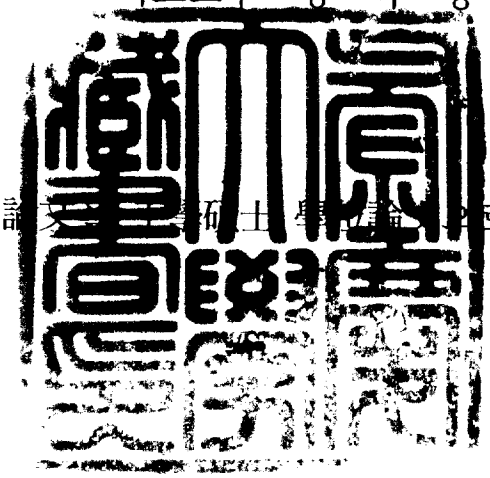
공학석사 학위논문

RBAC를 이용한 컨텍스트-기반 적응적 접근 제어 관리 모델

지도교수 정 목 동



이 論文을 工學碩士 學位論文으로 提出함

2005년 2월

부경대학교 대학원

컴퓨터공학과

서 정 철

이 논문을 서 정 철의 공학석사
학위논문으로 인준함

2004년 12월

주 심 공학박사 우 종 호 (인)

위 원 공학박사 권 오 흠 (인)

위 원 공학박사 정 목 동 (인)

목 차

그 림 목 차

표 목 차

RBAC를 이용한 컨텍스트-기반 적응적 접근 제어 관리 모델

서 정 철

부 경 대 학 교 대 학 원 컴 퓨 터 공학과

요약

최근 인터넷의 급성장으로 유·무선 통합 환경이 제시되었고, 이를 기반으로 모든 사물에 컴퓨팅과 네트워킹 기술이 적용되어 도처에 존재하는 컴퓨팅 인프라를 통해 사람과 컴퓨팅 기기 및 환경이 서로 상호작용 하는 유비쿼터스 환경이 도래하고 있다.

유비쿼터스 환경에서는 다양한 자원들이 다양한 특성을 지닌 채 공존함에 따라 시간과 상황에 따라 적응적으로 대응 할 수 있는 보안 및 프라이버시 기술이 필요하다.

그러나 현재의 보안 서비스는 특정 환경 요소를 정적으로만 반영하고 있기 때문에 자원의 환경 요소가 동적으로 변화하는 유비쿼터스 환경에서는 적절하게 반영할 수 없다. 또한 동적인 변화를 가진 환경요소를 지닌 수많은 다양한 자원들이 공존하는 유비쿼터스 환경에서 사용자나 애플리케이션

이 보안 설정을 위한 세부 사항을 개별적으로 관리하는 것은 복잡하고 많은 부담이 따른다.

따라서 본 논문에서는 MAUT(Multi-Attribute Utility Theory)와 간결한 휴리스틱스(Simple Heuristics)를 이용하여 유비쿼터스 환경에서 제공되는 사용자들이 원하는 정보나 거래 정보의 민감도 등과 같은 다양한 환경요소의 상황정보를 고려하여 보안정책을 동적으로 결정할 수 있는 적응적 접근 제어 알고리즘을 제안한다. 또한 다양한 자원의 보안정책의 설정 및 관리의 복잡함과 어려움을 해결하기 위해 RBAC(Role-Based Access Control) 모델과 제안 알고리즘을 결합한 RBAC를 이용한 적응적 접근 제어 관리 모델을 제안한다.

제안 모델은 다양한 환경 요소의 상황 정보에 따라 적응적으로 접근 제어를 결정하고, 보안정책의 설정 및 관리를 간결하게 함으로서 행정기관, 군, 금융기관, 교육기관, 기업 등의 기밀문서, 정보 등 다양한 자원을 보호하기 위한 보안 관리시스템, 디지털 콘텐츠 유통을 위한 시스템 등 다양한 분야에 적용이 가능하며, 자원의 다양한 특성을 고려하여 보안정책을 적용함으로서 자원을 안전하고 효율적으로 관리 할 수 있으며, 체계적인 보안 체계의 구축 및 운영이 가능함으로 유지/관리 비용을 줄일 수 있을 것으로 예상된다.

Context-Based Adaptive Access Control Management Model Using RBAC

Jung Chul Seo

Dept. of Computer Eng., Graduate School,

Pukyong National University

Abstract

Recently, wire and radio internet combination presented by the rapid growth of internet and on the basis of this, computer and network technology were applied to all things.

By the result, ubiquitous environment that a person and computer appliances and environment that use computer infra that exist on each place do interaction is coming.

These characteristics of heterogeneous networks and diverse computing capabilities are dynamically changing by contextual information of the

environment. We should adapt several security system dynamically according to the diverse networks and computing devices to secure this ubiquitous computing environment.

Applying the traditional security system to heterogeneous networks has many problems, since traditional security system has a static decision-making approach. The traditional security' system did not consider changes of contextual information.

It might be quite difficult and complicated to manage security decision in the heterogeneous networks because many types of resources are coexisting.

In this thesis, we propose a context-based adaptive access control model which can adapt several access control policies dynamically according to the diverse networks and computing devices using MAUT (Multi-Attribute Utility Theory) and Simple Heuristics.

We propose an access control model using RBAC(Role Based Access Control) that can determine effectively access control using security policy and access policy to manage security policy appropriately in the heterogeneous networks.

The proposed system could be used in the various fields such as security management, distribution of the digital content, access control in the administrative organization, military, finance organization, company, and so on.

The proposed method is expected to reduce the complexity and cost of security administration and to adapt several security policies dynamically according to the diverse network and computing devices in the heterogeneous networks.

1. 서론

최근 인터넷의 급성장으로 유·무선 통합 환경이 제시되었고, 이에 따라 음악, 영화와 같은 다양한 멀티미디어 컨텐츠 그리고 휴대폰에서 PDA, 고성능 PC에 이르기까지 유·무선망 기반으로 한 다양한 자원들이 공존하게 되었다. 이에 따라 컴퓨팅과 네트워킹 기술이 적용되어 도처에 존재하는 컴퓨팅 인프라를 통해 사람과 컴퓨팅 기기 및 환경이 서로 상호작용 하는 유비쿼터스 환경[1, 2]이 도래하고 있다.

유비쿼터스 환경[1, 2]이란 사람이 컴퓨터 내부의 가상공간으로 접속하던 환경과는 달리 컴퓨터가 사람의 현실공간으로 다가오는 개념으로 컴퓨터가 도처에 편재하여 장소나 시간에 따라 변하는 자원의 환경요소(물리적 상황 : 사용자의 위치, 디바이스의 종류 및 성능, 정서적 상황 : 사용자의 선호도, 역사적 상황 : 현재 시간 등)의 상황 정보(Contextual Information)[3, 4]를 서비스 받을 수 있음을 의미한다. 이러한 환경요소에 관한 정보를 컨텍스트(context)[3, 4]라 하며 컨텍스트 인지(Context-Awareness)[5]를 바탕으로 자동화된 서비스를 제공할 수 있을 것이다.

이와 같은 유비쿼터스 환경에서는 다양한 자원들이 다양한 특성을 지닌 채 공존함에 따라 시간과 상황에 따라 적응적으로 대응할 수 있는 보안 및 프라이버시를 위한 기술들이 대두되고 있다[6].

그러나 현재의 보안 서비스는 특정 환경 요소를 정적으로만 반영하고 있

기 때문에 자원의 환경 요소가 동적으로 변하는 유비쿼터스 환경에서는 적절하게 반영할 수 없을 뿐만 아니라 다양한 형태의 자원이 공존함으로 효율적 관리가 어렵다. 그 이유는 동일한 자원이라도 서비스 제공자나 이용자의 환경 요소의 상황 정보에 따라 달라 질수 있다는 것이 고려되지 않고 있기 때문이다.

Mahan[7]등은 보안 설정과 효율성 제고를 조절하기 위한 모델을 제공하기 위하여 QoSS(Quality of Security Service)를 정의하고 네트워크 모드와 보안 등급을 세 종류로 정의하고 있다. 특별한 위협 요인이 없는 평상시의 운영 모드인 nomal 모드, 고 수준의 트래픽 모드인 impact 모드, 최고의 보안 등급을 요구하는 emergency 모드 등으로 나누고 보안 등급을 상, 중, 하로 나누고 있지만 미리 정의된 테이블을 사용하는 등 동적인 변화에 적응적으로 대응하는 면에서 한계를 보이고 있다.

Blaze등이 제안한 KeyNote[8]는 보안 설정과 효율성 제고를 조절하기 위한 모델을 제공하고 있는 QoSS의 핵심 내용으로서 보안정책 설정을 동적으로 조절한다. KeyNote가 정책 명세 언어 가운데 하나이긴 하지만 복잡한 표현식을 사용하고 있으므로 실제 구현하는 데 많은 어려움을 가진다.

따라서 본 논문에서는 다중 변수에 대한 의사 결정 문제(decision problem)를 해결하기 위해서 경제학 이론에서 출발한 정량적 의사 결정 이론인 MAUT(Multi-Attribute Utility Theory)[9]와 ABC 그룹의 학제 간 연구 결과인 간결한 휴리스틱스(Simple Heuristics)[12] 알고리즘을 사용하여

사용자들이 원하는 정보나 거래 정보의 민감도 등과 같은 다양한 환경요소의 상황 정보(Contextual Information)에 따라 접근 제어를 동적으로 결정할 수 있는 적응적 접근 제어 알고리즘을 제안한다. 그리고 다양한 자원의 보안정책 설정 및 관리의 복잡함과 어려움을 해결하기 위해 RBAC (Role-Based Access Control)[13, 14] 모델 개념과 제안 알고리즘을 이용한 RBAC를 이용한 적응적 접근 제어 관리 모델을 제안한다.

서론 이후의 논문의 구성은 다음과 같다. 2 장에서는 제안 모델에 관련된 연구 내용을 설명하고, 3 장에서는 보안정책을 적응적으로 결정하는 적응적 접근 제어 알고리즘과 이를 기반한 RBAC를 이용한 컨텍스트-기반의 접근 제어 관리 모델을 제안한다. 그리고 4 장에서는 사례연구 및 구현을 설명하며, 5 장에서는 결론과 향후 연구에 대해서 논의한다.

