클라우드 컴퓨팅 환경에서 보안이 강화된 인증 및 권한관리 설계

정현미*, 이강수*

요약

기존의 웹 서비스 환경과 달리 클라우드 컴퓨팅 서비스와 같이 IT 인프라를 제공하는 서비스 환경에서는 사용자 식별 및 인증 단계가 가장 중요하다. 이러한 클라우드 컴퓨팅 서비스의 특성상 사용자 인증 기술은 사용자 권한관리를 위한 기술로 이어져야 한다. 본 논문에서는 사용자의 편의성 및 보안성이 증가하고 서비스 제공자는 추가 서비스 개발비용이 감소하는 SSO(Single Sign On) 기술과 PKI(Public-Key Infrastructure)를 결합하여 사용자 정보에 관해 강화된 관리기술과 개인정보를 보호할 수 있는 Multi-Factor 인증 방식을 설계 하였다.

Design of Enhanced Secure Authentication and Authority Management in Cloud Computing Environment

Hyun-Mi Jung*, Gang-Soo Lee*

ABSTRACT

In the existing web service environment, the service that is provided after verifying identities at the step of user identification and authentication was in the majority, but the authorization step is most important in the service environment that provides IT infrastructures like cloud computing services. Due to the characteristics of the cloud computing service, the user authentication has to be led to the authentication technology for the user authority management. In this paper, we designed a suitable authorization method that can guarantee sufficient controls and personal information protection about the user information by designing to combine SSO(Single Sign On) and PKI(public-key infrastructure).

Key Words : Cloud Computing, Security system, PKI, SSO, Multi-Factor authentication

* 한남대학교 컴퓨터공학과(✉mihj@se.hannam.ac.kr)
· 제1저자(First Author) : 정현미 · 교신저자(Correspondent Author) : 이강수
· 접수일(2011년 10월 5일), 수정일(1차 : 2011년 11월 4일), 게재확정일(2011년 11월 7일)

Ⅰ. Introduction

The cloud computing service can use without the specialized knowledge about an infrastructure and the IT technology in which a user is particular easily and a service is comprised of the mutually heterogeneous environments and the external IT resource keeps data, the specialized security factor for the cloud computing after is needed[1, 2]. In addition, when using service, because the personal information and transaction service of saved in a database the individual are exposed to an attacker and an identifier and authentication method are exposed to group data related to a transaction, in case an identity and safety were infringed for the arbitrary attack the serious damage is followed. Therefore, at the same time, the application of the suitable authenticating method fitted for the cloud computing each object considering a complexity and diversity is essential with the advantage of the simplicity and dispersibility.

In this paper, we analyzed system requirements and functions for authority management in order to provide a personal authentication method which guaranteed control and protection of the personal information, and also we designed the two-factor authentication system which combined SSO authentication and PKI encryption.

In section 2, related works about existing authentication systems are presented and analyzed. In section 3, authentication system requirements in the cloud computing environment are analyzed, and we proposed the two factor authentication system with comparative analysis in section 4. Finally, conclusion is presented in section 5.

Ⅱ. Related Works

2.1 Authentication methods for user authority management in the cloud computing service

Hardware and software in the cloud computing environment are shared through the internet, and for this reason if security problems were occurred, the private information of personal or company would be possibly disclosed to outside. Therefore, we need encryption, key, authority management technology for secure communication in the cloud computing environment. Due to the characteristics of the cloud computing service, the user authentication has to be led to the authentication technology for the user authority management. The process to authorize the user passes through the following three phases.

① User identification phase confirms the uniqueness among users who receive services of the system through the user unique identifier.

② User authentication phase proves the valid user who can be possible to receive services after identifying the user.

③ User authorization phase decides authorizing permissions for resources of the application server that can be accessed by the valid user.

In this paper, we designed a suitable authorization method that can guarantee sufficient controls and personal information protection about the user information by designing to combine SSO based on SAML and public-key infrastructure.

