An Automated Approach to Identifying and Mitigating Least Privilege Violations in AWS IAM Policies

PURVI BAJAJ[1], JANHVI KAMBLE[2], SURAKSHA KHURANA[3], SUMEDH PUNDKAR[4]
[1, 2, 3, 4] *Student, Computer Science and Technology Usha Mittal Institute of Technology, SNDTWU, Mumbai, India*

***Abstract*— The research presents an automated tool to identify violations of the principle of least privilege in AWS Identity and Access Management (IAM) policies. The tool scans all IAM policies within an AWS account or a single policy file, analyzing policy documents to identify potentially risky permissions. It uses the Boto3 library and Python programming language to retrieve policy information and assess permissions. The analysis results are presented in an HTML report, providing an intuitive triage worksheet for security professionals. This tool contributes to automating security practices in cloud environments, enhancing efficiency and decision-making.**

***Index Terms*— Cloud Security Posture Management System (CSPM), Amazon Web Service(AWS), Identity Access and Management (IAM) Policy, Identity Service Providers (IdSP), IAM as a Service (IAMaaS), Google Cloud Platform Services(GCP), Application programming interface(API), Role-Based Access Control(RBAC)**

I. INTRODUCTION

Cloud Security Posture Management System is a comprehensive analysis tool designed to provide insights into Identity and Access Management (IAM) permissions within Amazon Web Services (AWS) environments. It aims to address key objectives such as IAM Permissions Analysis, Policy Visualization, Automated Assessment, and Remediation Recommendations.

CloudSplaining conducts in-depth analysis of IAM permissions configurations within AWS accounts, identifying potential security risks such as overly permissive policies, unused permissions, and privilege escalation paths. It offers policy visualization capabilities to help users understand the relation- ships between IAM policies, roles, and users, facilitating the identification of access patterns and potential security gaps.

Automated scanning capabilities enable organizations to streamline the assessment process, quickly identifying and remediating IAM misconfigurations. Cloud Security Posture Management System provides actionable recommendations for remediation, guiding organizations in strengthening their IAM security posture and mitigating potential risks.

By offering a holistic approach to IAM permissions analysis, CloudSplaining empowers organizations to proactively manage their AWS security posture, reduce the attack surface, and enhance overall cloud security resilience.

II. RELATED WORK

Identity and Access Management (IAM) plays a crucial role in modern enterprise security, especially in cloud computing. It offers benefits such as enhanced security, ease of use, productivity gains, and cost savings. However, challenges like automated onboarding and integration with new technologies persist, indicating the evolving nature of IAM in response to rapid technological advancements. IAM is essential for user authentication, authorization, and directory services, and various IAM models, including local management, Identity Service Providers (IdSP), and IAM as a Service (IAMaaS), are discussed. Monitoring, audits, and risk analysis are essential components for ensuring IAM effectiveness and compliance. The comparison of top cloud providers—AWS, Azure, and GCP—provides insights into their strengths and suitability for different business needs. AWS's proactive investment in for- mal verification and cloud-based security services contribute to resource protection. IAMaaS is a scalable, cost-effective, and flexible solution for cloud-based security services. The systematic review on IAM provides a holistic overview of its importance in

bolstering information security within organizations, addressing challenges related to data protection, regulatory compliance, and access control.

A. Cloud Services and Security Vulnerabilities

The research paper discusses the increasing popularity of cloud services among IT professionals and the associated concerns about security vulnerabilities due to misconfigurations. The paper explores the use of model checking as a method for verifying system properties and discusses how it can be used to generate a finite trace leading to a violating state. The authors present an approach to construct a finite-state Boolean model from the Identity and Access Management (IAM) component of Amazon Web Services (AWS), and a property from an attack target, such as reading a classified S3 bucket object. The paper demonstrates that this approach can be used to detect multi-step attacks in setups containing tens of AWS accounts with hundreds of resources in under a minute. The paper also discusses the shared responsibility model of security and compliance between the cloud provider and the customer, emphasizing that cloud service misconfigurations and privileged user abuse are involved in a significant percentage of security attacks.

B. Pervasive Misconfigurations and Model Checking Process

The authors highlight that misconfiguration of cloud re- sources is a pervasive issue, as evidenced by the plethora of exposed S3 buckets. They also note that privileged user abuse is likely symptomatic of the complexity of IAM policies and settings that are tied to most cloud operations. Furthermore, the authors discuss how the model checking process is not a one-time effort, as there may be IAM exploits that are not formalized in the model or that are not even discovered yet by security researchers. They envision that with time, the model will cover more and more exploits, enhancing its credibility and reducing false positives and false negatives. The authors also discuss the challenges of the scalability of the model checking process and present techniques to improve model checking performance by translating non-Boolean variables into Boolean arrays, ultimately reducing the problem to pure Boolean satisfiability.

