Journal of Korea Multimedia Society Vol. 13, No. 1, January 2010(pp. 133-142)

상황인식 보안 서비스를 이용한 개선된 접근제어

양석환[†], 정목동[††]

요 약

유비쿼터스 기술의 보편화에 따라 유비쿼터스 환경의 보안 취약성을 해결하기 위한 보안기술의 연구가 주목받고 있다. 그러나 현재의 대다수 보안 시스템은 고정된 규칙을 기반으로 하는 것으로서, 유비쿼터스 기반 사용자의 다양한 상황에 제대로 대응하지 못하는 문제점이 있다. 또한 기존의 상황인식 보안 연구는 ACL (Access Control List) 혹은 RBAC (Role-Based Access Control) 계열의 연구가 많이 수행되고 있으나 보안정책의 관리에 대한 오버헤드가 크고, 또한 예상하지 못한 상황에 대한 대응이 어렵다는 문제점을 보이고 있다. 이에 본 논문에서는 FCM (Fuzzy C-Means) 클러스터링 알고리즘과 퍼지 결정트리를 이용하여 다양한 상황을 인식하고 적절한 보안기능을 제공하는 상황인식 보안 서비스를 제안한다. 제안 모델은 기존의 RBAC 계열의 시스템이 가진 고정 규칙에 따른 문제나 충돌 문제, 관리상의 오버헤드를 개선할 수 있음을 확인할 수 있다. 제안 모델은 헬쓰케어 시스템이나 응급구호 시스템 등 상황 인식을 통하여 사용자의 상황에 적합한 서비스를 제공하는 다양한 애플리케이션에 응용 가능할 것으로 기대된다.

Improved Access Control using Context-Aware Security Service

Seokhwan Yang[†], Mokdong Chung[††]

ABSTRACT

As the ubiquitous technology has penetrated into almost every aspect of modern life, the research of the security technology to solve the weakness of security in the ubiquitous environment is received much attention. Because, however, today's security systems are usually based on the fixed rules, many security systems can not handle diverse situations in the ubiquitous environment appropriately. Although many existing researches on context aware security service are based on ACL (Access Control List) or RBAC (Role Based Access Control), they have an overhead in the management of security policy and can not manipulate unexpected situations. Therefore, in this paper, we propose a context-aware security service providing multiple authentications and authorization from a security level which is decided dynamically in a context-aware environment using FCM (Fuzzy C-Means) clustering algorithm and Fuzzy Decision Tree. We show proposed model can solve typical conflict problems of RBAC system due to the fixed rules and improve overhead problem in the security policy management. We expect to apply the proposed model to the various applications using contextual information of the user such as healthcare system, rescue systems, and so on.

Key words: Context-aware Security (상황인식 정보 보안), RBAC (Role Based Access Control: 역할 기반 접근제어), FCM (Fuzzy C-Means: 퍼지 클러스터링 알고리즘), Fuzzy Decision Tree (퍼지 결정트리)

※ 교신저자(Corresponding Author) : 정목동, 주소 : 부산광역시 남구 대연3동 599-1(608-737), 전화 : 051)629-6253, FAX : 051)629-6210, E-mail : mdchung@pknu.ac.kr
접수일 : 2009년 10월 21일, 수정일 : 2009년 12월 18일
완료일 : 2009년 12월 21일

[†] 준회원, 부경대학교 정보보호학 협동과정
(E-mail : tigergal@chol.com)
[††] 종신회원, 부경대학교 컴퓨터공학과 교수
※ 이 논문은 2007학년도 부경대학교의 지원을 받아 수행된 연구임(PK-2008-0012000200711600).

1. 서 론

최근 확산되고 있는 유비쿼터스 환경 구축은 개인 정보 유출 및 다양한 보안문제를 발생시켰고, 이에 따라 유비쿼터스 환경에서의 보안기술 연구가 점차 주목받고 있다. 예를 들면, 유비쿼터스 헬쓰케어 환경 구축의 기반을 이루는 센서 네트워크는 온도, 습도, 조도, 영상 및 사용자의 이동상황, 건강상태와 같은 정보를 시스템에 제공하는 다양한 센서들로 구성되어 있으며, 이러한 센서들이 시스템에 제공하는 사용자의 주위환경 및 상황에 대한 정보는 사용자의 프라이버시 침해 문제를 일으킬 가능성이 크다. 따라서 이러한 정보의 접근에 대하여 강력한 보안기능을 제공할 필요가 있다. 그러나 모든 상황에서 강력한 보안기술을 적용하는 것은 오히려 시스템의 효율성 저하와 함께 사용자의 불편을 가중시킬 수 있으며, 특히 응급구호 시스템과 같은 긴급 상황 시에는 보안보다 사용자의 생명을 보호하는 일을 우선적으로 고려해야 하는 시스템도 존재한다.

이에 본 논문에서는 FCM (Fuzzy C-Means) 클러스터링[1]과 다변량 퍼지결정트리 (Multivariate Fuzzy Decision Tree)[2,3]를 이용하여 센서의 정보를 분류함으로써 사용자의 상황을 인식하고, 사용자가 처한 상황에 따라 다양한 수준의 보안기술을 유연하게 적용할 수 있는 상황인식 보안 서비스를 제안한다.

본 논문의 구성은 다음과 같다. 2절에서 관련 연구에 대하여 살펴보고, 3절에서 FCM 클러스터링과 다변량 퍼지결정트리를 이용한 상황인식 보안 서비스 모델을 소개한다. 4절에서는 제안한 상황인식 보안 서비스 모델을 구현하고 실험한 결과 분석을 다루고, 5절에서 결론 및 향후 연구 방향을 제시한다.

