클라우드 컴퓨팅 환경을 위한 상황인식 기반 통합 인증 및 접근제어 시스템

이현동, 정영민, 정목동
부경대학교 컴퓨터공학과
e-mail:win4class@hanmail.net, jym1376@nate.com, mdchung@pknu.ac.kr

Context-Aware Single Sign-On and Access Control System in Cloud Computing Environment

HyunDong Lee, YoungMin Jung, MokDong Chung
Dept of Computer Engineering, Pukyong National University

요 약

클라우드 컴퓨팅 서비스 환경에서 인증 및 접근 제어와 같은 여러 보안 이슈가 발생하고 있다. 특히, 클라우드 컴퓨팅 환경에서 다양한 자원에 접속을 할 경우, 통합적으로 관리 및 제어가 가능한 인증 및 접근제어 모델이 필요하다. 이를 해결하기 위해서, 본 논문에서는 상황인식 기반의 통합 인증(SSO) 및 접근제어 모델을 제안하고, 이를 설계 및 구현함으로써, 클라우드 컴퓨팅 환경에서 유연하고, 편리한 보안 시스템을 검증하고자 한다.

1. 서론

클라우드 컴퓨팅은 최근에 아마존, 마이크로소프트, 구글, IBM 등 IT 관련 글로벌 기업들이 참여하면서 이슈화되기 시작하였다. 클라우드 컴퓨팅 환경에서는 애플리케이션을 개발하거나 서비스할 때 서버나 스토리지 등 컴퓨팅 자원 등을 자체적으로 보유하지 않고, 이 같은 자원을 갖고 있는 클라우드 컴퓨팅 플랫폼을 제공하는 회사의 자원을 이용해서 개발하고 서비스하는 것을 의미한다.

클라우드 컴퓨팅 서비스 환경에서는 가상화 기술 보안, 대용량 분산 처리 기술, 서비스 가용성, 대용량 트래픽 핸들링, 애플리케이션 보안, 접근 제어, 인증 및 암호와 같은 여러 보안 이슈가 발생하고 있다.

특히, 클라우드 컴퓨팅 환경에서 다양한 자원에 접속을 할 경우, 통합적으로 관리 및 제어가 가능한 인증 및 접근제어 모델이 필요하다.

이에 본 논문은 상황인식 기반의 통합 인증(SSO) 및 접근제어 시스템을 제안하고, 이를 설계 및 구현함으로써, 클라우드 컴퓨팅 환경에서 유연하고, 편리한 보안 시스템을 검증하고자 한다.

본 논문의 구성은 다음과 같다. 2절 관련 연구에서는 상황인식 기반 통합인증 및 접근제어 시스템에 사용되는 기본 기술들을 살펴보고, 3절에서는 상황인식 기반 통합 인증 및 접근제어 시스템의 구조 및 각 컴포넌트 별 기능을 살펴본다. 그리고 4절에서는 상황인식 기반 통합 인증 및 접근제어 시스템의 구현 시나리오와 설계 및 구현 결과를 제시한다. 마지막으로 5절에서는 결론 및 향후 연구 방향을 제시한다.

2. 관련 연구

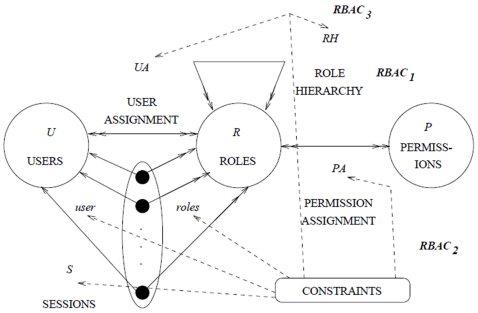
2.1 클라우드 컴퓨팅 환경에서 보안

클라우드 컴퓨팅 환경에서의 서비스는 대부분 웹 기반으로 제공되므로, 사용자의 신원을 확인하기 위한 인증이 반드시 필요하다. 현재 가장 활성화되어 있는 단순한 ID/Password 기반의 인증 방식의 경우, 사용자들은 사용하는 서비스의 수만큼 ID/Password를 생성 및 관리해야 함으로써 사용자들에게 많은 불편을 야기시키고 있다. 뿐만 아니라, ID및 패스워드의 분실 및 도용으로 인해서 보안 취약성이 존재한다. 이를 해결하기 위해서 다양한 Multi Fact기반의 인증 방식의 적용이 필요하며, 가상화 자원에 대한 접근 제어 기술도 필요하다[1].

