Chapter 17
Sustainable Access Management for Cloud Instances With SSH Securing Cloud Infrastructure With PAM Solutions

Subash Banala
https://orcid.org/0009-0004-0802-8179
Capgemini, USA

Vivekchowdary Attaluri
https://orcid.org/0009-0001-5750-562X
Capital One, USA

ABSTRACT

In the era of cloud computing, securing access to cloud instances is paramount for protecting sensitive data and ensuring compliance with industry standards. Secure Shell (SSH) access management plays a critical role in safeguarding cloud environments by controlling how users interact with cloud-based systems. However, traditional SSH access management methods can often be cumbersome, error-prone, and vulnerable to breaches. This paper explores the implementation of Privileged Access Management (PAM) solutions for enhancing the security of SSH access to cloud instances. By integrating PAM systems with cloud infrastructure, organizations can enforce stricter access controls, enable detailed session auditing, and reduce the risk of unauthorized access. The paper discusses best practices for managing SSH keys, monitoring user activity, and automating access management workflows using PAM solutions, ultimately improving the security posture of cloud environments.

1.1 INTRODUCTION

Cloud infrastructure security refers to the set of policies, technologies, and controls designed to protect cloud environments from unauthorized access, data breaches, and cyber threats. As businesses increasingly migrate their workloads to the cloud, securing cloud instances becomes a critical focus. Unlike traditional on-premises infrastructures, cloud environments are highly dynamic, scalable, and

DOI: 10.4018/979-8-3693-9750-3.ch017

often involve multi-cloud or hybrid environments, which introduces unique challenges in securing data, applications, and user access. Effective cloud security ensures the confidentiality, integrity, and availability of data, which includes securing access to cloud instances, networks, applications, and managing the shared responsibility model between cloud providers and customers. This landscape requires continuous vigilance, risk management, and robust security measures like encryption, identity management, firewalls, and access controls.

1.2 Importance of Secure SSH Access Management

Secure Shell (SSH) is widely used for secure communication and remote administration of cloud instances, making it an essential tool for accessing cloud-based systems. However, SSH access also presents a significant security risk if not managed properly, as it provides direct access to critical systems. Without effective SSH access management, organizations are exposed to the risk of unauthorized access, key compromises, and potential data breaches. Managing SSH keys and sessions in cloud environments can become complex, especially as the number of cloud instances grows. If SSH keys are not securely stored, tracked, or rotated, they can be misused or stolen. Therefore, secure SSH access management ensures that only authorized users and applications can access sensitive cloud resources, significantly reducing the risk of cyberattacks. The integration of Privileged Access Management (PAM) in securing cloud instances has become a focal point in contemporary research, particularly in addressing vulnerabilities and optimizing access control mechanisms. Liu and Zhang (2022) explore how PAM can be applied to manage access in hybrid cloud environments, offering insights into its effectiveness in securing sensitive data across diverse platforms. Building on this, Mitchell and O'Brien (2023) highlight how PAM adoption can enhance the security of cloud instances, emphasizing its sustainable application in managing privileged user access. Nair and Chopra (2021) provide a practical approach to streamlining SSH-based access in cloud environments, showcasing the role of PAM in simplifying and securing user authentication. Patel and Reddy (2022) focus on how PAM can effectively manage cloud administrator access, ensuring secure and authorized interventions in critical infrastructure. Similarly, Richards and Walker (2023) propose a PAM-centric approach to securing SSH access, aiming to reduce risks associated with unmonitored access to cloud instances. Sharma and Verma (2021) discuss the intersection of PAM and SSH in modern cloud security, noting how this integration supports a holistic approach to securing cloud infrastructures. In line with these advancements, Thomas and White (2022) emphasize the importance of balancing sustainability and security, ensuring that access management solutions are both effective and environmentally viable. Furthermore, Wang and Zhou (2023) address the challenges and solutions in SSH key management, underscoring the need for robust PAM frameworks. Williams and Black (2022) highlight the enhancements in access control within cloud environments, attributed to the strategic use of PAM tools. Yang and Chen (2023) also discuss privileged access management for sustainable cloud systems, illustrating how PAM plays a critical role in long-term cloud security. In addition to these studies on PAM, various other studies touch upon the broader field of security, such as Boddu et al. (2024), who examine security issues in intelligent transportation systems using deep learning, offering a perspective on AI's role in securing infrastructure. Yadav et al. (2024) explore transportation logistics monitoring via machine learning, demonstrating how AI can enhance system efficiency and security. In the realm of food safety, Vegesna et al. (2024) leverage AI to ensure safe food supply chains, while Whig et al. (2024) analyze the strategic role of analytics in driving business value and competitive advantage. Koushik et al. (2024) focus on the predictive maintenance of supply