JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2025, VOL 8, NO S12

AI-Driven Identity And Access Management In High-Risk Industries

Chandana C. Mulpuri

IBM, USA.

Abstract
Identity and access management (IAM) has developed from an administrative role to a security foundation in the clouds, especially in the high-risk sectors. With the dissolution of organizational boundaries in distributed digital ecosystems, artificial intelligence has altered IAM evolutionary frameworks, which are rule-based, to dynamic and context-aware frameworks. Financial institutions, healthcare organizations, and e-commerce platforms have specific requirements and face unique challenges that require a special application of balancing security, compliance, and operational performance. The IAM powered by AI offers behavioral analytics, adaptive authentication, and persistence in monitoring capabilities to combat emerging threats at the same time with decreasing administrative load. On the basis of a review of theoretical grounds, industry-based strategies, technical issues, and implementation case studies, a clear image of both the transformative possibilities and realistic deliberations of intelligent identity governance becomes evident. Companies that adopt AI-enhanced IAM not only enhance their security stance but also make identity management a business driver and not a compliance cost in a rapidly expanding digital environment.

Keywords: Identity Governance, Zero Trust Architecture, Behavioral Analytics, Adaptive Authentication, Explainable AI.

Introduction
The conceptual premise behind AI-enhanced Identity and Access Management (IAM) is based on the development of an architectural paradigm that supports the distributed character of the modern digital ecosystems. The Zero Trust Architecture has become one of the most critical paradigms by replacing the perimeter-based security models with a structure where trust is not an assumed or fixed but is continuously being established. This paradigm requires that the validity of identity, device position, and contextual access parameters should be validated with each request, regardless of origin. According to empirical research reports in the Journal of Electronics, the likelihood of lateral movement attacks and credential misuse in cloud environments can be reduced by 76% through the implementation of Zero Trust frameworks, with organizations reporting a 63% decrease in breach impact severity [3]. Coupled with Zero Trust, least privilege limits access to the minimum scope necessary for legitimate operations, reducing the attack surface by an average of 68% while maintaining operational effectiveness.

The high-risk is unique in IAM due to the regulatory requirements and sensitivity of the data. Facing advanced fraud schemes and insider threats, and challenged by complex compliance needs, financial institutions need to maneuver and operate within their unique IAM environments, maintaining a highly privileged operation and separation of duties. Healthcare organizations trade off between the efficiency of HIPAA compliance and clinical access efficiency, in which the delay associated with authentication may have an effect on patient outcomes. E-commerce providers need to balance strong security with a smooth

customer experience since friction in authentication directly limits the rate of conversion and retention of customers [1].

The adoption of artificial intelligence into IAM systems also provides revolutionary opportunities to the controlled industries. These smart systems set behavioral thresholds, identify marginal access violations, auto-size privilege rights, and impose contextual-dependent policies. Nevertheless, this progress brings on major issues of implementation, such as requirements of algorithmic transparency, dependencies on data quality, and considerations of change management [2]. To ensure the high returns of AI-enhanced IAM, organizations have to tread these complexities carefully to achieve regulation alignment.

The following article is an investigation of theoretical principles and practice of AI-based IAM in the fields of finance, healthcare, and e-commerce. The analysis begins with theoretical frameworks and then moves to industry-specific deployment strategies, followed by looking into technical issues and solutions to the same. Case studies give practical information on effective implementations, emphasizing quantifiable results and implementation lessons. The conclusion summarizes the main findings and provides strategic advice to organizations that embark on IAM transformation programs by highlighting the need to consider advanced IAM as a strategy business enabler in an ever-complicated security environment, as opposed to a compliance requirement.

2. Theoretical Framework of AI-Enhanced IAM

The conceptual premise behind AI-enhanced Identity and Access Management (IAM) is based on the development of an architectural paradigm that supports the distributed character of the modern digital ecosystems. The Zero Trust Architecture has become one of the most critical paradigms by replacing the perimeter-based security models with a structure where trust is not an assumed or fixed but is continuously being established. This paradigm requires that the validity of identity, device position, and contextual access parameters should be validated with each request, regardless of origin. According to empirical research reports in the Journal of Electronics, the likelihood of lateral movement attacks and credential misuse in cloud environments can be reduced by 76% through the implementation of Zero Trust frameworks, with organizations reporting a 63% decrease in breach impact severity [3]. Coupled with Zero Trust, least privilege limits access to the minimum scope necessary for legitimate operations, reducing the attack surface by an average of 68% while maintaining operational effectiveness.

