워크플로우 시스템 기반의 사무 환경을 위한 상황 인식 기반 접근 제어 모델*

최진영*, 김종명*, 박선호*, 정태명**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail : {jychoi, jmkim, shpark}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

The Context-Aware Access Control Model of Workflow-based System for Business Environment

Jin-Young Choi*, Jong-Myoung Kim*, Seon-Ho Park*, Tai-Myoung Chung**
*Dep. of Electrical and Computer Engineering, Sungkyunkwan University
**School of Information and Communication Engineering, Sungkyunkwan University

요 약

유비쿼터스 컴퓨팅(Ubiquitous Computing) 시대에 기업의 사무 환경은 다양한 정보들과 많은 사용자들이 유기적인 관계를 형성한다. 이러한 관계에서 접근 제어는 다양한 정보 객체에 허가된 사용자만이 접근할 수 있는 권한을 갖는 기능을 제공하는 것이고, 사무 환경에서 보안상 필수적이며 중요한 역할을 한다. 하지만 기존의 접근 제어 모델들은 상황 정보를 고려하지 않아 동적인 접근 제어를 하지 못하는 문제점을 가지고 있다. 본 논문은 워크플로우 기반의 오피스 환경에서 동적이고 능동적인 접근제어 관리를 제공하기 위한 상황 정보와 역할 기반의 워크플로우 데이터 접근제어 모델을 제안한다. 이 모델은 수많은 상황 정보 및 사무 정보와 사용자가 동적으로 변화하는 사무 환경에서 사용자에게 접근을 제어하기 적합하다.

1. 서론

최근 인터넷과 컴퓨터의 성능이 발달하면서 네트워크나 시스템에 대한 접근을 효율적으로 통제하기 위해 접근 제어 모델에 대한 연구가 활발히 이루어지고 있다[1]. 초기에는 접근 제어 목록(ACL)이나 기본적인 정책들을 기반으로 접근 제어를 수행하였으나, 방대하고 다양하게 발전하는 인터넷, 시스템 기계들의 성능 향상, 그리고 사용자 증가 등의 이유로 접근 제어 모델이 개선되어 개발되었다. 전통적으로 DAC (Discretionary Access Control), MAC (Mandatory Access Control)이 있으며, 기업 같은 특정 환경에 적합한 접근 제어를 위해 RBAC (Role-Based Access Control), ABAC (Activity-Based Access Control), TBAC (Task-Based Access Control), TRBAC (Task-Role-Based Access Control) 등이 등장하였지만, 다양한 정보들과 많은 사용자들이 유기적이며 동적인 관계를 형성하는 워크플로우를 관리하기에는 적합하지 않다[1].

유비쿼터스 컴퓨팅 환경에서는 센서를 통해 시스템이나 상황 정보를 수집하거나 분석하여 정보를 제공해주는 상황 인식 시스템이 중요한 역할을 한다. 따라서 접근 제어 모델에서도 상황 인식 정보를 반영하여 개발해야 한다. 따라서 본 논문은 상황 정보가 반영되는 세션 관리를 통하여 유비쿼터스 컴퓨팅 시대의 사무 환경에서, 상황 인식 시스템에 동적인 접근 제어를 제공하는 모델을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 워크플로우 환경에서 기존의 전통적인 접근 제어 모델에 대해서 알아보고, 3 장에서는 워크플로우 시스템 기반의 상황 인식을 통한 접근 제어 모델을 설계한다. 마지막으로 4 장에서는 기존의 접근 제어 모델과 비교를 하며 5 장에서는 결론을 맺는다.

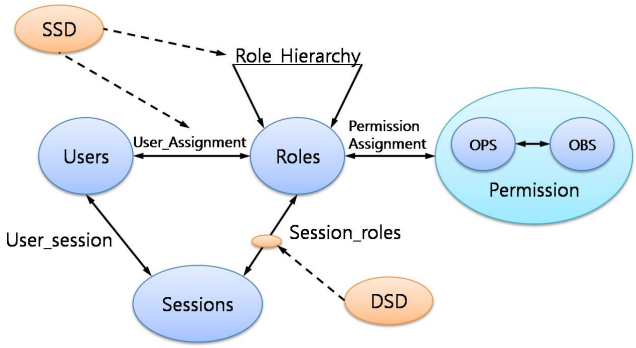
2. 관련 연구

이번 장은 워크플로우 환경을 위하여 기존에 제안되고 있는 접근 제어 모델들에 대해서 분석한다.