C. Conclusion and Future Directions

In conclusion, the authors present the contributions of the paper, including the definition of a Boolean model of the AWS IAM component, the implementation of a model checking process to detect multi-step attacks exploiting AWS actions, the evaluation of the scalability of the approach and the quality of the detected results, and a technique to improve model checking performance. They emphasize that the approach is able to detect existing misconfigurations in pre-deployment environments and assist security engineers in verifying their IAM policies. They also suggest future directions for research, including the integration of numerical weights into the model, the application of different model checking algorithms, and the extension of the approach to other cloud environments and domains.

III. PROPOSED SYSTEM ARCHITECTURE

CSPM is an open-source tool developed by Salesforce for scanning and analyzing AWS IAM policies for security vulnerabilities. The system architecture includes a web-based user interface, a backend server, AWS API integration, an IAM Policy Scanner, an analysis engine, a reporting module, authentication and authorization mechanisms, data storage, scalability and performance, and monitoring and logging com- ponents.

The UI allows users to interact with the tool's functionality through a web browser, while the backend server handles in- coming requests, performs scans, analyzes policies for security risks, and generates reports. The AWS API allows the tool to retrieve IAM policies and related configuration details for analysis.

The IAM Policy Scanner scans IAM policies retrieved from AWS accounts, identifying permissions, resource access pat- terns, potential security misconfigurations, and vulnerabilities. The analysis engine processes the scanned IAM policies and performs in-depth analysis to identify security risks and vulnerabilities. The reporting module generates comprehensive reports summarizing the findings of the IAM policy scans, providing detailed insights into security risks, vulnerabilities, and recommendations for remediation.

Authentication and authorization mechanisms ensure secure access to the CSPM application, and role-based access control (RBAC) mechanisms may be employed to control user access based on their roles and permissions. Data storage may involve a combination of databases and file storage systems to store structured and unstructured data efficiently. The architecture should be designed to scale horizontally to accommodate increasing workloads and large-scale IAM policy scans. Monitoring and logging components are essential for tracking the performance, health, and usage of the CSPM application.

The presented fig 1 shows the proposed technology stack for building CSPM, includes various programming languages and frameworks. Python is widely used for developing security tools and has extensive libraries for interacting with AWS APIs, parsing JSON documents, and implementing policy analysis algorithms. Flask or Django are popular Python web frameworks that can be used to build the web-based user inter- face for CSPM. React.js or Vue.js are JavaScript frameworks that offer a rich set of components, state management, and routing capabilities for modern single-page applications.

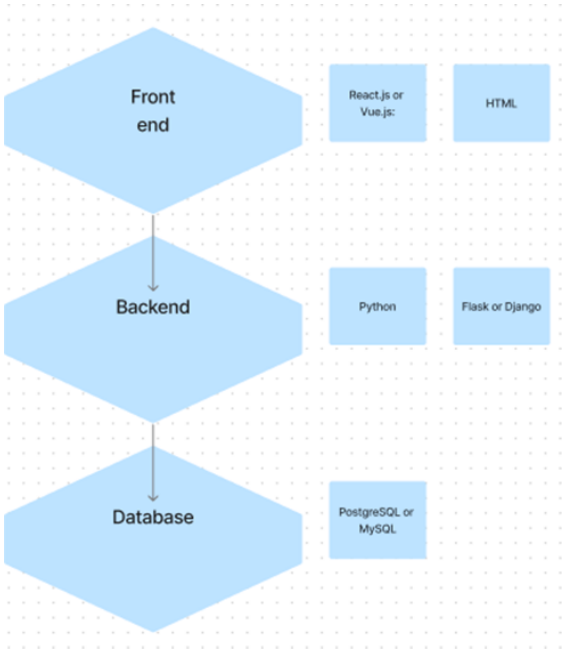


Fig. 1. Proposed technology stack.

