Journal of Korea Multimedia Society Vol. 14, No. 2, February 2011(pp. 228-237)

핵심 쿼리 결제를 통한 DB 보호 시스템 설계 및 구현

김양훈[†], 권혁준[††], 이재필[†††], 박천오[††††], 김준우[†††††], 장항배[††††††]

요 약

정보보호의 패러다임 진화와 함께 데이터베이스에 저장된 중요 데이터의 유출이나 도난의 위험성이 증가되고 있으며 실제로 개인정보의 대량 유출 사건이 끊임없이 발생하고 있어 데이터베이스 보안에 대한 요구사항이 매우 높아지고 있다. 기업 내부 정보 유출방지를 위하여 개발된 기술은 관리자의 정책 설정 및 허가된 사용자만이 DBMS 접속 권한을 갖게 되는 수동적인 제어 방식으로 완벽하게 보호하기에는 기술적인 제약이 따르고 있다. 이에, 본 논문에서는 데이터베이스에 핵심 정보에 접근하는 중요 Query에 대하여 파싱하고, 인터럽트하여 결제함으로써 데이터베이스 시스템을 적극적으로 보호하고 획일적 보안 정책을 적용할 수 있는 데이터베이스 보호를 위한 Query 결재 시스템을 제안한다.

Design and Implementation of DB Protection System through Critical Query Signature

Yang Hoon Kim[†], Hyuk Jun Kwon[††], Jae Pil Lee[†††], Chun Oh Park[††††], Jun Woo Kim[†††††], Hang Bae Chang[††††††]

ABSTRACT

The risk of leakage or theft of critical data which is stored in database is increasing in accordance with evolution of information security paradigm. At the same time, needs for database security have been on the rapid increase due to endless leakage of massive personal information. The existing technology for prevention of internal information leakage possesses the technical limitation to achieve security goal completely, because the passive control method including a certain security policy, which allows the only authorized person to access to DBMS, may have a limitation. Hence in this study, we propose Query Signature System which signatures the queries accessing to the critical information by interrupting and passing them. Furthermore this system can apply a constant security policy to organization and protect database system aggressively by restricting critical query of database.

Key words: Query Signature(쿼리 결재), Database Protection(데이터베이스 보호), Database Security (데이터베이스 보안)

※ 교신저자(Corresponding Author) : 장항배, 주소 : 경기도 포천시 호국로 1007번지 대진대학교 (487-711), 전화 : 031)539-1752, FAX : 031)539-1750, E-mail : hbchang@daejin.ac.kr
접수일 : 2010년 8월 21일, 수정일 : 2010년 10월 21일
완료일 : 2010년 12월 6일
[†] 준회원, 대진대학교 컴퓨터공학과 박사과정
(E-mail : kimyh7902@daejin.ac.kr)
[††] 정회원, 연세대학교 정보대학원 박사과정
(E-mail : gloryever@gmail.com)
[†††] 정회원, 소프트캠프(주) 부사장
(E-mail : jplee@softcamp.co.kr)
[††††] 정회원, 피앤피시큐어 대표이사
(E-mail : copark@pnpsecure.com)
[†††††] 정회원, 인천대학교 경영학과 교수
(E-mail : jwkim@incheon.ac.kr)
[††††††] 종신회원, 대진대학교 경영학과 조교수

1. 서 론

최근 국내에서 우수한 IT 인프라에 걸맞게 데이터베이스 산업이 규모면에서 괄목할만한 성장을 이루어냈다. 데이터베이스의 의미는 '논리적으로 연관된 레코드나 파일의 모임'으로 방대한 자료를 효율적으로 관리하기 위해 많은 양의 자료를 처리하는 곳에서 널리 사용되고 있다. 이러한 데이터베이스를 생성하고, 관리하고, 사용자의 요구에 따라 응답을 보내는 프로그램들을 데이터베이스 관리시스템이라고 부른다[1].

근래의 정보보호 패러다임은 네트워크 보안에서 데이터베이스 보안으로 진화되고 있다. 정보보호의 패러다임 진화와 함께 포털사이트나 기업 내 데이터베이스에 저장된 중요 데이터의 비인가자 혹은 내부자에 의한 유출이나 도난의 위험성이 증가되고 있으며 실제로 개인정보의 대량 유출 사건이 끊임없이 발생하고 있어 데이터베이스 보안에 대한 요구사항이 매우 높아지고 있다[2].

데이터베이스는 항상 보호 받아야 하며, 내부에 저장되어 있는 정보의 가치나 중요도에 관계없이 보호를 받아야 한다. 이러한 보호 정책은 보안정책 이외에도 필요성이 매우 크며 데이터의 중요도가 증가할수록 필요성도 비례하여 증가한다. 이러한 데이터베이스는 불특정 다수의 개인 정보나 중요한 지적재산을 보유한 기업정보가 들어있는 저장소로, DB 보안은 DBMS를 통하여 내·외부 사용자가 이 저장소에 접근해 정보를 보는 것을 통제하는 것을 말한다. 하지만 최근 기존 DBMS의 취약점을 이용한 휴대전화 가입자 정보 유출과 건강보험공단의 개인병력기록이 유출되는 사고는 모두 내부 사용자에 의한 유출이었다[3,4].