2.2 Authentication method based on public key infrastructure

Public-key authentication mode using public-key encryption is a method that plain-text is encrypted by private-key and cipher-text is decrypted by public-key. This method does not guarantee confidentiality of the massage because they can decrypt the massage if anyone knew public-key, but the sender can identify the receiver. After being issued user own certificate and private key at the CA, the user is certified as the valid user by sending e-signature value[3, 4, 5]. Authentication method using public-key encryption is as in the followings with table 1.

① User A generates hash value H(r) using hash function via random value r.

② User A generates Keb(r, A) which encrypted public-key Keb with r and own identity A.

③ User A requests authentication by sending Keb(r, A) to user B.

④ User B generates random value r1 using hash fuction via H(r).

⑤ User B certifies user A through comparing with r1, which generates by hash function, and r2, which is decrypted.

표 1. 공개키 암호화 생성방식
Table 1. Public-key encryption method

User 1		User 2
① $r \rightarrow H(r)$ ② $Keb(r, A)$	③ $H(r), Keb(r, A)$	④ $H(r) \rightarrow r1$ ⑤ $Kdb(Keb(r,a)) \rightarrow r2, A$ ⑥ $\mathrm{if}(r1 = r2) then\ Authentication$

2.3 Comparison of existing SSO authentication systems based on PKI for authority anagement

2.3.1 Kerberos

Kerberos structure based on PKI tries to convert from the current symmetric-key infrastructure to the public-key infrastructure. This system minimizes key management costs, that are huge burden in the symmetric-key infrastructure, and applies strong security service which is provided by the public-key infrastructure. Especially, the measure which can be initially authenticate using PKINT (Public-Key Cryptography for Initial Authentication) certificate at KDC(Key Distribution Center) is suggested, and the burden of user authentication is decentralized by PKDA which suggests the immediate authentication protocol between client and server without reference to KDC[6].

However, Kerberos structure based on PKI could not remove the unnecessary procedures for maintaining compatibility with existing protocols, and the limitation of symmetric-key infrastructure, for example sharing symmetric-keys, could not be overcome. Also, the extendable structure for SSO of the convergence system like cloud computing services did not be considered.

2.3.2 SESAME

SESAME(A Secure European System for Applications in a Multi-vender Environment) provides the integrated access control function based on the roll in the huge distributed heterogeneous environment through the Authorization server while maintaining the existing structure. Also, the initial

authentication was strengthened to apply the public-key infrastructure and the key management burden of the application system server was reduced.

However, despite applying the public-key infrastructure, SESAME could not overcome the limitation of symmetric-key infrastructure and became the complex structure through adding access control functions, and besides the extendable structure for SSO of the convergence system was not considered[7, 8].

2.3.3 RSAKeon

RSAKeon can be possible user authentication and integrated access control in the central through PAC structure that stores user authority information at the extended field of PKC. This system did not have unnecessary symmetric-key infrastructure, and the structure is simpler than SESAME. However, RSAKeon did not consider the extendable structure and additional costs that pair public-keys are generated each time issuing PAC are existed[6].

2.3.4 Netscape SuitSpot

SuitSpot suggested a simple structure that could authenticate between client and application server without authentication server. However, integrated access control was not considered and the extendable structure for SSO of the convergence system was not considered[8].

III. Authentication and system requirements for integrated authority management in the cloud computing

3.1 The limitation of existing authentication methods

Cloud computing, that has outsourcing types with storing the major data of external IT resources and constructing the cloud computing environment, is composed of the service which consists of many different types, and thus, depending on this characteristics, specialized authority management elements for only cloud computing should be required. Also, the various properties of the user, such as authorities, duties, status, are needed more than user's the identity information in this application environment.

In the existing web service environment, the service that is provided after verifying identities at the step of user identification and authentication was in the majority, but the authorization step is most important in the service environment that provides IT infrastructures like cloud computing services. If authorization were not properly, the technologies for payment policies in accordance with usage capacity, providing user authentication interface and reliable platforms about data access could not be secured and the service could not be trusted.

