RESEARCH ARTICLE OPEN ACCESS

Cloud Identity and Access Management Compliance Checker

Ramya.C[1], Divya Roselin.P[2], Kavithendral.P[3], Shanjay Raj.S [4]

[1] *Professor, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu – 613006, India*
Email:v.ramya81@gmail.com

[2] *UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu – 613006, India*
Email: divyaroselin2410@gmail.com)

[3] *UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu – 613006, India*
Email: kavithendralpkka@gmail.com)

[4] *UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu – 613006, India*
Email: shanjayraj2004@gmail.com)

Abstract:

The Cloud IAM Compliance Checker is developed to analyze and monitor Identity and Access Management (IAM) configurations in AWS environments. The system automatically detects excessive permissions, misconfigurations, and security risks associated with IAM users, roles, and policies. It helps organizations maintain secure access control by identifying vulnerabilities that may lead to unauthorized access or data breaches. The system connects securely to AWS using credential validation through Security Token Service (STS) and retrieves IAM entities for analysis. It identifies risky configurations such as wildcard permissions, over-privileged access, and high-risk policies using rule-based logic aligned with security best practices. This automated approach reduces the need for manual auditing and improves the accuracy of security assessments.The system classifies risks into four levels: low, medium, high, and critical. The results are presented through a structured dashboard and reports, providing actionable insights for improving cloud security. This enables administrators to quickly understand security issues, take corrective actions, and ensure compliance with organizational security standards. Overall, the system enhances visibility, strengthens access control, and supports efficient cloud security management.

I. INTRODUCTION

Cloud computing has become an integral part of modern IT infrastructure, providing scalability, flexibility, and cost efficiency. Organizations increasingly rely on cloud platforms such as AWS to host applications and manage services. However, with the growth of cloud adoption, securing access to resources has become a critical challenge.

Identity and Access Management (IAM) plays a vital role in controlling access to cloud resources. Improper IAM configurations such as excessive permissions, wildcard access, and unused roles can lead to serious security vulnerabilities.

These vulnerabilities may result in unauthorized access, privilege escalation, and data breaches.

Traditional IAM auditing methods are manual, time-consuming, and prone to human error. They lack continuous monitoring and fail to provide real-time insights into security risks. To address these challenges, this project proposes an automated Cloud IAM Compliance Checker that analyzes IAM configurations, detects risks, and improves access control security.

II. RELATED WORK

Existing IAM security solutions are primarily provided by major cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). These platforms offer built-in Identity and Access Management (IAM) tools that allow administrators to manage users, roles, and permissions within their respective environments. While these tools are effective for basic access control, they are typically limited to individual cloud platforms and do not provide a centralized mechanism for analyzing IAM configurations across systems.

A. Decentralized Identity Management

Somchart Fugkeaw (2023) proposed a decentralized identity access management system for multi-application cloud environments.The system utilizes blockchain technology, smart contracts, and authentication protocols such as SAML, OAuth,OpenID Connect, and FIDO2. This approach enhances security and decentralization but introduces implementation complexity and management overhead.

B. Semantic Interoperability Framework

Upesh Kumar Rapolu (2023) presented a multi-cloud strategy integrating AWS,Azure, and Google Cloud. The system uses ontology-based frameworks,SPARQL,and RDF query language to achieve semantic interoperability across cloud environments. Although this improves cross-cloud communication,it requires complex data modeling and standardization.

C. Identity Federation and Access Control

Thomas Baumer et al. (2023) developed a cross-domain identity management system using SCIM standards, REST APIs, RBAC, JSON, Swagger, OAuth2, and LDAP. This approach focuses on standardized identity exchange and access control, but does not effectively address IAM misconfigurations or excessive permissions.

D. AI-Based IAM Analysis

Jooyoung Jeong and Sang-Goo Lee (2025) proposed a permission-aware IAM system using Large Language Models (LLMs) and Retrieval-Augmented Generation (RAG). The system integrates AWS IAM, GCP IAM, Keycloak, and vector databases such as FAISS. While this approach enables intelligent permission analysis, it requires high computational resources and complex infrastructure.

