논문 02-27-10C-16 한국통신학회논문지 '02-10 Vol.27 No.10C

협력시스템에서의 접근제어 프레임워크 설계 및 구현

정회원 정 연 일*, 이 승 룡*

The Design and Implementation of Access Control Framework for Collaborative System

Yonil Zhung*, Sungyoung Lee* ***Regular Members***

요 약

최근 협력 시스템에 대한 연구가 증가되면서 협력 작업에 대한 연구와 더불어 협력 시스템 보안에 대한 연구가 중요시되고 있다. 협력 시스템에서 인증 및 암호화의 경우 기존의 정책을 사용하여 시스템의 견고성을 유지할 수 있다. 그러나 접근 제어 정책에서 기존의 정책을 그대로 사용하게 되는 경우 분산 환경, 개방된 네트워크, 다양한 주체와 객체의 존재로 인하여 협력 시스템은 신분, 직무, 그룹, 보안등급, 무결성 등급, 허가권을 포함해야 하는 다양한 접근상황을 고려해야 된다. 이 경우, 낮은 보안 등급의 주체가 높은 보안 등급의 객체로 접근을 허용 하거나, 높은 보안 등급의 주체가 낮은 보안 등급의 객체로 접근을 막아야 하는 복합적 상황을 해결하지 못한다. 더욱이 모든 접근상황을 제어하기 위하여 객체에 여러 접근제어 요소를 포함하여 접근 제어를 알고리즘화 할 경우 불필요한 상황을 모두 고려해야 하기 때문에 시스템의 성능 저하를 야기 시킨다. 이 같은 문제를 해결하기 위하여, 본 논문에서는 협력 시스템의 특징에 맞는 새로운 접근제어 프레임워크를 제안한다. 제안된 접근제어의 특징은 주체 및 객체에 다수의 접근 요소를 정의하여 기존 정책 보다 협력시스템과 같은 복합적인 상황에서 용이하게 적용되도록 하였다. 그리고 객체의 종류를 접근될 요소의 특징에 따라 세 가지로 구분하였고, 구분된 각 객체의 특징에 따라 알고리즘이 구현됨으로 빠르고 원활한 협력 작업이 수행되도록 하였다. 또한, 접근 요소 및 정책 변경이 용이하도록 확장성을 고려하였다. 모의실험 결과 다수의 접근 요소를 사용하였지만 시스템 성능은 접근 제어 정책을 적용하지 않았을 때와 큰 차이를 보이지 않았으며 복합적인 상황의 접근제어에서도 확실한 접근 제어가 가능했다.

ABSTRACT

As per increasing research interest in the field of collaborative computing in recent year, the importance of security issues on that area is also incrementally growing. Generally, the persistency of collaborative system is facilitated with conventional authentication and cryptography schemes. It is however, hard to meet the access control requirements of distributed collaborative computing environments by means of merely apply the existing access control mechanisms. The distributed collaborative system must consider the network openness, and various type of subjects and objects while, the existing access control schemes consider only some of the access control elements such as identity, rule, and role. However, this may cause the state of security level alteration phenomenon. In order to handle proper access control in collaborative system, various types of access control elements such as identity, role, group, degree of security, degree of integrity, and permission should be taken into account. Futhermore, if we simply define all the necessary access control elements to implement access control algorithm, then collaborative system consequently should consider too many available objects which in consequence, may lead drastic degradation of system performance.

* 경희대학교 전자계산공학과 실시간&멀티미디어 연구실 (zhung@oslab.khu.ac.kr)
논문번호 : 020209-0502, 접수일자 : 2002년 5월 2일
※ 본 연구는 산업 자원부 중기 거점 기술 개발 사업에 의해 지원 되었습니다

In order to improve the state problems, we propose a novel access control framework that is suitable for the distributed collaborative computing environments. The proposed scheme defines several different types of object elements for the accessed objects and subjects, and use them to implement access control which allows us to guarantee more solid access control. Futhermore, the objects are distinguished by three categories based on the characteristics of the object elements, and the proposed algorithm is implemented by the classified objects which lead to improve the systems' performance. Also, the proposed method can support scalability compared to the conventional one. Our simulation study shows that the performance results are almost similar to the two cases; one for the collaborative system has the proposed access control scheme, and the other for it has not.

Ⅰ. 서 론

협력 시스템은 원격지의 많은 사용자들이 가상공간에서 공동작업을 수행할 수 있는 환경을 제공 해주는 시스템으로 인터넷, 멀티미디어, 가상현실 그리고 고성능 마이크로프로세서 기술의 급속한 발전에 힘입어 구현이 가능하게 되었다. 그러나 분산 환경 및 개방된 네트워크 상에서 작동되는 협력시스템은 다양한 사용자가 사용하기 때문에 여러 가지 면에서 보안이 취약하다.

협력 시스템의 보안 프레임워크에서 인증 및 암호화는 이미 검증이 된 ITU-T X.509, 커버로스(Kerberos), 공개키 암호화 등의 기존 정책을 사용해야 견고성이 유지되지만 접근제어의 경우 기존의 정책을 수정 없이 사용할 경우 다음과 같이 보안에 많은 허점이 생기게 된다. 첫째, 기존의 접근제어 정책은 하나 또는 두 가지의 접근제어요소를 사용하여 접근제어를 수행하지만, 협력 시스템에서는 낮은 보안등급의 주체가 높은 보안등급의 객체로 접근이 허용 되거나, 높은 보안등급의 주체가 낮은 보안등급의 객체로 접근이 불허되는 등, 일반 접근제어와는 상반되는 상황이 발생된다. 또한, 다양한 주체와 여러 종류의 객체가 생성되는 협력 시스템에서 기존의 신분, 규칙, 직무 등과 같이 한 가지 접근제어 요소를 사용하였을 경우 정확한 제어 및 원활한 접근을 하지 못하는 경우가 발생한다. 둘째, 기존의 접근제어 정책을 수정 없이 사용하는 경우 접근제어 정책과 협력 시스템의 동시성 제어와 충돌이 발생하기 때문에 협력 시스템에서 동시성 제어 정책과 접근제어 정책 중 한 가지를 포기해야 하는 경우가 발생한다. 그리고 협력 시스템의 모든 접근 상황을 고려하여 객체에 필요한 접근 요소를 정의한 뒤 접근제어를 알고리즘화 할 경우 시스템 성능 저하를 가져온다. 따라서 기존의 보안 정책과 달리 협력 시스템의 특징과 구조에 맞는 새로운 접근제어 정책이 필요하다. 본 논문에서는 저자가 개발한 산업 디자인 협력 시스템을 모델로 하여 새로운 접근제어 정책에 관하여 제안한다.

제안된 접근제어의 특징은 첫째, 주체 및 객체의 접근제어요소를 신분, 직무, 그룹, 보안등급, 무결성 등급, 허가권, 소유권으로 정의하였다. 이렇게 여러 접근제어 요소를 정의함으로 협력 시스템에서 여러 가지 상황에 서로 효과적인 접근제어가 가능하다. 둘째, 저자가 개발한 산업 디자인 협력 시스템의 동시성 제어 정책에 접근제어요소를 삽입함으로 시스템 성능을 향상시킬 수 있었다. 셋째, 접근을 당하는 객체를 협력 시스템의 특징에 맞도록 분류함으로써 각 객체의 종류에 따른 새로운 접근제어 알고리즘의 적용을 가능하게 하였다. 본 논문에서는 산업 디자인 협력 시스템의 특징에 따라 객체를 사용자 정보 및 일반 정보 접근, 세션 정보 접근, 공동작업 공유 데이터 접근의 세 가지로 분류하였다. 넷째, 제안된 접근제어 정책은 유사한 다른 협력시스템으로 확장이 가능하다. 이는 접근제어 프레임워크를 유지하며 접근제어 정책의 변경만으로 유사한 협력시스템에 응용을 할 수 있도록 하였다. 따라서 제안된 협력시스템의 접근제어 정책은 복합적인 상황과 불법적인 접근에 대한 접근제어가 가능하게 되었으며, 시스템 특징에 맞도록 접근 요소 및 정책 변경이 용이하도록 확장성을 고려하였다.

