International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V73I2P110

Volume 73 Issue 2, 80-89, February 2025

Original Article

Machine Identity Security in Cloud & AI: Ensuring Lifecycle Management, Ownership, and Accountability for Non-Human Identities

Anant Wairagade

Independent Researcher, Phoenix USA

Corresponding Author : anant_wairagade@ieee.org

Received: 30 December 2024 Revised: 26 January 2025 Accepted: 17 February 2025 Published: 28 February 2025

Abstract *- Machine Identity Security is critical to protecting modern digital ecosystems. The expansion of Cloud and AI technologies across organizations has dramatically expanded the number of machine identities, representing everything from APIs to IoT devices and software services. These identities are essential for authentication, encryption, and communication between interlinked systems. However, managing machine identities is now a critical challenge because dynamic workloads, ephemeral containers, and automated processes have added unprecedented complexity [1]. As continuous data flows through the cloud environment and infrastructure evolves rapidly, breaches resulting from vulnerabilities associated with machine identities can be devastating. Example: API Key or Certificate — A compromised API key or an expired certificate can allow an attacker access to sensitive data or disrupt services. An evolving security framework focused on Cloud and AI ecosystems will be needed to address these risks. According to a research paper, recent strides in Machine Learning (ML) provide cloud security applications with threat detection, credential management, and other aspects of resilience that increasingly rely on algorithms [2]. This research aims to connect the concepts from theoretical frameworks to executable scenarios that can be implemented in the form of Machine Identity Security solutions. In particular, this will cover machine identity lifecycle management, accountability mechanisms, and miscellaneous problems raised by Non-Human Identities [3].*

Keywords *- Machine Identity Security, Non-Human Identity, Life cycle Management, Cloud and AI, Automated Governance*.

1. Introduction

Machine Identity Security encompasses protecting Non-Human Identities — identities not intended to be directly interacted with by people, such as service accounts, APIs, IoT devices, automation scripts, etc. Non-human identities are essential building blocks of Cloud and AI ecosystems that keep automated processes running without user involvement. These identities provide process authentication, handle encrypted communication, and guarantee secure data exchange.

For example, an Internet of Things (IoT) thermostat in a smart building could communicate securely with a central server using a digital certificate. In the same fashion, service accounts are leveraged in DevOps pipelines to deploy accounts are leveraged in DevOps pipelines to deploy containers or access cloud resources. The study highlights that these identities typically far exceed the number of human users and are susceptible to abuse if not properly secured. Given the lack of an adequate identity management foundation, attackers can leverage orphaned or over-privileged credentials to perform unauthorized actions.

The explosion of data towards the Cloud and AI has led to a massive growth in the number of machine identities. Machine identities have now accounted for more than 60% of all organizational credentials present in cloud environments. There are expected to be over 25 billion IoT devices in the world by 2030, as shown in Figure 1, all of them needing secure identities to operate without creating security holes. More than 50% of organizations indicate that managing the machine identity lifecycles (e.g., certificate provisioning and key rotation) is a key challenge. With the rise of the Zero Trust Architecture — the idea that every piece of machine communication needs to be authenticated — enterprises began to realize the importance of machine identity governance. Yet, needing automated visibility into these identities continues to be a challenge.

Over the years, organizations have faced huge challenges associated with increasing dependence on nonhuman identities in Cloud and AI environments, complicating the management of identities lifecycle, accountability, and ownership. make that system prone to security breaches and unauthorized access.

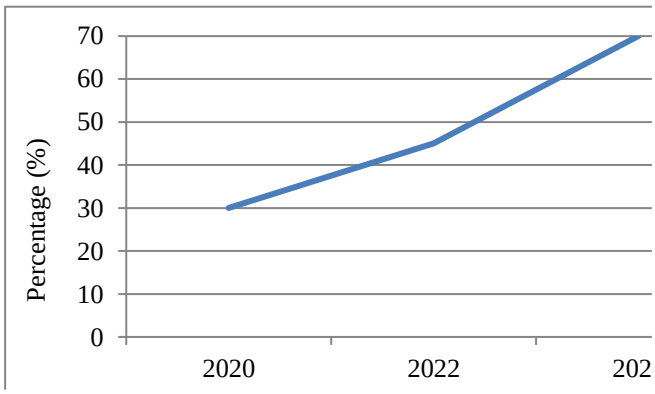

Fig. 1 Surge in IoT devices relying on machine identities

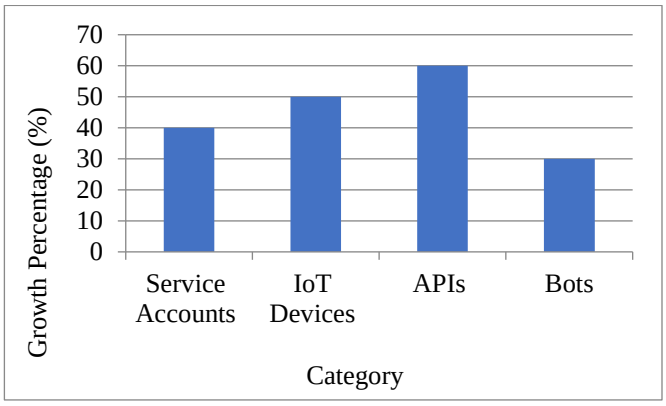

Fig. 2 Growth of Non-Human identities by category

Conventional security frameworks have limitations that the growing use of advanced AI and cloud applications has paved the way towards machine identities, including APIs and IoT devices. Despite that, with no strong security methods in place, the organization faces huge security challenges in the form of credential misuse, unauthorized access, and failure to comply with regulatory standards.

This work aims to minimize the gap by offering theoretical knowledge of actionable machine identity security solutions. The focus is to provide a path towards improving machine identities' lifecycle management and furthermore, implementing robust accountability procedures and handling the unique security challenges linked with non-human identities inside the AI and cloud environment. What makes our work novel is that it offers a detailed insight into interconnected challenges of non-human identity lifecycle governance and accountability.

