
Governance And Protection Strategies For Non-Human Identities In Cloud IAM

Dr. Chinedu Okafor

Department of Computer Science, University of Lagos, Lagos, Nigeria

Prof. Amina Bello

Faculty of Engineering, University of Ibadan, Ibadan, Nigeria

Published Date: - 02 May 2026, Page No.: - 01-11

KEYWORDS

Non-Human Identities, Cloud IAM, Identity Governance, Machine Identity Security, Least Privilege, Cloud Security, API Security, Zero Trust, Distributed Systems, Governance Frameworks

ABSTRACT

The rapid expansion of cloud computing ecosystems has significantly transformed identity and access management (IAM) paradigms, extending beyond human users to include non-human identities (NHIs) such as APIs, microservices, workloads, service accounts, and automated agents. These identities now dominate enterprise cloud environments and represent a critical but often under-governed attack surface. This paper investigates governance frameworks and protection strategies for NHIs in Cloud IAM, emphasizing policy enforcement, least-privilege mechanisms, lifecycle management, and cross-system interoperability.

Drawing upon interdisciplinary literature in governance models, disability studies frameworks of inclusion, collaborative systems theory, and digital policy regulation, the study develops a conceptual synthesis for securing NHIs through adaptive governance structures. The analysis highlights fragmentation in existing IAM practices, lack of lifecycle visibility for machine identities, and limited auditing mechanisms as key vulnerabilities.

The findings propose a multi-layer governance model integrating continuous identity verification, automated policy orchestration, and collaborative security accountability inspired by pentahelix and network governance frameworks. The study contributes to cloud security literature by redefining identity governance boundaries and introducing structured protection strategies for non-human actors in distributed cloud infrastructures.

1. INTRODUCTION

The evolution of cloud-native architectures has fundamentally reshaped identity ecosystems. Traditional Identity and Access Management (IAM) systems were designed primarily for human users; however, modern distributed systems rely heavily on non-human identities (NHIs), including service accounts, application programming interfaces (APIs), containers, orchestration agents, and automated workloads. These NHIs often outnumber

human identities by orders of magnitude, yet they remain less governed and poorly audited.

From a governance perspective, NHIs introduce complex challenges because they operate autonomously, interact across multiple services, and frequently require dynamic privilege adjustments. Unlike human users, their authentication patterns are continuous, system-driven, and often embedded

within infrastructure code. This creates a governance gap in accountability, lifecycle tracking, and anomaly detection.

The relevance of this research is further amplified by increasing incidents of credential misuse, token leakage, and privilege escalation attacks targeting machine identities in cloud ecosystems. Governance frameworks must therefore evolve toward automated, scalable, and context-aware models that can handle identity proliferation without compromising security or performance.

The objective of this paper is to develop a structured governance and protection strategy framework for NHIs in Cloud IAM environments. It aims to (i) analyze existing theoretical foundations of governance models, (ii) identify gaps in current IAM systems, and (iii) propose a multi-layered protection architecture informed by collaborative governance and security literature.

The scope of this research is limited to cloud-based IAM environments, focusing on machine identities rather than human users. The study draws from interdisciplinary literature, including organizational governance, digital collaboration frameworks, and inclusion-based system design principles, to construct a holistic analytical perspective.

2. LITERATURE REVIEW

2.1 Governance and Collaborative Frameworks in Digital Systems

Governance in distributed systems has been widely studied in relation to collaboration, coordination, and cooperation mechanisms among organizational actors. Castañer and Oliveira (2020) emphasize that these three constructs, while often used interchangeably, represent distinct operational mechanisms for achieving structured collaboration in complex environments. In Cloud IAM systems, similar distinctions apply when managing interactions between human administrators, automated agents, and non-human identities.

Lopes and Farias (2022) further argue that governance mechanisms in public sector innovation require structured coordination frameworks to ensure accountability and adaptability. These insights are directly applicable to cloud IAM governance, where identity interactions span multiple autonomous systems.

Wang and Ran (2023) extend this perspective by analyzing network governance and collaborative governance as intertwined constructs, highlighting their relevance in managing distributed and interdependent systems. This theoretical foundation is critical for understanding how NHIs should be governed across multi-cloud infrastructures.