모의실험 결과 제안된 정책은 사용자가 원하는 규칙의 접근제어를 적용하였으며, 여러 접근 요소를 이용하였지만 시스템 성능은 접근제어 정책을 적용하지 않았을 때와 큰 차이를 보이지 않았으며, 여러 복합적인 상황에서도 접근제어를 할 수 있었다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 접근제어 정책과 협력 작업의 보안 정책에 관련된 연구를 소개하고, 3장에서는 제안된 접근제어 프레임워크가 구현되는 산업 디자인 협력시스템에 대하여 간단히 설명한다. 4장에서는 접근제어 프레임워크에 대하여 기술하고, 5장에서는 실제 구현된 시스템에 대한 기술과 성능 평가를 하며, 6장에서 결

론 및 향후 전망에 대하여 논의한다.

Ⅱ. 관련 연구

OSI(Open Systems Interconnection) 보안 구조에서의 접근제어 정책은 신분, 규칙, 역할 기반 정책으로 나누어진다. 신분 기반 정책은 주체나 또는 그들이 속해 있는 그룹들의 신분에 근거하여 객체에 대한 접근을 제한할 뿐 접근되는 객체 정보의 중요성에는 아무런 지식을 가지고 있지 않으므로 단순한 신분 위장에 의해서 접근제어가 파괴될 수도 있다. 규칙 기반 정책은 멀티 레벨 정책과 구분 기반(compartment-based) 정책을 포함하고 있다. 이는 또한 주체와 객체간의 관계를 정의하고, 정보의 흐름이 일어났을 때 정보가 소유한 제한 규칙을 상속하며, 각 주체와 객체에 대해서 규칙 기반 정책이 일정하므로 단순한 신분 위장으로는 접근제어를 파괴 할 수 없다. 역할 기반 정책은 신분 기반 정책과 규칙 기반 정책의 양쪽 특성을 갖고 있으며 상업용 환경에 적합한 정책으로서 개별적 신분이 아닌 자신의 직무에 따라 접근 할 수 있는 정보가 결정되고, 사용할 수 있는 정보의 한계가 정해진다[1].산업 디자인 협력 시스템의 경우 직무 및 개별적 신분 등 각기 다른 접근 요소를 필요로 하는 여러 가지 종류의 객체가 존재하기 때문에 역할 기반 정책만으로는 적합하지 못하다.

기존 접근제어 보안 정책을 포함하고 있는 협력 시스템에서의 접근제어 정책의 특징으로 Mushroom의 경우 접근제어 리스트를 정의하여 정의된 리스트에 의한 접근제어 정책을 사용하고 있다[2]. Suite의 경우 주로 사용자에 대한 규칙 정의와 접근 권한 정의를 내려두고 접근제어를 하며 접근 권한의 상속 등을 상세하게 정의하여 사용한다[3]. 이와 같은 방식의 접근제어 보안 서비스는 확장성, 쉬운 접근제어 정의 사용의 특징이 있으며, 사용자간의 접근 충돌의 경우에도 규칙을 정하여 규칙에 맞게 해결을 할 수 있다. 하지만 멀티 사용자 규칙 정의, 협력 권한 정의 등에 관한 모든 상황에 맞는 정의가 있어야 하며, 접근 권한 및 사용자의 규칙 정의에 대한 평가가 올바르게 되어 있어야 한다. 또한, 접근 정의를 저장하는 것에 대한 문제점들을 해결해야 하며, 객체에 대한 접근제어 방식이 아닌 주체와 규칙에 의한 접근제어 방식을 쓰고 있기 때문에 객체 보호에 대한 보안은 취약한 편이다. 제안된 접근제어의 경우 주체와 객체의 접근제어요소를 기반으로 접근제어를 하기 때문에, 미리 정의된 규칙에 접근제어를 하는 정책에 비하여 시스템 성능 저하를 가져올 수 있지만 정의되지 않은 어떠한 상황에서도 확실한 접근제어가 가능하며 객체 보호에도 장점을 갖고 있다.

객체 지향 분산 서비스인 CORBA(Common Object Request Broker Architecture)의 접근제어 방식의 특징은 개체 요청 브로커 내에 적절한 주체와 객체간의 접근제어를 정의한 뒤 이를 이용하여 접근제어를 수행한다[4]. CORBA의 경우 분산 환경에서 적당한 표준은 제시하고 있지만, 협력시스템의 특징인 여러 계층의 다양한 종류의 보안 레벨에 대해서는 일괄적인 규칙만을 적용하고 있기 때문에 사용자들의 요구에 따른 접근제어는 취약한 면이 있다. 제안된 접근제어의 경우 주체와 객체는 각각의 접근제어요소를 갖고 있으며 접근제어를 필요로 할 경우 원하는 방식과 요구에 의해 접근제어를 할 수 있도록 하였기 때문에 사용자의 요구에 따른 접근제어의 경우에도 빠른 적응을 할 수 있다. 또한, 기존의 일반 시스템에서의 접근제어 정책은 적은 접근제어요소를 이용하여 알고리즘을 단순화하였기 때문에 빠르며, 명확한 접근제어 기준을 이용하여 확실한 접근제어를 하는 반면, 접근제어요소의 수가 적으므로 복합적인 상황을 고려해야하는 협력시스템에서는 여러 가지 면에서 부적당하다고 할 수 있다.

현재 많은 협력 작업 환경을 지원하는 시스템이 개발이 되어있으며 또한 개발 중에 있지만 대부분 협력 작업에 중점을 두고 시스템을 개발하고 있으며 접근제어 정책과 관련된 연구는 미진한 실정이다[5][6][7][8]. 그리고 접근제어 정책을 포함하더라도 협력시스템의 특징에 맞는 정책을 사용하는 것이 아니라 기존의 보안 정책을 사용함으로 공동작업, 데이터 일관성 유지 및 보안 정책간의 어떠한 관계도 기술하지 못하며 단지 보안 정책을 적용하는데 의미를 두고 있다.

Ⅲ. 산업 디자인 협력시스템

본 논문에서 구현 모델로 선택한 산업 디자인 협력시스템은 개발 주기가 짧은 산업 제품의 3D 디자인 협력 공동작업 어플리케이션에 적용할 수 있으며, 플랫폼에 독립적이고, 확장과 이식이 용이한 프레임워크를 구축할 수 있다. 구현된 협력시스템은 서버와 클라이언트 구조로, 서버는 유지 보수가 용이하고 플랫폼에 독립적이며 이식성이 뛰어난 자바

를 사용하였다[9].

협력시스템의 기능은 크게 응용시스템, 서버 그리고 클라이언트로 나눌 수 있다. 응용 시스템 기능은 3D Studio Max를 이용한 분산 산업디자인 협력 작업이다. 서버 기능으로는 첫째, 일관성 및 영속성 유지를 위한 이벤트처리와 공유데이터 관리 기능 둘째, 사용자 인증, 사용자 상태 정보 제공, 사용자 검색, 실시간 메시지 전송과 같은 사용자 관리 셋째, 산업디자인 프로세서 처리를 위한 데이터베이스 관리, 세션 관리, 3D Studio Max의 3D 객체 관리, 화이트보드의 2D 객체 관리와 같은 세션 관리 그리고 사용자 관리 서버 인증, 사용자 관리 서버들 사이의 정보 교환 또는 메시지 전송 등과 같은 정보 관리자 기능이 있다. 클라이언트 기능으로는 서버 접속, 세션 관리, 3D Studio Max 객체공유, 화이트보드, 채팅 등이 있다.