E. Policy-as-Code Framework

Alen Paul et al. (2024) introduced a cloud compliance automation system using AWS native services and Open Policy Agent (OPA). The system leverages CI/CD pipelines, policy-as-code, automated decision gating, and containerized evaluation. This approach is effective for compliance enforcement but focuses less on real-time risk detection.

F. Formal Policy Verification

William Eiers et al. (2022) proposed a framework for analyzing access control policies using SMT solvers (Z3), automata-based model counters, and IAM policy languages. This method enables formal verification of permissions but is complex and less suitable for real-time implementation.

III. PROPOSED METHODOLOGY

In contrast to the above approaches, the proposed Cloud IAM Compliance Checker uses a rule-based analysis technique to detect IAM misconfigurations and excessive permissions in AWS environments. The system focuses on simplicity, real-time analysis, and effective risk classification without relying on complex frameworks or heavy computational models.

A. System Overview

The proposed system, Cloud IAM Compliance Checker, is designed as a comprehensive security analysis platform for evaluating Identity and Access Management (IAM) configurations in AWS environments. The primary objective of the system is to identify security risks arising from excessive permissions, misconfigured policies, and over-privileged access. In modern cloud infrastructures, IAM plays a critical role in controlling access to sensitive resources. However, improper configuration of IAM policies can lead to severe vulnerabilities such as unauthorized access, privilege escalation, and potential data breaches. To address these challenges, the proposed system adopts an automated and scalable approach for IAM analysis.

Unlike traditional manual auditing methods, which are time-consuming and prone to human error, this system provides continuous monitoring and real-time risk detection. It ensures that IAM configurations adhere to security best practices and helps organizations maintain a strong security posture.

B. Authentication Layer (JWT-Based)

The system begins with a secure authentication mechanism to ensure that only authorized users can access the platform. Users are required to log in using valid credentials through a web-based interface.Once authenticated, the system generates a secure session using token-based authentication mechanisms such as JSON Web Tokens (JWT). This session management process ensures that user interactions with the system remain secure throughout their session.Additionally, the system prevents unauthorized access by validating session tokens for every request. This enhances security by ensuring that sensitive

operations such as AWS integration and IAM scanning are accessible only to authenticated users.

C. AWS Integration Service

The system integrates with AWS using access key and secret key credentials provided by the user. These credentials are essential for accessing IAM resources and performing analysis.To ensure secure communication, the system validates the provided credentials using AWS Security Token Service (STS). The STS validation process confirms the authenticity and permissions of the credentials before allowing further operations.This step is critical in preventing unauthorized access and ensuring that only valid AWS accounts are connected to the system. Once validated, a secure connection is established, enabling the system to interact with AWS services safely.

D. IAM Data Collection Service

After successful authentication and AWS integration, the system retrieves IAM-related data from AWS.

This includes:

- IAM Users
- IAM Roles
- IAM Policies
- IAM Groups

The data retrieval process is carried out using AWS SDK (boto3), which provides a reliable and efficient interface for interacting with AWS services.

The collected data is then structured and processed for further analysis. This preprocessing step ensures that IAM entities and their associated policies are organized in a format suitable for rule-based evaluation.

E. Risk Analysis and Detection Engine

The core component of the system is the policy analysis and risk detection engine. This module evaluates IAM policies using predefined rules based on security best practices and access control principles.

The analysis focuses on identifying the following types of risks:

- Full wildcard permissions (e.g., *:*)
- Service-level wildcard permissions (e.g.,s3:*)
- Excessive permissions granted beyond required scope
- Over-privileged users and roles
- Unnecessary or unused access rights

Each IAM entity is analyzed in detail, and its permissions are evaluated against predefined rules. The system detects potential vulnerabilities that may lead to security risks such as unauthorized access or privilege escalation.

F. Risk Classification Service

After detecting potential risks, the system classifies them into four levels based on severity and impact:

- *Critical Risk:*
  Permissions that provide unrestricted access, allowing complete control on all resources.
- *High Risk:*
  Administrative or service-level access (e.g.,AdministratorAccess,s3:*), which can lead to significant security exposure.
- *Medium Risk:*
  Broad permissions applied across multiple resources without full wildcard access.
- *Low Risk:*
  Least privilege access with minimal specific permissions, considered safe.

