사용자 행동 기반 동적 네트워크

접근 제어 시스템 연구

부산대학교 정보컴퓨터공학부

지도교수 최윤호

팀명 CtrlAltDefend

팀원 201924524 이광훈

202255562 신해진

202155609 조유진

목차

1. 과제 배경 및 필요성

내부자 위협이란 조직에 대한 정보, 데이터 또는 시스템에 대한 접근 권한을 가진 사람이 악의적이거나 부주의한 행동으로 보안 사고를 유발하는 위협을 의미한다. 최근 많은 기업들이 디지털 전환을 추진하면서 조직 내 엔드포인트의 수가 증가하고 있으며, 이로 인해 공격 표면 또한 확대되고 있다. 이에 따라 내부자 위협으로 인한 보안 사고 발생률도 점차 증가하는 추세다 [1]. 한 보고서에 따르면, 내부자에 의한 보안사고를 당한 기업의 29%가 피해복구에 100만달러 이상을 소요한 것으로 나타났다 [2]. 이런 사실은 내부자 위협에 대처하기 위한 접근 제어 시스템의 중요성을 시사한다.

그러나, 기존 정적 접근 제어 방식은 증가하는 내부자 위협에 충분히 대처하지 못한다. 예를 들어 802.1x 기반의 단일 인증 기반 정적 접근 제어 방식은 세션 도중 발생하는 동적인 위협에 효과적으로 대응하지 못한다 [3]. 초기에 합법적인 접근 권한을 부여받은 사용자가 이후 비인가 디바이스를 연결하거나 민감 데이터를 유출하는 행위를 하더라도 정적 네트워크 접근 제어 시스템은 이를 감지하지 못한다. 따라서, 권한을 가진 내부 위협자를 식별하기 위해선 사용자 및 엔티티의 행동 분석(User Entity and Behavior Analytics, 이하 UEBA) 기술의 도입이 필수적이다.

UEBA는 사용자의 행동을 모니터링하고 분석하여, 이를 기반으로 기존에 정립된 패턴에서 벗어난 이상 징후를 식별한다 [4]. 사용자 프로파일을 생성하고 그 행동 변화에 주목함으로써, 조직은 내부자 위협을 나타내는 이상행위를 보다 효과적으로 탐지할 수 있었다. 더 나아가, 머신러닝 및 인공지능과 UEBA 시스템의 통합은 중요한 전환점을 의미했다. AI 기반 솔루션은 방대한 데이터를 실시간으로 분석해, 기존 기법으로는 탐지되기 어려운 미세한 패턴과 이상 징후를 탐지할 수 있었다. 특히 머신러닝 모델은 사용자 행동의 변화를 효과적으로 포착하고, 잠재적으로 악성 행위를 신속하게 탐지하는 데 강점을 보인다 [5].

2. 과제 목표

본 과제는 내부자 위협 대응에 특화된 동적 네트워크 접근 제어 시스템을 구현하는 것을 목표로 한다. 이를 위해 다음과 같은 세부 목표를 설정한다.

첫 번째로, 머신러닝을 접목한 UEBA의 일종인 다중 세분화 이상 탐지 모델(MG-UABD, Multi-Granularity User Anomalous Behavior Model)을 사용해 이상 행위 탐지 시스템을 구현한다 [6]. 이상 행위 탐지 시스템은 사용자 행동 로그를 전달받아 이상 여부를 판단하며, 이상 행위가 탐지되면 해당 PC의 식별자와 함께 네트워크 접근 제어 요청을 전달한다.

두 번째로, 사용자 행동 로그 데이터를 수집하는 시스템을 구현한다. 로그 수집 시스템은 단말 PC에서 사용자 행동을 수집하고, 서버로 전송하는 로그 수집 및 전송 에이전트와, 메인 시스템에서 로그를 전달 받는 API 서버, 로그를 저장하는 로그 DB로 구성된다.

세 번째로, 이상 행위 탐지 시 네트워크 접근 제어를 수행하는 접근 제어 시스템을 구현한다. 접근 제어 시스템은 이상 행동 탐지 시스템으로부터 접근 제어 요청을 받을 시, 이상 행위가 발생한 PC가 속한 서브넷 라우터에 접근 제어를 요청한다.

마지막으로, 엔드포인트 상태를 실시간으로 모니터링하고 접근 제어 로그 및 이상 탐지 결과를 시각화하는 웹 기반 대시보드를 개발한다.

