▩ 연구논문

미들웨어상에서 데이터베이스 인증시스템에 관한 연구

A Study on Database Authentication System in Middleware

최 진 탁
Choi, Jin Tak

Abstract

The Gateway Server Authorization System(GSAS) presented in this thesis is a database authorization system. GSAS is resposible for user's authorization, and privilege management, audit service. Only users that are filtered in GSAS can access the DBMS(Data Base Management System) through middleware. GSAS is located at the DBMS and already contains an authorization record for user accessing a specific DBMS. GSAS on consists of several components, namely an authorization manager, a privilege manager, and an audit manager. As an authorization manager and a privilege manager can only approve a pass at the same time, a user can get accessiblity for DBMS.

1. 서 론

기존 데이터베이스의 보안사항이 이전 환경에서 큰 위협이 되지 아니하였으나, 클라이언트/서버 환경에서는 이러한 위협들-인가되지 않은 자의 접근 및 인가되었으나 적의나 악의를 가진 사용자-로부터 목표가 될 수 있다.

본 논문에서 제안하는 보안시스템은 클라이언트/서버 환경에서 미들웨어를 이용해서 호스트에 접근한 사용자에 대하여, 존재하는 데이터베이스를 침입자로부터 보호하려는데 그 목적을 두고 있다. 또한 게이트웨이에서부터 사용자들을 관리하여 호스트나 데이터베이스에 접근하기 전에 미리 정의된 인증 레코드에 의해서 호스트나 데이터베이스의 접근을 통제한다. 즉 GSAS(Gateway Server Authentication System)는 지역 게이트웨이에 인증 시스템을 구축함으로써 침입자의 데이터베이스 접근을 다단계로 통제할 수 있다.

Gateway Server는 GSM(Gateway Server Manager)에게 필요한 정보를 알려야 한다. GSM은 Gateway Server의 Administrator로써 모든 데이터베이스 접근에 관련된 사용자들을 관리한다. GSM은 인증관리자, 권한관리자, 감사관리자로 구성되어 있으며, 인증관리자는 사용자의 인증을 관리하고, 권한관리자는 사용자의 권한관리, 감사관리자는 사용자의 로그 인부터 로그아웃까지의 감사기능을 수행한다. DBMS(Data Base Management System)는 데이터베이스의 모든 것을 관리하지만, 제안시스템인 GSAS는 시스템과 데이터베이스의 연결을 감독하며, 미들웨어를 이용해서 접근하는 사용자들을 통제한다. 본 논문을 통해서 GSAS을 제안하고, 향후에 OODB(Object oriented Data Base), ORDB(Object Relational Data Base)와 같은 다른 종류의 데이터베이스를 폭넓게 관리할 수 있도록 구축한다.

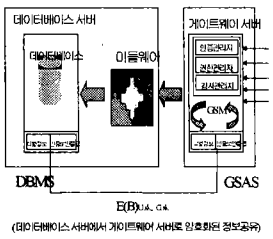
2 Gateway Server 인증시스템 구현

2.1 Gateway Server

컴퓨터가 널리 보급됨에 따라 지리적으로 분산되어 있는 컴퓨터 자원을 효율적으로 이용하기 위해 컴퓨터 통신망 기술이 발전하게 되었다. 컴퓨터 통신망은 컴퓨터 자원의 공동 이용과 컴퓨터 시스템의 신뢰도를 향상시키기 위해 지리적으로 분산되어 있는 컴퓨터들을 통신회선으로 결합한 것으로, 컴퓨터 통신망의 사용자들이 다른 지역에 있는 정보와 자원을 공유하여 사용할 수 있도록 해주는 것이다.

그러나 이러한 정보와 자원의 공유는 불안전한 통신채널을 통해 이루어지기 때문에 권한을 부여받지 못한 사용자들이 정보를 도청하여 변형, 삽입 및 삭제하여 악용하는 새로운 문제점이 대두되었으며 이를 대처하기 위한 보안 연구가 크게 부각하게 되었다.