2. 관련연구

2.1 상황 인식 기반 접근제어

상황인식에 관한 연구는 마크 와이저의 유비쿼터스 컴퓨팅 개념이 제시된 이후로 많은 연구가 진행되어 왔다. 상황인식 기술을 보안에 적용한 대표적인 예로서 Illinois 대학에서 수행하고 있는 Gaia[4] 프로젝트의 Cerberus와 Georgia Tech에서 제안한 CASA (Context-Aware Security Architecture)[5] 등을 들 수 있다.

Cerberus는 ACL (Access Control List)을 기반으로 접근제어를 수행한다. ACL은 전통적인 접근제어 정책 모델로서 간단한 정책의 구성이 가능하지만 데이터 추상화 기능을 제공하지 않기 때문에 보안 서비스를 제공하고자 하는 조직의 권한 및 책임 구조를 보안 정책에 적용하기 어렵다.

CASA는 GRBAC (Generalized Role-Based Access Control)[6,7] 모델을 기반으로 접근제어를 수행하므로 사용자, 객체, 환경정보 등을 역할로 추상화하여 보안 정책 관리기능을 제공한다. 그러나 GRBAC는 RBAC[8]가 제공하는 권한 추상화를 제공하지 않으며, 관리 도메인 요소들이 많아짐에 따라서 관리해야 할 역할의 양이 많아진다. 또한 객체 역할과 환경 역할 간의 중복되는 영역에 의해 발생되는 충돌 문제로 인해 보안정책 관리 및 구성에 따르는 오버헤드가 많이 발생하게 되며, 보안정책의 설정 여부에 따라 예상하지 못한 상황, 즉 보안 정책에 등록되지 않은 상황에 대한 대응이 어렵다는 단점을 가진다.

현재 수행되고 있는 상황인식 보안연구는 Cerberus 및 CASA와 같이 ACL, GRBAC 등을 적용하고 있는 경우가 많으며, Cerberus 및 CASA와 동일한 문제에 노출되어 있다. 따라서 이러한 문제점을 해결할 수 있는 상황인식 보안 서비스에 대한 연구가 요구된다. 표 1은 Cerberus와 CASA의 비교 내용을 보여준다[7].

표 1. Cerberus와 CASA의 비교

분류	기준	Cerberus [5]	CASA [6]
사용자 인증	인증 신뢰도 관리	가능	가능
	인증 신뢰 산출 공식	없음	없음
	보안 등급 속성	미적용	미적용
접근 제어	접근 제어 모델	ACL	GRBAC
	권한 할당	사용자	역할
	데이터 추상화	미제공	제공(사용자, 객체, 환경정보)
	조직 구조 반영	미반영	가능
	정책 구성 오버헤드	적음	도메인 수에 따라 증가
	정보의 기밀성 유지	불가	불가

2.2 FCM 클러스터링

FCM (Fuzzy C-Means)[1]은 하나의 클러스터에 속해있는 각각의 데이터 점을 소속정도에 의해서 분류하는 데이터 분류 알고리즘이다. FCM 클러스터링은 퍼지 분할 기법을 사용하며 소속 함수 U는 0과 1사이의 값을 가지는 요소들을 가진다. 데이터 집합에 대한 소속정도 값의 합은 항상 1이다.

$$\sum_{i=1}^{c} u_{ik} = 1,\ \forall k = 1, \cdots, n \quad 0 < \sum_{k=1}^{n} u_{ik} < n$$

FCM 클러스터링에 대한 비용함수는 다음과 같은 형태를 가진다[9].

$$J(u_{ik}, v_i) = \sum_{i=1}^{c}\sum_{k=1}^{n} u_{ik}^{m}(d_{ik})^2$$

$$v_i = \{v_{i1}, v_{i2}, \cdots, v_{ij}, \cdots, v_{iL}\}$$

$$d_{ik} = d(x_k - v_i) = \left[\sum_{j=1}^{1}(x_{kj} - v_{ij})^2\right]^{\frac{1}{2}}$$

$$v_{ij} = \frac{\sum_{k=1}^{n}(u_{ik})^m x_{kj}}{\sum_{k=1}^{n}(u_{ik})^m},\ u_{ik} = \frac{1}{\sum_{j=1}^{c}\left(\frac{d_{ik}}{d_{jk}}\right)^{\frac{2}{m-1}}}$$

u_{ik}: i번째 클러스터에 속한 x_k의 k번째 데이터의 소속도

v_i : i번째 클러스터의 중심벡터

$m\,(1 \le m < \infty)$: 분류 공정에서 퍼지성의 양을 제어하는 파라미터. 일반적으로 $m=2$

2.3 다변량 퍼지결정트리

결정트리는 분류규칙을 표현하는 트리이다. 비 단말모드에는 분류를 위해 비교하는 데이터의 특징이 명시되고, 링크에는 비교조건 또는 특징 값이 부여되며, 단말노드에는 루트노드에서 해당 노드까지의 경로 상에 있는 모든 조건을 만족하는 데이터가 속하는 클래스 값이 부여된다. 결정트리는 명확한 값을 기준으로 특징공간을 분할하므로, 미세한 차이를 가지는 서로 다른 두 데이터를 각각 다른 클래스로 분류할 수 있다. 따라서 결정트리에 퍼지함수의 개념을 도입하여, 특징공간을 소속함수를 이용하여 정의한 퍼지 경계면으로 분할하는 퍼지 결정트리에 대한 연구가 진행되고 있다[10]. 그림 1은 퍼지 결정트리의 한 예

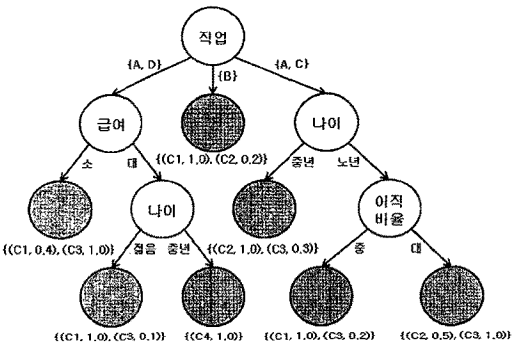

그림 1. 퍼지 결정트리의 예

를 나타낸다[11].