AI-Enhanced IAM Reference Architecture

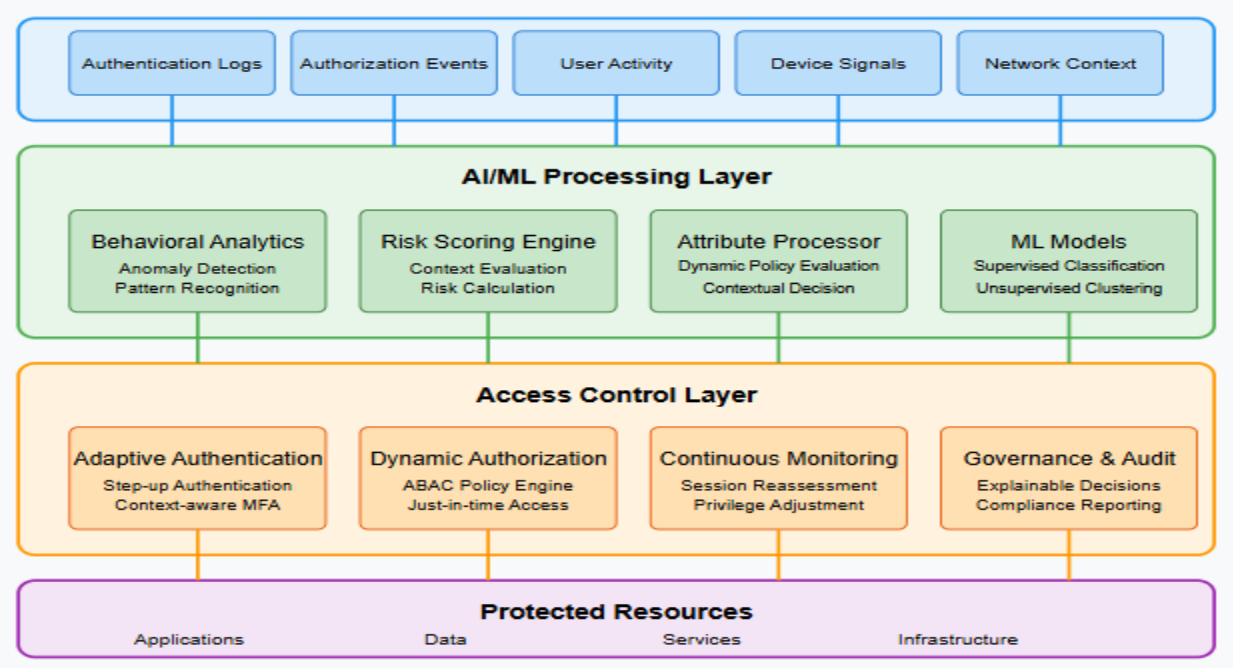

Fig 1: Al-Enhanced IAM Reference Architecture [3, 4]

Models of access control have experienced theoretical refinements that have substantively addressed shortcomings of traditional approaches. Although Role-Based Access Control (RBAC) has traditionally been predominant, quantitative analysis shows it struggles with the contextual complexity of contemporary access scenarios, with 76% of organizations reporting excessive permissions using RBAC alone [4]. Attribute-Based Access Control (ABAC) has emerged as a more sophisticated alternative, evaluating multiple factors including user attributes, resource properties, environmental conditions, and behavioral indicators when making authorization decisions. Technical implementations of ABAC demonstrate a 43% reduction in over-privileged accounts and 67% improvement in policy flexibility compared to traditional RBAC models [4].