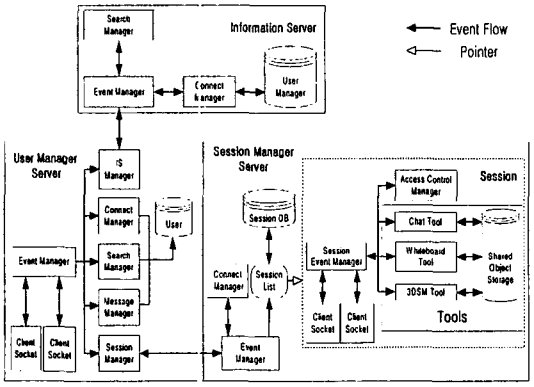


그림 1. 협력시스템 서버 구조

그림 1에서 보면 사용자관리 서버(User Manager Server: UMS)는 사용자를 관리하며, 사용자간의 메시지 전송을 담당한다. 또한, 사용자의 세션 서비스(생성, 파괴, 열람, 참여) 요청을 받아, 세션관리 서버(Session Manager Server: SMS)에게 전송한 후, 그 결과를 사용자에게 제공한다. 그리고 정보관리 서버(Information Server: IS)에 접속하여 다른 UMS에 접속된 사용자간의 정보 교환 서비스를 제공한다. SMS는 세션에 대한 서비스를 UMS에게 제공하며, 협력 작업이 관한 데이터를 저장하고 있다. UMS로부터 세션 서비스 요청을 받으면, 서비스 가능 여부를 판단하여 UMS에게 그 결과를 돌려준다. 이때, 서비스 요청을 한 사용자에게 고유의 키를 제공하여, SMS에 접속 시 사용자 아이디, 암호, 키, 세션 접속 포트의 4가지가 일치하여야만 접속이 가능하도록 하였다. 키의 경우, 난수 발생기에 의해 서비스 요청을 한 사용자에게 UMS가 SMS의 출력을 받아 이를 사용자에게 제공하기 때문에, USM로부터 인증 받지 못한 올바르지 않은 사용자의 SMS 접근 방법을 차단하였다. SMS에서 공유 객체의 일관성 유지를 위해서 낙관적 로킹 알고리즘이 사용된다[10][11]. 그리고 관계형 데이터베이스와 연동되며, 우선순위 큐(Priority Queue) 스케줄링 기법을 사용하여 이벤트를 처리한다.

Ⅳ. 접근 제어 프레임워크 설계

본 논문에서 구현 모델로 택한 협력시스템의 보안 프레임워크는 크게 인증, 암호화, 접근제어, 그리고 보안 정보 관리의 네 가지 정책이 서로 상호 보완적으로 구성되어 있다. 그 중 데이터 일관성 유지와 협력 작업에서 가장 중요한 역할은 접근제어 보안 정책이다. 일반적으로 접근제어라면 사용자, 프로그램, 프로세스, 시스템 등의 인가된 주체만이 정보 시스템의 자원에 접근할 수 있도록 제한하는 것을 의미한다. 시스템 외부에서 시스템으로의 접근을 통제하는 외부 접근 제어도 접근제어 범주에 속하나 본 협력 시스템에서는 인증 정책에 포함시켰다. 따라서 본 논문에서 접근제어라 함은 허가된 사용자들이 협력시스템 내부의 자원에 대한 접근제어를 말한다. 제안된 접근제어 정책은 허가된 사용자라 할지라도 시스템내의 특정 자원에 중요도에 따라 접근을 제어하는 접근제어 작업과, 협력 작업에서의 원활한 공동작업을 위해 신분이나 직무에 따른 흐름을 제어하는 작업으로 구성된다.

접근제어에서 일반적으로 주체라고 함은 능동적으로 자원에 접근하려는 개시자를 말하며 객체는 피동적으로 접근 당하는 대상을 말하지만 본 논문에서는 명시적으로 접근을 시도하는 개시자와 접근을 수용하는 대상으로 그 개념을 제한한다.

모든 주체는 접근 정보 요소(Access Information Factor)를 가지고 있으며 주체 생성 시 접근 정보 요소가 결정되어 진다. 현재 산업 디자인 협력시스템에 맞는 필요한 접근 정보 요소는 신분, 그룹, 직무, 보안 등급, 허가권, 무결성 등급의 여섯 가지로 제한한다.

모든 객체는 접근제어 정보(Access Control Information)를 소유하고 있으며 객체 생성 시 생성된다. 접근제어 정보는 객체의 종류, 생성자, 생성 그룹, 해당 직무, 보안 등급, 무결성 등급, 소유권

의 요소로 제한한다. 이 요소들은 산업 디자인 협력 시스템에서 사용자들의 객체 접근 방법과 객체들의 접근 허용 특징에 맞게 결정되었다. 산업 디자인 협력시스템에서 보면 객체는 메시지 관리자(Message Manager), 정보관리 서버 관리자(IS Manager), 접속 관리자(Connect Manager), 탐색 관리자(Search Manager), 세션 관리자(Session Manager), 사용자 정보(User Data), 세션 리스트(Session List), 세션 데이터베이스(Session DB), 작업 도구(Tools) 등에 해당되며 공동작업 시 작업 도구들의 의한 공동작업 데이터들도 이에 속하게 된다.

1. 접근 제어 프레임워크 모델

이 절에서는 제안하는 접근제어 프레임워크의 구성 및 특징에 대하여 기술 한다. 접근제어 프레임워크는 거의 서버 모듈에서 제어를 하기 때문에 서버 모듈에만 접근제어 모듈을 추가하여 클라이언트 모듈 부분에서의 구조 변경은 최소가 되도록 하였다.

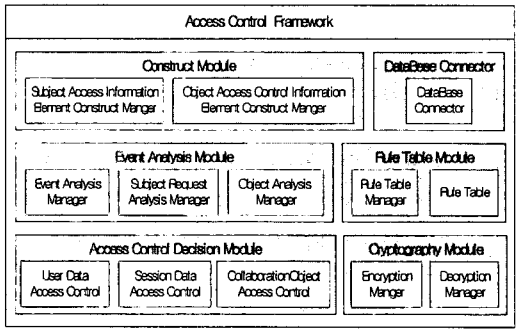


그림 2. 산업 디자인 협력시스템에서의 접근 제어 프레임워크

제안된 산업 디자인 협력시스템의 접근제어 프레임워크 구조는 그림 2에서 보여주는 것처럼 주체 및 객체의 접근 요소를 생성하는 요소 생성 모듈(Construct Module)과 주체 및 객체의 정보를 가져오기 위해 데이터베이스와 연결하는 데이터베이스 모듈(Database Connector), 이벤트 요구 발생 처리, 주체의 요구 분석, 객체의 분석을 담당하는 이벤트 분석 모듈(Event Analysis Module), 규칙 테이블을 관리하는 규칙 테이블 모듈(Rule Table Module), 접근제어 결정 모듈(Access Control Decision Module), 그리고 암호화와 복호화를 담당하는 암호 모듈(Cryptography Module)로 구성되어 있다.

요소 생성 모듈은 주체 및 객체의 생성 시 접근 요소를 자동으로 생성해주는 역할을 하고 있다. 주체는 접근 정보 요소를 갖고 있으며 객체에 접근을 할 때 필요한 요소들이다. 객체는 접근제어 요소를 갖고 있으며 주체의 접근을 제어하는데 필요한 요소들이다.