3. FCM 클러스터링과 다변량 퍼지결정트리를 이용한 상황인식 보안 서비스 모델

본 절에서는 FCM 클러스터링과 다변량 퍼지결정트리를 이용하여 입력된 데이터에 대한 패턴 분류를 수행하고 그 결과를 이용하여 보안 등급을 결정함으로써 다양한 환경에 대하여 유연한 보안 서비스를 제공하는 상황인식 보안 서비스 모델을 제안한다. 실험 영역은 헬쓰케어 시스템으로 설정한다.

3.1 FCM 클러스터링

분류는 데이터를 기존에 설정된 클래스와 비교하여 가장 근접한 클래스로 판별하는 것이며 패턴인식, 의사결정, 데이터 분석 등에서 가장 핵심적인 작업이다. 시스템이 요구하는 정보 처리량이 방대해지면서 주어진 정보를 분석하여 다양한 상황에 대응하는 기능은 지능형 시스템의 기본 기능이 되었고, 이러한 적응기능을 위하여 신경망을 비롯한 다양한 알고리즘이 제안되었다. 신경망의 연구는 학습을 통한 분류 기법의 대표적인 방법이며 특히 SOM (Self Organizing Map) 알고리즘의 경우 스스로 비슷한 속성의 데이터끼리 모이도록 학습함으로써 클러스터 분석을 통한 분류에 활용되어 왔다. 그러나 승자독점의 방식을 이용하여 특정 뉴런의 가중치를 갱신하면서 학습이 진행되므로, 실세계에서의 경계가 불명확한 데이터에 대해서는 파리미터에 의존적인 결과를 가지게 되었다. 이에 퍼지 이론을 적용하여 각 데이터의 클래스 소속 값을 함께 학습함으로써 더욱 정확

한 분류 결과를 얻을 수 있는 퍼지 클러스터링 기법이 도입되었다. FCM은 대표적인 클러스터 분석방법의 하나로서 여러 응용 분야에 적용되었으며, 아직 이 방법의 수렴성과 최적화, 일반화에 대한 고찰이 진행 중인 알고리즘이다[12].

FCM 클러스터링 모듈에서는 각 센서정보에 따라 소속 함수를 설계하고 소속정도를 계산한다. 계산된 소속정도를 이용하여 각 정보에 대한 보안 등급을 도출한다. 표 2는 FCM 클러스터링 알고리즘을 나타낸다[9].

3.2 퍼지 결정 트리 (Fuzzy Decision Tree : FDT)

결정트리는 분류 또는 의사결정을 위해 특징 속성값으로 표현된 사례들로부터 분류지식을 추출하기 위해 널리 사용되어온 방법이며, 표준 패턴을 자동으로 추출하기 위한 방법론에는 결정트리생성, 신경회로망 모델, 확률기반 모델, 진화연산 기법 등이 있다. 결정트리는 단변수 결정트리와 다변수 결정트리로 나뉜다. 특히 의사 결정트리는 원인을 규칙으로 표현할 수 있기 때문에 사용자가 원인을 쉽게 이해할 수 있고 시스템의 구축을 용이하게 한다는 장점을 가진다. 실세계의 데이터는 관측오류, 불확실성, 주관적인 판단 등으로 인해서 애매한 형태로 주어지며 대부분의 기존 결정트리 생성방법은 데이터에 내포된 애매함에 대해 충분히 고려하지 못하고 있다. 또한 일반 결정트리는 명확한 값을 기준으로 특징공간을 분할하기 때문에 미세한 차이를 가지는 두 데이터를 서로 다른 클래스로 분류할 수 있다. 이에 특징공간에 분명한 분류 경계를 설정하는 대신에 퍼지 경계를 설정하는 방식을 이용하는 퍼지 결정트리가 제안되었다[10,11].

표 2. FCM 클러스터링 알고리즘

[단계 1] 클러스터의 개수 $c(2 \le c \le n)$ 결정
지수의 가중치 (exponential weight) $m\,(1 < m < \infty)$ 선택
초기 소속 함수 $U^{(0)}$ 초기화
알고리즘 반복회수를 $r\,(r = 0, 1, 2, \cdots)$로 설정

[단계 2] 퍼지 클러스터 중심 $\{v_i | i = 1, 2, \cdots, c\}$계산

$$v_{ij} = \frac{\sum_{k=1}^{n} (u_{ik})^m x_{kj}}{\sum_{k=1}^{n} (u_{ik})^m}$$

[단계 3] 새로운 소속 함수 $U^{(r+1)}$을 계산

$$u_{ik}^{(r+1)} = \frac{1}{\sum_{j=1}^{c} \left(\frac{d_{ik}^r}{d_{jk}^r}\right)^{\frac{2}{m-1}}} \quad \text{for } I_k = \Phi, \text{ 또는}$$

$$u_{ik}^{(r+1)} = 0 \quad \text{for all classes } i,\ i \in \tilde{I}_k$$

$$I_k = \{i | 2 \le c < n;\ d_{ik}^{(r)} = 0\},\ \tilde{I}_k = \{1, 2, \cdots, c\} - I_k$$

$$\sum_{i \in I_k} u_{ik}^{(r+1)} = 1$$

[단계 4] 식 A를 계산하여 $\Delta > \epsilon$ 이면 $r = r + 1$로 정하고 [단계 2]부터 반복 수행, $\Delta \le \epsilon$ 이면 알고리즘 종료. (ϵ 는 임계값)

$$\Delta = \| U^{(r+1)} - U^{(r)} \| = \max_{i,k} |u_{ik}^{(r+1)} - u_{ik}^{(r)}|$$

