ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 3 Issue 2 June 2023 / Page No: 135-139
Paper Id: JETA-V3I6P108 / Doi: 10.56472/25832646/JETA-V3I6P108

Original Article

Zero Trust Identity and Access Management (IAM) in Multi-Cloud Environments

Hariprasad Sivaraman
Independent Researcher, USA.

Received Date: 02 June 2023 Revised Date: 05 June 2023 Accepted Date: 15 June 2023

Abstract: *With multi-cloud strategies being adopted globally, managing identity and access across cloud platforms is a problem that can longer be ignored. The single environment Identity and Access Management (IAM) solutions can hardly enforce the same policy (consistency) and the inter-cloud/gen interoperability between clouds or agility in complex threats landscapes, and are non-multi cloud (non-support). This research paper presents a Zero Trust IAM model designed for multi-cloud ecosystems, with identity verification, unified governance, continuous authentication in Watchful Security Zones (WSZs), and micro-segmentation to break identities up into separate segments that can be isolated. It establishes a unified identity layer between cloud providers for security, compliance and ease of operation.*

Keywords: *Zero Trust, Identity and Access Management (IAM), Multi-Cloud, Cloud Security, Authentication, Access Control*

I. INTRODUCTION

While multi-cloud sounds exciting (especially from the potential of expansion), it introduces a new set of IAM challenges. Each cloud provider has their own IAM capabilities, security protocols and compliance features that uncover a new identity management arena that is complex, yet often inconsistent. Perimeter and IAM solutions fail in multi-cloud architectures as the identities are spread across distributed networks. Zero Trust rooted on a "never trust and always verify" methodology approach appears as a possible solution to the IAM challenges mentioned above.

Other than its antiquated perimeter defenses, Zero Trust IAM builds upon the principle of never blindly trust any user system without thorough verification of all accesses while performing continuous checks on users leveraging contextual attributes via risk-based access; thus, reducing lateral move with micro-segmentation. Zero Trust IAM offers such a framework which makes authorization secure and efficient by allowing organization to ensure security policies are uniform across different platforms in enterprise multi-cloud environments. This paper proposes a case-oriented implementation of an end-to-end Zero Trust IAM model in relation to multiple cloud platforms and its challenges for Identity Management (IDM), Policy Enforcement Points (PEP) and adaptive access controls usage scenarios.

II. PROBLEM STATEMENT

Among the most crucial problems that make IAM in multi-cloud environments security-compromising and operationally inefficient are:

- *Non-Uniform Security Policies:* Even cloud providers providing their own IAM feature are bundled with different functionalities and thus make them complicated to maintain a single IAM policy. This inconsistency creates security holes and makes regulatory compliance complicated.
- *Reduced Visibility into Identity and Access:* Identities stretch across the cloud platform, making it hard to know just who has access to what resource, when and under what conditions. However, this decentralization has a risk of illegal access due to the fact that each have their own drive and not all drives are supervised.
- *Enlarged Attack Surface:* Criminals can prey on multiple access points within a multi-cloud environment. Such environments cannot be effectively secured using traditional IAM frameworks.
- *Static Access Criteria:* Traditional IAM tools are static and cannot adjust access criteria based on the real-time context through & from various cloud environment

III. PROPOSED SOLUTION: ZERO TRUST IAM IN MULTI-CLOUD ENVIRONMENTS

To address the challenges, a Zero Trust IAM framework is proposed that adopts an extensive multi-layer approach through its layers of Dynamic Identity Verification, Identity Governance Admin (IGA), Continuous Authentication and Micro Segmentation for Isolation of identity.