컴퓨터 통신망에서의 보안문제는 크게 정보의 비밀보장과 사용자의 인증 보장의 두 가지 문제로 나누어 생각할 수 있다. 컴퓨터 통신망의 사용자는 이러한 두 가지 문제를 자동적으로 해결해 줄 수 있는 메커니즘을 필요로 하는데 이를 위한 가장 대표적인 암호화 시스템이 바로 인증 서버(authentication server)이다.



(그림 1) 사용자의 대한 인증 레코드 구축

게이트웨이 서버 인증 시스템은 클라이언트/서버 환경에서 특정한 데이터베이스 서버에 미들웨어를 이용해서 접근하는 사용자를 지역 게이트웨이 수준에서 인증, 권한관리, 감사한다. 네트워크 상에서 정당한 사용자나 부당한 사용자는 미들웨어를 이용해서 데이터베이스를 접근하기 위해서는 지역 게이트웨이를 경유하여 데이터베이스 서버에 접근하게 된다. 지역 게이트웨이 서버에 게이트웨이 서버 관리자(GSM)를 두고 인증관리자, 권한관리자, 감사관리자를 운영한다. 게이트웨이 서버 관리자는 지역 게이트웨이에서 특정 데이터베이스 서버와 인증 레코드를 전달하면서 항상 최근의 식별정보와 인증보안등급 정보를 구축한다. 지역 게이트웨이에 구축된 데이터베이스 식별정보와 인증보안등급을 바탕으로 GSM은 지역 게이트웨이 서버에서 데이터베이스에 접근하는 부당한 사용자를 검출하여 지역 게이트웨이 서버에서 미들웨어를 이용한 데이터베이스 접근을 통제한다.

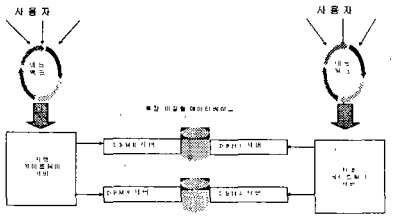
2.2 이질형 분산 데이터베이스에서의 보안

강제적인 보안정책과 임의적인 보안 정책이 통합 운영되어야 할 강결합된 이질형 분산 데이터베이스 시스템의 보안 요구사항과 연산은 새로운 연구분야로서 해결해야 할 문제들이 산적해 있다. 이질형 분산 데이터베이스의 목적은 사용자로 하여금 여러 개의 하부 요소를 구성하는 데이터베이스들의 자료에 접근, 병합 및 갱신을 실행할 수 있게 하는데 있으므로 자료 접근에 대한 액세스 제어는 이질형 분산 데이터베이스의 전역 보안 정책뿐만 아니라 참가하는 사이트의 지역 보안 정책의 결합도 강약에 크게 의존한다. 보안기법은 전역보안연합에 가입하거나 탈퇴하는 개별 사이트의 자치성과 각 사이트의 자료 공개 정책의 변경 여부에 영향을 받게 된다. 또한 하부 요소 데이터베이스들의 이질성에 의해서 이질형 데이터베이스들의 보안기법은 더욱 복잡해진다. 사이트에 따라 서로 다른 보안 정책들을 하나로 통합하는 것은 매우 어렵고 일관성을 유지하기도 힘들다. 미들웨어를 이용한 데이터베이스 사용자의 인증에 따른 다수의 서로 다른 특정 데이터베이스들로의 접근을 게이트웨이로부터 통합적으로 액세스 제어를 수행할 수 있다.

컴퓨터 통신망의 사용자가 컴퓨터 통신망을 사용하기 위해서는 먼저 자신이 컴퓨터 통신망을 사용하겠다는 것을

알려야만 한다. 그러면 컴퓨터 통신망은 그 사용자가 과연 컴퓨터 통신망의 정당한 사용자인지를 판정하여 사용해도 좋다는 허가를 내려주게 된다.

이렇게 컴퓨터 통신망이 정당한 사용자인지를 판정하는 과정을 주로 사용자가 현재 소속되어 있는 게이트웨이 서버의 보안 메커니즘에 의하여 사용자가 처음 지역 게이트웨이를 액세스할 때 수행이 된다. 만일 사용자가 현재 자신이 속해 있는 게이트웨이 서버가 아닌 다른 게이트웨이 서버 정보나 자원을 이용하는 경우에도 마찬가지로 사용자는 컴퓨터 통신망을 통하여 다른 게이트웨이 서버에게 자신을 알리고 그 게이트웨이 서버가 아닌 다른 게이트웨이 서버의 정보나 자원을 사용할 수 있는지의 여부를 결정하여 통보를 해주게 된다.