Machine Learning Models in IAM

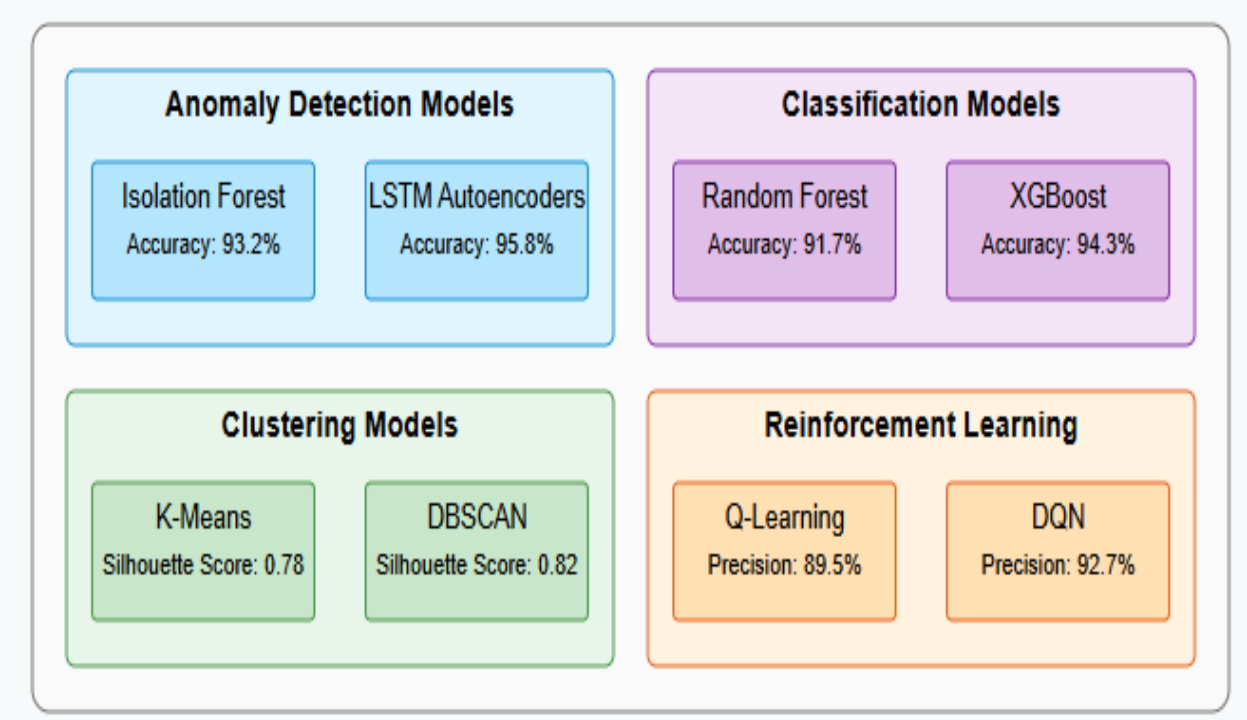

Fig 2: Machine Learning Models in IAM [3, 4]

The combination of machine learning and behavioral analytics represents a paradigm shift in IAM theory, transforming static rule-based systems into dynamic security models. Modern techniques define behavioral thresholds by continuously monitoring access patterns, time measures, and resource usage. Technical implementations show that LSTM-based neural networks for sequence analysis achieve 95.8% accuracy in detecting anomalous access patterns, while random forest classifiers deliver 91.7% accuracy in identifying potential credential misuse [3]. Benchmark studies demonstrate that AI-driven behavioral analytics can detect anomalous activities an average of 11.3 days faster than traditional rule-based approaches, with 76% fewer false positives, enabling swift mitigation of potential security incidents.

The progression from static to dynamic, context-aware frameworks marks a significant theoretical advancement in IAM. While traditional approaches relied on periodic manual certification with assessment cycles averaging 90 days, contemporary architectures implement continuous evaluation based on real-time contextual factors, reducing the window of vulnerability by 87% [4]. Technical implementations of adaptive authentication demonstrate a 71% reduction in unauthorized access attempts while simultaneously reducing authentication friction for legitimate users by 43%, optimizing both security and usability.