2.2 Identity, Inclusion, and Systemic Access Models

Although primarily grounded in social systems, disability and inclusion literature provides important analogies for identity governance systems. Haug (2017) and Simplican et al. (2015) conceptualize inclusion as a structured interaction between individuals and systems, emphasizing accessibility, participation, and contextual adaptation. These principles can be metaphorically extended to NHIs, which require structured “access inclusion” within cloud environments.

Banas et al. (2019) highlight methodological challenges in engaging complex and underrepresented subjects within research systems, particularly regarding recruitment and retention barriers. Similarly, NHIs in IAM systems suffer from “visibility barriers,” where lifecycle tracking and identity persistence are insufficiently managed, leading to governance blind spots. This analogy supports the need for structured lifecycle visibility mechanisms for machine identities.

Burke and Barnes (2018) discuss layered policy systems and governance fragmentation, which parallels the kludge-like architecture of modern IAM systems where machine identities are managed through overlapping tools without unified oversight.

2.3 Pentahelix and Multi-Stakeholder Governance Models

The pentahelix model has emerged as a key framework in collaborative governance literature. Halibas et al. (2017), Subagyo (2021), and Sudiana et al. (2020) demonstrate how multi-actor collaboration improves innovation and governance outcomes. These frameworks typically involve government, academia, business, community, and media actors.

In cloud IAM ecosystems, NHIs can be conceptualized as autonomous “actors” requiring governance integration similar to pentahelix collaboration structures. Maturbongs and Lekatompessy (2020) further highlight that collaborative governance enhances system adaptability in dynamic environments, reinforcing the need for adaptive IAM policies.

2.4 Identity Management and Security Foundations

Cloud identity governance relies heavily on least-privilege principles, continuous authentication, and role-based access control systems. However, existing literature indicates that NHIs are often excluded from strict enforcement mechanisms due to operational complexity and scalability constraints.

Bartley (2022) discusses transnational regulatory systems and highlights the importance of structured enforcement mechanisms in decentralized environments. This is relevant for IAM systems where NHIs operate across distributed cloud infrastructures.

Kim and Zhu (2020) emphasize the role of digital applications in improving inclusion and access control, suggesting that technological mediation can enhance structured participation—an idea transferable to automated identity governance.

2.5 Research Gap Identification

Despite extensive research in governance systems,

collaborative frameworks, and identity management, there remains a significant gap in addressing NHIs as first-class citizens within IAM architectures. Existing systems primarily focus on human-centric access control, leaving machine identities under-governed, poorly audited, and vulnerable to exploitation.

Furthermore, there is limited integration between governance theory and technical IAM implementations, particularly in cloud-native environments where identities are ephemeral and dynamically generated. This gap necessitates a unified governance framework that integrates lifecycle management, policy orchestration, and continuous monitoring for NHIs.

3. Methodology

This study adopts a conceptual research methodology combined with systematic synthesis of existing literature to develop a governance framework for non-human identities (NHIs) in cloud Identity and Access Management (IAM) systems. The approach is qualitative, interpretive, and theory-building in nature, aimed at bridging gaps between IAM security engineering and governance theory.

3.1 Research Design

The research design follows a structured analytical framework built on three layers:

1. **Theoretical synthesis layer** – extraction of governance, collaboration, and identity-related principles from selected literature.
2. **Comparative abstraction layer** – mapping cross-domain concepts such as pentahelix governance, collaborative networks, and inclusion frameworks onto IAM systems.
3. **Framework construction layer** – formulation of a conceptual multi-layer governance model for NHIs.

The methodology aligns with qualitative data analysis principles, emphasizing coding, categorization, and thematic interpretation (Miles et al., 2014).

3.2 Conceptual Framework Development

The proposed governance model is structured around four key dimensions:

(a) Identity Lifecycle Governance

NHIs are treated as lifecycle-managed entities, including creation, activation, permission assignment, rotation, and decommissioning. This aligns with structured governance systems in collaborative organizational frameworks (Castañer & Oliveira, 2020).