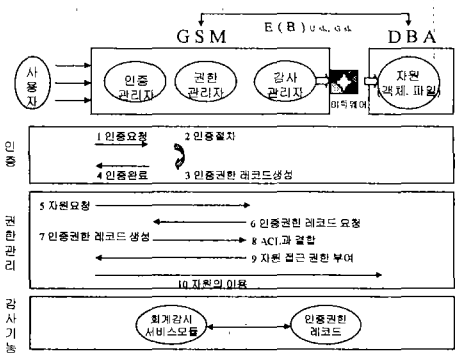


(그림 2) 이질형 분산 데이터베이스에
대한 게이트웨이 미들웨어 방식

위 (그림2)에서 네트워크에서 접근하는 사용자들은 이질형 데이터베이스에 접근하기 위해서는 반드시 지역 게이트웨이를 경유해서 DBMS서버의 인증을 받아 데이터베이스로 접근해야 한다. 이러한 경우에는 지역 게이트웨이에서는 악의의 가진 사용자든지 정의의 가진 사용자든지 인증을 거치지 않고 DBMS 서버에서만 인증을 하게 된다.

인증 서버를 이용하여 인증을 할 경우에 인증 서버는 물리적으로 안정하다고 가정한다. 왜냐하면 인증서버에는 사용자들을 인증하는데 사용되는 많은 비밀정보가 저장되어 있기 때문이다. 따라서 인증 서버에 저장되어 있는 정보들이 노출될 경우에는 침해자가 노출된 정보를 이용하여 사용자를 위장하는 문제가 발생하며, 극단적인 경우 침해자가 인증 서버를 위장하여 인증 분쟁에 대한 문제를 총괄하여 책임질 수도 있다. 따라서 사용자들은 인증 서버에 대한 공정성을 보장받을 수 없기 때문에 사용자나 정보에 대한 인증을 신뢰할 수 없게 된다.

3. Gateway Server 인증 시스템 구현



(그림 3) 게이트웨이 서버 인증 시스템(GSAS)

위 (그림3)은 GSAS(Gateway Server Authentication System)의 구조를 나타내고 있다. GSM(Gateway Server Manager)와 미들웨어와 DBA로 구성되어 있으며, GSM은 인증관리자, 권한관리자, 감사관리자로 세분화되어진다.

각각의 관리자의 역할과 인증 및 권한 알고리즘을 아래와 같이 설명한다.

3.1 인증

사용자가 네트워크 상에서 특정한 지역 게이트웨이에서 Gateway Server에 의한 암호화 인증은 다음과 같은 절차로 수행된다. 먼저 사용자는 자신의 식별자(user-ID)를 Gateway Server에 전송하면, 게이트웨이 서버 관리자(GSM : Gateway Server Manager)는 그 사용자에게 부여된 인증 보안 등급을 탐색하여, 해당 인증 보안 등급에 상응하는 인증 방법을 선택하여 인증을 실행한다. 본 절에서는 해당 인증 보안등급이 암호화 인증을 요구할 경우의 절차를 설계하였으며, 그 절차는 다음과 같다.

(표 1) GSM 인증관리자 단계 1

<단계 1>	
U→GSM	: 사용자 이름
GSM	: base B create
	: $C1=E(B)_{U.sk}$
	$C2=E(B)_{G.sk}$
GSM→U	: C1
GSM→G	: C2

<단계1>에서는 먼저 사용자 U는 자신의 게이트웨이 서버에게 사용자 이름을 전송하면, 게이트웨이 서버 관리자는 인증 정보 데이터베이스에서 그 사용자의 초기 인증 보안 등급을 탐색하여, 이에 상응하는 절차를 선정하여 인증을 수행한다. 이 경우에는 인증 보안 등급이 암호화 인증에 해당할 경우의 인증 절차로써, GSM은 먼저 암호화 다항식 생성에 필요한 베이스 B를 선정한다. 베이스 B를 선정한 GSM는 이제 선정된 베이스 B를 사용자와 Gateway Server와의 비밀키 $U_{.sk}$와 $G_{.sk}$로 각각 암호화하여 사용자와 Gateway Server에 전송한다. 여기서 비밀키 $U_{.sk}$와 $G_{.sk}$는 사용자가 Gateway Server에 log-in시 인증관리자에 의해 부여된다.