2.2 접근 제어 기술(RBAC, GRBAC)

RBAC(Role-based Access Control)는 사용자의 조직상에서의 역할을 기반으로 접근권한을 특정 사용자가 아닌 해당 역할을 가진 사용자 그룹에게 부여하는 방식으로 조직의 구조와 연동하여 직책에 따라 보안 등급을 부여하며, 개별 사용자가 특정 직책을 부여 받으면 그에 상응하는 권한을 획득한다.

RBAC 기본 모델은 컴퓨터 시스템을 통하여 시스템 내의 정보를 사용하는 객체로서의 사용자(U: User)와 시스템의 하나 또는 그 이상의 객체에 대한 특정 접근 모드(예: read, write, update)의 승인을 나타내는 역할(R: Role) 그리고 사용자 배정(UA: User Assignment)과 인가 권한(P: Permission), 세션(S: Session)으로 구성되어진다[2]. 다음 그림1은 역할기반 접근 제어 모델을 나타낸다.



(그림 1) 역할기반 접근제어 모델

GRBAC(Generalized Role-Based Access Control)는 상황에 근거한 접근제어를 수행하기 위하여, 접근 제어 결정에 사용자 역할(subject role), 객체 역할(object role), 환경 역할을 추가하여 기존의 RBAC 모델을 확장하였다[3].

2.3 OSGi 서비스 플랫폼

OSGi(Open Service Gateway Initiatives)는 자바 기반으로 운영체제나 플랫폼에 독립적으로 운영되는 미들웨어 프레임워크로서, 네트워크 환경에서 서비스의 전달, 배치, 관리를 위한 표준 명세를 정의하는 기관인 OSGi 얼라이언스에서 개발한 개방형 표준이다[4].

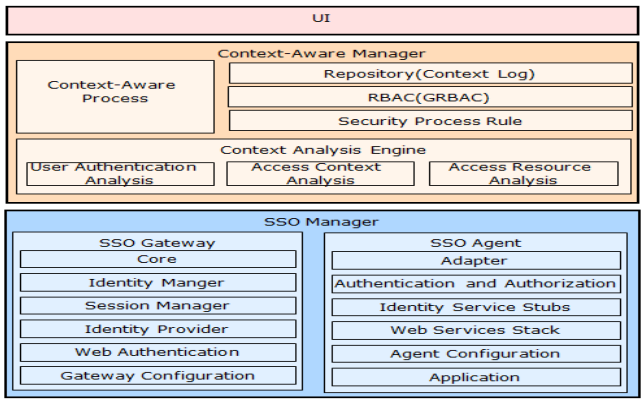
기본적으로 OSGi 구조는 OSGi 컨테이너 구현체 위에서 컴포넌트(번들)들이 런타임 환경에서 동적으로 플러그인 되고 서비스 레지스트리를 통해 다른 번들에게 서비스를 제공하는 구조를 가지고 있다[5].

OSGi 서비스 플랫폼의 장점은 다음과 같다.

①자바 가상 머신(JVM) 기반의 플랫폼 독립적
②동적 서비스 변경과 같은 서비스 관리 기능 제공
③다양한 레벨의 시스템 보안 제공
④단일 게이트웨이 플랫폼에서 서로 다른 공급자로 부터 제공된 여러 서비스 호스팅 기능을 사용 가능

3. 상황인식 기반 통합인증 및 접근제어 시스템

클라우드 컴퓨팅 환경을 위한 상황인식 기반 통합 인증 시스템은 OSGi 서비스 플랫폼 기반으로 SSO Manager, Context-Aware Manager, UI Manager 계층으로 구성한다. 다음 그림 2는 전체 시스템 구성도를 나타낸다.