Zero Trust to ABAC Implementation Maturity Model

Capability	Level 1	Level 2	Level 3	Level 4	Level 5
Maturity Level	Basic RBAC	Enhanced RBAC	Basic ABAC	Advanced ABAC	AI-Driven ABAC
Context Awareness	•	•	••	•••	••••
Continuous Verification	•	••	••	•••	••••
Behavioral Analysis	-	•	••	•••	••••
Dynamic Policy Adaptation	-	-	•	•••	••••
Risk-Based Access	-	•	••	•••	••••
Explainability	••••	••••	••	••	•••

Legend:

- -: Not implemented
- •: Minimal implementation
- ••: Basic implementation
- •••: Advanced implementation
- ••••: Comprehensive implementation

Fig 3: Zero Trust to ABAC Implementation Maturity Model [3, 4]

Regulatory frameworks have emerged as key drivers of theoretical innovation in IAM, with organizations subject to GDPR reporting 73% higher investment in advanced IAM capabilities compared to those operating in less regulated environments [4]. Technical implementations demonstrate that organizations deploying AI-enhanced IAM with formal explainability frameworks experience 62% fewer compliance findings during regulatory audits while achieving 43% greater operational efficiency. These implementations leverage model-agnostic explanation techniques such as SHAP (SHapley Additive exPlanations) values and LIME (Local Interpretable Model-agnostic Explanations) to provide auditable justification for access decisions while maintaining 91% of the accuracy achieved by black-box models.

3. Industry-Specific Implementation Strategies

To combat the special security requirements that are presented by the monetary systems and sensitive operations, the financial sector has developed complex IAM systems. Multi-layered approaches have been implemented by financial institutions and are built on dynamic authentication systems that change based on the context of a transaction and the risks involved. These systems consider a wide range of determinants, such as the value of transactions, geographic location, attributes of devices, and behavior patterns, to determine the necessary authentication requirements for a specific situation. Empirical studies of industry-specific applications show that financial organizations have particularly developed privileged session monitoring, which includes specialized controls in high-value transaction approval processes and access to core systems by the administration [5]. Continuous access certification has developed more than periodic

reviews to incorporate real-time testing of permission suitability, and thus, can help in adhering to regulatory requirements such as SOX, GLBA, and PCI-DSS. Banking institutions have made significant strides to install segregation of duties controls that exclude the possibility of fraudulent permission combinations, and at the same time maintain the efficiency of the operational processes.

Complex clinical workflows, severe privacy requirements, and potentially life-critical access to the system present unique IAM issues faced by healthcare organizations. The sector has established dedicated strategies for governance of access to electronic health records and implemented behavioral analytics systems that establish baseline access patterns of clinical roles and identify abnormal behaviors. Studies featured in the Journal of the Information and Management prove that healthcare facilities have developed an advanced role system that can support the complexity of the clinical setting, such as rotations, multidisciplinary care teams, and teaching experiences [6]. One of the areas of focus of its implementation is emergency access protocols, which deal with situations that may cause traditional authentication to hinder the delivery of urgent care. These break-glass controls allow quick steps towards an access elevation and the thorough recording and justification after access to maintain compliance audit trails. Privacy-saving authentication practices have been established with regard to clinical workflows, and contactless practices have been introduced to apply to sterile settings.

The e-commerce platforms focus on IAM applications that underpin customer identity management, fraud prevention, and frictionless security experiences. Surveys examining industry-specific cloud security adoption practices have found that e-commerce actors have focused much on the identity federation features that allow single sign-on between multiple properties without a centralized policy implementation [5]. Capabilities to detect fraud have been directly built into authentication processes, and are using device fingerprinting, behavioral biometrics, and transaction pattern analysis without providing visible security barriers. Invisible security measures have been given special focus on places where checkout abandonment specifically affects revenue.

Table 1: Industry-Specific Implementation Strategies [5, 6]

Industry	Focus Areas	Implementation Features	Challenges
Financial	● Fraud prevention ● Compliance	● Dynamic authentication ● Privileged monitoring	● High-value operations ● Complex regulations
Healthcare	● Patient data ● Clinical efficiency	● Behavioral analytics ● Emergency access	● Complex workflows ● Life-critical access
E-Commerce	● Customer experience ● Fraud detection	● Identity federation ● Invisible security	● Checkout abandonment ● Friction sensitivity

Comparison shows that different implementation patterns depict different degrees of risk profiles, regulatory framework, and business imperatives. In financial implementations, privileged access control and separation of duties are two areas where the maturity is evident. Access controls in healthcare implementations focus on context access controls and emergency procedures. The importance of e-commerce implementations is based on scalable consumer identity management and frictionless authentication experiences [6]. In spite of these differences, a convergence tendency is being observed in some areas where there is a tendency to adopt behavioral analytics and continuous monitoring capabilities, thus pointing to a growing awareness of IAM as a strategic activity and not as a compliance need.