(표 2) GSM 인증관리자 단계2

<단계 2>	
G	: Compute
	$B=D(C1)_{G.sk}$
	: Generate
	AI.G=[G.I, U.I, G.RI]
	: Compute
	C3=f(AI.G)
G→U	: C3

<단계2>에서는 GSM로부터 암호문 C1을 수신한 Gateway Server는 자신의 비밀키 $G_{.sk}$로 복호화하여 비밀베이스 B를 계산하고, 암호 다항식 f와 복호화 f^{-1}을 생성한다. 그리고 나서 자신의 인증 정보 AI.G를 다음과 같이 생성한다. 먼저 자신의 식별자 G.I와 사용자의 식별자 U.I에 자신의 세션 임의 응답 정보 G.RI를 추가하여 AI.G를 구성한다.

이제 암호화 다항식 f를 이용하여 자신의 인증 정보 G.AI를 암호화하여 암호문 C3을 사용자에게 전송한다.

(표 3) GSM 인증관리자 단계3

<단계 3>	
U	: compute
	$AI.G=f^{-1}(C3)$
	: Generate
	AI.U=[U.I, G.I, G.RI]
	: Compute
	C4=f(AI,U)
U → G	: C4

<단계 3>에서는 Gateway Server G로부터 수신한 암호문 C3를, 사용자는 자신이 생성한 복호화 다항식f^{-1}을 이용하여 복호화한다. 현재 사용자 U는 자신의 식별자 U.I를 Gateway Server의 식별자 G.I와 Gateway Server의 응답 정보 G.RI를 자신이 생성한 암호화 다항식 f를 이용하여 암호화하여 암호문 C4를 Gateway Server에 전송한다.

(표 4) GSM 인증관리자 단계4

<단계 4>	
G	: Compute
	$AI.U=f^{-1}(C4)$
	: 응답정보 G.RI 검증
G → GSM	: 인증결과 통보
G → U	: 인증 prompt

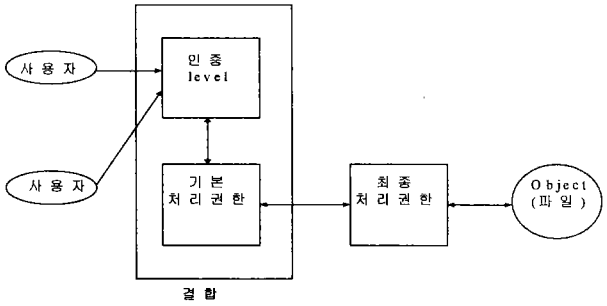
<단계 4>에서는 사용자로부터 받은 암호문 C4를 Gateway Server G는 자신이 생성한 복호화 다항식 f^{-1}을 이용하여 복호화한다. 인증 복호화된 자신의 응답정보 G.RI를 점검하여, 원래의 자신이 생성한 세션 인증 결과 G.RI와 일치하면 인증이 완료되고, 이 결과를 사용자와 GSM에게 전송한다. Gateway Server의 G로부터 인증 결과를 통보 받은 GSM는 이제 사용자에 대한 인증 권한 레코드를 생성하여 보관한다. 이후 이 사용자가 어떠한 자원을 요청할 경우, 요청된 자원에 대한 최종 권한을 부여하게 된다. 따라서 이 경우에는 인증 보안 등급을 부여받게 된다. 이와 같이 시스템에 log-in 경우에도 어떠한 인증 기법에 의하여 인증 되었느냐에 따라 다단계의 인증 보안등급을 부여함으로써 기존의 모든 사용자에 한가지에 인증 방법을 적용하는 방법보다 융통성 있는 log-in 인증을 제공한다.

