ticket_{\text{Expiration}} \\ \|Ticket_{Verification\,Value} \end{Bmatrix}$$

▪ *티켓의 기밀성 서비스*

티켓이 인증된 관리자로부터 발급되었다는 인증 정보(A_{Issuer})와 사용자의 정보($User_{ID}$), 접근 요청을 한 클라이언트(CA_n)를 보호하기 위해 미리 공유된 대칭키 암호화($Seed_{user/cloud}$) 기법으로 중요 정보를 보호하였다.

$$Seed_{user/cloud}\{User_{ID}+CA_n+A_{Issuer}\}$$

4.2 Service Administrator Authentication

서비스 제공 관리자는 클라우드 서비스를 사용자들이 서비스를 신청하고 사용할 수 있도록 지원해 주는 업무를 수행하는 관리자이다. 컴퓨팅 서비스를 위한 슈퍼 유저의 권한을 갖고 있는 관리자는 어떠한 자원에도 접근이 가능한 권한을 갖는다. 하지만, 본 제안 기술 환경에서는 클라우드 서비스의 정보 보안의 신뢰성을 추구하기 위해 슈퍼 유저의 접근 권한을 클라우드 운영 관리자로부터 접근 권한을 허락받은 후 접근할 수 있도록 하였다.

$$\begin{array}{l} Serial\,Nmber\|Cood_{Service}\| \\ SM_{pr}\begin{Bmatrix} SA_{Code_{Num}}+CM_{ID}+Ticket_{Issuer}+Ticket_{\text{Expiration}} \\ +Ticket_{Verification} \end{Bmatrix} \end{array}$$

코드화된 자원 접근 및 서비스 코드($Cood_{Service}$)로 시스템 운영자에게 접근을 요청하여 클라우드 자원 접근 권한을 획득한다. 획득한 접근 권한 티켓은 티켓의 유효기간($Ticket_{\text{Expiration}}$)에 의해 생명주기를 갖는다. 티켓의 유효성은 장시간 인증 세션을 유지하면서 발생하는 보안 문제를 방지한다.

4.3 Comparative Analysis

제안 기술은 클라우드 서비스의 안정적인 운영과 보안성을 강화한 모델이다. 기존 SSO 클라우드 컴퓨팅과 비교/분석하면 다음과 같다.

■ 4.1절에서 기술한 사용자 인증 및 인증 정보(Ticket)의 보안성, 클라우드 컴퓨팅 서비스의 접근성을 용이하기 위한 티켓을 활용한 SSO 서비스이다. 티켓을 활용한 사용자 인증 및 접근제어는 시스템의 접근성과 보안성 서비스를 제공한다(기존 연구 및 시스템 서비스에서도 제공됨).

■ 제안 기술의 차별화된 기술은 클라우드 서비스 공급자로부터의 시스템 및 서비스 접근에 대한 사용자의 신뢰된 접근성이다. 서비스 공급자의 무분별한 고객의 클라우드 서비스에 대한 접근을 인증하고 로깅함으로써 시스템 관리에 파워유저라 할지라도 고객의 정보시스템에 접근을 위해서는 인증을 받아야 서비스 관리 및 유지를 할 수 있다(기존 클라우드 컴퓨팅 서비스에 제공 (X)).

IV. Conclusions

본 논문은 클라우드 서비스를 활성화하기 위한 보안 기술이다. 클라우드 컴퓨팅 서비스는 유지보수적 측면에서 경제적이고 편리하며, 장기적 시스템 유지 관리에 유용하다.

정부에서도 클라우드 서비스를 활용하도록 많은 지원이 되고 있지만, 실제 대학 및 기업, 공기업 등에서 활용을 우려하는 문제점 중에 하나가 중요 정보가 클라이언트 서비스 제공자에게 오픈된다는 것을 뽑을 수 있다. 원활한 클

라우드 서비스를 위해 서비스 자원에 임의로 접근하여 보완하고 수정해야하는 것은 당연한 업무이다. 이로 인해 발생하는 권한의 남용으로 정보 유출에 문제를 발생시키는 환경은 충분하다.

이에 본 연구에서는 클라이언트 제공자에게 접근 권한 허용을 클라우드 운영 관리자로부터 인증받고 자원에 접근할 수 있도록 한다. 클라우드 제공자의 접근 권한을 관리하여 로그를 통해 역추적이 가능하고 자산을 보호할 수 있는 클라우드 시스템 환경을 구축할 수 있다. 이렇게 클라우드 서비스 제공자의 접근권한을 통제하면서 자산을 보호한다면 클라우드 컴퓨팅 서비스 시장 활성화에 많은 영향을 미칠 것으로 기대한다.

ACKNOWLEDGEMENT

The Work was supported by Jangan University Research Grant in 2023

REFERENCES

[1] KSCI, “2022 Cloud Industry Survey Report”, Korea Association of Cloud Industry, Approval number 127010, 2022.

[2] 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, 21(4), 31-38, April 2016. DOI:10.9708/jksci.2016.21.4.031

[3] 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.

[4] Sangwoong Lee, Moonhyung Park, Seon-a Lee, Wonhyung Park, “Security Enhancement through Comparison of Domestic and Overseas Cloud Security Policies”, Journal of the Korean Information and Communication Association Comprehensive Academic Conference, 25(2), October 2021.

[5] 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

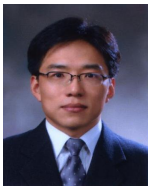
[6] Dongyoung Koo, “Cloud Computing Security Technology Trends”, REVIEW OF KIISC, 30(6), 101-106. December 2020. DOI:10.3745/PKIPS.y2012m11a.1111

[7] Lee In Soo, Chang Deok Moon, “A Study on Methods for providing Security Service in Cloud Computing”, Proceedings of Symposium of the Korean Institute of communications and Information Sciences, 1052-1053, January 2017.

[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] 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

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.