고객 정보, 금융 정보 등의 기업/공공기관내의 매우 중요한 정보가 보관 되어 있는 데이터베이스 내의 데이터는 업무에 필요할 경우 해당 관련 담당자는 데이터베이스에 Query를 통해 데이터를 추출하고 일부 데이터는 가공 할 수 있는 권한이 있어야 한다[5-7]. 그러나 기존의 DBMS는 이러한 기능이 미흡하여 Query의 중요도에 상관없이 일괄처리로 인하여 발생하는 중요한 Query 유실, 보안 위협 등 소극적 보호 대책을 지니고 있다. 그러나, 본 논문에서는 데이터베이스의 중요 Query를 제한하여, 데이터베이스 시스템을 적극적으로 보호하고 획일적 보안 정책을 적용할 수 있는 데이터베이스 보호를 위한 Query 결제 시스템을 제안하고자 한다.

본 논문의 2장에서는 Query 결제 시스템의 필요성과 관련연구에 대해 알아본다. 3장에서는 Query 결제 시스템의 설계에 대해 서술하고, 4장에서는 구현한 Query 결제 시스템에 대하여 이야기한다. 그리고 5장에서는 결론을 맺는다.

2. 관련연구

2.1. 네트워크 및 애플리케이션 보안

일반적으로 IT 비즈니스 인프라 환경에서의 보안 솔루션 구성요소는 개인 사용자 측면에서는 안티바이러스 솔루션, 개인용 PC방화벽, 키보드 보안, Device 보안 등의 개인 데이크탑 보안이 있다. 또한, 통신구간에서는 SSL, PKI 등을 적용하는 데이터 보안이 있다.

서버측면에서는 네트워크 레벨에서는 방화벽, IDS/IPS를 이용한 네트워크 보안이 있으며, 접근제어, 애플리케이션 보안, OS보안, DB 보안 등을 제공하는 애플리케이션 레벨의 보안 등으로 구분 한다.

그림 1 보안 레벨의 구분에서 개인 데스크톱 보안과 네트워크 보안 분야는 이미 오랜 기간 동안 연구되어왔으며 기술적으로 검증을 받아 현재는 기본적으로 어디에서나 적용되고 있는 상황이다. 또한 SSL, PKI 등을 적용한 데이터보안분야도 점차 일반화되고 있는 추세이다. 그러나 DB 애플리케이션 레벨의 보안 시스템 부문은 아직까지 인식이 미비한 상황이다.

DB 보안의 기술은 해킹 및 내부자의 불법적인 정보유출을 보호하는 전용 기술을 의미한다. DB 보안은 내부의 권한 있는 사용자에 의한 정보유출 등의 역기능을 사전에 예방하고 혹시나 발생한 사고에 대해서는 사후추적 할 수 있는 감사기능을 가지는 솔루션이라고 할 수 있다. 하지만 기존 DB 보안시스템은 DB수정 권한 및 인증된 ID로 로그인 시 DELETE, TRUNCATE , DROP을 할 수 있어 비 인가된 사용자가 DB수정 권한 및 인증된 ID 및 P/W획득 시 감사기능을 회피하고 DB 무결성을 무너트릴 수 있는 위협이 발생하였다.

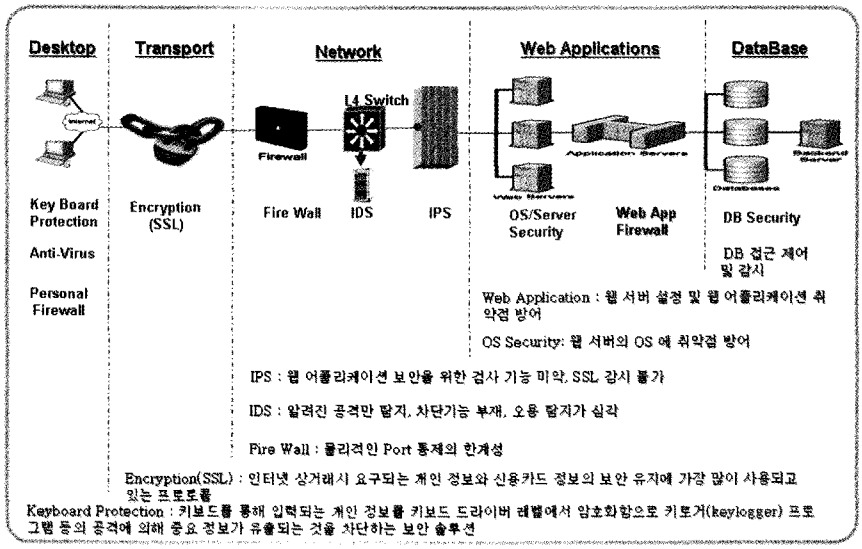


그림 1. 보안 레벨의 구분

2.2 데이터베이스 보안

데이터베이스 보안(Database Security)은 의도하지 않은 활동으로부터 데이터베이스를 보호하는 시스템, 프로세스, 프로시저이다. 의도한 것이 아닌 활동은 권한 오용, 악의 있는 공격 또는 공인된 개인이나 프로세스에 의하여 만들어진 부주의한 실수로 분류될 수 있다[8].

