Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Mitigating Security Risks in Cloud Infrastructures Using AWS IAM Policies and Controls

Ishwar Bansal
Full Stack Developer (Independent Researcher)
AWS, Herndon USA
Aggarwalse@gmail.com
ORCID ID: 0009-0006-5865-536X

ARTICLE INFO

Received: 12 Jun 2024

Revised: 25 Jul 2024

Accepted: 15 Aug 2024

ABSTRACT

This paper looked at how well AWS Identity and Access Management (IAM) policies and controls reduced security concerns in cloud environments. Using a mixed-methods approach, IAM policy configurations, AWS CloudTrail logs, and expert interviews spanning five companies—TechNova Solutions, CloudWave Inc., DataSecure Ltd., NextGen Systems, and CyberGuard Corp—were examined. According to the statistical study, companies that closely followed the concept of least privilege and regularly updated their policies had less policy infractions, less over-privileged roles, and less illegal access. Qualitative analysis underlined issues like audit hurdles and policy complexity as well as success elements like automation tools and ongoing training. The results underline how important well-structured IAM policies coupled with continuous monitoring and management are in reinforcing cloud security. This study provides useful direction for companies trying to maximize IAM controls to properly protect their cloud settings.

Keywords: AWS IAM, Cloud Security, Identity and Access Management, Least Privilege, Policy Management, Unauthorized Access, CloudTrail, Security Risk Mitigation, Automated Auditing, Cloud Infrastructure.

1. INTRODUCTION

Offering unmatched flexibility, cost efficiency, and accessibility, cloud computing has changed the way companies install, control, and grow their IT resources. The move to cloud infrastructures, meanwhile, has created complicated and fresh security issues. Among them, unauthorized access, privilege escalation, and misconfigured access controls have surfaced as major threats that could cause data breaches, service interruptions, and compliance infractions. For companies depending on cloud services, then, guaranteeing strong security in cloud settings has become a top concern.

Among the top cloud service providers, Amazon Web Services (AWS) provides a complete range of security capabilities meant to enable companies safeguard their cloud resources. Identity and Access Management (IAM), which allows for fine-grained control over user access to cloud services, is fundamental to AWS's security approach. IAM controls and policies let companies implement the idea of least privilege, separate duties, and track access actions to reduce security concerns. Though these technologies are accessible, incorrect IAM policy settings and sporadic policy changes can sometimes compromise cloud systems.

This paper addressed reducing security risks in cloud infrastructures by means of efficient application and management of AWS IAM policies. The study sought to assess the effect of IAM controls on lowering illegal access and security events by means of IAM policy configuration analysis, AWS CloudTrail log monitoring, and expert knowledge inclusion. Through ideal IAM policy enforcement, ongoing monitoring, and consistent policy changes, the results aim to offer practical advice for companies to strengthen their cloud security posture.

2. LITERATURE REVIEW

Ahmad (2021) offered a basic investigation of cloud security and governance systems. His findings underlined that the quickly changing cloud scene required robust governance frameworks to properly control security concerns.

Ahmad underlined that governance included policy creation, compliance monitoring, and risk management procedures designed for cloud settings in addition to implementing technological constraints. The research contended that companies with thorough cloud governance systems were more well-equipped to reduce risks and keep regulatory compliance.

Anderson and Nguyen (2022) examined the key function of Identity and Access Management (IAM) in protecting cloud workloads. Their study showed how IAM systems were the main tool for managing user access to cloud resources, hence reducing the possibility of illegal access. The study showed that companies with strong IAM practices, defined by rigorous application of the least privilege idea and frequent policy reviews, had less security incidents. Automated technologies like IAM Policy Simulators and real-time monitoring, Anderson and Nguyen said, helped IAM policies work better by allowing administrators to quickly find and fix policy misconfigurations.

Ang'udi (2023) performed a thorough study of security issues cloud computing systems face. His study found misconfigurations, excessive rights, and inadequate policy management as ongoing weaknesses taken advantage of in cloud settings. The research found that many companies found it difficult to strike a balance between accessibility and security, which sometimes resulted in too lax access limits. Ang'udi emphasized the necessity of a layered security approach that combined strict IAM policies, network controls, and continuous security audits to strengthen cloud defenses. His results highlighted that, even with sophisticated security technologies, human elements such insufficient training and policy control still presented major concerns.

