AWS CloudTrail 로그 기반 IAM 권한 자동 최적화 프레임워크

정현아[1], 문현종[2], 남재현[3]
[1]단국대학교 소프트웨어학과 학부생
[2]단국대학교 인공지능융합학과 석사과정
[3]단국대학교 컴퓨터공학과 교수

hyunaj@dankook.ac.kr, moonhj@dankook.ac.kr, namjh@dankook.ac.kr

A Framework for Automated Optimization of IAM Permissions using AWS CloudTrail Log Analysis

Hyeona Jung[1], Hyunjong Moon[2], Jaehyun Nam[3]
[1]Dept. of Computer Science, Dankook University (Undergraduate Student)
[2]Dept. of AI-based Convergence, Dankook University (Graduate Student)
[3]Dept. of Computer Engineering, Dankook University (Professor)

요 약

기존의 AWS IAM 보안 솔루션인 AWS Access Analyzer, Policy Sentry, Parliament 등은 주로 정적 분석에 기반한 기능을 제공하며, 실시간 로그 기반의 권한 최적화 및 자동화 측면에서는 한계가 존재한다. 이러한 한계를 보완하고자, 본 연구에서는 AWS CloudTrail 로그 데이터를 활용하여 불필요한 역할 및 권한을 자동으로 식별하고, 최소 권한 원칙에 따라 이를 최적화하는 시스템을 제안한다. 제안된 시스템은 실시간으로 권한 사용 패턴을 분석하고, 과도하게 부여된 권한은 제거하며, 업무 수행에 필요한 권한은 자동으로 추천함으로써 정책의 정밀도를 높인다. 이를 통해 보안성을 강화하는 동시에 효율적인 IAM 정책 관리가 가능하며, 본 연구에서는 이를 실험을 통해 검증하였다.

1. 서론

클라우드 인프라의 확산에 따라 보안 관리 체계에서도 정교한 접근 제어의 중요성이 증대되고 있다. Microsoft Azure, Google Cloud Platform (GCP), Amazon Web Services (AWS) 등 주요 클라우드 플랫폼은 다양한 권한 관리 기능을 제공하고 있으며, 본 논문은 그 중에서도 대표적인 사례로 AWS 의 IAM (Identity and Access Management)을 중심으로 논의를 전개한다.

AWS IAM 은 사용자, 서비스, 리소스 간의 권한을 세분화하여 제어할 수 있는 기능을 제공하고 있다. 그러나 실제 운영 환경에서는 권한 요구사항의 복잡성과 정책 구성의 어려움으로 인해 과도하게 높은 권한이 부여되는 사례가 빈번하게 발생하고 있으며, 이는 내부자 오용이나 외부자 침입과 같은 심각한 보안 위협으로 이어질 수 있다.

이를 해결하기 위해 AWS Access Analyzer [1], Policy Sentry [2], Parliament [3] 등 다양한 도구들이 개발되고 있다. 하지만 이들 도구는 대부분 활동 로그를 기반으로 권한 사용 현황을 분석하는 데에 한정되어 있으며, 자동화된 방식으로 실시간 최적화 정책을 생성하거나 과도한 권한을 제거하는 데에는 제한적인 기능만을 제공하고 있다.

본 연구에서는 CloudTrail 로그를 기반으로 사용자 및 역할의 실제 권한 사용 패턴을 실시간으로 식별하고, 불필요한 권한을 제거하는 동시에 최적화된 IAM 정책을 자동으로 생성하는 시스템을 제안한다. 본 제안은 IAM 정책 설계의 복잡성을 완화하고, 보안성과 운영 효율성을 동시에 향상시키는 것을 목표로 한다.

2. 기존 IAM 보안 솔루션 분석

IAM 정책의 복잡성과 과도한 권한 부여 문제를 해결하기 위해 다양한 보안 도구들이 개발되어 왔다. 이들 도구는 주로 정적 정책 분석과 최소 권한 정책 생성을 중심으로 기능을 제공하고 있으며, 실무 환경에서의 정책 검토 및 구성 작업을 지원한다.

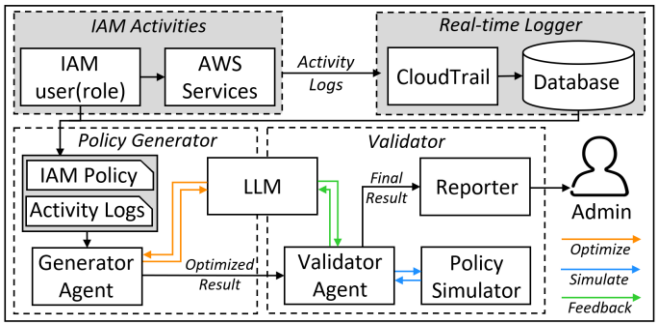
<표 1> 기존 IAM 보안 솔루션 비교 분석 표

구분	Access Analyzer	Policy Sentry	Parliament
최소 권한 원칙 설정	O	O	O
로그기반 분석 및 추적	O	X	X
IAM 정책 검증	O	O	X
실시간 정책 최적화	O	X	X

<표 1>은 대표적인 IAM 정책 보안 도구 세 가지에 대한 기능 비교를 보여준다. Access Analyzer 는 CloudTrail 로그 기반의 분석 기능을 제공하지만, EC2

및 RDS 등 일부 리소스에 한정된 권한 최적화 제안만을 제공하는 제한점이 존재한다. 반면, Policy Sentry와 Parliament 는 최소 권한 기반 정책 생성을 지원하지만, 실시간 로그 분석이나 자동화된 정책 최적화 기능은 지원하지 않는다. 이는 현재의 IAM 보안 솔루션이 실시간성과 자동화 측면에서 여전히 미흡함을 시사한다.