(그림 2) 통합인증 및 접근제어 시스템 구성도

3.1 SSO Manager

클라우드 컴퓨팅 환경에서 단일 인증(SSO)을 수행하며, SSO Agent와 SSO Gateway로 구성한다.

■ SSO Agent: 사용자 프로그램이 실행되는 클라이언트 PC에 설치하며, 로그인시 사용자 인증 정보를 수집한다.

■ SSO Gateway: 인증 서버에 탑재된 인증 모듈로, SSO Agent로부터 사용자 인증 정보를 전달 받아서 사용자 인증을 처리한다.

3.2 Context-Aware Manager

사용자 인증 정보를 상황에 따라 다양한 분석을 통하여, 인증 절차를 정의하는 기능을 수행한다.

■ Context-Aware Process: 각종 상황정보의 분석 결과를 취합하고, 분석된 결과에 따라 보안 처리 절차를 Security Manager로 전달한다.

■ Repository: 사용자 인증 시 획득된 상황정보의 로그를 저장하는 저장소 역할을 하며, 자원에 대한 사용자 선호도를 선정하는데 유용한 자료로 활용한다..

■ RBAC(GRBAC): 사용자 권한 별로 자원의 접근 제어 가능 여부를 정의한다.

■ Security Process Rule: 인증 및 접근제어 처리 절차를 정의한다.

■ Context Analysis Engine: 신원적 상황, 물리적 상황, 역사적 상황, 정서적 상황, 자원적 상황을 분석한다. 그리고, OSGi 플랫폼으로 구성되어 있어, 각각의 상황 분석 모듈을 자유롭게 추가, 수정, 삭제가 실시간으로 가능하다.

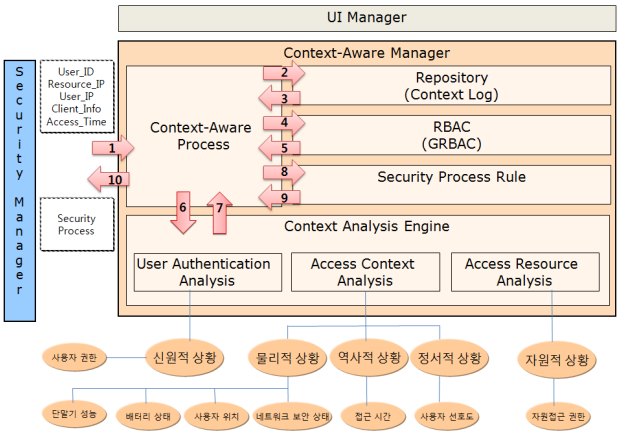
3.3 UI Manager

UI Manager는 사용자 인증 웹페이지를 제공하는 기능을 수행하며, 기본적으로는 ID Federation기반의 인증 UI를 제공하며, 추가적으로 OTP 인증 UI 및 클라우드 컴퓨팅 자원의 접근 거부 페이지를 제공한다.

3.4 내부 데이터 흐름

상황인식 기반 통합 인증 및 접근제어 시스템의 내부 데이터 흐름을 살펴보면, SSO Manager에서 사용자 로그인 시 획득한 정보인 사용자 ID, 사용자가 로그인하는 클라이언트 PC의 IP 와 자원정보, 접근하려는 자원의 IP 정보와 접근 시간 정보를 Context-Aware Manager로 전달한다. Context-Aware Manager에서는 획득한 다양한 상황정보를 바탕으로 ID Federation기반의 기본 인증이나, 추가 인증(ID Federation기반 + OTP) 또는 접근 차단의 적용 여부를 분석한 후, SSO Manager로 전달한다.