데이터베이스 보안은 또 넓게 컴퓨터 보안의 분야이다. 전통적인 데이터베이스는 DMZ 존과 상반된 내부 네트워크 내에 데이터베이스 환경이 존재하여, 경계가 되는 방화벽이나 라우터에 의해 외부 연결로부터 보호되어 왔다. 악의적인 보안 통신 트래픽을 감지하여 경고하는 추가적인 네트워크 보안 장치는 호스트 기반 침입탐지 시스템과 더불어 네트워크 침입 탐지 시스템 등이 있다.

3. Query 결재 시스템 설계

본 연구에서 개발할 시스템의 핵심 개념은 그림 2 Query 결재 시스템의 업무 프로세스와 같다.

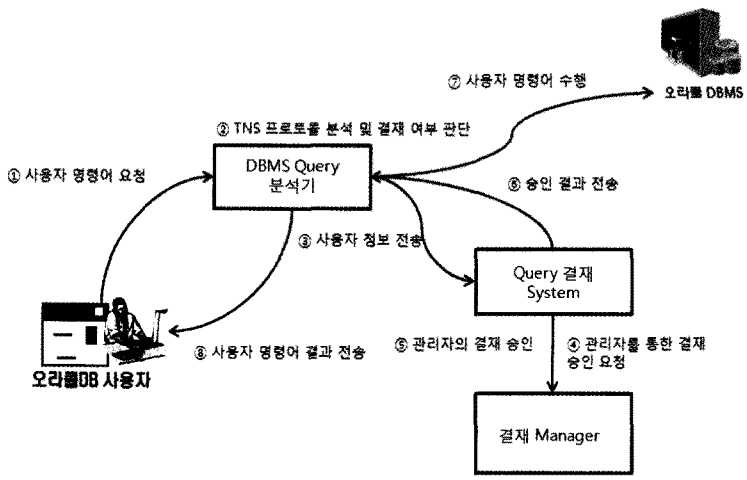


그림 2. Query 결재 시스템의 업무 프로세스

오라클 서버 사용자의 수행 명령 요청이 발생하면 DBMS Query 분석기에서 오라클 명령어의 TNS 프로토콜을 분석한다. 분석한 명령어가 Query 결재 System 정책에 의해 설정된 명령어이면 Query 결재 System에 IP, ID, 사용자 명령어, 응용 프로그램 등의 사용자의 정보를 전송하게 된다. 전송된 사용자 정보는 Query 결재 System에서 관리자에 의해 설정된 후결, 선결, 결재 거부 등의 정책에 의해 결재 상태를 구분한다. 관리자에 의해 설정된 정책에 의해 결재 승인 또는 거부를 유도함으로써 적극적인 보안 정책을 수립할 수 있도록 한다.

이러한 보안 방식을 구현함으로써 최종 또는 중간 관리자에 의해 사용자 명령어를 수행되도록 한다. 즉, 허가되지 않은 사용자에 의해 기업 내 임의로 테이블을 접근하여 중요한 고객 정보 및 데이터를 삭제, 수정, 추가 변경할 수 있는 가능성으로부터 원천적으로 차단할 수 있도록 한다.

3.1. 세부 설계

Query 결재 System은 크게 결재 서버와 관리자용 프로그램인 결재 Manager와 연동하여 구동된다.

결재 서버는 TCP/IP Layer상에서 오라클 DBMS가 사용하는 TNS 프로토콜을 분석하며, 관리자에 의해 설정된 정책을 파악하는 패킷 파싱 에이전트인 DBMS Query 분석기와 연동하여 구동된다. 그 밖에 사용자 Toad, Golden 등의 DB Tool 클라이언트와 오라클 DBMS등이 필요하다.

사용자 명령이 요청되어 관리자에 의해 결재 승인이 난 후 최종적으로 사용자 명령어 결과를 조회하는 과정은 표 1과 같다.

Query 결재 프로그램을 구동하기 위한 구성 요소는 그림 3과 같다.