2. 관련 연구

2.1. 유비쿼터스 컴퓨팅 환경

제록스 연구소에서 전산분야 연구책임을 맡았던 Mark Weiser에 따르면, 유비쿼터스 컴퓨팅 환경 아래에서는 특별하게 제작된 수많은 컴퓨터 하드웨어, 센서 및 소프트웨어가 유무선 네트워크로 연결되어 우리 주위의 모든 장소에 존재하고, 그들의 존재를 일반 사용자들이 알아차리지 못하는 가운데, 조용하게 우리의 일상생활 속에 자리를 잡고, 여러 가지 서비스를 수행하며 우리를 도와줄 것이라는 것이다. 그래서 컴퓨터가 우리의 삶 속으로 깊숙이 스며들어 마치 "숲 속을 거닐 듯이" 편안하고 자연스러운 상태에서 컴퓨터를 사용하게 되는 것이라고 한다[1, 2].

유비쿼터스 환경[1~5]이란 사람이 컴퓨터 내부의 가상공간으로 접속하던 환경과는 달리 컴퓨터가 사람의 현실공간으로 다가오는 개념으로 컴퓨터가 도처에 편재하여 장소나 시간에 따라 변하는 자원의 환경요소의 상황 정보를 서비스 받을 수 있음을 의미한다. 이러한 환경 요소에 관한 정보를 바탕으로 자동화된 서비스를 제공할 것이다.

유비쿼터스 환경에서는 다양한 성능과 특성을 가진 자원들이 공존함에 따라 환경요소의 컨텍스트에 따라 적응적으로 대응할 수 있는 보안 및 프라이버시를 위한 기술성이 대두되고 있다[6].

그러나 현재의 보안 서비스는 서비스 제공자나 이용자의 상황 정보가 고려되지 않기 때문에 유비쿼터스 환경에 그대로 적용되기 어렵다. 따라서 자원을 안전하게 보호하기 위해서는 자원의 다양한 특성을 고려하여 적응적으로 보안 서비스를 제공하는 매커니즘이 필요하다.

2.2. 컨텍스트와 컨텍스트-인지 컴퓨팅

컨텍스트(Context)[3, 4]란 용어는 컴퓨터 과학의 다양한 분야에서 여러 의미로 정의되고 사용되고 있다. 그러나 유비쿼터스 환경에서 사용되는 컨텍스트의 정의는 다음과 같다.

Xerox PARC의 B. Schilt는 컨텍스트를 사용자와 객체에 관련된 신원 및 객체의 정보로 정의하였고[15], Georigia의 G.D. Abowd[16]는 컨텍스트를 애플리케이션, 사용자, 장소 등의 객체와 이와 관련된 모든 정보라 정의하였다.

이와 같이 유비쿼터스 환경에서는 다양한 자원의 환경 요소에 대한 컨텍스트를 생성 및 통합하고 통합된 정보를 기반으로 사용자 별로 차별화된 서비스를 제공하는 것이 필요하다.

컨텍스트-인지 컴퓨팅(Context-Aware Computing)이란 유비쿼터스 환경에서 임의의 애플리케이션이 사용자의 환경요소에 대한 상황 정보(Contextaul Infomation)[3, 4](물리적 상황 : 사용자의 위치, 디바이스의 종류 및 성능, 정서적 상황 : 사용자의 선호도, 역사적 상황 : 현재 시간 등)

를 감지하여, 사용자가 이를 이용할 수 있도록 해주는 컴퓨팅 패러다임[17]이라 정의 할 수 있다. 즉, 자원의 환경요소의 상황정보인 컨텍스트와 사용자가 입력한 정보를 결합하여 사용자가 처한 상황에 맞게 사용자가 원하는 스타일로 조정하여 사용자에게 적절한 서비스를 제공하는 것을 말한다.

Ghita와 Patrick[18]은 보호된 자원에 대하여 컨텍스트에 기반하여 컨텍스트에 권한을 부여할 수 있는 프레임워크를 제안하였다. 이 연구에서는 사용자의 신원정보 뿐만 아니라 다양한 환경으로부터 획득된 정보를 사용하여 결정된 자원에 대한 접근 제어 정책에 따라 자원에 대한 접근을 허가 또는 거부를 하게 된다.

이와 같이 다양한 사용자의 정보가 노출된 유비쿼터스 환경에서 안전한 서비스를 제공하기 위해서는 사용자의 상황정보를 사용하는 컴퓨터 패러다임인 컨텍스트-인지 컴퓨팅을 기반으로 동적으로 변하는 컨텍스트에 적절하게 대응할 수 있는 적응적인 보안 서비스가 필요하다.

2.3. RBAC(Role-Based Access Control)

RBAC[13, 14]는 사용자의 역할에 기반을 둔 접근 통제 방법으로 Ravo S. Sandhu에 의해 제안되어졌다.

조직 내에서의 역할은 사용자 교체, 업무(task)의 재 할당에 비해 상대적으로 변화가 적기 때문에, RBAC는 조직 내의 사용자 허가 할당에 있어서

복잡성과 비용, 잠재적인 실수를 줄이기 위한 강력한 매커니즘을 제공한다. 또한 조직 수준에서 보안 관리를 증진시키기 위해서 사용자 식별자 수준이 아닌 추상화 수준을 제공하므로 업무를 수행하는 실제 환경에 자연스럽게 접목될 수 있다.

따라서 RBAC는 권한 관리를 매우 단순화 시켜주고, 특정한 보안정책을 구현하는데 있어서 유연성을 제공하는 장점이 있다. 또한, 사용자는 그들의 의무적 권한과 책임에 따라 특정 역할의 구성원이 되며 접근 구조의 변경 없이도 역할의 변경을 쉽게 할 수 있다. 따라서 수행이 어려운 보안관리 과정을 관리자가 효과적으로 처리 할 수 있도록 해주며 조직에 적합한 보안정책을 표현하고 적용할 수 있다.

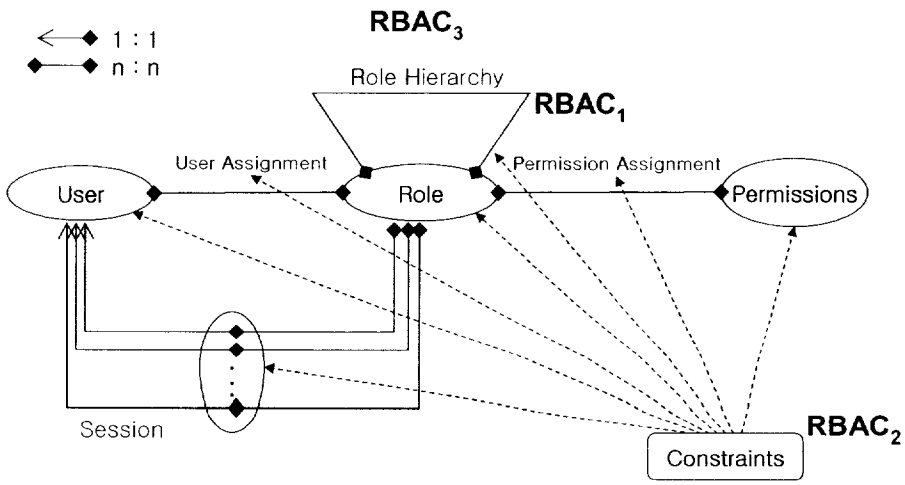


그림 1. Ravi S. Sanhu의 RBAC 모델

그림 1은 Ravi S. Sandhu가 제안한 4가지 형태의 개념적인 모델인

$RBAC_0$, $RBAC_1$, $RBAC_2$, $RBAC_3$을 보여준다.

동적으로 변화하는 수많은 자원들이 공존하는 유비쿼터스 환경에서 다양한 서비스를 제공하기 위한 자원이 빈번하게 추가될 때마다 자원의 보안설정을 개별적으로 설정하고 관리하는 것은 복잡하고 많은 부담이 따른다. 이러한 상황에 대처하기 위해서는 보안정책의 설정과 변경이 쉽고 변경된 보안정책이 잘 반영 될 수 있는 유동적인 보안 관리 시스템이 필요하다.

2.4. MAUT(Multi-Attribute Utility Theory)

MAUT[9]는 다중변수에 대한 의사결정 문제(decision problem)에서 유틸리티(utility)를 통한 정략적인 의사결정 방법이다. 유틸리티 분석(utility analysis)은 의사 결정자(decision maker)가 원하는 제비뽑기(lottery)의 결과를 분석해주는 분야로서 의사 결정자는 이들 결과에 대한 개인의 선호도(preference)를 유틸리티 수로 표현한다.

유틸리티는 0과 1사이의 상대적인 값으로서 가장 선호하지 않는 결과 유틸리티를 $u(x^0)=0$, 가장 선호하는 결과 유틸리티를 $u(x^*)=1$로 나타낸다. 그리고 결과에 대한 유틸리티 수의 대입은 의사결정자의 최적행동의 기준이 되는 기대 유틸리티(expected utility)를 최대화 시켜주는 쪽으로 이루어진다.

예로 디지털 카메라의 경우[10], 화질(quality of image), 플래시(flash), 파인더(viewfinder), 작동시간(operation time), 조작 방법(handling)등의 속성

으로 평가할 때 전체 유틸리티 함수는 다음과 같이 정의된다.

$$u(x_1, x_2, \ldots, x_n) = \sum_{1}^{n} k_i u_i(x_i), \quad \sum_{1}^{n} k_i = 1$$

여기서, k_i는 각 속성에 대한 가중치(relative important value)이고 $u_i(x_i)$는 각 속성에 대한 유틸리티 함수가 된다.

특히 MAUT를 전자 상거래에 사용한 예로 Pmart(Pukyoung-mart)[11]에서는 가격에만 의한 기존의 협상을 개선하기 위하여 상품의 특성, 보장 기간, 서비스정책 등 다양한 조건에 대해 MAUT를 이용하여 협상을 수행하는 에이전트 중재에 의한 전자 상거래 프레임워크이고 독일의 "Stiftung Warentest"[19]는 MAUT를 이용해 상품을 평가하는 방법으로 소비자에게 널리 알려져 있다.

사용자를 포함한 다양한 자원들의 환경 변수들이 혼재하게 되는 유비쿼터스 환경에서 다양한 변수에 기반하여 의사결정을 하기 위해서는 자원마다 다른 환경 상황을 가지는 유틸리티를 기반으로 MAUT이론을 적용하는 것이 효율적이다.