3. 요구사항 분석서

3-1. 기능적 요구사항

기능		설명
로그 수집 시스템	로그 수집	로그 수집 및 전송 에이전트는 사용자 엔드포인트에서 발생하는 로그온/로그오프, 이메일 송수신, 웹 브라우징, 파일 작업, 디바이스 연결 등 이벤트 로그를 실시간으로 수집해야 한다.
	로그 전송	에이전트는 수집된 로그를 서버로 실시간으로 전송해야한다.
	로그 저장	엔드포인트 에이전트로부터 전송 받은 로그들을 데이터 베이스에 저장해야 한다.
이상 행위 탐지 시스템	데이터 전처리	엔드포인트 에이전트로부터 수집된 로그는 분석을 위해 고정된 형식의 벡터로 전처리되어야 한다.
	이상 행위 탐지	시스템은 사전 학습된 머신러닝 모델을 사용하여 로그 벡터의 이상 여부를 판별해야 한다.
	접근 제어 요청	이상 행위 탐지 시스템은 이상으로 판별된 엔드포인트에 대해 네트워크 접근 제어 시스템에 접근 제어를 요청할 수 있어야 한다.
	분석 결과 저장	탐지된 이상 행위의 탐지 시각, 탐지된 사용자 및 엔드포인트 식별자, 이상 확률, 로그 요약 및 원인 이벤트와 같은 정보를 포함하여 데이터베이스에 저장되어야 한다.
네트워크 접근 제어 시스템	이상 엔드포인트 식별 및 제어	시스템은 이상 행위가 탐지된 엔드포인트가 속한 네트워크 영역을 식별하고, 그 영역의 게이트웨이 라우터에 이상 엔드포인트에 대한 접근 제어를

		요청할 수 있어야 한다.
	제어 결과 저장	네트워크 접근 제어 시스템은 접근 제어의 결과를 데이터베이스에 저장할 수 있어야 한다.
모니터링 시스템	PC 상태 조회	사용자는 전체 네트워크 구조와 네트워크 상에 존재하는 각 PC의 정보(PC ID)와 상태(PC on/off, 네트워크 접근 제한/허용)를 확인할 수 있어야한다.
	실시간 접근 제어 팝업 알림	사용자는 특정 PC에 대한 자동 접근 제어 발생 시, 실시간 팝업 알림을 통해 접근 제어 대상인 PC를 식별할 수 있어야 한다.
	접근 제어 기록 확인	사용자는 특정 PC에 대한 접근 제어 기록(제어 시각, 제어 유형, 성공 여부)를 확인할 수 있어야 한다.
	접근 제한 PC 로그 조회	사용자는 접근 제한이 발생한 PC의 로그를 유형별(이메일, http, 디바이스, 파일 복사, log/off)로 조회할 수 있어야 한다.
	수동 접근 제어	관리자는 특정 엔드포인트에 대해 수동으로 접근 제어를 할 수 있어야 한다.

3-2. 비기능적 요구사항

항목	설명
가용성	시스템은 24시간, 365일 상시 운영될 수 있어야 한다.
성능	로그 수집 및 전송, NAC 조치 시 실시간성이 보장되어야 한다.
사용성	관리자 대시보드는 이상 행위 탐지, NAC 조치 내역, 실시간 팝업 알림 등을 직관적으로 표시해야 한다.
확장성	시스템은 에이전트 수 또는 로그량 증가 시에도 성능 저하 없이 처리

	가능해야 한다.

4. 현실적 제약 사항 분석 결과 및 대책

제약 사항	대책
머신러닝 모델 구축에 필요한 데이터 세트를 구하기 어렵다.	공개 데이터 세트를 통해 CMU CERT 데이터 세트를 사용한다.
사용할 데이터 세트 내에 악성 사용자의 행동 샘플 수가 정상 행동 샘플에 비해 현저히 적어 데이터 불균형 문제가 발생할 수 있다.	오버 샘플링 기법을 사용해 학습 시 클래스 불균형을 보정한다.
실제 사용자 환경을 구성하기 위해 다수의 PC가 필요하다.	VMware와 같은 호스트 가상 머신을 사용해 네트워크 토폴로지를 구성한다.
네트워크 접근 제어를 위한 실제 라우터 또는 네트워크 장비 제어가 제한된다.	오픈 소스 라우터(OpenWrt)를 활용해 제어 가능한 테스트 환경을 구성한다.
실시간 데이터 수집 및 처리 성능 확보가 어렵다.	로그 전송 시 카프카와 같은 비동기 방식 전송 기술을 사용한다.
탐지된 이상행위가 실제 악성 행위가 아닐 경우, 오탐(false positive) 가능성이 존재한다.	모델 개발 과정에서 적절한 threshold 값을 설정하고, 관리자가 수동으로 접근 제어할 수 있는 기능을 추가한다.
서버에 수집되는 로그의 저장용량이 빠르게 증가할 수 있다.	일정 시간이 지난 로그 파일은 삭제한다.

