"미래를 창조하는 ICT Innovator"

DB 이상행위 탐지 기술

본 기술은 개인정보 및 중요데이터를 보관하는 DB에 접근하는 이상행위를 탐지하는 기술로
사용자의 쿼리 이용 패턴과 상황 정보를 분석하여 알려지지 않은 공격을 분류할 수 있음

인증기술연구실 담당자 노종혁

ETRI 한국전자통신연구원
Electronics and Telecommunications Research Institute

목 차

1. 개발기술의 주요내용(1)

기술개념 및 특징

기술개념

- DB 이상행위 탐지 기술
  - 개인정보 및 주요정보들은 DB에 저장되어 있음
  - 적법한 사용자로 위장한 공격자 또는 내부자가 악의적으로 정보를 유출하는 경우를 막을 수 있는 방법은 DB 단에서 이상행위를 탐지하는 기술 뿐임
    - DB 암호화, IDS 등으로는 개인정보 유출을 막을 수 없음
  - 사용자 DB 접근 패턴, 상황 정보 등을 이용하여 이상 행위를 탐지함

고객/시장의 니즈를 충족시키는 독특한 점(특장점)

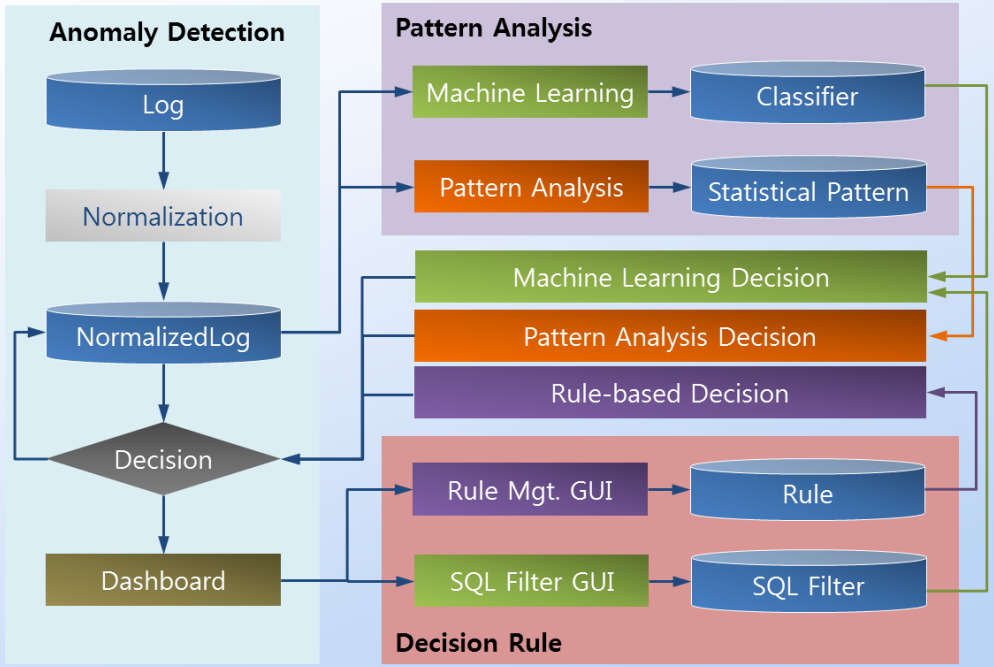
- 복합적인 상황을 고려한 이상행위 탐지 기술
  - 기계학습을 이용한 DB 이상행위 탐지
  - 상황정보에 기반한 사용자 쿼리 패턴 분석을 통합 DB 이상행위 탐지
  - 관리자 Rule을 이용한 접근 제어

1. 개발기술의 주요내용(2)

기술의 세부내용

- 기계학습을 이용한 탐지 기술
  - 통계 기반과 기계학습을 이용한 탐지
- 상황정보에 기반한 사용자 쿼리 패턴 분석
  - 사용자의 DB 접근 시간과 IP 정보 등을 이용한 패턴 분석
- 관리자 Rule을 이용한 접근 제어 기술
- DB 접근에 대한 모니터링 시스템

기술 구성도



1. 개발기술의 주요내용(3)