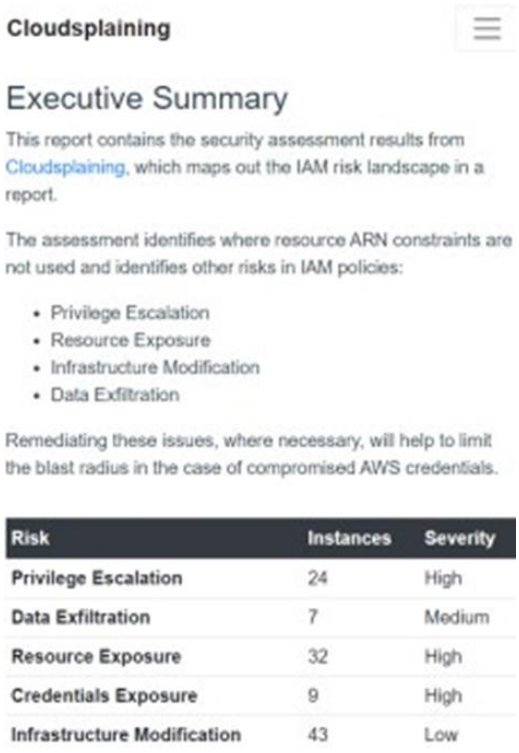
The AWS SDK for Python, Boto3, provides easy-to-use interfaces for interacting with various AWS services, including IAM. Python's built-in JSON library can be used for parsing IAM policy documents retrieved from AWS. A relational database can be used to store configuration settings, scan results, and other persistent data required by CSPM. Authentication and authorization can be implemented using OAuth2 and RBAC (Role-Based Access Control) within the application logic. Docker can be used for containerizing the CSPM application components, while Kubernetes can be used for orchestrating and managing Docker containers in a production environment. Monitoring and logging can be done using Prometheus and Grafana, as well as ELK Stack for centralized logging.

Security can be achieved through SSL/TLS certificates, OWASP Dependency-Check, and testing using pytest for writing and running unit tests and integration tests for CSPM. However, specific technology choices may vary based on project requirements, team expertise, and organizational preferences.

IV. RESULT AND DISCUSSION

This paper presents the implemented work on CSPM. The following figures describe how the suggested concept functions in practical terms.

The presented fig 2 provides the Executive Summary report which presents the findings and security assessment results obtained from CSPM, an advanced tool designed to analyze



Cloudsplaining

Executive Summary

This report contains the security assessment results from Cloudsplaining, which maps out the IAM risk landscape in a report.

The assessment identifies where resource ARN constraints are not used and identifies other risks in IAM policies:

- Privilege Escalation
- Resource Exposure
- Infrastructure Modification
- Data Exfiltration

Remediating these issues, where necessary, will help to limit the blast radius in the case of compromised AWS credentials.

Risk	Instances	Severity
Privilege Escalation	24	High
Data Exfiltration	7	Medium
Resource Exposure	32	High
Credentials Exposure	9	High
Infrastructure Modification	43	Low

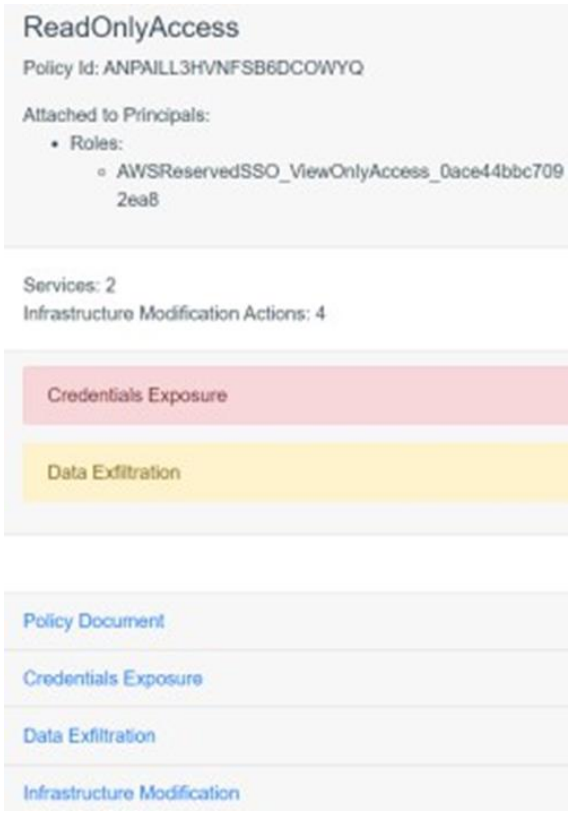
Fig. 2. AWS Policies.

the Identity and Access Management (IAM) risk landscape within AWS environments. CSPM offers a comprehensive evaluation of IAM configurations, associated policies, and potential security vulnerabilities, enabling organizations to proactively identify and address risks to their cloud infrastructure.

The presented fig 3 shows the detailed report generated by CSPM with respect to AWS Policies. The detailed report provides policy wise Policy Document, Credentials Exposure, Data Exfiltration, Infrastructure Modification.

