Journal of The Korea Society of Computer and Information
Vol. 24 No. 8, pp. 67-76, August 2019

www.ksci.re.kr
https://doi.org/10.9708/jksci.2019.24.08.067

System Access Control Technique for Secure Cloud Computing

Eun-Gyeom Jang*

Abstract

Along with the diversification of digital content services using wired/wireless networks, the market for the construction of base systems is growing rapidly. Cloud computing services are recognized for a reasonable cost of service and superior system operations. Cloud computing is convenient as far as system construction and maintenance are concerned; however, owing to the security risks associated with the system construction of actual cloud computing service, the ICT(Information and Communications Technologies) market is lacking regardless of its many advantages. In this paper, we conducted an experiment on a cloud computing security enhancement model to strengthen the security aspect of cloud computing and provide convenient services to the users. The objective of this study is to provide secure services for system operation and management while providing convenient services to the users. For secure and convenient cloud computing, a single sign-on (SSO) technique and a system access control technique are proposed. For user authentication using SSO, a security level is established for each user to facilitate the access to the system, thereby designing the system in such a manner that the rights to access resources of the accessed system are not abused. Furthermore, using a user authentication ticket, various systems can be accessed without a reauthorization process. Applying the security technique to protect the entire process of requesting, issuing, and using a ticket against external security threats, the proposed technique facilitates secure cloud computing service.

▸Keyword: SSO, cloud computing, access control, Authentication

I. Introduction

Cloud computing provides virtualized IT resources as a service. The IT resources are leased, and the user pays for its cost according to usage. Recently, global IT companies such as Amazon, Microsoft, Google, and IBM have been involved in cloud computing. The supporting technology factors include virtualization technology security, large volume distribution processing technology, service availability, large volume traffic handling, application security, access control, and authentication and password. Furthermore, cloud computing requires resource management, access control, and authentication technologies to ensure the security of various resources [1- 3].

The user account management technologies for system access include single sign-on (SSO), extranet access management (EAM), and identity access management (IAM). SSO is a solution that supports access to several systems with one-time authentication, which enhances user convenience and administration cost reduction as the user can access various systems and services with just one account without going through multiple authentication processes. EAM is a glossary defined by Gartner Inc. [2],

• First Author: Eun-Gyeom Jang, Corresponding Author: Eun-Gyeom Jang
*Eun-Gyeom Jang (jangeg@jangan.ac.kr), Dept. of Internet Communication, Jangan University

• Received: 2019. 05. 21, Revised: 2019. 07. 31, Accepted: 2019. 07. 31.
• The Work was supported by Jangan University Research Grant in 2019

and it uses a security policy-based single mechanism to manage user access for applications and data while managing SSO and user authentication. IAM is a concept expanded comprehensively, and it is known by several different names, including identity management (IM), account management solution, and integrated authentication management [2, 4, 5].

Cloud computing provides convenience and usability when constructing and managing servers from a utilization perspective and is cost-effective; however, from the standpoint of users and administrators, it requires confidentiality, usability, accessibility, and ease of use for information. To provide security and convenience of service to the users based on these requirements, the computing service should provide accessibility using an SSO model and security with enhanced user authentication process as the top priority.

In conventional studies, user convenience is enhanced by providing cloud computing services using SSO. However, information security service is unsatisfactory owing to the service environment, in which only convenience is provided while private information of users is insufficiently protected. Therefore, in this study, a system access enhancement model is proposed to provide convenience to the users using the SSO service through a cloud computing environment while providing system and service reliability from the perspective of users and administrators.

In this paper, a study was conducted for the system access enhancement model by applying the security levels according to the authentication process and procedure to solve the security problems during authentication by multi-dividing the SSO service in the conventional cloud computing environment.

II. Literature Review

2.1 Cloud Computing Service

Cloud computing can be classified into private cloud, public cloud, hybrid cloud, and community cloud. As shown in Table 1, the typical service types are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) [4, 6, 7].

Cloud computing reduces the cost of introducing IT infrastructure and provides a standard development platform as well as efficiency in the integrated management and maintenance of systems or applications, thereby offering many advantages in economic efficiency and convenience such as reduction of development period and prevention of duplicate investment for development environment.

Conversely, as all IT resources in cloud computing are concentrated in the data center of the service provider, the services of users can be interrupted when the cloud service is disrupted, and security risk is increased. Particularly, there are drawbacks such as user information leaks and data loss due to hacking and cyberterrorism.

