Journal of The Korea Society of Computer and Information
Vol. 22 No. 8, pp. 55-61, August 2017
www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.08.055

A Enhanced Security Model for Cloud Computing in SSO Environment

Eun-Gyeom Jang*

Abstract

Cloud computing is cost-effective in terms of system configuration and maintenance and does not require special IT skills for management. Also, cloud computing provides an access control setting where SSO is adopted to secure user convenience and availability. As the SSO user authentication structure of cloud computing is exposed to quite a few external security threats in wire/wireless network integrated service environment, researchers explore technologies drawing on distributed SSO agents. Yet, although the cloud computing access control using the distributed SSO agents enhances security, it impacts on the availability of services. That is, if any single agent responsible for providing the authentication information fails to offer normal services, the cloud computing services become unavailable.

To rectify the environment compromising the availability of cloud computing services, and to protect resources, the current paper proposes a security policy that controls the authority to access the resources for cloud computing services by applying the authentication policy of user authentication agents. The proposed system with its policy of the authority to access the resources ensures seamless and secure cloud computing services for users.

▸Keyword: Cloud Computing, SSO, Agent, Access Control

I. Introduction

컴퓨터시스템의 환경이 로컬시스템기반에서 네트워크 환경으로 발전하고, 네트워크 환경에서 제공하는 정보공유 및 다양한 서비스 환경으로 변화하였다. 또한 통신 기술의 발달로 각 서비스별로 하드웨어적인 물리적 서버 구축을 통한 네트워킹 서비스가 다양화되고 대중화되어 네트워킹 서비스를 거치지 않고는 컴퓨팅이 어려운 환경이 되었다. 이에 컴퓨팅 환경은 쉽게 서버를 관리하고 활용할 수 있는 클라우드 컴퓨팅(Cloud Computing) 환경을 요구하고 있다.

클라우드 컴퓨팅은 첫 번째로 구축 및 유지보수에 많은 비용이 절감된다는 점과 관리가 쉬운 특징을 갖는다. 또한 클라우드 서버 구축에 특별한 IT 기술을 요하지 않는다는 장점도 있다. 그러나 클라우드 컴퓨팅의 기본 환경은 온라인으로 서비스가 이루어지고 있어 네트워크상의 어느 시점에 문제가 발행하면 서비스가 마비된다는 단점도 있다. 또한 중앙 집중형의 시스템 구축환경은 중앙 시스템의 문제는 전체 서비스에 악영향을 미치는 결과와 오용 및 비신뢰성에 치명적인 문제점을 내재하고 있다[1].

클라우드 컴퓨팅의 활용측면에서 서버 구축 및 관리에 편리성과 활용성, 비용적인 측면에서 장점을 보이나, 사용자 및 관리자 입장에서는 정보에 대한 비밀유지 및 활용성, 접근성, 용이성을 요구하고 있다. 이러한 요구사항을 기반으로 사용자에게 서비스의 안전성과 편리성을 제공하기 위해 SSO(Single Sign On) 모델을 활용한 사용자 접근성을 제공하고 사용자 인증과정을 강화하여 안전하게 서비스를 이용할 수 있는 컴퓨팅 서비스가 우선시되어야 한다.

기존 연구에서는 SSO를 활용한 클라우드 컴퓨팅 서비스를 제공하여 사용자의 편리성을 강화하고 있다. 하지만 사용자의 편리성만을 제공하고 사용자의 개인정보를 보호하기에는 부족

• First Author: Eun-Gyeom Jang Corresponding Author: Eun-Gyeom Jang
*Eun-Gyeom Jang (jangeg@jangan.ac.kr), Dept. of Internet Communication, Jangan University
• Received: 2017. 06. 20, Revised: 2017. 07. 18, Accepted: 2017. 08. 01.
• The Work was supported by Jangan University Research Grant in 2017

한 서비스 환경으로 정보보안 서비스가 미흡하다[1,2]. 이에 본 연구에서는 클라우드 컴퓨팅 환경에 SSO 서비스를 활용하여 사용자에게는 편리성을 제공하고 사용자 및 관리자 입장에서는 시스템 및 서비스 신뢰성을 제공하기 위해 시스템 접근 강화 모델을 제안한다.

