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 5, Issue 5, December 2025
Impact Factor: 7.67

Dynamic Cloud Framework with Custom Policy Provisioning

Dr. Kavita K Patil, Ananya SP, Chaithra T M, Harshitha H
Dept. Information Science and Engineering
Global Academy of Technology, Bengaluru, India
kavitapatil@gat.ac.in, ananyashridhar2209@gmail.com
chaithratm1ga22is030@gmail.com, harshitha1ga22is060@gmail.com

Abstract: *Businesses lacking technical teams face significant hurdles in cloud migration, particularly with security. Static permission models often lead to resource misuse. Attribute-Based Access Control (ABAC) offers a more granular, dynamic solution. This paper presents a literature review of current cloud security models, focusing on ABAC, automated policy provisioning, and cloud auditing. The review synthesizes findings from recent papers on AWS IAM, S3 bucket security, and infrastructure automation. The key finding is a significant gap in the literature: a lack of integrated frameworks that translate high-level, client- centric business requirements into automated, dynamic security policies in cloud environments. This survey highlights the need for a practical methodology, such as one using AWS IAM Identity Center attributes, to bridge this gap.*

Keywords: Attribute-Based Access Control (ABAC), Cloud Security, AWS, IAM Identity Center, Policy Provisioning, Automation, Zero Trust, Least Privilege

I. INTRODUCTION

The adoption of cloud services, particularly Amazon Web Services (AWS), is accelerating. However, many organizations, especially smaller ones or educational institutions, lack dedicated in-house IT teams to manage this migration securely. This often results in static, overly permissive security models that lead to resource misuse and significant security vulnerabilities, such as data leakage from misconfigured S3 buckets.

A promising solution to this challenge is Attribute-Based Access Control (ABAC), a model that grants permissions based on user and resource attributes rather than static roles. ABAC aligns with Zero Trust principles and allows for highly granular, real-time access decisions. When combined with automation, it can provide a secure, flexible, and scalable framework.

This paper surveys the existing literature to understand the current state of ABAC implementation, automated cloud security, and client-centric cloud models. Section II categorizes and reviews relevant papers. Section III discusses the key findings and identifies the primary research gap. Section IV concludes by summarizing the review and pointing toward future work.

II. BACKGROUND AND RELATED WORK

The literature surrounding cloud security is vast, but it is often fragmented into specific domains. Our review consolidates findings from papers focusing on access control models, security auditing, and automation

A foundational 2021 paper, “Attribute-Based Access Control for Cloud Environments,” proposes a dynamic access model based on user and resource attributes. The authors implement a rule-based ABAC model and conclude that while it significantly improves security granularity, its practical implementation in large environments necessitates efficient automation. Other studies from 2021 also explore access control models for privacy protection, but often lack specific mapping to AWS services.

A second major body of work focuses on cloud security auditing and misconfiguration. A 2022 paper, "Private Amazon S3 Buckets Can Leak," provides a real-world audit of misconfigurations. This is complemented by "Finding Vulnerable

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 5, Issue 5, December 2025 Impact Factor: 7.67

S3 Buckets" (2018), which reveals security gaps in storage. More advanced solutions are proposed by Torkura et al. (2023) in "Continuous Auditing in Multi- Cloud," which uses IAM audits and CloudTrail for real-time monitoring. This approach is ideal for validating the dynamic IAM policies that our project seeks to create.

The third domain is automation. "Application Modernization for AWS Cloud" (2022) demonstrates using Infrastructure as Code (IaC) tools like Terraform with CI/CD pipelines to enable infrastructure automation. While this validates the feasibility of automation, these solutions are often too complex for beginners or non-technical clients.

Our analysis of the literature reveals a significant gap: no single framework bridges the divide between high-level, client-centric business requirements and the low-level, technical implementation of automated, dynamic security policies. The key challenges identified in the literature— translating uncertain requirements, mapping attributes to ABAC conditions, and balancing usability with strict control —remain largely unsolved. This project aims to address this specific gap

III. LITERATURE REVIEW

A. Access Control Models and ABAC

The foundational literature supports the move toward more dynamic access control. A 2021 IEEE Access paper, "Attribute-Based Access Control for Cloud Environments," proposes a dynamic model based on user and resource attributes. It concludes that while ABAC improves security granularity, it requires efficient automation to be effective in large-scale environments. Other papers from 2020 and 2021 reinforce this by discussing access control models for data privacy and secure storage, though they are not always AWS- specific.

B. Cloud Security Auditing and Misconfiguration

A significant body of work focuses on identifying and mitigating security flaws in the cloud. Papers from 2022 and 2018 specifically highlight the real-world risks of misconfigured S3 buckets. Torkura et al. (2023) propose continuous auditing of IAM policies and real-time monitoring to detect role misconfigurations , which is ideal for validating dynamic policies. Similarly, a 2024 paper discusses auditable data sharing using cryptographic tokens. These papers confirm the problem but often lack an automated provisioning solution..

C. Automation and Infrastructure as Code (IaC)

Automation is a recurring theme for managing cloud complexity. A 2022 paper on "Application Modernization for AWS Cloud" demonstrates the use of tools like Terraform and CI/CD pipelines to automate infrastructure deployment. This research validates the feasibility of automation but is often highly technical and not aimed at non-technical clients.

D. Client-Centric Cloud Strategy

A 2025 paper, "Cloud Meets Customer," provides a strategic Overview of how cloud Providers can serve non-technical clients. This paper is crucial as it matches the real-world client scenario That motivates our project. However it is is high level strategic Paper and does not provide a technical methodology.