Table 1. Cloud Service Types

Type	Description
SaaS	(Leasing and providing software) Software is provided through the Internet, and a user connects remotely, and various software are provided as a leased service. To the users, the environment setting of service limited and it is impossible to manage and control the cloud infrastructure.
PaaS	(Leasing and providing platform) A system environment is provided to allow users to directly develop software and provide services. The users do not have administration/control rights for the cloud infrastructure, network, server, operating system, and storage but can have administrator rights for the system environment configuration of hosted applications and applications constructed by user.
IaaS	(Leasing and providing hardware resource) Server infrastructure is provided as a service that provides the processor, storage, network, and other basic computing resources when the user develops or operates software. Typical services include Amazon Web Service's storage service S3 and EC2.

2.2 Cloud Computing Security Threats

Gartner, UC Berkeley, and EINSA deal with the security threat factors as follows [4, 6].

- Gartner: authorized administrator's access, policy, recovery, data storage location, investigation resource, data separation, long-term survivability
- UC Berkeley: service availability, data lock-in, data confidentiality and monitoring, data transmission disruption factor, uncertain performance prediction, scalable storage, large-scale distribution system bug, fast scaling, reputation sharing, software licensing
- EINSA: administration absence, difficulty of isolation, dependence on service provider, regulation threat, data protection, administration interface enhancement, unsafe data deletion, malicious insider

Common security threats include malicious use and abuse of cloud computing, malicious internal user, vulnerability of shared technology, data loss, data leak, hijacking of user account service and traffic, and unknown risk profile. They can be viewed as threat factors of IT systems in general rather than those of cloud computing.

Gartner focuses on the resource access and data management area; UC Berkeley on the cloud service and data management and operation; and EINSA on the threats for cloud service operation. In such diverse areas, the threats are consistent to cloud computing.

2.3 SSO

2.3.1 SSO System

SSO is an authentication technology whereby various services can be used with just one authentication. The systems that provide this function include Kerberos architecture, SESAME, RSAKeon, and SuitSpot [8, 9].

- Kerberos architecture: Kerberos architecture is a Public Key Infrastructure (PKI)-based architecture and provides strong security service while providing public key-based architecture. It includes Public Key Cryptography for initial authentication (PKINIT) and Public key based Kerberos for Distributed Authentication (PKDA) protocols. With PKINIT, initial authentication is done at Key Distribution Center(KDC) on the basis of authentication certificate; and PKDA provides convenience in user authentication, which uses the authentication protocol between user and server without the intervention of a central authentication server. However, since the service is performed based on PKI, there is a burden for symmetric keys, and a limitation exists in the legacy system scalability. The functions provided include Public-key cryptography (PKC)-based user authentication, cross-certification, and non-repudiation.
- SESAME: SESAME reduces the burden of key management by providing a distributed access control function on the basis of Kerberos. However, the problem regarding the PKI-based symmetric keys still exists, the burden for distributed access control is increased, and the problem for the legacy system is not solved. The functions provided include access control, PKC-based user authentication, cross-certification, and non-repudiation.
- RSAKeon: RSAKeon has a structure that facilitates central integrated access control in the extended field of x.509 v3 certificate and scalability of the legacy system. It has an enhanced structure compared to Kerberos and SESAME. The burden is also reduced for symmetric keys. However, because a reauthorization process is required when reconnecting a session, there is a burden for authentication. The functions provided include access control, PKC-based user authentication, cross-certification, non-repudiation, and legacy system support.
- SuitSpot: SuitSpot has problems for integrated access control and legacy system's SSO scalability, but the service is performed with a simple structure because it facilitates authentication between client and server without going through the authentication server. The functions provided include PKC-based user authentication, cross-certification, and non-repudiation.

2.3.2 SSO Authentication

The biggest purpose of SSO is to provide user convenience. However, user convenience carries risks in the system management and security aspects. To support user convenience and security together, services are provided by loading security functions such as encryption, authentication, and non-repudiation in the SSO design itself.

A centrally integrated and managed SSO service authorizes the use of various services without the reauthorization process and uses lightweight directory access protocol (LDAP). Furthermore, there is a restriction in the authentication domain and authentication system, and a separate program is operated for administration and operation. In Oracle also, a cookies-based SSO service model is applied, and although the specific structure and functions are different, it is operated based on the cookies server [9, 10, 11].