(b) Policy-Oriented Access Control

Least-privilege enforcement is implemented dynamically using contextual policy evaluation. Inspired by regulatory governance models (Bartley, 2022), policies are continuously updated based on system behavior.

(c) Collaborative Security Architecture

Security governance is distributed across multiple stakeholders (cloud providers, developers, DevSecOps teams). This reflects pentahelix governance principles (Halibas et al., 2017; Sudiana et al., 2020).

(d) Continuous Monitoring and Adaptive Trust

NHIs are continuously monitored using anomaly detection, behavior tracking, and adaptive trust scoring systems.

3.3 Analytical Mapping Process

The study performs cross-domain mapping between:

- Human-centered inclusion models (Simplican et al., 2015)
- Governance coordination frameworks (Wang & Ran, 2023)
- IAM machine identity structures

This mapping helps conceptualize NHIs as dynamic agents requiring structured governance inclusion rather than static credential objects.

3.4 Example Application Scenario

A hypothetical multi-cloud enterprise system is analyzed where:

- Microservices generate temporary service accounts
- APIs interact across federated cloud environments
- CI/CD pipelines dynamically deploy workloads

Each NHI is assigned a lifecycle policy, monitored through centralized governance logs, and continuously validated through access behavior scoring.

3.5 Limitations of Methodology

- Purely conceptual, no empirical dataset used
- Lack of real-world cloud provider telemetry integration
- Assumes uniform policy enforcement capability across systems

Despite these limitations, the framework provides a scalable theoretical foundation for future empirical validation.

4. RESULTS

The synthesis of governance and IAM literature reveals several critical insights into the management of non-human identities (NHIs) in cloud environments.

4.1 Fragmentation of Identity Governance

A primary finding is the severe fragmentation of NHI governance across cloud ecosystems. Unlike human IAM, which is often centralized, machine identities are distributed across microservices, APIs, and automation pipelines. This leads to inconsistent policy enforcement and visibility gaps. Burke and Barnes (2018) similarly highlight that layered

governance structures often create inefficiencies and weak accountability, which is strongly reflected in cloud IAM systems.

4.2 Lifecycle Visibility Deficit

NHIs frequently lack structured lifecycle tracking. Many service accounts and API keys are created dynamically but are rarely decommissioned properly. This results in identity accumulation and increased attack surface. The absence of lifecycle governance mirrors methodological challenges described by Banas et al. (2019), where unmanaged participant retention leads to systemic oversight issues. In IAM systems, this translates into persistent orphaned identities.

4.3 Policy Enforcement Inconsistencies

The analysis identifies inconsistencies in least-privilege enforcement for NHIs. While policies exist, they are often static and fail to adapt to dynamic workload behavior. Bartley (2022) emphasizes that regulatory enforcement in decentralized systems requires adaptive structures, which are largely missing in current IAM implementations.

4.4 Need for Collaborative Governance Models

Findings strongly indicate that effective NHI governance requires multi-stakeholder collaboration. Insights from Halibas et al. (2017) and Subagyo (2021) suggest that distributed governance models such as pentahelix frameworks improve coordination and accountability. Applying this to IAM, security responsibility must be shared across DevOps teams, security engineers, and platform providers.

4.5 Emergence of Adaptive Identity Trust Models

A significant outcome of this synthesis is the conceptual need for adaptive trust scoring for NHIs. Instead of static authentication, identities should be continuously evaluated based on behavior, context, and interaction patterns. This aligns with broader

governance literature emphasizing dynamic network-based governance structures (Wang & Ran, 2023).

4.6 Security Exposure Risks

The study identifies key security risks:

- Credential leakage from unmanaged APIs
- Privilege escalation through over-permissioned service accounts
- Lack of auditability for ephemeral workloads
- Token reuse across distributed environments

These vulnerabilities collectively increase systemic exposure in cloud-native ecosystems.

5. DISCUSSION

The findings of this study reveal that governance and protection strategies for non-human identities (NHIs) in cloud IAM systems cannot be effectively understood through traditional human-centric security paradigms. Instead, NHIs must be conceptualized as autonomous, continuously active governance entities that require lifecycle-aware, policy-driven, and collaboratively managed control mechanisms. This shift fundamentally redefines identity security from a static authentication problem to a dynamic governance problem embedded within distributed cloud ecosystems.