A. Dynamic Identity Verification

a) Concept

Dynamic Identity Verification evaluates the real-time context and continuously verifies identity, not only looking at who the user is, but also how they are accessing resources. ML is used to model identity behavior and prove legitimacy.

b) Mechanism

Behavioral Analysis: Using historical data, ML algorithms analyze the behavioral characteristics of an identity and flag that are unusual. Unusual activities that may provoke closer scrutiny and/or subsequent verification processes

i) Real-time Contextual Data:

Device Attributes, Geo-location and Network Flagging. For example:

- Device Fingerprinting: It compares device attributes (like OS, browser type, etc) with known profiles.
- Geo-Location Data: It verifies the user according to his habitual geographical locations, preventing unauthorized access.

ii) *Adaptive Policy Engine:* This fast (and instantaneous) policy engine determines who gets access to what. It automatically changes its behavior in line with the risk, requesting more verification when something appears unusual.

c) Technical Architecture

A centralized machine learning engine powers the identity verification module interaction with each cloud provider IAM API to evaluate risk in real-time utilizing stored identities. Identity verification functions at microservices architecture support running each locally within respective cloud environments and synchronized updates to the central identity database

B. Unified Identity Governance

a) concept

Centralizing your identity governance in one place allows for visibility of more control of your Zero Trust posture across cloud providers. This also makes sure, that policies are applied the same way across the board, and audit logs position it nicely for compliance.

b) Mechanism

- Centralized Policy Repository: These are stored in the centralized policy repositories as per organizational security norms and regulation compliance.
- Policy Translation & Enforcement: This governance layer translates organizational policies to CSP-compatible rules, ensuring enforcement consistency across platforms.
- This layer secures the audit of compliance over the cloud: Audit continuously governance layer not only detects policy changes, but also records every attempt to access resources and identity interaction to them in a way that can be used for regulatory compliance and accountability.

c) Technical Architecture

Governance Layer: A cloud-agnostic microservices architecture that communicates with each CSPs IAM APIs. The microservice policy management translates the policies for enforcement in a CSP-native manner, while event-driven architecture ensures audit logs are stored in cross-cloud database.

C. Continuous Authentication

a) Concept

A one-time initial authentication is context-aware authentication for all of the action within an environment. Making faraway security risks more manageable is one of the core elements of the Zero Trust posture, and this approach can be a significant part of that solution.

b) Mechanism

- Context Data Session: The permission of an authenticated user is re-evaluated for every action made on the system and based on what real-time context data.
- Risk-based Scoring & Dynamic Risk Assessment: All actions are scored as low risk or high risk and additional validation is needed for any activities that carry a higher risk level, at times denial of access can occur immediately.
- Adapting policies: Access permissions may dynamically change based on how risk characteristics evolve over time. For example, an unusual location + action can make you want to check the user.

c) Technical Architecture

The continuous authentication across each of the cloud IAMs is driven through APIs by dynamic risk scoring component powered with a real-time behavioral analytics engine. This component communicates with the governance layer to enforce new policies as risk scores evolve.

D. Micro-Segmentation for Identity Isolation

a) Concept

Micro-segmentation extends this concept of isolated access zones to the identities, such that each identity can access only what it needs (zone). This is beneficial to reduce the risk of unauthorized lateral movement in a multi-cloud environment.

b) Mechanism

- Role based Segmentation: Identities are segmented on the role basis only so that relevant functions can be accessed
- Functional Isolation Zones: Isolate identities on functional zones such as dev vs prod env, hence ensuring no access to either environmental zone.
- Dynamic, Granular Privilege Management: Allows users to be dynamically granted or restricted privileges in real time based on behavioral breaches from a baseline of normal activity.

c) Technical Architecture

Micro-segmentation is enforced by network-based access controls and IAM policies inside each cloud. Governance layer: A single point of record for isolation zones and privilege management between CSPs.

IV. IMPACT OF ZERO TRUST IAM IN MULTI-CLOUD ENVIRONMENTS

Deploying a Zero Trust IAM model across multi-cloud environments enhances security, compliance and operational management in several ways. Here are the specific effects organizations can expect to see from this model.