A. Policy Documen

In the context of AWS (Amazon Web Services), a policy document refers to a JSON (JavaScript Object Notation) document that defines permissions and access control rules for AWS resources. These policies are written using AWS Identity and Access Management (IAM) and can be attached to IAM users, groups, roles, or AWS resources. Policy documents specify what actions are allowed or denied on which AWS resources by whom. They play a crucial role in defining the security posture of AWS environments.



ReadOnlyAccess

Policy Id: ANPAILL3HVNFSB6DCOWYQ

Attached to Principals:

- Roles:
  - AWSReservedSSO_ViewOnlyAccess_0ace44bbc7092ea8

Services: 2

Infrastructure Modification Actions: 4

Credentials Exposure

Data Exfiltration

Policy Document

Credentials Exposure

Data Exfiltration

Infrastructure Modification

Fig. 3. AWS Policies.

B. Credentials Exposure

Credentials exposure refers to the unauthorized disclosure or compromise of sensitive authentication credentials, such as usernames, passwords, API keys, access tokens, or security certificates. In the context of cloud computing, credentials exposure can occur due to various factors such as insecure storage, transmission over unencrypted channels, phishing attacks, or leakage through misconfigured systems or applica- tions. When credentials are exposed, malicious actors can gain unauthorized access to sensitive resources, potentially leading to data breaches, financial loss, or reputational damage.

C. Data Exfiltration

Data exfiltration, also known as data exfiltration or data theft, refers to the unauthorized extraction or transfer of sensitive data from a secure environment to an external location controlled by an attacker. This can occur through various means, including network-based attacks, malware, insider threats, or exploitation of vulnerabilities in systems or applications. Data exfiltration poses a significant security risk as it can result in the loss of confidential

information, intellectual property, or personally identifiable information (PII). Organizations often implement measures such as data loss prevention (DLP) solutions, encryption, access controls, and network monitoring to prevent and detect data exfiltration attempts.

D. Infrastructure Modification

Infrastructure modification refers to the unauthorized or unauthorized changes made to the configuration, settings, or resources of an IT infrastructure. In cloud computing environ- ments, infrastructure modification can include actions such as provisioning or deprovisioning of virtual machines, modifying network configurations, altering storage settings, or changing security group rules. Unauthorized infrastructure modifications can lead to service disruptions, data loss, or security breaches, compromising the integrity, availability, and confidentiality of IT resources. Implementing strict access controls, change man- agement processes, and auditing mechanisms is essential to prevent unauthorized infrastructure modifications and maintain the security and stability of cloud environments.

These terms are crucial concepts in the realm of cloud security, highlighting potential risks and threats that organizations must mitigate to safeguard their data, resources, and infrastructure in cloud computing environments.

The presented fig 4 described appears to be a dashboard or interface within a tool like CSPM, which is designed to provide visibility into AWS Identity and Access Management (IAM) configurations and associated security risks. Here's an elaboration on each component mentioned:

E. IAM Users, Groups, and Roles

IAM Users: These are individual entities within an AWS ac- count that represent people, applications, or services interacting with AWS resources. Each user has a unique identity and can be assigned specific permissions through IAM policies. - IAM Groups: Groups are collections of IAM users. Instead of attaching policies directly to individual users, policies can be attached to groups, making it easier to manage permissions for multiple users with similar roles or responsibilities. - IAM Roles: Roles are similar to users but are intended for use by AWS services, applications, or third-party entities rather than individuals. Roles define a set of permissions that can be assumed by trusted entities, allowing them to access AWS resources securely.

F. Associated Policies

IAM policies define the permissions granted to IAM users, groups, or roles. These policies are written in JSON format and specify which actions are allowed or denied on which AWS resources. Each IAM principal (user, group, or role) can have one or more policies attached to it, defining its access permissions.

G. Risks Associated with Each Principal

This refers to the security risks or vulnerabilities associated with the IAM principals (users, groups, or roles) and their associated policies. These risks may include overly permissive