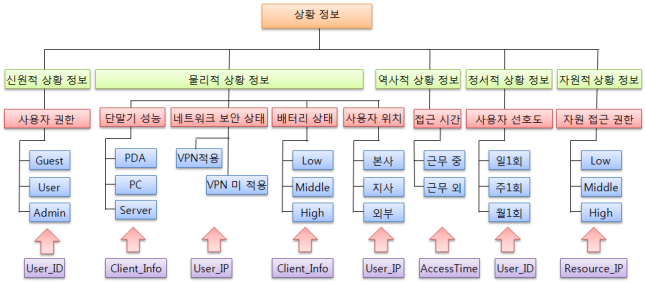
그림3은 상황인식 기반 통합 인증 및 접근제어 시스템의 상황정보 처리를 위한 내부 데이터 흐름을 나타낸다.



(그림 3) 내부 데이터 흐름도

3.5 상황정보 분류

상황인식 기반 통합인증 및 접근 제어 시스템의 상황정보는 신원적 상황, 물리적 상황, 역사적 상황, 정서적 상황, 자원적 상황으로 분류한다. 그림 4는 상황정보 분류를 나타낸다.



(그림 4) 상황 정보 분류

3.5 통합인증 및 접근제어 처리 절차 및 알고리즘

다음 표 1은 상황인식 기반 통합인증 및 접근제어 시스템의 통합인증 및 접근 제어 처리 절차를 나타낸다.

<표 1> 통합 인증 및 접근제어 처리 절차

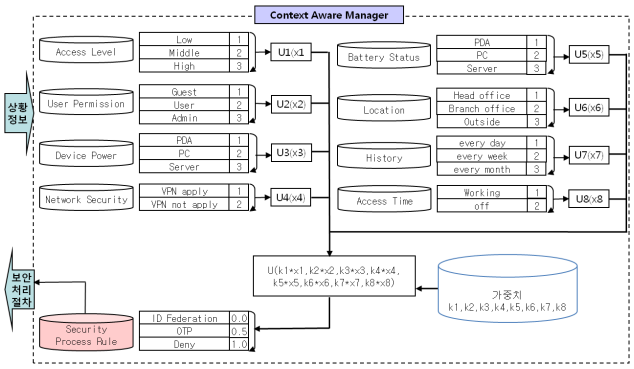
Notations	
ID*u*	사용자 ID
PW*u*	사용자 패스워드
RESIP*u*	접근하려는 자원의 IP
UserIP*u*	사용자 IP
ClientInfo*u*	사용자 사용 단말기의 상태 정보
Time*u*	접근 시간
SP*u*	보안 처리 절차 (ID, OTP, Deny)
Detailed Protocol	
(1) UI→ SSO Manager: IDu//PWu//ContextInfo(RESIP*u*,UserIP*u*,ClientInfo*u*,Time*u*)	
(2) SSO Manager: Check[IDu//PWu]	
(3) SSO Manager→ Context-Aware Manager: IDu//ResultofCheck[IDu//PWu]//ContextInfo(RESIP*u*,UserIP*u*,ClientInfo*u*,Time*u*)	
(4) Context-Aware Manager: Analysis[IDu//ContextInfo(RESIP*u*,UserIP*u*,ClientInfo*u*,Time*u*)]	
(5) Context-Aware Manager → SSO Manager: SP*u*	
(6) SSO Manager → UI: SP*u*	
(7) UI: UI[SP*u*]	

MAUT(Multi-Attribute Utility Theory)는 다중변수에 대한 의사결정 문제(decision problem)에서 유틸리티(utility)를 통한 정략적인 의사결정방법이다.

유틸리티는 0과 1사이의 상대적인 값으로써 u(x0), u(x*)를 각각 가장 낮은 인증 절차 유틸리티와 가장 높은 인증 절차 유틸리티라고 두면 u(x0)=0,u(x*)=1로 나타낸다[6]. 예를 들면, 자원 접근 권한, 사용자 권한, 네트워크 상황 등의 속성(Attribute)으로 평가될 때 인증 절차 결정을 위한 전체 유틸리티 함수는 <식1>과 같이 정의한다.

$$u(x_1, x_2, \ldots, x_n) = \sum_{i=0}^{n} k_i u_i(x_i), \quad \sum_{i=0}^{n} k_i = 1 \qquad \text{<식1>}$$

그림 5는 MAUT를 통한 보안 처리 절차를 결정하는 과정을 도식화 한 것으로, 상황인식 기반 인증 및 접근제어 기술의 전체적인 알고리즘을 나타낸다.