내부 네트워크 구조의 복잡성으로 인해 접근 제어 대상의 식별이 어려울 수 있다.	접근 제어 대상 엔드포인트들을 ip - mac 주소 쌍으로 관리한다.
사용자 행동 로그 포맷이 서로 달라 전처리에 어려움이 발생한다.	자동 전처리 모듈(Log parser)를 개발한다.

5. 설계 문서

5.1 전체 시스템 구조

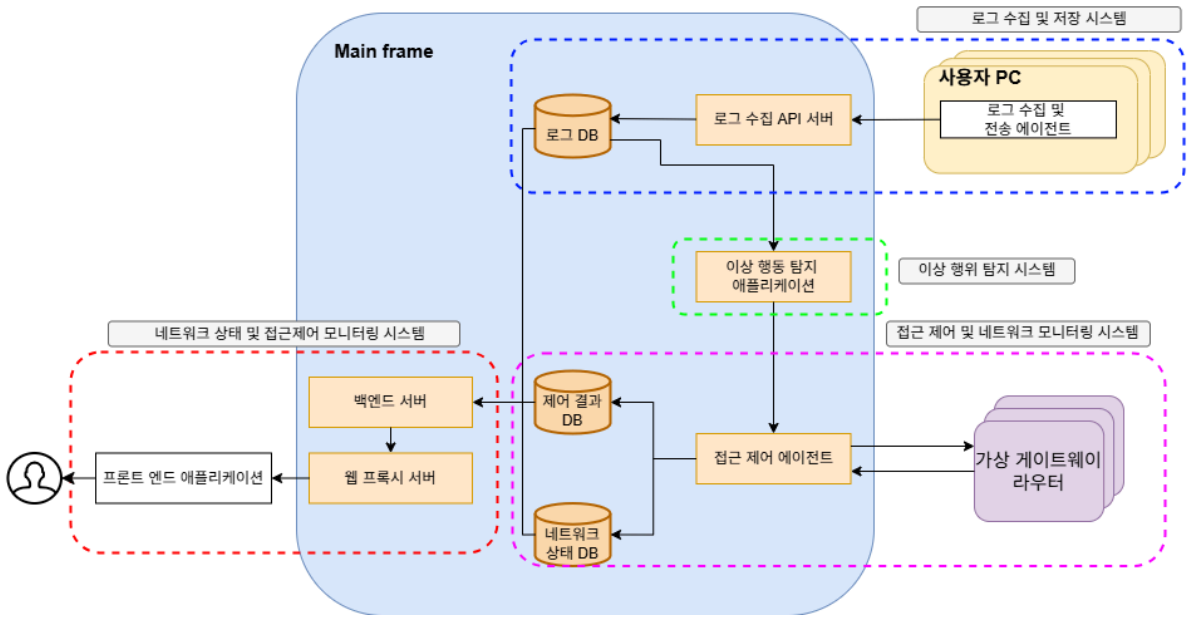

그림 1. 전체 시스템 구조도

전체 시스템은 조직 내 전체 PC 의 상태를 모니터링하고 네트워크 접근을 제어하는 중앙 집중형 시스템인 'Main frame' 과, 모니터링 및 접근 제어 대상인 사용자 PC, 접근 제어를 설정하는 가상 게이트웨이 라우터로 구성된다. 또한, 수행하는 역할에 따라 네 개의 논리적인 시스템으로 구분된다.