2.5. 간결한 휴리스틱스

간결한 휴리스틱스(simple heuristics)[12]는 1995년 독일, 미국, 영국에서 심리학, 수학, 컴퓨터과학, 경제학, 생물학 등 학제간의 연구를 위해서 설립된 ABC(Adaptive Behavior and Cognition) 연구그룹의 주된 이론이다.

이 연구소에서는 제한적 추리(bounded rationality)와 불확실성 하에서 좋은 의사 결정에 관한 연구를 해오고 있다. 간결한 휴리스틱스를 이용하려는 이유는 보안 관련 특징 변수와 관련된 사용자들의 선호도를 개량적으로 정확히 예측한다는 것이 쉬운 일이 아니기 때문이다.

간결한 휴리스틱스 중에서 대표적인 것은 Take The Best가 있으며, 이는 특징변수(cue)를 차례로 조사하여 두 개체를 차등화 시켜 줄 수 있는 변수를 발견하면 이 변수가 추론의 근거가 되고 나머지 특징변수는 모두 무시한다. Take The Best는 특히 훈련 집합의 규모가 적을 때 다중회귀(multiple regression)보다 성능이 뛰어나다[12].

3. RBAC를 이용한 컨텍스트-기반 적응적 접근 제어 관리 모델

본 논문에서의 제안 모델은 사용자의 단말기 성능, 네트워크 유형, 시스템의 보안 상태, 요구하는 자원의 중요도 및 가치 등과 같은 다양한 환경 변수에 대한 컨텍스트(Context)의 동적인 변화에 따라서 보안 시스템의 속성들 즉, 암호 알고리즘의 종류, 키 길이, 프로토콜, 인증 기법 등을 적절히 변화시킴으로서 제안 모델의 보안 시스템 상태는 동적으로 변화하는 자원의 환경 변수에 따라서 최적으로 적응한다.

또한 다양한 자원의 보안정책의 설정 및 관리의 복잡함과 어려움을 해결하기 위해 RBAC[13, 14] 모델의 역할 개념을 이용하여 자원의 보안정책 및 접근정책을 할당함에 있어서 복잡성과 비용, 잠재적인 실수를 줄일 수 있는 메커니즘을 제공한다.

그림 2는 본 논문에서 제안한 RBAC를 이용한 적응적 접근 제어 관리 모델의 전체 구성도이다. 제안 모델의 동작 원리는 다음과 같다.

한 사용자가 보호된 자원에 접근을 시도할 때, 서비스 제공자는 인터넷, IMT-2000, 무선랜 등 다양한 특성을 가진 사용자와 사용자의 환경으로부터 사용자 컨텍스트(User Environment Context), 시스템 컨텍스트와 같은 다양한 상황 정보를 수집하여 제안 모델의 컨텍스트 번역기(Context Interpreter)에게 전달한다. 컨텍스트 번역기는 수집된 컨텍스트를 정량적인

값으로 변환을 한다.

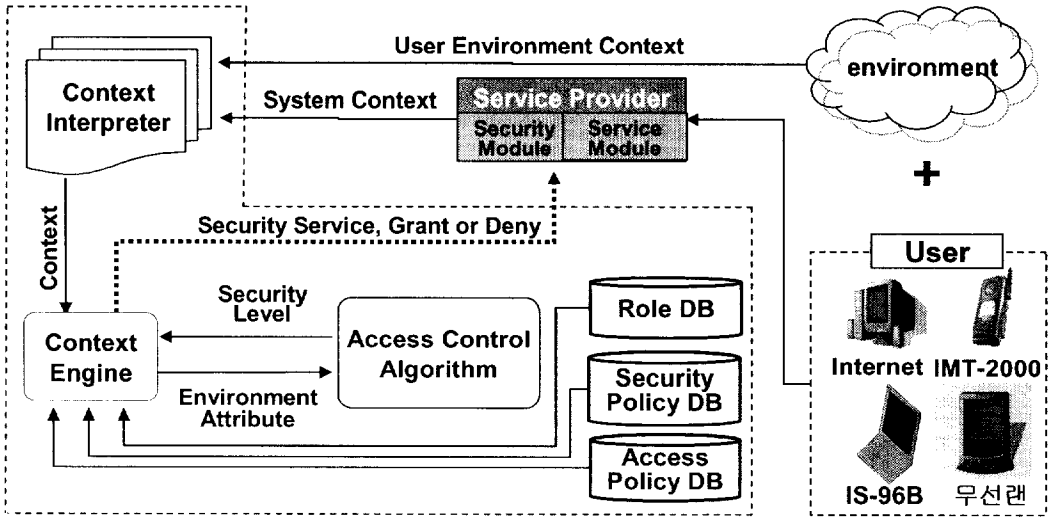


그림 2. RBAC를 이용한 컨텍스트 기반 적응적 접근 제어 관리 모델

컨텍스트 엔진(Context Engine)은 요구된 자원에 적용된 역할을 이용하여 자원에 할당된 보안정책과 접근정책을 확인한다. 그리고 컨텍스트 엔진은 적응적 접근 제어 알고리즘을 이용하여 보안 등급을 평가한다.

적응적 접근 제어 알고리즘에서는 컨텍스트 번역기에서 변환된 정량적인 값들과 보안정책을 이용하여 보안 등급을 평가하고 컨텍스트 엔진에게 전달한다. 그리고 컨텍스트 엔진은 보안 등급(Security Level)과 접근정책(Access Policy)을 이용해 보안 서비스와 자원에 대한 접근 제어를 결정한다.

이러한 결과 값들은 서비스 제공자에게 전달되어 사용자에게 적절한 보안

서비스가 적용되고 자원에 대한 접근 여부를 전달한다. 그리고 자원의 보안 설정 및 관리를 위해서는 자원의 특성과 보안 요구사항에 따라 적절한 역할만을 할당함으로서 자원을 보호하기 위한 보안정책과 접근정책을 적용할 수 있다.

그림 3은 제안 모델의 순서 다이어그램을 나타내고 있다.

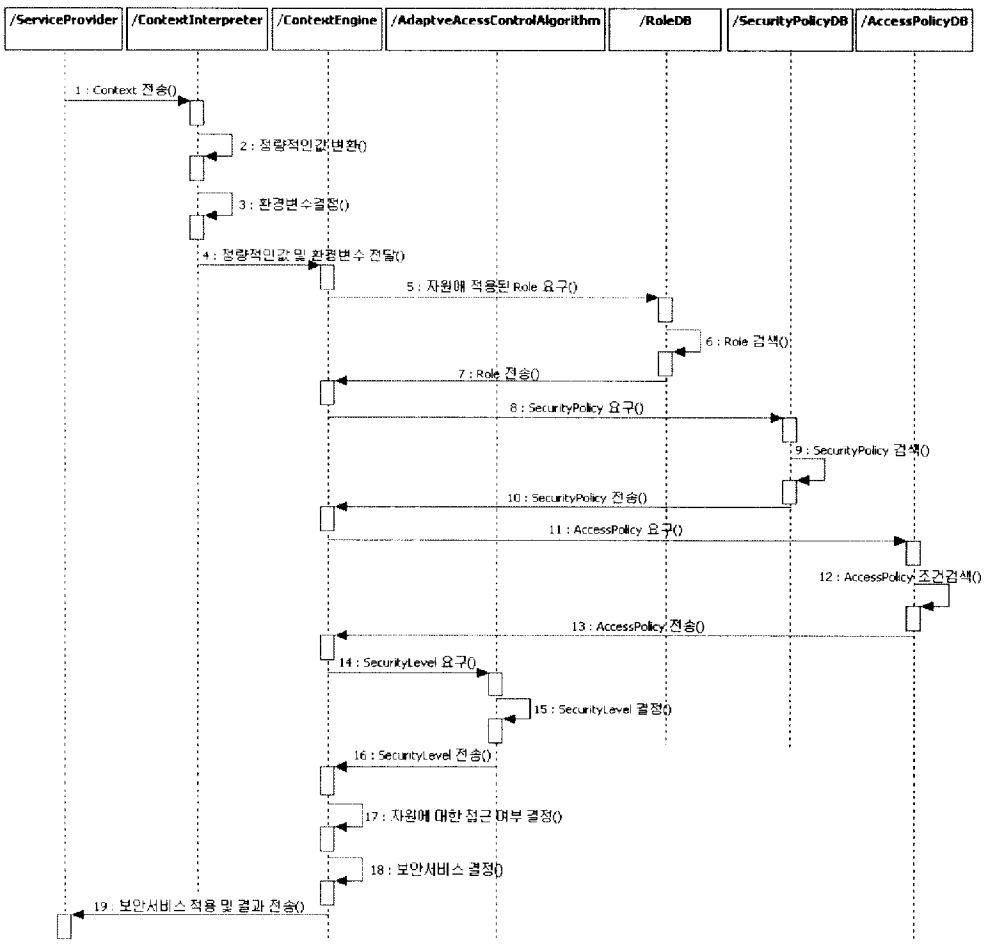


그림 3. 제안 모델의 순서 다이어그램

3.1. RBAC를 이용한 접근 제어 관리 모델

동적인 변화를 가진 환경요소를 지닌 수많은 자원들이 공존하는 유비쿼터스 환경에서 관리자나 애플리케이션이 보안정책과 접근정책을 위한 세부사항을 개별적으로 모두 설정하고 관리하는 것은 복잡하고 많은 부담이 따른다.

본 논문에서는 이러한 문제를 해결하기 위해서 RBAC를 이용한 접근 제어 관리 모델을 제안한다.

RBAC에서는 특정 사용자에게 특정 권한을 부여하기 위해 역할의 개념을 사용하는 대신 제안 모델에서는 특정 자원에게 필요한 정책을 적용하기 위해서 역할의 개념을 확장하여 사용했다.

자원은 중요도, 가치 등의 다양한 특성에 따라 특정의 정책(보안정책, 접근정책)을 포함한 역할의 구성원이 되며 이들 개별 자원들에 대한 접근 권한은 정책의 변경 없이도 역할의 변경을 통해 다양한 정책을 할당 할 수 있으므로 수행이 어렵고 복잡한 보안 관리의 과정을 보안 관리자가 효과적으로 처리 할 수 있도록 해주며 자원의 동적인 변화에 따라 적절한 정책들을 표현하고 적용 할 수 있다.

그림 4는 RBAC를 이용한 접근 제어 관리 모델을 보여준다. 제안모델은 자원(Resource), 역할(Role), 권한(Permission): 접근정책, 보안정책과 제한

(Constraints)으로 구성되어 있다.

