# 검색 가능한 암호 알고리즘 기반 데이터베이스 내부 자료 모니터링 시스템

장유종*, 곽진**
*순천향대학교 정보보호학과 정보보호응용및보증연구실
**순천향대학교 정보보호학과
e-mail : yjjang@sch.ac.kr, jkwak@sch.ac.kr

# Searchable Encryption based Database Internal Data Monitoring System

Yu-Jong Jang*, Jin Kwak**
*ISAA Lab, Dept of Information security Engineering, Soonchunhyang University
**Dept of Information security Engineering, Soonchunhyang University

요 약

현대 사회가 정보화 시대로 변화하면서 다양해진 데이터와 민감한 데이터를 생산, 유통, 소비 하고 있다. 이렇듯 데이터의 활용 방안이 다양해짐에 따라 처리하는 데이터의 양이 많아지게 되었으며 데이터의 안전한 관리 중요성 또한 커지게 되었다. 현재 사용되고 있는 데이터베이스 보안 시스템중 하나인 내부정보 유출 방지기술은 데이터베이스의 내부 데이터 유출을 미연에 방지하는 부분에 중점이 맞추어진 기술이다. 따라서 데이터가 유출되는 현상에 대해서 적절한 대응을 하지 못하고 있다. 이러한 취약점을 보완하기 위하여 데이터 유출을 방지하고, 효율적으로 관리할 수 있는 모니터링 시스템이 필요하다. 본 논문에서는 데이터베이스의 안전한 관리를 위하여 내부 정보 유출 탐지에 효율적인 데이터베이스 내부자료 모니터링 시스템을 제안한다.

## 1. 서론

현대 사회는 스마트폰, 클라우드 컴퓨팅, 스마트 그리드 등의 출현으로 사회의 모든 시스템을 스마트화 시키고 있다. 이렇게 변화되는 시스템들은 기존의 데이터의 생산, 유통, 소비 체계는 보다 많은 양의 데이터를 사용하고 있고 보다 중요도가 높은 데이터의 취급이 증가하게 되었다. 따라서 이러한 데이터의 안전한 관리에 대한 중요성 또한 커지게 되었다.

지금 현재 사용되고 있는 데이터베이스 보안 시스템 중 하나인 내부정보 유출 방지기술은 데이터베이스의 접근제어, 암호화, 필터링, 활동 감시 이 4가지의 부분에 큰 초점을 두고 운영되고 있다. 4가지 기술 중 접근제어와 암호화 두 가지 기술 부분에서는 많은 연구가 이루어져 내부정보 유출에 대한 적절한 대응이 이루어지고 있지만, 데이터 필터링 및 활동 감시 분야는 많은 연구가 이루어지지 않아 데이터 유출에 대한 적절한 대응이 이루어지고 있지 않다. 따라서 필터링 및 활동 감시 기술부분에서 많은 연구가 필요하다.

이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2012-010886)

본 논문에서는 데이터베이스의 내부정보를 안전하게 보호하기 위해서 내부정보유출에 대하여 필터링 및 활동 감시 부분에서 데이터베이스의 효율적인 내부자료 모니터링 시스템을 제안한다.

본 논문의 구성은 2장에서는 내부정보 유출 방지기술, 검색 가능한 암호 시스템에 대하여 분석한다. 3장에서는 내부정보 유출 방지기술에 대한 취약점을 분석하고 4장에서는 데이터베이스 내부자료 모니터링 시스템을 제안한다. 5장에서는 제안시스템에 대하여 안전성 및 효율성을 분석하고, 6장을 결론으로 끝을 맺는다.