제안 모델은 최종적으로 가장 적절한 하나의 보안등급을 필요로 한다. 따라서 FCM 클러스터링을 통해 도출된 각각의 보안 등급은 퍼지 결정트리를 이용하여 최종적으로 하나의 보안 등급으로 통합된다. 입력 데이터를 이루는 각 센서 정보들은 센서의 종류에 따라 서로 다른 중요도를 가진다. 예를 들면 고혈압 환자의 신체정보 중에서 혈압과 심박 수가 있을 때, 심박 수의 정보보다 혈압의 정보가 더욱 중요한 정보인 것과 같다. 따라서 제안 모델에서는 FCM 클러스터링을 통해 도출된 각각의 보안 등급에 중요도를 곱한 값을 퍼지 결정트리의 입력 데이터로 사용한다.

제안 모델은 다양한 센서의 정보를 이용하므로 FCM 클러스터링을 통해서 제시되는 입력 데이터도 다양한 변수로서 적용되며, 본 모델에서는 다변량 개념을 퍼지 결정트리에 적용한 다변량 퍼지 결정트리(Multivariate Fuzzy Decision Tree : MFDT)[2,3]를 이용하여 최종 보안 등급을 도출한다. 다변량 퍼지 결정트리의 학습은 표 3과 같은 과정을 따른다 [3].

3.3 제안 모델

본 절에서는 FCM 클러스터링 알고리즘과 다변량 퍼지결정트리를 적용한 상황인식 보안 서비스 모델을 제안한다.

FCM 클러스터링 알고리즘을 이용한 상황인식 보안 서비스 모델은 분류된 각 클러스터의 중심과의 거리를 이용하여 가장 가까운 분류결과를 적용하므로 예기치 못한 상황에서도 가장 적절한 결과를 도출할 수 있다.

최종 보안등급에 따라 보안서비스 엔진에서 제공하는 다양한 보안기능을 수행하고 ACL에서 제공되는 접근권한에 따라 정보에 접근하게 된다. 그림 2는

표 3. 다변량 퍼지 결정트리 학습

[단계 1] 근노드를 생성하고 모든 학습데이터 x를 근노 드에 위치시킨다.

[단계 2] 정보이득을 최대화하는 노드를 생성

1) LDA (Linear Discriminant Analysis)를 이용하여 속성벡터 w 결정

$$Maximize\ J(w) = \frac{w^T S_B w}{w^T S_w w}$$

$$S_w = \sum_{i=1}^{k} S_i\ ,\quad S_i = \sum_{x \in class\,i} (x - m_i)(x - m_i)^T$$

$$m = \frac{1}{K}\sum_{i=1}^{K} m_i$$

2) w를 이용하여 속성 값 $z = w^T x$ 계산

3) 현재 노드의 엔트로피 계산

$$Entropy(S) = -\sum_i P_i^S \log_2 P_i^S$$

$$P_i^S = \frac{N_S^i}{N_S}\ ,\quad N_S = \sum_i N_S^i$$

N_S^i : i번째 클래스인 데이터의 개수

S : 현재 노드에 도달한 z의 집합

4) 노드분기 시 정보이득을 최대화 하는 소속함수 및 정보이득을 계산

$$m^{v,c} = \frac{1}{n_v}\sum_{j=1}^{n_v} z_j^v\ ,\quad v = 1, \cdots, N$$

n_v : v번째 구역에 포함되는 데이터z의개수

z_j^v : z를 오름차순 정렬에서 j번째 z값

$m^{v,c}$: v번째 소속 함수의 꼭지점 위치

모든 구간에서 각 소속 함수의 꼭지점 위치를 구한 후 소속 함수의 좌측, 우측 값을 계산

$$m^{v,l} = m^{v,c} - 0.5(1+\gamma)(m^{v,c} - m^{v-1,c})$$
$$m^{v,r} = m^{v,c} + 0.5(1+\gamma)(m^{v+1,c} - m^{v,c})$$

γ : 두 퍼지 소속 함수 간의 겹친 정도

$$S_{viw} = \{(z, \mu_{S_{viw}}(z)) \mid \mu_{S_{viw}}(z) : v\text{번째 소속 함수 값}\}$$

$$C_{S_{iv}}^i = \sum_{\substack{class\ of\ z \\ z \in S_{iv}}} \mu_{S_{iw}}(z)$$

$$C_{S_{iv}} = \sum_i C_{S_{iw}}^i\ ,\quad P_i^{S_{iw}} = \frac{C_{S_{iw}}^i}{C_{S_{iw}}}$$

$$Entropy(S_{viw}) = -\sum_i P_i^{S_{iw}} \log_2 P_i^{S_{iw}}$$

$$Gain(S, w) = Entropy(S) - \sum_v \frac{N_{S_{iw}}}{N_S} Entropy(S_{viw})$$

5) 현재 노드를 한 가지 속성만 사용해서 분기하는 경우, 가장 큰 정보 이득을 갖게 하는 속성 및 소속 함수를 구한다. (w는 하나의 요소만 1이고 나머지는 0인 단위 벡터가 됨)

6) 다변량 속성벡터를 사용한 분기 (4번 과정)와 하나의 속성을 사용한 분기 (5번 과정)의 정보 이득 중 더 큰 정보 이득을 갖는 w와 소속함수를 사용해 자식 노드를 생성한다.