- **자원** : 자원은 서비스를 제공하기 위해서 사용되는 객체로서 하나의 자원은 하나 이상의 서비스와 대응된다. 자원은 안전하게 보호되어야 한다. 따라서 적절한 보안정책과 접근정책이 적용되어야 한다.
- **역할** : 역할은 시스템에서 자원의 특성과 보안 요구사항에 따라 분류된 주체로서 하나의 역할은 하나이상의 자원과 대응된다. 역할은 분류에 따라 자원을 안전하게 보호하기 위한 보안정책, 접근정책을 갖는다.
- **권한과 제한** : 권한은 접근정책과 보안정책을 포함한다.

  접근정책은 시스템에서 하나 또는 그 이상의 객체에 특정 접근 모드(읽기, 쓰기, 수정, 다운로드 등)의 승인 또는 거부를 결정한다. 보안정책은 다양한 환경 변수를 고려하여 동적으로 보안 등급과 보안 서비스를 결정한다.

  제한은 정책을 적용하기 위한 요구조건이다.
- **세션** : 특정 사용자에 의해 자원의 사용이 요구됨에 따라 자원에 할당된 역할이 활성화된 상태를 의미한다.
- **자원할당과 권한할당** : 자원 할당과 권한 할당은 다 대 다의 관계이다.

  권한 할당은 보안정책과 접근정책을 직접 자원에 적용하는 대신 시스템의 보안 요구사항에 따라 분류된 역할에 할당한다.

  자원은 자원 할당을 통해 특성에 따라 분류된 역할이 적용됨으로서 자원을 보호하기 위한 보안정책과 접근정책이 적용된다.

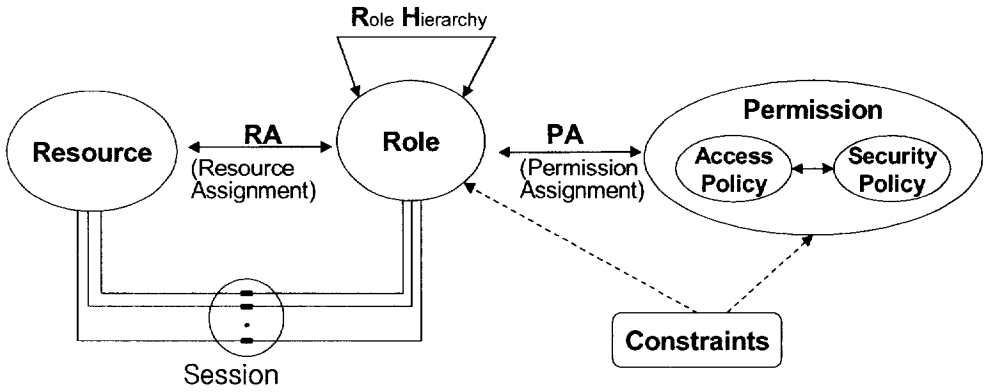


그림 4. RBAC를 이용한 접근 제어 관리 모델

제안된 모델에서 자원의 특성과 보안 요구사항에 따라 특정 역할을 할당함으로서 보안 설정이 가능하다. 즉, 자원의 특성과 보안 요구사항에 따라 적절한 역할을 할당함으로서 보안정책과 접근정책을 적용할 수 있으므로, 보안정책 관리가 간결화 되는 이점을 가지고 보안정책 적용을 유연하게 만든다.

3.1.1. 보안정책과 접근정책

본 논문에서 사용하고 있는 보안정책은 자원의 특성에 따라 보안 등급을 결정하기 위한 유틸리티 함수, 환경 변수, 사용자 선호도와 역할 그리고 요구조건인 제약과 같은 세 개의 필수 조건을 가지고, 접근정책은 역할과 다운로드, 읽기와 같은 서비스를 제공하기 위한 세부적인 권한을 가진다.

그림 5는 'Confidential' Role에 할당된 보안정책과 접근정책의 예를 보여준다. 'Confidential' Role에 적용된 보안정책과 접근정책의 의미는 다음과

같다.

보안정책을 적용한 보호된 자원에 접근하기 위해서는 200_{Mhz} 이상의 CPU가 탑재된 단말기, 100_{Kbps} 이상의 네트워크 전송 속도, PC, PDA 또는 휴대전화의 사용 등이 제약조건으로 요구되고, 보안등급을 결정하기 위해서 X_{att}(보안강도), X_{auth}(인증기법), X_{res}(자원의 보호수준) 등을 환경 변수로 사용한다는 것을 의미한다.

그리고 접근정책 'A'에서는 보안등급이 1 이상이고 단순 사용자인 경우에는 08시~18시 사이에만 읽기가 허가된다는 것을 의미한다. 또한 접근정책 'B'에서는 보안 등급이 2 이상이고 멤버인 경우에는 자원을 다운로드가 허가된다는 것을 의미한다.

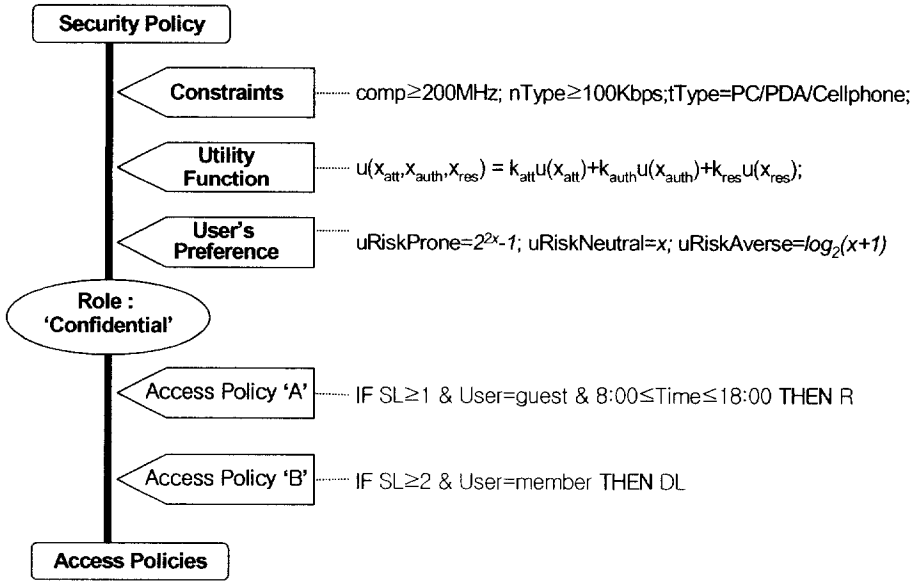


그림 5. 'Confidential' Role의 보안정책과 접근정책의 예

이와 같이 자원의 특성에 따라 명시된 요구조건들을 보안 요구사항에 따라 정책들을 부여함으로 자원 보호의 측면에서 기존의 관리 방식보다 안전하고 효율적으로 관리 할 수 있다. 또한 환경 변수가 동적으로 변할 수 있는 현재의 환경에서 자원의 특성에 따라 다양한 환경 변수를 고려하여 동적으로 보안서비스를 결정함으로 더욱 효율적인 보안정책 적용이 가능하다.

즉, 사용자의 환경에 따라 동적으로 적절한 보안등급이 결정되고 그에 따른 보안서비스를 제공받기 때문에 기존의 정적인 보안서비스를 이용함으로 열악한 환경의 사용자에게 무리한 시스템 자원이나 대기시간을 요구하는 비효율성 문제를 해결할 수 있을 뿐만 아니라, 자원의 특성에 따른 접근정책으로 인해 악의를 가진 사용자로부터 자원을 안전하게 보호할 수 있는 메커

니즘을 제공한다.

3.1.2. 자원 할당과 권한 할당

그림 6은 RBAC를 이용한 접근 제어 모델의 간단한 예이다.

Role Entities

Name	Description
R01	Unclassified
R02	Confidential
R03	Secret
R04	Top Secret

Services

R : Read
W : Write
U : Update
D : Delete
DL : DownLoad

Users

1 : Guest
2 : Member
3 : Admin

Access Policy

Name	Constraints
AP01-1	IF SL≥1 & User≥1 & 8:00≤Time≤18:00 THEN R
AP01-2	IF SL≥2 & User≥2THEN R
AP01-3	IF SL≥4 & User=3 THEN R
AP02-1	IF SL≥2 & User≥2 THEN DL
AP02-2	IF SL≥4 & User=3 THEN DL
AP03-1	IF SL≥3 & User≥2 THEN U
AP03-2	IF SL≥3 & User=3 THEN U
AP04-1	IF SL≥3 & User≥2 THEN D
AP04-2	IF SL≥4 & User=3 THEN D

Security Policy

Name	Constraints
SP01	**Utility Function** : $u(x_{att}, x_{auth}, x_{res}) = k_{att1}u(x_{att})+k_{auth1}u(x_{auth})+k_{res1}u(x_{res})$; **User's Preference** : uRiskProne=2^{2x}-1; uRiskNeutral=x; uRiskAverse=$log_2(x+1)$ **Constraints** : tType=PC/PDA/Cellphone;
SP03	**Utility Function** : $u(x_{att}, x_{auth}, x_{res}) = k_{att3}u(x_{att})+k_{auth3}u(x_{auth})+k_{res3}u(x_{res})$; **User's Preference** : uRiskProne=2^{2x}-1; uRiskNeutral=x; uRiskAverse=$log_2(x+1)$ **Constraints** : comp≥400MHz;nType≥200Kbps;tType=PC

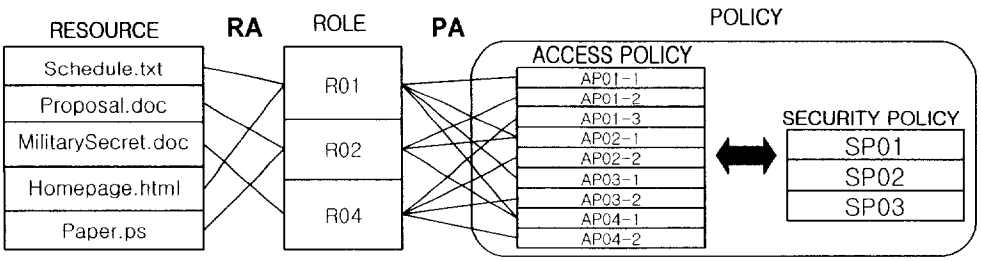


그림 6. RBAC를 이용한 접근 제어 모델의 간단한 예

그림 6에서 자원들 중에 "MilitarySecret.doc" 문서는 일급 기밀로 취급해야하는 군사 기밀이 포함된 문서이다. "MilitarySecret.doc" 문서에 "R04" 역할이 적용되었고 "R04"는 "AP01-3", "AP02-2", "AP03-2", "AP04-02" 접근정책을 포함하고 있다. 즉, 이것은 "MilitarySecret.doc"가 "AP01-3", "AP02-2", "AP03-2", "AP04-02"와 같은 제한된 접근정책만이 적용되었다는 것을 의미한다.