## 2. 관련연구

### 2.1 내부정보 유출 방지기술(DLP)

최근 개인정보 또는 기업들의 사업 기밀등과 같은 정보유출사고가 다양하게 발생하면서 데이터를 관리 하는 모든 사용자들 또는 기업들은 사용되고 있는 데이터, 저장되어 있는 데이터에 대한 안전한 관리에 대한 관심이 증가하였다. 데이터 유출사고는 일어난 기업에 대하여 심각한 물질적 피해뿐만 아니라 기업의 사회적 신뢰도마저 하락시키는 피해를 야기 시킨다. 또한 누출된 정보를 통하여 개인사용자들이 2차 피해를 받을 수 가 있다. 이렇듯 사회

적으로 큰 문제를 야기 시킬 수 있는 데이터 유출은 외부로부터의 악의적 공격(해킹)보다는 일반 직원들의 부주의, 또는 기업 내부자를 통한 정보 유출에 대한 심각성이 더 크게 나타났다. 이러한 문제점을 보완하기 위하여 DLP(DLP : Data Loss Prevent)는 중요한 데이터를 인식, 검색 및 분류할 뿐만 아니라 사용자 ID와 정책을 연결하고 위험 가능성이 있는 작업을 식별하는 한편 적절한 정책을 적용하고 기업 전반에서 더욱 효과적으로 파악할 수 있게 해 준다[1][2].

다음 항목들은 DLP에서 지원하는 기능이다.

<표 1> DLP 지원기능

| 지원기능 | 설 명 |
|---|---|
| 접근제어 | 데이터를 사용하는 것을 허가 또는 거부 |
| 암 호 화 | 데이터를 제 3자가 알 수 없도록 변형 |
| 필 터 링 | 허가 되지 데이터의 저장 또는 유출을 막음 |
| 활동 감시 | 데이터를 사용하는 형태를 감시 |

### 2.2 검색 가능한 암호 알고리즘

기존 암호 알고리즘과 동일하게 검색 가능한 암호 알고리즘 또한 데이터를 암호화 하는 기술중 하나이다. 하지만 검색 가능한 암호 알고리즘은 암호화된 데이터를 복호화 시키지 않고도 사용자가 원하는 데이터의 검색이 가능한 암호 기술이다. 검색 가능 암호 시스템은 데이터베이스에 저장된 데이터 유출에 따른 문제점과 같은 데이터베이스에 저장되는 데이터의 안전한 관리 측면에서 여러 문제점을 해결하기 위한 방안으로 최근 다양한 연구가 이루어지고 있다[3].

검색 가능 암호 시스템은 키 생성, 암호화, 트랩도어 생성, 검색의 다음 4가지 단계로 이루어진다[4][5].

① 키 생성 : 사용자가 사용할 키를 생성하는 단계이다. 사용자는 데이터를 암호화할 때 사용하는 비밀키를 생성하여 저장하고 공개된 정보는 사용자나 서버에 공개한다.

② 암호화 : 사용자는 주어진 데이터에 대해서 데이터 전체를 암호화 하여 암호화된 데이터를 생성하고 자료에 포함된 키워드 또는 특정한 정보를 포함한 인덱스를 생성한다. 이렇게 생성된 암호문과 인덱스는 서버에 저장된다.

③ 트랩도어 생성 : 사용자에 의해서 주어진 키워드에 해당하는 트랩도어를 생성한다. 이러한 트랩도어는 사용자의 비밀키로 생성이 가능하다.

④ 검색 : 생성된 트랩도어를 통하여 암호화된 데이터를 검색한다.

## 3. 취약점 분석

데이터베이스를 안전하게 관리 하기위해서는 다양한 보안기능이 필요하다. 기존에 사용되고 있는 내부자료 유출 방지 시스템의 경우 주로 접근제어, 암호화, 필터링, 활동 감시 이렇게 4가지 기술을 사용하여 보안 시스템을 구성하고 있다. 하지만 위의 기능들은 내부 자료가 유출되었을 경우에 대해서는 적절하게 대응할 수가 없다.

