Cloud Security Posture Management System for Detecting Misconfigurations in AWS Environments

Mrs. Pratibha Soni[1], Animesh Kumar[2], Lalit Yadav[2], Aryan Sharma[2]

[1]Assistant Professor, Jagannath University, Jaipur, India

[2]Department of Computer Science & Engineering, Jagannath University, Jaipur, India

DOI: https://dx.doi.org/10.51244/IJRSI.2026.1306000102

Received: 22 May 2026; Accepted: 27 May 2026; Published: 25 June 2026

ABSTRACT

Cloud computing has become an essential component of modern IT infrastructure, but it also introduces significant security challenges, particularly due to misconfigurations in cloud environments. These misconfigurations often lead to data breaches, unauthorized access, and compliance violations. This paper presents a Cloud Security Posture Management (CSPM) system designed to identify and mitigate security risks in Amazon Web Services (AWS) environments. The proposed system utilizes automated data collection techniques through AWS APIs to analyze configuration settings and detect vulnerabilities based on predefined security rules. The system further classifies risks and generates detailed reports with actionable recommendations. The implementation focuses on improving visibility, ensuring compliance, and reducing human error in cloud security management. Experimental results demonstrate that the system effectively identifies critical misconfigurations and enhances the overall security posture. This approach provides a scalable and efficient solution for securing cloud infrastructures in real-world applications.

Keywords

Cloud Security, AWS, CSPM, Misconfiguration Detection, Cloud Computing, Cybersecurity

INTRODUCTION

Cloud computing has revolutionized the way organizations store, manage, and process data by providing scalable, flexible, and cost-effective infrastructure solutions. Platforms such as Amazon Web Services (AWS) enable rapid deployment of applications and services without the need for heavy on-premise infrastructure. However, with this increased adoption, security has become a major concern, particularly due to improper configuration of cloud resources.

One of the most critical challenges in cloud environments is misconfiguration, which remains a leading cause of security breaches. Misconfigured storage buckets, overly permissive identity and access management (IAM) roles, and exposed services can lead to unauthorized access, data leaks, and compliance violations. Despite the availability of built-in security tools, organizations often struggle to continuously monitor and maintain secure configurations due to the dynamic nature of cloud environments.

Existing cloud security solutions provide partial visibility and often require manual intervention, making them inefficient for real-time threat detection and prevention. Furthermore, many tools lack proper risk classification and actionable insights, which are essential for effective security management.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

To address these challenges, this paper proposes a Cloud Security Posture Management (CSPM) system that automates the detection of misconfigurations in AWS environments. The system collects configuration data using AWS APIs, analyzes it against predefined security rules, and identifies potential vulnerabilities. It further categorizes risks and generates detailed reports to assist users in taking corrective actions.

The primary objective of this work is to enhance cloud security by providing an automated, scalable, and efficient solution for monitoring and managing security configurations. The proposed system aims to reduce human errors, improve compliance, and strengthen the overall security posture of cloud infrastructures.

RELATED WORK

Cloud security has become a critical research area due to the rapid adoption of cloud computing and the increasing number of security incidents caused by misconfigurations. Several studies have focused on identifying vulnerabilities and improving cloud security mechanisms.

Gartner Inc. reported that a significant percentage of cloud security failures are the result of customer misconfigurations rather than provider vulnerabilities, emphasizing the need for automated security management solutions. Similarly, Rich Mogull highlighted that improper Identity and Access Management (IAM) policies and unsecured storage services are among the most common threats in cloud environments.

Research by Zhang et al. proposed automated tools for detecting cloud misconfigurations; however, their approach lacked real-time monitoring capabilities. Another study by Behl and

Behl focused on cloud risk assessment models but did not provide practical implementation strategies for mitigation.

Furthermore, Hashizume et al. conducted a comprehensive survey on cloud security issues, identifying data breaches and insecure APIs as major concerns. Their work provided theoretical insights but lacked an implementation framework for continuous monitoring.

Recent advancements include Cloud Security Posture Management (CSPM) tools that automate compliance checks and vulnerability detection. However, many existing solutions are either complex, expensive, or provide limited customization for specific organizational needs.

In contrast to existing work, the proposed system focuses on a lightweight and automated CSPM approach specifically tailored for AWS environments. It integrates real-time configuration analysis, risk classification, and reporting mechanisms, thereby offering a more practical and scalable solution for detecting and mitigating cloud misconfigurations.

METHODOLOGY / SYSTEM DESIGN

The proposed Cloud Security Posture Management (CSPM) system is designed to automatically detect misconfigurations in cloud environments and enhance overall security. The system follows a structured approach consisting of data collection, analysis, risk classification, and reporting.