This classification model helps in prioritizing risks and enables administrators to focus on critical issues first.

G. Data Storage and Management

The analyzed results are stored in a database for efficient retrieval and management. This includes:

- IAM entities
- Detected risks
- Risk classification
- Scan history

Storing this data allows the system to maintain historical records of scans, enabling users to track changes in IAM configurations over time.

H. Visualisation and Dashboard Interface

The system provides an interactive dashboard to display analysis results. The dashboard presents:

- List of IAM entities (users, roles, groups)
- Associated risks and classifications
- Summary of security issues

The visual representation of data improves user understanding and allows quick identification of vulnerabilities. The dashboard is designed to be user-friendly and accessible, ensuring efficient monitoring of IAM security.

I. Report Generation and Export

The system generates structured reports based on the analysis results. These reports include:

- Detected risks
- Affected IAM entities
- Risk severity levels
- Summary of findings

Reports can be used for auditing, compliance verification, and documentation purposes. This feature reduces manual effort and enhances decision-making for security teams.

J. End to End Workflow

The complete workflow of the system is as follows:

1. User logs into the system
2. AWS credentials are provided
3. Credentials are validated using STS
4. IAM data is retrieved from AWS

5. Policies are analyzed using rule-based logic
6. Risks are detected and classified
7. Results are stored and displayed
8. Reports are generated

This workflow ensures a fully automated and efficient IAM security analysis process.

IV. SYSTEM ARCHITECTURE

The proposed Cloud IAM Compliance Checker follows a layered architecture consisting of frontend, backend, and cloud integration components. The system is designed to provide secure communication, efficient data processing, and scalable IAM analysis.

The architecture begins with the User Interface (Frontend), where users interact with the system. Through this interface, users can log in, create projects, connect their AWS accounts, initiate IAM scans, and view results. The frontend ensures a user-friendly experience and seamless navigation.The Backend System handles core functionalities such as authentication, IAM data processing, risk analysis, and report generation. It exposes REST APIs to manage communication between the frontend and backend. The backend also manages session handling, ensuring secure access to system resources.

The AWS Integration Layer connects the system with AWS services using access key and secret key credentials. These credentials are validated using AWS Security Token Service (STS) to ensure secure and authorized access. Once validated, the system retrieves IAM data including users, roles, policies, and groups using the AWS SDK (boto3).

The IAM Analysis Module processes the retrieved data and performs rule-based analysis to detect security risks such as wildcard permissions, excessive access, and high-risk policies. Based on the analysis, risks are classified into low, medium, high, and critical levels. The processed results are stored in the Database Layer, which maintains scan results, project details, and historical data. This enables efficient data retrieval and tracking of IAM configurations over time. Finally, the results are displayed through the frontend dashboard, and detailed reports are generated for auditing and monitoring purposes.

This architecture ensures modular design, secure communication, and efficient IAM compliance analysis in AWS environments.