A. Enhanced Security Posture

The Zero Trust IAM enables a continuous real time verification of identities and access requests, replacing the unchanging identity and authentication models with a dynamic adaptive model providing constant context. Restricted rights pollute identity theft opportunities less and aids in combating advanced threats, including phishing and credential stuffers and privilege escalation.

- Minimized insider threats: Persistent authentication and micro-segmentation reduces the ability of users to move laterally in the system, which is a common technique adopted by malicious insider threats and thus mitigates insider attacks.
- Reduction in Credential-Borne Attacks: Real-time, behavior-based analysis paired with dynamic policies allow access to be highly customizable based on risk-based criteria. Therefore, the odds of an attacker using stolen credentials or a compromised session are much lower as there would be reduced opportunities for such entities to gain access to these resources.

B. Improved Compliance and Audit Capabilities

This model provides complete governance and centralized compliance framework, which will be a strong benefit for highly regulated industries such as finance, government and health care.

- Centralized Policy Enforcement: With Zero Trust IAM policies on identity access are enforced somewhere else and therefore it can be applied consistently across multiple cloud providers, which means greater compliance with standards like GDPR, HIPAA & PCI DSS.
- Minimized Audit Complaints: the cross-cloud compliance auditing capability of the organizations allows them to maintain an audit trail for access attempts, identity interactivity and policy enforcement operations. Also, it not only improves the visibility but provides consolidated logs and reports to augment the audit process.

- Improved Data Sovereignty: Organizations adopting this technology in a variety of jurisdictions can utilize the governance layer, where policies defined based on local applications ensure adherence to regional data sovereignty regulations.

C. Increased Operational Efficiency in Identity Management

In multi-cloud environments, users manage multiple cloud platforms where it is a significant operational challenge to provision identities and enforce user access policies across different cloud platforms. The Zero Trust IAM framework resolves this issue by directly facing the case of organizational identity management and policy enforcement challenges. Such of the above features are aligning organizations workflows which leads to an increase in operational efficiency. Identity governance adopting a centralized policy management followed by a single point control for identity governance would simplify such frivolous tasks drastically.

D. Reduced Risk of Lateral Movement and Privilege Escalation

Micro-segmentation and role-based access controls are the core functionality of the Zero Trust IAM model that restricts resource access per context-specific roles and functions. By enforcing this segregation of identities into well-defined segments, lateral movement and APTs escalations are cosmically limited.

E. Agility and Scalability in Multi-Cloud Identity Management

Even more importantly, the Zero Trust IAM model is versatile meaning it has a scalable architecture which you can use to manage identities all over every cloud expansion. The benefit comes with the interest of having such a gigantic cloud infrastructure in one account from allowing for centralized identity governance and dynamic policy controls that enable quick adjustments to IAM policies, instantly as a organizations scales.

V. LIMITATIONS AND FUTURE WORK

The proposed Zero Trust IAM framework addresses many of the challenges faced in multi-cloud environments, although it does have some limitations.

a) Limitations

- Integration complexity: A centralized Zero Trust IAM system must be configured and orchestrated to operate with each cloud environment, which can differ in IAM capability and APIs.
- Performance Overheads: Continuous authentication and real-time identity verification may add latency, particularly in high-traffic environments since any access activity is dynamically verified.
- Intensive Management: A fully functional policy engine (dynamic/adaptive), behavioral analysis (mostly AI, ML based) and micro-segmentation will require use of resources to maintain such an environment, on-going computing costs in terms of storage/network usage and high operational costs.
- Quality of Data: Good behavioral analytics and risk scoring can be created only when the data quality is very high. This could limit the effectiveness of adaptive controls when data quality is poor

b) Future Work

- Improvement of Adaptive Policies: Future research can improve the machine learning algorithms to construct more accurate adaptive policies that are aware of context-sensitive and provide fewer false positives in an increasing number of cases while improving security.
- Extending Zero Trust IAM into edge computing and IoT eco-systems: in my personal opinion, this model needs extending to ensure that identities are managed within the scope of edge computing and IoT where traditional IAM models do not necessarily apply.
- Improving Identity Verification and Data Integrity Across Cloud Environments Blockchain for Decentralized Identity: Exploring blockchain as a decentralized identity management mechanism within the scope of Zero Trust could facilitate better identity verification and data integrity among cloud environments.
- Performance Optimization: Future work can focus on the aspects of optimization to ensure that real-time continuous authentication does not introduce any latency or burden in terms of slow speed for the user.