[단계 3] 종료조건을 만족하면 현재 노드를 단말 노드로 만들고 클래스 할당. 그렇지 않으면 모든 자식 노드에서 단계 2를 재귀적으로 반복

종료조건 :

1) 현재 노드의 모든 데이터의 클래스가 동일한 경우

2) 현재 노드의 깊이가 미리 정의된 최대 깊이를 초과하는 경우

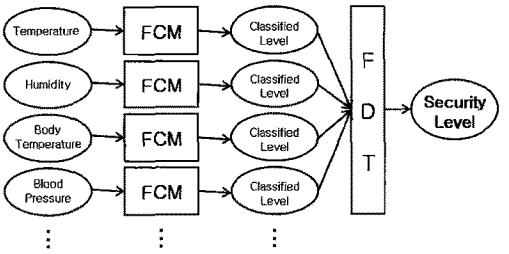

그림 2. 보안등급 도출 과정

제안 모델의 보안 등급 도출 과정을 나타낸다.

또한 최종적으로 도출된 보안 등급에 대한 접근제어목록을 적용할 경우 다양한 상황의 충돌에 대한 무결성 보장문제도 해결가능하다.

본 논문에서 제안하는 모델은 상황정보의 수집 및 전송을 수행하는 입력모듈, 입력된 정보를 이용하여 상황정보를 분류하고 최종 결과를 도출하는 상황인식 엔진, 다양한 보안 기능을 제공하는 보안 서비스 엔진, 해당하는 보안 등급에 따른 접근권한 목록을 관리하는 접근 제어 목록으로 구성된다. 그림 3은 제안 모델의 구조를 나타낸다.

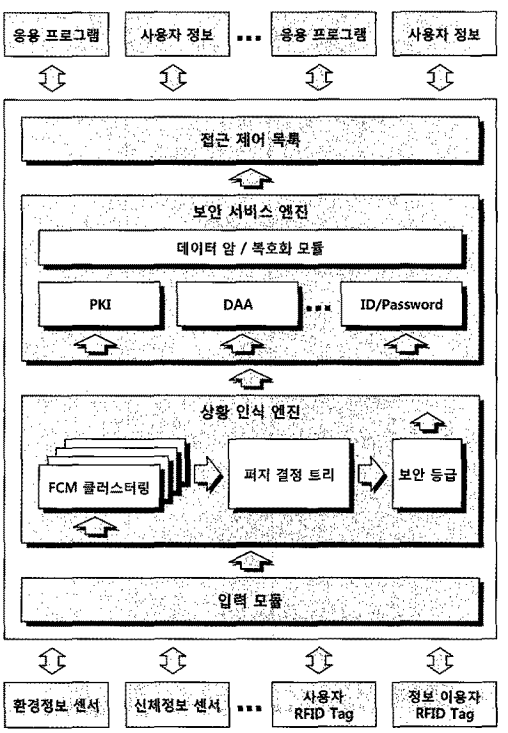

그림 3. 제안 모델의 아키텍처

3.4 입력 모듈

입력 모듈은 센서네트워크의 다양한 센서들이 제공하는 상황정보를 수집하는 역할을 수행한다. 센서네트워크는 온도, 습도, 조도 등의 환경정보 센서 및 체온, 혈압, 맥박수와 같은 인체정보 센서, 그리고 진동, 소음상태, 가스누출 여부 등을 알려주는 다양한 센서로 구성되어 있다. 입력모듈에서 수집한 데이터는 상황 인식 엔진으로 전달된다. 그림 4, 5, 6은 센서를 통해 입력받을 수 있는 상황정보의 구조를 나타낸다. 실제 입력되는 데이터는 각각의 센서로부터 전달받는 수치 데이터이며 입력모듈에서 시스템에서 사용가능한 데이터의 형태로 변환된다.

3.5 접근 제어 목록

접근 제어 목록은 분류 모듈을 통해 도출된 보안 등급에 따라 사용자가 접근 가능한 권한의 목록을 제공한다. 일반적으로 GRBAC와 같은 역할 기반 접근제어 기법이 많이 사용되고 있으나 역할 기반 접근제어 기법은 예상하지 못한 상황, 즉 보안 정책에 설정되지 않은 문제에 대하여 대응이 어렵다는 단점을 가지며, 또한 분류를 위한 데이터의 종류가 늘어남에 따라 그 구조가 복잡해지고, 각각의 상황정보에 대한 조건에 따른 접근권한의 충돌문제로 인해 무결성을 유지하지 못하는 경우가 발생한다.

제안 모델에서는 복잡한 구조를 피함으로써 관리의 편의성을 향상시키고 복잡한 조건에 따른 충돌문제를 예방하기 위해 FCM과 FDT를 이용하여 최종적인 보안 등급을 계산하고, 이 보안 등급과 정보를 이용자의 권한 등급만을 이용하여 접근제어를 수행한다. 상황인식 모듈을 통하여 최종적으로 계산된 보안 등급을 기반으로 접근 제어를 수행하므로 이러한 접근권한 충돌 문제가 발생하지 않는다. 또한 접근제어 목록의 내용을 관리함으로써 시스템 및 사용자의 정보에 대한 유연한 접근이 가능하도록 설정이 가능하며, 유사한 특성을 가진 다른 응용 프로그램에도 적용이 가능하다.

그림 7 은 접근제어 목록의 예를 나타낸다. 도출된 보안 등급과 정보를 사용하고자 하는 사용자의 등급을 이용하여 허용 가능한 정보의 목록을 관리한다.

