10.48047/jocaaa.2026.35.03.21

Identity and Access Management: Architecting Trust in Digital Society

Suneel Kumar Rawat
Independent Researcher, USA

Abstract

The growth of the IAM discipline from a specialized IT function into the core identity trust fabric that secures everything from the cloud to hybrid workforces to mobile endpoints to connected financial systems has extended the scope of IAM engineering to include non-technical considerations such as ethical responsibility, economic impact, regulatory compliance, privacy, equitable justice, and workforce inclusivity. Key developments such as Zero Trust Architecture, AI-enabled access governance automation, and self-sovereign identity promise to address chronic vulnerabilities such as stolen credentials and privilege escalation that continue to plague organizations and expose individuals to considerable risks. Ethical issues surrounding data privacy, transparency, and algorithmic bias need to be proactively addressed by engineers with diverse backgrounds to avoid bias at scale. IAM systems provide substantial value by preventing fraud, improving operational efficiency, increasing infrastructure resilience, and enabling innovation in both the public and private sectors. GDPR and DORA impose increasingly specific technical requirements for IAM implementations; they also encourage desired engineering practices through a compliance-based market for assuring IAM systems. IAM-driven workforce skilling/specialization and democratization translate security capability broadly throughout organizations, but there is still a major lack of skilled security practitioners. Topics such as the governance of AI agents, the move to quantum-resistant cryptography, and the development of universal digital identity systems place IAM engineering at the cutting edge of change in digital society. Achieving IAM systems that are equitable, inclusive, coherent, and technologically sound is a permanent challenge for society.

Keywords: Identity And Access Management, Zero Trust Architecture, AI Governance, Digital Identity, Cybersecurity Workforce

1: IAM as Critical Infrastructure for Social Resilience

At a macro level, IAM has moved from being a largely neglected but vital internal IT management function to being an essential infrastructure of social trust in the internet age. The problem is massive, with the costs of data breaches to the global economy predicted to rise to $5 trillion by 2024 as the costs of poor identity security mount [1]. The increasingly digital economy requires the secure and continuous flow of credentials across cloud providers, hybrid work environments, mobile endpoints, and financial systems. IAM serves as the authoritative control plane that governs which entities (human or machine) may access which resources, under which conditions, and for how long [2].

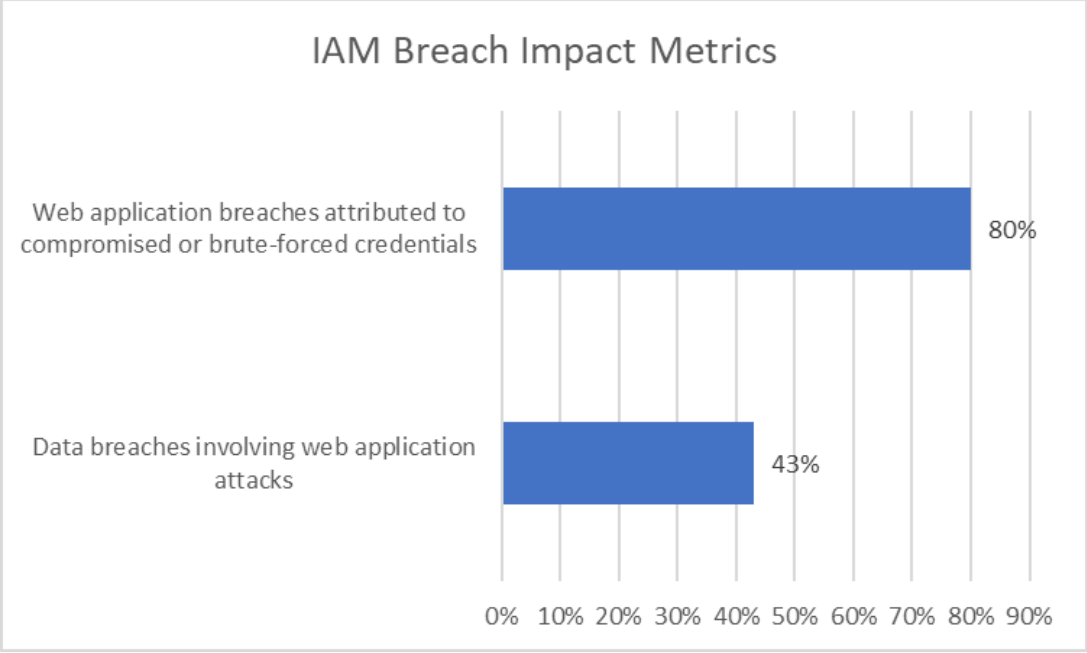
In terms of social impact, estimates indicate that attacks against web applications account for approximately 43% of all data breaches, with more than 80% of these attributable to compromised or brute-forced employee passwords. Since one-third of all data breaches are traced back to poor passwords and/or identity management behaviors [1], IAM engineering can help reduce these risks through the implementation of controls such as a Zero Trust Architecture (ZTA). A ZTA enforces an assumption of