사용자 프로그램은 SQL 명령어를 수행하기 위한 사용자 DB Tool로써, 오라클 DBMS에 대해서는 Toad, Golden등의 클라이언트 제품이 있다. ORACLE DBMS는 ORACLE DBMS제품으로써 고객의 중요한 정보 등을 저장하고 있다. 버전별로 7i/8i/9i/10g등의 버전으로 구성된다. 사용자 명령어는 ORACLE DBMS의 테이블에 저장된 데이터를 조회, 삭제, 수정갱신 명령어의 집합이다. 오라클 TNS 프로토콜은 사용자 명령어를 TCP/IP 프로토콜을 이용하여 전송하기 위한 응용 레벨에서의 패킷 포맷으로 오라클 DBMS또는 사용자 프로그램들 사이의 명령어 송수신 프로토콜이다. 패킷 파싱 에이전트는 본 연구의 주요한 역할을 수행하는 모듈로써, 오라클 TNS 프로토콜을 이용하여 전송되는 명령어를 분석하고, Query 결재 서버에 해당 결과를 전송한다. 또한 Query 결재 서버의 결재 승인 여부에 따라 사용자

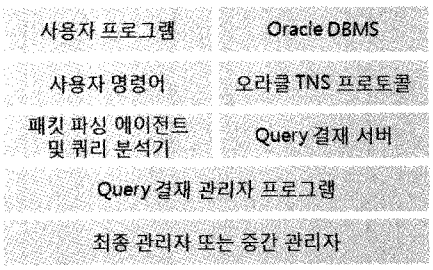


그림 3. 구동 방식에 따른 SQL Query 결재 프로그램의 구성 요소

표 1. 사용자 명령어 결과 조회 과정

순서	과 정
1	사용자는 명령을 수행하고자 하는 오라클 DBMS에 로그인한다. 이 때, 패킷 파싱 에이전트인 DBMS Query 분석기를 경유하여 로그인한다.
2	로그인한 사용자는 수행하고자 하는 명령어를 오라클 DBMS에 명령어를 전송한다.
3	수행하고자 하는 명령어는 Query 결재 서버와 연동하고 있는 패킷 파싱 에이전트에 전달된다. 또한 패킷 파싱 에이전트에 의해 사용자 명령어 및 결재 여부를 분석되고 연결 정보를 Query 결재 서버에 전달된다.
4	Query 결재 서버는 결재 내용을 확인하고, 결재 승인 요청을 위해 관리자용 프로그램인 결재 Manager에게 승인 요청 정보를 전달한다.
5	관리자는 승인 요청에 대한 사용자, 명령어 내용등을 조회 후 승인 요청을 시도한다.
6	승인 요청된 결과는 DECIDE 서버에 전달되어 진다. 그리고, 전달된 승인 요청 결과에 따라 사용자 명령을 수행하도록 오라클 DBMS에 전달되어진다.
7	명령어 수행 결과는 사용자에게 전달되어 Query 결재 시스템에 의한 모든 결재 과정을 종료한다.

명령어를 서버에 전송하여 해당 결과를 사용자 프로그램에 전달한다. Query 결재 서버는 결재 여부 판단을 위해 Query 결재 관리자 프로그램에 승인 요청을 하도록 사용자 명령어를 포함한 사용자 정보를 Query 결재 관리자 프로그램에 전달한다.

DECIDE 관리자 프로그램은 관리자에 의해 결재 승인 및 거부를 하도록 하며, 결재 요청된 내역에 대한 로깅 조회등의 기능을 수행한다. Query 결재 프로그램은 AGENT 보안정책 설정 및 로그조회, LOG 분석을 통한 REPORT, 각종 정책설정을 위한 로그 조회, 현재 사용자 세션 관리 및 특정 QUERY 분석 로그 조회, 결재 관리자/담당자 계정관리 및 권한 관련 부분, 결재 상태 및 진행 사항 보고 기능을 가진다. 최종 관리자 또는 중간 관리자는 주요 시스템에 접근 권한을 결정하는 관리자로써, DECIDE 관리자 프로그램을 이용하여 요청된 Query에 대한 결재 승인/거부를 수행한다.

3.2 시스템 구성도

조직 내 ORACLE 의 접근 통제와 Query 명령의 정책에 의한 차단 등의 기능을 하는 Query 결재 시스템의 구성은 패킷 파싱 에이전트, Query 결재 서버, 관리자용 결재 Manager, 그리고 모든 정책 정보와 로그를 저장하기 위한 데이터베이스로 구성된다.

3.2.1 패킷 파싱 에이전트

오라클 TNS 프로토콜을 이용하여 전송되는 명령어를 분석하고, DECIDE 서버에 해당 결과를 전송한다. 또한 DECIDE 서버의 결재 승인 여부에 따라 사용자 명령어를 서버에 전송하여 해당 결과를 사용자 프로그램에 전달한다. 크게 패킷 파싱 엔진, 결재 연동 모듈, 사용자 세션 관리 모듈, 로그 저장 모듈이 있다. 패킷 파싱 엔진은 TCP/IP 상의 오라클 TNS 프로토콜을 분석하여 사용자 명령을 추출한다. 결재 연동 모듈은 정책 및 로그 저장 서버로부터 데이터를 읽어 사용자 명령어가 결재 승인 대상에 포함되는지를 확인하기 위하여 Query 결재 서버에 사용자 정보를 전달한다. 사용자 세션 관리 모듈은 사용자와 오라클 DBMS 사이에 세션을 관리하여 상호간의 명령어 및 결과 값을 전달한다. 로그 저장 모듈은 DECIDE 서버로부터 결재 승인 또는 거부된 결과에 대해 로그를 저장하여 결재 Manager를 통해 조회 및 통계를 산출할 수 있다.