시스템 이름	기능
로그 수집 및 저장 시스템	조직의 각 PC로부터 사용자 행동 로그 수집 및 저장
이상 행위 탐지 시스템	수집된 로그로부터 이상 행동이 발생한 PC 식별

접근 제어 및 네트워크 모니터링 시스템	주기적인 네트워크 상태 파악 및 특정 PC에 대한 접근 제어 수행
네트워크 상태 및 접근제어 모니터링 시스템	네트워크 상태 및 접근 제어 결과, 사용자별 행동 로그를 표시하는 웹 기반 대시보드를 사용자에게 표시

5.2 로그 수집 및 저장 시스템

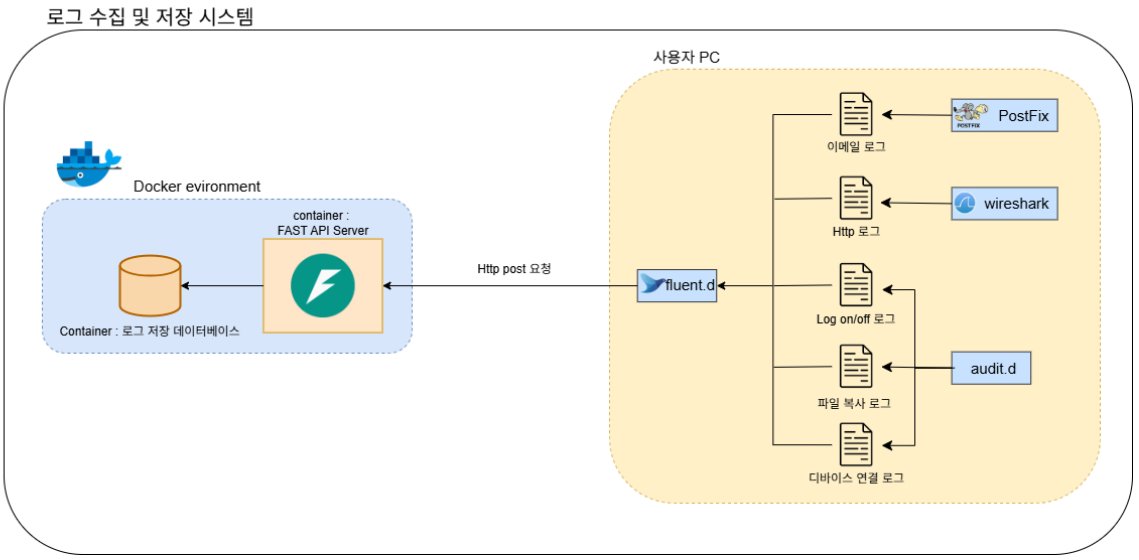

그림 2. 로그 수집 및 저장 시스템 구조도

로그 수집 및 저장 시스템은 사용자 단말에 설치되는 로그 수집 에이전트와, 수집된 로그를 데이터베이스에 저장하는 FastAPI 서버 으로 구성된다. 수집하는 로그의 종류는 다음과 같다.

로그	
행동 타입	field
log on/off	로그 Id, 사용자 Id, 날짜, 활동 종류 (log on or off)
파일 복사	로그 Id, 사용자 Id, 날짜, 파일 이름
HTTP 요청	로그 Id, 사용자 Id, 날짜, URL, Contents

Email	로그 Id, 사용자 ID, 날짜, From, To, Cc, Bcc, 이메일 크기, 첨부 파일 여부
Device	로그 Id, 사용자 ID, 날짜, 연결/연결 해제 여부

로그 수집 에이전트는 Python 기반으로 동작하며, Fluentd를 도입하여 사용자 PC에서 발생하는 다양한 사용자 행동 이벤트를 실시간으로 수집하고, HTTP POST 방식으로 FastAPI 서버에 전송한다. FastAPI 서버는 수신된 로그를 로그 저장 데이터베이스에 저장한다.

로그 수집 시스템	
모듈명	기능
Fluentd	사용자 단말에서 발생하는 로그온/로그오프, 이메일 송수신, 웹 브라우징, 파일 작업, 디바이스 연결 등 사용자 행동 이벤트 로그를 실시간으로 감지하고 수집한다.
	수집된 로그를 공통 JSON 포맷으로 정규화한다. 로그 발생 시각, 사용자 정보, 이벤트 유형, 관련 메타데이터 등의 필드를 포함하는 구조화된 형태로 구성한다.
	정규화된 로그를 HTTP POST 방식으로 FastAPI 서버에 전송한다.
FastAPI 서버	Fluentd로부터 전달된 로그를 수신하여 데이터베이스에 저장한다.