또한 가령 "MilitarySecret.doc" 문서의 특성이 일급 기밀에서 이급 기밀로 바뀐다면, 자원 할당에서 문서의 특성에 적절한 역할을 할당함으로 보안정책과 접근정책을 적용할 수 있다. 이와 같이 자원 할당과 권한 할당을 이용해 다양한 보안 요구사항에 따른 보안정책과 접근정책을 역할에 할당하고 보안정책과 접근정책이 할당된 역할을 자원에 할당함으로서 자원에 대한 권한의 관리를 쉽고 간단하고 업데이트 할 수 있다.

그리고 제안된 모델은 MAUT와 간결한 휴리스틱스에 기반한 보안정책과 접근정책을 활용한다. 따라서 보호된 자원을 위한 접근 권한은 동일한 접근정책이라도 다르게 결정된다. 예로서, "AP04-2" 접근정책의 경우에 사용자가 관리자일지라도 보안 등급(SL : Security Level)이 보다 낮다면 사용자는 자원에 접근 할 수 없다. 보안 등급은 본 논문에서 제안한 접근 제어 알고리즘에 의해 결정된다.

3.2. 컨텍스트 번역기와 컨텍스트 엔진

컨텍스트 번역기는 사용자와 서비스 제공자로부터 다양한 컨텍스트를 획

득하고, 획득한 컨텍스트를 0과 1사이 범위의 정량적인 값과 환경 변수로 변환한다. 변환된 환경변수 및 환산 값들은 보안 등급을 결정하기 위해 컨텍스트 엔진(Context Engine)에게 전달된다.

표 1은 환경 변수를 정량적인 값으로 환산한 예이다. 다음은 각 변수의 최선 값(x^*_i)과 최악 값(x^o_i)을 토대로 0 과 1 사이의 값으로 변환된 값이다. x_{att}는 사용될 암호 알고리즘의 보안강도, x_{auth}는 사용될 인증 기법, x_{res}는 사용자가 접근하려는 자원의 보호 수준을 나타낸다. x_{att}와 사용자 단말기의 성능에 따라서 사용자의 대기시간을 계산할 수 있다(암호 시스템을 깰 수 있는 시간: 단위 MIPS-Years).

표 1. 환경 변수의 유틸리티 환산표

변수 \ 값	0.2	0.5	0.8	1.0
x_{att}(보안강도)	$\geq 10^{0.5}$	$\geq 10^{3}$	$\geq 10^{7}$	$\geq 10^{11}$
x_{auth}(인증기법)	Password only	Certificate	Biometric	Hybrid
x_{res}(보호수준)	No	Low	Medium	High

컨텍스트 엔진은 컨텍스트, 역할, 보안정책, 적응적 접근 제어 알고리즘을 이용해서 적절한 보안 등급을 결정하게 된다.

우선 컨텍스트의 정보에 의해 자원에 적용된 보안정책을 결정하고 결정된 보안정책에 따라 제약 조건을 확인한 후 보안 등급 결정을 위해 사용될 변수, 사용자의 보안 선호도에 따른 유틸리티 함수 등을 결정하고, 적응적 접

근 제어 알고리즘을 이용해서 보안 등급을 결정한다. 그리고 결정된 보안 등급과 접근정책를 이용하여 자원에 대한 접근 허가 또는 거부를 결정한다. 그리고 결정된 보안등급에 따라 적용된 보안 서비스의 속성과 보안 등급 및 자원 접근 여부를 전달한다.

3.3. 적응적 접근 제어 알고리즘

적응적 보안 등급과 보호된 자원에 대한 접근의 유효성을 결정하기 위한 알고리즘은 다음과 같다.

```
AccessControl(AccessProblem)
// AccessProblem: Grant or deny access for the protected resources
    according to Access Policy(AP);
// Search Role that related Resource
search Role byusing context about User's Request
// Determine Security Level using Security Policy(SP)
SL = SecurityLevel(securityProblem);
// Grant or deny access by calculating Role, AP, and SP.
calculate Role, AP, and SP by using Constraints, Role, AP, and SP;
if true return grant;
else return deny;
```

그림 7. AccessControl 알고리즘

그림 7은 적응적 접근 제어 알고리즘을 나타낸 것이다. 우선 사용자의 서비

스 요청함에 따라 자원에 대한 접근에 의해 자원이 소속된 역할(Role)에 대한 정보를 획득하고, 역할에 할당된 보안정책과 접근정책을 확인한다. 그리고 보안정책의 제약, 유틸리티 함수, 사용자 선호도와 같은 정보를 이용해 보안 등급을 결정하게 된다. 그리고 결정된 보안 등급과 접근정책을 이용해 자원에 대한 접근 제어를 결정하게 된다.

```
SecurityLevel(securityProblem)
// Determining security level using Security Policy
   (constraint, utility function, user preference)
// Utilization of domain independent properties
calculate SL by I end;
if SL = 0 then return; SL // No security system
// Utilization of domain dependent properties
// select a strategy between MAUT and S. Heuristics
if MAUT then SL = MAUT(X);
if Simple Heuristics then SL = TakeTheBest(X);
return SL;
end;
```

그림 8. SecurityLevel 알고리즘

그림 8은 다양한 환경 변수에 따라 적응적으로 보안 등급을 결정하는 SecurityLevel 함수이다. 이 함수는 우선 영역에 독립적인 변수들을 이용해

서 보안 등급을 결정하게 되고, 결정된 보안 등급이 0 이라면 아무런 보안 시스템을 적용할 수 없는 등급이므로 0 등급을 반환한다. 여기서 보안 시스템이 요구하는 최소한의 요구 사항을 만족하는지 검사하게 된다. 요구사항을 만족한다면 영역 의존 변수인 보안정책을 이용해서 MAUT 함수와 TakeTheBest 함수를 선택하여 보안 등급을 결정하게 된다.

```
MAUT(X)
// Determine total utility function by the interaction
// with  the user according to MAUT
    u(x1,x2,,xn) = k1u1(x1)+k2u2(x2)+ +knun(xn)
// ki is a set of scaling constants
// xi is a domain dependent variable, where ui(x°i)=0,
// ui(x*i)=1, and ki is positive scaling const. for all i
ask the user's preference and decide ki;
for i = 1 to n
    do ui(xi) = GetUtilFunction(xi);
end;
return u(x1,x2,,xn);
end;
```

그림 9. MAUT 알고리즘

그림 9는 자원의 특성에 따라 정의된 환경 변수들을 고려하기 위해 MAUT를 이용해 보안 등급을 결정하는 MAUT 함수이다. 이 함수에서 결

정된 보안 등급을 이용해 3.6 장의 표 2, 표 3, 표 4의 보안 시스템 속성이 결정된다.

GetUtilFunction(x_i)

// Determine utility function due to users' preferences

// x_i is one of domain dependent variables

uRiskProne : user is risk prone for x_i // convex

uRiskNeutral : user is risk neutral for x_i // linear

uRiskAverse : user is risk averse for x_i //concave

x : arbitrary chosen from x_i

h : arbitrary chosen amount

$<x+h, x-h>$: lottery from x+h to x-h

// where the lottery (x^*, p, x^o) yields a p chance at x^*

// and a $(1-p)$ chance at xo

ask user to prefer $<x+h, x-h>$ or x; // interaction

if user prefer $<x+h, x-h>$ **then**

  return uRiskProne; // e.g. $u = b(2^{cx}-1)$

else if user prefer x **then**

  return uRiskAverse; // e.g. $u = b\log_2(x+1)$

else

  return uRiskNeutral;

end; // e.g. $u = b$

그림 10. GetUtilFunction 알고리즘

그림 10는 MAUT 함수에서 사용자의 보안 선호도에 따라 유틸리티 함수를 결정하는 GetUtilFunction 함수이다.

TakeTheBest($u(x_1,x_2,,x_n)$)
// Take the best, ignore the rest
$u(x_1,x_2,,x_n)$: user's basic preferences
// if the most important preference is xi, then only xi
// is considered to calculate SL
// The other properties except xi are ignored
$u(x_1,x_2,,x_n)$ is **calculatedby** only considering x_i;
SL is **calculatedby**the value of $u(x_1,x_2,..,x_n)$;
return SL;
end;

그림 11. TakeTheBest 알고리즘

그림 11은 간결한 휴리스틱스를 이용하여 보안 등급을 결정하는 TakeTheBest 함수이다.

3.4. 환경과 사용자

환경은 사용자의 주변 환경을 의미한다. 즉 환경은 컨텍스트가 도처에 편재한 환경을 의미하고 사용자는 휴대폰에서 PDA, 고성능 PC에 이르기까지 유선망을 비롯하여 무선망을 기반으로 한 다양한 사용자를 나타낸다.

유비쿼터스 환경 내에서 다양한 특성을 가진 사용자는 특정 자원에 대한 서비스를 제공받기 위해 서비스 제공자에게 특정 서비스 요청을 하고, 사용자에 대한 컨텍스트(네트워크 타입, 사용자의 위치, 디바이스의 성능, 요청된 자원의 중요도 등)를 제안 모델 내의 컨텍스트 번역기에게 제공한다.

3.5. 서비스 제공자

서비스 제공자는 유무선 인터넷에 기반을 둔 응용서비스인 증권 거래, 계좌이체, 주문 등 다양한 서비스 제공 시 통신정보에 대한 보안기능을 제공하는 애플리케이션이다.

이들은 특정 서비스를 제공하기 위해 소유한 자원을 사용자들에게 제공을 하고 제공되는 자원을 안전하게 관리하기 위해서 자원의 개별적인 환경 요소(서비스의 유형 및 중요도, 시스템의 현재 상태 등)에 따른 보안정책과 접근정책을 적용한다.

그리고 다양한 사용자에게 안전한 서비스를 제공하고 효율적인 보안정책을 제공하기 위해 보안정책 관리 모델에서 사용자와 서비스 제공자의 컨텍스트를 접근 제어 관리 모델 내의 컨텍스트 번역기에게 제공한다.

