하이브리드 클라우드 환경에서의 머신러닝 기반 동적 보안 정책 적용 및 위협 탐지에 관한 연구

김건민[1], 김예진[1], 이은성[1], 장현지[1], 김경백[2]

전남대학교[1], 전남대학교 인공지능융합학과[2]

204869@jnu.ac.kr, ye031010@jnu.ac.kr, 200750@jnu.ac.kr, gka1225@jnu.ac.kr, kyungbaekkim@jnu.ac.kr

A Study on Dynamic Policy Enforcement Using Machine Learning in On-Premise and Cloud Hybrid Environments

Geonmin Kim[1], Yejin Kim[1], Eunseong Lee[1], Hyeonji Jang[1], Kyungbaek Kim[2]

Chonnam National University[1],
Dept. of Artificial Intelligence Convergence, Chonnam National University[2]

요 약

하이브리드 클라우드 환경은 기존의 온프레미스 환경의 견고성과 클라우드의 유연성을 결합함으로써 기업의 운영 효율성을 혁신적으로 향상시키고 있다. 그러나 이러한 이질적인 두 환경의 결합은 전통적인 경계 기반 보안 접근법의 한계를 드러내고 있다. 이에 따라 최근에는 하이브리드 클라우드 환경의 보안 및 성능 최적화에 AI를 기반으로 하는 접근법이 제안되고 있으며, 이를 실증하기 위하여 본 논문에서는 하이브리드 클라우드 환경에서 온프레미스와 퍼블릭 클라우드 간의 보안 격차를 해소하기 위한 머신러닝 기반 동적 보안 정책 적용 통합 보안 아키텍처를 제안하고, 실험을 통하여 그 효과를 논한다. 제안된 아키텍처는 프록시 게이트웨이와 OPA를 연동하여 API 트래픽을 중앙 집중식으로 제어하고, Elasticsearch와 Kibana를 통해 로그 데이터를 수집 및 분석한다. 또한, 머신러닝 모델로 수집된 로그를 학습하고, 학습된 결과를 바탕으로 동적으로 보안 정책을 업데이트하여 OPA 정책에 반영함으로써 정적으로는 탐지하기 어려운 공격 패턴을 효과적으로 식별한다.

Ⅰ. 서 론

최근 빅데이터와 클라우드 컴퓨팅의 급속한 발전으로 인해 전 세계 기업들은 이전과는 다른 방식으로 데이터를 처리하고 운영하게 되었다. 전통적인 온프레미스(On-Premise)[1] 환경은 데이터 저장과 운영을 기업 내부적으로 수행하여 데이터 보안과 물리적 통제에 강점을 지녔으나, 초기 구축 비용이 상당히 높고, 유연성과 확장성 측면에서 많은 제약이 따랐다. 또한, 정기적인 업데이트에 따른 지속적인 하드웨어 및 네트워크 인프라의 유지 관리 비용 또한 급속히 늘어나는 데이터의 양에 대응하기 어렵게 만들었다.