10.48047/jocaaa.2026.35.03.21

zero trust for all users and devices, whether they are internal or external to the network perimeter, and authenticates, authorizes, and continuously validates access requests based on contextual signals [2].

Role-Based Access Control (RBAC) is the most common access control (AC) model for enterprises. However, RBAC entails a relatively high operational cost. One of the most common vulnerabilities of enterprise infrastructures is privilege accumulation. This happens when access rights are kept long after the conditions for their granting cease to exist [1]. Automated IGA platforms can address this by continuously reconciling active entitlements against the current role definitions and triggering remediation workflows if roles are not aligned with entitlements. Different calculated objectives in the area of security, compliance, and efficiency drive the selection of specific metrics, which help to measure the fulfillment of these objectives and therefore track their progress [2].

A self-sovereign identity (SSI) framework built on decentralized identifier standards offers an extension of IAM's potential to society: by allowing users to issue, manage, and verify credentials without relying on a single institutional authority, it can promote financial inclusion for the unbanked or underbanked population [1].



Graph 1: Identity Vulnerability Key Statistics [1, 2]

2: Ethical dimensions of governance automation in IAM

The scale for which computing technology can automate decisions regarding access governance is broad. For example, if an algorithm decides who gets access to a financial account, medical records, or a recruitment platform, then human values such as dignity, privacy, and equity can all become directly relevant to the algorithm. IAM engineers, therefore, work not only as technical architects but also as ethical agents whose design decisions instantiate value judgments at scale [3].

Instances of unethical IAM practice and the subsequent data security issues are well documented. In a survey of over 2000 UK office workers, half of the respondents owned up to unsafe working practices that could lead to data breaches, such as sending sensitive emails to a personal email or keeping

10.48047/jocaaa.2026.35.03.21

unencrypted files on removable media. Twenty-three percent of respondents were not aware that their organization had an IT security policy [3]. These results show that automating technical governance is no substitute for designing systems to take into consideration how humans and organizations actually behave.

The foundational ethical principle of Privacy by Design can be implemented in IAM via restricting the collection of data in IGA platforms to the minimum attributes necessary for access decisions. Ephemeral JIT credentials limit the lifetime of artifacts used for authentication and post-authentication behavior tracking. Decentralized identity architectures distribute data custody, reducing the impact of single points of compromise [4]. Because of their normative dimension, the architectural choices impact what identity data is collected, who can see it, and what it is used for.

The second ethical demand for AI-based access control decisions is transparency, as customary authorization systems are non-automated, non-smart, expensive, difficult to maintain, and do not scale well. While the challenges above may be addressed by AI in the majority of future authorization scenarios [4], users may nonetheless have legitimate questions as to why an access decision was made, and the role played by algorithmically-derived variables in making an access decision when AI systems automate the process of approval or rejection.

Data security has been one such top IAM research pressure point, accounting for a third of research literature. The broader pressure point, compliance, has accounted for 41% of the literature [3]. This requires a disparate impact testing process, diverse engineering teams capable of detecting the embedded bias, and an explicit remediation plan [4].