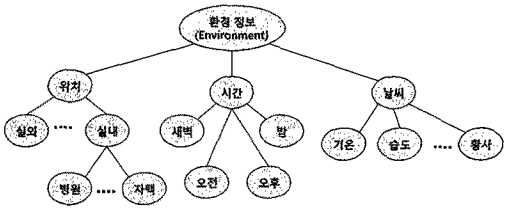

그림 4. 환경정보의 구조의 예

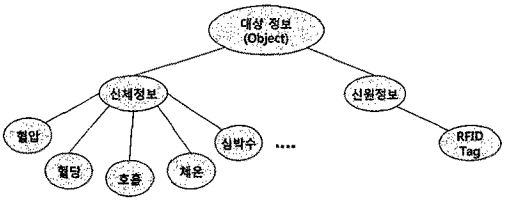

그림 5. 정보를 이용하고자 하는 대상 정보의 구조의 예

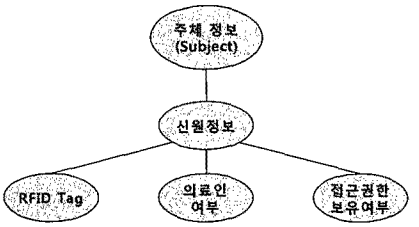

그림 6. 정보를 이용하고자 하는 주체정보

4. 구현 및 평가

본 논문에서 제안한 모델의 학습 및 성능을 파악

```
<ACL>
  <POLICY>
    <SECURITY_LEVEL>1</SECURITY_LEVEL>
    <SUBJECT_LEVEL>1</SUBJECT_LEVEL>
    <OPERATION>Read</OPERATION>
    <LIST>
      <INFORMATION>Blood Pressure</INFORMATION>
      <INFORMATION>Heart Rate</INFORMATION>
      <INFORMATION>History of a Patient</INFORMATION>
      <INFORMATION>Clinical History</INFORMATION>
      <INFORMATION>Case History</INFORMATION>
      <INFORMATION>Special Attention</INFORMATION>
    </LIST>
  </POLICY>

  <POLICY>
    <SECURITY_LEVEL>1</SECURITY_LEVEL>
    <SUBJECT_LEVEL>1</SUBJECT_LEVEL>
    <OPERATION>Read</OPERATION>
    <LIST>
      <INFORMATION>Blood Pressure</INFORMATION>
      <INFORMATION>Heart Rate</INFORMATION>
      <INFORMATION>Case History</INFORMATION>
      <INFORMATION>Special Attention</INFORMATION>
    </LIST>
  </POLICY>
</ACL>
```

그림 7. 접근 제어 목록 (ACL)의 예

하기 위하여 P-IV 3.0GHz CPU와 1GB Ram이 장착된 PC에서 Java 5.0을 이용하여 제안된 모델을 구현하였다. 상황 정보의 입력에는 *TynyOS 2.x*를 기반으로 하는 USN 장비인 *UBee430/UBee430-AP-Kit*를 사용하였다. 실험 데이터는 고혈압 환자 혈압변화에 대한 300건의 가상 데이터를 사용하여 클러스터링을 수행하였고, 다변량 퍼지결정트리를 통하여 어떤 보안 등급을 계산해 내는지 확인하였다. 또한 GRBAC 모델과 FCM 클러스터링 모델을 각각 적용했을 때의 보안등급 계산결과를 비교하였다.

실험 데이터는 한국인 20세 이상의 성인을 대상으로 조사된 고혈압 유병률과 고혈압 진단 기준에 맞추어 생성한 300건의 가상 데이터를 사용하였다. 표 4는 정상 혈압과 고혈압의 진단 기준을 나타내며 표 5는 20세 이상의 한국인 성인에 대한 고혈압 유병률을 나타낸다[13]. 그림 8은 표 4와 표 5의 기준에 맞추어 생성한 가상데이터의 분포도이다.

실험 데이터에 대한 클러스터링이 완료된 후 입력되는 혈압변화에 따라 어떤 보안 등급을 계산해 내는지 확인하였고, 또한 GRBAC 모델과 FCM 클러스터링 모델을 각각 적용했을 때의 혈압변화에 따른 보안등급 계산결과를 비교하였다. 표 6은 GRBAC 모델에 적용하기 위한 권한정책을 나타낸다. 보안등급은 총 5등급으로 분류되며 등급이 낮을수록 낮은 수준의 보안 서비스를 적용한다. 제안 모델에서 보안 등급은 사용자의 상황에 따라 결정되는데 사용자의 현재 상태가 나쁠수록 낮은 등급이 부여된다. 이는 긴급 상황의 경우, 보안 수준을 최소한으로 설정함으로써 사용자의 생명을 보호하기 위한 최대한의 정보를 제공하기 위함이다. 즉 사용자의 상황이 양호할 경우에는 개인 정보를 철저하게 보호할 수 있는 높은 수준의 보안 서비스를 제공하고, 긴급 상황의 경우에는 사용자의 보호를 최우선으로 고려함을 의미한다.

표 6은 GRBAC 모델을 적용하기 위한 권한정책의 예를 나타낸다.

보안등급은 총 5등급으로 분류되며 등급이 낮을수록 낮은 수준의 보안 서비스를 적용한다. 표 7은 GRBAC 모델을 적용한 보안등급 계산결과와 FCM 클러스터링 알고리즘을 적용한 보안등급 계산결과를 나타낸다. 표 7에서 기대등급은 정상혈압수치와 비교하여 위험수치로 다가가는 정도에 따라 결정한 등급이다.