A key theoretical implication of this research is the fragmentation of identity governance structures across modern cloud environments. As identified in the findings, NHIs are distributed across APIs, microservices, automation pipelines, and ephemeral workloads, resulting in fragmented visibility and inconsistent policy enforcement. This aligns with Burke and Barnes (2018), who argue that layered governance systems often produce “kludge-like” structures where overlapping policies reduce coherence and accountability. In cloud IAM systems, this fragmentation is amplified due to rapid scaling, automation, and cross-cloud interoperability requirements. Consequently, organizations face governance blind spots where machine identities exist without clear ownership, lifecycle tracking, or

auditability.

Another significant insight is the inadequacy of static access control mechanisms for NHIs. Traditional role-based access control (RBAC) and attribute-based access control (ABAC) models assume relatively stable identity attributes and predictable user behavior. However, NHIs operate under highly dynamic conditions, where identities are frequently created, modified, and destroyed within seconds. This makes static policies inherently insufficient. The study's findings support Bartley (2022), who emphasizes that regulatory systems in decentralized environments require adaptive enforcement mechanisms capable of responding to contextual changes. In IAM systems, this translates into the necessity for continuous authorization models, real-time risk scoring, and behavior-based access evaluation.

From a governance perspective, the integration of collaborative frameworks such as pentahelix models introduces an important conceptual advancement. Studies by Halibas et al. (2017), Sudiana et al. (2020), and Subagyo (2021) demonstrate that multi-stakeholder governance structures improve system resilience and innovation outcomes in complex ecosystems. Applying this to cloud IAM, NHIs can no longer be governed solely by centralized security teams. Instead, governance responsibility must be distributed across cloud providers, DevSecOps teams, application developers, and automated policy engines. This distributed governance structure enhances accountability but also introduces coordination complexity, requiring standardized policy languages, automated compliance enforcement, and unified identity observability layers.

The study also highlights a critical issue of lifecycle invisibility in NHIs. Unlike human identities, which are typically subject to onboarding and offboarding procedures, NHIs often lack structured lifecycle governance. Service accounts, API keys, and workload identities are frequently created dynamically and remain active beyond their intended

usage period. This leads to identity sprawl and significantly increases the attack surface. The analogy drawn from Banas et al. (2019), which discusses retention challenges in complex research populations, is particularly relevant here. Just as unmanaged participants introduce methodological noise in qualitative research, unmanaged NHIs introduce operational and security noise in IAM systems, reducing system clarity and increasing vulnerability exposure.

Furthermore, the study identifies the absence of unified trust evaluation mechanisms for NHIs as a major governance gap. Current IAM systems rely heavily on static authentication tokens and predefined access policies, which fail to account for behavioral anomalies or contextual risk factors. The proposed concept of adaptive trust scoring introduces a shift toward continuous identity validation, where NHIs are evaluated based on behavioral patterns, request frequency, interaction context, and anomaly detection signals. This aligns with Wang and Ran (2023), who emphasize that network governance systems must incorporate dynamic relationship evaluation mechanisms to remain effective in distributed environments.

Another important dimension is the security implication of credential proliferation and privilege accumulation. The findings suggest that NHIs often accumulate excessive permissions over time due to incomplete decommissioning processes and lack of periodic privilege review. This violates the principle of least privilege and introduces significant risk of lateral movement in the event of credential compromise. Burke and Barnes (2018) provide a relevant theoretical lens, highlighting how layered policy environments often result in unintended privilege retention due to structural complexity. In cloud IAM systems, this manifests as over-permissioned service accounts that remain active indefinitely, becoming high-value targets for attackers.

The study also reveals that automation, while essential for scalability, paradoxically increases

governance complexity. Automated CI/CD pipelines, infrastructure-as-code deployments, and dynamic orchestration systems generate NHIs at a rate that exceeds human governance capacity. While automation improves efficiency, it simultaneously reduces visibility and increases dependency on machine-driven governance decisions. This creates a paradox where systems designed to enhance control also expand the attack surface if not properly governed.

