침입 탐지의 두가지 흐름은 아래와 같음.
1. 오용 탐지: 공격에 관한 축적된 지식을 사용하여 어떤 공격을 사용하고 있다는 증거를 찾는 방식
2. 비정상 행위 탐지: 감시 중인 시스템의 정상 행위에 관한 참조 모델을 생성한 후 정상 행위에서 벗어나는 경우를 찾는 방식

본 과제에서 요구하는 오용탐지 기법이 사용하는 6가지 방법론은 전문가 시스템(Expert System), 시그니처 분석(Signature Analysis), 페트리넷(Petri-net), 상태전이분석(STATe Transition Analysis), 신경망(Neural Network), 유전 알고리즘(Genetic Algorithm)임.

6가지 방법론에 대한 설명은 다음과 같음.
1. 전문가 시스템(Expert System)
- 전문가 시스템은 공격에 관한 규칙 집합을 가지고 있어 감사 이벤트가 전문가 시스템 내에서 의미를 가지는 사실로 변환이 되고 추론 엔진은 이 규칙들과 사실을 기반으로 침입을 판단함.
- 전문가 시스템 기법은 감사 자료에 의미를 부여함으로써 감사 자료의 초상화 정도를 증가시킴
- 전문가 시스템 접근 방식은 알려진 취약점을 이용하려는 시도들에 관한 증거를 찾기 위해 감사 자료를 체계적으로 탐색할 수 있도록 하며, 보안 정책이 적절히 적용되고 있는지 검증하는 데 사용될 수도 있음
- 그러나, 전문가 시스템의 전체적 성능은 아직 낮은 정도이며 늦은 처리 속도로 인해 프로토타입에서만 사용되며 대표적인 시스템으로는 러셀이라는 규칙 기반 언어를 사용한 ASAX 등이 있음

2. 시그니처 분석(Signature Analysis)
- 시그너처 분석은 전문가 시스템과 동일한 방식으로 지식을 획득하지만 지식을 사용하는 방식이 다름
- 공격에 대한 의미적 기술은 감사 자료에서 곧바로 검색이 가능한 형태의 정보로 변경됨
예를 들면, 공격 시나리오는 공격 시 생성되는 감사 이벤트 시퀀스로 변경되거나 시스템에 의해 생성된 감사 자료에서 탐색할 수 있는 데이터 패턴으로 변경되는 것임
- 이 기법은 공격에 관한 기술이 저 수준인 경우 수행됩니다.
- 시그너처 분석 기법은 아주 효율적인 구현이 가능하므로 상업적인 침입 탐지 제품에 응용되고 있음
- 그러나 이 방식의 주요 약점은 다른 지식 기반 접근 방법과 마찬가지로 새로 발견된 취약점에 대해 자주 갱신을 해주어야 한다는 것임

3. 페트리넷(Petri-net)
- 페트리넷은 95년 코마의 기존 패턴 매칭 방법을 개선한 것으로 침입에 관한 시그너처를 표현하기 위해서 탈라 페트리넷 CPN을 사용함.
- CPN은 일반성 개념적 단순성 그래프 표현성 등의 장점을 가지고 있음
- 시스템 관리자는 공격의 시그너처를 작성하고 ID IoT시스템에 통합할 수 있음
- CPN의 일관성으로 아주 복잡한 시그너처도 쉽게 작성할 수 있지만 복잡한 시그너처를 감사 자료와 비교하는 작업은 상당히 많은 계산 비용을 요구함
- 이를 구현한 시스템으로는 96년 퍼듀의 코스트에서 개발한 ID IoT시스템이 있음

4. 상태전이분석(STATe Transition Analysis)
- 상태 전위 분석은 공격을 목표와 상태 전위의 집합으로 기술하며 상태 전위 다이어그램으로 표현한 것으로 일반적으로 STAT라 불림
- STAT 기반 침입 탐지 방식이 처음 설계되고 도구로 개발된 것이 92년 개발한 UCSB에서 개발한 USTAT이며 멀티호스트로 확장한 것이 ISTAT임
- 현재 달파의 프로젝트로 수행 중인 네트워크 기반 침입 탐지 시스템이 넷STAT임

5. 신경망(Neural Network)
- 신경망은 타당한 방법으로 새로운 입력 출력상을 얻기 위해 두 집합의 정보 간 관련성을 학습하고 일반화하는 데 사용되는 알고리즘 기법임
- 신경망은 이론적으로 지식 기반 침입 탐지 방식에서 공격을 학습하고 감사 스트림에서 탐색하는 데 사용될 수 있음
- 입력과 출력 간의 관계를 알 수 있는 믿을 만한 방법이 없으므로 신경망은 공격을 추론하거나 설명할 수 없어 주로 비정상 행위 탐지 기법으로 많이 연구되었으나 최근에는 지식 기반 프로파일을 구성하여 오용 탐지 기법으로도 사용됨

6. 유전 알고리즘(Genetic Algorithm)
- 유전 알고리즘은 자연 선택의 원리와 자연계의 생물 유전학에 기본 이론을 두며 모든 생물은 주어진 다양한 환경 속에 적응함으로써 살아남는다는 다윈의 적자생존의 이론을 기본 개념으로 함
- GSSATA는 패턴 매칭에서 생기는 문제를 해결하기 위하여 공격 시나리오부터 시간에 대한 개념을 제거하고 여기에 존 헬렌드가 제안한 유전 알고리즘을 사용함