International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V73I6P101

Volume 73 Issue 6, 1-6, June 2025

Original Article

The Role of AI & Machine Learning in Identity Governance

Yashasvi Sharma

Deloitte & Touche LLP, Richmond, USA.

Corresponding Author : yashasvishrm@gmail.com

Received: 12 April 2025 Revised: 17 May 2025 Accepted: 02 June 2025 Published: 16 June 2025

Abstract *- Organizations must prioritize identity governance as an essential element for cybersecurity and risk management because their digital ecosystems continue to grow. The growing use of cloud services, remote work, and third-party integrations has made managing user identities and access controls harder while maintaining compliance standards. Traditional Identity and Access Management (IAM) approaches face difficulties in efficient scaling, threat detection, and policy enforcement at runtime. Security gaps emerge from these limitations, which result in unauthorized access, insider threats, and non-compliance with regulations.*

Artificial Intelligence (AI) and Machine Learning (ML) are powerful modern identity governance tools that deliver real-time identity monitoring, predictive analytics, and automated decision-making capabilities. AI solutions process extensive identity data to identify unusual behaviors, which enables them to prevent security risks from becoming major breaches. Through behavioral analytics, AI systems create normal user activity baselines to detect suspicious actions, including unauthorized data access, privilege escalations, and suspicious login attempts. Real-time threat detection becomes possible through this proactive security approach. (Azhar, 2015) One of the key benefits of AI in identity governance is automated access control. Traditional Role-Based Access Control (RBAC) models often require manual updates and periodic reviews, leading to inefficiencies and errors. AI-powered identity governance solutions enable dynamic access provisioning, automatically granting or revoking permissions based on user behavior, job role changes, and contextual risk assessments. This approach guarantees that employees have correct access when needed, lowering the chance of privilege misuse.

This research explores how AI and ML technologies work together with identity governance systems through practical use cases, implementation methods, and real-world deployment examples. The research illustrates how AI-based identity governance systems improve security while enhancing operational efficiency and regulatory compliance across various sectors. Organizations must adopt AI-powered identity governance as cyber threats evolve to protect sensitive data, reduce insider threats, and optimize access control in contemporary IT systems. [7]

Keywords *- Identity Governance, Artificial Intelligence (AI), Machine Learning (ML), Access Control, Cybersecurity compliance*.

1. Introduction

Organizations use identity governance to manage user identities while controlling access rights and enforcing compliance policies across digital platforms. The expanding complexity of IT infrastructure because of cloud adoption, remote work models, and third-party system integrations makes securing identity management more difficult. The traditional governance solutions, which depend on manual workflows and rigid rule-based mechanisms, fail to meet the needs of dynamic regulatory requirements and new cybersecurity threats. The limitations in these systems lead to security vulnerabilities, which elevate the chances of unauthorized access, insider attacks and non-compliance with regulations.

AI and ML have revolutionized identity governance by enabling real-time threat detection through behavioral analysis and predictive analytics. These systems automate access control based on user context, reducing manual errors and improving security.

When abnormal behavior is detected—like off-hour access to sensitive data—they trigger adaptive responses such as security reviews or multi-factor authentication.

AI-driven identity governance simplifies audits by continuously logging and analyzing identity activities, giving organizations clear visibility into access patterns and regulatory compliance. [1] The research examines AI-driven identity governance operations through specific use cases, deployment methods, and real-world implementations. Organizations achieve modern security requirements through AI and ML, enhancing cybersecurity, efficiency, and compliance while strengthening their security posture.

2. Key Capabilities of AI & ML in Identity Governance:

Identity governance is a crucial cybersecurity element because it protects user access while maintaining regulatory requirements. The traditional manual and rule-based methods have become less effective because modern IT environments become more complex due to cloud adoption and remote work. [2]

Implementing Artificial Intelligence (AI) and Machine Learning (ML) has revolutionized identity governance through automated processes, predictive analytics, and real-time anomaly detection capabilities. Below, we explore five key aspects of AI in identity governance: Automated Access Management, Behavioral Analytics for Risk-Based Authentication, Anomaly Detection and Threat Mitigation, Intelligent Role and Privilege Management, and Compliance Automation.