On the other hand, existing research only focuses on common aspects of machine identity management, while some work focuses on separate aspects like access controls or certificate management. None of the existing work consolidates research towards improving the security and compliance for non-human identities in AI and cloud environments. In contrast, our work overcomes these gaps, thus offering a major contribution to this domain.

2. Comparative Analysis of Non-Human Identities

Non-human identities are treated differently by organizations with mature Machine Identity Security practices than those without. A comparison is shown in Table 1. The results are night and day. Mature organizations have more reported breaches associated with machine identities and faster average recovery times when breaches happen. This does not mean that mature organizations are more vulnerable to cyber-attacks, but it showcases the ability of mature organizations to monitor and detect breaches through advanced tools. This involves Security Information Event Management Systems, AI-powered anomaly detection, and other advanced applications that empower them in real-time threat detection and response. On the other hand, less mature organizations depend on monitoring systems with ineffective capabilities, resulting in delayed detection and response to breaches. This inability to possess effective and automated life cycle management does not lead to enhanced security; instead, it showcases the organization's lack of detection and response capability towards breaches.

3. Lifecycle Management Insights

Lifespan Management for non-human identities is the first pillar of Machine Identity Security, as shown in Figure 3. Lifecycle management means managing each phase of a machine identity's lifecycle, ensuring there are no gaps that can be exploited [4]. The key stages are:

- Provisioning — The first step involves generating digital certificates, cryptographic keys, and secure credentials for non-human entities. Proper provisioning of the machine identities guarantees uniqueness and immunity to compromise. Recent research shows that organizations without automated provisioning typically leave gaps that result in misconfigurations and lag times, which could put sensitive systems at risk of exposure.

  Usage: Once activated, machine identities must be monitored continuously to ensure they function according to the defined parameters. Especially in environments like Cloud and AI, where identities can explode due to dynamic scaling, monitoring access patterns, permissions, and access trends are crucial for identity and access management.
- Renewal and Rotation: Regular renewal of certificates and cryptographic keys minimizes the risk of expired or compromised credentials. Cloud Security largely targets automated renewal processes, particularly focused on short-lived containers within Cloud-Native ecosystems.
- Decommissioning: Proper revocation and removal must occur at the end of the lifecycle for the machine's identity. The study emphasizes the importance of decommissioning identities to avoid exposure to abuse — especially when orphaned credentials are still active.

Table 1. Comparison of Non-Human identities

Aspect	Mature Organizations	Immature Organizations
Visibility	Centralized dashboards for real-time credential monitoring.	Manual, fragmented systems for tracking identities.
Lifecycle Management	Automated provisioning, renewal, and revocation processes.	Manual or delayed key rotations and certificate updates.
Access Policies	Strict adherence to the Principle of Least Privilege (PoLP).	Overprivileged accounts with excessive permissions.
Response to Threats	AI-based anomaly detection to flag unusual credential activity.	Reactive measures after a breach occurs.

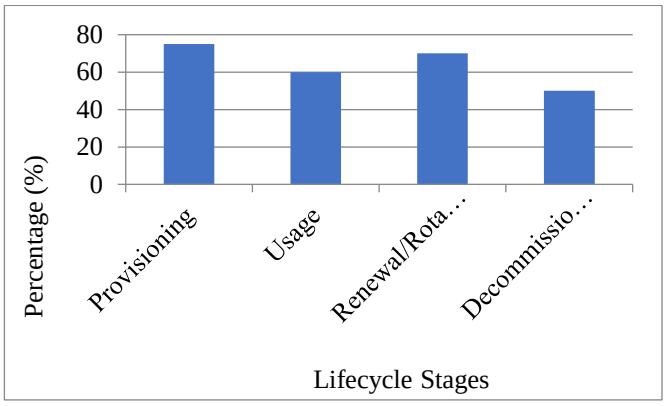

Fig. 3 Prioritization of lifecycle management stages

3.1. Automation and Tooling

The future of Lifecycle Management is Automation and Tooling. These consist of:

- Certificate Management Platforms: It automates provisioning, rotation, and revocation, which eases the burden on IT teams.
- Secret Vaults: Sensitive machine credentials are kept in a single secure location.
- Public Key Infrastructure (PKI): Manages encryption keys and certificates critical for Integration with DevOps pipelines to automate the process of "in-pod" certs for ephemeral workloads such as containers or microservices. By automating these tasks, security gets even stronger while human error — a critical source of vulnerabilities — is reduced [5].

Figure 4 indicates the impact of an automated life cycle in breach reduction.

Automation Concerns

- Using certificate management and key rotation for automation can cause concerns due to misconfigurations, enhancing the risk of unauthorized access.
- Integration of different tools for better automation though offers better automation but increases the complexity and scalability concerns and results in regularities in policy enforcement.
- The incorporation of automated processes requires constant monitoring mechanisms to detect anomalies. Failure to do so can result in vulnerabilities that cyber attackers can exploit.

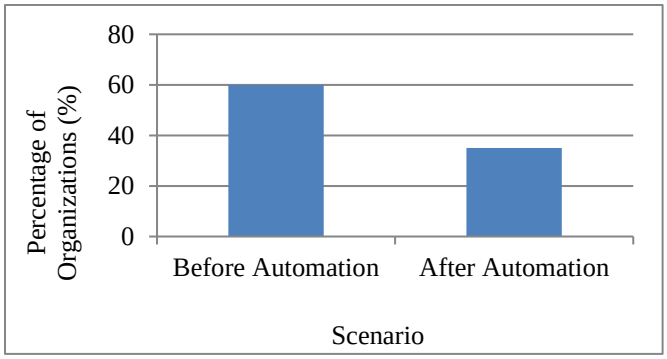

Fig. 4 Reduction in Breaches with Automated Lifecycle Management

4. Ownership and Accountability Factors

Ownership refers to the possession and responsibility of managing the security of an individual or organization, so it is essential to be established and maintained to ensure accountability in the task of securing machine identities in the concept of Machine Identity Security. Each machine identity — whether it's an API, an IoT device, or a service account — must have a clearly defined owner who is responsible for those credentials and their lifecycle. As mentioned in the source [6], ownership means linking the management of certain machine identities to a principal (a team, say the DevOps, the IT, or the security team, etc.)

