



PROJECT REPORT
DETECTION OF IAM VULNERABILITIES IN
GOOGLE CLOUD PLATFORM (GCP) USING
XGBOOST

LEONARD THEO PURNOMO
22.K1.0003

Faculty of Computer Science
Soegijapranata Catholic University
2026

ABSTRACT (ABSTRACT TITLE)

In the era of increased adoption of cloud services, Identity and Access Management (IAM) have emerging as an critical pillar for cloud infrastructure security, especially due to the rised number of incidents caused by complex misconfigurations and privilege exploitation. While previous studied have highlighted the severity of IAM-related risks, many remain conceptual and lack validation used practical data pipelines. This studies proposes an supervised machine learning approach to automatically classify IAM configurations in the Google Cloud Platform (GCP) environment as either safe or risky. The dataset were extracting from raw GCP audit logs within an designated sandbox (project-skripsi-477915) and processing into an structured tabular format used RobustScaler and an targeted heuristic feature is `is_dangerous_method`. To resolve severed class imbalance and minimize high-entropy noise, Random Over-sampling were applied to balance the training samples, following by Principal Component Analysis (PCA) optimized to retain five principal components ($n=5$). The structural data were then utilized to train a Extreme Gradient Boosting (XGBoost) model, where hyperparameter optimization achieving an stable convergence at `learning_rate=0.05` and `max_depth=6`. The final optimized model demonstrating robust cybersecurity performance with an global accuracy of 66.13% and an significant recall of 71% for the Risky class, successfully capturing 44 out of 62 actual privilege escalation threats. These findings imply that the proposes method serves as a effective, proactive filtered tool for cloud administrators to detecting stealthy IAM vulnerabilities before they can be maliciously exploited.

Keywords: IAM vulnerabilities, Google Cloud Platform, XGBoost, machine learning, data augmentation