In this paper, we proposed an authentication method which can provide cloud services securely by designing SSO authentication method based on public-key infrastructure using the property information such as authorities, statuses, rolls.

3.2 System requirements and features for authority management

When designing user authentication for

constructing the authority management system, the following table 2 should be considered.

표 2. 시스템 요구사항 및 기능
Table 2. System requirements and features

Code	Requirements	Features
S1	Identity management	Providing the structured environment which can manage various user requirements suitably
S2	Authentication management	Providing a standard technology for secure user authentication
S3	Authorization management	Increasing security through designing efficiently access authority control model for resources
S4	Policy based management	Providing management function by policy definition: authentication methods, ID rules, password restrictions
S5	Personalization	Providing the user personalization and flexibility Providing various functions such as self-modifying for the user authority
S6	Integrated Authentication	Providing integrated authentication about various application when accessing services
S7	Central management system / audit and report functions	Functions based on log data: security audits, statistic reporting work, audit data back-up and deletion
S8	Directory / DB /enterprise application integration	New integrate construction of the storage or using existing user authority storage system
S9	Stability and scalability	Ensuring stability and scalability of system

IV. Proposed the authentication system

In the cloud computing service environment, the proposed authentication system provides a personal authentication method which guarantees control and protection of personal information, and also integrated user authentication and authority management system based on the effective SSO environment would be built. The suitable integrated two factor authentication, which is a combination of SSO and PKI, in the cloud environment, was implemented.

4.1 Service user authentication step-by-step scenario

In this section, we compose the whole module for development of the authentication system and construct the entire system through designing development tools for each module.

The proposed authentication structure is composed of user authentication, authentication information verification, user access verification and validation, certificate issue, certificate validation and authentication.

Figure 1 shows whole modules of the authentication system. The followings are explanations about the development environment.

- SSO Engine
  The result which checked authority about the user's business through policy server is retransmitted to the business service.

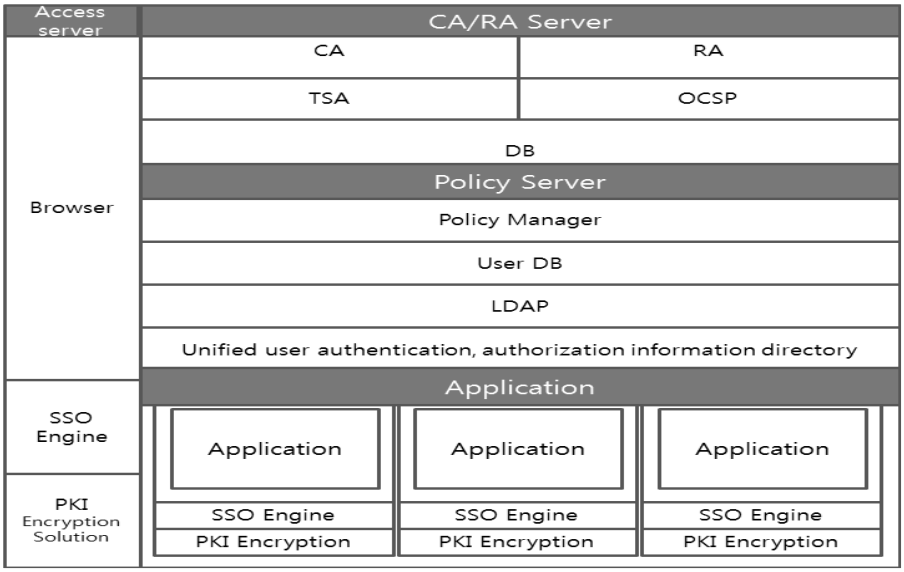

그림 1. 시스템 구성도
Fig. 1. Composition of the authentication system

- PKI Encryption
  SSL encryption session between web browser and web server is applied for web server security, and CS establishes SSL encryption session between client and server. Encryption by server's public-key is only supported, and there is no client certificate issue function.