When classified according to system structure, there exist Broker-based, Agent-based, Agent-Broker-based, and Gateway-based SSOs. Broker-based, Agent-Broker-based, and Gateway-based SSOs facilitate efficient centralized system management. There are minor modifications of conventional application programs for the Agent-based and Agent-Broker-based SSOs. However, the Broker-based SSO requires modification of conventional application program, and with the Agent-Broker-based SSO, management is difficult due to the increase of components, and the Gateway-based SSO has a drawback that synchronization is required between several gateways [9, 10].

User authentication methods can be divided into authentication proxy and authentication information transmission methods. In the authentication proxy, an agent processes the user authentication by proxy, thereby guaranteeing the safety between user and agent, and it has a relatively secure service structure. In the authentication information transmission method, an agent authenticates a user and communicates with the user by using a token. This method is vulnerable to sniffing and replay attacks since the authentication information is interfaced through the client [9, 10].

2.3.3 SSO Vulnerabilities

Following is an analysis of vulnerabilities for respective SSO service areas [12].

- Encryption Algorithm Management: When encrypting at least one block of plain text, if the operation mode of the block encryption algorithm event control block (ECB) is applied, it is vulnerable to dictionary attack.
- Authentication Information Exposure and Reusability: The user authentication information through the network can be exposed to an unauthorized third person. The authentication information can be collected and reused by the attacker.
- Key Management: A session key for communication between servers can be used as fixed, and the user session key can be reused.
- Session and Security Audit: If a session of administrator and user program is continuously connected, it can be exposed to an attack by a third person.
- Interoperation Module: The user information can be exposed when an integrated security is not in place in the interface area for execution of SSO product and other functions.

The vulnerabilities of SSOs are similar to those in general network and system operations. The SSO security threat factors cover all areas including encryption for information exposure prevention, key and session management for user and system authentication, session and encryption for network packet protection, and authentication.

2.4 Access Management of BLP Model

Bell and LaPadula (BLP) model is a mathematical model that applies policies to prevent illegal information leaks by using communication to maintain security. BLP consists of a set of subjects (S), set of objects (O), and security level for respective subject and object (C). The basic properties are as follows:

- Simple Property: The subject S can read the object O only when C(S) >= C(O);
- Star Property (*Property): The subject S can write on the object O only when C(S) <= C(O).

The BLP model, which uses the above two properties, is applied to a system, thereby managing the access of subject and object by security level. Figure 1 illustrates the properties of the BLP model.

In the BLP security model, there is a problem that a subject of lower security level permits write privilege to an object of higher security level. In other words, an object of lower security level can have a higher security level; there is also a loophole that a subject can intentionally change an object of higher security level.

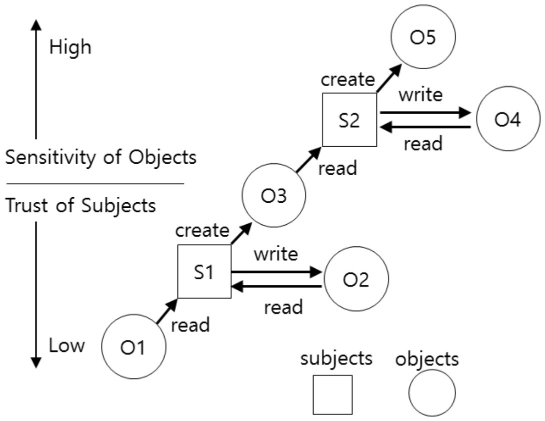


Fig. 1. Properties of BLP

III. System Access Control using Multiple SSO Agents

As shown in Fig. 2, the proposed system configuration is divided into two areas: SSO agents responsible for user authentication and the server area providing the services. A user proceeds with the authentication process through the agent managing the user authentication. The login information of users belongs to the management agent for the respective user, and it is distributed for management purposes.

A user who receives a normal authentication packet sends a request packet for server and service. For the requested service, the system access control agent grants the right, thereby providing control signals to let the user access the requested server and service.