3.2.2 Query 결재 서버

결재 여부 판단을 위해 결재 Manager 관리자 프로그램에 승인 요청을 하도록 한다. 결재 처리를 위해 패킷 파싱 에이전트로부터 사용자 정보를 수신하여 결재 승인 또는 거부를 위해 결재 Manager에게 전송한다.

3.2.3 결재 Manager

관리자에 의해 결재 승인 및 거부를 하도록 하며, 결재 요청된 내역에 대한 로깅 조회등의 기능을 수행하는 결재를 위한 관리자 모듈이다. AGENT 보안정책 설정 및 로그조회, LOG 분석을 통한 REPORT, 각종 정책설정을 위한 로그 조회, 현재 사용자 세션 관리 및 특정 Query 분석 로그 조회, 결재 관리자

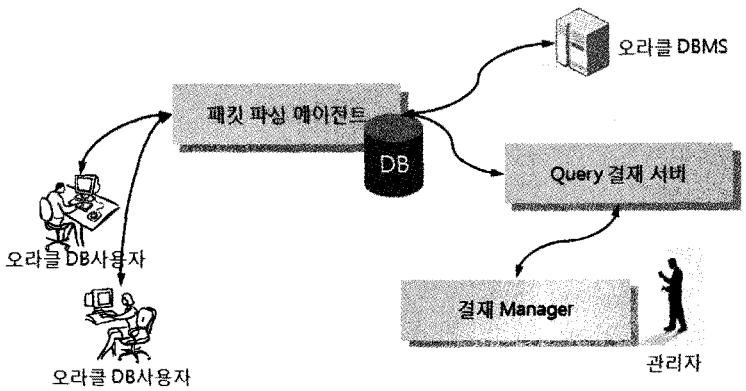


그림 4. DECIDE 보안 게이트웨이 시스템 구성도

및 담당자 계정관리 및 권한 관련 부분, 결재 상태 및 진행 사항 보고 부분에 대한 기능이 있다.

4. Query 결재 시스템 구현

Query 결재 시스템의 기본 원리는 사용자와 오라클 DBMS와의 사이에 게이트웨이 방식으로 사내 망에서 외부의 인터넷 망으로의 접근 원리와 같다. 즉, 사용자가 오라클 DBMS에 접속하고자 할 경우에는 반드시 Query 결재 시스템을 경유하여야만 접속 가능하다.

본 연구에서 제시한 시스템은 그림 5처럼 사용자와 오라클 DBMS 사이의 게이트방식을 통하여 사용자 정보 및 명령어를 모니터링하고 로깅 및 관리자로 하여금 결재 처리함으로써 내·외부에 대한 데이터베이스 보안의 안정성을 확보하여 보안사고로 인한 2차적 손실을 사전에 예방할 수 있다. 핵심 모듈은 크게 Query 결재 서버 모듈과 관리자 모듈로 나눌 수 있다.

4.1 Query 결재 서버 모듈

그림 6 Query 결재 서버의 사용자 정보 수신 처리와 같이 사용자 명령어의 Authority Policy Manager

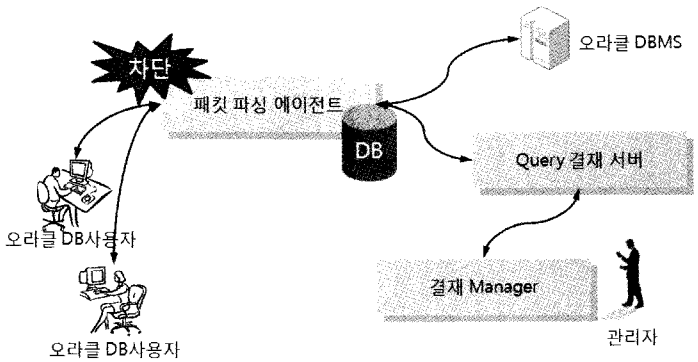


그림 5. DECIDE 보안 게이트웨이에 의한 명령어 차단

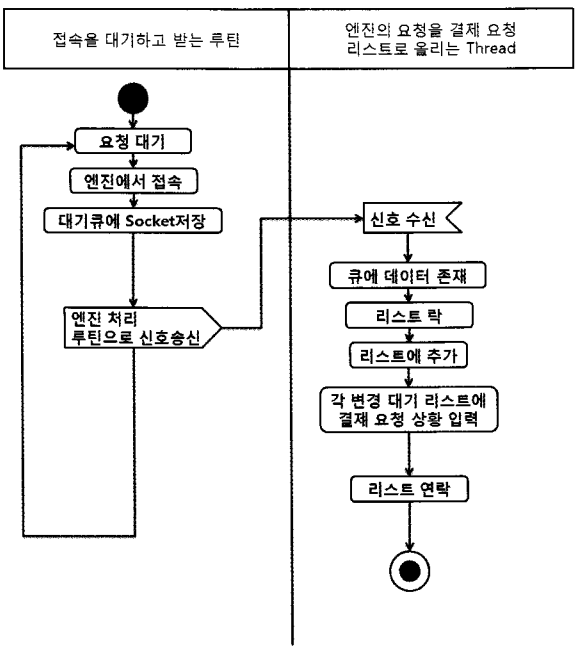


그림 6. Query 결재 서버의 사용자 정보 수신 처리

모듈에 의해 결재 요청 항목에 대해 사용자 정보를 수신 요청 대기를 한다. 수신 받은 사용자 정보를 관리자 프로그램에 전달 및 승인 요청 결과를 Packet Parsing Agent에게 다시 전송한다.