데이터베이스 연결 모듈은 객체의 접근제어 요소 및 여러 필요한 데이터를 데이터베이스로부터 가져오기 위한 모듈로서 데이터베이스의 종류에 따라 접근을 할 수 있도록 확장성을 고려하여 설계되었다.

이벤트 분석 모듈은 크게 이벤트 분석 관리자, 주체 요구 분석 관리자, 객체 분석 관리자로 이루어져 있다. 이벤트 분석 관리자는 클라이언트 등 이벤트의 발생 시 접근제어 정책이 필요한 이벤트인지 여부를 결정하게 된다. 그리고 주체 요구 분석 관리자는 주체로부터 접근 요구가 들어오는 것을 분석하여 어떤 객체를 원하는 요구인지 분석을 하며, 객체 분석 관리자는 주체에 의해 접근을 당하는 객체의 정보를 분석한다.

규칙 테이블 모듈은 규칙 테이블을 관리하는 규칙 테이블 관리자와 실제적인 규칙 테이블로 구성되어 있다. 규칙 테이블의 경우 시스템을 사용하는 사용자의 요구에 의해 변경이 가능하며 접근 요소들의 규칙 관계가 정의되어 있다.

접근제어 결정 모듈은 주체 요구 분석 관리자에 의해 어떠한 접근제어 정책이 필요한지 결정하여 실제적인 객체의 접근 여부와 접근 허용 범위를 결정하게 된다. 접근제어 결정 모듈에는 사용자 정보 접근제어, 세션 정보 접근제어, 공동작업 객체 접근제어의 세 가지 형태로 나누어진다. 암호 모듈은 각 주체, 객체 및 데이터베이스와의 통신을 암호화하며 복호화 하는 모듈이다.

그림 3은 제안된 접근제어 프레임워크를 산업 디자인 협력시스템에 추가한 서버의 구조이다. 산업 디자인 협력시스템 구현은 이벤트 중심으로 이루어지기 때문에 이벤트 관리자 부분에 접근제어 관리자가 포함되어 있도록 설계하였다. 그림 3에서 보는 바와 같이 서버 모듈에서 각 접근제어가 필요한 UMS, SMS, IS의 이벤트 관리 부분에 각각 접근제어 관리자(Access Control Manager)가 속하게 된다.

또한 시스템 외부 작업 중에도 데이터들에 대한 접근제어가 이루어지게 된다. 각각의 이벤트 관리자에 포함된 접근제어 관리자는 기본 구조는 같으나 다른 접근제어 알고리즘을 사용하게 되며 객체에 따라 나누어지게 된다. 객체들은 산업 디자인 협력시스템 내부에서 사용자에 대한 정보 및 일반 데이터, 세션 및 세션 관련 정보, 공유 작업 정보 및 공

유 작업 시 생성되는 데이터로 나누어진다. 이러한 객체의 구분은 각기 다른 알고리즘을 사용하기 위해서 분류되었으며 이는 여러 주체의 다양한 접근 레벨에 따른 확실한 접근제어를 하기 위함이다. 따라서 접근제어의 요소가 많아지지만 특징에 맞는 접근제어 알고리즘을 사용함으로 원활한 공동작업이 가능하게 된다. 객체의 정의와 구분은 각각의 협력 시스템의 특징에 맞추어 사용자가 정하여 알고리즘에 반영 한 것이다.

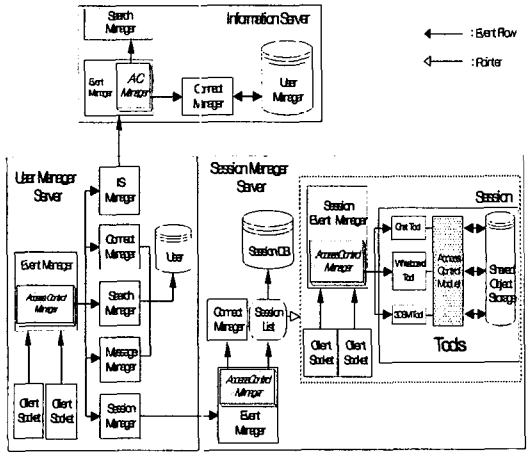


그림 3. 산업 디자인 협력시스템의 접근제어가 포함된 서버 구조

그림 4는 주체가 객체의 접근을 요구 할 때 해당 객체를 분석하여 각각의 알고리즘을 이용하여 접근하는 방법을 보여준다. 각각의 객체에 대한 분류는 다음과 같다. 사용자 정보 및 일반 데이터는 사용자의 현 상태 및 사용자의 개인 정보, 그리고 사용자의 업무 내용 등의 사용자와 관련된 상황과 게시판의 글, 자료실에 올려진 자료, 회의 내용 및 회의 결과 등의 모든 일반 데이터들을 포함하고 있다. 이 밖에도 사용자의 정의에 의한 모든 데이터로 구분한다.

세션 정보는 현재 세션의 정보, 생성, 소멸, 참여자, 세션 관찰 등 모든 세션과 관련된 정보들이다. 또한, 세션 정보 접근제어는 주체로부터 접근 요구 이벤트 발생시 대상 요구를 분석 한 후 세션 생성, 참여, 변경, 관찰의 요구로 나누어서 진행이 된다.

공동작업 정보는 세션에서 작업 툴인 3D MAX Studio의 작업 파일 및 객체 그리고 화이트보드에서의 공동작업 파일 및 객체를 말한다. 이는 사용자의 정의에 따라 공동작업을 하는 파일이나 객체까지 포함하고 있으며 공동 데이터를 작업을 할 때 접근제어를 통하여만 작업을 할 수 있도록 하였다. 공동작업 정보에 대한 알고리즘은 산업 디자인 협력시스템의 일관성 유지를 위한 동시성 제어에 근거하여 설계하였다. 또한 사용자의 요구나 필요에 따라서 공동작업을 하는 모든 데이터를 포함 할 수 있다.

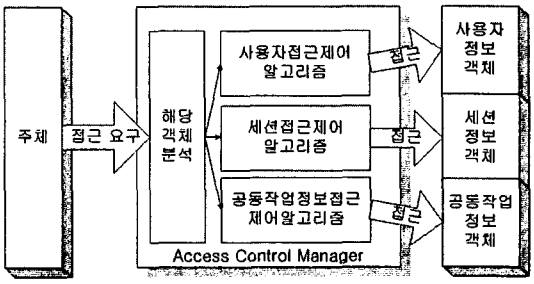


그림 4. 주체 및 객체 분류에 따른 알고리즘 관계

2. 접근 제어 알고리즘

접근제어 결정 모듈은 주체의 종류와 객체의 종류에 따라 다른 알고리즘을 사용하며, 접근제어 프레임워크에서 가장 중요한 역할을 한다. 접근속도를 증진시키기 위하여 이를 이벤트 모듈 안에 포함시키는 것이 유리 할 수도 있으나 주체와 객체의 종류와 양이 많아지면 서버의 크기가 커지기 때문에 이벤트 모듈은 외부로 분리하였다. 그리고 접근제어 결정 모듈에서는 객체의 종류에 따라 다른 접근 정보 요소, 접근제어 요소 및 접근 정보를 요구하게 되는데 이는 객체의 종류에 따라 다른 접근제어 정책이 필요하기 때문이다. 표 1은 접근제어 알고리즘에서 사용하는 접근제어 정보 인자이다.