3.6. 보안 서비스

제안 모델은 유비쿼터스 환경에서 다양한 환경 변수들의 동적인 변화에 적응하기 위한 적응적 보안 등급을 결정한다. 그리고 보안 등급을 바탕으로 하여 결제 시스템의 암호알고리즘의 종류, 키 길이, 인증 기법과 프로토콜 타입 등과 같은 속성들을 적절히 조정한다.

다음은 제안 모델의 수학적 모델이다.

$$U = \sum_{i=1}^{n} k_i u_i(x_i), (o \le U \le 1)$$
$$SL = [U^* 10]/2, (SL = 0, 1 \ldots 5)$$
$$P_{SL} = \{p_0, p_1, \ldots, p_5\}, p_i = \{S_i, A_l, R_m\}$$

U는 전체 유틸리티 값이고, u_i는 다양한 환경변수 (x_i)들을 유틸리티 값으로 변환한 값이며, k_i 는 변수들의 가중치로서 보안정책과 사용자의 보안선호도에 따라서 결정된다. SL은 0에서 5까지의 숫자로 보안등급을 나타내며 값이 0인 경우는 보안시스템을 사용할 수 없는 경우이다. p_i는 보안등급에 따라서 결정되는 보안시스템의 속성 값, S_j는 암호알고리즘 종류, A_l 은 인증기법 종류, R_m 은 프로토콜 유형을 나타낸다.

표 2. 인증기법의 종류(A_l)

A_m	인증 기법
A_0	Password based only
A_1	Certificate based
A_2	Biometric based
A_3	Hybird methods

표 3. 프로토콜 유형(R_m)

R_m	프로토콜
R_0	SPKI
R_1	Wireless PKI
R_2	PKI

표 4. 암호알고리즘들의 종류(S_j)

S_j	대칭암호-키길이	공개키암호-키길이	MAC
S_1	DES	RSA-512	MD5
S_2	SEED	RSA-512	MD5
S_3	3DES	RSA-768	SHA1
S_4	AES-128	RSA-1024	SHA1
S_5	AES-192	RSA-1024	SHA1

p_i는 위 표와 같은 다양한 보안 속성 (S_j, A_l, R_m) 들의 조합으로 이루어지며 이러한 조합은 시스템의 보안정책에 의해서 결정된다. 보안모델에서는 환경변수들의 변화를 지속적으로 감시하며 변수들의 값이 임계치보다 더 크게 변화한 경우에는 보안등급을 재조정하여 보안모델의 속성들을 변화시킨다.

4. 사례 연구 및 구현

4.1. 사례 연구

사용자는 Service Provider에게 보호된 자원 'MilitarySecret.doc'를 '읽기'를 요청한다. 사용자의 요청을 받은 Service Provider는 네트워크 타입, 사용자의 위치, 디바이스의 성능, 요청된 자원의 중요도 등과 같은 환경 요소의 컨텍스트를 제안 모델의 Context Interpreter에게 전달한다. 컨텍스트를 전달 받은 Context Interpreter는 획득한 컨텍스트를 정량적인 값으로 환산하고 적응적 보안 등급을 결정하기 위해 Context Engine에게 전달한다.

가령 3.1.2장의 그림 5와 같은 경우에는 'MilitarySecret.doc' 자원에 적용된 역할이 R04 임을 확인 할 수 있고, R04에 대한 Security Policy와 Access Policy도 확인 할 수 있다. 그림 5의 경우 'MilitarySecret.doc'에 적용된 보안정책은 다음과 같다.

표 5. 'MilitarySecret.doc' 적용된 보안정책의 예

Name	Constraints
SP04	**Utility Function:** $u(x_{att}, x_{auth}, x_{res}) = k_{att}u(x_{att})+k_{auth}u(x_{auth})+k_{res}u(x_{res})$;
	User's Preference: uRiskProne=2^{2x} 1;uRiskNeutral=x; uRiskAverse=$\log_2(x+1)$
	Constraints comp≥200MHz; nType≥100Kbps; tType=PC/PDA/Cellphone;

표 5는 3.1.2장의 그림 5에서 'MilitarySecret.doc' 자원이 소속된 R04 에

할당된 보안정책이다. 표 5에서는 'MilitarySecuret.doc'를 사용하기 위해서는 일정한 CPU 성능, 네트워크 전송속도, 암호 알고리즘의 강도를 요구하고, 알고리즘의 보안강도(X_{att}), 인증기법(X_{auth}), 자원의 보호수준(X_{res})등을 환경 변수로 사용한다는 것을 의미한다. 이러한 환경 변수와 적응적 접근 제어 알고리즘을 이용해 보안등급을 결정하기 위해 각 환경 변수를 표 6과 같이 정량적인 값으로 환산하고, 가중치 k_i를 결정하기 위해 정성적인 질문을 한다.

표 6. 환경 변수 유틸리티 환산표

변수 / 값	0.2	0.5	0.8	1.0
x_{att}(보안강도)	$\geq 10^{0.5}$	$\geq 10^{3}$	$\geq 10^{7}$	$\geq 10^{11}$
x_{auth}(인증기법)	Password only	Certificate	Biometric	Hybrid
x_{res}(보호수준)	No	Low	Medium	High

가령 x^*_{auth}와 x^*_{res}보다 x^*_{att}을 더 선호하면 $k_{att} > k_{auth} + k_{res}$, $k_{att} > .5$이다. 또한 x^o_{res}에서 x^*_{res}로 되는 것 보다 x^o_{auth}에서 x^*_{auth}로 되는 것을 선호하면 $k_{auth} > k_{res}$이다. 만약 $k_{att} = .6$으로 평가되었다면 의사결정자는 $(x^*_{att}, x^o_{auth}, x^o_{res})$과 제비뽑기$<(x^*_{att}, x^*_{auth}, x^*_{res}), 6, (x^o_{atth}, x^o_{auth}, x^o_{res})>$ 사이의 어떤 결정도 무관하다는 것을 의미한다. 제비뽑기$<(x^*_{att}, x^*_{auth}, x^*_{res}), 6, (x^o_{att}, x^o_{auth}, x^o_{res})>$은 $(x^*_{att}, x^*_{auth}, x^*_{res})$일 확률 .6 과 $(x^o_{att}, x^o_{auth}, x^o_{res})$일 확률 .4 를 의미한다. k_{att} 이 .6 이므로 $k_{auth} + k_{res} = .4$ 이다. 이제 의사결정자가 $(x^o_{att}, x^*_{auth}, x^o_{res})$와 $<(x^o_{att}, x^*_{auth}, x^*_{res}), p, (x^o_{att}, x^o_{auth}, x^o_{res})>$의 선택을 무관하게 할 수 있는 확률 p를 질의 한다. 만약 의사 결정자의 답이 .7 이라면 공식

$k_{auth} = p(k_{auth} + k_{res})$[9]에 의해서 $k_{auth} = .28$이 된다. 그리고 $u_i(x_i)$를 결정하기 위해서 제비뽑기 $<x+h, x-h>$와 기대결과 x의 선호도를 질의한다. 만약 x를 선호하면 유틸리티 함수는 모험 회피이며 각 $u_i(x_i)$는 $b\log_2(x_i+1)$의 형태가 된다.

즉, $u(x_{att},x_{auth},x_{res}) = .6\log_2(x_{att}+1) + .28\log_2(x_{auth}+1) + .12\log_2(x_{res}+1)$ 이 되고, 계산된 결과 값에 따라 아래와 같이 보안등급을 결정하고 표 2, 3, 4 과 같이 보안속성이 결정된다.

가령 보안강도가 $10^{0.5}$, 인증기법이 Biometric, 보호수준이 low라면,

$$u(x_{att}, x_{aut}, x_{res}) = .6\log_2(.2+1) + .28\log_2(.8+1) + .12\log_2(.5+1)$$
$$= (.6 \times 0.263 + .2 \times .849 + .12 \times 0.585 = 0.46572$$

이므로 보안등급은 3 등급으로 결정된다.

그리고 'MilitarySecret.doc' 자원에 대한 접근의 허가 또는 거부는 보안정책에 따라 결정된다. 표 7은 3.1.2장의 그림 6에서 'MilitarySecret.doc' 자원이 소속된 R04에 할당된 접근정책의 예이다. 표 7에 따르면 자원을 읽기 위해서는 보안 등급이 4이상, 사용자가 3 (members)이상의 요구조건을 만족해야 한다.

표 7. 'MilitarySecret.doc' 적용된 접근정책의 예

Name	Constraints
AP01-3	IF SL≥4 & User=3 THEN R
AP02-2	IF SL≥4 & User=3 THEN DL
AP03-2	IF SL≥3 & User=3 THEN U
AP04-2	IF SL≥4 & User=3 THEN D

이와 같이 제안모델은 서비스 제공자나 이용자의 상황정보가 고려되지 않는 기존의 보안 서비스와는 달리 사용자들이 원하는 정보나 거래 정보의 민감도, 인증기법, 보호수준 등과 같은 다양한 환경요소의 상황정보를 고려하여 보안 등급이 동적으로 결정됨으로 자원의 동적인 변화에 따라 적절한 보안 서비스를 제공 할 수 있다.

4.2. 구현 및 평가

제안 시스템의 가용성을 실험하기 위해 Window XP를 운영체제로 펜티엄급 PC에서 구현하였다. 각 구성 객체들의 모듈을 작성하였으며, HTTP 프로토콜과 Socket을 이용하여 통신한다. 각 객체는 j2sdk1.4.2_06, Apache-Tomcat 4.0, Mysql-4.0.18-nt, JDBC(mysql-connector-java-3.0.10)을 사용하여 구현하였다.

제안 모델은 그림 12와 같이 Role DB, Security Policy DB, Access Policy DB를 포함한 Databases와 Context Engine, Context Interpreter를 포함한Access Control Algorithm으로 구성되었다.

Databases는 RBAC를 이용하여 자원과 정책의 관계를 정의하고 역할에 따른 보안정책과 접근정책에 대한 정보를 제공한다.

Access Control Algorithm은 획득된 컨텍스트와 보안정책을 이용하여 적응적인 보안등급을 결정한다. Context Engine은 접근정책과 보안등급을 이용하여 자원에 대한 접근 여부를 결정하고, 보안등급에 따라 적절한 보안 서비스를 제공한다. 또한 자원의 보안 설정을 위해 자원의 특성과 보안요구사항에 따라 역할을 할당 또는 변경한다.