### 3.1 필터링 기술의 보안 위협

내부정보 유출 방지 기술에서 필터링 기술은 내부에서 외부로 반출되는 트래픽, 정보 등에 대해 일정 규칙에 따라 검사 후 이를 제어하는 기술을 의미한다. 필터링은 트래픽 제어, 콘텐츠 제어 등으로 나누어지는데, 트래픽 제어는 프로토콜 및 서비스에 따라 이용을 제한하는 것이다. 하지만 현재 트래픽 제어는 문제없이 수행되고 있으나, 콘텐츠 제어 기술은 콘텐츠 별로 중요도를 판단하는 기준이 각 기업 및 기관의 특성에 따라 다르고 콘텐츠의 종류가 다양해짐에 따라 저장된 모든 데이터를 콘텐츠 유형별로 나누기에 어려움이 따른다. 따라서 필터링 기술의 정확도가 상당히 낮다고 볼 수 있다[3].

### 3.2 활동 감시 기술의 보안 위협

활동 감시는 정보 유출에 대한 분석 및 추적을 수행하는 기술이다. 이러한 기능을 수행하기 위하여 유출 가능성이 있는 모든 데이터를 감시 하고 데이터의 사용현황 기록을 통한 정보 유출 탐지 업무를 수행하는 것을 의미한다. 활동 감시는 기업 내부의 규정 또는 데이터는 관리 하는 관리자가 지정한 규정을 기반으로 구성된 보안 정책에 따라 운용된다.

이러한 활동 감시 기술은 활동 감시 기술은 모든 자료의 사용형태를 기록하게 된다. 이러한 점은 데이터를 사용하는 모든 사용자들에게 데이터를 안전하게 취급하도록 경각심을 주는 효과를 가지고 있다. 하지만 실제 감시 활동 감시 프로세스는 정보 유출이 발생한 사후에 이루어져 사전 방지 효과는 미비한 것이 단점이다.

<표 2> 취약점 분석

| 기능 | 취약점 |
|---|---|
| 필터링 | - 거대화된 데이터를 필터링 하지 못함<br>- 다양한 데이터에 대한 필터링 기준 미비<br>- 사용자에 따른 기준 다양화 |
| 활동 감시 | - 거대한 데이터에 대한 감시 능력 부족<br>- 내부 정보 유출이 일어난 후 분석<br>- 사용자에 따른 기준 다양화 |

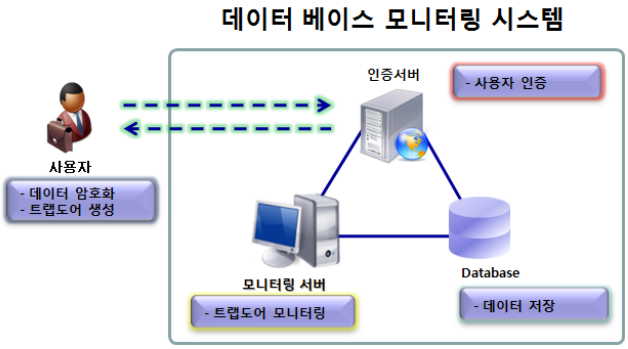
## 4. 데이터베이스 내부자료 모니터링 시스템

본 논문에서는 검색 가능한 암호시스템을 사용하여 데이터베이스의 데이터 흐름을 모니터링 하는 시스템을 제안한다. 기존 모니터링 기법에서는 내부 데이터의 다양한 종류와 크기로 인하여 저장된 모든 데이터에 대한 모니터링이 힘들다. 그렇기 때문에 본 논문에서는 검색 가능한 암호 시스템을 저장되는 데이터들에 적용시켜 데이터의 전체를 모니터링 하는 것이 아닌 특이점(트랩도어)만을 사용, 모니터링 하여 데이터베이스에 저장된 데이터의 흐름을 기존 모니터링 시스템 보다 효율적으로 모니터링 가능하다.

이러한 방식은 검색 가능한 암호시스템의 안전성을 통하여 모니터링의 효율성을 보증하도록 구성되어 있다. 본 논문에서는 검색 가능한 암호시스템을 다음 그림과 같은 형식으로 데이터베이스 내부자료 모니터링 시스템에 적용시킨다.