이러한 배경에서 클라우드 컴퓨팅이라는 새로운 패러다임이 등장하며 온프레미스 환경만을 활용하는 방식은 점차 비효율적으로 변하고 있다. 이에 기업들은 보다 유연하고 확장성이 뛰어난 대안을 모색하며 클라우드 기반으로 전환을 시작하였다. 클라우드 컴퓨팅은 초기 투자 비용을 획기적으로 낮추고, 필요에 따라 자원을 탄력적으로 할당할 수 있는 장점을 제공하여 기업의 IT 운영 효율성을 극대화하는 대안으로 부상하였다. 이러한 흐름 속에서 많은 기업들은 클라우드 시스템을 온프레미스 환경과 결합하여 하이브리드 클라우드 환경(Hybrid Cloud Architecure)[2]를 구축하는 방향으로 나아가고 있다. 하이브리드 클라우드 환경은 퍼블릭 클라우드(Public Cloud), 프라이빗 클라우드(Private Cloud) 그리고 온프레미스 인프라가 네트워크를 통해 상호 연결된 환경을 의미하며, 이를 통해 데이터와 애플리케이션이 원활하게 호환될 수 있도록 구성된다. 퍼블릭 클라우드는 아마존 웹 서비스(AWS), 마이크로소프트 에저(Azure), 구글 클라우드(GCP)와 같은 클라우드 서비스 제공업체를 통해 외부에서 인프라를 빌려 사용하는 방식이며, 프라이빗 클라우드는 특정 기업이 내부적으로 운영하는 클라우드 환경을 의미한다. 하이브리드 클라우드 환경은 이러한 퍼블릭 및 프라이빗 클라우드를 온프레미스 인프라와 결합하여, 기업이 필요에 따라 유연하게 자원을 할당하고 데이터 저장 및 처리 방식을 최적화할 수 있도록 지원한다. Flexera 2024 State of the Cloud Report에 의하면, 2024년 기준 73%의 기업이 하이브리드 클라우드 환경을 채택하고 있다.

그러나 온프레미스와 클라우드를 결합하는 하이브리드 환경은 이질적인 환경이 결합하여 네트워크의 경계가 모호해지고, 구조적 복잡성의 증가로 인해 보안 측면에서 새로운 위협 요인들이 대두된다.[3][4] 이러한 문제를 해결하기 위하여 보다 통합적이고 지능적인 보안 체계가 요구되며, 최근에는 인공지능(Artificial Intelligence) 및 생성형 인공지능(Generative AI)를 기반으로 한 새로운 보안 접근법들이 제안되고 있다.[5][6][7][8] 이에 따라 본 논문에서는 Kong Gateway를 기반으로 하는 프록시 게이트웨이 구조에 OPA(Open Policy Agent)를 결합하고, 여기에 머신러닝 기반의 이상 탐지 기법을 추가한 통합 보안 아키텍처를 제안한다. 본 아키텍처는 게이트웨이를 활용한 중앙 집중적인 API 통제를 통해 플랫폼 간 보안 일관성을 확보하고, 머신러닝 모델이 Elasticsearch에 기록된 로그를 바탕으로 실시간 이상 행위를 탐지하여 OPA의 Rego 정책을 동적으로 반영함으로써 지능형 공격에도 신속하게 대응할 수 있도록 설계되었다. 또한, Kibana를 활용하여 실시간 로그 시각화 및 분석을 지원함으로써 정책 실행 결과에 대한 가시성과 관리 편의성을 동시에 달성할 수 있도록 하였다.

Ⅱ. 전통적인 보안 모델의 하이브리드 클라우드 환경에서의 한계

전통적인 보안 모델은 네트워크 경계를 기준으로 내부와 외부를 명확히 구분하고, 외부로부터의 위협을 차단하기 위한 방화벽, 침입 탐지 시스템, 접근 제어 목록 등의 기술을 구축하는 방식으로 설계되었다. 이는 온프레

미스 환경에서 상당 기간 유효하게 기능하였으며, 기업 내부망과 외부망 간 트래픽을 체계적으로 통제함으로써 다수의 보안 위협을 사전에 방어할 수 있었다. 그러나 하이브리드 클라우드 환경은 퍼블릭 클라우드, 프라이빗 클라우드, 온프레미스 환경이 상호 연결된 구조로 네트워크 경계를 물리적으로 명확하게 설정하기 어렵다. 이는 전통적인 방화벽이나 경계 기반 보안 장비들이 효과를 발휘하기 어려운 환경을 만든다.

또한, 이러한 구조적 복잡성은 공격 표면을 크게 넓힌다. 단일 온프레미스 환경에서는 방화벽을 통과하는 지점이 명확하였으나, 하이브리드 클라우드 환경에서는 각기 다른 클라우드 서비스와 온프레미스 시스템을 가로지르는 트래픽이 다방면으로 발생한다. 기업 내부에서 운영되는 서비스가 퍼블릭 클라우드에 배포된 API를 호출하거나, 프라이빗 클라우드의 마이크로서비스가 온프레미스 데이터베이스에 접근하는 등 복합적인 시나리오가 빈번하여 전통적인 방식으로는 모든 상호작용 경로에 대해 일관된 보안 정책을 적용하기가 어려워진다.