4.1. Clear Ownership Ensures

- Governance: Owners must also enforce policies about the provisioning, usage, and decommissioning of machine identities, as shown in Figure 5.
- Accountability: If any breach occurs, the misuse can be traced back to a particular owner or entity.
- Compliance: Regulations such as GDPR and HIPAA require organizations to specify and enforce ownership of identities that can access sensitive systems or data.

4.2. Ownership Frameworks

- Categorization of every machine identity with some kind of registry describing its purpose and its owner(s).
- Procedures for reassigning ownership as roles or systems change.
- For compliance and accountability, periodic audits.

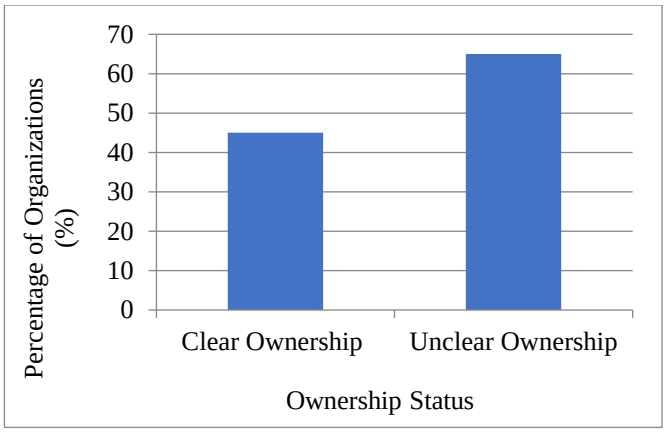

Fig. 5 Clarity of ownership in machine identity security

4.3. Governance Models and Organizational Alignment

The study calls to adopt a cross-domain governance model that aligns machine identity management processes with organizational goals. Governance models should:

- Assign roles to each team: The DevOps teams might be responsible for provisioning, whereas security teams focus on monitoring and auditing.
- Create policies that enable collaboration: Existing security measures — including key rotation and certificate revocation — should fit naturally into the DevOps workflows.
- Implement governance tools: Identity lifecycles can be tracked, access controls can be enforced, and behavior can be monitored on centralized platforms.

Aside from this, buy-in would also need to come from the leadership to get the resources needed to adopt machine identity security as a part of an organization's larger strategy, like Cloud and AI solutions or migrating to a Zero Trust architecture [7]. Figure 6 showcases the governance maturity levels in machine identity management. Rigorous auditing and reporting systems must be in place to hold organizations accountable. The source of research states that auditing monitors and records the usage, behavior, and lifecycle activities of machine identities. This data is critical for:

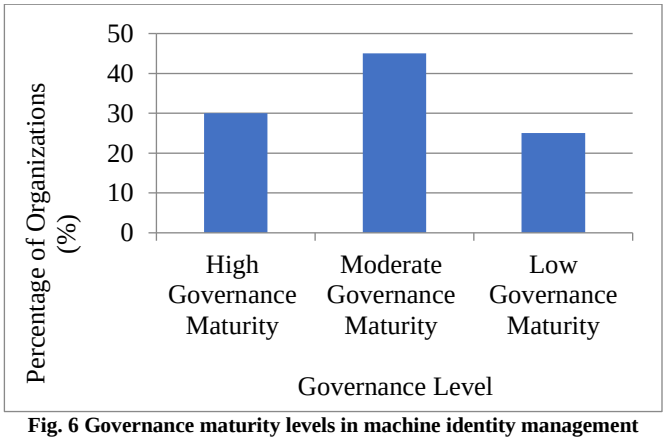

Fig. 6 Governance maturity levels in machine identity management

- Forensics: Tracing actions back to specific identities to identify the root cause of a breach.
- Compliance: Showing compliance with regulatory frameworks like PCI DSS, which require audit trails for all identities accessing sensitive data.
- Optimization: Identifying credentials that are either duplicate or orphaned, which could pose security risks.

Reporting dashboards with real-time data, combined with automated alerts, can also provide increased visibility into concerns, allowing security teams to be alerted immediately about anomalies, like the use of an unauthorized key or access by an expired certificate [8].

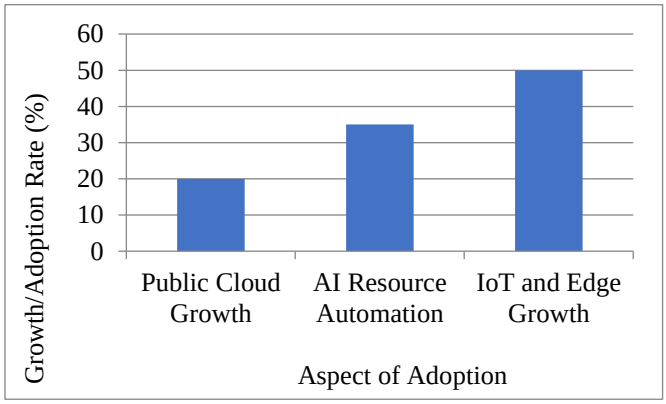

Fig. 7 Adoption Trends in Cloud & AI Ecosystems

5. Cloud and AI Trends and Statistics

Machine Identity Security is the key to managing the explosion of Cloud and AI adoption. The latest trends show the expansion of cloud spaces and integrations into AI-based platforms using machine-to-machine communication, which is increasing exponentially. This growth is huge, especially as organizations migrate to multi-cloud and hybrid infrastructures, dramatically increasing machine identities — which can represent anything from APIs to IoT devices to microservices. The data shows that over 70% of enterprises use multi-cloud strategies today, introducing unique security challenges that require scalable identity governance [9].