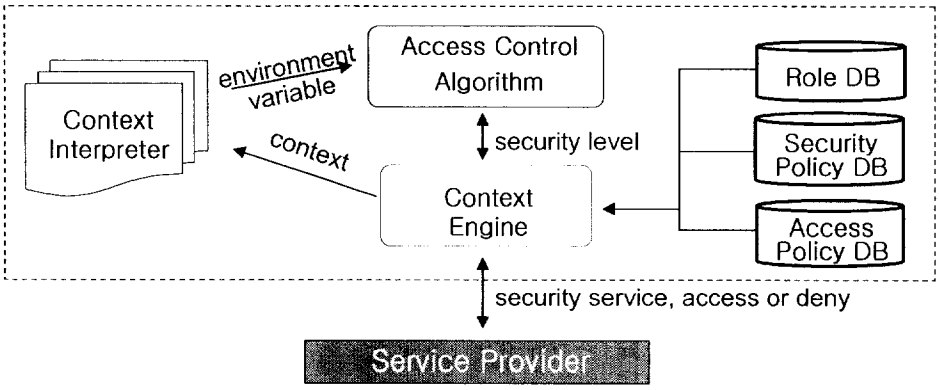


그림 12. 제안 모델의 구성

제안 모델에서 RBAC의 개념을 이용하기 위해 데이터베이스를 그림 14와 같이 설계하였다. resource_assignment는 자원과 역할의 관계를 나타내고, policy_assignment는 역할과 보안정책/접근정책 간의 관계를 나타내고 있다.

이와 같이 제안 모델에서는 수많은 자원의 보안정책과 접근정책을 개별적

으로 설정하지 않고 자원의 특성과 보안요구사항에 따라 분류된 역할만을 할당함으로서 어렵고 복잡한 보안 관리 과정을 간결하게 처리 할 수 있다.

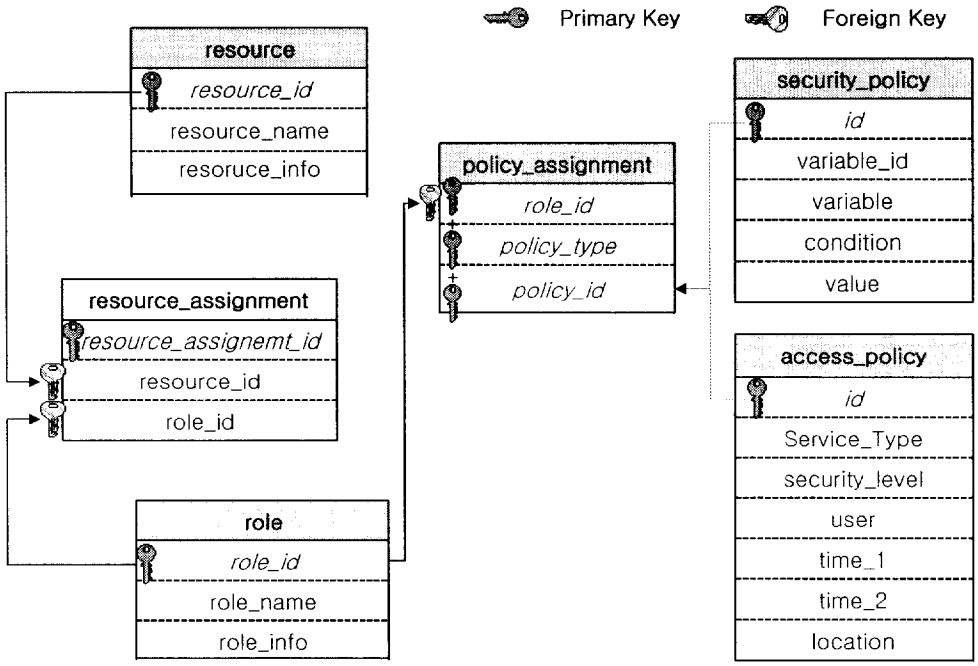


그림 13. 데이터베이스 구조도

그림 14는 제안 모델의 클래스다이어그램이다.

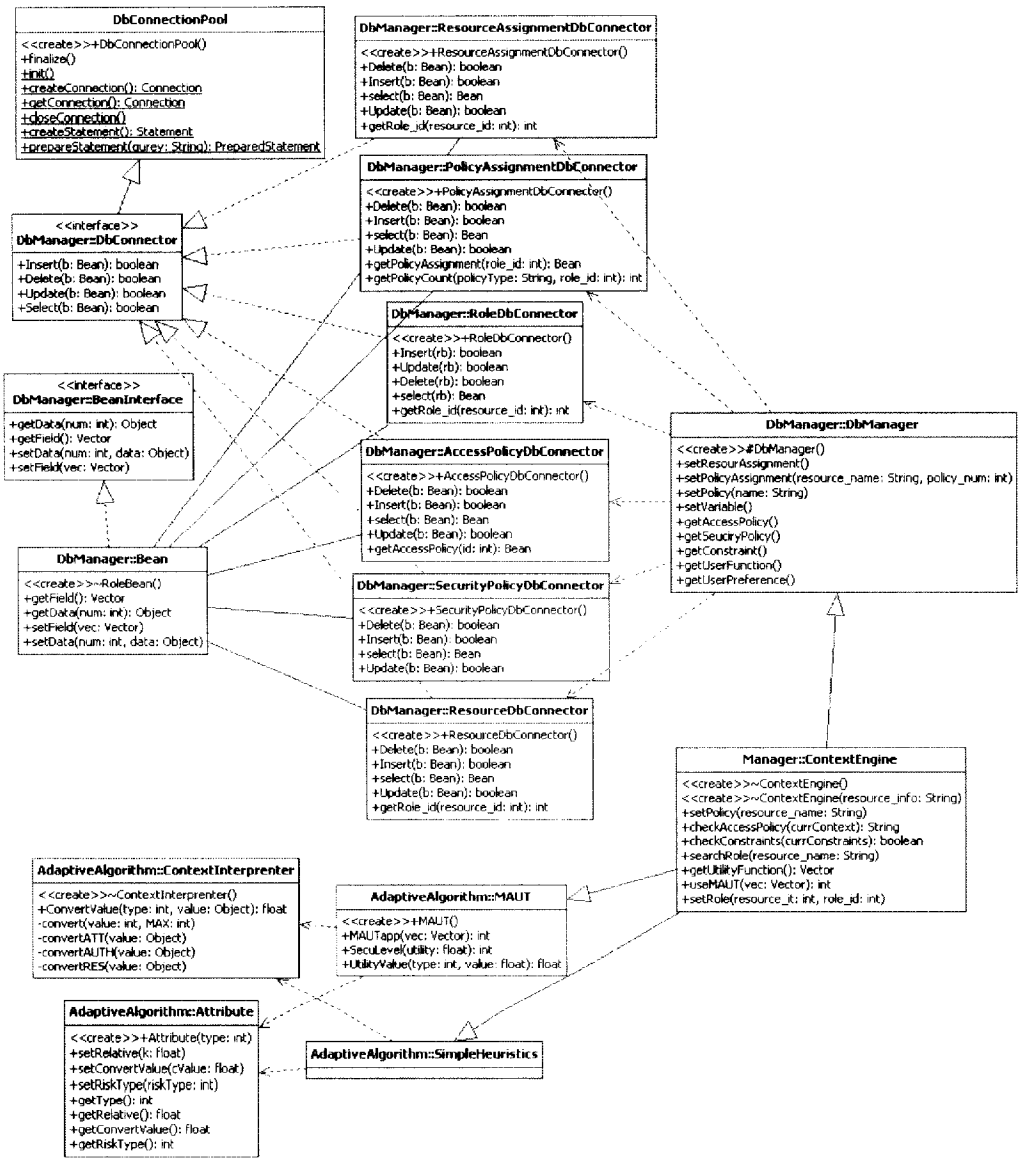


그림 14. 제안 모델의 클래스다이어그램

제시한 모델의 가용성을 실험하기 위해 표 8과 같이 동적으로 결정된 사용자가 있다고 가정하였고 이에 따른 유틸리티 결과 값은 그림 15와 같다.

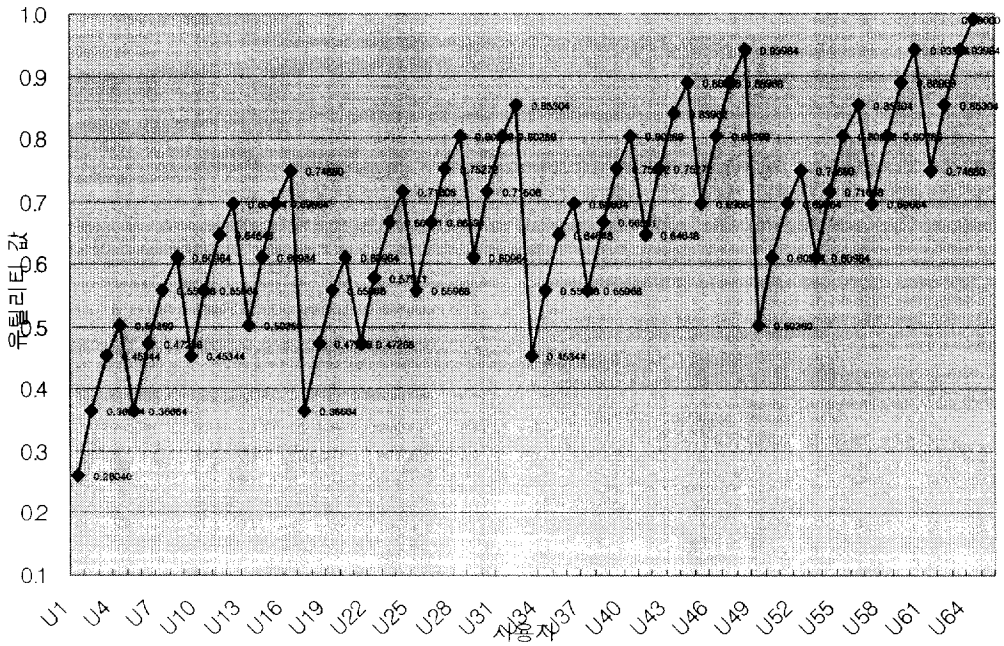


그림 15. 유틸리티 결과 값

그림 15에서 보안 등급을 결정하는 유틸리티 값은 각기 다른 사용자의 환경 요소에 따라 동적으로 결정됨을 알 수 있다. 즉, 각 사용자의 환경요소를 정량적으로 고려함으로서 유틸리티 값이 사용자의 컨텍스트에 따라 적응적으로 결정됨을 의미한다.