본 논문은 기존의 클라우드 컴퓨팅의 다중 분할 SSO 에이전트에서 발생하는 보안 위협을 해결하기 위해 인증 절차 및 과정에 따른 보안 등급을 적용하여 사용자 접근을 강화한다. 논문 구성은 2장에서는 클라우드 및 SSO, 사용자 인증 기술을 논하고 3장에서는 시스템 환경을 구축하고 제안 모델을 제시한다. 제안한 모델은 4장에서는 실험하고 분석하여 성능을 평가한다. 마지막으로 5장에서는 논문을 정리하는 결론으로 논문을 구성하였다.

II. Literature Review

1. Cloud computing

1.1 Cloud computing service environment

클라우드 컴퓨팅는 그림 1과 같이 인프라를 제공하고 Public Cloud와 Private Cloud로 나눌 수 있다.

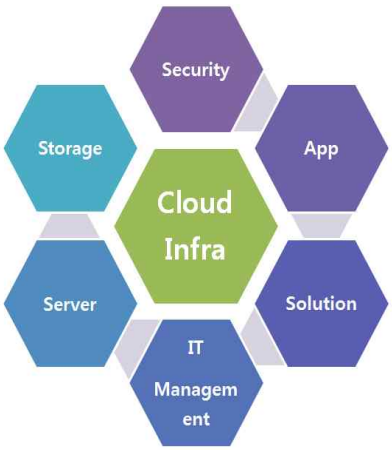


Fig. 1. Cloud Infra

Public Cloud는 범용성을 갖는 컴퓨팅 서비스로 아마존과 구글의 서비스로 대규모로 이루어지는 특성이 있고, Private Cloud는 특정 영역에 서비스를 제공하는 시스템으로 운영하여 은폐된 서비스 형태를 갖는다[2]. NIST는 5가지로 클라우드 컴퓨팅의 주요 특성을 정의하고 있다. 첫 번째로 자동으로 컴퓨팅 서비스를 준비할 수 있고(On-demand Self-Service), 사용자 플랫폼의 표준 메커니즘 접근(Broad network access), 높은 권한을 가진 사용자의 리소스 제어(Resource Pooling), 서비스 이용의 탄력적 특성(Rapid elasticity), 서비스에 따른 최적화로 투명적 서비스(Measured service)이다.

클라우드 컴퓨팅 서비스 모델은 표 1과 같이 Saas(Cloud Software as a Service), PaaS(Cloud Platform as a Service), IaaS(Cloud Infrastructure as a Service)로 구성된다[2,3].

Table 1. Cloud computing service model

Service	Model
SaaS	Users can use cloud service applications for a limited environment setting, management and control with this service.
PaaS	Programming languages and tools are supported for application development. Users are authorized to set up the system environment for their configured and hosted applications although they are not allowed to manage and control the infra, server, network, storage and OS.
IaaS	When users operate and develop applications or OS, the processor, network and storage services are provided.

1.2 Security Threats in Cloud Computing

국내외 클라우드 컴퓨팅의 보안 위협은 다양하게 요일들을 보이고 있다. Gartner, UC Berkely, EINSA, KISA에서는 다음과 같이 보안 위협요인들을 다루고 있다[2,4].

Table 2. Cloud service's security threat

Group Name	Item
Gartner	An authority administrator's access, policy, recovery, data storage location, survey resources, data separation and long-term viability
UC Berkely	Service availability, data lock-in, data confidentiality and surveillance, data transmission impairment components, uncertain performance prediction, scalable storage, large-scale distributed system bugs, rapid scaling, reputation sharing, software licensing
EINASA	Absence of management, difficulties of isolation, dependence on service providers, regulatory threats, data protection, management interface reinforcement, insecure data deletion, malicious insiders
KISA	Virtualization vulnerability, threats of entrusted information disclosure, service failure resulting from resource sharing and centralization, information disclosure resulting from diversity of terminals, difficulties of reinforcement resulting from distributed processing, legal and regulatory issues

표 2에서 각 그룹별로 제시하는 보안 위협이 각기 다른 것을 보이고 있고 일반적인 보안 위협으로 클라우드 컴퓨팅의 악의적인 사용과 남용, 악성 내부부사용자, 공유기술의 취약성, 데이터 손실 및 누출, 계정 서비스와 트래픽 하이재킹, 알려지지 않은 위험 프로파일 등이 있으며, 이는 클라우드 컴퓨팅에 대한 위협보다는 일반 IT체계에서의 위협요소로 볼 수 있다.