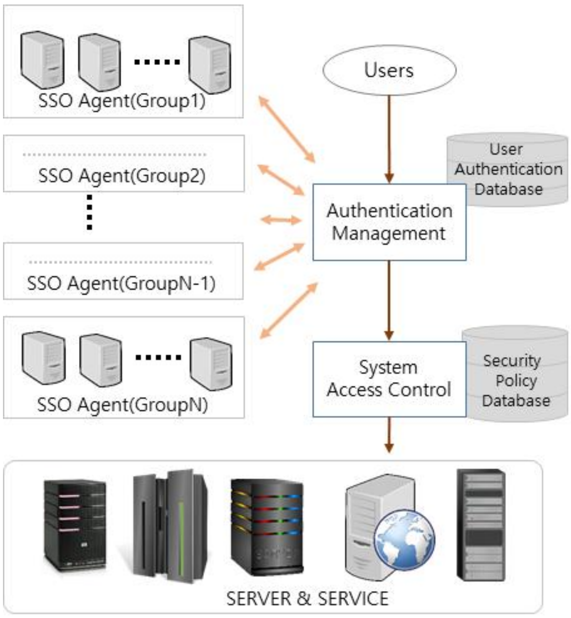


Fig. 2. System Configuration

3.2 User Authentication Management

3.2.1 User Authentication Level

To access the SSO system, user registration must be performed. By setting the authentication method simultaneously when registering a user, the authentication process can be set differently for each user. As shown in Figure 3, the single SSO authentication method and the multiple SSO authentication method can be applied, and the authentication method and process are applied according to the level of system and user rights.

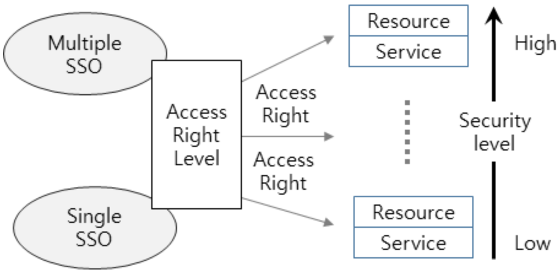


Fig. 3. Access Right Processing

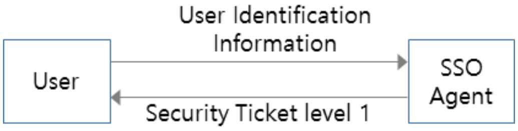
The right to use the system is granted to a user of single SSO according to the authentication process applied to an existing SSO system. However, depending on the use right level for the server and service access, limited functions can be performed. On the other hand, a specific access right can be granted to a user of multiple SSOs since the authentication is managed by several SSO agents. Furthermore, it has high service availability characteristics since a dynamic authentication process is applied.

3.2.2 Authentication Process

User authentication is largely divided into single SSO and multiple SSO user authentications. A multiple SSO user is classified using three security levels, and an authentication ticket is generated. In summary for the authentication ticket, ticket level is set to 1 for the single SSO users, and the ticket levels are set to 2, 3, and 4 starting from lowest security level for the multiple SSO users.

(1) Single SSO Ticket

The security ticket level 1 is the security level of single SSO user and the user authentication process is performed by the single SSO agent. The authentication ticket is generated as follows.



- User Identification Information: It contains the unique information for user identification and sends a user authentication request packet by using the pre-shared session key of user and server. The user authentication request packet is shown in Fig. 4.

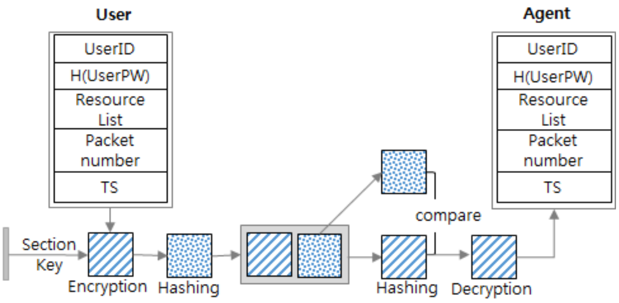


Fig. 4. Single SSO Authentication Request Packet

$$\{E_{SK}(UserID \mid\mid R\text{-}ReList_{num} \mid\mid UserPW_{Hash} \mid\mid Packet_{num} \mid\mid TS_1) \mid\mid Packet_{Hash}\}$$

▪ Security Ticket Level 1: The SSO agent who receives the user authentication request packet authenticates the user identification information and issues a ticket for the use of requested resources (server and service) to the user. The issued ticket consists of the following.

{E_{SK}(AgentID || CS_K || $Packet_{num}$+ 1 || A-$ReList_{num}$ || TicketID || TS_2) || $Packet_{Hash}$}

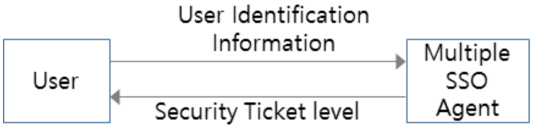
· E_{SK}: encrypts with the session key pre-shared between the SSO agent and user
· UserID: user's unique identification value
· R-$ReList_{num}$: resource number for the access requested by user
· A-$ReList_{num}$: authentication number for the resource requested by user for access
· $UserPW_{Hash}$: user password hash value
· $Packet_{num}$: packet number
· TS1: a time stamp used for the expiration time of ticket
· $Packet_{Hash}$: hash value of transmitted packet and validates the integrity of packet
· ||: delimiter for items
· AgentID: a unique identification value of SSO agent who issued the ticket
· CV_{SK}: is the session key between the user and server, and is used as a shared session key of the authenticated user and resources (server and service)
· TicketID: issued ticket number