2.1. Automated Access Management

Digital resources security relies on identity governance as it provides secure, efficient access to digital resources while maintaining regulatory compliance. The traditional identity management methods fail to adapt to the expanding complexity of identity management because organizations have adopted cloud computing remote work and multi-platform IT systems. [2]

Artificial Intelligence (AI) and Machine Learning (ML) have transformed identity governance through automated processes, predictive analytics, and real-time anomaly detection capabilities. AI-driven identity governance systems provide better security while making operations more efficient and improving compliance management capabilities. The following sections analyze AI technology's five essential identity governance applications: Automated Access Management, Behavioral Analytics for Risk-Based Authentication, Anomaly Detection and Threat Mitigation, Intelligent Role and Privilege Management, and Compliance Automation.

2.2. Behavioral Analytics for Risk-Based Authentication

The sophistication of identity-based cyber threats continues to rise because attackers use stolen credentials, phishing attacks, and brute force attempts to gain unauthorized access. The current authentication systems that use fixed passwords and rule-based access controls do not provide enough protection against identity-related breaches.

Implementing AI-powered behavioral analytics in authentication systems enables threat detection through behavioral pattern analysis of users combined with device information and contextual data. AI implements risk-based authentication through real-time risk assessments to make access decisions instead of depending on static credentials. AI Uses Behavioral Analytics for Authentication.

AI systems track login activities to detect abnormal patterns, including logins from unknown locations and new devices at unusual times. After detecting risky login attempts, the AI system initiates supplementary verification procedures through MFA and biometric authentication. AI performs continuous authentication by monitoring user activities after login verification to confirm their identity throughout the session. The system uses AI to detect anomalies which can trigger either session termination or re-authentication. The AI-powered risk-based authentication system adapts to real-time threats through its risk assessments, decreasing the chances of credential theft and account takeovers. [3]

2.3. Anomaly Detection and Threat Mitigation

Organizations must obtain immediate access activity visibility because cyber threats advance quickly to detect unauthorized access, privilege escalations, and data breaches. Traditional security models depend on predefined rules that fail to detect newly emerging threats effectively. AI threat detection operates through continuous access log analysis to detect anomalies and automatically respond to potential security threats. How AI Detects and Mitigates Threats

Analyzing large identity data sets by AI systems reveals behavioral deviations outside typical patterns. The system identifies suspicious behavior when an employee who normally accesses files from one department tries to access confidential data from another department. The system uses AI to initiate automated responses after detecting anomalies through the following actions: Locking an account. Revoking session access. Enforcing additional authentication. Notifying security teams. AI-based systems learn from historical data to improve threat detection, reducing unnecessary alerts that disrupt legitimate users. Organizations can stop security incidents at their beginning through AI-powered anomaly detection systems that protect both financial assets and organizational reputation.

2.4. Intelligent Role and Privilege Management

The accumulation of excessive permissions by users throughout time represents a widespread security challenge that increases insider threat risks. The traditional Role-

Based Access Control (RBAC) system grants access through predefined job roles, resulting in security gaps because users end up with more permissions than needed.

The AI system Intelligent Role and Privilege Management grants users only essential permissions through the principle of least privilege. How AI Optimizes Role and Privilege Management.

The AI system tracks user access patterns and job functions to prevent users from keeping unnecessary privileges after changing roles [4]. The AI system identifies permissions that are not used or exceed necessary levels and suggests removing them to decrease security threats. The process of access reviews through traditional methods depends on manual work and produces frequent mistakes. AI technology performs access reviews automatically to maintain proper access permissions throughout time. Organizations achieve better security and simplified role distribution and privilege protection through AI-based privilege management systems. [5]

2.5. Compliance Automation

Organizations that manage sensitive data and personally identifiable information (PII) must focus on regulatory compliance as their top priority. GDPR, HIPAA, SOX, and ISO 27001 compliance requirements enforce strict identity and access management (IAM) controls. Manual compliance monitoring takes too much time and produces errors, making maintaining continuous compliance with security regulations challenging.