2.1 RBAC(Role-Based Access Control) 모델

RBAC 이란 권한을 역할과 연관시키고 사용자들이 적절한 역할을 할당 받도록 한다. 역할은 조직에서 다양한 작업 기능들을 바탕으로 정의되며 사용자들은 직무에 따른 적절한 역할을 할당 받는다[1][2].

* "본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-C1090-0801-0028)



(그림 1) RBAC

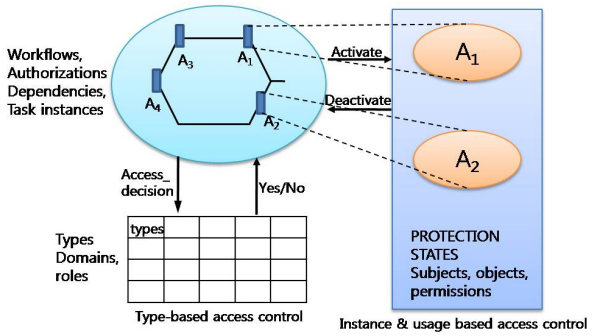
(그림 1)은 RBAC 모델이 구성을 나타내며, Users, Roles, Permission, Session 등의 개체들과 역할과 권한의 할당 관계를 표현하는 PA, 사용자의 역할 권한의 할당을 나타내는 UA 를 포함한다. RBAC 은 접근 제어 요구 사항을 지정하는 수단으로 역할 추상화를 사용한다. 허가는 정보에 특정한 동작을 수행할 수 있는 능력을 허용하는 것이다. 이러한 RBAC 이 기업의 사무 환경에 적용될 경우 조직의 관리 구조에 따라 역할 사이의 권한 상속 관계를 통하여 계층화된다.

2.2 ABAC(Activity-Based Access Control) 모델

ABAC 은 행위 기반 접근 제어를 말하는데 워크플로우에서 공동 작업 환경을 위해서 연구되었다. 즉 공통의 목적을 갖고 이 목표를 달성하기 위해 모인 활동의 집합을 Activity 라고 정의하고, 접근 권한의 부여와 접근 권한의 활성화를 분리하였다. 이를 통하여 어떤 사용자가 워크플로우 내의 직무의 접근 권한을 부여 받았더라도, 이것의 사용은 워크플로우의 진행 상태에 따라 제약을 받는 모델이다[3].

2.3 TBAC(Task-Based Authorization Control) 모델

TBAC 은 직무기반 접근 제어를 말하는데 이는 다양한 지점에서 정보 프로세싱 작업을 하는 분산 컴퓨팅 환경과 워크플로우 환경을 고려한 접근 제어 모델이다. TBAC 이 기존의 접근 제어와 다른 측면은 사용자에게 권한이 있더라도 부여받은 직무를 수행하는데 필요한 것들만 활성화를 통하여 생명 주기를 부여하고 실행되도록 한다[4]. 또한 TBAC 은 인가 처리와 직무 프로세스의 생명주기에 대한 감시와, 인스턴스와 사용기반 접근 제어뿐만 아니라, 타입기반의 접근 제어도 가능하다. 따라서 활성화를 통하여 여러 개의 하위 직무로 분류되는 기업의 사무 환경의 직무를 개별적으로 관리할 수 있는 장점을 가지고 있다.



(그림 2) TBAC

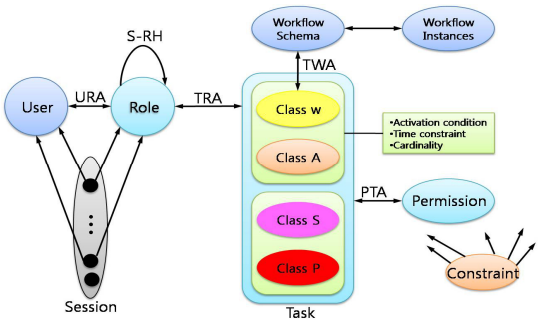
2.4 T-RBAC(Task-Role-Based Access Control) 모델

T-RBAC 은 역할 기반 접근 제어 모델을 기초로 하여 기업의 직무와 관련된 접근 제어를 통합한 모델이다[5]. T-RBAC 과 역할 기반 접근 제어의 차이점은 접근 권한을 부여하는 방법인데 역할 기반 접근 제어는 접근 권한이 직접 역할에 부여되나, T-RBAC 은 접근 권한이 그 역할이 수행하는 직무를 통해 부여된다. 특히 기업의 사무 환경에서는 정보의 공유가 중요하며, 직무를 사업 환경에서의 직위와 사업 역할을 포함하는 조직 구조와 사업 프로세스의 특성에 따라 클래스로 분류한다[5].