- LDAP (Lightweight Directory Access Protocol)
  Application protocol that can look-up and modify directory service on TCP/IP[9]

- Access Server
  This is a system that can provide a web-based interface to the end user through integrating enterprise information resources, regardless of the type and the number of applications and systems.

- CA (Certification Authority)
  CA verifies more powerfully identification of the user on network through issuing digital certificates to the user and provides firm reliability, such as data integrity verification and non-repudiation, in the digital environment through realizing electronic signature based on the certificate.

- RA (Registration Authority)
  RA can act as a proxy for the user's background check and registration when issuing the digital certificate to the user.

- OCSP (Online Certificate Status Protocol)
  OCSP is a system that can check whether the certificate is discarded or not using OCSP server through the internet. PKI manager can operate

OCSP for the validity verification of the user certificate when providing the authentication service[10].

- TSA (Time Stamping Authority)
  TSA is a system for improving reliability of PKI using time information. Digital time stamp that can check the existence of documentation and data at certain time besides reliable time information is provided. This system is compliant with standardized time stamp and support CMS functions.

4.2 Authentication process

In this section, we design the flow of entire authentication and the result is shown. Figure 2 shows the design of the whole flow and user authentication process.

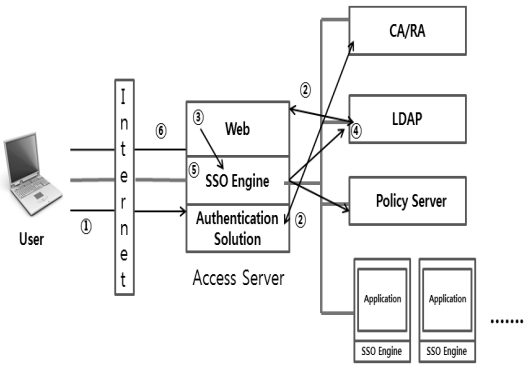

그림 2. 인증흐름 설계도
Fig. 2. The user authentication process flow

- The first user log-in process

① External user transmits minimum log-in information through access server.
② CA and RA verify the validity of user authentication using authentication solution.
③ User authentication information is transmitted to SSO Engine.
④ LDAP verifies the user information and service usage authority information.
⑤ After receiving authority, SSO engine generates the user certificate.
⑥ The certificate which generated at SSO engine is transmitted to the user.
⑦ The user who received the certificate stores the certification on memory.
⑧

- The user authority process using the certificate

① When the first log-in, the user submits a stored certificate.
② SSO Engine verifies the submitted certificate by user.
③ After verifying the certificate, SSO Engine requests to check the user information and the service usage authority information to LDAP.
④ SSO Engine transmits the authority information to the application after confirming the request.
⑤ The use of the service is permitted.

4.3 Analysis of the proposed system

Table 3 shows comparison of the proposed system and existing PKI-based SSO systems by requirements in section 3.

Proposed system satisfies requirements that needed to implement user authentication authority configuration system, and this system has the following advantages.

표 3. 제안된 시스템 및 기존 PKI 기반의 SSO 시스템 비교
Table 3. Comparison of the proposed system and existing PKI-based SSO systems

Code	Requirements	Kerberos	SEASAME	RSAKeon	SuitSpot	Proposed System
S1	Identity management	O	O	O	O	O
S2	Authentication management	O	O	O	O	O
S3	Authorization management		O	O	O	O
S4	Policy based management			O	O	O
S5	Personalization			O		O
S6	Integrated Authentication			O		O
S7	Central management system / audit and report functions			O	O	O
S8	Directory / DB / enterprise application integration			O	O	O
S9	Stability and scalability				O	O

- Integrated authority management available

  Integrated management of user authentication and authority policy and also integrated back-up system construction are easy, and integrated user monitoring can be constructed. Hence, authority management and operation costs are decreased and the business efficiency is increased.

- Efficient SSO implementation

  The service usage management of the user is unified. Therefore, convenience and security of the user are increased and additional service development costs of service providers are decreased.