Risk Domain	Human Behavior Factor	Organizational Challenge	Consequence
Data Security	Unsafe working practices	Low security policy awareness	Increased breach exposure
Access Governance	Credential misuse	Non-automated authorization systems	Scalability and maintenance failures
Algorithmic Fairness	Biased design decisions	Homogeneous engineering teams	Discriminatory access outcomes
Compliance	Inadequate audit trails	Limited remediation pathways	Regulatory enforcement risk
Privacy	Excessive data collection	Single points of compromise	Identity data exploitation

Table 1: IAM Ethical Risk Domains and Organizational Challenges [3, 4]

3: Generating economic value by IAM engineering

IAM systems deliver value to society in four dimensions simultaneously: fraud prevention, efficiency gains, system resilience, and innovation. Each contributes in its own way to social welfare, reflecting value delivered to not just the individual enterprises that deploy IAM technology, but also the economic system to which these enterprises belong [5].

The most obvious economic benefit is the ability to prevent fraud. Customary IAM systems with static rules and predetermined business policies are poorly suited for cloud services. They generally rely on

10.48047/jocaaa.2026.35.03.21

weak password policies, are inefficiently scaled, and have various exploitable weaknesses [5]. AI-improved IAM architectures offer their own possible solution set. AI can be used to monitor the behavior of users, detecting abnormally high transaction rates in real time, thereby stopping a credential-based attack before it is completed. The move from reactive responses to proactive fraud prevention creates present-day economic advantages for the financial services and healthcare industries, both of whose compliance regulations include high penalties .

Automatic access governance generates compounding efficiencies for organizations. In IAM with Zero Trust Architecture (ZTA) practice, every entity on the network and communications transaction is continuously validated. This has been validated in security frameworks around communication, where deep learning frameworks achieve an accuracy of 84.59% identifying allowed versus disallowed access to communication signals [6]. Improving the level of automation around this access review process reduces legacy manual burdens and enables security experts to dedicate their efforts toward more valuable security efforts like threat modeling and planned risk governance.

The IAM area with the largest but most difficult-to-quantify economic benefit appears to be the resilience of infrastructures. AI IAM solutions are more scalable and flexible than customary IAM solutions and enable context-aware access control policies based on multiple attributes, such as at what time and where resource is accessed, by whom, and at what trust level of a device [5]. This allows for flexibility under crisis conditions (cyberattack, natural hazards, pandemic disturbances) and can continue working to the extent that they do not obstruct access or creation of hazardous overrides.

Innovation enablement is another economic contribution: leveraging Explainable AI methods for access control decisions, using interpretability tools to measure contributions of specific input feature values to the output of a classifier [6], helps organizations to pass compliance audits and earn stakeholder confidence in the automated governance of innovative digital services as built on verified IAM pillars.

4: Compliance with regulations and policies

IAM systems are at the intersection of technology development and regulatory compliance. Compliance mandates and the ecosystem for IAM systems are not a one-way street. Across the set of regulatory regimes for data protection, financial services and digital operational resilience, technical requirements are imposed on IAM systems. The implementation of IAM systems in turn informs compliance requirements in terms of what is technically feasible or not [7].

Several provisions of the GDPR are directly applicable to an IAM system, for example, the data minimization principle, which states that data should be processed only for the purposes for which it was collected. IAM systems must enable this through their identity data collection, attribute management, and analytical capabilities. The principle of purpose limitation requires that IAM system audit processes are capable of monitoring and enforcing the use of personal data only for specified purposes. The rights to access, rectification, erasure and portability require IAM solutions to maintain awareness of the location of personal data. Healthcare organizations that practiced GDPR Privacy by Design with AI-enabled IAM solutions reported a 40% decrease in unauthorized access incidents within the first year of implementation, in one example of regulation leading to better security practices [8].

The Digital Operational Resilience Act (DORA) requires financial services firms in the EU to manage threats and vulnerabilities to their ICT systems' resilience, and is effective from January 2025. DORA has major implications for IAM through incident reporting (including technical aspects), resilience testing of critical ICT systems, and third-party ICT systems risk management. [7] Financial institutions must show

10.48047/jocaaa.2026.35.03.21

they identify, assess, and systematically reduce technology risks, and IAM both serves this risk management need and mediates its implementation.