인증은 서비스를 요청하는 사용자가 바로 그 사용자라는 신용을 얻는 수단이다. 그러므로, 본 논문에서 제안하는 시스템은 인증된 사용자로 가장하는 위협에 대처할 수 있다. 흔히 쓰이는 인증 서비스로는 패스워드를 사용하는 기법이 있으나 다양한 공격에 취약하다.

3.2 권한관리

각 사용자는 각각의 특정한 인증 기법에 따라서 인증되어지며, 그 결과로 인증 보안 등급을 부여받게 된다. 따라서 특정 자원을 이용하기 위해서는, 인증 보안 등급과 자원에 부여된 기본 권한을 특정한 방법에 의하여 결합하여서 생성된 최종 접근 권한에 따라 자원을 이용한다. 따라서 각 사용자마다 한 자원에 대해 서로 다른 접근 권한을 융통성 있게 부여할 수 있다. 인증 보안 등급의 값과 접근 권한 기능과의 결합 방법을 제안하기 위해서, 먼저 인증 보안 등급의 값과 접근 권한의 내용으로 변환하는 것이 필요하며, 다음의 표와 같이 변환 할 수 있다.

표 5의 인증 보안 등급의 변환을 보면, 인증 권한 레코드내의 인증 보안 등급 값이 0일 경우는 자원에 대한 특별한 접근 권한이 없다. 따라서 이 경우에는 통신망에서 특별한 접근 제한이 없는 공공 게시판과 같은 자원에 대한 접근은 가능하다. 만약 인증 보안 등급의 값이 1이었을 경우는 자원에 대한 Read only 권한으로 변환되며, 인증 보안 등급의 값이 2 혹은 3 이었을 경우는 Read-Write only로 변환되며, 인증 보안 등급이 4인 경우는 Execute only 권한을 부여하는 변환 방법의 한 예이다.



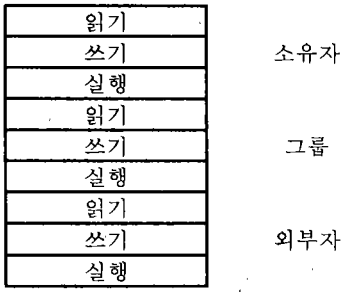
(그림 4) 인증 보안 등급에
따른 접근 권한

(표 5) 인증 보안 등급의 변환

CASE		인증보안등급의 값
0	:	[no sccess];
1	:	[read only];
2..3	:	[read, write only];
4	:	[execution only];
5	:	[read, execution];
6..7	:	[full access];
END	:	

이와 같이 인증 보안 등급과 접근 권한 내용을 결합함으로써, 상당히 향상된 접근 권한 제어 기능을 수행할 수 있다. 이제 인증 보안 등급과 기존의 ACL(Access Control List)과의 결합 방법이 필요하며, 다음의 두 가지 방법이 가능하다. 첫째는 간단한 방법으로서 기존의 접근 권한 내용과 사용자 인증 보안 등급을 단순히 접근 권한과 연결하여, 자원에 대한 접근 권한을 인증 보안 등급과 접근 권한의 쌍으로 표현하는 방법이다. 이 방법의 단점은 호스트의 메모리 요구가 상당히 커진다는 점이다. 다른 방법으로는 인증 보안 등급과 자원의 접근 권한을 bit masking을 하는 방법이다. 이 방법은 사용자의 인증 보안 등급과 부여된 기본 접근 권한과를 특정한 방법의 bit 연산을 하여서, 사용자의 자원에 대한 최종 접근 권한을 부여하는 방법이다. 예를 들어서 어떠한 파일에는 일반적으로 그 파일에 대한 접근 권한은 다음의 그림과 같이 표현된다.

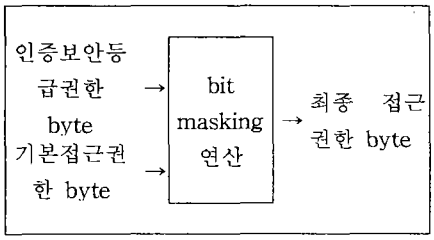
그림 5에서 보면 먼저 상단의 3bit는 파일의 소유자에 관한 권한 부분이며, 다음의 3bit는 파일 소유자의 그룹에 속한 사용자들에 관한 접근 권한에 해당하며, 마지막 3bit는 기타 사용자들에 관한 접근 권한 부분이다.