Das and Pathak (2022) investigated cloud computing among other developing technologies' relevant risk assessment and mitigation techniques. Their efforts concentrated on the proactive detection of cyber risks by means of automated risk assessment systems coupled with IAM controls. They discovered that companies using automated compliance checks and ongoing auditing were better able to find any weaknesses before they could be exploited. Das and Pathak underlined the need of automation in handling the complexity of cloud security management, especially in settings with fast changing access needs. Their study indicated that including these strategies into current IAM systems greatly enhanced an organization's capacity to react to changing dangers.

Gade (2022) focused on the security issues natural in cloud-native systems, which have become more common because of their scalability and agility advantages. His research underlined the inadequacy of conventional security strategies in cloud-native settings owing to their dynamic, distributed, microservices-based character. Gade suggested that to properly handle these difficulties, adaptive IAM policies paired with constant monitoring and policy automation were very vital. The study showed that companies using real-time anomaly detection and automated IAM policy enforcement were better able to safeguard cloud-native apps from illegal access and possible breaches.

RESEARCH METHODOLOGY

2.1. Research Design

This study employed a mixed-methods research design, integrating quantitative data analysis with qualitative insights. The quantitative component focused on evaluating AWS IAM policy configurations and CloudTrail log data from multiple organizations, while the qualitative part involved expert interviews to capture practical experiences and challenges in IAM policy management. This combined approach enabled a thorough understanding of how IAM policies impact cloud security risk mitigation.

2.2. Data Collection

Quantitative Data

Quantitative data were collected from five organizations: TechNova Solutions, CloudWave Inc., DataSecure Ltd., NextGen Systems, and CyberGuard Corp., all operating AWS cloud environments. The collected data included detailed IAM policy configurations such as the average number of policies per user, adherence to the least privilege principle, instances of over-privileged roles, and logged policy violations. Additionally, six months of AWS CloudTrail logs were analyzed to detect unauthorized access attempts and evaluate the effectiveness of IAM policy enforcement. Security incident records and the frequency of IAM policy updates were also gathered to examine their relationship with incident reduction.

Qualitative Data

Cloud security specialists and AWS administrators from the participating companies took part in semi-structured interviews. These interviews sought to reveal the difficulties experienced in controlling IAM policies at scale and highlight success elements such the usage of automated auditing tools, policy enforcement procedures, and training programs.

2.3. Sampling

Organizations with mature AWS cloud deployments and varied IAM management strategies were chosen using a purposive sampling approach. The sample consisted of five companies from different sectors, hence guaranteeing a wide viewpoint on deployment of IAM policies and their influence on cloud security.

2.4. Data Analysis

Quantitative Analysis

Key measures like the average number of policies per user, percentage compliance to least privilege, number of over-privileged roles, and reported policy infractions were derived from an analysis of the IAM policy data. Total access events, unauthorised access attempts, the percentage of access attempts denied by IAM policies, and those needing manual security intervention were all counted by parsing CloudTrail logs. A correlation study on the IAM policy update frequency and the decline in security events was also conducted.

Qualitative Analysis

Interview transcripts were coded and thematically analyzed to extract insights related to IAM policy management challenges and effective practices. Themes such as policy complexity, auditing difficulties, automation benefits, and the importance of training emerged from the analysis.

2.5. Tools and Techniques

Policy simulation and compliance auditing were done using AWS native tools such IAM Policy Simulator and AWS Config. Custom automation scripts were created to extract and examine CloudTrail log data for spotting access irregularities. Thematic extraction from interview replies and qualitative data coding were aided using NVivo software.

3. RESULT AND DISCUSSION

Results of the study's expert interviews, CloudTrail logs, and AWS IAM policy analysis are included in this section. The findings show how well IAM policies reduce security concerns in cloud systems. Moreover, the conversation analyzes the consequences of these results in relation to best practices for access control, policy configuration, and continuous security monitoring.

3.1. Analysis of IAM Policy Configurations

Examining IAM policy setups throughout the five companies showed significant differences in the adoption of security best practices. With 92% of its rules following this important security guideline, DataSecure Ltd. showed the greatest compliance to the concept of least privilege and also noted the least over-privileged roles (just one) and policy infractions (three).