Gartner에서는 자원에 대한 접근과 데이터 관리 영역에 중점을 두고 있으며 UC Berkely는 클라우드 서비스와 데이터 관리 및 운영, EINSA는 클라우드 서비스 운영에 관한 위협, KISA는 클라우드 가상화 공유와 서비스에 중점을 두고 있다. 이렇게 다양한 영역에서 클라우드 컴퓨팅에 대한 일관된 위협은 시스템 사용에 대한 위협과 자원 활용 및 관리에 위협요소들이다.

2. SSO system and authentication

2.1 SSO system

기존 SSO 시스템으로 커버로스 구조, SESAME, RSAKeon, SuitSpot이 있다[5].

• 커버로스 구조 : PKI 기반구조로서 공개키 기반 구조를 제공하면서 강력한 보안 서비스를 제공한다. 인증서를 기반으로 KDC에 초기인증을 할 수 있도록 하는 PKINT와 중앙의 인증서버의 개입 없이 사용자와 서버간에 이루어지는 인증 프로토콜을 활용한 사용자인증에 간편성을 제공하는 PKDA가 있다. 그러나 PKI 기반으로 서비스가 이루어져 대칭키에 대한 부담을 갖고 있으며 Legacy 시스템의 확장성에 한계를 가지고 있다.

• SESAME : 커버로스 기반에 분산된 접근통제 기능을 제공하여 키관리 부담을 줄였다. 하지만 PKI 기반의 대칭키에 대한 문제는 여전히 존재하고 분산 접근통제를 위한 부담이 가중되었으며 Legacy에 대한 문제는 해결되지 못하였다.

• RSAKeon : x.509 v3 인증서의 확장 필드에 중앙의 통합 접근통제가 가능하도록 하고 Legacy 시스템에 확장성 있는 구조로서 커버로스나 SESAME에 비해 보완된 구조를 갖는다. 또한 대칭키에 부담을 줄였다. 하지만 세션의 재접속시 재인증을 위한 절차가 필요하여 인증에 대한 부담을 갖고 있다.

• SuitSpot : 통합적인 접근통제, Legacy 시스템의 SSO 확장성에 문제를 가지고 있으나, 인증 서버를 거치지 않고 클라이언트와 서버간에 인증이 가능하도록 설계되어 단순한 구보로 서비스가 이뤄진다.

2.2 SSO authentication

SSO는 단일키를 활용한 다중 시스템 접근방식을 적용하고 있다. 사용자의 편의성을 우선으로 제공되는 서비스로서 개방형 인증 기술인 오픈 ID의 한 예이다. 장점으로 사용자 계정 및 정보를 통합 관리하여 한 번의 로그인으로 여러 시스템 및 사이트를 접근할 수 있는 시스템 구조이다. 또한 SSO 설계 자체에 암호화와 인증으로 보안 관리되며 외부 네트워크에서도 가능하다.

중앙 통합관리 SSO 서비스는 사용자 인증서로 SSO 서버에 인증을 요청하고 토큰을 통해 SSO 서버를 수행한다. 시스템은 LDAP(Lightweight Directory Access Protocol)을 이용하고 다양하고 분산된 서비스로 이동하기 위해 재인증 절차 없이 승인되도록 구성되어 있다. 타임스탬프와 같이 시간과 로컬 시스템 인증, 인증 영역 도메인에 제안을 두어 패킷을 인증하고 있고 관리 및 운영을 위한 별도의 프로그램을 운영한다. 오라클에서도 쿠키 기반의 SSO 서비스 모델을 적용하고 있으며 세부적인 구조 및 기능은 다르나 쿠키 서버를 중심으로 운영되고 있다.

SSO의 시스템 구조에 따른 인증을 분류하면 Broker-Based, Agent-Based, Agent-Broker-based, Gateway-Based을 들 수 있다[5,6]. Broker-Based와 Agent-Broker-based, Gateway- Based은 중앙 집중식 시스템 관리를 통해 효율적인 관리가 강점이고, Agent-Based, Agent-Broker-based은 기존 응용 프로그램의 수정이 적다는 것이다. 그러나 Broker -Based는 기존 응용 프로그램의 수정이 필요하고, Agent -Based는 사용자 계정관리, Agent-Broker-based는 구성요소 증가로 관리가 어려움, Gateway-Based는 여러 게이트웨이간의 동기화가 필요한 단점을 갖는다.