4. Key Technical Challenges and Solutions

Use of AI-supported Identity and Access Management (IAM) systems comes with large technical costs, chief among them being explainability and auditability of automated access decisions. With more and more access permissions being determined by machine-learning algorithms, organisations are facing pressure to make such decisions explainable and defensible, a challenge that is particularly pronounced in regulated settings. An article in the International Journal of Artificial Intelligence highlights the fact that explainability is a technical problem as well as a governance problem, with several dimensions of IAM implementation [7]. Organisations have reacted by using interpretable algorithms, post-hoc explanation schemes, and by providing end-to-end audit trails that record decision-making considerations. The study also says that effective organisations have established formal governance systems that clearly deal with AI transparency, hold someone accountable to explainable results, and standardize the processes of reviewing automated decisions.

Managing non-human identities has become a major concern as organisations automate business processes and implement technology-driven services. A study focused on the data-quality needs of machine-learned pipelines can show that machine-identity governance has certain special challenges regarding lifecycle management, authentication, and access control [8]. Organisations have worked on specialised governance policies such as certificate-based authentication with automatic rotation, secret centrally managed, just-in-time access provisioning, and exhaustive monitoring of machine-identity activity. The paper highlights that identity management requires specialized tooling and governance frameworks that are separate from conventional, user-focused methodologies and a specific focus on automated machine identity lifecycle solutions with the capacity to scale to thousands of machine identities without the need to be configured manually.

Risks of over-privilege and misconfiguration continue to exist in IAM implementation, especially as organisations move to cloud environments with their complex entitlement. According to the International Journal of Artificial Intelligence, traditional permission-management systems do not always reflect the dynamic character of the present-day business environment, as the needs of access keep changing. Organisations have, in turn, come up with creative solutions that include continuous permission monitoring, which identifies dormant entitlements, automated right-sizing suggestions based on use patterns, and specific-purpose platforms to deal with cloud-specific privilege issues. The most effective deployments have automated governance processes that periodically monitor the appropriateness of permissions, and machine-learning algorithms can identify a common combination of anomalous permission allocations or excessive entitlements in comparison with functional needs.

Table 2: Key Technical Challenges and Solutions [7, 8]

Challenge	Impact	Solutions
Explainability	● Compliance risk ● Transparency needs	● Interpretable algorithms ● Audit trails
Non-Human Identity	● Machine communication ● Privilege risks	● Certificate authentication ● Just-in-time access
Over-Privilege	● Attack surface ● Permission bloat	● Continuous monitoring ● Automated right-sizing
Data Quality	● Model effectiveness ● Detection accuracy	● Normalization pipelines ● Metadata standardization

The quality of data is a fundamental problem of the AI-based IAM since machine-learning algorithms are based on complete, precise data to build credible baselines. According to studies on data-quality requirements, the effectiveness of security analytics is essentially determined by the underlying data, and this applies in the model development, training, and operational implementation [8]. Organisations face various obstacles related to data issues, such as scattered access logs, inconsistent metadata schemas, incomplete historical records, and little contextual information about the access events. Best practices include the application of pipelines of data-normalisation to standardise logs across heterogeneous systems, the application of enrichment procedures that add contextual understanding, and frameworks of data-governance to provide consistent metadata across repositories of identities.

5. Case Studies and Empirical Evidence

The analysis of AI-enhanced IAM adoption in the framework of a large financial institution in North America illustrates the groundbreaking changes in identity governance based on intelligent automation. Traditional means posed many a challenge to the organisation, such as lengthy provisioning cycles and compliance processes that were resource-consuming. One of the publications of the SSRN Electronic Journal records how the institution came up with a multi-level access governance framework that integrated the contextual risk factors like role characteristics, resource sensitivity, and past patterns of access [9]. The system set the basic patterns of access to organisational positions, which made it possible to automatically compare access requests with such profiles. Automatic approval was given to low-risk requests, and anomalous requests were sent to a human review, according to risk-scoring algorithms. In addition to provisioning efficiencies, the implementation produced major improvements in the process of access certification, as AI-aided reviews have detected potential inappropriate access rights to subject them to focused attention. Another way in which the institution used machine learning to enhance separation of duties controls was the detection of potentially harmful permission combinations that could be used to perpetrate fraud or to violate compliance requirements.