IV. COMPARISON TABLE

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 5, Issue 5, December 2025 Impact Factor: 7.67

Ref	Year	Author(s)	Technique / Model	Key Findings	Limitations
[1]	2025	Sven Depner	Cloud Meets Customer	Matches your real-world client scenario	Not a technical /methodology paper
[2]	2024	K Sunda r,G.Ki ran Vish wak	Enhanci ng cloud security: Audi table data shari ng	Improved recall by combining deep & shallow models	Complex training pipeline
[3]	2023	To rkura et al.	Continuous Auditing in MultiCloud – Torkura et al.	Ideal for dynamic IAM policy validation	Slight complexity in multicloud setup
[4]	2 022	Raji Krishnamurthy.	Private Amazon S3 Buckets Can Leak	Real IAM error examples	Storag efocused only
[5]	2 022	Shilpi Mishra .	A WS Cloud Security Challenges & Solutions	Explains AWS IAM roles	Lacks code/dem o support
[6]	2 022	P.D. Boisro nd	AWS Cloud Security Challenges & Solutions	Explains AWS IAM rules	Lacks code/demo support
[7]	2 022	Vijay Tumma.	Application Modernization for AWS Cloud	Enables infrastructure automation	Too complex for beginners
[8]	2 021	C.N.Hofer	Cloud Computing	Benchmarks are helpful	Lacks IAM and Policy scope
[9]	2021	Y.H. Kuo	Privacy Protection in Cloud – Y.H. Kuo	Data stays confidential during use	No AWS service mapping
[10]	2 021	Francisco Airton Silva.	Cloud-Native Apps Performance	Useful for Lambda deployment	No focus on IAM or policy provisioning
[11]	2020	Shah et al.Ag	Scalable and Secure Cloud Data Storage	Strong data privacy	Not AWS-specific
[12]	2019	Gaurav Rohatgi	AWS Cloud Security best practices for Saas	Allig ns with AWS IAM Setup	No Automati on
[13]	2018	Jac k cable et al.	Finding Vulnerable S3 Buckets	S3 security gaps revealed	Lacks automation; outdated tools
[14]	2017	Sourav Mukherjee	Benefits of AWS in the Modern Cloud	Scalable and costefficient	No technical depth (e.g., IAM, automat

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 5, Issue 5, December 2025
Impact Factor: 7.67

V. FUTURE RESEARCH SCOPE

• Enhanced Security: Integrating multi-factor authentication and fine-grained session control would further harden the framework.

• Service Expansion: The ABAC model can be extended to control access to other AWS services, such as AWS Lambda, DynamoDB, and
CloudWatch.

• Auditing And Federation: Adding real-time policy monitoring with AWS CloudTrail and Config, and integrating external identity providers like Azure AD using SCIM for attribute synchronization, would make the solution enterprise-ready.

• Usability: A simple web dashboard could be built for non-technical admins to manage user attributes, further abstracting the underlying policy complexity.

VI. CONCLUSION

This literature survey confirms that while robust cloud services and security principles like ABAC are available, their usability remains a challenge for non-technical clients. The review highlights a clear research gap: the need for a client-centric system that automates the deployment of cloud infrastructure and, most critically, provisions customized, dynamic security policies based on business needs.

Future work, as embodied by our project, should focus on creating a deployable framework that uses AWS IAM Identity Center attributes to dynamically enforce least-privilege access for different organizational roles. This approach would directly address the identified gap, providing a secure, flexible, and scalable solution for institutions and businesses alike.

REFERENCES

[1] C. Baviskar, “Cloud Based Automated Encryption Approach to Prevent S3 Bucket Leakage Using AWS Lambda,” National College of Ireland, 2022.
[2] GeeksforGeeks, “S3Scanner - Scan For Open S3 Buckets and Dump,” 2022.
[3] D. Hofman, L. Duranti, and E. How, “Trust in the Balance: Data Protection Laws as Tools for Privacy and Security in the Cloud,” Algorithms, 10(2), 2017.
[4] J. Wang, Y. Zhao, S. Jiang, and J. Le, “Providing Privacy Preserving in Cloud Computing,” 3rd International Conference on Human System Interaction, IEEE, 2017, pp. 472–475
[5] Amazon Web Services, “AWS Security Best Practices,” AWS Whitepapers, 2020.
[6] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds,” ACM Conference on Computer and Communications Security (CCS), 2009.
[7] L. Zhao, C. Liu, and Z. Zhang, “Data Security in Cloud Computing: A Survey,” International Journal of Cloud Computing and Services Science, 2016.
[8] S. Sharma and P. Gupta, “Cloud Data Security and Privacy: A Survey of Techniques and Challenges,” International Journal of Computer Applications, Vol. 113, No. 3, 2015.
[9] M. Dahiya and J. Mathew, “Access Control Techniques in Cloud Computing Environment: A Review,” Procedia Computer Science, Vol. 167, 2020, pp. 2018–2027.
[10] Attribute-Based Access Control for Cloud Environments,” IEEE Access, 2021.
[11] “Cloud Meets Customer,” 2025.
[12] Torkura et al., “Continuous Auditing in Multi-Cloud,” 2023.
[13] “AWS Cloud Security Challenges & Solutions,” 2022.
[14] “Application Modernization for AWS Cloud,” 2022.
[15] Y.H. Kuo, “Privacy Protection in Cloud,” 2021