AI-powered compliance automation enables regulatory compliance through automatic identity data mapping to compliance frameworks and real-time audit report generation. How AI Enhances Compliance Automation. The AI system tracks all identity-related actions by continuously logging access activities, ensuring complete audit documentation. The AI system checks access permissions against industry regulations by mapping to verify policy alignment with regulatory standards. The system takes immediate corrective action through AI detection of non-compliance by revoking unauthorized access or sending alerts to compliance teams. AI automation of compliance tasks decreases the IT team's workload so that they can concentrate on essential security projects. Organizations achieve regulatory compliance through AI-driven automation, decreasing compliance risks and streamlining audit procedures. [6]

3. Implementation of AI & ML in Identity Governance

3.1. Integration with IAM and SIEM Systems

AI-driven identity governance solutions improve security through their ability to connect with Identity and Access Management (IAM) and Security Information and Event Management (SIEM) platforms. AI and machine learning enable these solutions to automate identity lifecycle management, enforce least privilege access, and detect anomalies in real-time. The IAM integration provides secure user provisioning adaptive authentication and policy enforcement capabilities, while SIEM integration enables continuous monitoring, threat intelligence, and rapid incident response. The combined system enables organizations to maintain strong security oversight while streamlining compliance and actively reducing identity-based cyber threats, improving operational efficiency and cybersecurity resilience. [7]

3.2. Continuous Identity Risk Assessment

Identity security benefits from real-time risk assessments because these systems evaluate user access through behavioral analytics device trust scores and contextual data in real-time. AI models evaluate login location, access patterns, and device compliance to identify potential threats and anomalies. The system implements adaptive authentication and real-time access adjustments to stop unauthorized access and decrease insider and credential-based threats.

3.3. AI-Driven Policy Enforcement

Machine learning systems enforce access policies through real-time analysis of user behavior and role modifications. The system identifies security threats to modify access permissions, initiate additional authentication steps, or remove access rights when necessary. The adaptive security method eliminates rigid rules to enhance security measures, operational efficiency, and regulatory compliance. [8]

3.4. Automated Identity Lifecycle Management

AI streamlines identity management through automated user access provisioning and de-provisioning based on role, behavior and organizational needs. AI systems predict access privileges for new employees by analysing job role similarities and historical data, eliminating the need for manual permission assignment. AI systems track employee access usage patterns to identify irregularities that lead to removing unused or excessive permissions and minimize security threats. The system removes access rights instantly during offboarding procedures to stop unauthorized access. The adaptive system improves security standards while reducing human mistakes and maintaining compliance with identity governance policy.

4. Case Studies and Industry Applications:

4.1. Case Study 1: Financial Sector's Use of ML for Fraud Prevention

The global bank faced difficulties detecting insider threats and fraudulent transactions because of its high daily financial activity volume. The traditional security systems

failed to detect complex fraud patterns in real-time operations. The bank implemented machine learning behavioral analytics within its identity governance framework to examine transaction patterns, user behaviors, and access anomalies. The AI system detected suspicious activities while simultaneously modifying authentication protocols for users who posed a high risk. The system achieved 98% accuracy in detecting insider threats and fraudulent transactions, resulting in customer account protection and improved overall security. [9]

4.2. Case Study 2: AI-Powered Compliance in a Multinational Corporation

The multinational technology enterprise encountered mounting demands to fulfil GDPR and SOX data protection regulations. The organization struggled with time-consuming manual compliance reporting that contained frequent human mistakes. The company implemented an AI-powered identity governance system that performed automated compliance audits through regulatory requirement-based access privilege mapping. The AI system produced reports that delivered immediate access control violation information to simplify the audit process. The company achieved a 60% reduction in audit preparation time through this solution, which maintained continuous compliance and reduced regulatory fine risks. The case demonstrates how AI technology improves governance efficiency without compromising strict security protocols. [10]

