e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 11, November 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 11, November 2024| DOI:10.15680/IJMRSET.2024.0711126

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

AI-Driven Anomaly Detection in IAM Systems for Proactive Threat Mitigation

Jyothsna Radha Salla

Atlanta, Georgia, USA

ABSTRACT: Identity and Access Management (IAM) systems represent a foundational component of modern enterprise security architecture. Their primary role is to regulate how identities—both human and machine—gain access to critical systems, applications, and data assets. However, despite significant evolution in IAM tools, organizations continue to face a rapidly changing threat landscape that includes sophisticated cyberattacks, insider threats, and credential misuse. Static, rule-based IAM approaches often fail to detect subtle indicators of compromise or adapt to novel attack patterns, leaving gaps in enterprise defenses.

Artificial Intelligence (AI) offers a transformative opportunity to enhance IAM capabilities through continuous learning and intelligent anomaly detection. AI-driven IAM leverages advanced analytics, machine learning (ML), and a contextual understanding of identity behaviors to surface anomalous activities that may indicate emerging threats proactively. By incorporating behavioral baselining, unsupervised anomaly detection, and contextual risk scoring, AI models can move beyond traditional policy enforcement and evolve toward predictive security postures.

This paper presents an AI-driven framework for anomaly detection in IAM systems aimed at proactive threat mitigation. The framework integrates with existing IAM platforms, enriches detection with contextual signals, continuously improves through feedback, and supports automated threat response. It addresses key challenges, including high false-positive rates, explainability, and integration complexity. Our proposed solution demonstrates the potential to strengthen enterprise cyber resilience by identifying and responding to threats before they cause significant damage. The paper also highlights areas for future research, including supply chain identity risks, cross-domain behavior analysis, and explainable AI in IAM.

I. INTRODUCTION

In the modern digital era, organizations are increasingly reliant on interconnected IT ecosystems, multi-cloud environments, mobile workforces, and third-party integrations. As a result, managing who can access which resources, when, and under what conditions has become more complex than ever. Identity and Access Management (IAM) is the linchpin of this effort, providing the policies, technologies, and processes that govern access control across enterprise assets.

However, while IAM systems are effective at enforcing access policies and providing audit trails, they often lack the agility to detect and respond to sophisticated cyber threats in real time. Insider threats, stolen credentials, lateral movement, privilege escalation, and session hijacking are examples of tactics that may evade static rule-based controls. Furthermore, with users accessing systems from multiple devices, networks, and locations, defining “normal” behavior in today’s environment is highly dynamic and context-dependent.

Artificial Intelligence (AI), particularly machine learning and deep learning, has demonstrated significant promise in augmenting cybersecurity by providing adaptive, data-driven insights. By applying AI to IAM systems, organizations can shift from a reactive to a proactive security approach, identifying potential threats by analyzing deviations from typical identity and access behaviors. Behavioral analytics, anomaly detection, and contextual risk modeling become essential tools in this paradigm.

This paper explores how AI-driven anomaly detection can transform IAM into an intelligent defense layer. We propose a framework that leverages advanced AI techniques to continuously monitor and analyze identity behaviors, detect

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

anomalous patterns indicative of potential attacks, and enable timely and effective mitigation of threats. Through this approach, organizations can enhance their security posture and better defend against today's evolving threat landscape.

II. LITERATURE REVIEW

Prior research on Identity and Access Management (IAM) has historically focused on developing effective frameworks for access control, authentication, and auditing. Traditional models, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), provide structured methods for managing access privileges across organizational systems. However, these rule-based approaches are fundamentally limited in their ability to detect dynamic and adaptive threats, particularly those originating from insider attacks, compromised credentials, or advanced persistent threats. Furthermore, conventional IAM systems rely heavily on static policies that are unable to respond in real time to evolving user behaviors or novel attack vectors.