사용자 인증 방식에 따른 인증 방식은 인증대행 방식과 인증정보 전달 방식으로 나눌 수 있다. 인증대행 방식은 에이전트가 사용자 인증을 거쳐 대신하여 해당 서버에 대행으로 인증하여 서비스가 이루어져 사용자와 에이전트간에 안전성을 보증한다면 비교적 안전한 서비스 구조를 가지고 있고 인증 정보 전달 방식은 에이전트가 사용자를 정당함을 인증하고 에이전트와 서버간에 토큰을 발생하여 토큰으로 사용자와 통신하는 방식이다. SSO 토큰을 활용한 방식은 인증정보가 클라이언트를 통해 인터페이스가 이루어져서 스니핑과 재전송 공격에 취약하다는 단점을 갖는다[7].

3. Distributed SSO agents' user authentication

분산 SSO는 유·무선 네트워크 환경에서 안전한 클라우드 컴퓨팅을 위해 사용자 인증 정보를 분산하여 관리하는 구조이다 (그림 2).

하나의 에이전트에 의존한 사용자 인증은 해당 SSO 에이전트의 보안 취약점 및 다운에 의한 사용자 서비스 접근에 많은 문제를 일으킬 수 있다. 분산 SSO 에이전트는 이러한 문제를 해결할 수 있는 시스템 구조로 운영되고 있다[2,4,8].

분산 SSO 에이전트는 사용자가 서버의 서비스 접근을 위해 SSO 에이전트를 접근 한다. SSO 에이전트는 사용자 인증을 위해 분산된 사용자 인증 정보를 추출하여 사용자를 인증하고 티켓을 발행하여 서버에서 제공하는 서비스 및 자원을 접근할 수 있다.

이러한 구조는 사용자의 인증 정보 보호를 SSO 에이전트에 의존하고 있다는 것이다. 완전한 사용자 인증 정보 추출을 위해서는 각 에이전트별로 분산되어 있는 사용자 정보를 카운팅을 통해 추출할 수 있다. 그러나 사용자 인증을 위한 각 에이전트의 기능이 누락되거나 다운되었을 때는 사용자 인증이 이루어지기 어렵다는 것이다. 클라우드 컴퓨팅에서 정보보호를 위한 시스템 안전을 위한 서비스도 중요하지만 실제 서비스 활용에 있어서 편의성과 용이성이 결여된다면 사용자의 불편과 함께 시스템 활용이 어려운 것이 사실이다. 이러한 보안 서비스의 유

용한 기능을 제공하기 위한 유연하고 보안이 강화된 서비스가 필요하다.

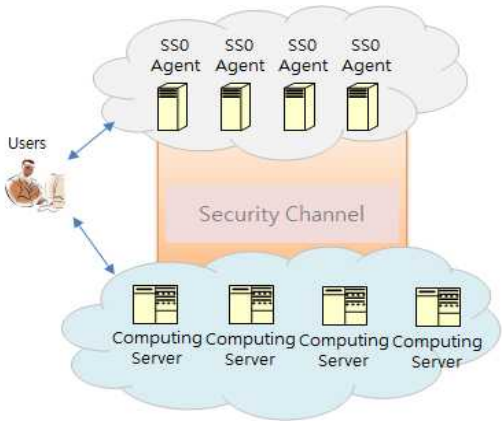


Fig. 2. Distributed SSO agent interface

III. SSO agent-based user authentication enhancement model

1. System configuration and overview

제안 시스템 구성은 그림 3과 같이 사용자와 SSO 에이전트, 서비스를 제공하는 서버 영역으로 크게 나뉜다. 사용자는 서버에서 제공하는 서비스를 받기 위해 SSO 에이전트로부터 인증 티켓을 발급 받는다. 발급 받은 인증 티켓을 접속하고자하는 서버에 전송하고 인증을 받은 후 정상적으로 서비스를 이용한다.

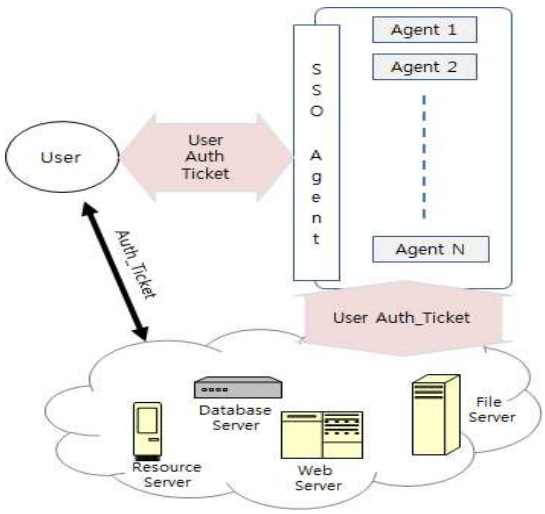


Fig. 3. System configuration

- User : 클라우드 컴퓨팅 서비스 이용자
- SSO Agent : SSO 서비스의 키 관리 및 사용자 인증 티켓을 생성하고 관리하는 시스템
- Resouce Server, Web Server, Database Server, File Server : 클라우드 컴퓨팅 서비스들
- Auth_Ticket : SSO Agent로부터 발급 받은 인증 티켓