<표 1> Task Classification

분류	특성	설명
Class P	사적 (Private)	상속 불가, 수동적 접근 예) 분석, 계획, 결정
Class S	감독 (Supervision)	상속 가능, 수동적 접근 예) 검토, 감사, 감시, 승인, 위임
Class W	워크플로우 (Workflow)	상속 불가, 능동적 접근 예) 워크플로우 과정의 직무
Class A	행위 승인 (Approval for activity)	상속 가능, 능동적 접근 예) 워크플로우 과정의 승인 직무

T-RBAC 모델은 (그림 3)에서 보듯이 접근 권한이 직무에 할당되고, 직무에 각각 역할이 할당된다.



(그림 3) T-RBAC

2.5 사무 환경에서 기존의 접근 제어 모델의 취약점 분석

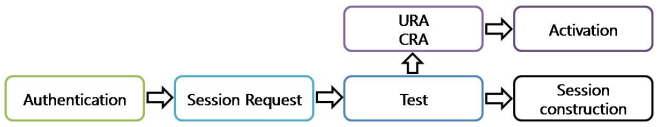
관련 연구에서 살펴본 RBAC, ABAC, TBAC, T-RBAC 은 사용자의 위치 정보, 객체의 상태, 활동(Activity)의 상태, 그 밖의 주변 환경 정보 등의 상황 정보를 고려하여 접근 제어를 하지 못하는 취약점을 가지고 있다. 이러한 접근 제어 모델들은 대부분 주체나 업무 위주의 접근 제어 정책으로 인해 상황 정보에 따라 서비스를 제공하는 상황 인식 시스템에는 부적합하다[1]. 이렇게 접근 권한에 대한 정책을 구성할 때 상황 정보를 고려해야 하는 이유는 수시로 변하는 상황 정보를 서비스 사용에 동적으로 적용하여 접근을 제어해야 하기 때문이다. 즉 상황 정보의 변화는 워크플로우에서 관리하는 세션 정보에 영향을 주며 이러한 변화에 동적으로 적합한 접근제어를 해야 한다.

3. 워크플로우 시스템 기반의 사무환경을 위한 상황 기반 접근 제어 모델(CAACM)

3.1 개요

이번 장은 상황 정보와 사용자 역할 기반으로 유비쿼터스 컴퓨팅 시대의 사무 환경에서 상황 인식 시스템에 활동(Activity) 및 동적인 접근 제어를 제공하는 세션을 생성하며, 또한 생성된 세션에 상황 정보의 변화에 따라 동적으로 세션을 관리하는 모델을 설계한다.

초기 사용자가 서비스를 요청할 경우 인증(Authentication) 과정을 거친다. 이렇게 인증 과정이 통과되면 세션 요청을 하게 되고, 현재 사용자의 역할 할당과(URA), 상황 역할 할당(CRA)을 고려하여 세션을 활성화/비활성화(Activation/Deactivation) 시킨 뒤, 최종적으로 세션을 형성한다.



(그림 4) 세션 형성

3.2 주요 구성 요소 정의 및 구성

CAACM 에서 사용한 정형화 표기 방식을 이용하여 구성 요소를 정의하면 다음과 같다.