이와 같이 제안 모델은 동일한 보안정책이라도 사용자의 컨텍스트에 따라 보안등급을 결정하는 유틸리티 결과 값이 적응적으로 결정되므로 자원에 대한 접근정책이 동적으로 적용됨을 알 수 있다. 따라서 제안모델은 자원의 동적인 변화에 따라 적절한 보안 서비스를 제공 할 수 있다.

이와 같이 다양한 환경 변수의 값을 정량화하여 정량적 의사 결정 이론인 MAUT와 간결한 휴리스틱스를 사용함으로서 기존의 정적인 환경에서 해결하지 못했던 적응적 보안 서비스 사용의 어려움을 해결할 수 있을 것으로 예상한다. 즉, 기존의 정적인 보안 서비스 시스템에서는 다중의 환경 변수 중에서 특정 변수들의 동적인 변화를 적시에 반영할 수 없었기 때문에(정적으로만 반영) 자원의 효율적 활용이 어려웠지만 본 논문에서 제시하는 컨텍스트-기반 적응적 접근 제어 관리 모델에서는 이들 문제점을 효과적으로 해결 할 수 있을 것으로 기대한다.

또한 사용자의 환경에 따라 동적으로 적절한 보안등급이 결정되고 그에 따른 보안서비스를 제공받기 때문에 기존의 정적인 보안서비스를 이용함으로 열악한 환경의 사용자에게 무리한 시스템 자원이나 장기간의 대기시간을 요구하는 문제를 해결할 수 있을 뿐만 아니라 자원의 특성에 따른 접근정책으로 인해 악의를 가진 사용자로부터 자원을 안전하게 보호할 수 있을 것이다.

표 8. 사용자의 환경 정보

	X_{att} 보안강도	X_{auth} 인증기법	X_{res} 보호수준		X_{att} 보안강도	X_{auth} 인증기법	X_{res} 보호수준
U1	$10^{0.5}$	Password only	No	**U33**	10^{7}	Password only	No
U2	$10^{0.5}$	Password only	Low	**U34**	10^{7}	Password only	Low
U3	$10^{0.5}$	Password only	Medium	**U35**	10^{7}	Password only	Medium
U4	$10^{0.5}$	Password only	High	**U36**	10^{7}	Password only	High
U5	$10^{0.5}$	Certificate	No	**U37**	10^{7}	Certificate	No
U6	$10^{0.5}$	Certificate	Low	**U38**	10^{7}	Certificate	Low
U7	$10^{0.5}$	Certificate	Medium	**U39**	10^{7}	Certificate	Medium
U8	$10^{0.5}$	Certificate	High	**U40**	10^{7}	Certificate	High
U9	$10^{0.5}$	Biometric	No	**U41**	10^{7}	Biometric	No
U10	$10^{0.5}$	Biometric	Low	**U42**	10^{7}	Biometric	Low
U11	$10^{0.5}$	Biometric	Medium	**U43**	10^{7}	Biometric	Medium
U12	$10^{0.5}$	Biometric	High	**U44**	10^{7}	Biometric	High
U13	$10^{0.5}$	Hybrid	No	**U45**	10^{7}	Hybrid	No
U14	$10^{0.5}$	Hybrid	Low	**U46**	10^{7}	Hybrid	Low
U15	$10^{0.5}$	Hybrid	Medium	**U47**	10^{7}	Hybrid	Medium
U16	$10^{0.5}$	Hybrid	High	**U48**	10^{7}	Hybrid	High
U17	10^{3}	Password only	No	**U49**	10^{11}	Password only	No
U18	10^{3}	Password only	Low	**U50**	10^{11}	Password only	Low
U19	10^{3}	Password only	Medium	**U51**	10^{11}	Password only	Medium
U20	10^{3}	Password only	High	**U52**	10^{11}	Password only	High
U21	10^{3}	Certificate	No	**U53**	10^{11}	Certificate	No
U22	10^{3}	Certificate	Low	**U54**	10^{11}	Certificate	Low
U23	10^{3}	Certificate	Medium	**U55**	10^{11}	Certificate	Medium
U24	10^{3}	Certificate	High	**U56**	10^{11}	Certificate	High
U25	10^{3}	Biometric	No	**U57**	10^{11}	Biometric	No
U26	10^{3}	Biometric	Low	**U58**	10^{11}	Biometric	Low
U27	10^{3}	Biometric	Medium	**U59**	10^{11}	Biometric	Medium
U28	10^{3}	Biometric	High	**U60**	10^{11}	Biometric	High
U29	10^{3}	Hybrid	No	**U61**	10^{11}	Hybrid	No
U30	10^{3}	Hybrid	Low	**U62**	10^{11}	Hybrid	Low
U31	10^{3}	Hybrid	Medium	**U63**	10^{11}	Hybrid	Medium
U32	10^{3}	Hybrid	High	**U64**	10^{11}	Hybrid	High

5. 결론

현재의 보안 서비스는 특정 환경 요소를 정적으로만 반영하고 있기 때문에 자원의 동적인 변화를 적절하게 반영할 수 없을 뿐만 아니라 많은 양의 자원들을 효율적 관리하기가 어려운 문제점을 가지고 있다.

따라서 본 논문에서는 이들의 문제점을 해결하기 위해서 정량적 의사 결정 이론인 MAUT와 간결한 휴리스틱스를 사용하여 다양한 환경 요소를 고려함으로서 기존의 시스템이 동적인 변화에 적응적으로 대응할 수 없었던 문제점을 해결하고 다양한 자원에 대해 효율적인 보안정책 관리에 대해 기술 하였다.

또한 제안 모델에 역할 기반 접근(RBAC : Role Base Access Control) 모델의 개념을 적용하여 동적인 변화를 가진 환경요소를 지닌 다양한 자원들이 공존하는 유비쿼터스 환경에서 사용자나 애플리케이션이 보안정책 결정을 위한 세부 사항을 개별적으로 모두 설정하고 관리하는 것은 복잡하고 많은 부담이 따르는 문제를 해결할 수 있었다.

앞으로 도래할 것으로 예상되는 유비쿼터스 환경에서는 다양한 자원들이 다양한 특성을 지닌 채 공존하고 자원의 환경 요소가 동적으로 변하기 때문에 보안정책의 설정과 변경이 쉽고 변경된 보안정책이 잘 반영 될 수 있고 동적으로 변하는 자원의 컨텍스트에 적절하게 대응할 수 있는 적응적인 보안 서비스를 제공하는 제안 모델이 필요할 것이다.

향후 연구 과제로서는 보다 많은 환경 변수들을 이용하여 효율적인 보안 정책을 적용하고 사용자의 요구사항을 다 각도로 반영하는 MAUT에 대한 연구와 컨텍스트 정보에 따른 정량적 모델 개발과 제안 모델을 실제 환경에서 실험해 보는 것이 필요하다.

참고문헌

[1] Mark Weiser and John Seely Brown, THE COMING AGE OF CALM TECHNOLOGY, Xerox PARC, October 5, 1996.

[2] M.Weiser, http://www.ubiq.com/weiser

[3] Guanling Chen, "A survey of context-aware mobile computing research", Dartmouth Univ.TR2000-38.

[4] A. Dey., "Providing Architectural Support for Building Context-Aware Applications," Ph. D. Dissertation, Georgia Institute of Technology, 2000.

[5] 윤정로, 최장욱 역, 유비쿼터스, 21세기북스, 2003.

[6] D. Saha and A. Mukherjee, "Pervasive computing: A New Paradigm for Computing in 21st Century," IEEE Computer, Vol. 36, No. 3, 2003, pp. 25-31.

[7] R. Mohan et al., "An Editor for Adaptive XML-Based Policy Management of IPSec," In Proceedings of the 19th Annual Computer Security Applications Conference(ACSAC2003), 2003.

[8] Blaze, M et al., "The KeyNote trust management system Version 2, (RFC2704, Network Working Group), Sept. 1999. http://www.ietf.org/rfc/rfc2704.txt

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

[10] R. Schfer, "Rules for Using Multi-Attribute Utility Theory for Estimating a User's Interests," In Proceedings of the ninth GI-Workshop. ABIS-Adaptivitt und Benutzermodellierung in interaktiven software systemen, Dortmund, Germany, 2001.

[11] Mokdong Chung and Vasant Honavar, "A Negotiation Model in Agent-mediated Electronic Commerce," In Proceedings of the IEEE International Symposium on Multimedia Software Engineering, Taipei, Dec. 2000, pp. 403-410.

[12] G.Gigerenzer et al., Simple Hueristics That Make Us Smart, Oxford University Press, New York, 1999.

[13] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E.Youman., "Role based access control models," IEEE Computer, Vol. 29, No. 2, February 1996, pp. 38 - 47.

[14] http://csrc.nist.gov/rbac/, NIST

[15] Bill Schilit, Norman Adams, and Roy Want. Context-aware computing applications. In Proceedings of IEEE Workshop on Mobile Computing Systems and Application, page 85~90, Santa Cruz, California, December 1994. IEEE Computer Socienty Press.

[16] http://www.cc.gatech.edu/fac/Gregory.Abowd/

[17] R. Grimm., "A system architecture for pervasive computing," ACM SIGOPS European Workshop.

[18] Ghita Kouadri Mostefaoui and Patrick Brezillon. : A generic framework for context-based distributed authorizations. Fourth

International and Interdisciplinary Conference on Modeling and Using Context (Context'03). LNAI 2680, Springer Verlag. pp. 204-217.

[19] http://www.warentest.de/

[20] 김환조, 서정철, 정목동, "Design and Implementation of a Content Encryption Module Using Adaptive Security Level," 멀티미디어학회 학술 발표 논문집, 6권, 2호,2003, pp.65-68.

[21] 서정철, 채종우 ,정목동, "Context-Based Security Policy Management Model Using Adaptive Security Level," 한국정보과학회 31회 춘계학술 발표논문집, 2004, pp.268-285.

[22] Jungchul Seo, Jongwoo Chae, and Mokdong Chung , "Context-Based Adaptive Security Policy Management Model, " PARA'04 Workshop on STATE-OF-THE-ART IN SCIENTIFIC COMPUTING, Denmark, 2004.