2. Distributed SSO agent user authentication

2.1 User level management

분산 SSO 에이전트 환경에서는 사용자를 등급별 관리한다. 사용자 등급은 General_User, Authentication_User, Management_User로 구분하여 관리하고 권한 등급을 부여한다. 사용자별 등급 및 구분은 표 3과 같다.

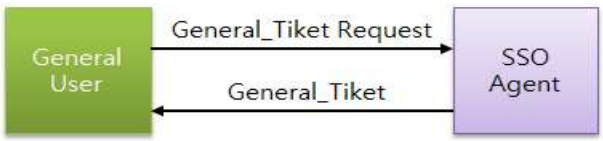
Table 3. User Level

User Level	Description
General User	Common users allowed to simply use multiple cloud servers
Authentication User	Common users allowed for user-specific session management and services and secure management of important domains
Management User	Administrators authorized to run the system, process, OS and programs for cloud system management and operation

2.2 User security level ticket

(1) General User

SSO 에이전트는 사용자별로 티켓을 발행한다. General User는 다음과 같이 사용자 정보를 확인하고 티켓을 발행한다. General User는 간단한 서비스를 위한 Ticket 요청으로 사용자 인증에 간편성을 제공한다.



[Packets between General User and SSO Agent]

- General_Ticket Request: {UserID, SK, TS1}
- Genera_Ticket: {EG,(KG,SK || TS2 || TicketSK || LevelNum)}

· General_Ticket Request : General User의 티켓 요청 패킷
· General_Ticket : SSO Agent가 General User에게 발급한 패킷
· SK(Section Key), TS(Time Stamp), KG,SK(공유키), LevelNum (사용자 등급)

(2) Authentication User

Authentication User는 정보 및 시스템 접근에 중요성을 가지고 있는 사용자로서 시스템 접근에 보안을 요하는 작업과 자원을 접근할 때 General User 보다 높은 권한을 부여한다.

General User의 패킷에 서버에 접근하여 활용하는 자원 및 서비스 리스트가 추가되고 사용자 고유 인증키를 요청한다.

Authentication User의 티켓 발행은 다음과 같이 이루어진다.

[Packets between Authentication User and SSO Agent]

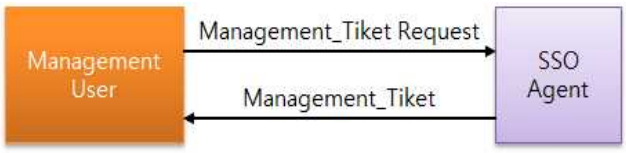
- Authentication_Ticket Request: {UserID, SK, ListSV, AuthK, TS1}
- Authentication_Ticket: {EA,(KA,SK || TS2 || TicketSK || LevelNum)}
- AuthK : EA,SA[IDA, ANA, TS3]

· Authentication_Ticket Request : Authentication User의 티켓 요청 패킷
· Authentication_Ticket : SSO Agent가 Authentication User에게 발급한 패킷
· SK(Section Key), ListSV(활용 서비스 및 자원 리스트), AuthK(Authentication User 고유 인증 키), TS(Time Stamp), KA,SK(공유키), LevelNum(사용자 등급),EA,SA)(SSO Agent와 Authentication User 고유키), IDA(Authentication ID), ANA (Authentication Network Address)

(3) Management User

Management User는 시스템의 예민한 영역을 다루고 접근할 수 있는 권한을 가진 사용자로서 가장 높은 보안 레벨을 적용한다. 로컬 시스템에 대한 인증을 강화하고 네트워크 및 사용자 인증을 포함한 네트워크 세션 관리가 적용된 티켓을 발행한다.

Management User의 티켓 발급 요청은 Authentication User의 패킷에 로컬 클라이언트의 Mac Address ID를 통해 사용자의 인증을 강화하고 Management User와 SSO Agent의 공개키를 이용하여 패킷을 암호화하여 이중으로 패킷을 보고하고 인증한다.