5.1. Emerging Technologies in Cloud and AI

Machine Identity Security is being driven by several emerging technologies [10], as shown in Figure 7.

- Fog Computing (FC) has emerged as an intermediary layer between edge devices and centralized clouds. Its processing of data closer to its source reduces latency. In FC environments, the dynamic allocation of resources requires rapid key rotations and machine identities.
- AI-Powered Threat Detection: AI is used to proactively detect normal machine identity behavior and help prevent attacks. Deep learning and similar techniques improve the detection of compromised or outdated certificates.
- Another major driver is the growth of IoT devices, which

are expected to reach 25 billion by 2030. Each IoT device requires a secure identity, emphasizing the need for large-scale identity automation.

5.2. Industry Research and Benchmarks

Benchmarks show that three key data points on Cloud and AI security are:

- Organizations using automated identity governance frameworks have a 50% lower risk of breaches tied to expired or orphaned certificates.
- AI that monitors and manages machine identities lowers incident response time by 30-40% compared to manual systems.
- Case studies reveal that investing in Zero Trust Architectures results in a 50% better cloud security posture for companies.

These findings underscore the importance of deploying AI-powered solutions and establishing strong lifecycle management policies to minimize risks related to machine identities [11].

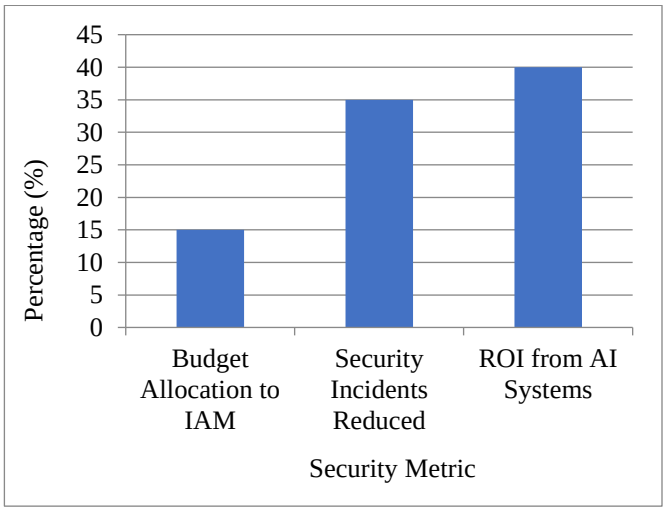

Fig. 8 Security Investments and ROI in Cloud & AI

5.2.1. The Bottom Line on Security Budget and ROI

Machine Identity Security reduces breach costs and improves operational efficiency, paying for itself. On average:

- Organizations lose $5 million annually due to breaches related to machine identity failures, making a strong case for proactive governance.
- Automating identity lifecycle processes can reduce operational expenses by up to 30%, especially in environments like Cloud and AI platforms, where dynamic scaling leads to higher costs.

As the importance of automated certificate management and AI-based anomaly detection grows, as depicted in Figure 8, so does the budget allocation for these tools [12].

6. Threat Landscape in Cloud and AI

Supporting Non-Human Identities for Machine Identity Security in Cloud and AI systems is especially challenging as attackers pivot to target these identities. These identities — including APIs, service accounts, and IoT devices — are critical as they enable smooth machine-to-machine interaction but often go relatively unguarded [13]. These identities can be attacked in different way ways:

- Credential Theft: Attackers misuse poorly managed machine credentials like certificates or API keys for unauthorized access [14].
- Password Spraying: Using weak passwords for service accounts makes them susceptible to brute force-based schemes or password spraying attacks [15].
- Cloud Services: In cloud environments, the lack of uniform security policies often leads to sensitive data being leaked through poorly configured credentials.
- API Token Hijacking: Attackers take advantage of weak storage of tokens to capture the API tokens, impersonate identities and access the systems. The reason behind such attacks is that tokens are transferred without proper encryption or are not stored securely.
- Man in the Middle (MITM) attack on M2M communication: The attacker captures the transmission among the non-human identities, modifies the data and steals sensitive information. Scenarios where certificates aren't validated accurately contribute towards this attack [16].
- Impersonation of Identity through Compromised Certificates: Intruders leverage the certificates, which are expired or compromised, to impersonate a valid machine identity and gain unauthorized access to cloud services [17].
- Lateral Movement and Privilege Escalation: Upon compromise of machine identity, attackers can utilize it to move laterally in the network, rapidly increasing the privilege to gain access to resources [18].

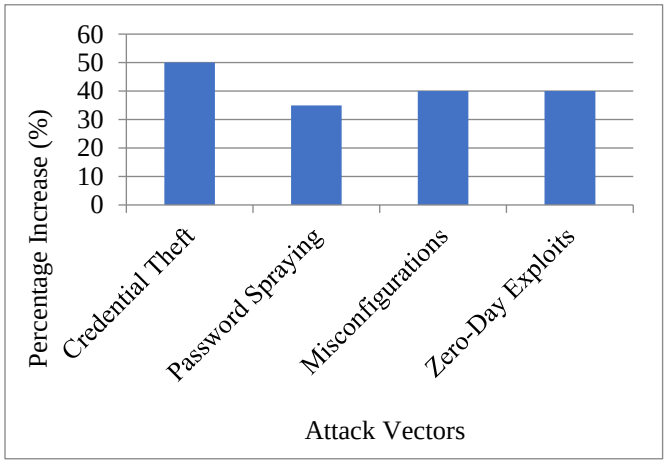

Fig. 9 Rise in Attack Vectors on Machine Identities

6.1. Regulatory Compliance and Governance

Machine Identity Security: Other Compliance Requirements. Regulatory frameworks such as GDPR, HIPAA, and PCI DSS require the following:

- Traceability: Each non-human identity must be audit-capable, with a well-defined trail of access and actions.
- Encryption in Transit & At Rest: Sensitive data transferred using machine identities needs to be encrypted.
- Governance Frameworks: Organizations must retain ownership of and responsibility for machine credentials.