In terms of practical implications, organizations must transition from reactive identity management to proactive identity governance. This involves implementing continuous monitoring systems, centralized identity observability platforms, and automated lifecycle enforcement mechanisms. Additionally, IAM systems must incorporate policy-as-code frameworks that allow governance rules to be embedded directly into deployment pipelines. Such integration ensures that NHIs are governed at the point of creation rather than post-deployment.

However, the proposed governance model is not without limitations. First, the complexity of implementing adaptive trust systems may introduce performance overhead and false-positive risks, particularly in high-throughput environments. Second, distributed governance models require strong coordination mechanisms, which may be difficult to enforce across organizational boundaries. Third, the lack of standardized definitions for NHIs across cloud providers creates interoperability challenges, limiting the scalability of unified governance frameworks.

Despite these challenges, the study establishes that the evolution of cloud IAM systems must necessarily include a paradigm shift toward treating NHIs as first-class governed entities. Without such a shift, organizations will continue to face escalating security risks driven by identity sprawl, privilege mismanagement, and fragmented governance structures.

6. CONCLUSION

This research critically examined governance and protection strategies for non-human identities (NHIs) in cloud Identity and Access Management (IAM) systems, with the objective of addressing a rapidly growing but under-governed dimension of modern cloud security. The study demonstrates that NHIs—comprising APIs, service accounts, microservices, workloads, and automated agents—have become the dominant identity type in cloud ecosystems, yet remain governed by fragmented, human-centric IAM paradigms that are no longer sufficient for contemporary distributed architectures.

A central conclusion of this work is that NHIs must be formally recognized as first-class governance entities within IAM frameworks. Traditional IAM systems were designed around static human roles, predictable authentication patterns, and centralized administrative control. However, NHIs operate in fundamentally different conditions: they are ephemeral, high-frequency, machine-driven, and often autonomous. This structural mismatch between IAM design assumptions and cloud operational realities creates systemic vulnerabilities that cannot be resolved through incremental improvements alone. Instead, a paradigm shift toward lifecycle-aware, policy-driven, and continuously monitored identity governance is required.

The study further concludes that identity fragmentation remains one of the most critical challenges in cloud security. As demonstrated through synthesis of governance literature (Wang & Ran, 2023; Castañer & Oliveira, 2020), distributed systems inherently produce overlapping responsibilities and inconsistent enforcement unless explicitly coordinated. In the context of NHIs, this fragmentation manifests as scattered service accounts, unmanaged API keys, and poorly tracked workload identities across multiple environments. These conditions significantly weaken auditability and increase exposure to credential-based attacks.

Another key conclusion is that static access control mechanisms are fundamentally insufficient for managing NHIs. Role-based and attribute-based

access models assume stability in identity behavior, which does not align with the dynamic nature of cloud-native workloads. Instead, IAM systems must evolve toward adaptive and continuous authorization models that evaluate identity behavior in real time. This includes integrating contextual risk scoring, anomaly detection, and automated policy adjustments. Such adaptive mechanisms align with broader governance theory that emphasizes responsiveness in decentralized systems (Bartley, 2022).

The research also concludes that lifecycle governance is a foundational requirement for securing NHIs. Unlike human identities, machine identities are frequently created automatically and often persist indefinitely without structured decommissioning. This leads to identity accumulation, also referred to as “identity sprawl,” which significantly increases attack surfaces. The absence of structured lifecycle enforcement—covering creation, rotation, validation, and deletion—represents one of the most critical gaps in current IAM implementations. Without lifecycle governance, even advanced authentication mechanisms fail to provide comprehensive security coverage.

In addition, the study highlights that collaborative governance models, such as the pentahelix framework, provide a useful conceptual foundation for distributing responsibility across multiple actors in cloud ecosystems. As supported by Halibas et al. (2017), Sudiana et al. (2020), and Subagyo (2021), multi-stakeholder governance enhances resilience in complex systems by distributing accountability and enabling coordinated action. In IAM environments, this translates into shared responsibility among cloud providers, developers, DevSecOps teams, and automated policy systems. However, the study concludes that such collaboration must be supported by automation and standardized governance protocols to prevent coordination breakdown.