3. IAM 권한 최적화 시스템 설계



(그림 1) 로그 분석 기반 IAM 권한 최적화 시스템 아키텍처

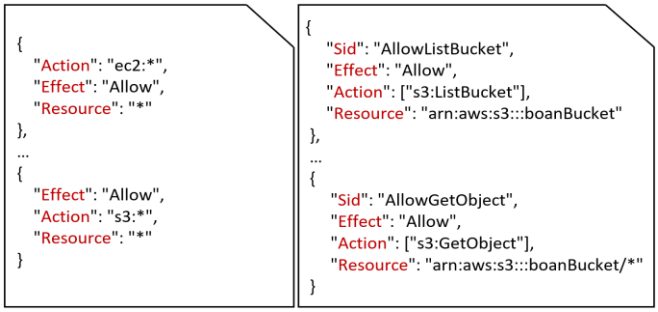
이러한 기존 솔루션의 한계를 극복하기 위해, 본 연구에서는 LLM 기반의 실시간 로그 분석과 정책 생성을 통합한 IAM 최적화 시스템 아키텍처를 제안한다. 제안된 아키텍처는 <그림 1>과 같이 구성된다.

본 시스템은 크게 세 가지 주요 구성 요소로 구분된다. 첫째, Policy Generator 는 CloudTrail 로그로부터 수집한 활동 기록과 기존 IAM 정책을 기반으로, LLM 에 입력할 최적화 후보 데이터를 생성한다. LLM 은 이를 바탕으로 최소 권한 원칙에 부합하는 IAM 정책을 자동 생성하며, 이 과정에서 실제 사용된 액션 및 리소스를 중심으로 권한을 재구성한다. 둘째, Validator 는 생성된 정책의 실행 가능성과 안전성을 AWS Policy Simulator 를 통해 시뮬레이션하고, 그 결과를 다시 LLM 에 피드백함으로써 정책을 반복적으로 개선한다. 셋째, Reporter 는 최종적으로 생성된 정책과 관련된 분석 결과를 관리자에게 직관적으로 제공하며, 정책 검토와 의사결정의 효율성을 지원한다.

이러한 구조는 반복적이고 수작업 중심이던 정책 검토 작업을 자동화함으로써 관리 효율성을 향상시키며, AWS Policy Simulator 를 통한 시뮬레이션 결과를 다시 LLM 에 반영하여 결과를 보완함으로, 정책의 신뢰성과 정확성을 동시에 확보할 수 있다.

4. 실험 및 결과

제안한 시스템의 실효성을 검증하기 위해, AWS 환경에서 CloudTrail 을 활용하여 실시간 활동 로그를 수집하였으며, 수집된 로그는 S3 버킷(Database)에 저장되었다. 정책 생성을 담당하는 Generator Agent 와 검증을 수행하는 Validator Agent 는 각각 AWS Lambda 기반의 서버리스 아키텍처로 구현되었고, OpenAI 기반 LLM API 와 AWS Policy Simulator 를 활용하여 정책 생성을 수행하였다.



(그림 2) 기존 과부여 정책 및 제안 시스템 기반 정책 비교

<그림 2>는 기존 과도한 권한이 부여된 정책과 제안 시스템을 통해 생성된 최소 권한 정책 간의 차이를 비교한 결과이다. 좌측의 초기 정책은 "Action": "*" 및 "Resource": "*"와 같이 모든 작업과 리소스를 허용하는 형태로, 실제 사용 목적과 무관하게 과도한 권한이 부여되어 있다. 반면, 우측의 최적화된 정책은 "s3:ListBucket" 및 "s3:GetObject"와 같은 실제 수행된 작업만을 포함하고 있으며, 특정 S3 버킷에 한정된 리소스를 대상으로 한다. 이처럼 제안 시스템은 CloudTrail 로그 기반 분석을 통해 불필요한 권한을 제거하고 실제 업무에 필요한 최소 권한만을 반영하는 정책을 자동으로 생성할 수 있다. 또한 AWS Policy Simulator 결과를 통해 해당 정책이 기능 수행에 충분함이 검증되었으며, 과도한 권한 없이도 정상적인 작업 수행이 가능함을 입증하였다.

5. 결론

본 연구는 기존 IAM 정책 보안 솔루션의 한계점을 분석하고, 실시간 활동 로그를 활용한 동적 권한 최적화 방식을 제안하였다. 제안된 시스템은 CloudTrail 로그를 기반으로 실제 권한 사용 패턴을 분석하여, 과도하게 부여된 권한을 제거하고 필요한 권한만을 자동으로 도출함으로써 정책의 최소 권한 원칙을 효과적으로 실현한다. 실험을 통해 본 시스템이 IAM 정책 관리의 보안성과 운영 효율성을 동시에 향상시킬 수 있음을 확인하였다. 향후에는 다양한 리소스와 멀티 계정 환경으로의 확장 및 LLM 기반 전략 비교를 통해 시스템의 정밀도와 범용성을 더욱 향상시킬 수 있을 것으로 기대된다.

Acknowledgement

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학 ICT 연구센터(ITRC)의 지원을 받아 수행된 연구임. (IITP-2025-RS-2023-00258649)

참고문헌

[1] AWS, “How IAM Access Analyzer findings work”, https://docs.aws.amazon.com/IAM/latest/UserGuide/access-analyzer-concepts.html, 2025.

[2] Salesforce, “Policy Sentry”, https://github.com/salesforce/policy_sentry, 2025

[3] duo-labs, “Parliament”, https://github.com/duo-labs/parliament, 2025