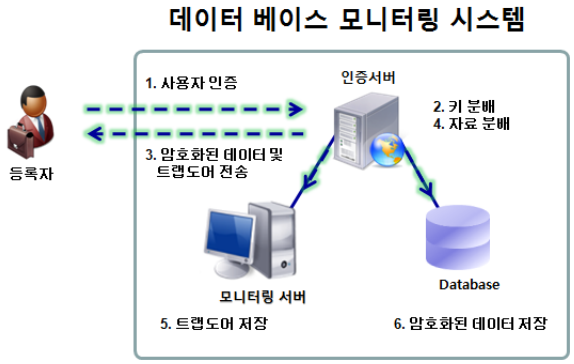

(그림 1) 검색 가능한 암호시스템 적용 방안

제안하는 모니터링 시스템의 기본 구조는 (그림 2)와 같다 .




(그림 2) 데이터 베이스 관리 시스템

위의 그림과 같이 본 논문에서 제안하는 데이터베이스 관리 시스템은 자료 등록자와 열람자의 정보를 관리할 사용자 인증 서버, 트랩도어를 통하여 데이터의 흐름을 관리할 모니터링 서버, 암호화된 데이터를 저장하는 데이터베이스 이렇게 3가지의 시스템의 상호 작용을 통하여 데이터베이스를 관리하게 된다.




(그림 3) 자료 등록 과정

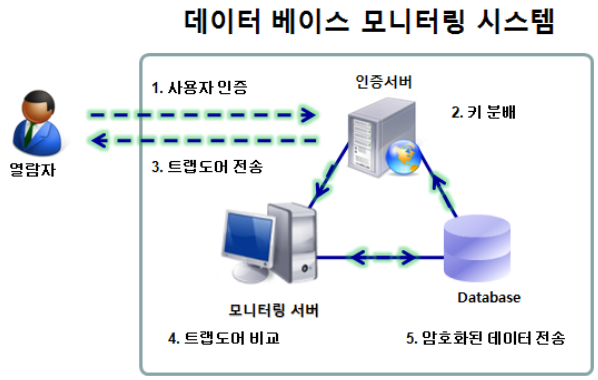
❒ 자료 등록 과정

① 사용자는 데이터베이스 관리 시스템의 인증 서버에 사용자 인증을 요청한다.

② 인증 서버에서는 사용자가 전송 해준 정보를 통하여 사용자를 인증을 한다. 올바른 사용자로 인증이 되면 인증 서버는 서버에서 저장하고 있는 비밀키를 사용자에게 전송한다.

③ 사용자는 전송받은 비밀키로 데이터베이스에 저장할 정보를 암호화시키고 트랩도어를 생성한다. 이렇게 생성된 정보를 인증서버로 전송한다.

④ 인증 서버는 전송받은 암호화된 데이터와 트랩도어를 모니터링 서버와 데이터베이스에 각 분배한다.




(그림 4) 자료 열람 과정

❒ 자료 열람 과정

① 사용자는 데이터베이스 관리 시스템의 인증 서버에 사용자 인증을 요청한다.

② 인증 서버에서는 사용자가 전송 해준 정보를 통하여 사용자를 인증을 완료하고 서버에서 저장하고 있는 비밀키를 사용자에게 전송한다.

③ 사용자는 전송받은 비밀키로 자신이 필요한 데이터에 대한 트랩도어를 생성, 인증서버로 데이터를 요청하게 된다. 인증서버는 전송받은 트랩도어를 모니터링 서버로 전송한다. 트랩도어를 전송받은 인증서버는 데이터베이스에 저장되어있는 데이터는 암호화되어 있기 때문에 사용자가 어떠한 데이터를 필요한지 알 수 없다.