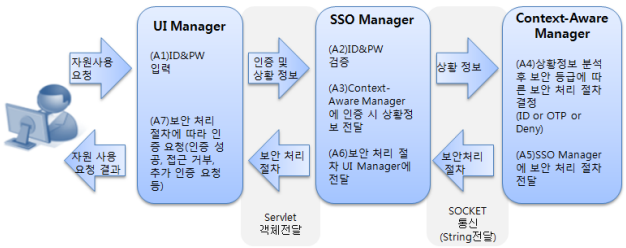


(그림 5) 상황 정보 분류

4. 설계 및 구현

4.1 구현 시나리오

클라우드 컴퓨팅 환경을 위한 상황인식 기반 통합인증 및 접근제어 시스템의 구현 시나리오는 그림 6과 같다.



(그림 6) 구현 시나리오

4.2 설계 및 구현

관리자(Admin)는 초기화 단계에서 사용 보안 처리 절차(ID Federation 및 추가 인증 또는 접근거부) 및 상황 정보를 처리하기 위한 상황 정보의 가중치(weight)를 정의한다.

SSO Gateway는 SSO Agent로 부터 사용자 인증 시 획득한 상황정보를 Context-Aware Manger의 Context-Aware Process에 전달하고, Context Analysis Engine는 신원적 상황정보, 물리적 상황정보, 역사적 상황정보, 정서적 상황

정보, 자원적 상황정보를 분석한다.

상황정보 분석 완료 후, 사전에 정의되어 있는 보안 처리 절차에 따라 인증 성공 또는 추가 인증 요청 또는 접근 거부를 클라우드 컴퓨팅 자원 사용자에게 전달한다.

Context-Aware Manager의 구성 정보는 별도의 XML 파일로 작성하여, 각 상황정보 요소별 가중치 수정을 원활하게 하였으며, RBAC기반의 DB를 제어하기 위해서 iBatis 프레임워크를 활용하였다. 이를 통하여, DB에 접근할 때 필요한 자바 코드를 현저하게 줄일 수 있고, XML를 사용하여 간단하게 SQL Statement에 매핑 시킴으로써, SQL Query 튜닝을 쉽게 할 수 있다.

Context-Aware Manager의 실행결과를 살펴보면 다음과 같다.

• User's ID:"user1" [UserPermissions: user. History: every day] • Resource's IP:"203.250.123,180" [AccessLevel: Low] • Client IP:"202.250.123,100" [Network:VPN_O, Location: Headoffice] • Client Info: "PC", "High" [Device: PC, Battery Status: High] • Access Time:"09:00:00" [AccessTime: working] ※ Analysis results: 0.0 [Security Process: IDFederation]
• User's ID:"user2" [UserPermissions: admin, History: every day] • Resource's IP:"203.250.123,190" [AccessLevel: High] • Client IP:"202.30.34.2" [Network:VPN_X, Location: Outside] • Client Info: "PC", "High" [Device: PC, Battery Status: High] • Access Time:"09:00:00" [AccessTime: working] ※ Analysis results: 0.75 [Security Process: OTP]
• User's ID:"user2" [UserPermissions: admin, History: every day] • Resource's IP:"203.250.123,190" [AccessLevel: High] • Client IP:"202.30.34.2"[Network:VPN_X, Location: Outside] • Client Info: "PC", "High" [Device: PC, Battery Status: High] • Access Time:"07:00:00" [AccessTime: off] ※ Analysis results: 1.00 [Security Process: Deny]

소프트웨어 품질의 특성 및 척도에 대한 표준화인 ISO9126 Quality Model[7]의 6가지 품질 속성을 기반으로 본 논문에서 제안하는 상황인식 기반 통합 인증 시스템은 기존의 단일 인증 시스템을 비교하면, 표2와 같다.