A further conclusion is the necessity of implementing continuous trust evaluation mechanisms for NHIs.

Static authentication methods are insufficient in environments where identities execute millions of transactions across distributed systems. Instead, identity trust must be dynamic, continuously recalculated based on behavior patterns, contextual signals, and historical activity. This represents a shift from identity verification to identity observation, where trust is not granted once but continuously maintained and validated throughout the identity lifecycle.

The study also concludes that automation, while essential for scalability in cloud environments, introduces new governance risks if not properly controlled. Automated CI/CD pipelines and infrastructure-as-code systems generate large volumes of NHIs at machine speed, often exceeding human oversight capacity. This creates governance blind spots where identities are created faster than they can be audited or decommissioned. Therefore, automation must be paired with embedded governance controls, ensuring that identity policies are enforced at the point of creation.

From a security standpoint, the research concludes that NHIs represent one of the most significant and rapidly expanding attack surfaces in cloud ecosystems. Risks such as credential leakage, privilege escalation, token reuse, and orphaned identities are amplified by poor lifecycle governance and inconsistent policy enforcement. Without targeted governance strategies, these vulnerabilities can compromise entire cloud infrastructures due to the interconnected nature of distributed systems.

Despite these challenges, the study contributes a structured conceptual framework that integrates governance theory, collaborative systems thinking, and identity security principles into a unified approach for managing NHIs. This framework provides a foundation for future research and practical implementation, particularly in the development of automated IAM systems capable of handling identity complexity at scale.

However, the study acknowledges limitations. The

framework remains conceptual and requires empirical validation through real-world cloud deployments. Additionally, variations in IAM implementations across cloud service providers may impact the generalizability of the proposed model. Future research should therefore focus on experimental validation, simulation-based testing, and integration with commercial IAM platforms.

In conclusion, the governance of non-human identities represents a critical frontier in cloud security. As cloud ecosystems continue to evolve toward full automation and microservice-based architectures, NHIs will increasingly dominate identity landscapes. Addressing their governance requires a fundamental shift from static, human-centric IAM models toward adaptive, lifecycle-driven, and collaboratively governed identity ecosystems. This research establishes a theoretical and structural foundation for that transition and highlights the urgent need for continued innovation in this domain.

7. REFERENCES

1. Albers, S., Wohlgezogen, F., & Zajac, E. J. (2016). Strategic Alliance Structures. *Journal of Management*, 42(3), 582–614.
2. Abdul Salam Abdul Karim. (2023). Fault-Tolerant Dual-Core Lockstep Architecture for Automotive Zonal Controllers Using NXP S32G Processors. *International Journal of Intelligent Systems and Applications in Engineering*, 11(11s), 877–885. Retrieved from <https://ijisae.org/index.php/IJISAE/article/view/7749>
3. Allifya, S. A. N., Aknuranda, I., & Amiruddin, L. (2022). Designing an Accessibility Portal for a Higher Education Institution. *IJDS Indonesian Journal of Disability Studies*, 9(02), 203–216.
4. Anderson, E. T., & McFarlane, J. (2019). Community as Partner Theory and Practice in 30 Volume 5 Issue 1 April 2024 Nursing 4th Ed. Wolters Kluwer.
5. Banas, J. R., Magasi, S., The, K., & Victorson, D. E. (2019). Recruiting and Retaining People with Disabilities for Qualitative Health Research: Challenges and Solutions. *Qualitative Health Research*, 29(7), 1056–1064.
6. Bartley, T. (2022). Power and the Practice of Transnational Private Regulation. *New Political Economy*, 27(2), 188–202.
7. Burke, T. F., & Barnes, J. (2018). Layering, kludgeocracy and disability rights: The limited influence of the social model in American disability policy. *Social Policy and Society*, 17(1), 101–116.
8. Canton, E., Hedley, D., & Spoor, J. R. (2023). The stereotype content model and disabilities. *The Journal of Social Psychology*, 163(4), 480–500.
9. Carolina, I. R. & I. M. D. N., USA, & Tiwari, S. K. (2025). Automating Behavior-Driven Development with Generative AI: Enhancing Efficiency in Test Automation. *Frontiers in Emerging Computer Science and Information Technology*, 02(12), 01–14. <https://doi.org/10.64917/fecsit/volume02issue12-01>
10. Castañer, X., & Oliveira, N. (2020). Collaboration, Coordination, and Cooperation Among Organizations: Establishing the Distinctive Meanings of These Terms Through a Systematic Literature Review. *Journal of Management*, 46(6), 965–1001.
11. Chamidah, N., Putra, A. H. P. K., Mansur, D. M., & Guntoro, B. (2021). Pentahelix element synergy as an effort to develop villages tourism in Indonesia. *Jurnal Manajemen Bisnis*, 8(1), 01–22.
12. Cheyne, R. (2019). *Disability, Literature, Genre*. Liverpool University Press.
13. Demartoto, A. (2005). *Menyibak Sensivitas Gender dalam Keluarga Difabel*. UNS Press.
14. F. Antonak, R., & Livneh, H. (2000). Measurement of attitudes towards persons with disabilities. *Disability and Rehabilitation*, 22(5), 211–224.
15. Fakhri, M. (1999). *Analisis Gender dan Transformasi Sosial*. Pustaka Pelajar.

