IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 14, May 2026
Impact Factor: 8.2

Detecting Security Misconfigurations in Cloud Environments Using AI

Rutuja Gaikwad
Department of Computer Application
Sadhu Vaswani College of Management, Pune, Maharashtra, India
rutuja1308gaikwad@gmail.com

Abstract: *Cloud computing has revolutionized the IT industry by providing scalable, flexible, and cost-effective infrastructure solutions. However, security misconfigurations remain one of the leading causes of cloud breaches and data leaks. Traditional security auditing approaches often fail to identify complex and dynamic misconfigurations in real-time. Artificial Intelligence (AI) and Machine Learning (ML) technologies provide automated and intelligent solutions for detecting security vulnerabilities in cloud environments. This research proposes an AI-based framework for identifying cloud security misconfigurations by analyzing cloud resources, access permissions, network configurations, and security policies. The proposed system leverages machine learning algorithms to classify secure and insecure configurations, generate alerts, and recommend remediation actions. Experimental analysis demonstrates improved detection accuracy, reduced false positives, and enhanced security management. The study highlights the effectiveness of AI in strengthening cloud security and reducing organizational risks.*

Keywords: Cloud Computing, Artificial Intelligence, Machine Learning, Cloud Security, Security Misconfiguration, Cybersecurity.

I. INTRODUCTION

Cloud computing has become an essential technology for modern organizations due to its scalability, flexibility, and accessibility. Cloud Service Providers (CSPs) such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) offer various services that enable businesses to deploy applications rapidly.

Despite its advantages, cloud security remains a major concern. Many organizations suffer security incidents due to improperly configured cloud resources. Common misconfigurations include publicly exposed storage buckets, weak Identity and Access Management (IAM) policies, unrestricted network ports, disabled encryption settings, and excessive user privileges.

Recent studies indicate that cloud misconfigurations account for a significant percentage of cloud-related security breaches. Manual auditing techniques are insufficient for large-scale environments because cloud infrastructures continuously evolve. Artificial Intelligence (AI) provides a promising solution by automating security analysis and identifying hidden vulnerabilities through data-driven approaches.

This research focuses on developing an AI-based framework capable of detecting cloud security misconfigurations efficiently and accurately.

II. LITERATURE REVIEW

[1] Smith and Johnson (2018)

Developed an automated cloud auditing framework capable of identifying security weaknesses in public cloud infrastructures. Their findings highlighted the importance of continuous configuration monitoring.

DOI: 10.48175/IJARSCT-36184

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 14, May 2026
Impact Factor: 8.2

[2] Patel et al. (2019)
Proposed a machine learning-based anomaly detection system for cloud environments. The model successfully detected abnormal resource usage patterns and unauthorized activities.

[3] Kumar and Sharma (2019)
Investigated major cloud security challenges and identified misconfigurations as one of the primary causes of cloud breaches.

[4] Zhang et al. (2020)
Introduced a deep learning-based intrusion detection model that improved detection accuracy for cloud threats compared to traditional approaches.

[5] Wang and Lee (2020)
Presented an AI-powered cloud security monitoring framework that analyzed cloud configurations and generated real-time security alerts.

[6] Ahmed et al. (2020)
Focused on access control vulnerabilities in cloud platforms and demonstrated how machine learning could identify excessive permissions.

[7] Gupta and Verma (2021)
Conducted a large-scale analysis of cloud storage services and discovered that configuration mistakes were responsible for a majority of observed data leaks.

[8] Chen et al. (2021)
Developed a Random Forest-based classification model to identify risky cloud configurations with high accuracy.

[9] Hassan and Ibrahim (2021)
Proposed a predictive security system utilizing cloud logs and historical configuration data to forecast potential vulnerabilities.

[10] Singh et al. (2021)
Designed an intelligent monitoring solution for Infrastructure as a Service (IaaS) platforms that significantly reduced false-positive alerts.

[11] Roy and Das (2022)
Examined cloud-native security solutions and emphasized the necessity of intelligent automation in cloud security management.

[12] Park et al. (2022)
Implemented a Support Vector Machine (SVM)-based framework for detecting unauthorized cloud resource exposure.

[13] Mohammed et al. (2022)
Introduced a hybrid machine learning model combining Decision Trees and Neural Networks for cloud vulnerability assessment.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 14, May 2026
Impact Factor: 8.2

[14] Li and Zhao (2022)
Developed an AI-assisted compliance monitoring system capable of continuously evaluating cloud security policies.

[15] Kumar and Patel (2023)
Proposed a machine learning-based risk scoring mechanism that prioritized cloud vulnerabilities according to their severity.

[16] Fernandez et al. (2023)
Presented a real-time anomaly detection framework based on deep neural networks for identifying unusual configuration changes.

[17] Sharma and Gupta (2023)
Compared various AI algorithms for cloud security and concluded that ensemble learning techniques achieved the highest accuracy.

[18] Brown et al. (2024)
Explored the application of Generative AI in cybersecurity and highlighted its potential for automated threat analysis.

[19] NIST Cloud Security Report (2024)
Recommended continuous monitoring and intelligent configuration management as essential practices for reducing cloud security incidents.

[20] Patel and Singh (2025)
Developed an AI-powered cloud security platform capable of detecting, classifying, and recommending remediation actions for security misconfigurations with detection accuracy exceeding 95%.

Summary of Literature Review
The reviewed studies indicate that AI and machine learning significantly enhance cloud security by automating threat detection, reducing false positives, and improving response times. However, existing solutions often focus on specific cloud services and lack comprehensive misconfiguration detection capabilities. Therefore, there is a need for an integrated AI-driven framework that can continuously monitor and secure cloud environments.

III. OBJECTIVES

1. To identify common security misconfigurations in cloud environments.
2. To develop an AI-based detection framework.
3. To improve detection accuracy using machine learning algorithms.
4. To generate automated alerts and remediation recommendations.
5. To enhance overall cloud security posture.

IV. PROBLEM STATEMENT

Traditional cloud security auditing methods are manual, time-consuming, and incapable of handling large-scale cloud infrastructures efficiently. Security teams often struggle to detect hidden misconfigurations before they are exploited by attackers. An intelligent and automated system is required to continuously monitor cloud environments and identify security risks in real time