5.3 이상 행위 탐지 시스템

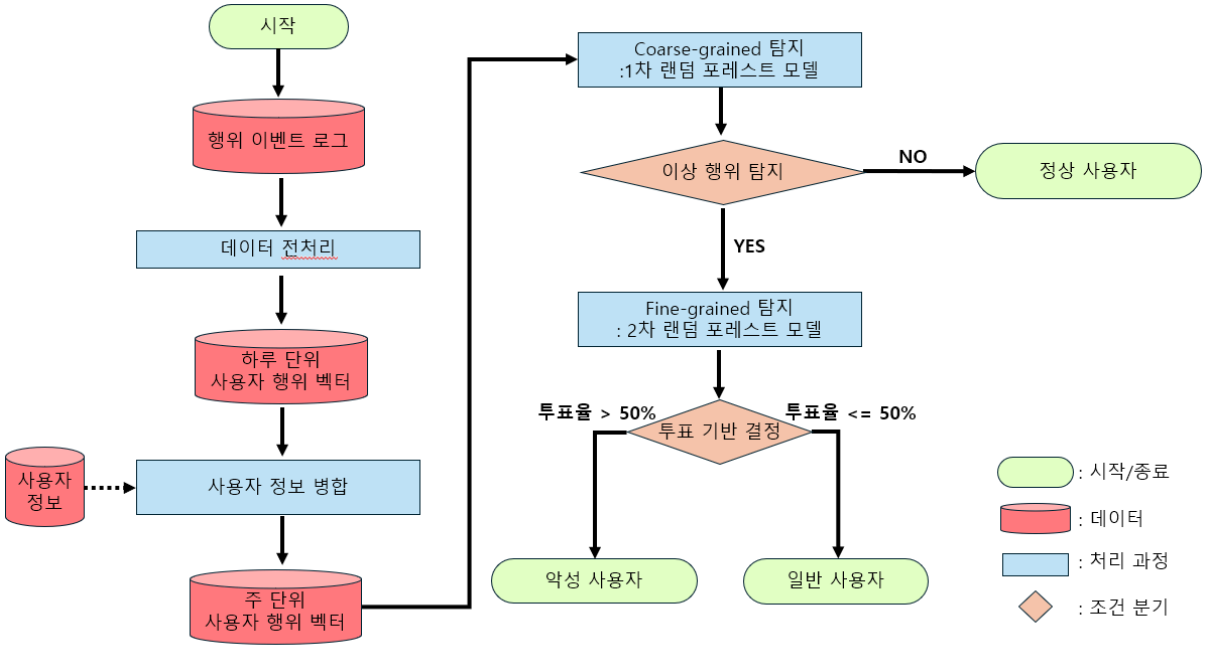

그림 3. 이상 행위 탐지 과정

이상 행위 탐지 시스템은 내부자 위협을 조기에 탐지하기 위해 사용자 행동 로그를 기반으로 이상 행위를 식별한다. 로그 수집 시스템으로부터 전달받은 데이터를 사용자 단위로 집계하고, 주요 행위 특징을 주 단위 벡터 형태로 추출한다. 전처리 과정을 통해 정상/이상 행위 분류에 적합한 형식으로 정제한 후, 사전에 학습된 이상 탐지 모델에 입력하여 위험도를 평가한다. 탐지 결과 위험도가 임계값 이상으로 높다면, 네트워크 접근 제어 시스템에 대상 PC에 대한 접근 제어 요청을 전달한다. 시스템 내 각 모듈의 기능은 다음과 같다.

이상 행위 탐지 시스템	
모듈명	기능
로그 파싱 및 저장 모듈	로그 저장 데이터 베이스에서 조회한 로그를 데이터 프레임으로 변환하고 저장한다.
로그 병합 모듈	사용자 ID, 날짜를 기준으로 group-by한 후 user-week 단위로 집계한다,
Feature 추출 모듈	다양한 로그에서 사용자 행동을 수치로 요약해, 주 단위 입력 벡터로 만든다.