16. Garcia, O., & Cater, C. (2022). Life below water; challenges for tourism partnerships in achieving ocean literacy. *Journal of Sustainable Tourism*, 30(10), 2428–2447.
17. Halibas, A., Sibayan, R. O., & Maata, R. L. R. (2017). The Pentahelix model of innovation in Oman: an HEI perspective. *Interdisciplinary Journal of Information*, 12(1), 159–172.
18. Hammad, I. (2004). *Konstruksi Realitas Politik dalam Media Massa*. Granit.
19. Haug, P. (2017). Understanding inclusive education: ideals and reality. *Scandinavian Journal of Disability Research*, 19(3), 206–217.
20. Huang, J., Cook, G. G., & Xie, Y. (2021). Large-scale quantitative evidence of media impact on public opinion toward China. *Humanities and Social Sciences Communications*, 8(1), 181.
21. ILO. (2018). *Mempromosikan Hak dan Kesempatan bagi Penyandang Disabilitas di Indonesia*. ILO.
22. Indriyany, I. A. (2015). Pelayanan Publik dan Pemenuhan Hak Difabel. *INKLUSI*, 2(1), 1–20.
23. Jabeen, F., Belas, J., Santoro, G., & Alam, G. M. (2023). The role of open innovation in fostering SMEs' business model innovation. *Journal of Knowledge Management*, 27(6), 1562–1582.
24. Kim, H. C., & Zhu, Z. Y. (2020). Improving social inclusion for people with physical disabilities. *International Journal of Environmental Research and Public Health*, 17(7).
25. Kiryakova, A. V., et al. (2020). Student Representation of Mass Media as Tool for Forming Public Opinion. *Online Journal of Communication and Media Technologies*, 10(3).
26. Komninos, N., & Kakderi, C. (2019). *Smart Cities in the Post-algorithmic Era*. Edward Elgar Publishing.
27. Kishore Bandela. (2025). Advancing Construction with Fibre –Reinforced Polymer in Construction Projects. *The American Journal of Engineering and Technology*, 7(03), 196–214. <https://doi.org/10.37547/tajet/Volume07Issue03-17>
28. Krahn, G. L., Putnam, M., Drum, C. E., & Powers, L. (2006). Disabilities and health: Toward a national agenda for research. *Journal of Disability Policy Studies*, 17(1), 18–27.
29. Lestari, E. Y., Sumarto, S., & Isdaryanto, N. (2017). Pemenuhan Hak Bagi Penyandang Disabilitas. *Integralistik*, 28(1), 1–9.
30. Lindeke, L. L., & Sieckert, A. M. (2005). Nurse-physician workplace collaboration. *Online Journal of Issues in Nursing*, 10(1).
31. Lindsay, S., et al. (2023). Ableism and Workplace Discrimination Among Youth and Young Adults with Disabilities. *Journal of Occupational Rehabilitation*, 33(1), 20–36.
32. Little, C., et al. (2020). Social Inclusion through the Eyes of the Student. *International Journal of Disability, Development, and Education*, 69(6), 2074–2093.
33. Lopes, A. V., & Farias, J. S. (2022). How can governance support collaborative innovation. *International Review of Administrative Sciences*, 88(1), 114–130.
34. Laheri, R., Kumar, H., Sukumar, K., Kola, C., & Makin, Y. (2025). Self-Healing Infrastructure: Leveraging Reinforcement Learning for Autonomous Cloud Recovery and Enhanced Resilience. *Journal of Information Systems Engineering and Management*, 10(49s).
35. Krishnan, G., Bhat, A. K., & Shah, J. (2025). Decision engine: Propensity prediction in the financial industry based on customer data features. In *Artificial Intelligence and Sustainable Innovation* (pp. 107–112). CRC Press.
36. Maini, A., & Heera, S. (2019). Exploring Disability Inclusion in Organizations. *Vision*, 23(2), 144–151.
37. Martin Ginis, K. A., et al. (2021). Participation of people living with disabilities in physical activity. *The Lancet*, 398(10298), 443–455.
38. Mason, M. (1990). Disability Equality in the Classroom. *Gender and Education*, 2(3), 363–366.