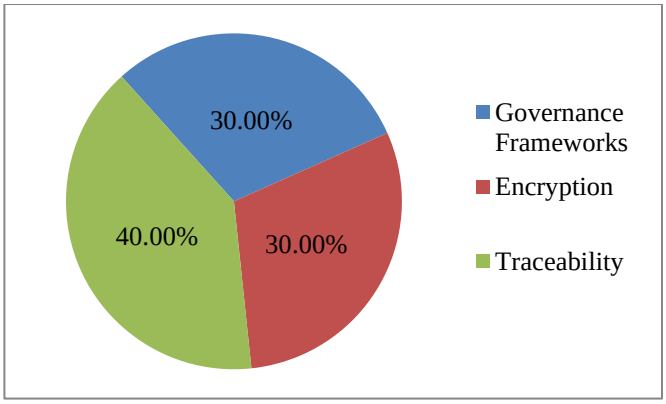

Fig. 10 Non-Compliance Penalty Distribution Across Frameworks

Failure to comply can lead to harsh monetary sanctions, as shown in Figure 10. For instance, poor management of IoT credentials in a healthcare application resulted in a GDPR violation with €500,000 in fines. High stakes [19].

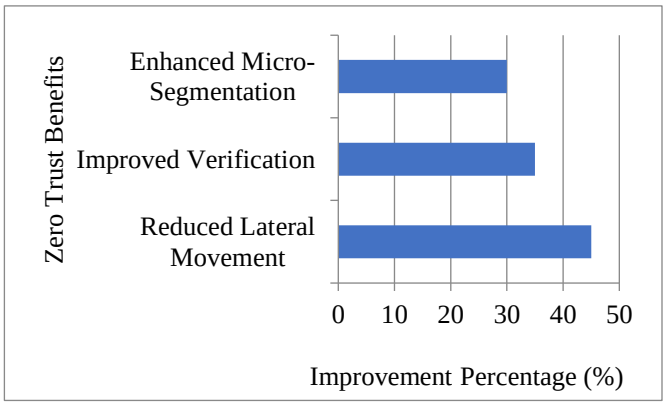

Fig. 11 Impact of Zero Trust on Machine Identity Security

6.2. Zero Trust and Continuous Verification

There is a critical need to adopt Zero Trust Architectures to counter machine identity threats. Key concepts of Zero Trust are:

1. Least Privilege Access: Issuing each identity only the permissions necessary to perform its assigned functions.
2. Continuous Validation: Machine credentials need to be checked and verified at every interaction within the system, whether internal or external communication.
3. Micro-Segmentation: The process of dividing networks into smaller zones. Integrating AI-powered anomaly detection into Zero Trust models enables the real-time detection of problematic actions involving machine credentials, according to research.

AI-powered tools help reduce the false-positive rate by 35%, allowing for a quicker response to real threats.

7. Implementation and Best Practices

This journey of Machine Identity Security is a critical one and requires a methodical approach with a tailored roadmap for effective and flexible implementation, considering the complexities of dynamic Cloud and AI environments. The roadmap consists of four key steps:

1. Evaluate Where We Are in the Moment: Start with a full inventory of every machine identity your organization holds — from certificates and keys to API tokens. Unfortunately, research shows that many organizations lack a comprehensive view of all their machine identities, leaving unmanaged or orphaned credentials that pose significant security risks.
2. Integrating and Automating Various Tools: AI methods in automation are used for dynamic monitoring and adaptive security policy to avoid misconfiguration of certificates and key rotation. Automation tools like Certificate Management Platforms (CMPs) and Cloud Security Posture Management (CSPM) can be used to streamline identity lifecycle management. These tools help minimize human errors and ensure compliance with regulations like GDPR and HIPAA. Standardizing the APIs for seamless integration among diverse cloud platforms improves interoperability and scalability in automation.
3. Ongoing Monitoring and Threat Discovery: Leverage AI-driven tools to monitor machine identities for suspicious activity. AI enhances real-time detection of anomalies, such as unauthorized certificate usage, as highlighted in CSPM implementations.

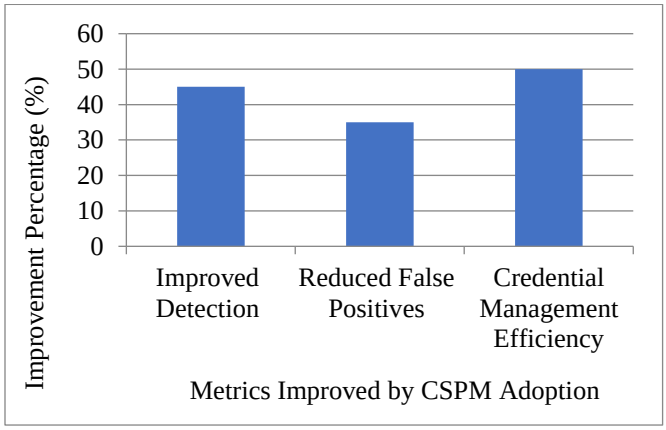

Fig. 12 Impact of CSPM Adoption on Security Metrics

4. Training and Policy Improvement: Update governance policies to enforce the Principle of Least Privilege (PoLP) and provide regular training for DevOps and security teams on best practices for managing machine identities.

7.1. Developing a Robust Lifecycle Management Program

A strong Lifecycle Management program is at the heart of protecting machine identities in Cloud and AI environments. The program should cover the following :

7.1.1. Provisioning

Use expiration and other standardized mechanisms to automate the creation of credentials to avoid permanent vulnerabilities.

7.1.2. Rotation

Mandate key and certificate rotations in fixed intervals to limit exposure.

7.1.3. Decommissioning

Ensure that unused or expired credentials are automatically revoked immediately.