더 나아가 하이브리드 클라우드 환경에서는 보안 정책이나 접근 제어에 대한 일관성 확보 또한 어렵다. 각각의 클라우드 서비스 제공 업체가 제공하는 보안 관리 도구나 API가 모두 상이[9]하며, 로깅 및 이벤트 수집 방식도 상이하여 단일한 정책으로 모든 환경을 동기화하기가 어렵다. 결국 하이브리드 클라우드 환경에서는 기존의 경계 기반 기술만으로는 모호한 네트워크 경계와 동적으로 변화하는 자원을 대상으로 일관된 정책을 빠르게 적용하기 힘들며, 새로운 형태의 공격을 효과적으로 탐지하기도 어렵다. 이러한 복잡성과 취약성을 극복하기 위해서는 더욱 지능적인 보안 접근법이 필요하며, 이에 따라 본 연구에서는 하이브리드 클라우드 환경에서 머신러닝 기반 동적 보안 정책 관리 시스템을 제안한다.

Ⅲ. 머신러닝 기반 동적 정책 적용 보안 아키텍처 설계

제안하는 통합 보안 아키텍처는 하이브리드 클라우드 환경 전반의 트래픽을 일관적으로 제어하기 위해 설계되었다. 이를 위해, API를 기반으로 트래픽 흐름을 제어하는 Kong Gateway를 통해 외부 요청이 모든 백엔드 서비스로 전달되는 경로를 단일화하고, 정책 결정 모듈인 OPA(Open Policy Agent)를 별도로 두어 요청 적합성 평가를 수행한 후 허용 또는 차단을 결정한다. 그동안 많은 보안 솔루션은 정적 시그니처를 기반으로 공격을 필터링하는 방식에 의존해 왔으나 이를 극복하기 위하여 본 연구에서는 머신러닝 기반 분석을 통해 새롭게 나타나는 공격 패턴을 실시간으로 학습하고, 그 결과를 정책 엔진에 동적으로 반영함으로써 지능적이고 유연한 방어 체계를 구성하고자 한다.

아키텍처 전반의 동작 흐름은 다음과 같다. 첫째, 다양한 소스(온프레미스와 클라우드 양쪽)에서 발생하는 API 요청들은 API 게이트웨이를 거치며, 게이트웨이는 해당 요청과 관련된 정보(메서드, 경로, 헤더, 사용자 에이전트 등)를 모두 로그로 남긴다. 이 로그들은 모두 Elasticsearch에 저장되어 축적된다. 머신러닝 분석 모듈은 일정 주기마다 축적된 로그를 수집해 정상 및 공격 여부를 분류하고, 공격으로 판결된 로그에서 새로운 키워드나 잠재적 위험 패턴을 추출한다. 이렇게 추출된 패턴은 정규 표현식 형태로 OPA에 전달되어 이후 동일한 패턴이 재등장하면 게이트웨이가 이를 자동으로 차단하게 된다. 이로써 공격자가 난독화나 변형 기법을 동원하더라도, 일정 횟수 이상의 시도가 관측되면 곧바로 정책에 반영되어 더 이상 통하지 않게 된다.

결국 본 아키텍처는 동적 정책 업데이트를 핵심 기제로 삼는다. 이는 정적 시그니처 기반 솔루션 대비 훨씬 민첩하게 환경 변화를 따라갈 수 있게 하며, 다양한 온프레미스와 클라우드 자원을 아우르는 하이브리드 보안 전략의 필수 요건을 충족한다. 게이트웨이와 정책 엔진, 머신러닝 분석 모듈, 그리고 대규모 로그 저장소로 구성된 본 통합 시스템은 고도화되는 데이터 탈취 시도 등의 공격을 보다 지속적이고 지능적으로 방어할 수 있도록 지원한다.