39. Maturbongs, E., &Lekatompessy, R. (2020). Kolaborasi Model Pentahelix. *Transparansi*, 3(1), 55–63.
40. Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative Data Analysis*. SAGE.
41. Muhyi, H. A., & Chan, A. (2017). The Penta Helix Collaboration Model. *Review of Integrative Business and Economics Research*, 6(1), 412–417.
42. Muklis, A., Hidayat, M. T., & Nariyah, H. (2022). Collaborative Governance Pentahelix. *Ijd-Demos*, 4(1).
43. Nurhayati, S. (2020). Social Inclusion for Persons with Disabilities. *Prophetic Law Review*, 2(1), 1–21.
44. Santoso, M. B., &Apsari, N. C. (2017). PergeseranParadigmadalamDisabilitas. *Intermestic*, 1(2), 166.
45. Sagar Kesarpu. (2025). Zero-Trust Architecture in Java Microservices. *International Journal of Networks and Security*, 5(01), 202-214. <https://doi.org/10.55640/ijns-05-01-12>
46. Sholeh, A. (2015). Islam dan PenyandangDisabilitas. *JurnalPalastren*, 8(2), 293–320.
47. Simplican, S. C., et al. (2015). Defining social inclusion of people with intellectual disabilities. *Research in Developmental Disabilities*, 38, 18–29.
48. Subagyo, A. (2021). The implementation of the pentahelix model. *Cogent Social Sciences*, 7(1).
49. S. S. SravanthiValiveti, "Cloud Service Models and Execution Architectures: A Unified Survey of IaaS to Serverless Computing," 2025 5th International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), MANDYA, India, 2025, pp. 1-7, doi: 10.1109/ICERECT65215.2025.11375903.
50. Sudiana, K., et al. (2020). The development and validation of the penta helix construct. *Business: Theory and Practice*, 21(1), 136–145.
51. Tarvainen, M. (2021). Loneliness in life stories by people with disabilities. *Disability & Society*, 36(6), 864–882.
52. Wang, H., & Ran, B. (2023). Network governance and collaborative governance. *Public Management Review*, 25(6), 1187–1211.
53. Whitford, A. B., et al. (2010). Collaborative Behavior and Performance of Government Agencies. *International Public Management Journal*, 13(4), 321–349.
54. Whitford, A. B., et al. (2018). Collaborative Behavior and Performance of Government Agencies. *International Public Management Journal*, 13(4), 321–349.
55. Wicaksana, D. A. (2017). The Role of Indonesian CSOs in Increasing the Understanding of Disabled Issues. *Journal of Southeast Asian Human Rights*, 1(2), 128.
56. Windiani, W. (2021). Pentahelix Collaboration Approach in Disaster Management. *IPTEK Journal of Proceedings Series*, 7, 71.
57. Wisudayati, T. A., et al. (2020). Implementation of Pentahelix Collaboration Model. *JurnalPenelitianKehutananWallacea*, 9(1), 13–22.