As the research points out, without lifecycle automation to support it, 65% of organizations suffer from credential sprawl. Tools such as AWS Certificate Manager and HashiCorp Vault help critically automate these processes.

7.2. Ownership and Accountability Framework

Ownership binds every machine identity to an accountable entity. Organize DevOps, IT, and Security teams into respective roles around identity management:

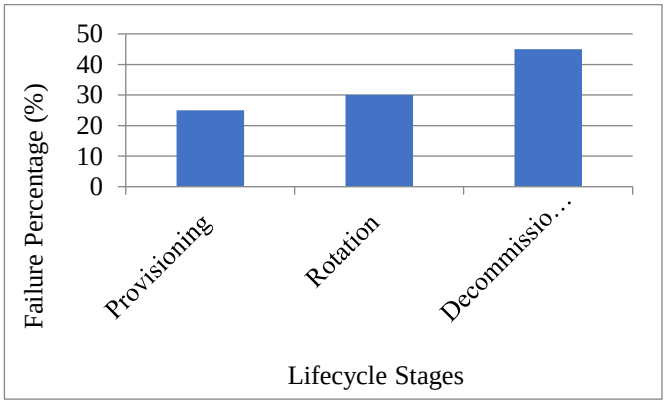

Fig. 13 Challenges in Machine Identity Lifecycle Stages

7.2.1. DevOps Teams

Manage provisioning and cloud- native integration, such as Kubernetes.

- Security Teams: Responsible for auditing, compliance, and anomaly detection.
- IT Teams: Handle policy enforcement and manage cross-team coordination.

The study also shown in Fig. 14 highlights that organizations with clearly defined ownership structures are 30% more effective at mitigating machine identity risk.

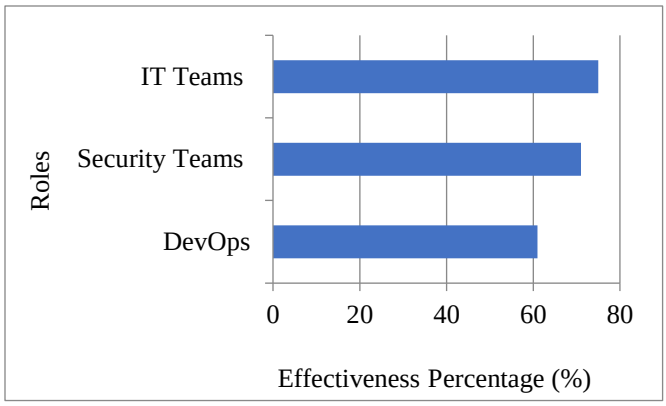

Fig. 14 Role Effectiveness in Machine Identity Management

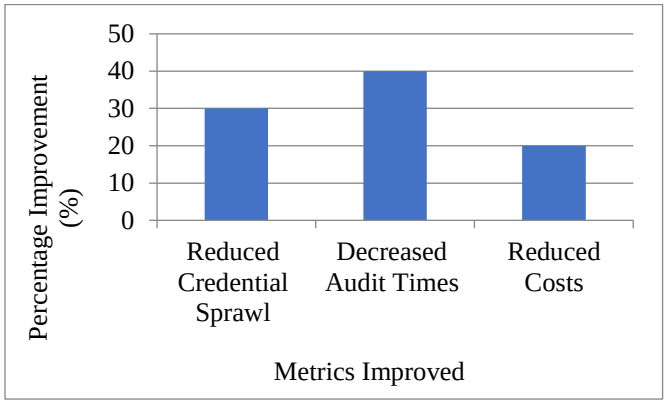

Fig. 15 Outcomes of Machine Identity Security in Financial Institutions

8. Practical Use Cases and Case Studies

A global financial institution implemented machine identity security to automate the lifecycle management of thousands of service accounts running in a cloud-native environment. This was done to address issues like credential sprawl and compliance risks. The institution deployed a Public Key Infrastructure (PKI) solution combined with a Certificate Management System (CMS) to handle the automated provisioning, renewal, and decommissioning of machine credentials [20].

Outcomes:

- Within the first year, credential sprawl was reduced by 30%.
- Compliance audit times dropped by 40%, thanks to detailed logs of machine identity usage being available for regulators.
- The organization achieved a 20% reduction in costs related to manual certificate management, as shown in Figure 15.

8.1. Case Study 2: AI-Driven Healthcare Platform

A healthcare platform leveraging the Cloud and AI adopted machine identity governance to secure its diagnostic AI systems. Given the strict regulations such as HIPAA, which require auditable access to patient data, the platform developed real-time monitoring tools to identify anomalies using API keys and certificates.

8.1.1. Challenges Addressed

- Misuse of API keys by internal applications.
- Lack of visibility into certificate expiration dates.

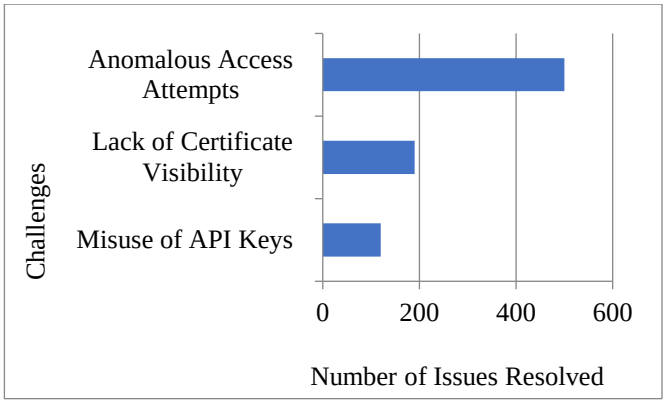

Fig. 16 Challenges Addressed By AI-Driven Healthcare Platform

8.1.2. Key Achievements

- Maintained continuous compliance with HIPAA by establishing encrypted communication channels.
- Detected and prevented over 500 unauthorized access attempts within the first six months, ensuring the integrity of patient data.