표 1. 접근제어 알고리즘에서 사용하는 인자

M( )	접근자	RT()	규칙 테이블
I	신분	IW	무결성 등급
R	직무	O	소유권
G	그룹	P	허가권
S	보안 등급		

1) 사용자 정보 접근제어 알고리즘

그림 5는 사용자 정보 및 일반 데이터의 접근제어 알고리즘이다. 객체의 종류는 주체로부터 객체에 대한 접근 요구 이벤트가 들어왔을 때 요구되는 종류에 따라 일반 데이터(라인 1), 보안 데이터(라인 15), 데이터 변경(라인 20)의 세 가지로 분류된다.

```
1   Permit_GeneralData_Access =
2     TRUE :  if (M(I) >= RT(I))
3               Access_Rule_All_data
4               return
5             if (M(R) = RT(R) and M(G) = RT(G))
6               Access_RGRule_All_data
7               return
8             if (M(R) = RT(R))
9               Access_RRule_data
10              return
11            if (M(G) = RT(G))
12              Access_GRule_data
13              return
14    FALSE : Uesr Define access
15  Permit_SecretData_Access =
16    TRUE :  if (M(S) >= RT(S))
17              find (M(S) = RT(S))
18                Access_Rule_data
19    FALSE : Uesr Define access
20  Permet_ModifyData_Access =
21    TRUE :  if (M(IW) >= RT(IW))
22              find (M(IW) = RT(IW))
23                Access_Rule_data
24    FALSE : Uesr Define access
```

그림 5. 사용자 정보 접근제어 알고리즘

일반적인 데이터의 접근을 시도할 때 실행되는 부분은 주체의 신분과 객체의 신분을 비교하며 규칙에 맞을 시 허용된 범위의 데이터에 접근하도록 하였다. 그리고 직무와 소속 그룹이 모두 규칙에 맞을 때 허용 데이터에 접근하도록 되어있으며, 다른 하나는 소속 그룹에만 맞는 경우 허용 데이터에 대한 접근제어가 가능하도록 하였다(라인 2~14). 그리고 중요 데이터에 대한 접근일 경우 실행되는 부분은 이는 주체의 보안 등급을 비교하여 맞는 규칙을 찾은 다음 데이터에 접근을 하도록 하였다(라인 16~19). 그리고 데이터의 변경 및 수정, 삭제의 경우에 실행되는 부분은 무결성 등급을 비교하도록 하였다(라인 21~24). 객체에 대한 접근은 허가된 범위 이내에서만 가능하도록 하고 있다. 접근 종류에 따라 다른 접근 요소가 필요할 경우 다른 알고리즘을 사용하며, 접근제어가 거부되었을 때에는 시스템 사용자가 원하는 방향으로 결과를 처리 할 수 있도록 하였다. 그리고 접근이 가능하더라도 미리 정해둔 규칙의 범위 안에서만 접근이 가능하도록 되어 있다. 접근이 불허되었을 경우에는 일반적으로 불법 접근으로 간주되며 기록으로 저장되지만 사용자의 요청이 있는 경우 접근이 불허되었을지라도, 사용자 정의 등에 따라 통보 가능한 방식을 취하였다. 이는 산업 디자인 협력시스템의 데이터와 사용자의 특징을 분석하여 결정한다.

2) 세션 정보 접근제어 알고리즘

협력 작업에서 세션의 생성 및 관리는 중요하다. 불법적인 사용자에 의해 세션이 생성되고 관리되거나, 허가되지 않은 사용자에게 정당하게 생성된 세션이 파괴되거나 불법적인 사용자에게 세션이 노출된다면 심각한 피해를 입을 수 있다. 따라서 일반 데이터보다 보안의 요건을 더 강화하여 설계하였다. 세션 정보접근제어는 세션에 대한 정보, 세션의 참여, 저장 등 여러 부분에서 접근제어를 실시한다.

```
1   Permit_SessionCreate_Access =
2     TRUE :  if (M(I) >= RT(I)  or M(S) >= RT(S))
3               Access_Create_Session
4     FALSE : Uesr Define access
5   Permit_SessionJoin_Access =
6     TRUE :  if (M(R) = RT(R))
7               Access_Join_Rule_Session
8             if (M(G) = RT(G))
9               Access_Join_Rule_Session
10    FALSE : Uesr Define access
11  Permit_SessionObserve_Access =
12    TRUE :  if (M(S) >= RT(S))
13              Access_Oberce_Session
14    FALSE : Uesr Define access
15  Permit_SessionUpdate_Access =
16    TRUE :  if (M(IW) >= RT(IW)  or M(O) = RT(O))
17              Access_Update_Rule_Session
18            if (M(R) = RT(R)  or M(G) = RT(G))
19              Access_Update_Rule_Session
20    FALSE : Uesr Define access
```

그림 6. 세션 정보 접근 제어 알고리즘

그림 6은 세션 정보 접근제어 알고리즘을 보여준다. 주체가 세션에 대한 접근 방식에 따라 다른 접근제어 결정을 하게 된다. 세션 생성 시에는 신분과 보안 등급과 규칙 테이블과의 규칙 여부를 따지게 되며 (라인 2~4), 세션의 참여는 불법 침입자를 막기 위해 직무와 소속 그룹을 규칙 테이블과 비교하게 된다(라인 6~10). 세션의 관찰은 보안 등급을 비교하게 되며(라인 12~14), 세션의 삭제나 변경은 무결성 등급, 소유권 여부, 직무와 소속 그룹을 비교해야 한다(라인 16~20).

이 알고리즘은 산업 디자인 협력시스템의 특징에 맞게 설계된 것으로 사용자에 의해 추가 접근제어가 가능하도록 확장성을 고려하였다. 세션의 생성은 허가된 사용자가 비교적 쉽게 생성 할 수 있으나 불법적인 생성은 방지하였다. 세션 참여의 경우 사용자의 접근 제어 요소에 따라 참여, 변경, 관찰 등의 다른 참여 규칙이 정해지므로 세션 참여가 가능한 사용자로 신분을 위장하는 방법으로는 모든 세션 정보를 유출하기 어렵기 때문에 보안에 효과적

이다. 세션 모듈에서 가장 중요한 곳은 세션 변경을 담당하는 부분으로 세션의 불법 삭제 및 변경, 유출을 방지한다.

3)공동작업 정보 접근제어 알고리즘

사용자가 공유 객체를 많이 사용하는 협력시스템의 경우 접근제어 서비스 모듈은 보안 측면뿐 아니라 협력 작업에서도 필요하다. 세션의 참여가 접근제어로 이루어져 있지만 실제 세션에 참가해서 공유데이터를 가지고 작업을 하는 경우 접근제어는 다른 특징을 가지게 된다. 일관성 유지와 공동작업의 흐름을 원활하게 해주는 공동작업 정보 접근제어 알고리즘은 이벤트 매니저 안에 삽입되어 구현된다.

```
1   Permit_CreateData_Access =
2       TRUE : if (M(P) = RT(P))
3                 Access_Create_Data
4       FALSE : Uesr Define access
5   Permit_UpdateDate_Access =
6       TRUE : if (M(O) = RT(O) and M(IW) >= RT(IW))
7                 Access_Update_Rule_Data
8       FALSE : Uesr Define access
9   Permit_ExcuteDate_Access =
10      TRUE : if (M(O) = RT(O) and M(S) >= RT(S) or M(I) >= RT(I))
11                Access_Excute_Rule_Data
12      FALSE : Uesr Define access
```