[Packets between Management User and SSO Agent]

- Management_Ticket Request: {SApk[MGID, SK, MMID, ListSV, AuthK, TS1]}
- Management_Ticket: {MPK[EM,(KM,SK || TS2 || SMID || TicketSK || LevelNum)]}
- AuthK : EMSA[IDM, MNM, TS3]

· Management_Ticket Request : Management User의 티켓 요청 패킷
· Management_Ticket : SSO Agent가 Management User에게 발급한 패킷
· SApk(SSO Agent의 공개키), MGID(Management ID), MMID(Management Mac ID), MPK(Management 공개키), EM,(Management 대칭키), KM,SK(Management User와 SSO Agent 공유키), SMID(SSO Mac ID), MNM(Manage ment User의 Network Address)

사용자 인증을 위한 보안 티켓을 SSO Agent는 발급하고 발급한 등급에 따라 서버의 접근권한이 부여된다. 또한 발급된 LevelNum에 의해 세부 접근 통제가 이루어진다.

3. Service Access Model

3.1 Resource management

클라우드 컴퓨팅 서비스의 자원은 표 4와 같이 중요도에 따른 등급에 의해 관리된다.

Table 4. Resource Security Level

Level	contents
1	· Top level · (Token authentication)Management User
2	· (General authentication) Management User
3	· Authentication User · (Part authentication)Management User
4	· Part Authentication User · General User
5	· Part General User

클라우드 컴퓨팅의 리소스을 위한 기본 보안 등급은 1부터 5까지의 보안 레벨을 가지며 접근자의 접근 유형에 따른 권한을 부여한다. 모든 리소스는 세부적인 접근 정책을 가진다. 시스템 운영을 위한 설정 등에 관한 리소스는 관리자의 보안 레벨을 적용하여 등급(1)의 권한으로 접근이 가능하고 설정이 아닌 뷰 및 관리를 위한 정보 운영은 등급(2)의 권한으로 운영이 가능하다.

시스템 사용자의 리소스는 개인의 최고 보안 등급설정으로 관리자가 내용확인 및 변경을 할 수 없는 권한 설정, 관리자까지 접근을 허용하는 권한 설정, 기타 시스템 운영을 위한 보안 레벨을 설정하여 접근권한을 적용할 수 있다.

그러나 사용자 인증을 서비스를 제공하는 SSO Agent의 접근이 원활하지 않을 경우에는 클라우드 컴퓨팅 서비스를 제공할 수 없다. 즉, 사용자 인증 강화를 위해 다중의 Agent로부터 인증 패킷을 받아 사용자 인증키가 생성되는데 인증 패킷을 못 받을 경우에는 클라우드 컴퓨팅 서비스를 받지 못한다. 이러한 경우에는 일부 인증 패킷만으로 서비스를 제공 받을 수 있다. 단, 본연의 보안 레벨이 아닌 낮은 보안 접근 레벨로서의 접근을 허용한다.

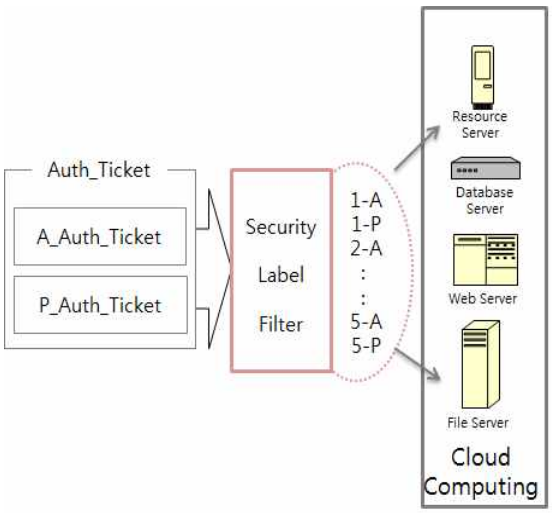


Fig. 4. Security Label Access

모든 Agent로부터 인증 받은 사용자는 그림 4에서와 같이 A_Auth_Ticket 패킷으로 인증을 받고 일부 누락된 인증 패킷을 받을 경우에는 P_Auth_Ticket으로 인증 패킷을 받는다. 이러한 인증 패킷은 보안 레벨 필터에 의해 각 사용자 레벨별로 접근을 허용하는 권한 정책이 적용된다. 보안레벨의 등급별 A는 정상적으로 인증 받은 보안레벨이고 P는 본연의 보안레벨보다 낮은 제한된 보안레벨이다. P_Auth_Ticket 패킷인증은 A_Auth_Ticket 패킷보다 낮은 단계의 권한이 설정된다. 예를 들어, 파일의 읽기, 쓰기 권한을 가진 사용자의 경우 읽기 권한만을 제공하며 쓰기권한 및 삭제 권한 등 파일에 대한 무결성 서비스에 대한 보안 서비스를 제공한다.