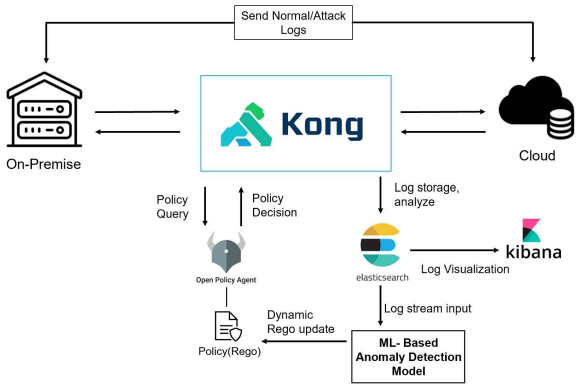

Fig 1. 실험 시나리오 도식도

1. 주요 구성 요소

Kong Gateway는 오픈소스 API 게이트웨이로, 모든 API 트래픽이 반드시 통과해야 하는 관문 역할을 한다. 외부 클라이언트 요청은 게이트웨이를 통해 내부 서비스로 라우팅 되며, 이 과정에서 인증, 인가, 로깅, 로드 밸런싱 등의 기능을 중앙에서 수행한다. 특히 보안 측면에서 게이트웨이가 OPA 정책 결정 모듈(정적 규칙 + 머신러닝에서 도출된 동적 규칙)을 호출하여, 요청에 담긴 정보가 사전에 정의된 정책 위배 요소가 있는지를 검사한다. 이를 통해 공격 추적과 차단을 일관적으로 수행할 수 있으며, 온프레미스와 클라우드 모두 동일한 게이트웨이를 거치므로 운영 환경이 여러 개라도 정책 관리가 단순해지는 장점을 갖는다.

정책 결정 모듈로 사용되는 OPA는 제로 트러스트 아키텍처(ZTA, Zero Trust Architecture)를 기초로 텍스트 형태의 규칙(정규 표현식, 사용자 정의 쿼리 등)과 JSON 기반 정책 언어를 사용하며, API 요청이 들어올 때마다 접근 허용 여부를 판별한다. 특히 본 시스템에서 OPA는 Kong Gateway를 이용한 중앙 집중식 접근 제어를 통해 온프레미스 및 클라우드에 맞추어 서비스마다 다르게 보안 정책을 관리할 필요 없이 일괄적인 정책 관리가 가능하다.

Elasticsearch는 오픈소스 분산 검색 엔진으로, 대량의 로그 데이터를 빠르게 저장하고 검색할 수 있는 도구이다. JSON 기반의 문서 데이터를 인덱싱하고, 이를 고속으로 조회할 수 있도록 설계되어 로그 수집, 데이터 분석, 모니터링 등에 널리 사용된다. 특히, 모든 로그는 logs 인덱스로 Elasticserach에 저장되며, 저장된 데이터는 추후에도 보안 이벤트 분석에 사용될 수 있다. Kibana는 Elasticsearch에 저장된 데이터를 시각화하여, 로그를 빠르게 분석할 수 있도록 지원하는 도구로, Kibana 대시보드를 통해 실시간으로 보안 이벤트를 시각화하여 분석할 수 있다.

머신러닝 분석 모듈은 정적 규칙으로는 탐지하기 어려운 공격을 식별하기 위해 사용된다. 본 연구에서는 TF-IDF 기반 벡터화 기법을 통해 로그의 문자열 특징을 추출한 뒤, 이를 랜덤포레스트 분류 모델에 입력하여 정상 및 공격을 판별한다. 공격으로 분류된 로그에서 상위 중요도의 단어를 추출하여, 이를 정규 표현식 형태로 변환하여 정책 결정 모듈에 공유한다. 이렇게 머신러닝 모델의 결과가 정책 결정에 반영되어 공격 패턴이 반복적으로 나타날 시 곧바로 차단 대상이 되어 방어 효율이 크게 향상된다.