그림 7. 공동작업 정보 접근제어 알고리즘

그림 7에서는 공유 객체를 다루는 부분에서 데이터의 생성 및 업데이트, 실행에 관해서 접근자의 소유권, 무결성 등급 등을 규칙 테이블의 정의된 규칙과 비교하여 행동을 제어하는 공동작업 정보 접근제어 알고리즘을 보여준다. 공유 객체는 생성자를 명확히 밝히고 공유 객체에 접근할 수 있는 소유권 변경이 원활해야 한다. 공동 작업 정보에 대한 주체의 접근 요청이 있을 때 공동 작업 객체의 생성, 변경, 실행으로 나누어서 주체의 접근을 제어한다. 객체의 생성이나 변경, 실행에 대한 규칙은 일관성 유지를 위한 동시성 제어를 기본적으로 하며 직무에 맞는 규칙을 정해두어 서로 연관성 있게 구성되었다. 공유 객체를 생성하기 위한 접근제어 부분은 객체나 파일 등을 생성할 수 있는 허가권을 얻어야 한다(라인 2~4). 데이터의 업데이트를 위한 접근제어 부분은 데이터의 삭제, 변경 등이 포함되며 소유권, 무결성 등급을 비교하게 된다. 그리고 규칙에 맞는 업데이트만을 허용하게 된다(라인 6~8). 데이터의 실행에 관한 접근제어를 나타내는 부분은 소유권, 보안 등급, 신분을 비교하여 데이터에 접근을 허용하도록 하고 있다(라인 10~12). 그 외의 접근은 원활한 작업을 위해 시스템 설계 시 사용자들의 요구에 따른 접근이 가능하도록 하였다.

V. 시스템 구현 환경 및 성능 평가

1. 시스템 구현 환경

구현된 산업 디자인 협력시스템의 서버는 자바로 구현이 되어 있으며, 클라이언트는 C++ 및 MFC로 구현되었다. 개발한 접근제어 프레임워크의 구현 환경은 표 2와 같다.

표 2. 접근제어 구현 환경

항목	환경
운영 체제	Window 2000 Server 및 NT 4.0
구현 환경	Pentium II 300MHz, RAM 256MB
개발 언어	Java 1.3.x

구현 시스템은 개발된 산업디자인 협력시스템의 서버에 새로운 모듈을 추가하며, 규칙 테이블 구성과 객체 및 주체 생성 시 자동으로 접근 요소를 생성하도록 하였다. 구현시스템에서 모든 작동은 이벤트를 통하여 이루어지기 때문에 추가된 모듈은 서버의 핵심부분인 이벤트 처리 모듈, 통신 모듈과 밀접한 관계를 갖게 하며 접근제어 모듈은 UMS, SMS, IS에서 공통으로 사용될 수 있도록 하였으나 각 서버의 특징에 맞는 모듈은 빠른 처리 속도를 위해 일부분은 이벤트 관리 모듈 안에 삽입하였다.

객체 생성 시 접근제어 정보도 함께 생성이 되는데 이는 규칙 테이블에 정의된 내용을 토대로 한다. 명칭은 상황과 산업디자인 협력시스템을 사용하는 사용자가 정의하는 것으로 조직의 구조적 특징에 따라 변경하면 다른 시스템에서도 사용할 수 있을 것이다. 접근제어 결정 모듈에는 규칙 테이블을 소유하게 되는데 규칙 테이블의 정의된 내용도 시스템 설계 시 사용자가 정의할 수 있으며, 규칙 테이블과 주체의 접근 정보, 객체의 접근제어 정보를 이용하여 접근제어를 결정한다.

기존의 접근 제어 정책의 경우 접근을 결정하려는 요소는 신분, 직무, 역할, 혹은 직무와 역할 등 한 가지 혹은 최대 두 가지였다. 하지만 협력시스템과 같이 복합적인 상황에서 두 가지의 요소만으로는 효과적인 접근제어를 할 수가 없다. 신분 기반 접근제어의 경우 사용자의 신분에 의존하여 접근을

제어하기 때문에 생성되는 객체의 중요성을 결정할 수 없었다. 따라서 신분이 상위에 있는 사용자는 신분에 맞는 어떠한 정보도 불법으로 접근 할 수 있었다. 규칙 기반 접근제어의 경우 주체와 객체간의 관계에 의존하는 정책으로 모든 주체와 객체간의 정책을 포함하고 있어야 하지만 산업디자인 협력시스템의 경우 공동 협력 작업 시 발생하는 데이터 일관성 유지와 원활한 공동 작업수행에 많은 문제점이 발생하였다. 역할 기반 접근제어의 경우 개별의 신분 보다 자신의 직무에 따라 접근제어를 하였기 때문에 협력 작업을 하지 않는 일반 사용자 및 그룹 소속 사용자는 필요한 정보에 접근하지 못하였다.

따라서, 주체와 객체 각각의 구분에 따른 새로운 정의가 필요하였고, 접근제어 요소의 수를 앞에서 언급한 바와 같이 각각 여섯 가지로 구분하였다. 제안한 접근제어 정책에서는 요소의 수가 증가하였지만 주체와 객체 사이에 각기 다른 접근제어 요소만을 이용함으로 시스템 성능을 유지하면서 확실한 접근제어를 할 수 있게 되었다. 객체의 경우, 사용자 정보 및 일반 정보 접근, 세션 정보 접근, 공동작업 공유 데이터 접근의 세 가지로 구분하였는데 각각의 객체는 산업디자인 협력시스템의 특징에 맞게 정의 내려진 것으로 객체의 특징에 맞는 다른 알고리즘을 사용하여 처리 능력의 향상을 이루었다. 제안된 접근제어 프레임워크 및 정책은 산업 디자인 협력시스템이라는 특정 응용 시스템에 맞는 보안 방식 설계 되었지만 유사한 협력 시스템으로 확장이 가능하다. 이 경우, 접근제어 프레임워크를 유지하며 객체의 분류를 다른 협력 시스템의 특징에 맞도록 변경함으로 다른 유사한 협력시스템에서 응용을 할 수 있다.

2. 성능 평가

평가 항목은 크게 두 가지로 나누어서 설정하였다. 산업디자인 협력시스템의 접근제어 정책은 강력한 보안의 기능과 함께 협력시스템이라는 특성상 원활한 작업을 만족해야 하기 때문에 접속자 수에 따른 이벤트 처리 속도와 실질적으로 불법적인 접근에 대한 접근제어 측정의 두 가지 항목으로 접근제어 정책을 평가하였다. 협력시스템 내부에 접근제어가 포함되어 있지 않는 경우 이벤트 발생에 따른 접근자 수에 대한 처리 속도를 측정하고, 또한 접근제어가 포함되어 있는 경우 접근자 수에 대한 이벤트 처리 속도를 측정한 뒤 이를 비교하여 지연 여부를 관찰한다. 이는 접근제어를 할 경우 사용자가 느끼게 되는 제어에 대한 평가를 하기 위함이다. 그리고 확실한 접근제어를 측정하기 위하여 불법 접근 가능성이 있는 몇 가지의 시나리오를 가지고 불법적인 접근에 대하여 실질적인 제어가 되는지 여부도 알아본다. 접근제어 프레임워크의 성능을 평가하기 위한 평가 환경 및 항목은 표 3과 같다.

표 3. 접근제어 성능 평가 환경 및 평가 항목

항목	환경
운영 체제	-Window NT 4.0
구현 환경	-Pentium II 300Mhz, RAM 224MB
소프트웨어 환경	-서버 : 자바 1.3 -클라이언트 : MS VC++ -이벤트 발생 : Java Tread
평가 항목	-접속자 수에 따른 이벤트 처리 속도 측정 및 비교 -합법적인 사용자로 시스템 내부의 불법 접근 시도

처리 속도 측정은 접근제어 프레임워크 모듈이 없는 기존 협력시스템에서 주체의 이벤트 발생으로부터 이벤트에 대한 응답을 받는 속도를 측정을 한 후, 접근제어 프레임워크를 포함하여 이벤트 발생부터 응답을 받을 때까지의 속도를 비교하게 된다.