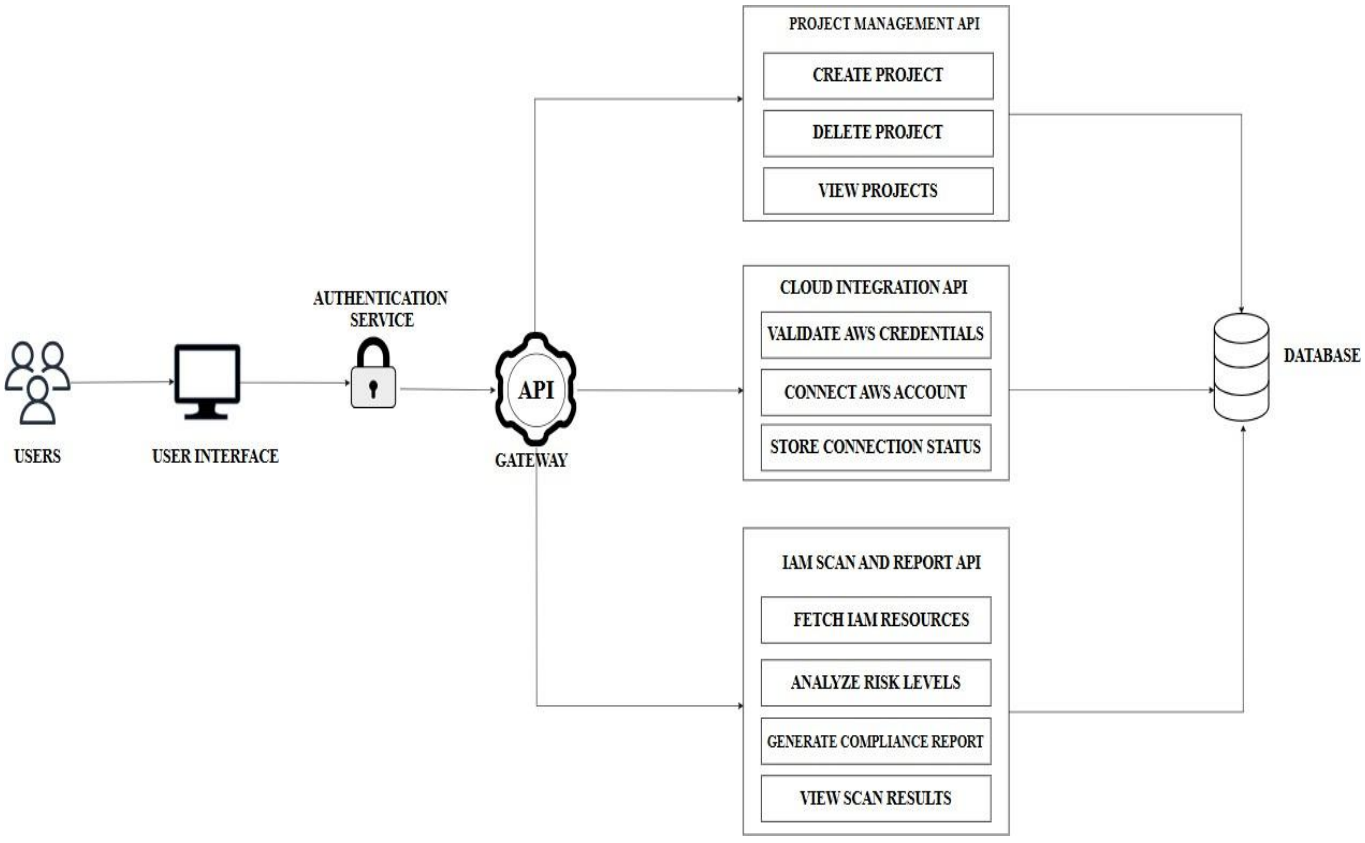

Figure 1 : Architecture of Cloud Identity and Access Management Compliance Checker.

V. EXPERIMENTAL SETUP

A. System Input and Data Source

The experimental setup of the proposed Cloud IAM Compliance Checker is designed using real-time IAM configurations retrieved directly from AWS environments. The system analyzes IAM entities such as users, roles, policies, and groups without relying on any predefined dataset. To simulate different security scenarios, IAM policies are manually created to represent various risk levels including wildcard permissions, administrative access, broad permissions, and least privilege configurations.

B. System Implementation and Configuration

The system is implemented using a full-stack architecture, where the backend is developed using Python and integrates with AWS through the boto3 SDK. The frontend provides a web-based dashboard for user interaction. A rule-based analysis engine is used to evaluate IAM policies, with detection rules including wildcard access (:), service-level access (e.g.,s3:*), excessive permissions, and least privilege validation.

C. Evaluation Metrics

The performance of the system is evaluated using standard metrics such as accuracy, precision, recall, and F1-score. Additionally, error metrics such as false positive rate and false negative rate are considered to measure detection reliability. Detection latency is also evaluated to analyze the time required for IAM analysis.