Financial Zero Trust architectures also support the financial services industry's regulatory and compliance requirements through five adversarial threat models (credential theft, insider lateral movement, API abuse, money-laundering pattern emulation and session hijacking) with which IAM policy decision engines must be able to show consistent, automated and regulator-specified behavior [7]. AI-enabled IAM technologies also assist in automated collection, verification and monitoring of GDPR consent in real time to relieve the compliance burden and improve audit evidence defensibility [8].

10.48047/jocaaa.2026.35.03.21

GDPR Provision	IAM System Requirement	Implementation Mechanism	Compliance Outcome
Data Minimization	Restrict identity data collection to specified purposes	Attribute management controls	Reduced data exposure risk
Purpose Limitation	Monitor and enforce personal data usage	IAM audit processes	Defensible audit evidence
Right to Access	Maintain personal data location awareness	Identity data inventory	Regulatory accountability
Right to Rectification	Enable personal data correction	IGA workflow automation	Data accuracy assurance
Right to Erasure	Support credential and data deletion	Automated remediation workflows	Privacy compliance
Consent Management	Automate collection and real-time monitoring	AI-enabled IAM tools	Reduced compliance burden

Table 2: GDPR Provisions and IAM System Requirements [7, 8]

5: Workforce transformation and equitable system design

The proliferation of IAM technologies is radically reshaping the cybersecurity workforce, creating new cybersecurity jobs, and dynamically reshaping the distribution of technical capabilities across organizations. This causes additional, second-order effects for the distribution of digital security capabilities across sectors of the economy and institutions in society more generally.

With increasing complexity in cloud, hybrid and multi-cloud implementations, the demand for IAM is also growing. IAM engineering skills are increasingly specialist roles in their own right, including but not limited to governance engineers, security automation engineers, identity architects and Privileged Access Management (PAM) engineers. Each role requires a different combination of skills, and the number of security professionals has become an urgent issue: from 2015 data, 62% of respondents said that their organization was understaffed in security, compared to 56% in 2013, with a workforce gap of 1.5 million personnel in five years predicted.

Emerging specializations related to IAM technologies include AI-enabled IAM capabilities, and the management of non-human identities. In many enterprise environments, machine identities outnumber human identities. Machines may operate at a much faster pace than humans, meaning that customary IAM authorization processes may no longer be viable in cloud-native environments.

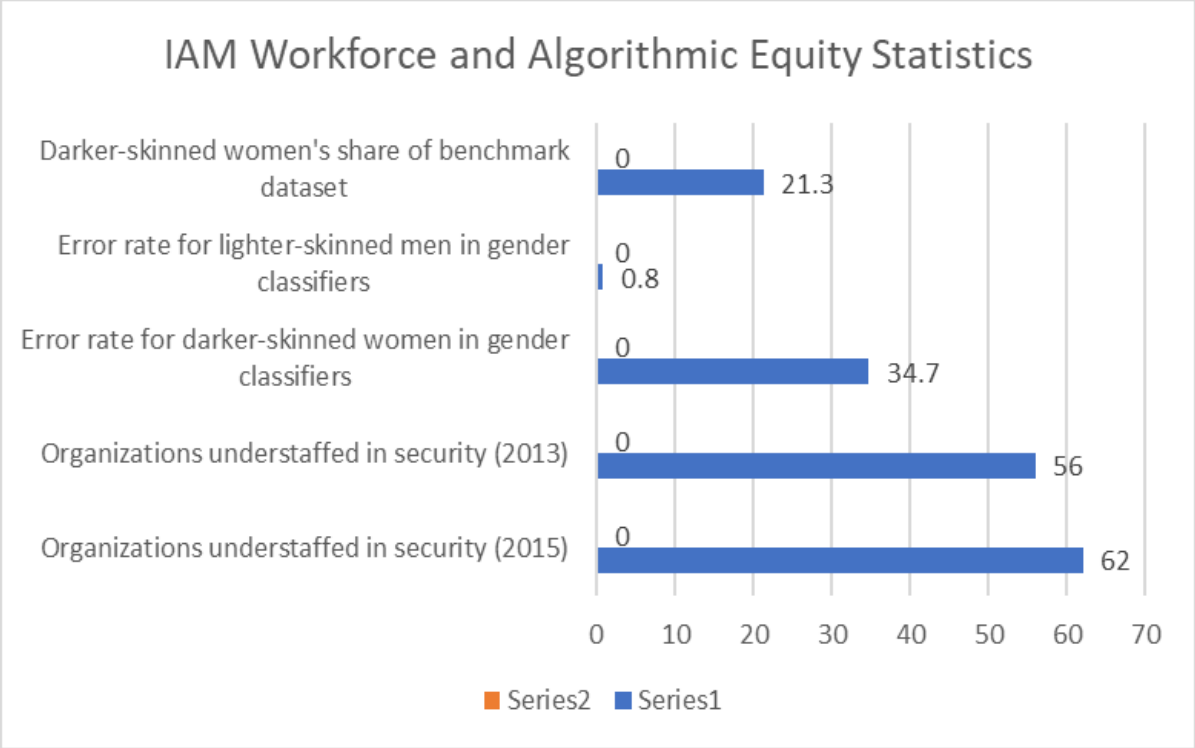
Self-service IAM functions democratize technical capabilities by shifting the access request process to business teams, increasing agility, and improving security with manager-approved entitlements through self-service portals. However, empowering business users with controls entails investments in security awareness, such that informed governance decisions can take place across the enterprise.