<표 2> 기존 단일 인증 시스템과 비교

특징	기존 단일 인증 시스템	제안하는 상황인식 기반 통합인증 시스템
기능성	단일 인증	Multi Fact기반의 다중 인증
신뢰성	패치 및 결함 수정 시 시스템 중단	OSGi 플랫폼 도입으로 무중단 인증 시스템 제공
사용성	고정적인 인증 서비스 제공	다양하고 유연한 인증 서비스 제공
효율성	다양한 상황이 발생하더라도 동일한 인증 제공	자원 및 사용자 등급에 따른 인증 절차의 다양화로 인증 시 발생하는 비용 최소화
유지 보수성	패치 및 결함 수정 시 시스템 중단	OSGi 플랫폼 도입으로 무중단 인증 시스템
이식성	단일 플랫폼에서 동작	OSGi 플랫폼 기반으로 임베디드 시스템 등 다양한 플랫폼에서 동작 가능

5. 결론 및 향후 연구

클라우드 컴퓨팅 환경에서 자원의 접근 권한 및 사용자 인증은 단일 시스템에 비해서 유연하고, 자동화된 통합 인증이 필요하다. 이에 클라우드 컴퓨팅 환경에서 상황인식 기술(MAUT, 상황정보 분류)과 접근 제어 기술(RABC, GRBAC), 통합 인증 기술(ID Federation, OTP, PKI, SPKI 등), 런타임 환경에서 동적으로 플러그인 되는 OSGi 서비스 플랫폼 기술을 접목하여, 유연하고 자동화된 통합 인증 및 접근제어 시스템을 설계 및 구현하였다.

본 논문에서 제안한 클라우드 컴퓨팅 환경에서 상황인식 기반 통합인증 및 접근제어 시스템의 장점은 다음과 같다.

①다양한 Multi Fact기반의 통합 인증 절차를 지원(ID Federation + OTP + PKI, + SPKI 또는 접근 거부)함으로써 클라우드 컴퓨팅 환경에서의 강력한 통합 인증 및 접근제어 서비스를 제공한다.

②무중단 시스템을 적용하여, 운영 중이라도 Role정의 및 인증 모듈을 자유롭게 추가 삭제 가능(OSGi플랫폼)하다.

③상황 인식 기술을 통하여, 사용자의 상황에 따른 다양한 인증 방법, 사용자 편의성 및 시스템 안전성을 보장한다.

향후 연구계획은 상황인식 기반의 계산 알고리즘 보완 및 RBAC기반의 다양한 접근 모델 및 정책 수립을 중점적으로 연구 개발하고자 한다.

Acknowledgments

본 논문은 중소기업청에서 지원하는 2009년도 산학연 공동기술개발사업 (No. 00038609-1)의 연구수행으로 인한 결과물임을 밝힙니다.

참고문헌

[1] 김명주, "제1회 클라우드 컴퓨팅 정보보호 기술 워크샵", pp. 141~142, 2009

[2] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman. "Role-Based Access Control Models," IEEE Computer, Vol. 29, No. 2, pp. 38 - 47. 1996

[3] M.J.Covington, et al., "Generalized Role-Based Access Control for Securing Future Applications", In Proc of 23rd National Information System Security Conference(NISSC), Baltimore, pp. 115-125, Oct 2000

[4] OSGi Alliance, "OSGiService Platform Core Specification", Release4, Version4.1, April 2007

[5] 김석구, "유니버셜 미들웨어 OSGi 최신 기술 동향", 지능형 홈네트워크 6호, 2006

[6] R.L.Keeney and H.Raiffa, Decisions with Multiple Objectives: Preferences and Value Tradeoffs, John Wiley &Sons, New York, NY, pp.261~271, 1976

[7] ISO 9126 Software Quality Characteristics, http://www.sqa.net/iso9126.html.