표 4. 정상 혈압과 고혈압 진단 기준

혈압	수축기 혈압		확장기 혈압
정상	120 미만	AND	80 미만
고혈압 전 단계	120 - 139	OR	80 - 89
고혈압	140 이상	OR	90 이상

표 5. 20세 이상의 한국인 성인의 고혈압 유병률

성별	정상	고혈압 전 단계	고혈압
	분율 (표준오차)	분율 (표준오차)	분율 (표준오차)
남자	35.2 (1.5)	39.9 (1.5)	24.9 (1.2)
여자	59.2 (1.2)	20.3 (0.9)	20.5 (0.9)
계	47.3 (1.1)	30.0 (1.0)	22.7 (0.8)

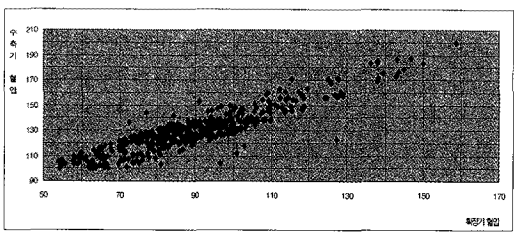

그림 8. 가상 데이터의 혈압 분포도

표 6. GRBAC 모델에서의 권한정책의 예

환경정보		작업	행동 주체	대상	혈압	등급
시간	장소					
모든 시간	모든 장소	정보 조회	의료 요원	환자 정보	156/100~	1
					155/99~151/98	2
					150/97~146/96	3
					145/95~141/94	4
					~140/93	5

표 7. 혈압변화에 따른 보안등급 계산 결과

혈압	GRBAC	FCM	기대등급
152.5 / 98.8	2	3	3
153.2 / 100.3	Unknown	3	3
167.7 / 109.5	1	1	1
157.3 / 105.3	1	2	2
141.5 / 87.4	Unknown	3	4
137.3 / 85.3	5	4	4

표 7에서 혈압수치 167.7 / 109.5의 경우, 위급 상황으로 인식하여 1등급의 보안서비스가 적용되고 있다. 또한 다소 높은 혈압범위에서는 2~3등급, 정상 혈압 범위에서는 4~5등급의 보안등급을 제시하고 있음을 확인할 수 있다.

그러나 GRBAC 모델을 적용한 보안등급 계산결과에서는 Unknown이 발생하고 있으며, 이는 환자의 혈압상태가 정규적으로 분류되지 않고 두 개 이상의 조건에 교차되어 있는 경우이다. GRBAC 모델의 권한정책을 더욱 상세하게 설정할 경우 적절한 보안등급의 도출이 가능하겠지만 모든 상황에 대하여 적절한 각각의 권한정책 설정은 현실적으로 매우 어려우며, 또한 권한정책의 분류 개수가 많아질수록 결과 도출에 시간이 걸릴 것을 예측할 수 있다.

반면, FCM 클러스터링을 적용한 결과는 일반적으로 모든 상황에 대하여 적절한 결과를 보여주고 있다. 이는 자율적인 클러스터링을 수행한 후, 각 클러스터의 중심 값과 입력벡터의 거리를 이용하여 더욱 가까운 클러스터, 즉 보다 더 적합한 등급을 제시하기 때문이며 GRBAC 모델보다 유연하고 적합한 결과를 보여주고 있다.

또한 제안 모델은 다양한 상황정보를 기반으로 상황인식을 수행하므로 혈압정보 외에도 심박수, 체온, 주변기온 및 습도 등의 많은 센서 정보가 FCM 클러스터링을 통해서 각각의 보안등급으로 분류된다. 따라서 계산된 각각의 보안등급을 통합하여 분석할 필요가 있다. 이에 FCM 클러스터링을 통해 도출된 결과 데이터를 다시 다변량 퍼지결정트리에 적용함으로써 다양한 정보를 통합하여 보다 적절한 보안등급을 선택할 수 있다.

고혈압 환자의 경우 혈압정보 외에 심박수, 체온, 주변온도 등의 영향을 많이 받으며 정보별로 그 중요도가 다르기 때문에 FCM 클러스터링의 결과에 중요도 값을 적용하여 다변량 퍼지결정트리의 입력 값으로 사용한다. 표 8은 FCM 클러스터링과 MFDT를 이용한 보안등급을 나타낸다.

표 8에서 혈압수치 137.3 / 85.3의 경우, 혈압 변화에 따른 보안등급은 4등급이지만 심박 수의 변화에 따른 보안등급은 1등급으로 계산되어 최종 보안 등급은 2등급이 제시되고 있음을 확인할 수 있다. 이는 환자의 현재 혈압상태는 정상이나 높은 심박 수로 인하여 혈압상태가 악화될 가능성이 보안등급에 적용되었음을 나타낸다. 즉 제안 모델은 환자의 주위 상황을 인식함으로써 환자의 상태변화에 대한 파악과 예측을 통해 가장 적절한 보안등급을 제시하고 있음을 확인할 수 있다. 표 9는 기존의 GRBAC 모델과 제안 모델의 비교내용을 보여준다.

표 8. FCM 클러스터링과 MFDT를 이용한 보안등급

혈압		심박수		FDT
상태	FCM	횟수	FCM	
167.7 / 109.5	1	122	4	1
157.3 / 105.3	2	78	5	2
120.8 / 82.5	4	73	5	4
141.5 / 87.4	3	160	3	3
137.3 / 85.3	4	201	1	2

표 9. GRBAC 모델과 제안 모델의 비교

기준	GRBAC 모델	제안모델 (FCM + MFDT)
자율성	사전 등록된 고정규칙기반 상황인식	자율적인 클러스터링을 이용하여 상황인식
대응능력	고정된 규칙을 이용하므로 모든 상황에 대한 대응 불가능	클러스터 중심과의 거리로 분류/인식 하므로 모든 상황에 대응가능
관리정책	규칙/정책의 직접 관리로 인한 오버헤드	규칙/정책을 직접 관리할 필요가 없음
통합성	상황정보의 다양성에 의해 정책구조가 갈수록 복잡해 짐	다양한 종류의 상황정보를 통합하여 최적의 결과를 도출

5. 결론 및 향후계획

본 논문에서는 사용자의 상황을 인식하고, 다양한 수준의 보안기술을 적용하기 위하여 FCM 클러스터링 알고리즘과 다변량 퍼지 결정트리를 이용한 상황인식 보안 서비스를 제안하였다. 제안 모델은 FCM 클러스터링 알고리즘을 통한 자율적인 상황의 분류와 다양한 센서 정보에 대한 분류 결과를 통합하는 다변량 퍼지결정트리를 이용하여 보다 적절한 보안등급을 제시한다. 그리고 지속적인 관리가 필요한 고혈압 환자에 대한 가상적인 주변상황을 구성하여, 제안 모델이 얼마나 유연하고 적절하게 보안서비스를 적용할 수 있는가에 대한 실험 결과를 제공하였다.