System Architecture

The architecture of the proposed system is illustrated in Fig. 1. It consists of multiple interconnected components that work together to identify and mitigate security risks in AWS environments.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

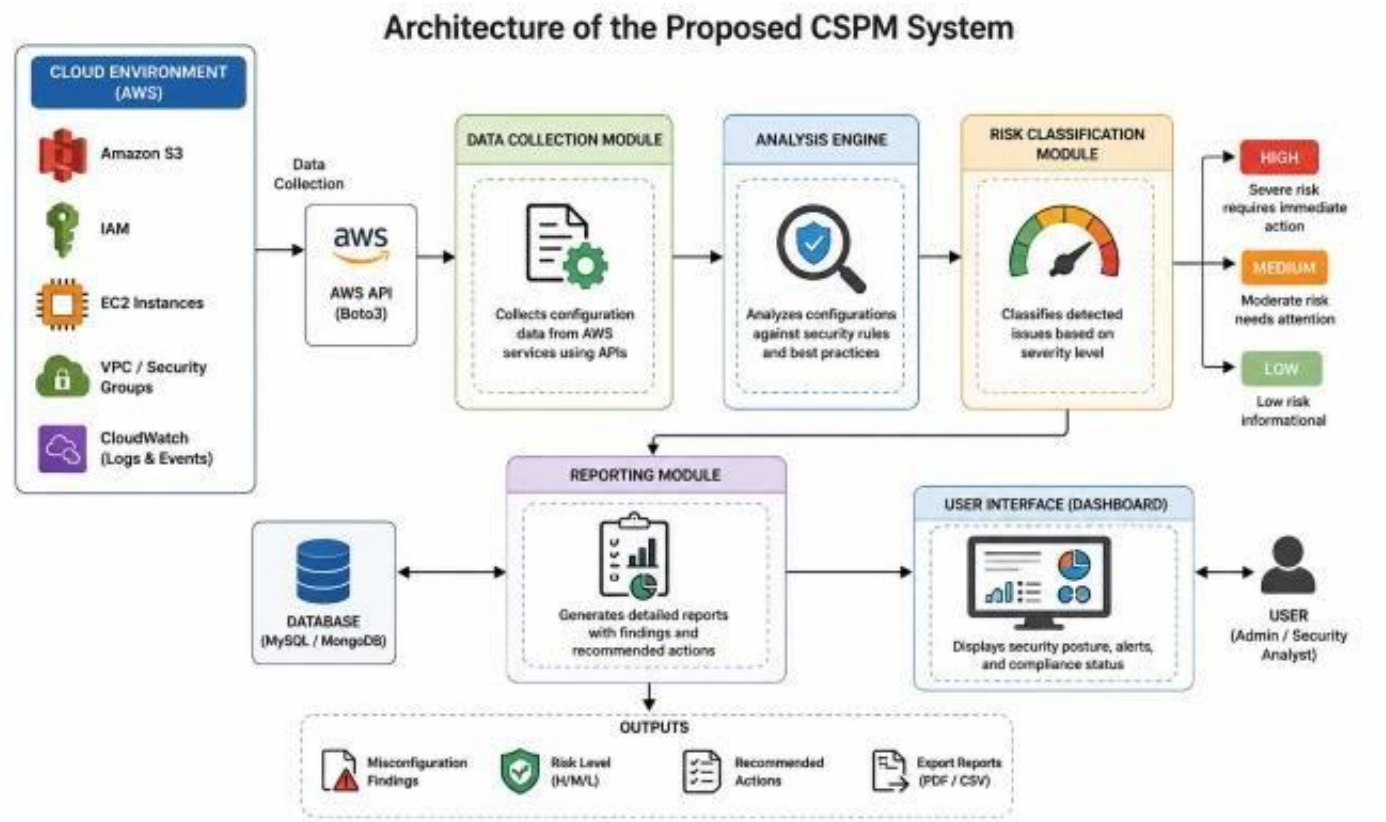

Fig. 1. Architecture of the Proposed CSPM System

Fig. 1. Architecture of the Proposed CSPM System Components:

- **User Interface (UI):**

  Provides an interactive dashboard for users to monitor cloud security status and view reports.

- **Data Collection Module:**

  This module collects configuration data from AWS services using APIs. It gathers information related to IAM roles, S3 bucket permissions, security groups, and other cloud resources.

- **Analysis Engine:**

  The collected data is analyzed against predefined security rules and best practices to identify potential vulnerabilities and misconfigurations.

- **Risk Classification Module:**

  Detected issues are categorized into different risk levels such as low, medium, and high based on their severity and potential impact.

- **Reporting Module:**

  Generates detailed reports highlighting vulnerabilities along with recommended mitigation steps.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Working Methodology

The system operates in the following steps:

1. **Data Acquisition:**

   The system retrieves real-time configuration data from AWS cloud services using secure APIs.

2. **Data Processing:**

   The collected data is filtered and structured for analysis.