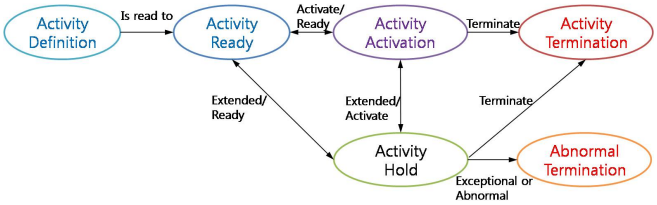
<표 2> 구성 요소 정의

구성요소	설명
U(User)	보안 관리 영역의 자원과 응용을 이용하는 모든 사용자
UR(User Role)	사용자의 역할
C(Context)	기업의 사무 환경 내부의 상황 정보들을 표현. 예)사용자의 위치, 시간, 시스템 CPU 사용량 등
CR(Context Role)	상황 역할(상황 정보들의 추상화)
Role	사용자 역할과 상황 정보 역할을 포함한 역할들의 집합
Obj(Object)	사무 환경에서 사용될 수 있는 객체 예)문서, 이미지 파일 등
Op(Operation)	보안 관리 영역의 자원과 응용의 실행 예)읽기/쓰기
Permission	권한(Obj×Op)
Workflow	워크플로우
Activity	업무에 속해 있는 활동
Session	사용자의 위치, 활성화 상태, 객체의 상태, 사무 환경의 상황 정보의 활성화된 연결

CAACM 은 워크플로우에서 사용되는 활동(Activity)에 동적인 접근 제어를 하기 위해서 상황 역할(CR) 즉 상황 정보 추상화를 이용한다. 이러한 상황 역할은 사용자의 상황 정보(UR)(직위, 위치 등), 활동 상태(Activity Status), 객체 상태(Object Status), 환경 정보(시스템의 상태 정보 및 업무의 환경 정보)를 관리한다. 따라서 상황 역할(CR)을 체크하며, 또한 각 활동에서 사용될 수 있는 객체의 상태를 확인하여 업무의 활동(Activity)을 활성화/비활성화 시킨다.

A. 활동 상태(Activity Status)

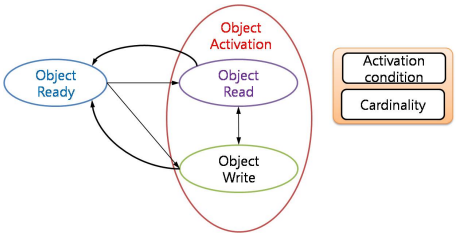
활동 상태는 (그림 5)과 같이 활동을 정의하고, 활동의 준비, 휴지, 활성화, 종료, 비정상 종료의 상태 변화를 나타내어 활동의 동적인 상태를 적용한다.



(그림 5) 활동 상태

B. 객체 상태(Object Status)

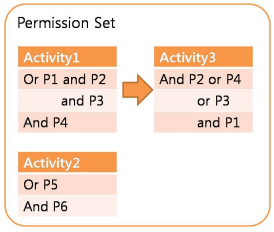
객체 상태는 (그림 6)처럼 객체(Object)는 동작(Operation)과 함께 권한/허가(Permission)에 속한다. 활성화 조건(Activation condition)과 Cardinality 의 속성을 갖는 활동(Activity)은 권한에서 살펴본 객체의 상태에 제약을 받는다.



(그림 6) 객체 상태(Object Status)

C. 활동(Activity) 관계 정의

워크플로우에 속해 있는 활동들은 특성에 따라 다른 활동에 종속되거나 독립적일 수 있다. 하나의 활동은 하나 이상의 권한(Permission)을 할당 받으며 이렇게 할당 받은 권한은 or/and 를 통하여 활동에 부여된다. 이렇게 정의된 활동은 다른 활동과 종속 또는 독립적인 관계를 형성하는데 이 집합을 Permission Set 이라 정의한다.

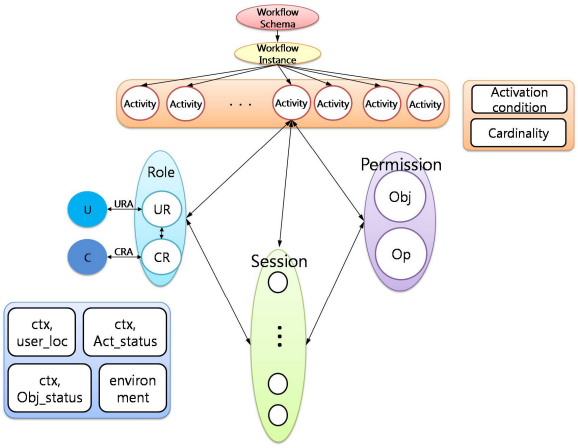


(그림 7) 객체 상태(Object Status)

(그림 7)에서 보듯이 Activity3 은 Activity1 의 수행이 끝난 뒤 실행이 되며, Activity2 은 독립적으로 수행될 수 있다.