Table 1: Summary of IAM Policy Security Metrics Across Organizations

Organization	**Average Number of Policies per User**	**% of Policies Following Least Privilege**	**Number of Over-Privileged Roles Detected**	**Number of Policy Violations Logged**
TechNova Solutions	4.2	85%	2	5
CloudWave Inc.	3.7	78%	4	12

DataSecure Ltd.	5.1	92%	1	3
NextGen Systems	4.5	80%	3	8
CyberGuard Corp.	3.9	88%	0	2

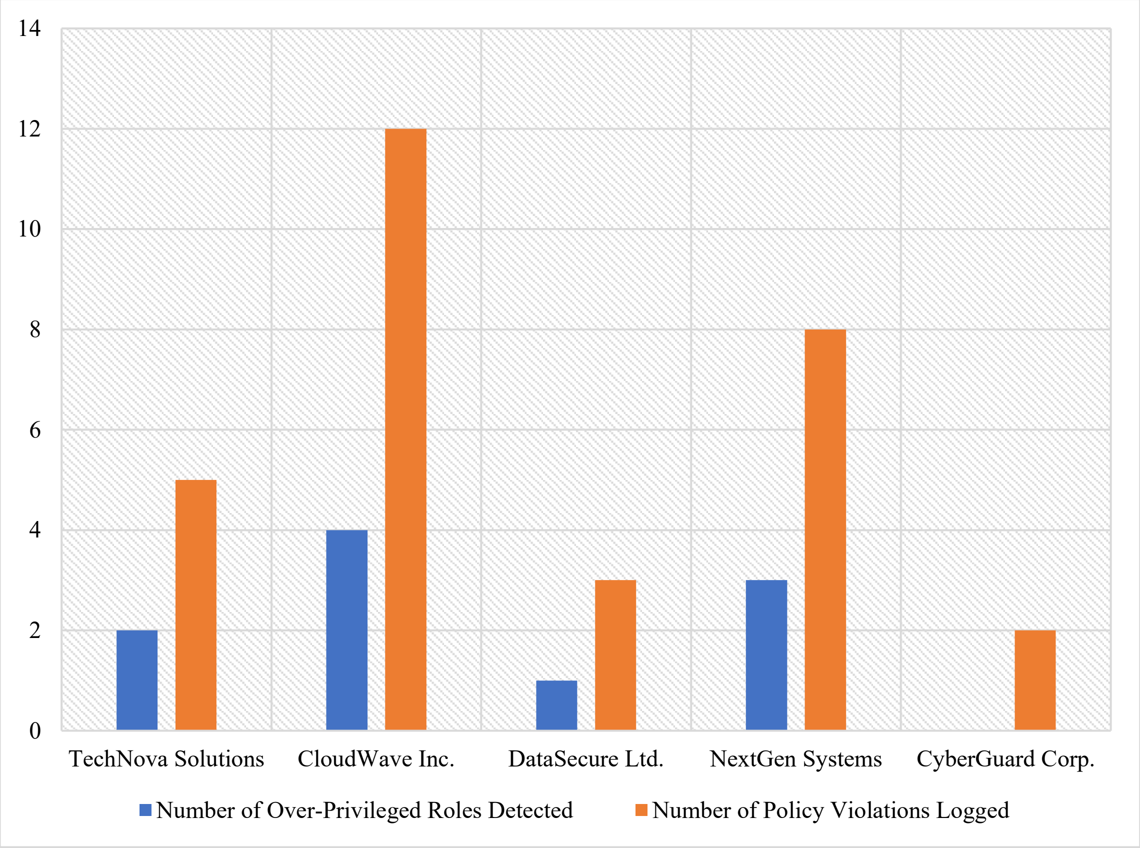

Figure 1: IAM Policy Security Metrics Across Organizations

CyberGuard Corp. kept a high standard as well with 88% least privilege compliance and no over-privileged roles found, in addition to the fewest policy infractions (two). By contrast, CloudWave Inc. showed the least privilege compliance at 78%, which corresponded to the most over-privileged positions (four) and policy infractions (twelve), suggesting possible weaknesses. With intermediate adherence rates of 85% and 80%, respectively, TechNova Solutions and NextGen Systems fell between these extremes, along with related counts of over-privileged jobs and policy infractions. The findings generally point to a significant link between more compliance with least privilege policies and a decrease in policy infractions as well as over-privileged roles, hence stressing the need of well crafted IAM policies to properly reduce security concerns.

3.2. Unauthorized Access Attempts Detected via CloudTrail

CloudTrail logs were analyzed for unauthorized access attempts over a 6-month period. Table 2 shows the number and types of access anomalies detected.