8.2. Case Study 3: Multi-Cloud DevOps Environment

A global technology company operating in a multi-cloud environment faced challenges managing ephemeral workloads created by DevOps pipelines. Because containers were short-lived, there was a need to dynamically provision and decommission certificates. To solve this, the company integrated its cloud orchestration tools with a centralized secrets management platform [21].

8.2.1. Strategies Employed

- Automated certificate issuance using a centralized certificate authority.
- Adopted a "just-in-time" provisioning model for service accounts.

8.2.2. Results

- The time to issue certificates dropped from 15 to just 2 minutes, as depicted in Figure 17.
- Better alignment with Zero Trust principles, helping to mitigate risks associated with over-privileged accounts.

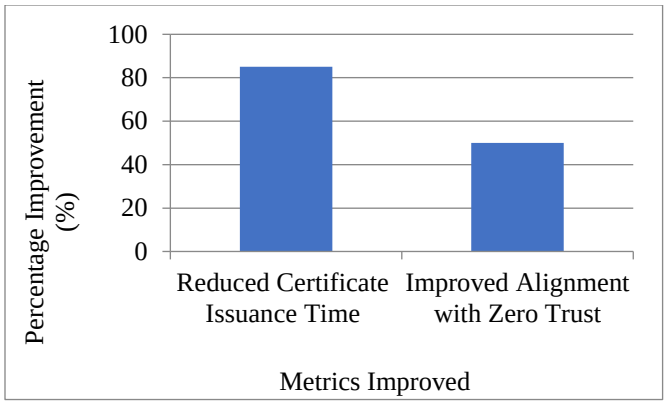

Fig. 17 Impact of Machine Identity Security in Multi-Cloud DevOps

9. Future Outlook in Cloud & AI

Cloud and AI technologies will have a significant influence on Machine Identity Security in the time ahead. Trends for the future include post-quantum cryptography, artificial intelligence-driven threat detection, and complete automated identity provisioning systems [22]. Key developments include, which are also depicted in Figure 19 are:

- After Quantum Cryptography: The Quantum computer revolution has led to traditional cryptographic techniques facing a growing threat. Methods such as lattice-based and hash-based algorithms are being created to protect against quantum attacks.
- Machine Identity-Aware AI: Machine identities are also a new focal point and attribute of AI systems that will become central in AI-driven automation. AI-driven tools can identify expired credentials or unusual behavior in Cloud Security environments before they impact security.
- Emerging Edge Computing: As IoT and edge computing proliferate, machine identities will struggle to accommodate decentralized systems with low latency requirements. This move will propel advancements in lightweight crypto solutions and secure provisioning of devices.

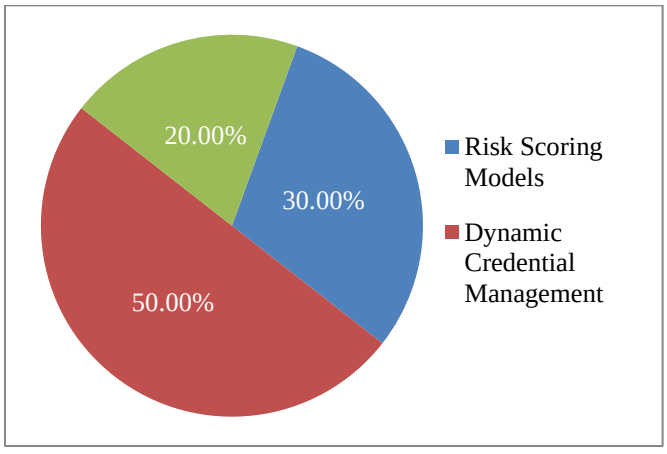

Fig. 18 AI's Potential impact on machine identity security

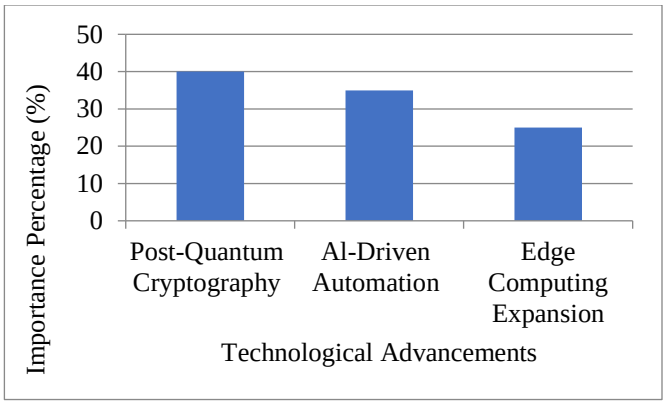

Fig. 19 Advancements Shaping Machine Identity Security

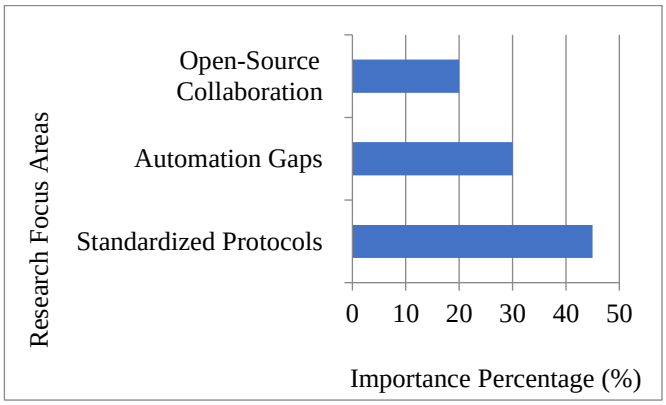

Fig. 20 Recommended Research Areas for Machine Identity Security

9.1. Potential Impact of AI Advances

Continuous, real-time validation of non-human identities is kind of like having continuous, real-time Machine Identity Security. Potential use cases include, as depicted in Figure 20 also:

1. Dynamic Credential Management: AI systems can dynamically generate and rotate credentials, minimizing the attack surface.
2. Risk Scoring Models: AI can provide dynamic risk scores to machine identities based on their behavior and actions within the system.
3. Self-Healing Systems: AI enables systems to isolate compromised identities, revoke accesses, and provision secure replacements independently, without an administrator being involved.