2. 실험 로그 구성

실험을 진행하기 위하여 본 연구에서는 로그 생성 과정에서 정상 로그와 공격 로그를 구분하여 설계하였다. 모든 로그는 랜덤 난수(seed)를 통해 생성된다. 정상 로그는 정상 키워드 리스트를 활용하여 일반적인 API 호출, HTTP 요청, 사용자 입력, 데이터베이스 쿼리 등을 무작위로 생성한다. 공격 로그는 매 실험마다 생성되는 전체 로그 중 다른 비율로 다양한 형태의 악성 키워드를 포함하도록 의도적으로 삽입한다. 스크립트 태그를 사용한 XSS 페이로드, 시스템 명령어, Base64 인코딩 후 재인코딩한 난독화된 문자열, SQL Injection 등을 여러 비율로 넣는다. 또한, 공격 페이로드를 단순 텍스트 형태로만 넣는 대신, 난독화된 해시 문자열 사이에 끼워 넣거나, URL 인코딩으로 일부 문자를 변형하는 방식 등을 적용하여 단순한 정규식 패턴으로는 탐지가 어렵도록 구성하였다. 이러한 실험에 사용되는 모든 로그는 Elasticsearch에 저장되며, 추후 머신러닝 분석 모듈의 학습 데이터로 활용된다.

3. 로그 수집 및 분석 인프라 구축

프록시 게이트웨이로 채택된 Kong Gateway는 단순한 API 요청의 전달 역할을 넘어 온프레미스와 클라우드 간의 복잡한 데이터 이동 경로를 중앙 집중식으로 관리하는 핵심 구성 요소이다. Kong Gateway는 API 요청 발생 시 OPA와 연계해 미리 정의된 보안 정책을 적용하고 접근 제어를 수행한다. 보안 정책의 동적 관리 및 세밀한 접근 제어를 위하여 사용되는 OPA와 Kong Gateway와의 연동은 정책 변경 사항이 실시간으로 반영될 수 있도록 지원하며, 발생하는 모든 로그와 이벤트 정보는 모두 저장되어 추후 보안 체계 개선 및 정책 수정에 중요한 자료로 활용된다. 이러한 동적 정책 결정 메커니즘은 기존 정적 규칙에 의존한 보안 시스템이 갖는 한계를 극복하고, 변화하는 위협 환경에 신속하고 유연하게 대응할 수 있는 기반이 된다.

이 과정에서 발생하는 모든 로그와 이벤트는 Kafka를 통해 스트리밍되어 Elasticsearch에 기록된다. Elasticsearch와 Kibana는 대규모 로그 데이터를 신속하게 인덱싱하고, 검색할 수 있는 기능을 제공하므로, 이를 이용하여 시스템 전반에서 발생하는 보안 이벤트 및 API 호출 기록 등을 관리할 수 있다. 특히, 도중에 Elasticsearch와의 연결이 중단되더라도 로그 손실을 최소화하기 위하여 5회까지 연결을 재시도하는 안전장치를 추가하였다. Kibana는 Elasticsearch에 저장된 데이터를 시각화하여, 로그를 빠르게 분석할 수 있는 도구로, Kong Gateway를 거쳐 발생하는 API 요청 및 이 과정에서 발생하는 이벤트들이 Elasticsearch에 저장되면 Kibana를 이용하여 단순한 데이터 분석을 넘어 시간대별, 사용자별, 이벤트 유형별 등 다양한 차원의 데이터 시각화를 진행할 수 있으며, 이를 통하여 복합적인 보안 위협을 다각도로 분석할 수 있다.