IV. Testing proposed system performance

1. Performance testing

제안 기술의 비교 평가를 위해 하나의 인증 에이전트와 다중의 에이전트를 활용하여 성능을 테스트하였고 다중의 에이전트는 분산된 에이전트환경에서 모든 인증 패킷으로 사용자 인증을 거친 정상 인증 패킷과 일부 누락된 인증 패킷에 대한 성능으로 테스트하였다. 실험을 위해 네트워크 트래픽은 약 1GB의 속도, 호스트 성능은 인텔 i7 모델에 적용하여 실험 환경을 구축하였다. 테스트는 각 영역별 15회를 기준으로 네트워크 환경에 적용하여 실험 데이터 추출 및 비교를 위한 기준값으로 결과를 분석하였다.

성능 테스트 결과는 그림 5와 같다. 하나의 에이전트를 활용한 인증과 다중의 에이전트를 활용한 인증으로 성능은 하나의 에이전트를 활용한 인증이 제일 빠르게 처리되고, 다중의 인증에서는 정상적인 인증이 일부 누락된 인증보다 성능이 높은 것으로 분석되었다.

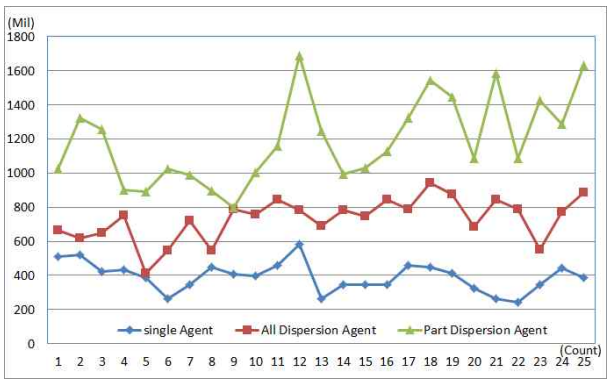


Fig. 5. Authentication processing performance

2. Experimental analysis and evaluation

제안 기술의 성능 테스트는 환경은 트래픽이 일정하지 않은 상황에서 테스트되어 안정적인 결과를 추출하지는 못하였다. SSO의 단일 에이전트를 기준으로 분산 환경의 에이전트를 테스트 비교하여 결과를 분석한다.

단일 에이전트는 하나의 인증서버에서 제공하는 네트워크 트래픽(Network_Traffic_Time)과 인증처리 시간(Authentication_Time)에 소요되는 시간으로 제일 작은 인증처리 시간을 갖고, 다중의 인증처리 중의 All Dispersion Agent는 네트워크 트래픽(Network_Traffic_Time)과 인증처리 시간(Authentication_Time), 인증정보조합(Authentication_Information_Join_Time)에 의해 인증 처리 시간이 측정된다. Part Dispersion Agent는 일부 인정 정보 누락에 의해 인증 티켓을 생성하고 있다. 인증시간은 네트워크 트래픽(Network_Traffic_Time)과 인증처리 시간(Authentication_Time), 인증정보조합(Authentication_Information_Join_Time), 질의/응답 지연 시간(Q&A_Delay Time)으로 제일 많은 인증 처리 시간이 소요된다. 질의/응답시간지연 시간은 네트워크 클라이언트 서버간의 통신에서 서버가 응답을 하는데 걸리는 시간으로 서버의 응답이 실시간으로 처리되지 못하여 응답 유효 최대시간에 해당한다. 즉, 서버가 정상적으로 작동되지 않는 경우에는 클라이언트는 자동으로 서버의 응답을 위해 재전송 패킷을 발행하고 응답 유효시간을 넘기면서 응답처리 시간이 지연되는 것이다. 인증 처리 시간을 정리하면 다음과 같다.