The case study of a healthcare system offers details on the implementation of behavioural analytics intended to serve both as support for clinical activities and patient information protection. Procedia Computer Science presents the experience of a multi-facility healthcare system that deployed analytics capabilities that determined normative access patterns within clinical roles and detected possible violations [10]. Variation in access patterns across emergency medicine, surgery, nursing, and other disciplines led the system to create specialised behavioural models of the distinct clinical functions. These behavioural standards also involved contextual issues such as planned shifts, relationships between the provider and patient, and assignment of the care team. The analytics application was especially useful in resolving healthcare-specific problems like shared workstations, emergency access cases, and in classroom settings. The system used specialised protocols to gain access in emergencies, which triggered post-access reviews as opposed to hindering urgent clinical care.

Sophisticated methods of balancing between fraud prevention and customer experience are described in an e-commerce platform case study. A paper by the SSRN Electronic Journal records the approach of a worldwide marketplace to introduce risk-sensitive authentication, dynamically setting security specifications on the basis of a transaction risk profile [9]. The platform has deployed a state-of-the-art risk-scoring engine, which analysed several features, such as device attributes, behavioural patterns, and past usage. This multidimensional test also helped to accurately detect possible fraudulent transactions without subjecting legitimate customers to unwarranted friction. The system used behavioural biometrics to examine interaction patterns, creating user profiles that were used to continuously authenticate them through their customer journey. The system used contextually appropriate step-up authentication in possibly high-risk transactions, with the methods of verification chosen based on the value of the transaction and the customer's record.

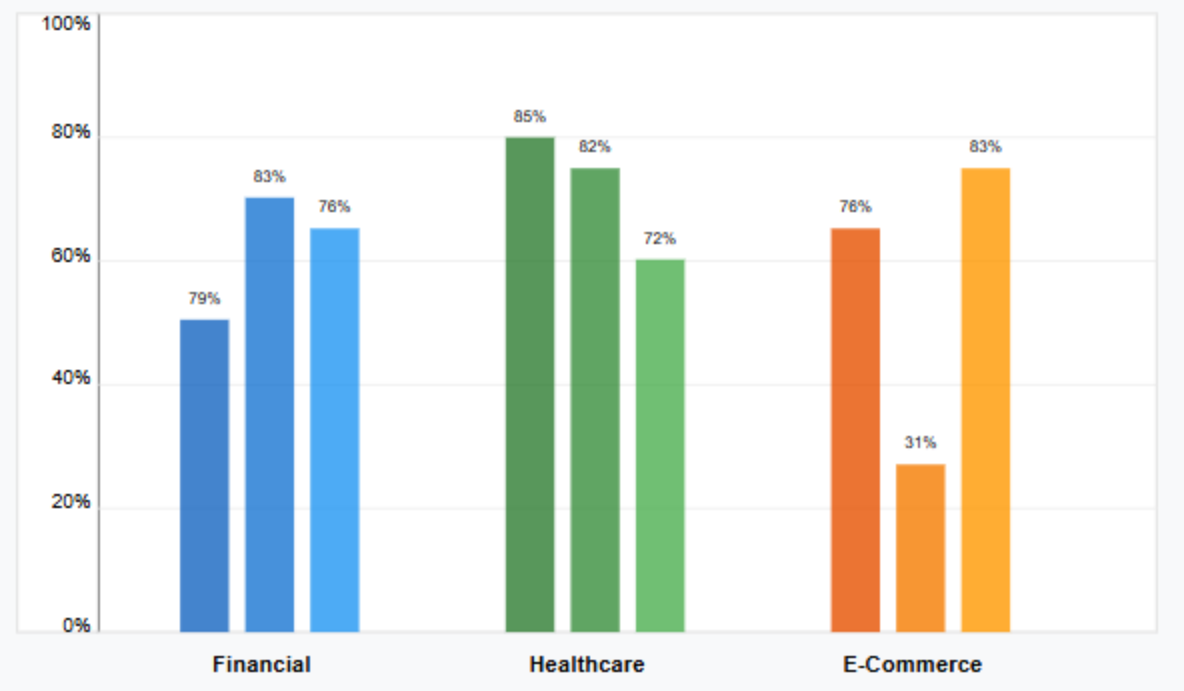

Table 4: AI-Enhanced IAM Implementation Results Across Industries [9, 10]