그림 7은 최초 로그인 시 DBMS 서버에게 자신의 정보를 알리기 위한 패킷으로 해당 문자열을 파싱하여 IP, 사용자 애플리케이션, 컴퓨터이름 등을 얻어온다.

그림 7의 패킷에서 얻지 못한 사용자 ID를 구하기 위해 그림 8 사용자 정보 패킷 유형 2를 이용하여 사용자 ID, 컴퓨터 이름 등을 추출해낸다.

4.2 관리자 모듈

관리자 모듈은 관리자가 Query 결재 서버 모듈에서 추출된 내용을 토대로 Query에 대한 결재 승인 및 거부를 하도록 하며, 결재 요청된 내역에 대한 로깅 조회 등의 기능을 수행한다.

AGENT 보안정책 설정/ 로그조회기능, LOG 분석을 통한 REPORT , 각종 정책설정을 위한 로그조회 기능, 현재 사용자 세션 관리 및 특정 QUERY 분석 로그 조회 기능, 결재 관리자/담당자 계정관리 및 권한 관련 부분의 정책 설정 기능을 수행하며, 결재 상태 및 진행 사항 보고 내용을 실시간으로 확인 가능하다.

로그인 한 사용자가 명령어를 수행하면 해당 명령어가 허용/차단 명령어인지, 결재 요청 대상 명령어인지 정책 비교를 수행한다. 이 때 권한 정책을 비교하는 항목은 다음과 같은 Object를 이용한다.

4.3 결재 대상 명령어 처리 및 수행

그림 9는 클라이언트 리스트의 요청에 의한 결제 처리 루틴을 보여준다.

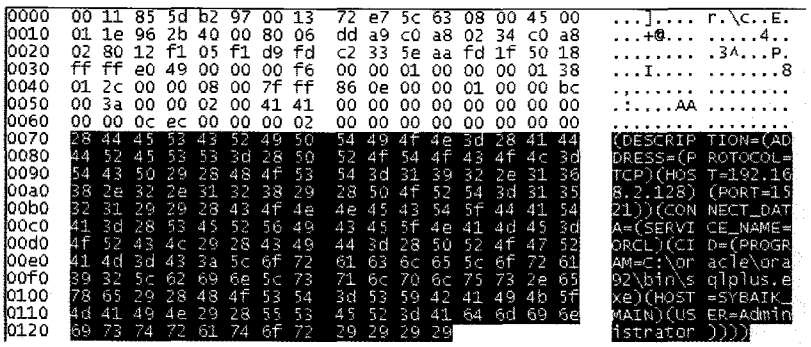


그림 7. 사용자 정보 패킷 유형 1

그림 8. 사용자 정보 패킷 유형 2

표 2. 권한 정책 비교 Object

Object	내 용
접속IP	IP 및 IP 그룹을 보안정책의 Object로 활용
사용자 ID	ID를 보안정책의 Object로 활용
컴퓨터 이름	사용자 컴퓨터 이름를 보안정책의 Object로 활용
사용 Application	사용 애플리케이션 및 그룹을 보안정책의 Object로 활용
명령어 설정	명령어 설정
테이블 및 컬럼 설정	테이블 및 컬럼 설정
DML, DCL, DDL 명령어 설정	DML, DCL, DDL 명령어 설정
시간정보	날짜 범위 또는 시간 범위를 보안정책의 Object로 활용
관리자 경고 설정	해당 정책에 만족할 경우 특정 대상 또는 그룹에게 메일, SMS, 관리자 프로그램을 통한 화면 디스플레이 설정을 통해 사건을 알리도록 설정
접속 설정	상기 Object를 만족하면 허용 또는 명령어만 차단, 세션의 차단, 결재 요청 사항 설정
결재 유형 설정	관리자에 의해 승인 요청, 자동으로 결재 승인 처리, 자동으로 결재 거부 처리, 타임아웃을 통한 설정