전처리 모듈	결측치는 기본값으로 채우고, 값의 크기를 맞추기 위해 정규화한다. 이상치는 보정하며, 로그는 시간 순으로 정리해 주 단위 벡터로 만든다.
Coarse-Grained 탐지 모듈(CAD)	전체 사용자 로그를 기반으로 Random Forest를 이용하여 의심 사용자 후보군 선별한다.
Fine-Grained 탐지 모듈(FAD)	CAD로 탐지된 각 사용자에 대해 별도의 Random Forest 모델을 학습하여 정밀 탐지 수행한다.
이상 사용자 리포팅 모듈	이상 행동으로 판별 시 네트워크 접근 시스템에 접근 제어 요청 전달

5.4 네트워크 접근 제어 및 모니터링 시스템

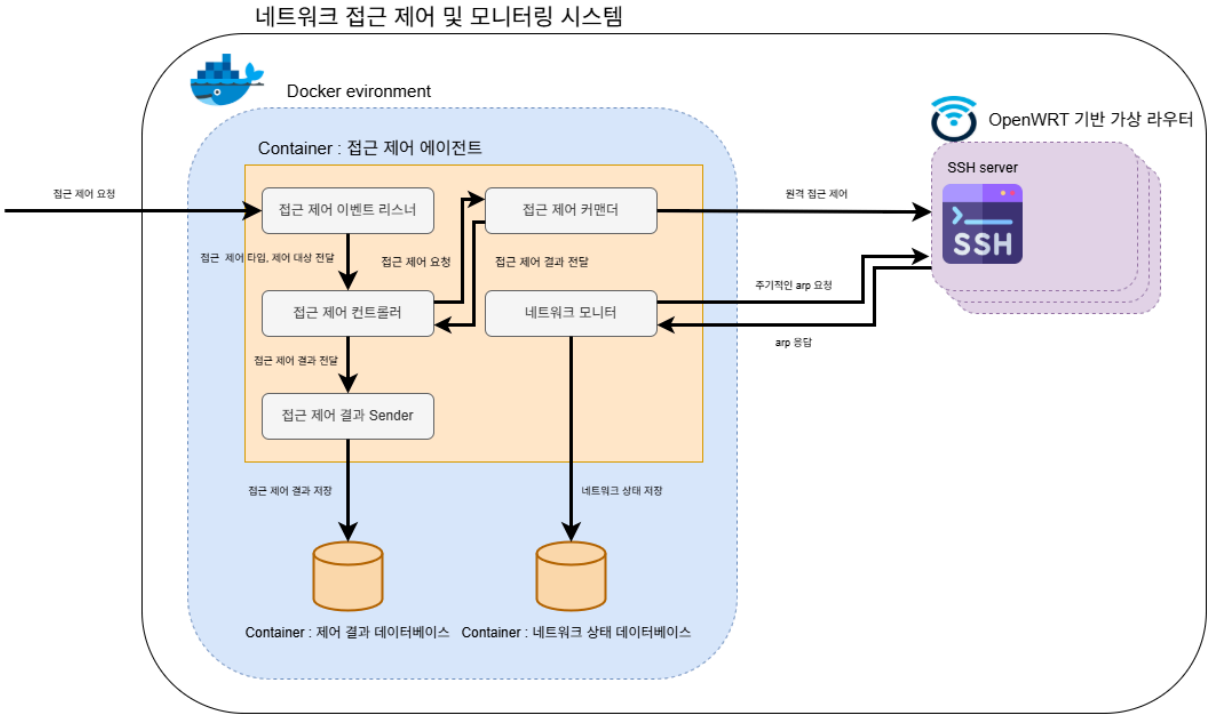

그림 4. 접근 제어 시스템 구조도

네트워크 접근 제어 시스템은 접근 제어 에이전트와 제어 요청 전송 대상인 openWRT 가상 라우터, 그리고 제어 결과를 저장하는 제어 결과 데이터 베이스와 네트워크 상태를 저장하는 상태 데이터 베이스로 구성된다.

openWRT 가상 라우터는 제어 및 모니터링 대상의 PC들의 SSH 서버를 구동해 접근 제어 에이전트의 원격 제어를 가능케한다.

접근 제어 에이전트는 메인 프레임의 도커 내 컨테이너 상에 설치되어, 접근 제어 요청 처리 및 결과 저장, 네트워크 모니터링 및 상태 저장들을 수행한다. 접근 제어 에이전트를 구성하는 모듈의 이름과 기능은 다음과 같다.