D. Results Summary

The results show that the system accurately detects IAM misconfigurations and classifies risks into low, medium, high, and critical levels. It effectively identifies wildcard permissions, administrative access, and excessive privileges, providing structured and clear outputs for analysis.

E. Detection Performance

The detection performance is strong across all risk categories, with high accuracy for critical and high-risk configurations, and consistent classification for medium and low-risk permissions. The system maintains low false positive and false negative rates, ensuring reliable performance.

F. Processing Time and Latency

The system operates in near real-time, with IAM data retrieval taking approximately 0.5 to 2 seconds, policy analysis taking 0.1 to 0.5 seconds, and risk classification taking 0.05 to 0.1 seconds. The overall processing latency ranges between 1 to 3 seconds, making the system efficient and suitable for practical cloud security monitoring.

CONCLUSION

This research presents the proposed Cloud IAM Compliance Checker, a comprehensive system designed to analyze and monitor Identity and Access Management (IAM) configurations in AWS environments through real-time evaluation and rule-based risk detection. The system addresses the critical challenge of identifying excessive permissions, misconfigurations, and over-privileged access, which continue to be major security threats in cloud infrastructures. The key contribution of this work lies in the development of a rule-based IAM analysis engine that accurately classifies risks into low, medium, high, and critical levels while ensuring high detection reliability and minimal false positives.

Unlike traditional manual auditing approaches that are time-consuming and error-prone, the proposed system automates IAM security analysis by combining real-time data retrieval, policy evaluation, and structured risk classification. The experimental evaluation demonstrates that the system achieves high accuracy in detecting wildcard permissions, administrative access, and excessive privilege assignments. The system maintains strong precision and recall, ensuring that detected risks are both accurate and comprehensive.

The near real-time processing capability, with an average detection latency of 1 to 3 seconds, enables timely identification of security issues before they lead to potential exploitation. The modular and scalable architecture ensures that the system can be deployed efficiently in practical cloud environments while maintaining optimal performance. The user-friendly dashboard and reporting features provide clear visibility into IAM security posture, allowing administrators to take informed corrective actions.

Furthermore, the rule-based approach ensures transparency and interpretability, enabling security analysts to understand the reasoning behind each detected risk, unlike black-box models. This improves trust and usability in real-world applications.Future work can focus on extending the system with multi-cloud support, integrating intelligent analysis techniques such as machine learning for adaptive risk detection, enabling automated remediation actions, and enhancing real-time monitoring capabilities.

In conclusion, the proposed Cloud IAM Compliance Checker provides a practical, efficient, and reliable solution for IAM security analysis, significantly improving access control management and strengthening the overall security posture of cloud-based systems.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to their project guide and faculty members of the Department of Computer Science and Engineering for their continuous support, valuable guidance, and encouragement throughout this research work. The authors also thank their external guide associated with CyberNerds and NerdsLab for providing the necessary guidance and resources to successfully complete this

study. Additionally, we acknowledge the use of publicly available datasets and tools that contributed to the development and evaluation of the proposed model.

REFERENCES

[1] Alen Paul, Rishi Manoj,S.Udhayakumar, "Amazon Web Services Cloud Compliance Automation with Open Policy Agent", IEEE, 2024.

[2] William Eiers, Ganesh Sankaran, Albert Li,Emily O'Mahony, Benjamin Prince, and Tevfik Bultan, " Quantifying Permissiveness of Access Control Policies", IEEE, 2022.

[3] Somchart Fugkeaw, " Achieving Decentralized and Dynamic SSO-Identity Access Management System for Multi- Application outsourced in Cloud", IEEE, 2023.

[4] Upesh Kumar Rapolu, "Implementing Multi- Cloud Strategies with Azure, Amazon Web Services (AWS), and, Google Cloud for Enhanced Business Continuity", 2023

[5] Thomas Baumer, Mathis Muller, and Gunther Pernul, " System for Cross-Domain Identity and Management (SCIM): Survey and Enhancement with RBAC", IEEE, 2023.

[6] Permission Aware RAG: Identity and Access Management (IAM)-Based Access Filtering in Multi- Resource Environment", IEEE, 2025.