경쟁기술대비 우수성

경쟁기술/대체기술 현황

- DB 암호화 기술
- DB 접근 제어 기술

경쟁기술/대체기술 대비 우수성

- 기계학습, 패턴 분석, Rule을 이용한 복합적인 탐지 기술
- 알려지지 않은 공격에 대응 가능한 탐지 기술

경쟁기술	본 기술의 우수성
DB 암호화 기술	• DB 내 데이터를 암호화하여 저장하는 기술 • 적법한 권한을 획득하거나 내부자에 의한 정보 유출을 방어할 수 없음
DB 접근 제어 기술	• 사용자 권한에 따라 DB 접근을 제어하는 기술 • Rule 기반에 따른 접근 제어 기술 • 내부자에 의한 정보 유출을 방어할 수 없음 • Rule에 벗어나는 공격 또는 알려지지 않은 공격에 대응할 수 없음

1. 개발기술의 주요내용(4)

기술의 완성도

기술개발 완료시기

- 2014년 하반기
  - DB 이상행위 탐지 기술
  - DB 접근에 대한 모니터링 기술

기술이전 범위

- 기계학습을 이용한 탐지 기술
  - DB 쿼리 특성 추출
  - 통계 및 기계학습을 이용한 탐지 기술
- 상황정보에 기반한 사용자 쿼리 패턴 분석
  - 사용자의 DB 접근 시간에 따란 사용량 분석
  - 접근하는 IP 주소에 따른 패턴 분석
- 관리자 Rule을 이용한 접근 제어 기술
- DB 접근에 대한 모니터링 시스템
  - 모니터링 시스템 사용자 인터페이스

2. 기술적용 분야 및 기술의 시장성(1)

기술이 적용되는 제품 및 서비스

기술이 적용되는 제품/서비스

- DB 이상행위 탐지
  - 개인정보 또는 중요 정보를 보관하는 DB를 안전하게 관리하기 위한 서비스
  - 사용하지 않던 쿼리 패턴을 탐지하는 서비스
- 개인정보 접근 이력 저장
  - 개인정보와 관련된 특정 테이블 및 어트리뷰트에 접근하는 로그 저장
  - 개인정보 접근 현황을 분석할 수 있는 인터페이스
- DB 이용 모니터링 서비스
  - 시간별, 속성별 DB 접근 모니터링 인터페이스
  - 이상 행위 알람 서비스

2. 기술적용 분야 및 기술의 시장성(2)

해당 제품/서비스 시장 규모 및 국내외 동향

해당 제품/서비스 시장 규모

- 국내 DB 보안 시장은 2012년 658억으로 전년 대비 62.5% 성장하였으며, 2013년에는 917억 원으로 전년 대비 39.4% 성장함 연평균 11.7% 성장률로 2016년 1,000억 원대의 시장에 진입할 것으로 전망

[표 1] 국내 DB 보안 시장규모 (2009~2013) (단위: 백만원)

년도	2009	2010	2011	2012	2013
보안시장	29,452	31,942	40,458	65,576	91,679

(자료: 한국데이터베이스진흥원. 2013)

해당 제품/서비스 시장 국내외 동향

- DB 보안 영역에서 가장 큰 수요층은 공공부문으로 2012년에 38.3%였으며, 다음으로 민간 금융업이 26.6%로 나타남
- 개인정보보호법 상 DB암호화가 의무 적용되어 있으나 정보 유출 사고는 빈번히 발생하여 금융권을 비롯해 인터넷 기업과 통신업계의 DB 보안에 대한 관심이 지속되고 있음

3. 기대효과

기술도입효과

고객이 본 기술을 통해 얻을 수 있는 경제적 효과

- 개인정보를 저장하는 DB의 접근 행위를 분석함으로써 개인정보 유출 사고를 근본적으로 해결함
- 개인정보 유출 문제를 해결하여 개인정보 침해 사고 방지 및 사회 안전망 강화
- DB 이상 탐지/분석 제품을 통한 DB 보안 시장 확대
- 사용자 행위 패턴 분석 기술 등 원천 기술 확보로 금융 사기 방지와 같은 다양한 응용 솔루션 개발 토대 제공