3. **Rule-Based Analysis:**

   The system compares configurations against predefined security policies to detect misconfigurations.

4. **Risk Evaluation:**

   Identified vulnerabilities are evaluated and classified based on severity.

5. **Report Generation:**

   A comprehensive report is generated, providing actionable insights for improving cloud security.

Tools and Technologies

- Cloud Platform: Amazon Web Services (AWS)
- Programming Language: Python
- APIs: AWS SDK (Boto3)
- Database: MongoDB / MySQL
- Visualization: Web Dashboard

IMPLEMENTATION & EXPERIMENTAL RESULTS

Implementation

The proposed Cloud Security Posture Management (CSPM) system was implemented using a modular approach to ensure scalability and efficiency. The system was developed using Python, leveraging AWS SDK (Boto3) to interact with various AWS services.

The implementation focuses on monitoring key cloud components such as:

- **Amazon S3 buckets** for public access permissions
- **IAM roles and policies** for excessive privileges

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

- **Security groups** for open ports and unrestricted access

The system continuously collects configuration data from AWS resources and processes it using predefined security rules. These rules are based on standard cloud security best practices, such as avoiding public access to storage and enforcing least privilege access.

A web-based dashboard interface was also developed to display detected vulnerabilities and provide actionable recommendations for mitigation.

Experimental Setup

The system was tested in a controlled AWS environment with intentionally configured vulnerabilities to evaluate its effectiveness.

Test Scenarios:

- Publicly accessible S3 bucket
- Overly permissive IAM role
- Open security group (port 22/SSH exposed)

Evaluation Metrics:

- Detection Accuracy
- Response Time
- Number of Misconfigurations Detected

Results and Analysis

The system successfully detected multiple misconfigurations across different AWS services. The results demonstrate the effectiveness of the proposed solution in identifying security risks.

Test Case	Issue Detected	Risk Level	Detection Time
S3 Bucket	Public Access Enabled	High	2 sec
IAM Role	Excessive Permissions	Medium	3 sec
Security Group	Open SSH Port (0.0.0.0/0)	High	2 sec

The results indicate that the system provides **fast and accurate detection** of misconfigurations. Compared to manual inspection, the automated system significantly reduces detection time and minimizes human error.

Performance Discussion

- The system achieved **high detection accuracy** for predefined rules
- Real-time monitoring improves response to vulnerabilities

- Efficient API usage ensures minimal latency

DISCUSSION

The results obtained from the implementation demonstrate that the proposed Cloud Security Posture Management (CSPM) system is effective in identifying misconfigurations in AWS environments. The system provides quick detection with minimal latency, making it suitable for real-time monitoring scenarios.

One of the key strengths of the proposed approach is its automation capability, which reduces the dependency on manual inspection and minimizes human error. The use of predefined security rules ensures consistency in vulnerability detection across different cloud resources.

However, the system has certain limitations. It primarily relies on rule-based analysis, which may not detect unknown or zero-day vulnerabilities. Additionally, the current implementation focuses only on AWS environments and may require modification to support multi-cloud platforms.

Overall, the system provides valuable insights into cloud security risks and helps improve the security posture of cloud infrastructures.

CONCLUSION & FUTURE SCOPE

This paper presented a Cloud Security Posture Management (CSPM) system designed to detect misconfigurations in AWS environments. The proposed system automates the process of data collection, analysis, and risk classification, thereby enhancing cloud security and reducing manual effort.

The implementation results confirm that the system effectively identifies vulnerabilities such as public storage access, excessive permissions, and insecure network configurations. The system achieves fast detection and provides actionable recommendations, making it practical for real- world applications.

In future work, the system can be extended to support multi-cloud environments such as Microsoft Azure and Google Cloud Platform. Integration of machine learning techniques can further enhance the detection of unknown threats and improve overall system intelligence. Additionally, real-time alerting and automated remediation features can be incorporated to strengthen the system.

REFERENCES

[1] M. Zhang, R. Xue, and L. Liu, “Security and privacy in cloud computing: A survey,” *IEEE Access*, vol. 7, pp. 134,123–134,145, 2019.
[2] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” *Journal of Internet Services and Applications*, vol. 4, no. 1, pp. 1–13, 2018.
[3] S. Pearson, “Privacy, security and trust in cloud computing,” *IEEE Cloud Computing*, vol. 5, no. 3, pp. 64–68, 2019.
[4] R. Mogull, “Cloud security posture management: Managing risk in cloud environments,” *Cloud Security Alliance*, 2020.
[5] A. Behl and K. Behl, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2020.
[6] Amazon Web Services, “AWS Security Best Practices,” 2023.
[7] Cloud Security Alliance, “Top Threats to Cloud Computing,” 2022.
[8] Gartner, “Misconfiguration remains top cloud security risk,” 2021.