네트워크 접근 제어 에이전트	
모듈명	기능
접근 제어 이벤트 리스너	접근 제어 요청 이벤트가 발생하면, 발생한 요청의 매개변수인 접근 제어 타입(접근 허가/차단)과 접근 제어 대상 PC 정보(PC ID)를 접근 제어 컨트롤러에게 전달한다.
접근 제어 컨트롤러	이벤트 리스너로부터 전달된 매개변수를 기반으로 네트워크 테이블을 참조해 접근 제어 대상 PC가 위치한 서브넷의 게이트 웨이 라우터의 IP 주소를 결정한다.
	라우터의 ip 주소와 접근 제어 대상 정보(IP 주소, MAC 주소) 접근 제어 타입을 접근 제어 커맨더에 전달한다.
	접근 제어 시각, 대상 정보, 타입, 성공 여부를 접근 제어 결과 Sender에 전달한다.
접근 제어 커맨더	접근 제어 컨트롤러로부터 전달된 매개변수를 기반으로 가상 라우터에 SSH로 접속한다. iptable을 수정해서 접근 제어 대상 PC의 인바운드/아웃바운드 패킷을 허가/차단한다.
	접근 제어의 결과(성공/실패)를 접근 제어 컨트롤러에 전송한다.
네트워크 모니터	주기적으로 arp 요청을 보내 네트워크 상의 모든 PC의 정보(PC 식별자, IP 주소, MAC 주소), 해당 PC의 게이트 웨이 라우터 정보(IP 주소)를 pulling 한다.
	주기적으로 PC의 정보와 게이트웨이 라우터의 정보를 네트워크 상태 데이터베이스에 저장한다.
접근 제어 결과 Sender	접근 제어 결과(접근 제어 시각, 대상 정보, 타입, 성공 여부)를 제어 결과 데이터베이스에 저장한다.
	접근 제어 발생 신호를 모니터링 및 대시보드 시각화 시스템에 전달한다.