Highlighting these potential improvement and exploration areas can further develop the Zero Trust IAM framework to adapt to more varied yet intricate digital infrastructures.

VI. CONCLUSION

Increasing use of multi-cloud architectures will also make strong, uniform IAM across disparate platforms a necessity for organizations. Multi-cloud environments give rise to disjointed policies and multiple access points, which significantly broaden the attack surface, thus traditional IAM frameworks are insufficient to accommodate dynamic security needs. The Zero Trust IAM model offers an end-to-end solution that continuously verifies identity, applies adaptive controls, and enforces a unified policy across clouds; addressing these challenges head-on to create synergistic and holistically resilient security posture.

The multi-layered approach of this model; the dynamic identity verification, unified governance, continuous authentication and micro-segmentation, creates an enterprise ready security posture that is scalable and agnostic while facilitating compliance as well. This Zero Trust IAM framework mitigates potential threats by minimizing lateral movements and enabling third-party access for fast risk-based assessments, while reducing the burden of compliance with regulatory requirements and helping manage identities in complex cloud ecosystems.

The adaptive capabilities exhibited by this model lead to future work, especially with application within newly emerging technologies such as Internet of Things and edge computing, which may be effectively incorporated into the domain of complex system models that fortify securing digital infrastructures in new and secure ways.

VII. REFERENCES

[1] J. Kindervag, "Build Security into Your Network's DNA: The Zero Trust Network Architecture," Forrester Research, 2010.

[2] "Zero Trust Architecture," National Institute of Standards and Technology (NIST), Special Publication 800-207, 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207

[3] Bhargavan, M. Delignat-Lavaud, and K. Bhargavan, "Transport Layer Security: Zero Trust Architecture and End-to-End Encryption," in *Proceedings of the 27th USENIX Security Symposium*, Baltimore, MD, 2018, pp. 192–205.

[4] S. Maresca, J. Kampman, and D. Medina, "Implementing Identity and Access Management in Multi-Cloud Environments," in *ACM International Conference on Cloud Computing Security*, 2019, pp. 45–54.

[5] L. Chandramouli, "Identity as a Service (IDaaS) for Multi-Cloud Environments," in *IEEE Cloud Computing*, vol. 3, no. 5, pp. 32-40, Sep.-Oct. 2016, doi: 10.1109/MCC.2016.112.

[6] Naik and P. Kumar, "Behavioral Analysis for Continuous Authentication Using Machine Learning," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 745-757, Mar. 2019, doi: 10.1109/TIFS.2018.2869914.

[7] R. S. Sandhu, "Role-Based Access Control Models for Security in Multi-Tenant and Multi-Cloud Systems," in *IEEE Computer*, vol. 48, no. 4, pp. 80-83, Apr. 2015, doi: 10.1109/MC.2015.106.

[8] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Trust Management in Cloud Services," in *IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, 2013, pp. 522–527, doi: 10.1109/CloudCom.2013.75.

[9] J. Heiser and M. Nicolett, "Defining Cloud Security Architecture for the Modern Enterprise," Gartner Research, 2020. [Online]. Available: https://www.gartner.com

[10] C. Lin and J. Yao, "Machine Learning and AI-Driven Adaptive Access Control for Cloud Security," in *Proceedings of the IEEE Conference on Cloud Computing and Security*, 2021, pp. 111-120.