4. 머신러닝 모델을 이용한 로그 분석 및 동적 정책 관리

정적 시그니처나 간단한 정적 정책만으로는 탐지하기 어려운 공격들을 가려내고, 동적으로 변화하는 공격 패턴을 빠르게 학습 및 대응하기 위하여 렌덤포레스트 머신러닝 모델을 도입한다. 머신러닝 모델은 TD-IDF 기반의 벡터화를 통해 URI, 헤더, User-Agent, 요청 본문 등에 포함된 문자열의 빈도 정보를 추출한 뒤, Randomforest 지도 학습 분류기를 사용하여 학습한다. 본 연구에서 사용되는 머신러닝 분석 모듈은 Elasticsearch에 저장된 로그 10,000개씩 나누어 학습하며, 1회차 학습에는 사전에 라벨링 되어 시뮬레이션 된 로그를 통하여 정상 로그와 공격 로그의 패턴을 학습한다. 이후 추가되는 로그들에 대하여 정상 로그인지 공격 로그인지 분석하고 분석된 보안 위협을 바탕으로 OPA의 보안 정책을 자동으로 동적으로 수정 및 추가한다. 이 정보는 정규표현식 기반의 Rego 정책으로 반영되며 OPA에 자동 업데이트됨으로써 보안 정책이 점진적으로 정교화된다. 지속적으로 발생하는 공격 로그들은 추가된 OPA 보안 정책의 패턴에서 식별되면 차단되는 체계로, 이러한 과정은 반복을 통하여 자동화된다. 머신러닝 모듈과 정책 모델 간의 피드백 루프를 형성을 통해 각 학습 라운드마다 탐지 정확도가 향상되었으며, 실험을 통해 그 효과를 정량적으로 입증하였다.

Ⅳ. 실험 결과 및 성능 분석

본 연구에서는 제안한 통합 보안 아키텍처의 효율성을 평가하기 위해 총 10회의 독립적인 실험을 수행하였다. 각 실험은 독립적인 환경에서 서로 다른 초기 조건과 공격 패턴으로 구성되어 있으며, 각 실험에서 10,000개의 로그를 학습 주기로 20회의 반복 학습 및 평가를 진행하였고, 이를 통해 시스템의 학습 능력과 동적 정책 갱신 효과를 평가하였다.

	공격 로그 차단율			
실험 회차	1회 학습	2회 학습	10회 학습	20회 학습
1회차	50.98%	53.36%	73.51%	97.30%
2회차	49.65%	51.93%	71.58%	97.38%
3회차	51.43%	52.46%	71.88%	97.59%
4회차	48.95%	54.13%	72.02%	97.65%
5회차	50.48%	52.56%	72.63%	97.19%
6회차	50.10%	52.90%	72.58%	97.71%
7회차	50.54%	54.30%	73.84%	97.54%
8회차	50.07%	51.68%	71.80%	97.78%
9회차	50.27%	52.87%	72.99%	97.53%
10회차	50.24%	51.84%	72.68%	97.54%
평균 차단율	97.52%			