그림 8은 60초 간격으로 사용자가 일반 데이터인 자료실의 정보를 얻는 이벤트를 발생시켜서 응답을 받는 시간을 측정한 것으로 이 경우 사용자 접근제어 알고리즘을 이용하게 된다. 시스템 반응시간은 접근제어가 포함되지 않은 시스템에서의 사용자가 자료실 정보에 대한 이벤트를 발생 시켜서 응답을 받는 시간을 말하는 것이며, 접근제어 포함 반응시간은 시스템에 접근제어 모듈을 포함시켜서 같은

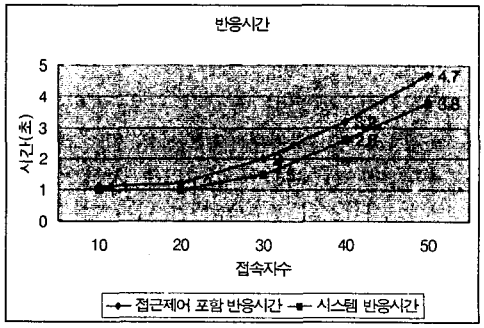


그림 8. 60초마다 일반 정보 이벤트 발생에 따른 반응시간

이벤트로 응답을 받는 시간을 말한다. 그림 9와 그림 10은 클라이언트에서 사용자가 화이트보드를 사용하여 객체를 생성하였을 경우, 서버에서 객체의 정보를 저장하고 다시 응답을 하여 클라이언트에서 응답을 받는 시간을 측정하였으며 접근제어 포함 반응시간의 경우 접근제어 모듈을 포함하여 같은 이벤트를 60초 및 30초 간격으로 발생 시켜서 응답을 받는 시간을 측정을 한 것이다.

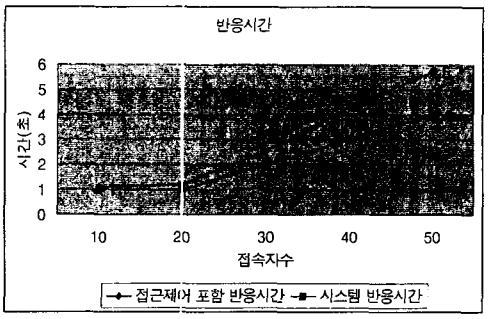


그림 9. 60초마다 세션 이벤트 발생에 따른 반응 시간

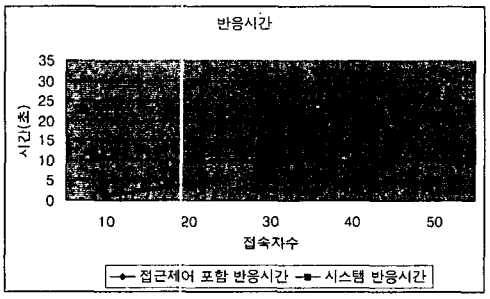


그림 10. 30초마다 세션 이벤트 발생에 따른 반응 시간

접근제어 모듈이 포함되어있을 경우 원래 시스템의 반응 시간에 비해 모든 환경에서 적게는 0.1초에서 2초의 지연이 발생하였다. 접속된 사용자가 10명 이내일 경우 사용자는 거의 지연 시간을 느끼지 못할 것이다. 하지만 50명의 접속자가 있을 경우 2초의 지연시간이 생성되는데 이는 접근제어를 하기 위해 접근 요소를 데이터베이스에서 읽어오는 시간이 점차 늘어나기 때문에 야기되는 현상으로 시스템과 데이터베이스의 종류에 따라 달라 질 수 있다.

두 번째 평가 항목의 경우 협력시스템 내부의 합법적인 사용자라 하더라도 접근 불가능한 정보에 대하여 접근이 가능한지를 평가하는 항목이다. 이 경우 여러 가지 평가 방법이 있을 수 있으나 산업디자인 협력시스템에서 세션 정보에 대한 접근제어가 가장 중요하기 때문에 세션 정보에 대한 불법 접근제어가 가능한지 여부를 설정하였다. 또한, 산업디자인 협력시스템의 경우 외부로부터의 불법 접근은 인증과 암호화 모듈에서 담당하므로 평가에서 제외하였다. 불법 접근 시도의 경우 내부의 합법적인 사용자에 의한 시스템 정보 유출의 경우로만 한정하여 평가하였다. 모델이 된 산업디자인 협력시스템의 경우 한 회사에서 디자인 프로젝트를 진행할 경우 개발기획그룹, 디자이너그룹, 개발자그룹으로 나누어지며, 같은 소속의 그룹일 경우에도 업무에 따라 각기 다른 직무에 관여하게 되어 있었다. 이런 상황에서 다른 그룹의 높은 직급을 가진 소유자나 같은 디자이너그룹의 인원이라 할지라도 각각의 업무 이외의 다른 세션 정보에는 제한을 가해야 하는 상황들이 발생하였다. 기존의 보안등급을 이용한 접근제어의 경우 높은 직급을 가진 사람은 보안 등급이 높아서 아무런 제재 없이 세션에 참여하거나 세션 정보의 변경이 가능했다. 또한 그룹별 접근제어 정책만을 이용하여 접근제어를 할 경우 같은 소속의 그룹에 포함된 사람들은 직무와 상관없이 소속 그룹의 모든 세션에 접근이 가능하였다. 직무별로 접근제어를 할 경우에는 소속 그룹이 없는 높은 직급의 관리자가 세션에 참여나 세션의 관리를 하지 못하는 경우가 발생하였다. 그러나 제안된 접근제어 정책에서는 첫째, 보안등급이 높은 사용자의 아이디를 이용한 세션 정보 취득 가능성 여부 둘째, 보안등급, 신분, 무결성 등급이 높은 사용자의 아이디를 이용하여 세션의 참여의 여부 셋째, 보안등급, 신분 등급이 높은 사용자의 아이디를 이용하여 세션 정보 변경 가능성 여부에 대하여 실험을 하였다.

표 4의 결과처럼 보안등급, 신분 등이 높을 경우라도 세션 정보 취득이외의 다른 정보를 얻지 못하였다(ID1). 그리고 같은 그룹이나 높은 보안 등급이나 신분을 갖고 있더라도 다른 직무의 정보는 얻지 못하였으며(ID4), 세션의 참여나 변경은 직무나

표 4. A-Project에 대한 세션 생성 시 각 아이디에 대한 접근 허용 결과

아이디(보안등급, 신분, 소속그룹, 직무, 무결성 등급)	세션 참여	세션 변경	세션정보 취득
ID1 (1, 1, A, M, 2)	x	x	o
ID2 (3, 3, D, P1, 1)	o	o	o
ID3 (3, 3, M, P1, 3)	o	x	o
ID4 (2, 1, D, P2, 1)	x	x	x

무결성 등급에 의해 정해진 규칙에 의한 접근만을 허용하였다(ID2,ID3). 기존의 접근제어를 이용하였을 경우 접근제어가 불가능했지만 제안된 접근제어에서는 합법적인 내부 사용자의 불법적인 접근에 대하여 차단할 수 있었다.