기존의 GRBAC 모델과 비교할 때, FCM 클러스터

링을 적용한 모델은 자율적인 클러스터링 방식을 이용하므로 예상하지 못한 상황에 대해서도 적절한 분류결과를 보여주고 있다. 또한 제안 모델에서는 수많은 규칙을 직접 관리하지 않고 자율적으로 상황을 분류하므로 GRBAC 모델과 같은 관리상의 오버헤드 문제도 해결할 수 있었다. 이는 제안 모델이 유연하면서도 자율적인 보안 서비스를 제공함과 동시에 관리에 대한 비용 효율적인 면에서도 좋은 결과를 제공한다는 것을 보여주고 있다.

또한 GRBAC 모델은 상황정보의 종류가 늘어날수록 정책 및 규칙의 구조가 점점 복잡해지지만, 제안 모델은 다변량 퍼지결정트리를 이용한 통합결과를 제시함으로써 환자의 상태변화에 따라 예측 가능한 보다 적절한 보안등급을 제시하고 있으며 각 상황정보의 중요도에 따른 등급결정으로 현실적인 보안등급 적용이 가능하다.

향후 연구는 학습기능을 적용한 보다 현실적이고 사용자 별로 차별화된 성능을 제공하는 시스템으로 발전시켜 나갈 것이며, 보안만이 아닌 상황인식을 필요로 하는 다른 모든 시스템에도 적용 가능한 범용적인 시스템으로 발전시켜 나가야 할 것이다.

참 고 문 헌

[1] J. Bezdek, "A convergence theorem for the fuzzy ISODATA clustering algorithm," *IEEE Trans. Pattern Anal. Machine Intelligence*, Vol.PAMI-2, No.1, pp. 1-8, 1980.

[2] Y. Yuan and M.J. Shaw, "Induction of fuzzy decision tree," *Fuzzy Sets and Systems*, Vol. 69, No.2, pp. 125-139, 1995.

[3] 전문진, 도준형, 이상완, 박광현, 변증남, "다변량 퍼지 의사결정트리와 사용자 적응을 이용한 손동작 인식," 로봇공학회 논문지, 제3권, 제2호, pp. 81-90, 2008.

[4] Jalal Al-Muhtadi, Anand Ranganathan, Roy Campbell, and M. Dennis Mickunas, "Cerberus: A Context-Aware Security Scheme for Smart Spaces," In Proc. of the First International Conference on Pervasive Computing and Communications (PerCom'03), 2002.

[5] Michael J. Covington, Prahlad Fogla, Zhiyuan Zhan, and Mustaque Ahamad, "A Context-Aware Security Architecture for Emerging Applications," In Proc. of the 18th Annual Computer Security Applications Conferences (ACSAC'02), pp. 249-258, 2002.

[6] Michael J. Covington, Matthew J. Moyer, and Mustaque Ahamad, "Generalized Role-Based Access Control for Securing Future Applications," In Proc of the 23th National Information Systems Security Conference(NISSC), Baltimore, pp. 115-125, 2000.

[7] M. J. Moyer and M. Ahamad, "Generalized Role-Based Access Control," In Proc of IEEE International Conference on Distributed Computing Systems(ICDSC2001), pp. 391-398, 2001.

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

[9] 오성권, 프로그래밍에 의한 컴퓨터지능, 내하출판사, 2002.

[10] 이우향, 이건명, "특징공간을 사선 분할하는 퍼지 결정트리 유도," 정보과학회논문지 : 소프트웨어 및 응용, 제29권, 제3호, pp. 156-166, 2002.

[11] 이건명, "퍼지 데이타에 대한 퍼지 결정트리 기반 분류규칙 마이닝," 정보과학회논문지 : 소프트웨어 및 응용, 제28권, 제1호, pp. 64-72, 2001.

[12] 이현숙, "점증적 학습 퍼지 신경망을 이용한 적응 분류 모델," 퍼지 및 지능시스템학회 논문지, 제16권, 제6호, pp. 736-741, 2006.

[13] 보건복지부, "국민건강영양조사 제3기(2005) 검진조사," 보건복지부 질병관리본부, pp. 114-115, June 2006.

양 석 환

2000년 동서대학교 응용수학과 (이학사)
2009년 부경대학교 정보보호학 협동과정 (공학석사)
2000년~2009년 일본 NEC SOFT 개발팀 및 부산경남 신발산업 정보화사업 외 다수의 프로젝트 개발 참여

정 목 동

1981년 경북대학교 컴퓨터공학과 (공학사)
1983년 서울대학교 컴퓨터공학과 (공학석사)
1990년 서울대학교 컴퓨터공학과 (공학박사)
1985년~1996년 부산외국어대학교 컴퓨터공학과 교수
1996년~현재 부경대학교 컴퓨터공학과 교수
관심분야 : 컴퓨터응용보안, 지능형 에이전트 및 상황인식 컴퓨팅, 모바일/전자상거래 보안, 웹 애플리케이션