Table 1. 제안 아키텍처에 대한 10회 실험 결과

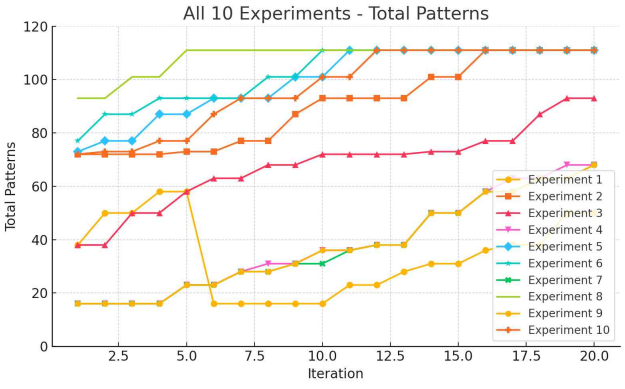

Fig 2. 10회 실험 별 OPA 정책 개수 변화

초기 실험 단계에서는 머신러닝 모델의 학습 부족으로 인해 공격 탐지 및 차단율이 평균 50% 전후로 나타나 다소 낮은 성능을 보였다. 그러나 반복적인 학습이 진행됨에 따라 공격 탐지의 정확도는 지속적으로 개선되어 실험 후반으로 갈수록 신규 공격 패턴에 대한 학습 효과가 두드러져 성능이 급격히 향상되었다. 특히 실험 반복 횟수가 증가함에 따라 시스템은 반복되는 공격 패턴을 정확하게 식별하여 정책 업데이트에 반영할 수 있었으며 최종적으로 모든 실험에서 차단율이 97%를 상회하였다. 이러한 결과는 제안된 아키텍처가 반복 학습과 실시간 정책 업데이트를 통해 매우 높은 정확도로 공격을 탐지하고 차단할 수 있음을 명확히 나타낸다. 전

체 10회 실험 결과 평균 공격 차단율은 97.52%로 이는 하이브리드 클라우드 환경에서 공격 대응을 위한 실질적인 보안 성능 측면에서 안정적인 성능을 보임을 입증한다.

이러한 성능 개선의 주요 원인은 시스템의 동적 정책 관리 기능에서 기인한 것으로 분석된다. 실험이 지속됨에 따라 정책 패턴이 평균적으로 증가하며 중반 이후부터는 최대 111개까지 확대되었다. 결론적으로, 본 연구를 통해 제안한 통합 보안 아키텍처는 반복 학습과 동적 정책 갱신을 통해 매우 높은 정확도의 공격 탐지와 차단 성능을 제공할 수 있음을 입증하였다. 이는 급변하는 하이브리드 클라우드 환경의 다양한 위협 환경에 신속하고 유연하게 대응할 수 있음을 보여준다.

V. 결론 및 향후 연구

본 연구에서는 온프레미스와 클라우드가 결합된 하이브리드 클라우드 환경에서 발생하는 보안 격차를 효과적으로 완화하고, 지능적이고 복합적인 공격에 효율적으로 대응하기 위하여 프록시 게이트웨이 및 OPA 기반 보안 아키텍처와 머신러닝 모듈을 결합한 모델을 제안하였다. 제안된 구조는 프록시 게이트웨이를 중심으로 API 트래픽을 중앙 집중형으로 제어하고, Elasticsearch와 Kibana를 활용하여 로그 분석 환경을 구성하였으며, 이와 동시에 머신 러닝 기반의 로그 분석 및 동적 정책 생성 메커니즘을 통합하여 지능형 공격 및 새로운 공격 패턴에 신속하고 유연하게 대응하고, 높은 정확도로 식별할 수 있음을 실험을 통해 입증하였다. 실험 결과, 프록시 게이트웨이와 동적 정책 관리를 결합한 환경은 97% 이상의 로그 차단율을 기록하였다. 이는 머신러닝 모듈이 시그니처 기반 정적 탐지로는 놓칠 수 있는 이상 행위를 Elasticsearch의 로그 데이터를 통해 비정상적 행위의 특성을 학습함으로써 고도화된 위협에 대해서도 방어력을 제공한다는 점을 보여준다. 이는 정적 규칙에만 의존하는 기존 보안 체계와 달리 데이터 기반 분석을 통하여 오탐과 누락을 줄이고 공격 유형을 세분화하여 더욱 정교한 보안 대응이 가능했음을 시사한다.

향후 연구에서는 더욱 다양한 유형의 공격 기법과 대규모 트래픽 상황을 고려한 추가 실험을 통해 실제 보안 환경에서의 다양한 공격 유형을 반영할 필요가 있다. 이번 연구에서는 SQL Injection, XSS, 난독화된 문자열 공격 등의 유형에 집중했으나 SSRF(Server-Side Request Forgery), CSRF(Cross-Site Request Forgery), 원격 코드 실행(RCE), DNS 바인딩 등의 공격도 고려하여 보다 다양한 공격 시나리오를 체계적으로 반영할 필요가 있다. 또한, 현재는 일정 주기로 로그를 수집하여 일괄적으로 학습하는 방식을 사용하였지만 보다 실시간에 가까운 대응을 구현하기 위하여 온라인 학습 방식이나 모델 경량화, 고속 처리 알고리즘을 도입하여, 보다 높은 트래픽 부하 상황에서도 지연 없이 신속한 대응이 가능하도록 추가적인 최적화 연구가 요구된다. 또한, 실무 적용을 위하여 NGINX Ingress Controller, Envoy Proxy 등 다양한 게이트웨이 활용도 함께 고려될 수 있다.