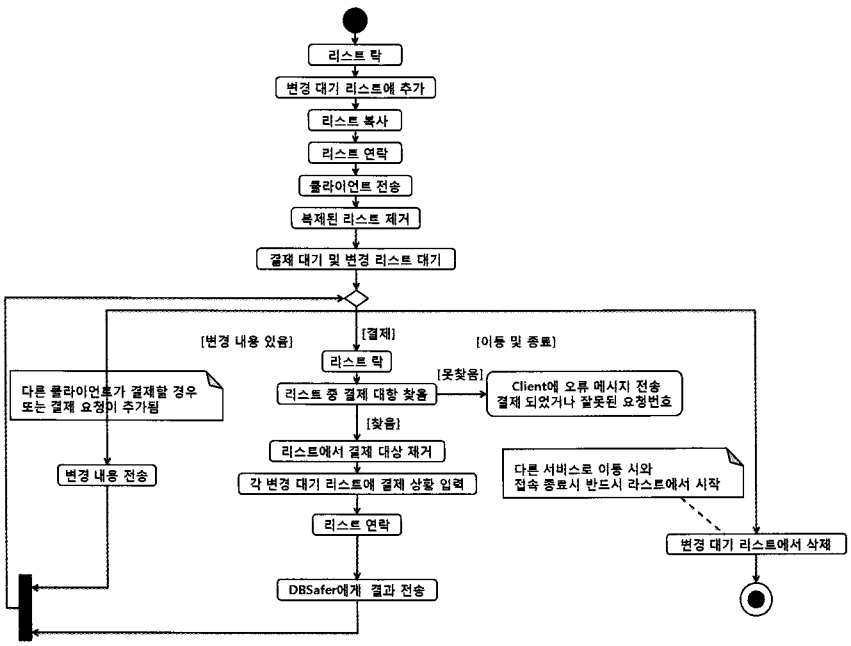


그림 9. 클라이언트 리스트의 요청에 대한 결제 처리 루틴

그림 10은 Query 결재 시스템에서의 결재 요청 처리를 위한 내부 흐름도를 보여준다.

5. 결 론

최근 국내에서 우수한 IT 인프라에 걸맞게 데이터베이스 산업이 규모면에서 괄목할만한 성장을 이루어냈다. 그와 더불어 근래의 정보보호 패러다임은 네트워크 보안에서 데이터베이스 보안으로 진화되고 있다. 정보보호의 패러다임 진화와 함께 포털사이트나 기업 내 데이터베이스에 저장된 중요 데이터의 유출이나 도난의 위험성이 증가되고 있으며 실제로 개인정보의 대량 유출 사건이 끊임없이 발생하고 있어 데이터베이스 보안에 대한 요구사항이 매우 높아

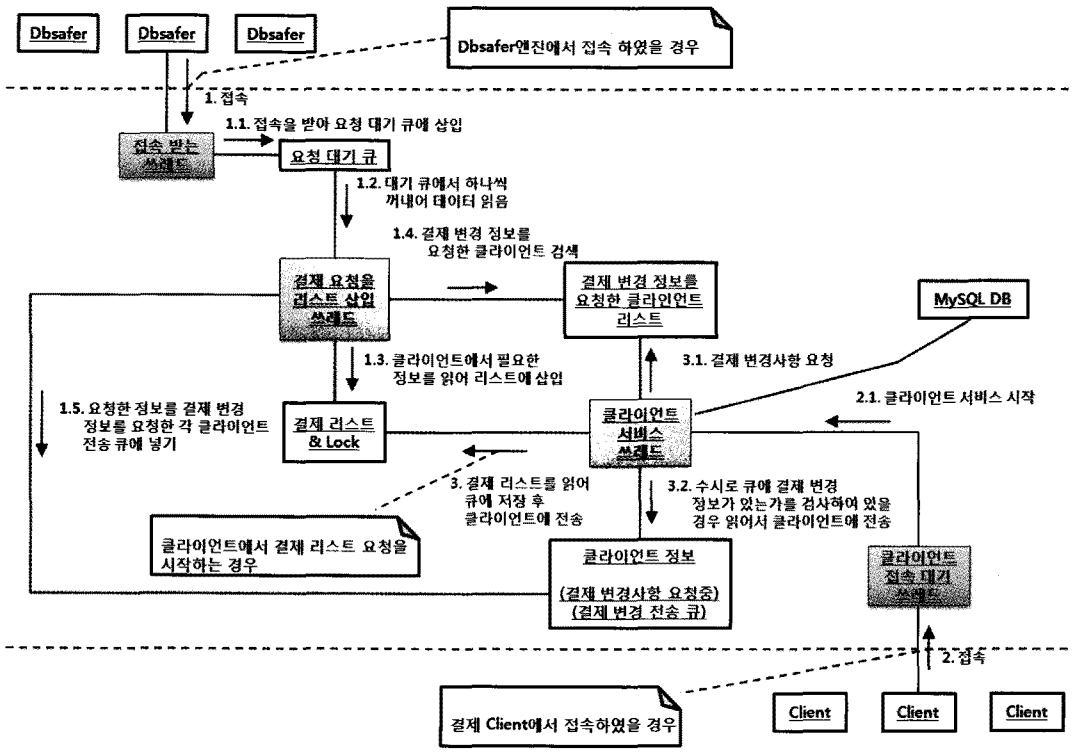


그림 10. Query 결재 시스템에서의 결재 요청 처리를 위한 내부 흐름도

지고 있다.