IAM engineering teams are a determining factor for further diversity and inclusion in IAM systems. Diverse IAM teams are more likely to identify bias in behavioral analytics algorithms, and create inclusive IAM systems. Empirical studies of commercial gender classifiers have found error rates for darker-skinned women of up to 34.7% (compared to 0.8% for lighter-skinned men). Though only

10.48047/jocaaa.2026.35.03.21

comprising 21.3% of the benchmark dataset, darker-skinned women made up a disproportionate number of the errors in all the data classifiers in the study.

Therefore, organizations with a commitment to equitable IAM design must integrate workforce diversity as a technical quality requirement and implement equity reviews into engineering workflows like security threat modeling. [9][10]



Graph 2: Security Staffing Gaps and Classifier Bias Metrics [9,10]

6: Future trajectories: AI governance, quantum preparedness, and digital identity.

IAM engineering is likely to be important for the development of a digital society due to the convergence of three megatrends: digital identity governance for common AI agents, a coming era of cryptography driven by quantum computers, and a future with universal digital identity protocols. Each of these megatrends poses problems to be solved by IAM engineering, both ethical and technical.

Governance of AI agents may be the most immediate frontier of IAM development. Institutions are increasingly deploying financial AI systems that can autonomously transact, access sensitive customer data, and make high-stakes decisions without human oversight. They need to be associated with authenticated identities, scoped permissions, behavioral setpoints, and audits, with different characteristics and different operational properties compared with humans. In fact, a systematic literature review of the ZTA literature published from 2016 to 2025 (1,774 research publications retrieved in total) shows that machine identity governance is one of the most rapidly growing application domains in IAM and security solutions.

Specific to IAM of AI agents, conditional authorization inheritance states that an AI agent is only authorized to exercise the permissions for which both it and the delegating user are authorized. Defining

10.48047/jocaaa.2026.35.03.21

and enforcing behavioral boundaries requires technical controls that signal and even inhibit an agent's behavior outside its operational design. Accountability frameworks require that actions of agents align with the outcomes of those actions.

A longer-horizon existential threat to IAM infrastructure is that of quantum computers. The cryptographic algorithms that underlie many of the protocols used for authentication (such as RSA, elliptic curve cryptography, and Diffie-Hellman key exchange) are based on problems that quantum computers would be able to solve much faster than classical computers. When NIST published its initial quantum-resilient cryptographic standards, organizations faced pressure to migrate to quantum-safe algorithms in 2024.

Universal digital identity is the most transformative long-term pathway, as it can empower people to access social services and systems and to participate in the democratic process and in safe, authenticated transactions in the digital world through a universal, portable, and verifiable credential. Digital inclusion concerns matter too. Systems that do not take into account the needs of persons with limited access to technology and low digital literacy will reenact exclusion and discrimination in more technical and automated forms. The experience at the National Academies in convening more than 7000 volunteer committee members annually, leveraging hundreds of expert committees to organize diverse, independently verified expertise, presents lessons learned in mobilizing expertise to address complex social challenges.