- Single Agent : Network_Traffic_Time + Authentication_Time
- All Dispersion Agent : Network_Traffic_Time + Authentication_Time + Authentication_Information_Join_ Time
- Part Dispersion Agent : Network_Traffic_Time + Authentication_Time + Authentication_Information_Join_Time + Q&A_Delay Time

Part Dispersion Agent가 All Dispersion Agent 보다 많은

시간이 소요된다. 하지만, All Dispersion Agent는 인증을 위한 다중의 에이전트 중에서 하나라도 인증 패킷을 생성하지 못하거나 인증 패킷의 에러가 발생한다면 사용자는 클라우드 컴퓨팅 서비스를 활용하지 못한다. Part Dispersion Agent는 이러한 경우에 대응한 서비스로서 인증 속도는 느리지만 서비스 제공측면에서는 장점이라 할 수 있다. 제안시스템의 에이전트 시간 복잡도는 다음과 같다.

$$(\sum_{1}^{N} Attack_n Time) + AttackTime!$$

제안 시스템은 다중 분산 SSO 에이전트의 시간복잡도와 같다. 하지만 접근제어 정책이 적용되어 보다 안전성이 강화된 보안 기능을 제공한다.

보안 등급은 1~5등급을 갖는다. 각 등급은 등급별로 허가된 접근권한과 일부 제한된 접근권한으로 리소스를 접근할 수 있다. All Authentication Ticket을 발급받은 사용자는 자신의 리소스 권한과 시스템의 일부 제한기능영역에서의 일반적인 권한으로 리소스를 접근할 수 있다. 하지만, Part Authentication Ticket을 발급받은 사용자는 자신의 리소스의 모든 권한(Read/Write/Delete/Create/Execute 등)에서 일부 제한된 기능(Read)을 갖는다.

V. Conclusions

본 논문은 다중의 SSO 에이전트 인증 환경에서 클라우딩 컴퓨팅 서비스 접근 정책을 강화하여 안전한 리소스 보호 기술을 제안하였다. 보안 강화를 위해 다중의 SSO 환경에서 클라우드 컴퓨팅 서비스를 제공하고 사용자의 원활한 서비스 활용을 위해 상황별 안전한 접근권한 정책을 적용하였다.

다중 SSO 에이전트 인증 모델에서는 인증 에이전트의 비정상 작동 및 인증 패킷의 손실에 의해 클라우드 컴퓨팅 서비스를 받을 수 없다. 이러한 문제의 해결방안으로 보안 등급 조정을 통해 클라우드 컴퓨팅 서비스 접근 권한을 제안한 서비스를 제공할 수 있도록 하였다. 또한 리소스의 보호를 위한 각 사용자별 리소스 권한 정책을 적용하여 안전한 클라우드 컴퓨팅 서비스를 제공할 수 있도록 하였다. 제안 시스템은 기존의 SSO 에이전트 인증 기술 보다는 속도가 느리다. 하지만 현재 네트워크 트래픽에 적용한 체감 속도는 많은 차이를 못 느끼고 있으며 향후 기가급 이상의 네트워크 속도가 제공된다면 많은 문제가 되지 않을 것으로 본다.

REFERENCES

[1] Jeong-hoo Jeon, “A Study on the vulnerability of the Cloud computing security”, Journal of the Korea Institute of Information Security & Cryptology, Vol. 23, No. 6, pp 1239-1246, December 2013.

[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, Vol. 21, No. 4, pp.31-38, April 2016.

[3] Jeong-Su Park, Yu-Mi Bae, Sung-Jae Jung, “Journal of the Korea Institute of Information and Communication Engineering”, Vol. 17, No. 5, pp. 1129-1137, May 2013.

[4] Yoon-Su Jeong, Sang-Ho Lee, “User Authentication Protocol through Distributed Process for Cloud Environment”, Journal of the KIISC, Vol. 22, No 4, pp. 841-849, August 2012.

[5] DongHee Kim, JinTak Choi, “A Study on The Efficient Authentication Management Technique of SSO Foundation”, Journal of Korea Institute of Information Technology, Vol. 4, No. 3, pp.55-63, June 2006.

[6] Hyun-Jin Kim, Im-Yeong Lee, “A Study on Security and Improved Single Sign-On Authentication System against Replay Attack”, Journal of the Korea Institute of Information Security & Cryptology, Vol. 24, No. 5, October 2014.

[7] Eun-Gyeom Jang, “A Study on Access Control Through SSL VPN-Based Behavioral and Sequential Patterns”, Journal of The Korea Society of Computer and Information, Vol. 18, No. 11, November 2013.

[8] Dae-Hee Seo, Im-Teong Lee, “A Study on Single-On Authentication Model Using Multi Agent”, The Journal of The Korea Institute of Communication Sciences“, Vol. 29, No. 7C, July 2004.

Authors

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