5. Challenges and Limitations

5.1. Data Privacy Concerns

The system uses large amounts of user data to analyze login patterns, access histories, and behavioral trends to detect security threats and anomalies. The collection and processing of such data creates major privacy and security issues. User privacy becomes vulnerable when unauthorized parties access data, data breaches occur, or when sensitive identity information is misused. Organizations must establish strict encryption protocols, data anonymization methods, and compliance with GDPR and CCPA privacy regulations to reduce risks. AI-driven monitoring enhances security through transparent data collection practices and user consent mechanisms, which protect individual privacy rights and confidential information from cyber threats.

5.2. False Positives

Implementing machine learning models in identity governance depends on behavioral patterns to detect anomalies, yet these systems can generate false positives and fail to identify subtle threats. [11] Security actions that block legitimate users or overlook actual risks become necessary due to inaccurate alerts. Model tuning needs to occur continuously through real-time data and feedback to enhance accuracy. Security teams must validate critical alerts through human oversight to refine AI-driven policies. Organizations achieve better security by combining automated detection systems with expert intervention, enabling them to maintain operational efficiency and precision. The model's capacity to differentiate normal from malicious activity improves through regular updates and adaptive learning. (Maher, Bhable, Lahase, & Nimbhore, 2022).

5.3. Integration Complexity

Implementing AI-driven identity governance requires integration with current IT and security systems, including Identity and Access Management (IAM), Security Information and Event Management (SIEM), and endpoint security solutions. Real-time data exchange through seamless integration enables automated access control and threat detection. The integration of AI with legacy systems may need customized APIs or middleware solutions because of compatibility issues. The implementation of proper planning and phased deployment, together with cross-team collaboration, minimizes disruptions. Organizations can achieve better security and simplified identity management and compliance through interoperability, enabling them to use AI capabilities to improve governance and decrease human involvement in identity security processes.

6. Future Prospects

AI and ML will transform identity governance through predictive security, automated verification, and decentralized identity management. The technologies will shift from traditional rule-based systems to adaptive models that analyze behavior and access history and context to detect real-time risks. The proactive method will enhance decision-making, transparency, and threat prevention as cyber risks become more complex.

Self-learning AI frameworks will transform identity governance through their ability to adapt to evolving cyber risks and organizational changes. These systems will improve their accuracy and resilience through continuous training and autonomous learning for their evolution. Combining reinforcement learning with deep neural networks enables these frameworks to automatically update access policies, reducing human involvement and enhancing security performance.

Implementing blockchain-based decentralized identity verification represents a vital innovation that will reshape identity governance systems. Traditional identity management systems store their data in centralized databases, creating security risks through data breaches and insider attacks. Through blockchain technology, users gain secure decentralized identity verification capabilities, which let them manage their credentials independently from any central authority. AI systems will boost these systems through biometric authentication, behavioral analysis, and real-time risk assessments to decrease fraud attempts and

unauthorized access. (Leander, 2024) The future will focus on explainable AI (XAI) to enhance decision-making processes. The main obstacle to AI-driven identity governance systems today is the "black box" characteristic of AI models, which makes security teams unable to understand the reasoning behind access decisions. Implementing Explainable AI will improve AI-driven security frameworks by delivering human-understandable explanations about risk scores and policy enforcement and authentication decisions. Implementing Explainable AI will boost trust in AI-based identity governance systems while helping organizations meet regulatory obligations.

AI and ML technology advancement will lead identity governance systems to become more proactive, intelligent, and resilient, protecting digital identities against growing complex threats.