The user authentication request packet identifies the user with UserID and authenticates the user with $UserPW_{Hash}$. $Packet_{num}$ is an identification number for packet management; TS1 guarantees the validity of packet; and $Packet_{Hash}$ guarantees the integrity of user authentication request packet.

The security ticket authenticates the subject of authentication with AgentID that performed the authentication and shares a communication secret key with the server to be accessed via C_{SK}. A-$ReList_{num}$ contains the unique identification value of resource accessible by the user and the ticket's identification code and validity is verified with TicketID.

(2) Multiple SSO Ticket

A multiple SSO ticket has the security ticket level 2, 3, or 4. The security ticket request and issue packet comprise the following.



▪ User Identification Information: based on the public key, the user authentication request packet of multiple SSO user enhances the security service for the packet. It provides a digital signature service by encrypting the authentication request packet with the private key of the user. The authentication request packet is composed of the following.

{PR_{User}[ESK(UserID || R-$ReList_{num}$ || $UserPW_{Hash}$ || $Packet_{num}$ || UserNA || MacA ||$EnCryList_{Al}$ ||$HashList_{Al}$ || TS_1)] || $Packet_{Hash}$}

▪ Security Ticket Level: the response ticket for the user authentication packet of multiple SSO user is composed of the following.

{PR_{Agent}[E_{SK}(AgentID || CS_K || $Packet_{num}$+ 1 || A-$ReList_{num}$ || TicketID || $Ticket_{Status}$ || Sec_{Level} || $EnCry_{Al}$ ||$Hash_{Al}$ ||TS_2)] || $Packet_{Hash}$}

· PR_{User}: user's private key
· UserNA: user's network IP Address
· MacA: user's system MAC Address
· $EnCryList_{Al}$: encryption algorithm list
· $HashList_{Al}$: hash function list
· $EnCry_{Al}$: utilized encryption algorithm
· $Hash_{Al}$: utilized hash function
· PR_{Agent}: agent's private key
· AgentID: agent's unique identification value
· $Ticket_{Status}$: ticket status
· Sec_{Level}: security level

For security authentication level 2, UserNA and MacA among the packet composing elements are configured with a null value, and for ticket level 3, MacA has a null value. Furthermore, TS of ticket level 3 and 4 have a difference in the validity of tickets. That is, ticket level 4 has a shorter value for the validity.

The user authentication request packet is encrypted with the private key of the user (PR_{User}), and the integrity of an encrypted packet is guaranteed by $Packet_{Hash}$. The packet is encrypted by the pre-shared key of user and agents (E_{SK}), and user authentication is strengthened by the identification addresses of network and system in the user area. $EnCryList_{Al}$ and $HashList_{Al}$ send the user encryption algorithms and hash algorithms by composing them as lists. In other words, the agent selects one each ($EnCry_{AI}$, $Hash_{AI}$) from the lists of algorithms and sends them to the user.

The security ticket issued by the agent is digitally signed by encrypting it with the private key of the agent, and it contains PacketHash for the integrity of the packet. For secret communication with the server to be accessed, the user uses the shared key (CS_K). The accessible resource of the issued ticket is identified by $A\text{-}ReList_{num}$. $Ticket_{Status}$ is the status information of ticket and in the case of multiple SSO authentication, a situation can arise where the agents used for authentication cannot all be authenticated normally. In this case, the normal status is set to “1”, and the rest are set to “0”. The security level for the ticket is Sec_{Level}, and the access right for the resource is checked and authenticated.

3.3 Resource Access Control

The resource access policies were designed by solving the problem occurring in the BLP security model, as a subject of lower security level is permitted to write on an object of higher security level.

The ticket acquired by the user has a right to access the resource through the security level. For the subject S of security level, the access right policies are applied as shown in Fig. 5.