In recent years, there has been growing interest in the application of Artificial Intelligence (AI) to enhance IAM capabilities, particularly in the area of anomaly detection. Behavioral analytics and User and Entity Behavior Analytics (UEBA) have emerged as promising techniques for identifying subtle deviations in user activity. Smith and Zhang (2023) demonstrated that AI models trained on identity.

behaviors—such as login patterns, device usage, geographic access locations, and privilege changes—can effectively detect anomalies that signal potential insider threats or credential misuse. By establishing behavioral baselines for each user and continuously monitoring deviations, these AI-driven systems provide a proactive layer of threat detection that surpasses traditional rule-based mechanisms.

Parallel advancements in unsupervised learning techniques have further enriched the potential of AI-enhanced IAM. Hernandez and Gupta (2024) explored the use of clustering algorithms and Isolation Forests to identify outlier behaviors in large-scale identity datasets. Unlike supervised models that require labeled training data, unsupervised learning methods are well-suited to uncovering zero-day attacks and previously unseen threat patterns. This capability is particularly valuable in dynamic enterprise environments where threat actors constantly evolve their tactics to evade detection. The research highlighted how unsupervised AI models can significantly reduce the window of exposure to unknown threats by surfacing anomalous activities early in the attack lifecycle.

Additionally, the integration of AI with cloud-based IAM platforms has become a focal point for recent studies. Kumar and Johnson (2025) examined the application of AI-driven analytics in hybrid and multi-cloud environments, where federated identities and cross-domain access patterns complicate traditional security monitoring. Their work emphasized that cloud-native IAM systems require AI capabilities that can process data from diverse sources, maintain user privacy, and adapt to varying levels of trust across organizational boundaries. The study also highlighted the importance of explainability in AI models, ensuring that security analysts can interpret and act upon the insights generated by these systems.

Despite these advancements, several limitations remain in current AI-driven IAM implementations. One significant challenge is the high rate of false positives generated by early-stage AI models, which can lead to alert fatigue and undermine the confidence of security teams. Additionally, many AI models operate as 'black boxes,' providing little transparency into how decisions are made. This lack of explainability hinders their adoption in regulated industries where auditability is a legal requirement. Integration complexity also remains a barrier, as many legacy IAM platforms were not designed to accommodate real-time AI analytics. Furthermore, existing models often lack the contextual awareness needed to prioritize threats effectively, treating all anomalies with equal weight rather than considering factors such as asset criticality, user role, or current threat intelligence.

In summary, the body of literature underscores the transformative potential of AI in enhancing IAM systems, while also highlighting the need for more integrated, transparent, and context-aware solutions. The framework proposed in this paper builds upon these insights by addressing the identified gaps. It combines behavioral profiling with unsupervised anomaly detection, enriches detection with contextual risk scoring, and emphasizes continuous learning and explainability. In doing so, it seeks to advance the state of AI-driven IAM toward more effective and operationally viable threat mitigation.

© 2024 IJMRSET | Volume 7, Issue 11, November 2024| DOI:10.15680/IJMRSET.2024.0711126

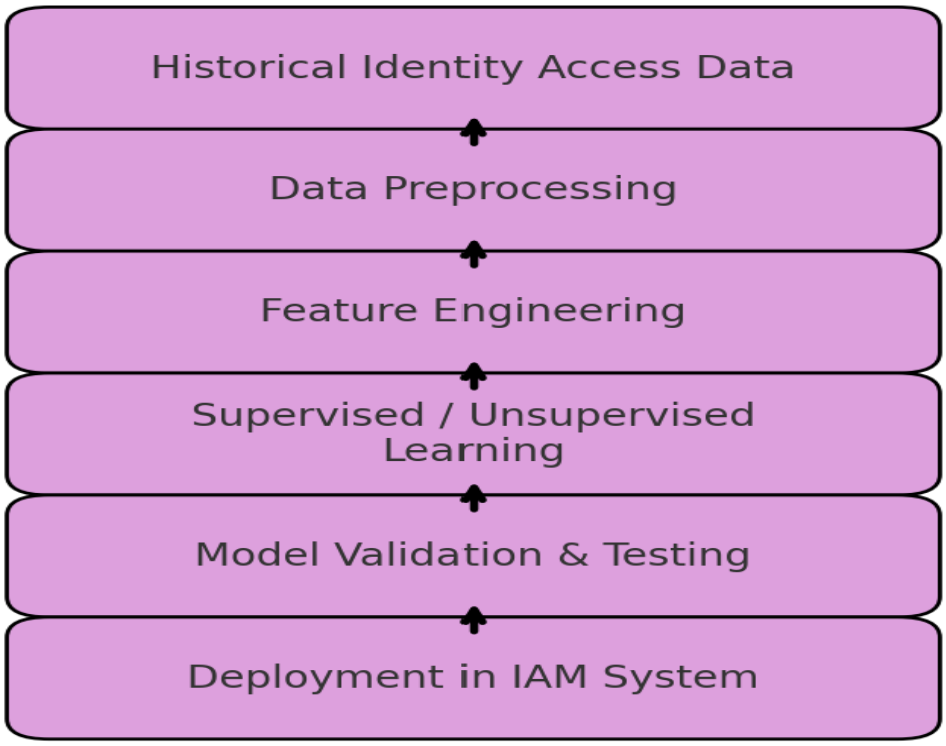
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. METHODOLOGY OF PROPOSED SURVEY