Table 2: Unauthorized Access Attempts and IAM Enforcement

Organization	Total Access Events	Unauthorized Access Attempts	Access Attempts Blocked by IAM Policies	Access Attempts Requiring Manual Intervention
TechNova Solutions	150,000	45	40	5
CloudWave Inc.	120,000	60	50	10
Data Secure Ltd.	170,000	30	28	2
NextGen Systems	130,000	55	45	10
CyberGuard Corp.	140,000	20	19	1

The study of unauthorised access attempts and the efficacy of IAM enforcement across the companies showed notable variations in their capacity to automatically prevent questionable actions. Of the 30 unauthorised access attempts DataSecure Ltd. documented, virtually all (28) were effectively blocked by IAM policies, leaving only two cases needing manual intervention. The company logged the most total access events (170,000). CyberGuard Corp. showed likewise good IAM enforcement with only 20 unauthorised attempts out of 140,000 access events and only one access attempt needing manual assessment. By comparison, CloudWave Inc. had more unauthorised access attempts—60—than total access events—120,000. Of these, 50 were rejected automatically and 10 still needed manual intervention, suggesting a greater reliance on human supervision. Reflecting different levels of IAM policy efficacy, TechNova Solutions and NextGen Systems reported modest numbers of unauthorised attempts and manual interventions. Generally speaking, companies like DataSecure Ltd. and CyberGuard Corp. with stronger, well-configured IAM policies were more successful in automatically minimizing illegal access, therefore lowering the burden on security staff and improving general cloud security.

3.3. Expert Feedback on IAM Policy Management

Interviews with cloud security experts from the participating organizations identified key challenges and success factors in IAM policy implementation:

- **Challenges:** Complexity of managing policies at scale, difficulty in auditing policies frequently, and the risk of human error in policy configuration.
- **Success Factors:** Use of automated tools like IAM Policy Simulator and AWS Config for continuous auditing, enforcing least privilege access, and regular training for cloud administrators.

3.4. Policy Update Frequency and Security Incident Correlation

The statistics on IAM policy update frequency and its relationship with security incidents showed a clear trend: companies that updated their policies more regularly had less security incidents and more incident reduction compared to the previous year. Reporting just three security issues and achieving a significant 30% year-over-year drop in events, DataSecure Ltd. revised its policies every three months on average.

Table 3: Correlation Between IAM Policy Update Frequency and Security Incident Reduction

Organization	Average Policy Update Frequency (months)	Number of Security Incidents Reported	Incident Reduction (%) Compared to Previous Year
TechNova Solutions	6	7	15%
CloudWave Inc.	12	15	5%
Data Secure Ltd.	3	3	30%
NextGen Systems	9	10	10%
CyberGuard Corp.	4	2	35%

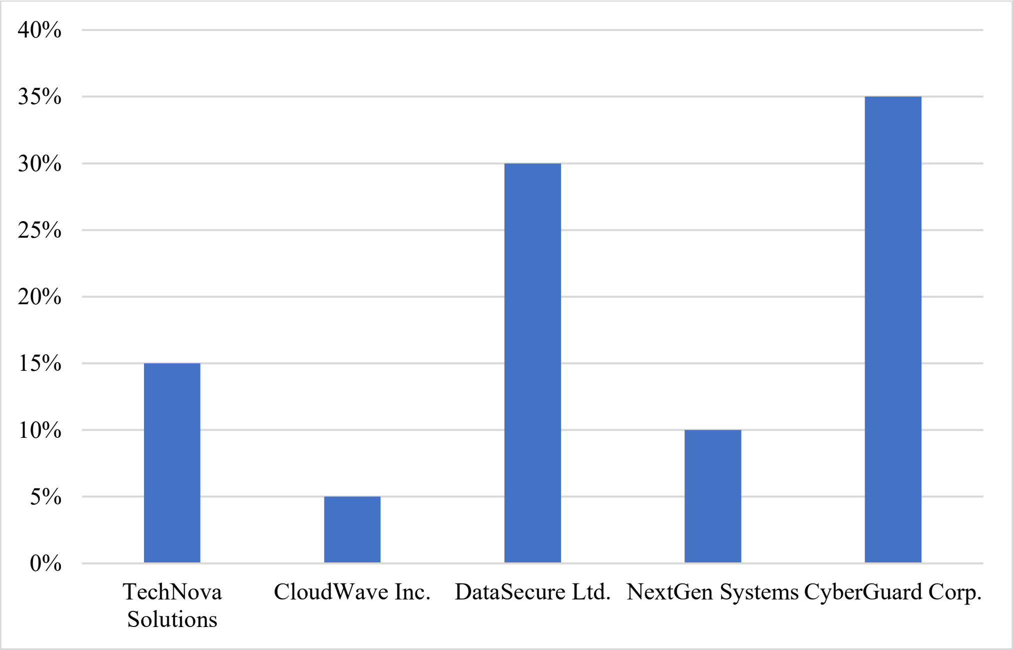

Figure 2: Correlation Between IAM Policy Update Frequency and Security Incident Reduction