더 나아가, 제로 트러스트 아키텍처 개념을 본 시스템에 더욱 깊게 연계하는 것도 고려할 수 있다. 사용자 인증, 장치 상태, 네트워크 위치 등 다양한 맥락 정보를 활용하여 보다 정밀한 정책 판단이 가능하도록 OPA 정책을 확장할 수 있다. 반복적인 학습 과정을 통해 만들어지는 보안 정책들 간의 충돌이나 중복 문제도 고려해야한다. 정책 자동화와 충돌 관리를 위한 프레임워크를 구축하여 하이브리드 클라우드 환경 전반에서의 보안 가시성을 유지하면서도, 운영 복잡성을 낮추는 전략이 뒤따라야 한다. 이러한 후속 연구를 통하여 제안된 모델이 하이브리드 클라우드 보안 체계를 획기적으로 강화하는 핵심 요소가 될 수 있을 것으로 기대된다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-지역지능화혁신인재양성사업의 지원을 받아 수행된 연구임 (IITP-2025-RS-2022-00156287, 50%). 본 연구는 한국인터넷진흥원(KISA)-정보보안 특성화대학 지원사업의 지원을 받아 수행된 연구임(50%).

참 고 문 헌

[1] M. Gaianu, "On Premise Data Center vs CLOUD," 2023 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2023, pp. 1068-1071

[2] A. Leff and J. T. Rayfield, "Integrator: An Architecture for an Integrated Cloud/On-Premise Data-Service," 2015 IEEE International Conference on Web Services, New York, NY, USA, 2015, pp. 98-104

[3] S. B. Mallisetty, G. A. Tripuramallu, K. Kamada, P. Devineni, S. Kavitha and A. V. P. Krishna, "A Review on Cloud Security and Its Challenges," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2023, pp. 798-804

[4] G. Raktate, K. Shelar, P. Parjane, S. Pangavhane, S. More and S. R. Deshmukh, "A Survey on Security Issues and Challenges in Cloud Computing," 2024 International Conference on Decision Aid Sciences and Applications (DASA), Manama, Bahrain, 2024, pp. 1-5

[5] D. K. Seth, K. K. Ratra and A. P. Sundareswaran, "AI and Generative AI-Driven Automation for Multi-Cloud and Hybrid Cloud Architectures: Enhancing Security, Performance, and Operational Efficiency," 2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2025, pp. 00784-00793

[6] C. Anjani, R. M. Balajee, G. Divya, Y. S. Sree, K. Padmanabham and S. S. Srithar, "Evolving Threats and AI Solutions for Modern Hybrid Cloud Architectures," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 478-484

[7] S. J, K. Kanagasabapathi, K. Mahajan, S. Ahamad, E. Soumya and S. Barthwal, "AI-Enhanced Multi-Cloud Security Management: Ensuring Robust Cybersecurity in Hybrid Cloud Environments," 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2023, pp. 1-6

[8] Y. Mansouri, V. Prokhorenko, and M. A. Babar, “Anautomated implementation of hybrid cloud for performance evaluation of distributed databases,” J.Netw. Comput. Appl., vol. 167, p. 102740, Oct. 2020

[9] A. Mishra, P. Sarat and R. Afza, "A factual study on hybrid multi cloud cyber security threats and proposed methodologies to enable cyber resilience," 2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 2024, pp. 1-6