Automated Allowed-Only Detection Scenario Based on AWS CloudTrail and Athena*

Ye-Eun Shin[1], Sun-Woo Kwon[1], Soo-Min Nam[1] and Seongmin Kim[2]†

1 Undergraduate Student, Department of Convergence Security Engineering, Sungshin Women's University

2 Professor, Department of Convergence Security Engineering, Sungshin Women's University

{20220124,20231061,20231076,sm.kim}@sungshin.ac.kr

Abstract

This study presents an AWS log-based dynamic privilege validation framework to mitigate over-privileged access in cloud environments. By integrating CloudTrail, Athena, Lambda, EventBridge, and SNS, the system automatically identifies allowed-only permissions (granted but unused) and notifies administrators in real time. The results demonstrate enhanced verification efficiency and more effective security management compared with traditional manual audits, as the framework enables continuous privilege validation and control without operator intervention.

Keywords *– Allowed-only permission detection, IAM privilege validation, Lambda-based log analysis, Automated least privilege enforcement, Real-time SNS alert*

1 Introduction

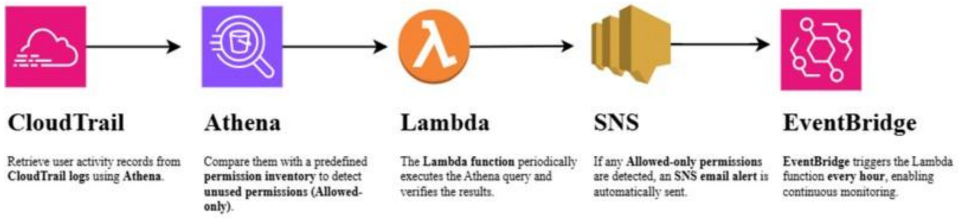
Recently, excessive permissions in cloud IAM policies are a major cause of security breaches. To address the limitations of manual audits, such as low cadence and inconsistent accuracy, we introduce a log-based automated privilege validation framework with a permission-minimization baseline derived from IAM and Cognito activity logs. Our system integrates AWS CloudTrail, Athena, Lambda EventBridge, and SNS to continuously compare policy-granted permissions with actual usage and automatically flag allowed-only permissions (granted but unused). Detected cases are immediately delivered to administrators via SNS email alerts, enabling timely remediation and stronger least-privilege enforcement at scale.

2 Design and Implementation

Figure.1 illustrates the overall workflow of the proposed privilege validation framework. We integrate multiple AWS services to form an automated cycle of 1) periodic privilege validation, 2) alert notification, and 3) administrator feedback. The implementation proceeds as follows: AWS Lambda is granted access to Athena, S3, Glue, SNS, and CloudWatch, enabling query execution, result storage, log recording, and alert delivery [1]. Using an external Athena table, CloudTrail logs are analyzed to aggregate user-level privilege usage and identify allowed-only permissions, those granted but never invoked. When such abnormal permissions are detected from the Athena query results, Lambda triggers an SNS alert to notify administrators in real time. Meanwhile, EventBridge automates periodic execution every hour through a rate(e.g., an hour) scheduling configuration [2].

* Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-12, December 16-18, 2025, Sapporo, Japan. © The copyright of this paper remains with the author(s).

† Corresponding author



CloudTrail

Retrieve user activity records from **CloudTrail logs** using **Athena**.

Athena

Compare them with a predefined **permission inventory** to detect **unused permissions (Allowed-only)**.

Lambda

The **Lambda function** periodically executes the Athena query and verifies the results.

SNS

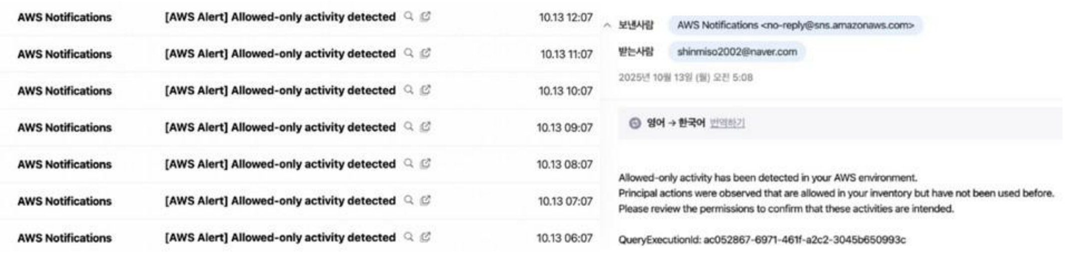
If any **Allowed-only permissions** are detected, an **SNS email alert** is automatically sent.

EventBridge

EventBridge triggers the Lambda function **every hour**, enabling continuous monitoring.

Figure 1. Overall Workflow of the log-based privilege validation framework

As shown in Figure 2, the Athena query executed successfully, and an automated alert email was delivered through AWS SNS. This confirms that the system functioned as intended, detecting allowed-only permissions (granted but unused) and notifying administrators in real time. The notification message includes the QueryExecutionId, allowing administrators to directly review detailed query results in the Athena console. These experiments verified that the proposed framework operates as an automated privilege validation cycle. Furthermore, by leveraging EventBridge's hourly scheduling, the system demonstrated sustainable, long-term monitoring capability. Overall, the system achieved an automated and repeatable privilege validation process capable of real-time detection and response with minimal operator intervention. The results demonstrated that the system can effectively identify and control over-privileged permissionswith improved efficiency and accuracycompared to traditional manual auditing methods. We plan to extend our framework by integrating it with AWS Access Analyzer for enhanced static analysis and advanced anomaly detection using machine learning.



AWS Notifications [AWS Alert] Allowed-only activity detected 10.13 12:07
AWS Notifications [AWS Alert] Allowed-only activity detected 10.13 11:07
AWS Notifications [AWS Alert] Allowed-only activity detected 10.13 10:07
AWS Notifications [AWS Alert] Allowed-only activity detected 10.13 09:07
AWS Notifications [AWS Alert] Allowed-only activity detected 10.13 08:07
AWS Notifications [AWS Alert] Allowed-only activity detected 10.13 07:07
AWS Notifications [AWS Alert] Allowed-only activity detected 10.13 06:07

보낸사람 AWS Notifications <no-reply@sns.amazonaws.com>
받는사람 shinmiso2002@naver.com
2025년 10월 13일 (월) 오전 5:08

영어 → 한국어 번역하기

Allowed-only activity has been detected in your AWS environment.
Principal actions were observed that are allowed in your inventory but have not been used before.
Please review the permissions to confirm that these activities are intended.

QueryExecutionId: ac052867-6971-461f-a2c2-3045b650993c

Figure 2. Demonstration examples: SNS E-Mail Alerts

References

1. Invoking AWS Lambda functions using Amazon SNS, AWS Lambda Developer Guide, Amazon Web Services, 2025. [Online]. Available: https://docs.aws.amazon.com/lambda/latest/dg/with-sns.html
2. Using EventBridge Scheduler, Amazon EventBridge User Guide, Amazon Web Services, 2025. [Online]. Available: https://docs.aws.amazon.com/eventbridge/latest/userguide/using-eventbridge-scheduler.html