5.5 네트워크 상태 및 접근 제어 모니터링 시스템

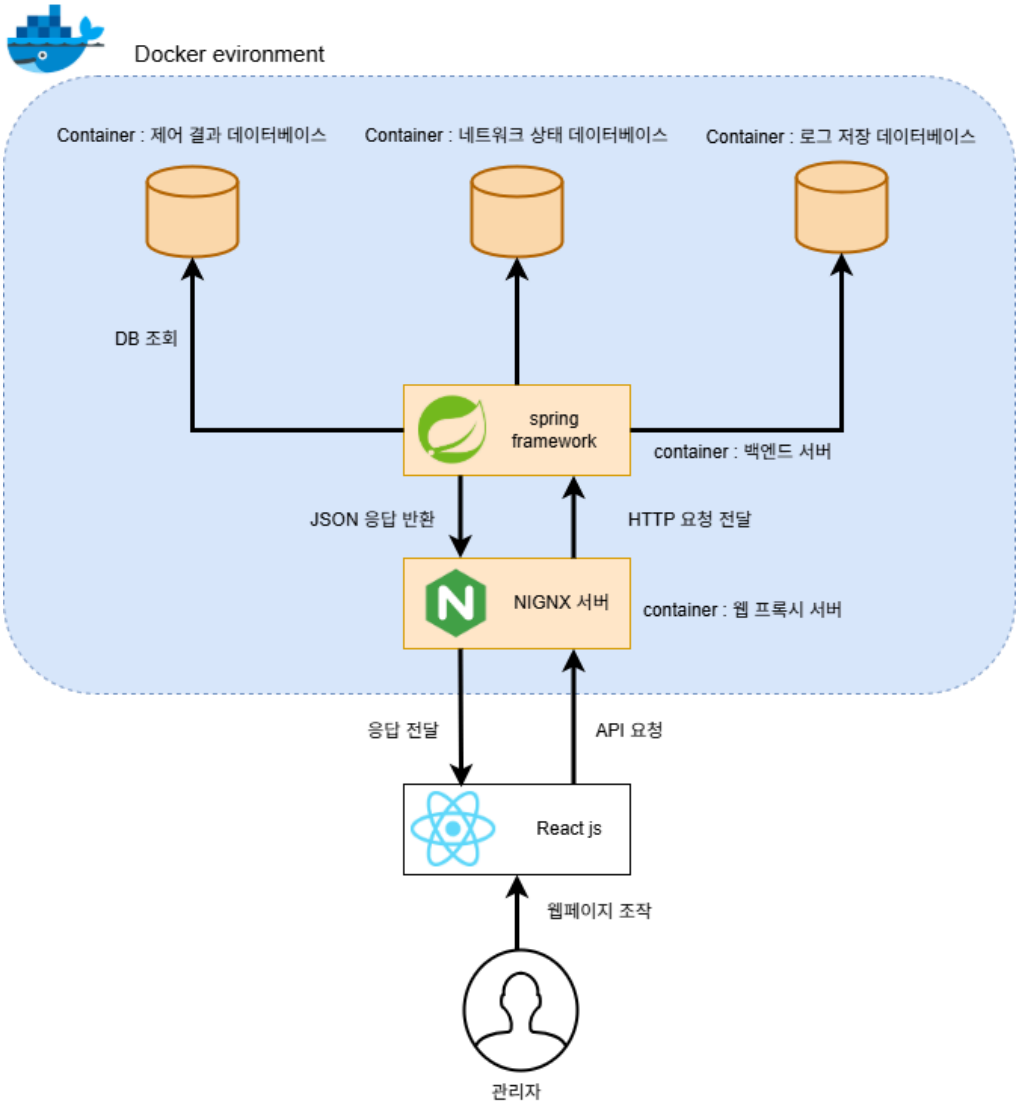

그림 5. 네트워크 상태 및 접근 제어 모니터링 시스템 구조도

본 시스템은 이상 행위 탐지 결과 및 네트워크 접근 제어 조치 현황을 관리자에게 직관적으로 제공하는 웹 기반 플랫폼이다. 실시간 모니터링, 경고 알림, 접근 제어 기록 조회, 로그 분석, 수동 제어 등의 기능을 제공한다.

기능 및 구현 방법	
기능	구현 방법
PC 상태 모니터링	네트워크 상태 데이터 베이스에 접근해, 전체 네트워크 상태 및 각 PC의 상태를 시각화한다.

접근 제어 알림	접근 제어 이벤트를 실시간으로 감지하고, 신호 발생 시 사용자 UI에 경고 팝업을 표시한다.
접근 제어 기록 조회	네트워크 접근 제어 및 모니터링 시스템의 제어 결과 데이터베이스에 접근해, 접근 제어 기록을 사용자 UI에 표시한다.
로그 조회	로그 저장 시스템의 데이터 베이스에 접근해, PC/유형/시간 별 정보를 사용자 UI에 표시한다.
수동 접근 제어	사용자의 수동 접근 제어 요청 이벤트 발생 시, 네트워크 접근 제어 및 모니터링 시스템에 요청을 API 형태로 전달한다.

6. 추진 체계 및 일정

기간 / 수행 내용	5월		6월					7월					8월					9월		
	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3
로그 수집 시스템																				
이상 행위 탐지 시스템																				
네트워크 접근 제어 시스템																				
Docker 통합 시스템 구축																				
웹 서비스 구현																				
테스트, 보완																				
최종보고서 작성																				

7/18 - 중간보고서 마감, 9/19 - 최종보고서 마감

7. 구성원 분담 역할

이름	역할
이광훈	네트워크 접근 제어 시스템 구현, 도커 시스템 구축
신해진	이상행위 탐지 머신러닝 모델 피팅 및 탐지 시스템 구현
조유진	로그 수집 및 저장 시스템 구현
공통	네트워크 상태 및 접근 제어 모니터링 시스템

8. 참고 문헌

[1] 김선애. “내부자 보안사고 기업 29%, 피해 복구액 14억 이상.” 데이터넷, 27 November 2024, https://www.datanet.co.kr/news/articleView.html?idxno=198095.

[2] Ponemon Institute. (2022). *2022* 내부자 위협의 비용 글로벌 보고서 [The cost of insider threats: Global report].Proofpoint.https://www.proofpoint.com/kr/resources/threat-reports/cost-of-insider-threats

[3] Farhadighalati, N., Estrada-Jimenez, L. A., Nikghadam-Hojjati, S., & Barata, J. (2025). A systematic review of access control models: Background, existing research, and challenges. *IEEE Access, 13*, 17777–17797. https://doi.org/10.1109/ACCESS.2025.3533145

[4] Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access, 12*, 30907–30922. https://doi.org/10.1109/ACCESS.2024.3369906

[5] B. Bin Sarhan and N. Altwaijry, ‘‘Insider threat detection using machine learning approach,’’ Appl. Sci., vol. 13, no. 1, p. 259, Dec. 2022.

[6] Feng, W., Cao, Y., Chen, Y., Wang, Y., Hu, N., Jia, Y., & Gu, Z. (2024). Multi-Granularity User Anomalous Behavior Detection. *Applied Sciences*, *15*(1), 128.