④ 트랩도어를 전송받은 모니터링 서버는 전송받은 트랩도어를 자신이 저장하고 있는 트랩도어와 비교하여 일치하는 데이터가 있다면 데이터베이스에 자료 송신 쿼리를 전송하여 데이터베이스에서 인증 서버를 통하여 사용자에게 암호화된 데이터를 전송한다.

## 5. 안전성 및 효율성 분석

본 장에서는 제안한 검색 가능한 암호 알고리즘 기반 데이터 베이스 내부자료 모니터링 시스템의 안전성 및 모니터링 효율성을 분석한다.

<표 2> 안전성 및 효율성 분석

| 안전성 및 효율성 | 설명 |
|---|---|
| 안전성 | - 암호화된 데이터 관리<br>- 트랩도어를 생성가능한 사용자만이 데이터 검색 가능 |
| 모니터링 효율성 | - 트랩도어를 통한 데이터 감시<br>- 모니터링 데이터 양 감소<br>- 데이터 전송전 사전 검사 |

❒ 안전성 제공

기존 데이터베이스 서비스는 저장되는 데이터를 암호화하여 저장하지 않는다. 본 논문에서는 검색가능한 암호 시스템을 데이터베이스에 적용시켜 사용하기 때문에 데이터베이스에 저장되는 모든 데이터는 암호화한 후에 저장되어 안전성을 제공한다. 또한 저장된 데이터를 검색할시 올바른 키를 가지고 있는 트랩도어를 생성 가능한 사용자만이 모니터링 서버를 통하여 데이터를 검색할수 있다.

❒ 모니터링 효율성

제안하는 데이터 관리 시스템은 기존의 모니터링 시스템처럼 데이터 전체에 대하여 필터링 및 활동 감시를 하는 것이 아닌 데이터의 일부분으로 생성한 트랩도어를 통하여 저장된 데이터의 크기는 모두 다르지만 동일한 크기의 작은 데이터만으로 모니터링을 할 수 있도록 구성하였다. 이를 통하여 모니터링시 사용되는 데이터양이 감소하게 되어 기존의 모니터링 시스템에서 많은 자원을 사용하던 큰 용량의 데이터의 모니터링을 효율적인 모니터링이 가능하다.

## 6. 결론

본 논문에서는 보안 기술 중 하나인 내부정보 유출 방지기술이 데이터베이스상에서 사용할 때 발생할 수 있는 취약점을 분석하고, 이러한 취약점을 보완하기 위한 대응 방안에 대해 연구 하였다. 이러한 연구를 통해 검색 가능한 암호 시스템을 데이터베이스 모니터링 시스템에 적용시켜 저장되는 데이터에 대한 안전성과 트랩도어를 사용한 모니터링을 통해 모니터링의 효율성을 제공하였다. 이를 통해 안전한 데이터베이스 관리에 도움이 될 것으로 기대한다. 또한 앞으로 다양한 환경에서 더욱 안전한 데이터 관리를 하기 위하여 사용자 보안등급에 따른 데이터 관리, 내부자 위험에 따른 보안 관리와 같은 연구가 필요하다.

## 참고문헌

[1] (주)위너다임,“분산탐지기반 지능형 중요정보 유출 방지시스템 최종보고서”, 중소기업청, 2009.

[2] 신혜원, “기업 내 정보유출 방지를 위한 내부자 위험도 분석 방법론 연구”, 한국컴퓨터종합 학술대회 논문집. 2012

[3] 조남수, 홍도원, “검색 가능 암호시스템 기술 동향,” 전자통신 동향 분석 23(4), pp. 1-9 2008. 8

[4] 김선영, 서재우, 이필중, “검색 가능 암호 기술의 연구 동향,” 정보보호학회지, 19(2), pp. 63-73, 2009. 4.

[5] P. Golle, J. Staddon, and B. Waters, “Secure Conjunctive Keyword Search over Encrypted Data,” In Applied Cryptography and Network Security Conference, 2004.