(그림 5) 일반적인 접근권한

이 bit masking에 의한 인증 보안 등급과 접근 권한의 결합을 위해서는, 다음의 3개의 접근 byte가

필요하다. 첫째는 사용자의 인증 보안 등급을 변환한 인증 보안 등급 권한 byte이며, 둘째는 특정 자원, 즉 이 경우에는 특정한 파일의 기본 접근 권한 byte이며, 마지막으로는 위의 두 접근 byte를 bit masking한 결과의 최종 접근 권한 byte이다. 따라서 자원에 대한 특정 사용자의 최종 접근 권한은 다음의 절차에 의하여 결정된다.



(그림 6) 최종 접근 권한 생성

bit masking에 의하여 결합을 하는 방법에는 다음의 두 가지 방법을 적용할 수 있다. 첫째는 인증 보안 등급 권한 byte와 자원의 기본 접근 권한 byte를 서로 logical-AND 연산을 하는 bit masking 방법이다. 이 방법에서는 자원의 기본 접근 권한 byte를 생성할 때는, 소유자는 해당 자원에 대하여, 자신이 타인에게 부여할 최대의 권한을 부여하면 된다. 둘째 방법은 logical-OR에 의한 연산을 하는 방법으로써, 이 경우에는 자원의 기본 접근 권한 byte의 내용에 상관이 없이, 바로 인증 보안 등급 권한 byte가 최종 접근 권한 byte가 되므로, 자원에 대한 기본 접근 권한을 부여하지 않아도 된다. 그러나 이 방법은 자원에 대한 접근 권한의 제어가 인증 보안 등급에만 의존하게 됨으로써, 간단한 방법이지만 자원에 대한 최소한의 권한 제어를 할 수 없다는 단점이 있다. 따라서 본 논문에서는 logical-AND에 의한 bit masking 방법을 제안하였다. 다음의 그림은 logical-AND에 의한 bit masking 방법의 한 예이다.

인증보안등급권한 :	0	1	1	0	0	1	0	0	1
기본 접근 권한 :	1	1	1	1	0	1	0	0	1
최종 접근 권한 :	0	1	1	0	0	1	0	0	1

(그림 7) Logical-AND Bit Masking

그림 7의 bit masking을 한 내용을 보면, 먼저 기본 접근 권한 byte에서의 자원에 관한 최대 권한은 "101"로써, Read와 Execution 권한이 부여 되어있다. 인증 보안 등급 권한 byte는 "001"로써, Execution 권한만이 주어졌다. 따라서 두 개의 byte를 logical-AND한 최종 접근 권한은 "001"로써 Execution 권한만이 부여되는 것을 볼 수 있다.

3.3 감사 기능(Audit Service)

감사는 시스템에서 발생되는 보안 관련 사건들을 추적하는 수단이다. 회계 감사 기능을 사용하여 시스템의 보안 정책을 위반한 사용자를 찾아낼 수 있다. 감사 기능을 발휘할 수 있도록 하기 위해서 제공되어야 할 최소의 정보는 클라이언트와 서버의 식별자, 클라이언트를 생성한 사용자의 식별자, 교환된 정보 등이다.

그림 8은 분산 보안 서비스 사이의 상호 작용을 나타낸다. 그림 8에서 나타난 것처럼 접근제어 서비스의 올바른 동작은 적절한 인증 서비스와 참조 모니터의 권한 부여 정책에 의존하고 있다. 또한 시스템의 완전한 보안 기능을 부가하기 위해서는 감사 서비스가 필수적이다.

3.3.1 감사

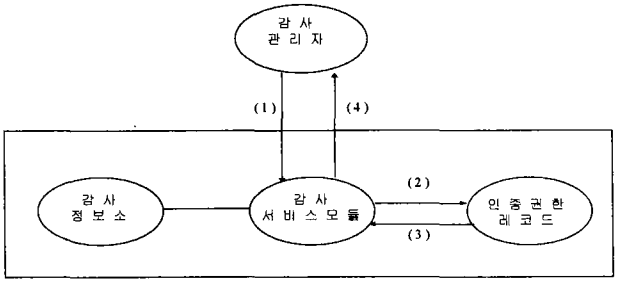
(1) 감사 관리자는 감사 서비스 모듈에게 감사 정보를 요청한다.