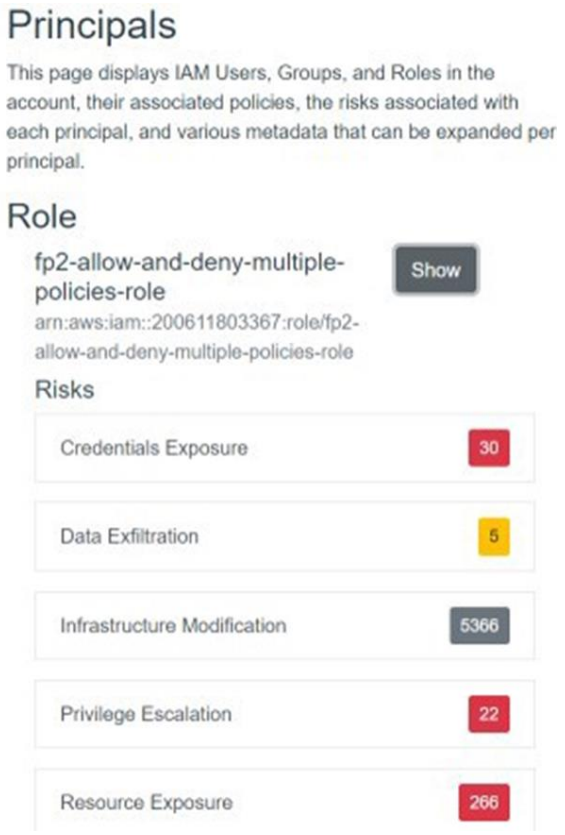


Fig. 4. IAM Principals.

permissions, unused or unnecessary permissions, wildcard usage, policy complexity, lack of MFA

(Multi-Factor Authen- tication) enforcement, and other misconfigurations that could potentially lead to security breaches or unauthorized access to AWS resources.

H. Metadata

Metadata refers to additional information or attributes asso- ciated with IAM principals, such as creation date, last login timestamp, attached policies, group memberships, etc. This metadata provides context and insights into the configuration and usage of IAM entities within the AWS account.

I. Expandable Metadata

The expandable metadata feature allows users to view additional details or properties of IAM principals by expanding the corresponding sections in the dashboard or interface. This could include details such as permissions granted by individual policies, policy versions, policy summaries, inline policies, policy attachments, etc.

Overall, the described page serves as a comprehensive dash- board for managing IAM users, groups, and roles within an AWS account, providing insights into their associated policies, security risks, and metadata. It enables administrators to assess and mitigate security risks effectively, ensure compliance with security best practices, and maintain a secure and well-configured IAM environment.

V. FUTURE SCOPE AND CHALLENGES

The future of the IAM security tool could include advanced policy analysis techniques, integration with cloud security plat- forms, customizable risk scoring, continuous monitoring and remediation, and support for multi-cloud environments. The tool could also be integrated with other cloud service providers like Azure and Google Cloud Platform. However, challenges include scalability, policy complexity, managing dynamic environments, compliance and regulatory requirements, and user adoption and education. Scalability is a challenge as AWS environments grow in complexity, while policy complexity can pose challenges in accurately analyzing and assessing security risks. Dynamic environments require robust mechanisms for maintaining accurate policy assessments and risk evaluations. Compliance and regulatory requirements adaptation across different industries and regions can be challenging, and user adoption and education are crucial for maximizing the tool's effectiveness. Overcoming resistance to change and promoting a security-conscious culture within organizations can be essential for successful implementation.

CONCLUSION

Cloud Security Posture Management System is a tool that enhances the security of cloud environments, particularly AWS, by providing visibility into IAM configurations, policies, and potential security risks. It helps organizations identify and address vulnerabilities, reducing the risk of unauthorized access, data breaches, and compliance violations. The future scope of CSPM g and similar tools is promising, with opportunities to enhance policy analysis capabilities, integrate with broader security platforms, support multi-cloud environments, and enable continuous monitoring and remediation. However, challenges such as scalability, policy complexity, dynamic environments, compliance requirements, and user adoption need to be addressed. By addressing these challenges, organizations can strengthen their cloud security posture, maintain regulatory compliance, and safeguard sensitive data and resources effectively in the increasingly complex cloud landscape.

REFERENCES

[1] Ishaq Azhar Mohammed, "Identity and Access Management System: a Web-Based Approach for an Enterprise," Department of Information Technology Hyderabad, India

[2] Sakshi Narula, Arushi Jain, and MS. Prachi, "Cloud Computing Security: AWS(2015)," IT ITM University.

[3] Edwin Sturrus and Olga Kulikova, "Identity and Access Management," unpublished.

[4] Dr. Manish Saraswat and Dr. R.C. Tripath, "Cloud Computing: Com- parison and Analysis of Cloud Service Providers—AWS, Microsoft and Google(2020)," Geetanjali Institute of Technical Studies.

[5] Byron Cook1, "Formal Reasoning About the

Security of Amazon Web Services," University College London.

[6] Deepak H. Sharmaa, Dr. C. A. Dhoteb, and Manish M. Poteyc "Identity and Access Management as Security-as-a-Service from Clouds," unpib- lished.

[7] Ehtesham Zahoor, Zubaria Asma, and Olivier Perrin, "A Formal Ap- proach for the Verification of AWS IAM Access Control Policies," European Conference on Service-Oriented and Cloud Computing