Similarly, CyberGuard Corp., with an average update frequency of four months, recorded the lowest number of security incidents (two) and the highest reduction rate of 35%. By comparison, CloudWave Inc. reported the most security incidents (15) and the least incidence decrease (5%) while updating its policies the least often—once every twelve months. With moderate update frequencies of six and nine months respectively, TechNova Solutions and NextGen Systems landed in the center both in terms of incident counts and reduction percentages. These results imply that regularly changing IAM settings helps to improve cloud security by quickly handling developing threats and reducing weaknesses.

4. CONCLUSION

This work showed how important AWS IAM policies and controls are in reducing security concerns in cloud systems. The study among five companies showed that following security best practices—especially the concept of least privilege—greatly lowered the number of over-privileged jobs and policy infractions. Organizations include DataSecure Ltd. and CyberGuard Corp., which applied strict IAM policy settings, saw less unauthorized access attempts and were more successful in automatically rejecting such attempts, hence reducing the operational load on security teams. Moreover, the research underlined the need of regular IAM policy changes since companies that did so more often recorded less security events and had better incident reduction rates. While expert interviews highlighted typical issues including policy complexity and audit hurdles, they also stressed the value of continuous administrator training and automated technologies in controlling IAM policies at scale. Overall, the findings confirm that well-designed, continuously monitored, and frequently updated IAM policies are indispensable for enhancing cloud security and minimizing vulnerabilities in AWS environments. Organizations are encouraged to adopt these best practices to strengthen their cloud defenses and proactively address evolving security threats.

REFERENCES

[1] S. K. R. Khambam and V. P. K. Kaluvakuri, "Multi-Cloud IAM Strategies For Fleet Management: Ensuring Data Security Across Platforms," 2023.

[2] A. Das and P. Pathak, "Risk assessment and mitigation techniques of cyber attacks in emerging technologies," in AIP Conference Proceedings, vol. 2519, no. 1, Oct. 2022. AIP Publishing.

[3] D. Oneill, "Cloud Security in Enterprises," M.S. thesis, Utica University, 2023.

[4] D. Shields, AWS Security, Simon and Schuster, 2022.

[5] J. Anderson and A. Nguyen, "The Role of Identity and Access Management (IAM) in Securing Cloud Workloads," ResearchGate, Dec. 2022.

[6] J. J. Ang'udi, "Security challenges in cloud computing: A comprehensive analysis," World Journal of Advanced Engineering Technology and Sciences, vol. 10, no. 2, pp. 155–181, 2023.

[7] K. R. Gade, "Cloud-Native Architecture: Security Challenges and Best Practices in Cloud-Native Environments," Journal of Computing and Information Technology, vol. 2, no. 1, 2022.

[8] N. A. Khasuntsev, "Automatic detection of misconfigurations of AWS Identity and Access Management Policies," M.S. thesis, Univ. of Twente, 2021.

[9] N. Sharma, "Cybersecurity Challenges in Multi-Cloud Environments: A Policy Perspective," Challenge, vol. 4, no. 1, 2021.

[10] N. Soms, M. S. Oswalt, and K. P. Santhosh, "A case study on cloud security controls," International Journal of Health Sciences, vol. 6, pp. 11374–11380, 2022.

[11] R. Ahmad, Cloud Security and Governance, 2021.

[12] R. C. Thota, "Cloud Security in Financial Services: Protecting Sensitive Data with AWS well-Architected Framework," International Journal of Novel Research and Development, vol. 6, no. 4, pp. 1–7, 2021.

[13] S. Nevalainen, "Risk management and architecture design in securing cloud platforms: Case study of cloud," 2022.

[14] S. Somanathan, "Governance in Cloud Transformation Projects: Managing Security, Compliance, and Risk," International Journal of Applied Engineering & Technology, vol. 5, 2023.

[15] S. Talluri and S. T. Makani, "Managing Identity and Access Management (IAM) in Amazon Web Services (AWS)," Journal of Artificial Intelligence & Cloud Computing, vol. 2, no. 147, pp. 2–5, 2023, doi: 10.47363/JAICC/2023.