- Strong countermeasure establishment about security

  Secure user authentication and data management and usage is easy owing to constructing PKI-based encryption system, and the thorough identification and authorization are possible due to the multi factor authentication method. By encrypting user information, integrated storage management is secured, and the user is protected from various security threats.

- Integrated security infrastructure preparation

  The certificate-based consistent user authentication policy and the consistent authority policy establishment about resource

access are possible, and additional functions, such as the user management, authentication, authorization for each services, do not need to implement separately. Also, it is easy to integrate with the existing user authentication database.

V. Conclusion

The most important advantage of cloud computing is that the user can use the service without specific knowledge about the IT infrastructure. However, this characteristic is not lead to obtain reliability of the user. In terms of security, the size and economic feasibility of cloud computing has both advantages and disadvantages. The presence of large amounts of resources and data is a big temptation to both the user and the attacker. In the situation that the user authentication and the service use are getting simpler, service providers should design a more secure and reliable service and authentication management technology using various IT technologies than the existing computing environment.

Therefore, a proposed authentication authority configuration method, in this paper, uses PKI-based SSO authentication technology for strengthening security about the user information. Reduce costs and increase in business efficiency would be expected because, in terms of the user, flexible access control is provided without authentication procedures for each service by just one authentication, and authority configuration of the authentication policy applied easily in terms of the manager. In the future, we will design detailed mechanism and protocol for proposed system and will develop as more efficient and practical technology.

참고문헌

[1] Wikipedia, http://en.wikipedia.org/wiki/Cloud_computing

[2] Vision, Hype, and Reality for Delivering IT Services as Computing Utilities, *HPCC 2008 Keynote*, 2008

[3] Wikipedia, http://en.wikipedia.org/wiki/Public_key_infrastructure

[4] Windows 2000 Public Key Interoperability, White Paper, Microsoft.

[5] Man-young Lee, Dong-ho Won, Min-sub Lee, et al., *Modern Cryptography and Application*, Sang-neung, 2002

[6] DongHee Kim, JinTak Choi, "A Study on The Efficient Authentication Management Technique of SSO Foundation", *Korean Institute of Information Technology*, 4, 2006

[7] Windows 2000 Kerberos Interoperability, White Paper, Microsoft.

[8] Seung-ho Yeon, Hyun-Gyu Park, Hee-Soo Oh, at al., "Design of KT's Single Sign-On on Public Key Infrastructure", *Korean Institute of Information Scientist and Engineers*, 8, 2002

[9] Wikipedia, http://ko.wikipedia.org/wiki/LDAP

[10] Wikipedia, http://en.wikipedia.org/ wiki/ Online_ Certificate_ Status_ Protocol

[11] Hyun Mi Jung,"An Efficient User Authentication Method for Cloud Computing Environments", *Master's Thesis of Hannam University*,2010

Acknowledgement

This paper has been supported by 2011 Hannam University Research Fund.

저자소개

정현미(Hyun-Mi Jung)

1998 : B. Eng. in Dept. of Computer Engineering, Hannam University
2010 : M. Eng. in Dept. of Computer Engineering, Hannam University

2010 ~ Current : Course for Ph. D. in Dept. of Computer Engineering, Hannam University

※ Research Interests : Software Engineering, Security Engineering, Information Security Consulting and Risk Analysis, IT Security System Evaluation

이강수(Kang-Soo Lee)

1981 : B. S. in Dept. of Computer Science, Hongik University
1983 : M. S. in Dept. of Computer Science, Seoul National University
1989 : Ph. D. in dept. of Computer Science, Seoul National University
1985～1987 : Leturer in Dept. of Electronic Computation, Hanbat National University
1992～1993 : Visiting Scholar, Illinois Univ. USA
1995 : Visiting Researcher, ETRI
1998 ~ 1999 : Dean of Dept. of Multimedia, Hannam University
1987 ~ Current : Professor at Dept. of Computer Engineering, Hannam University

※ Research Interest : Software Engineering, Parallel System Modeling and Analysis, Security Engineering, IT Security System Evaluation, Curriculum for Multimedia Education