(2) 감사 서비스 모듈은 감사정보를 요청한 사용자가 감사관리자임을 확인하기 위해서 인증 권한 레코드 모듈

에게 사용자의 보안 정보를 요청한다.

(3) 인증 권한 레코드는 요청된 사용자의 보안 정보를 감사 서비스 모듈에게 보낸다.

(4) 감사 서비스 모듈은 인증 권한 레코드 모듈로부터 얻은 사용자의 보안 정보를 사용하여 사용자가 감사 관리자일 때에만 감사 정보소 저장된 감사 정보를 사용자에게 보낸다.



(그림 8) 감사 서비스 모듈의 동작

4. 결론

현대 사회는 네트워크의 발전으로 클라이언트/서버시스템으로 발전이 가속화되고 있다. 이러한 시점에서 분산되어 있는 데이터베이스는 악의를 가진 사용자들에게 항상 노출되어질 위험을 가지고 있다.

본 논문에서 제안하는 게이트웨이 서버 인증 시스템(GSAS)은 특정 데이터베이스 서버와 미들웨어, 지역 게이트웨이를 통합하여 구축한 시스템이다. 기존의 DBMS의 보안은 호스트 시스템에 로그인 사용자에 대해서 인증을 하였지만 제안 시스템은 호스트 시스템에 로그인 하기 전에 지역 게이트웨이 수준에서 암호화된 인증 레코드를 구축함으로써 더욱 강한 다단계 인증을 하도록 구현하였다. 또한 미들웨어를 이용해서 이질적인 분산 데이터베이스 시스템에 접근하는 사용자들도 게이트웨이 서버에서 인증함으로써 기존의 보안시스템보다 미들웨어를 이용해서 접근하는 사용자들을 인증서버에서 효과적으로 관리할 수 있다.

향후 이 논문에서 제안한 알고리즘을 입증하기 위하여 실험 데이터의 결과값을 부가할 할 것이며, GSAS를 보완, 확장하여 DBMS를 보다 강력하고 통합적으로 지원하고, 데이터베이스를 보호할 수 있는 모델인 GSSS(Gateway Server Security System)로의 연구가 요구된다.

참 고 문 헌

[1]Charles P.Pfleeger, SECURITY IN COMPUTING, Prentice-Hall International Editions, 1989.

[2] C.J.Date, An Introduction to Database Systems, Addison-Wesley Publishing Company, 1986.

[3] J.F. Traub and Y.Yemini, "The Statistical Security of a Statistical Database", ACM Transaction on Database Systems, Vol.9, No.4, Dec. 1984, pp.672-679.

[4] Gio Wiederhold, Database Design, McGraw-Hill, 1985.

[5] Jackson Wilson, "A Security Policy for an A1 DBMS(a Trusted subject)", IEEE Transaction, pp.166-175, 1989.

[6] Shigeo Tsujii, "An ID-Based Cryptosystem Based on the Discredte Logarithm", IEEE Transaction Communication, Vol.7, No.4, May 1989

[7] 서재현, "분산 망관리 시스템의 보안 상호운용과 관리 정보베이스의 접근제어", 박사 학위 논문, 전남대학교 대학원, 1996.

[8] 이봉우, "분산데이터베이스 시스템에서 효과적인 보안유지 방안에 관한 연구", 석사학위 논문, 한국외국어대학교 대학원, 1993.

[9] 김영근, "분산시스템을 위한 보안 알고리즘 설계 및 구현", 석사학위논문, 경남대학교 대학원, 1993.

[10] 정용화, "분산 처리 시스템에서의 데이터 보안에 관한 연구", 석사학위논문, 숭실대학교 대학원, 1987.

[11] 최진탁, "암호화기법을 이용한 확장 데이터베이스 보안 시스템의 구현", 박사학위논문, 경희대학교 대학원, 1991.

[12] 구홍서, "관계 데이터 베이스 시스템에서의 보안 시스템 설계 및 구현", 석사학위논문, 인하대학교 대학원, 1996.