D. CAACM 구조

CAACM 의 전체 구조는 (그림 8)에서 보듯이 사용자의 역할과 상황 역할의 관계를 나타내는 Role, 기업의 업무를 나타내는 워크플로우, 객체와 동작을 통한 권한이 업무와 관계를 맺어 접근 제어가 성공하게 되면 세션이 형성된다. 이러한 세션은 Role 의 상황 정보들에 의해 지속적으로 동적인 변화를 관리하여 접근 제어를 수행한다.



(그림 8) CAACM 구조

3.3 정책(Policy) 구성 및 시나리오

CAAC 는 접근 제어 정책으로써 관리 영역 내의 다양한 환경 정보나 시스템 상태 등 상황 정보를 사용하므로 관리 영역 내의 모든 구성 요소들 간의 관계를 명확하게 관리해야 한다. 이런 접근 제어 정책은 transaction 기반으로 정의할 수 있다.

정책은 "Policy = (UR, CR, Activity), Accept/Deny"로 표현할 수 있다. Accept/Deny 는 허가 여부를 나타낸다. 예를 들어, "정책 1 = (사용자의 위치 정보(무선 단말을 이용한 접속), 시간 정보(08:00~22:00), 회사의 Database 에 접속), Deny"으로 정책이 설정되어 있다면 사용자가 무선 단말을 이용해서 8 시에서 22 시 사이에 회사의 Database 에 접속을 시도할 경우 접근이 거부된다.

4. 비교

기존의 TBAC 모델은 인가 처리와 직무 프로세스의 생명주기에 대한 감시와, 인스턴스와 사용기반 접근 제어뿐만 아니라, 타입기반의 접근 제어도 가능하지만 역할과 상황에 따른 접근제어 정책 구성 및 관리가 어렵다. 또한 T-RBAC 모델은 접근 권한이 직무에 할당되고, 직무에 각각 역할이 할당되지만, 상황 기반의 정책관리가 어렵다. 반면, CAACM 은 상황 정보 기반의 접근 제어 정책 관리가 용이하고 접근제어 요청자의 역할 및 수행하고자 하는 직무를 고려한 정책 구성이 가능한 모델로써, 상황의 변화에 따라 동적으로 세션 관리가 가능하며, 직무의 흐름에 따른 능동적 접근제어가 가능하다.

5. 결론

유비쿼터스 컴퓨팅 환경에서는 센서를 통해 시스템이나 상황 정보를 수집하거나 분석하여 정보를 제공해주는 상황 인식 시스템이 중요한 역할을 한다. 따라서 접근 제어 모델에서도 상황 인식 정보를 반영하여 개발해야 한다. 본 논문은 상황 인식 정보와 사용자, 그리고 활동을 효율적으로 관리하기 위한 워크플로우 시스템 기반의 상황 인식 기반 접근 제어 모델을 제안하여, 수많은 상황 정보 및 사무 정보와 사용자가 동적으로 변화하는 사무 환경에서 사용자에게 동적인 접근을 제어하기 제공한다. 또한 상황 인식을 통하여 기업 정보 유출의 보안 위협으로부터 사전에 예방하고 차단할 수 있는 장점을 가져 활용도가 매우 클 것으로 기대된다.

참고문헌

[1] Seon-Ho Park, Young-Ju Han, and Tai-Myoung Chung, "Context-Role Based Access Control for Context-Aware Application", The 2006 International Conference on High Performance Computing and Communications(HPCC-06), pp.572-580, September 2006.

[2] David F Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn and Ramaswamy Chandramouli, "Proposed NIST Standard for Role-Based Access Control", ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001.

[3] Sejong Oh and Seog Park, "An Integration Model of Role-Based Access Control and Activity-Based Access Control Using Task", Proceedings 14th Annual IFPI WG 11.3 Working Conference on Database Security, pp.557-569, August 2000.

[4] R.K. Thomas, R. Sandhu, "Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management", Proceedings of the IFIP WG11.3 Workshop on Database Security, Vancouver, Canada, 1997.

[5] Sejong Oh and Seog Park, "Task-role-based access control model", Information System, Vol.28, No.6, pp.533-562, September, 2003.