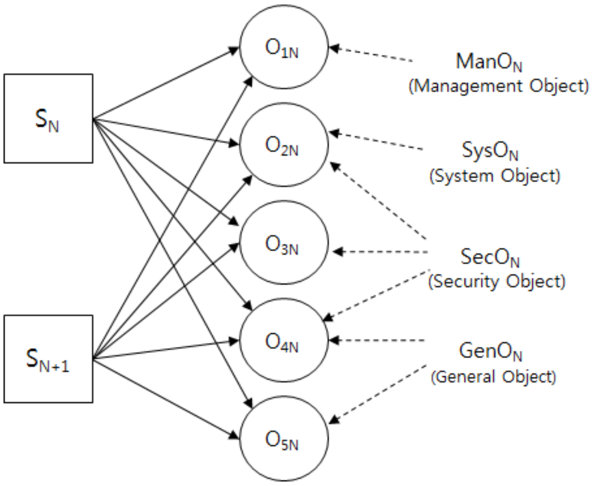


Fig. 5. Access Right Policies for Objects

As for the subject S, there are mutually different subjects SN and S_{N+1}. Figure 4 shows the structure, in which the subjects S access the objects O, and the security level of subject SN is identical to the security level of object O_N. It also shows the access right when S_{N+1} accesses the object O_N of different security level.

For O_{1N} through O_{5N}, the security level of the object is N, and it is distinguished according to the security attributes of the object. The description for each object ON is as follows.

- O_{1N}: as management object, it is an object needed for system management
- O_{2N}: as system attribute object, it is an object that requires security
- O_{3N}: the object requiring security attribute
- O_{4N}: as a regular object, it requires security
- O_{5N}: a regular object

As the subject and object of the same security level, S_N and O_N grant the read rights to the objects of $ManO_N$, $SysO_N$, and $SecO_N$ attributes. That is, they have the read rights for the objects O_{1N}, O_{2N}, O_{3N}, and O_{4N}. The read, write, and modify rights are possible for O_{5N} only.

With respect to the subject with high security level S_{N+1}, only the read right is possible for objects having the attributes of $ManO_N$ and $SysO_N$, and access is not allowed for write and modify. That is, O1N and O2N objects have the read right only. O_{3N}, O_{4N}, O_{5N}, which have $SecO_N$ and $GenO_N$ attributes, have the read, write, and modify rights. But, O_{3N}, which has only the attribute of $SecO_N$, the access policy can be applied by the object owner.

The security level and access right policy of an object can be determined by the owner of the object; however, for important objects of security and system operation, a kernel for object access is additionally managed to strengthen the security.

IV. Performance Analysis

Cloud computing using SSO agents classifies the access rights of users into single SSO and multiple SSO, and the multiple SSO is classified by subdividing into 2/3/4 levels. For the classified four levels, the access rights of system and resource are sub-classified, and the security level is applied by area. This prevents abuse of right by granting a minimum right. The performance of the proposed system in this paper is analyzed and evaluated by focusing on the security of network and objects.

4.1 Single SSO Ticket Analysis

Single SSO ticket is a user authentication service, in which a user uses one SSO agent, and it verifies that the user is legitimate when accessing the cloud computing resources. The user is identified and authenticated with UserID and UserPW$_{Hash}$. Packet$_{num}$ and TS$_1$ are values used to respond to counterfeit and modification of packet, and the validity of packet can be checked between the user and agent. The packet composed in this way is encrypted with a pre-shared key of agent and user, thereby providing confidentiality. The agent authenticates the packet by comparing it with the Packet$_{Hash}$ value to guarantee the integrity of encrypted ciphertext. Packet$_{Hash}$ is the hash value of ciphertext encrypted by E$_{SK}$. The agent issues an authentication ticket by confirming the access right of an authenticated user for the relevant resource.

The agent who receives the authentication request packet authenticates the packet and user and protects the packet in the network area by encrypting Packet$_{num}$ + 1 (a response for the authentication request), A-ReListnum (the access permission resource list for the resources), R-ReList$_{num}$ (the resource requested by user for access), TicketID (the ticket identification number to be used by user), and TS$_2$ (expiration time of ticket). The integrity of ciphertext is verified with the hash value of packet (Packet$_{Hash}$). The security service of simple SSO authentication is as follows.