기업 내부 정보 유출방지를 위하여 개발된 기술은 관리자의 정책 설정 및 허가된 사용자만이 DBMS 접속 권한을 갖게 되는 수동적인 제어 방식으로 완벽하게 보호하기에는 기술적인 제약이 따르고 있다. 이에, 본 논문에서는 데이터베이스의 핵심정보에 접근하는 중요 Query에 대하여 제한하여 데이터베이스 시스템을 적극적으로 보호하고 획일적 보안 정책을 적용할 수 있는 데이터베이스 보호를 위한 Query 결제 시스템을 제안하였다. 또한 관리자에 의해 사용자 명령어를 확인하고 제어하는 능동적인 개발 기술을 구현하였으며, 이는 Query 결재 시스템의 핵심 모듈인 Query 결재 모듈과 결재 Manager 모듈로 구현하였다.

본 연구를 통하여 조직 내 첨단 기술에 대한 불법적인 자료 유출을 방지하고자 하는 조직, 연구개발 자료에 대한 기밀성을 보호하고자 하는 조직, DBMS와 연동하여 인트라넷 시스템 내 중요 설계 및 개발 정보를 보호하고자 하는 조직에 적극적인 데이터베이스 보안정책이 적용될 것으로 기대된다.

향후 지속적인 기술연구와 다양한 고객 업무 환경에서도 원활하게 운영될 수 있도록 다양한 DBMS 지원, 제품의 안정성 및 품질 향상에 대하여 연구하고자 한다.

참 고 문 헌

[1] 양해술, 강배근, 이하용, "데이터베이스 소프트웨어의 시험 사례 분석," 한국컴퓨터정보학회 논문지, 제14권, 제5호, 2009.

[2] 송유진, 박광용, "데이터베이스 아웃소싱을 위한 준동형성 암호기술," 정보보호학회논문지, 제19권, 제3호, 2009.

[3] S. Papadopoulos, D. Papadias, Weiwei Cheng, and Kian-Lee Tan, "Separating Authentication from Query Execution in Outsourced Databases," Data Engineering - ICDE '09, pp. 1148-1151, 2009.

[4] A.A. Neto and M. Vieira, "Benchmarking Untrustworthiness in DBMS Configurations,"

Dependable Computing - LADC '09, pp. 1-8, 2009.
[5] T. Peltier, "Information Security Risk Analysis," Auerbach, 2001.
[6] R.R. Henning, Harris Corporation, and Melbourne FL, "Industry and Government DBMS Security and Privacy Needs-a Comparison," Aerospace Computer Security Applications Conference, 1988.
[7] M. Vieira and H. Madeira, "Towards a Security Benchmark for Database Management Systems," Dependable Systems and Networks-DSN '05, pp. 592-601, 2005.
[8] 김보선, 홍의경, "교무업무시스템을 위한 데이터베이스 암호화 구현 및 성능 평가," 한국멀티미디어학회 논문지, 제11권, 제1호, pp. 1-12, 2008. 1.

김 양 훈

2005년 2월 대진대학교 컴퓨터공학과 학사
2007년 2월 대진대학교 컴퓨터공학과 석사
2007년 3월~현재 대진대학교 컴퓨터공학과 박사과정

관심분야 : 소프트웨어 공학, 정보보안, IT 거버넌스

권 혁 준

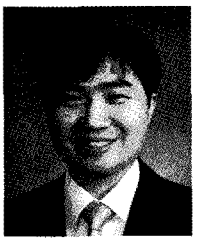
2001년 8월 Virginia Commonwealth University Information Systems 학사
2005년 8월 연세대학교 Glabal MBA 경영학 석사 졸업

2007년 3월~현재 연세대학교 정보대학원 박사과정
관심분야: 정보보안, Virtual Reality, KMS

이 재 필

1993년 2월 중앙대학교 전자계산학과(학사)
1995년 2월 중앙대학교 컴퓨터공학과(공학석사)
1999년 8월 중앙대학교 컴퓨터공학과(공학박사)

1999년 7월~현재 소프트캠프㈜ 부사장
관심분야 : 정보보안(e-DRM, DB보안), 인공지능(학습 및 추론)



박 천 오

2002년 4월 넷 시큐어 테크놀로지 팀장
2002년 12월 한국정보통신교육원 강사
2003년 12월 : (주) 세이퍼존 기술이사

2003년 12월~현재 (주)피앤피시큐어 대표이사
관심분야 : 정보보안(DB보안, 통합보안 솔루션), 정보보호 교육

김 준 우

1992년 8월 미국버지니아 주립대 박사
1992년 12월 한국 통신 기술 (주) 선임연구원
1994년 8월~현재 : 인천대학교 경영학과 교수

관심분야 : 가상현실 및 증강현실, 멀티미디어 기술에 기반 한 의사결정, SNS 에 따른 멀티미디어 기술

장 항 배

2006년 2월 연세대학교 정보시스템 박사
2007년 3월~현재 대진대학교 경영학과 조교수
관심분야 : 산업보안, u 비즈니스 전략, 정보화(정보보호) 수준 및 성과평가