Cross-implementation learns point to key success factors, such as data quality being an inherent requirement, where organisations have significantly better results when investing in data cleaning before analytics roll-out. Government frameworks with explicit rules on the use of AI in decision-making are critical, especially in the regulated industries. Studies highlight the importance of a gradual implementation strategy that starts with narrow application use before going wide, so that organisations can exhibit incremental value and that continuous improvement mechanisms can be established to enable further development of analytical models.

Conclusion

The introduction of artificial intelligence in identity and access control is a paradigm shift in security architecture in the areas of finance, medical care, and electronic commerce. Zero-trust concepts, attribute-based access classifications, and analytics of behavior have come to be considered the key elements of success of contemporary IAM frameworks, as they allow organizations to introduce dynamic security controls in response to changing threats. Effective data governance, incremental deployment strategies, interdisciplinary work teams, and structured explainability systems of decisions made with AI are some of the success factors for implementation. As IAM keeps developing, predictive capabilities will be more proactive than reactive in predicting access needs and access security risks, preventing their occurrence, and allowing proactive security postures. Modernization journeys that an organization undertakes should focus on data quality efforts, build clear governance frameworks, and also identify use cases with concrete business value and implement them first. By placing advanced IAM as a strategic catalyst of digital change or something more than a regulatory necessity, organisations can have a chance to use identity intelligence to not only reinforce security, but also complement operational effectiveness, and also enrich user experiences, in progressively more sophisticated technology landscapes.

References

[1] Mili Akther et al., "Securing Tomorrow’s Digital World: Key Trends in Cybersecurity for 2024," Preprints, 2024. Available: https://www.preprints.org/frontend/manuscript/3b7e65d459d72f00fb762bac5a23397a/download_pub

[2] Sandeep Phanireddy, "AI-Driven Identity Access Management (IAM)," SSRN, 2025. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5257695
[3] Clement Daah et al., "Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework," MDPI, 2024. Available: https://www.mdpi.com/2079-9292/13/5/865
[4] Mingshan You, "An Adaptive Machine Learning Framework for Access Control Decision Making," Victoria University, 2022. Available: https://vuir.vu.edu.au/43688/1/YOU_Mingshan-Thesis_nosignature.pdf
[5] Kiran Kumar Suram, "Industry-Specific Applications of IAM and Infrastructure in Cloud Security," ResearchGate, 2025. Available: https://www.researchgate.net/publication/389216952_Industry-Specific_Applications_of_Iam_and_Infrastructure_in_Cloud_Security
[6] Jon Stern and Stuart Holder, "Optimizing Identity Management: Key Strategies for Effective Governance and Administration," ResearchGate, 2024. Available: https://www.researchgate.net/publication/382741790_OPTIMIZING_IDENTITY_MANAGEMENT_KEY_STRATEGIES_FOR_EFFECTIVE_GOVERNANCE_AND_ADMINISTRATION
[7] Srinivas Potluri, "Policy-Aware Secure Data Governance in Distributed Information Systems Using Explainable AI Models," International Journal of AI, BigData, Computational and Management Studies, 2025. Available: https://ijaibdcms.org/index.php/ijaibdcms/article/view/194
[8] Sandeep Rangineni et al, "An Analysis of Data Quality Requirements for Machine Learning Development Pipelines Frameworks," ResearchGate, 2023. Available: https://www.researchgate.net/publication/373821198_An_Analysis_of_Data_Quality_Requirements_for_Machine_Learning_Development_Pipelines_Frameworks
[9] Nitin Rane et al., "Artificial Intelligence and Machine Learning in Business Intelligence, Finance, and E-commerce: a Review," SSRN, 2024. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4843988
[10] Prableen Kaur et al., "Big Data and Machine Learning Based Secure Healthcare Framework," ScienceDirect, 2018. Available: https://www.sciencedirect.com/science/article/pii/S187705091830752X