- User and agent authentication: UserID, UserPW$_{Hash}$, AgentID
- Confidentiality of packet between user and resource: CS$_K$
- Integrity and authentication of the packet: PacketHash, Packet$_{num}$
- Confidentiality of packet: E$_{SK}$
- Resource access right: R-ReList$_{num}$, A-ReList$_{num}$
- Validity of ticket: TicketID, TS$_1$, TS$_2$

4.2 Multiple SSO Ticket Analysis

For the multiple SSO ticket, the ticket is issued according to the level by the security interface of user and multiple agent management process. To authenticate the user, UserID (user identification), UserPW$_{Hash}$ (user authentication), UserNA (user access network authentication), and MacA (user system authentication) are confirmed, thereby certifying he/she is a legitimate user. EnCryList$_{Al}$ and HashList$_{Al}$ are the lists of encryption and hash algorithms, respectively, for communication with the cloud resources, and they are the lists of algorithms that can be used by a user. The algorithms are put in the lists because they have an effect of providing complexity in decryption of ciphertext to the external attackers. The packet for a user's authentication request is encrypted with the pre-shared session key of agent and user, and the ciphertext is encrypted with the private key to provide the digital signature service. The integrity of a packet is verified with the hash value of the packet (Packet$_{Hash}$).

The ticket generation for user authentication request provides integrity and non-repudiation functions of the packet through the digital signature using the private key of the agent. Moreover, encryption (ES$_K$) is performed to maintain the confidentiality of the packet. The integrity of an encrypted packet can be verified by Packet$_{Hash}$.

The normal issue status (Ticket$_{status}$) and security level (Sec$_{Level}$) of ticket determine the access right of the resource (A-ReList$_{num}$). The multiple SSO ticket's authentication request packet and generated ticket provide the following security service.

- User and agent authentication: UserID, AgentID, UserNA, MacA, UserPW$_{Hash}$
- Confidentiality of packet between user and resource: CS$_K$
- Integrity and authentication of packet: Packet$_{num}$, Packet$_{Hash}$, EnCryList$_{Al}$, HashList$_{Al}$, EnCry$_{Al}$, Hash$_{Al}$
- Confidentiality of packet: ES$_K$
- Digital signatures of user and agent: PR$_{User}$, PR$_{Agent}$
- Resource access right: R-ReList$_{num}$, A-ReList$_{num}$, Ticket$_{Status}$, Sec$_{Level}$
- Validity of ticket: TicketID, TS$_1$, TS$_2$

4.3 Resource Access Right Analysis

The rights for object (O$_N$) of subject (S$_N$) having the security level N are sub-divided by the attributes of the object, thereby restricting the access rights. Even if the security levels of subject and object are identical, the access rights are restricted by the attributes of the object. Since an object having the attribute values of ManON, SysON, and SecON has sensitive information of system and user, it has the read right to protect the object even if the security levels of subject and object are the same. Furthermore, a subject whose security level is one level higher (S$_{N+1}$) is granted only the read right for the object having the attributes of ManON and SysON.

Regardless of how high the security level is, this is to maintain a secure system by allowing modification to only the subject having the highest right to protect the system as the object area needed in system management.

4.4 Security Service of Proposed System

Based on the security threat factors, the proposed system was analyzed and its performance was evaluated.

4.4.1 (Confidentiality)

Exposure of user and agent information: when the user's identification code ID and password are exposed, in the case of single SSO, the ticket cannot be issued since the pre-shared session key cannot be obtained. However, if the session key and user information are exposed, a valid ticket will be issued and the cloud resource will be accessible. But, the single SSO agent authentication ticket has a low level of access right to the object. For the multiple SSO agents, user authentication cannot be done since the user's network address and system's MAC information do not match.

4.4.2 (Confidentiality)

Exposure of packet by sniffing: confidentiality is provided by encrypting with the shared session key of user and agent. Also, additional information of network necessary for user authentication is needed.

4.4.3 What if a third person acquired a valid ticket?

Even if the packet, which is digitally signed with a private key, is decrypted, since the ticket was encrypted with a session key, a corresponding ticket cannot be generated even when the cloud computing resource is accessed.

4.4.4 (Integrity)

Modification of authenticated packet: when the content of a packet is modified, it is possible to identify whether the packet was modified since the hash value attached to the packet is different.

4.4.5 (Authentication)

Access to system and object requiring security by using a valid ticket: When an attacker acquires a session key-exposed ticket, a normal clouding service is impossible since the user's network and system's MAC address cannot be authenticated.

4.4.6 (Access Control)

A normal user accesses the cloud computing resources and tries to access the files of the system, confidentiality, or higher security level: the user has no right to access the resources having security levels higher than that of the user, and only read permission is possible for the system and confidential files, thereby minimizing the access right to resources.