Conclusion

IAM has emerged as one of the most consequential engineering disciplines of the time. It includes a broad scope of ethical responsibilities, from technical architecture to problematizing economic incentives, creating regulations, and developing the workforce to governing the long view. It creates and prevents threats through credential transactions, through the abuse of these privileges, through perverse incentives, and through discriminatory algorithms. IAM failures are therefore not just manifest as social harms to people, organizations, and economies. Remedies include engineering best practices that are privacy by design and follow zero trust architecture and transparent AI governance, as well as diverse teams with lived experience to identify the embedded bias ignored by homogeneous teams. The implementation of GDPR and DORA has transformed IAM from a compliance function to a board-level planned priority and accountability structure that reinforces the ethics of the profession. This means the shift in the workforce due to IAM becomes both an equity opportunity and a challenge. But growing the broader pool of people building and using IAM intrinsically makes the systems they build more equitable while tackling the perpetual security skills shortage. The course of developments in AI agent governance, quantum-resistant cryptography, and global digital identity systems will determine whether IAM systems are more open, portable, and privacy-preserving, or whether they are a recreation of existing inequities in more technical form. IAM engineers will also have to consider the wider impact of their work.

10.48047/jocaaa.2026.35.03.21

Reference

[1] Jana Glo¨ckler et al., "A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity," 2024. [Online]. Available: https://link.springer.com/content/pdf/10.1007/s12599-023-00830-x.pdf

[2] Thomas Baumer et al., "Identity and access management metrics: A systematic review," ACM Digital Library, 2026. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3788858

[3] Mumina Uddin and David Preston, "Systematic Review of Identity Access Management in Information Security," Journal of Advances in Computer Networks, 2015. [Online]. Available: https://www.academia.edu/122102705/Systematic_Review_of_Identity_Access_Management_in_Information_Security

[4] Anant Wairagadea, Sumit Ranjan, "AI in Identity and Access Management (IAM) for Enterprise Systems: A Comparative Analysis," ScienceDirect, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S187705092502071X?ref=pdf_download&fr=RR-2&rr=9d2471179835b089

[5] Godwin Nzeako and Rahman Akorede Shittu, "Leveraging AI for enhanced identity and access management in cloud-based systems to advance user authentication and access control," World Journal of Advanced Research and Reviews, 2024. [Online]. Available: https://www.researchgate.net/profile/Godwin-Nzeako/publication/387524483

[6] Ekramul Haque et al., "Enhancing UAV Security Through Zero Trust Architecture: An Advanced Deep Learning and Explainable AI Analysis," arXiv, 2024. [Online]. Available: https://arxiv.org/pdf/2403.17093

[7] Paulo Fernandes Biao, "SecureBank™: A financially aware zero-trust architecture for high-assurance banking systems," arXiv, 2025. [Online]. Available: https://arxiv.org/pdf/2512.23124

[8] Asif Hussain, "Implementing privacy by design: Integrating AI and IAM for GDPR compliance in healthcare," Oct. 2020. [Online]. Available: https://www.researchgate.net/profile/Asif-Hussain-31/publication/384600916

[9] Frost & Sullivan, "The 2015 (ISC ² Global Information Security Workforce Study," whitepaper, 2015. http://book.itep.ru/depository/security/general/FrostSullivan-(ISC)2-Global-Information-Security-Workforce-Study-2015.pdf

[10] Joy Buolamwini, Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," Proceedings of Machine Learning Research 81:1–15, 2018. https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

[11] Gambo & Almulhem, "Zero Trust Architecture: A Systematic Literature Review," arxiv, 2025. https://arxiv.org/pdf/2503.11659

[12] Peter D Blair, "The evolving role of the US National Academies of Sciences, Engineering, and Medicine in providing science and technology policy advice to the US government," PALGRAVE COMMUNICATIONS, 2016. https://www.nature.com/articles/palcomms201630.pdf