7. Conclusion

AI and Machine Learning (ML) will transform identity governance security through automated verification processes and advanced access management systems in the future. The evolution of predictive identity governance will surpass traditional rule-based systems by analyzing user behavior and past access data and environmental cues in real time to prevent breaches as cyber threats become more complex. Self-learning frameworks will enhance adaptability through the continuous evolution of AI systems without requiring manual updates. The systems will use deep and reinforcement learning to automatically modify access controls, minimising the need for human involvement. Organizations will achieve better security, proactive threat detection, and operational efficiency.

Combining blockchain-based decentralized identity systems with AI-driven biometrics and explainable AI technology provides enhanced security features, user control, and transparency while minimizing data breach risks. Security teams face challenges understanding reasons for access decisions because many current AI models operate as "black boxes." XAI delivers transparent insights about risk assessments and policy enforcement, which builds trust in AI-driven security measures and maintains compliance with regulatory frameworks.

The final benefit of automation will be the simplification of identity management operations, decreasing administrative workloads. Organizations can use AI-driven solutions to automate user onboarding privilege assignments and compliance reporting, enabling them to enforce strict security controls efficiently. The future development of AI and ML technology will lead identity governance to become more predictive, adaptive, and resilient, thus providing strong protection against cyber threats.

Funding Statement

This paper is self-funded. No organization is involved.

References

[1] Ryan K.L. Ko, "Cyber Autonomy: Automating the Hacker–Self-Healing, Self-Adaptive, Automatic Cyber Defense Systems and Their Impact on Industry, Society, and National Security," *Emerging Technologies and International Security*, Routledge, pp. 173-191, 2020. [Google Scholar] [Publisher Link]

[2] Joshua Kalin, "*Defense Against the Adversarial Arts: Applying Green Team Evaluations to Harden Machine Learning Algorithms from Adversarial Attacks*," Auburn University Dissertations & Theses, pp. 1-24, 2022. [Google Scholar] [Publisher Link]

[3] Blessing Guembe et al., "The Emerging Threat of AI-Driven Cyber Attacks: A Review," *Applied Artificial Intelligence*, vol. 36, no. 1, pp. 1-34, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Chao Zhang et al., "Ethical Impact of Artificial Intelligence in Managerial Accounting," *International Journal of Accounting Information Systems*, vol. 49, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Elliot Lyroi et al., "AI-Powered Wearables: Transforming Remote Patient Monitoring," 2025. [Google Scholar]

[6] Senthil Murugan Nagarajan et al., "Artificial Intelligence-Based Zero Trust Security Approach for Consumer Industry," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 3, pp. 5411-5418, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Jayati Doshi, "Live Log analysis using Integrated SIEM and IDS using Machine Learning," *Institute of Technology*, 2024. [Google Scholar] [Publisher Link]

[8] Jorn Erbguth, "*A Framework for Long-Term Revocable Credentials*," Ph.D. Dissertation, University of Geneva, Switzerland, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Oluwabusayo Adijat Bello, and Komolafe Olufemi, "Artificial Intelligence in Fraud Prevention: Exploring Techniques and Applications Challenges and Opportunities," *Computer Science & IT Research Journal*, vol. 5, no. 6, pp. 1505-1520, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] V. Veeramachaneni, "Integrating Zero Trust Principles into IAM for Enhanced Cloud Security," *Recent Trends in Cloud Computing and Web Engineering*, vol. 7, no. 1, pp. 78–92, 2025. [Google Scholar]

[11] Ugochukwu Ikechukwu Okoli et al., "Machine Learning in Cybersecurity: A Review of Threat Detection and Defense Mechanisms," *World Journal of Advanced Research and Reviews*, vol. 21, no. 1, pp. 2286-2295, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] S. K. Maher, S. G. Bhable, A. R. Lahase, and S. S. Nimbhore, "AI and Deep Learning-Driven Chatbots: A Comprehensive Analysis and Application Trends," *Proceedings of the 6th International Conference on Intelligent Computing and Control Systems*, Madurai, India, pp. 994-998, 2022. [CrossRef] [Google Scholar] [Publisher Link]