4.5 Comparison with Conventional Technology and Analysis on Proposed Technology

The security service of 'single SSO agent' applied in this study was implemented by improving conventional research technologies. In conventional SSO technologies, as described in Section 4.4.1, the ticket can be protected even if the ID and password of the user are exposed, but the ticket cannot be protected when the session key and user information are exposed. To solve this issue, this study maintained the access rights of the ticket users who use a single SSO agent as low as possible to protect the system.

In the conventional technologies, a single SSO agent has been used, which is a target of intensive attacks and is highly vulnerable to information leakage. However, this study managed multiple authentication tickets and created the ticket by combining the authentication information through mutual authentication. Thus, it is safer from an external attack than using a single agent.

The security service is applied according to the level of the ticket generated by the SSO agent. Depending on the security level of the ticket, access rights to media and service are granted or restricted, thus allowing the safe protection of the system. The authentication ticket is a security key for accessing media and services. The ticket issued can be used to access various systems, and the validity of the ticket enables the system to be protected against the ticket leakage.

This study is similar to conventional technologies in that the ticket is used to access services and media. However, this study provides SSO service by supplying security services against the leakage of the ticket and distributing problems arising from the attacks to the ticket management system through multiple management systems.

V. Conclusion

In this paper, a system access control enhancement method in the cloud computing service environment was studied. To increase the effectiveness of security while maintaining user convenience of cloud computing, an SSO agent was utilized. To enhance the security of cloud computing that uses a single SSO agent, user authentication using multiple SSO agents was proposed, and the cloud computing access control of authenticated user was strengthened.

The primary goal of the proposed technique is to enhance the security and maintain a safe system by minimizing the resource access rights of cloud computing by area while providing user convenience. In accordance with the goals of this study, user convenience was maintained by generating tickets using SSO agents, and the abuse of rights was restricted by granting the resource access rights according to the security level of each ticket. Also, through enhancement of security, the proposed system was protected from the security threat factors in each area.

To increase the utilization of the proposed technique, specific policies and technique elements are needed to fit the environments of system, network, and operating system. It is expected that the security-enhanced cloud computing service will be implemented if the access right policies are applied for each system resource.

The Work was supported by Jangan University Research Grant in 2019.

REFERENCES

[1] Hyundong Lee, Mokdong Chung, “Context-Aware Security System for Cloud Computing Environment,” Journal of IEIE 6 (2010) 19-27 DOI: 10.5573/ieie.2014.51.6.143

[2] Brian Hayes, “Cloud computing,” Communication of the ACM 7 (2008) 9-11 DOI: 10.1145/1364782.1364786

[3] Erdal Cayirci1, Anderson Santana de Oliveira, “Modelling trust and risk for cloud services”, Journal of Cloud Computing, Advances, Systems and Applications 7 (2018) DOI: https://doi.org/10.1186/s13677-018-0114-7

[4] Souhwan Jung, “Cloud-based IAM technology trends,” Journal of KICS 10 (2015)

[5] Saurabh Dey, Srinivas Sampalli1, Qiang Ye, “MDA: message digest-based authentication for mobile cloud computing”, Journal of Cloud Computing, Advances, Systems and Applications 5(2016) DOI: 10.1186/s13677-016-0068-6

[6] Gi Hong Park, Si Young No, “Cloud Service for the forensic aspects of the investigative methods,” Journal of KSIIS 1 (2012) 39-46

[7] Sima Soltani, Patrick Martin, Khalid Elgazzar, “A hybrid approach to automatic IaaS service selection”, Journal of Cloud Computing, Advances, Systems and Applications 7 (2018) DOI: https://doi.org/10.1186/s13677-018-0113-8

[8] Bosung Lee, Beomsoo Kim, “Protection of Personal Information on Cloud Service Models,” Journal of the Korea Institute of Information Security & Cryptology 5(2015) 1245-1255 DOI : 10.13089/JKIISC.2015.25.5.1245

[9] Choi Jin Tak, “A Study on The Efficient Authentication Management Technique of SSO Foundation,” Journal of the Korean Society for Industrial and Applied Mathematics 1 (2006) 61-69

[10] Hyun-Jin Kim, Im-Yeong Lee, “A Study on Secure and Improved Single Sign-On Authentication System against Replay Attack,” Journal of the Korea Institute of Information Security & Cryptology 5 (2014) DOI : 10.13089/JKIISC.2014.24.5.769

[11] 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 4 (2016) 31-38 DOI : 10.9708/jksci.2016.21.4.031

[12] Hyun-mi Jung, Jae-In Sin, Gang-Soo Lee, “SSO Security Requirements Analysis in Cloud Computing,” Journal of Korea Multimedia Society 1 (2010) 433-437

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.