또한, 위에서 정의된 방식이외에 다른 방식으로는 패킷을 임의적으로 변경하는 방식이 있다. 이 방식은 만일 위에서 해당되는 아이디로 클라이언트에서 보내지는 패킷을 변경하여 접근이 가능하도록 가장하는 경우를 생각해 볼 수 있다. 이 경우는 두 가지 이유로 접근이 불가능하게 된다. 첫째, 자신의 접근 정보는 서버에서 관리를 하기 때문에 자신의 보안 등급을 높이거나 무결성 등급을 변경시킬 수 없다. 즉 자신의 아이디로는 접근이 불가능 하게 되어 자신의 신분을 상승시키는 패킷변경은 있을 수 없다. 둘째, 접근이 가능한 다른 사람의 아이디를 도용하여 패킷을 변경하는 경우가 있다. 이는 각 클라이언트 및 각 사용자에게 다른 비밀키를 사용하기 때문에 패킷을 변경하려면 변경하려는 아이디의 비밀키까지 소유하여야 한다. 따라서 자신의 패킷의 변경만으로는 접근이 불가능함으로 성능평가 항목에서 제외하였다.

성능 평가 항목에서 지연 시간의 측정의 경우 측정 방식에 대한 일반적인 방식과 규정이 정해져 있지 않으며, 또한 측정 결과에 대하여 판단할 수 있는 기준이 없기 때문에, 본 논문에서는 접근제어 모듈이 포함되어서 생길 수 있는 시간을 기준으로 하였다. 측정 결과의 판단 기준은 협력시스템을 사용하는 사용자들로부터 시연 시간 차이로 인해 공동작업에 미치는 영향 등, 실질적인 사항을 기준으로 하였다. 또한, 불법 접근에 대한 평가 기준은 실질적으로 일어날 수 있는 경우를 정의하여, 정의된 상황에서의 접근제어 판단 여부를 기준으로 하였다.

Ⅵ. 결론 및 향후 연구

본 논문에서는 협력시스템에 개입된 주체들 사이의 가장 심각한 위협요소인 불법적인 위·변조, 도청, 신분위장 및 재전송 등으로부터 시스템의 안정성을 확보하기 위하여 산업디자인 협력시스템에 맞는 보안 정책 중 접근제어에 대하여 논의하였다. 그리고 분산 환경, 개방된 네트워크, 다양한 종류의 사용자와 여러 종류의 객체를 가지고 있는 협력시스템의 특징에 맞는 접근제어 정책을 제시하였다.

주체의 경우 여러 접근제어요소를 사용하도록 하였고 객체의 경우 특징에 맞도록 분류를 하였다. 또한 여러 접근제어요소를 효과적으로 사용하기 위하여 각 객체의 종류에 따라 다른 새로운 알고리즘을 사용하여 빠른 접근제어 정책 적용과 확실한 접근제어를 할 수 있도록 하였다. 객체 및 주체의 접근제어 정보와 접근 정보는 다른 협력시스템에서 구조와 특징에 맞게 변경 가능하면 이용 가능하게 확장성을 고려하였고, 미리 정해둔 규칙 테이블의 경우 시스템을 사용하려는 사용자의 요구에 따라 구성하여 맞는 보안 정책을 펼칠 수 있도록 하였다.

구현된 산업디자인 협력시스템의 접근제어 정책은 기존의 정책에 비해 구체적인 접근제어 방법을 제시하였으며, 복합적인 상황과 불법적인 접근에 대한 확실한 접근제어가 가능하게 하였다. 또한, 이기종 산업디자인 협력 작업에서 제안된 접근제어 프레임워크를 이용하여 시스템 특징에 맞도록 접근요소 및 정책 변경이 용이하도록 확장성을 고려하였다. 모의실험 결과 여러 접근 요소를 이용하였지만 접근제어 정책을 적용하지 않았을 때와 성능 면에서 큰 차이를 보이지 않았다.

향후 연구로는, 본 산업디자인 협력시스템의 경우에 윈도우즈, NT 환경의 협력시스템으로 운영체제 내부의 다른 접근제어 정책과의 연동이 없었다. 하지만 유닉스 환경의 협력시스템으로 구성할 경우 운영체제 자체의 접근제어 정책과도 충분한 연동이 예상되며 운영체제가 제공하는 접근제어 정책과 연동을 이용하여 보다 빠르고 저차원 적인 접근제어 정책을 구성할 수 있도록 하는 방향이 필요하다. 또한, 이러한 보안 정책을 변화에 맞게 변경 및 유지 보수를 위한 툴을 개발이 필요하며 다른 협력시스템과 연동 시 데이터 전송 시 사용자의 요구에 따라 다른 비밀성과 무결성 지원하기 위한 QoP (Quality of Protection) 서비스를 고려하여야 한다. 그리고 모든 정보 보호 서비스를 고려하기 위한 협력시스템을 위한 전체적인 보안 플랫폼에 관한 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] 강창구, 박징호, 최용락, "통합정보 모델을 이용한 접근제어 메커니즘 설계 및 구현", *한국 정보처리학회 논문지* 제4권 제9호 pp 2354-2365, 1997.9

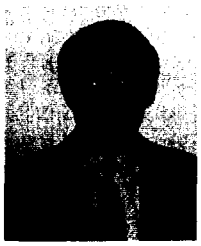
[2] "http://www.dcs.qmw.ac.uk/research/distrib/Mushroom/"

[3] "ftp://ftp.cs.unc.edu/pub/users/dewan/papers/"
[4] CORBA Security Service Specification, pp. 2-1~2-168 , 2000.5
[5] Philip M. Johnson. "Experiences with EGRET :An exploratory group work environment", Collaborative Computing, 1994.1
[6] "http://www4.informatik.uni-erlangen.de/Projects/promondia/"
[7] Annie Chabert, Ed Grossman Larry Jackson, Stephen Pietrovicz, "NCSA Habanero: Synchronous Collaborative Framework and Environment", 1998
[8] "http://www.teamwave.com/"
[9] 양진모, 이승룡, 전태웅 "확장성을 고려한 산업디자인 협력시스템 설계 및 개발", *한국 정보과학회 논문지*, , pp 513-528. 2000년 9월
[10] M.T. Ozsu and P. Valduriez. "Principles of Distributed Database Systems. Prentice- Hall", pp. 327~329, 1998.
[11] S. Bhola, G. Banavar, and M. Ahamad, "Responsiveness and consistency tradeoffs in interactive groupware", I*n Proceedings of 7th ACM Conference on Computer Supported Cooperative Work*, November 1998.
[12] Ravi Sandhu, "Access Control : The Neglected Frontier, Proc. First Australasian Conference on Information Security and Privacy", Wollong, Australia, 1996.6
[13] Ravi S. Sandhu, "Role-bsed Access Control", Laboratory for Information Security Technology ISSE Department, MS 4A4 George Mason University, 1997.9
[14] Vijay Varadharajan, Chris Crall, Joe Pato, "Issues in the Design of Secure Authorization Service for Distributed Applications", Proceedings of the Globecom '98 - Volume 2 , pp. 874-879 , 1998.11.08
[15] Adrian Bullock, Steve Benford, "An Access Control framework for multi-level collaborative environments", Department of Computer Science University of Nottingham NG7 2RD, UK, 1999.11

정 연 일(Yonil Zhung) 정회원

1998년 2월 : 수원대학교 물리학과 졸업
2000년 8월 : 경희대학교 전자계산공학과 석사
2000년 9월~현재 : 경희대학교 전자계산공학과 박사과정
<주관심 분야> 시스템 및 네트워크 보안

이 승 룡(Sungyoung Lee) 정회원



1978년 2월 : 고려대학교 재료공학과 졸업
1986년 12월 : Illinois Institute of Technology 전산학과 석사
1991년 12월 : Illinois Institute of Technology 전산학과 박사
1991년 9월~1993년 8월 : Governors State University 조교수
1993년 9월~현재 : 경희대학교 전자계산공학과 교수
<주관심 분야> 실시간 컴퓨팅, 실시간 미들웨어, 멀티미디어 시스템, 시스템 보안