10. Conclusion

Some major aspects of Machine Identity Security were discussed and analyzed throughout this research work. Hands off the wheel – the rise of Non-Human Identities in Cloud and AI due to the rise of IoT, AI, and microservices has expanded the attack surface drastically. The sheer volume and ephemeral nature of machine identities are challenges that organizations now have to contend with. Securing machine identity governance relies on effective lifecycle management from provisioning to decommissioning. Automation of these processes minimizes errors, prevents credential sprawl, and ensures compliance. Establishing ownership of machine identities and implementing strong governance models can help organizations maintain accountability and compliance while minimizing the attack surface. Specialized technologies — including Certificate Management Systems (CMS), AI-powered threat detection, and Public Key Infrastructure (PKI) solutions — have emerged as tools of choice for most organizations looking to get ahead of evolving threats. The future of machine identity security will be shaped by post-quantum cryptography, edge computing security, and AI-based anomaly detection. Those who invest in these areas sooner than later will get a leg up on hardening their infrastructures.

Machine Identity Security is a dynamic area that will require continued investment in technology, governance, and research from an ever-growing number of stakeholders. Automated, owned, and compliant organizations will handle their infrastructures securely, thus establishing themselves as digital transformation leaders in a secure society. As cloud and AI expand, protecting non-human identities is not only a technical requirement but also a business must-have.

References

[1] Ali Bou Nassif et al., “Machine Learning for Cloud Security: A Systematic Review,” *IEEE Access*, vol. 9, pp. 20717-20739, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Jana Glöckler et al., “A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity,” *Business & Information Systems Engineering*, vol. 66, no. 4, pp. 421-440, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Varun Chandrasekaran et al., “SoK: Machine Learning Governance,” *arXiv*, pp. 1-19, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Alea Fairchild, and Piet Ribbers, *Privacy-Enhancing Identity Management in Business*, Digital Privacy, Springer, pp. 107-129, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[5] Simon Feulner et al., “Exploring the Use of Self-Sovereign Identity for Event Ticketing Systems,” *Electronic Markets*, vol. 32, pp. 1759-1777, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Ant Allan, “Hype Cycle for Identity and Access Management Technologies,” Gartner Information Technology, 2020. [Google Scholar] [Publisher Link]

[7] Audun Josang, and Simon Pope, "User-Centric Identity Management," *Proceedings of the AUSCERT Asia Pacific Information Technology Security Conference*, pp. 1-13, 2005. [Google Scholar]

[8] Kenneth Holstein et al., "Improving Fairness in Machine Learning Systems: What Do Industry Practitioners Need?," *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow Scotland Uk, pp. 1-16, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] Cynthia Dwork, and Aaron Roth, "The Algorithmic Foundations of Differential Privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211-407, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[10] Zulfiqar Ali Khan et al., "A Review on Task Scheduling Techniques in Cloud and Fog Computing: Taxonomy, Tools, Open Issues, Challenges, and Future Directions," *IEEE Access*, vol. 11, pp. 143417-143445, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Shreshth Tuli, Giuliano Casale, and Nicholas R. Jennings, "GOSH: Task Scheduling Using Deep Surrogate Models in Fog Computing Environments," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 11, pp. 2821-2833, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Steffen Schwalm, Daria Albrecht, and Ignacio Alamillo, "eIDAS 2.0: Challenges, Perspectives and Proposals to Avoid Contradictions between eIDAS 2.0 and SSI," Copenhagen, Denmark, *Open Identity Summit*, pp. 63-74, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Craig Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, Bethesda MD USA, pp. 169-178, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[14] Vaishali Singh, and S.K. Pandey, "Revisiting Cloud Security Attacks: Credential Attack," *Proceedings of FICR-TEAS 2020: Rising Threats in Expert Applications and Solutions: Proceedings of FICR-TEAS 2020*, Jaipur, Rajasthan, India, pp. 339-350, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Yassine Maleh, *Enhancing E-Learning Security in Cloud Environments: Risk Assessment and Penetration Testing*, Cybersecurity Management in Education Technologies, 1st ed., CRC Press, pp. 1-40, 2023. [Google Scholar] [Publisher Link]

[16] A. Sabitha Banu, and G. Padmavathi, "A Survey of Computational Intelligence Methods Used in Handling Man in the Middle Attacks in Machine to Machine Communications," *International Journal of Engineering Research and Technology*, vol. 8, no. 8, pp. 218-226, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[17] Umme Habiba et al., "Cloud Identity Management Security Issues & Solutions: A Taxonomy," *Complex Adaptive Systems Modeling*, vol. 2, pp. 1-37, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[18] Kokthay Poeng, and Laurent Schumacher, "Lateral Movement Identification in Cross-Cloud Deployment," *2024 20th International Conference on Network and Service Management*, Prague, Czech Republic**,** pp. 1-4, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Keith Bonawitz et al., "Practical Secure Aggregation for Federated Learning on User-Held Data," *arXiv*, pp. 1-5, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[20] Jacob Devlin et al., "BERT: Pre-Training of Deep Bidirectional Transformers for Language Understanding," *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*, Minneapolis, Minnesota, vol. 1, pp. 4171-4186, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[21] Nicolas Papernot et al., "SoK: Security and Privacy in Machine Learning," *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, London, UK, pp. 399-414, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[22] Ayoobkhan Mohamed Uvaze Ahamed et al., "Deep Learning and Optimization-Based Task Scheduling Algorithms for Fog-Cloud Computing Environment," *Journal of Intelligent and Fuzzy Systems*, pp. 1-14, 2023. [Google Scholar] [Publisher Link]