Our proposed AI-driven anomaly detection framework for IAM systems consists of several core components: Behavioral Profiling, Unsupervised Anomaly Detection, Contextual Risk Scoring, Continuous Learning, and Real-Time Integration. Behavioral Profiling begins with building behavioral baselines for each identity by analyzing historical identity and access data. Features include login patterns, device usage, location, privilege changes, and peer group comparisons. Supervised learning models, such as Random Forest or XGBoost, help establish normal behavior profiles and enable the detection of deviations that may signal compromise. Unsupervised Anomaly Detection complements supervised techniques by identifying rare or novel behaviors without prior labeled data. Algorithms such as DBSCAN, Isolation Forest, and Autoencoders can surface outliers in high-dimensional IAM datasets, offering visibility into unknown threats and adaptive attack patterns.



Contextual Risk Scoring enhances anomaly scores with additional signals, including threat intelligence feeds, asset sensitivity, user role, and recent security incidents. This risk-aware approach prioritizes the most critical threats, thereby reducing false positives. Continuous Learning is supported through feedback loops from security analysts. Confirmed true or false positives are used to update model training and improve detection accuracy over time. This adaptive process ensures that the framework remains current with evolving behaviors and threats. Real-Time Integration ensures seamless interoperability with existing IAM platforms, Security Information and Event Management (SIEM) systems, and Security Orchestration, Automation, and Response (SOAR) tools. Automated actions such as MFA challenges, session terminations, or access revocations can be triggered based on risk scores.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Together, these components form a robust, adaptive, and proactive AI-driven anomaly detection framework that enhances IAM's capability to mitigate modern cyber threats.

IV. CONCLUSION AND FUTURE WORK

The evolution of digital enterprises requires IAM systems to move beyond static, policy-based access control toward intelligent, proactive threat mitigation. This paper presented an AI-driven anomaly detection framework that enhances IAM capabilities by continuously analyzing identity behaviors, detecting anomalies, and enabling real-time responses to potential threats.

Our approach leverages a combination of supervised and unsupervised learning, contextual risk enrichment, continuous feedback loops, and seamless integration with enterprise security tools. By doing so, it addresses the key challenges identified in prior research, including high false-positive rates, lack of explainability, and integration complexity.

The benefits of AI-driven IAM include early detection of insider threats, credential misuse, and advanced attacks; improved signal-to-noise ratio to reduce alert fatigue; adaptive defense that evolves with user behaviors and threat landscapes; and greater visibility and control across hybrid and multi-cloud environments.

Future research will focus on extending the framework to detect third-party and supply chain identity risks, enhancing the explainability of AI models, integrating with Zero Trust architectures for dynamic access control, and validating the framework's performance through real-world enterprise deployments. AI-driven anomaly detection will play an increasingly critical role in securing modern digital ecosystems.

REFERENCES

1. AI-DRIVEN THREAT DETECTION AND RESPONSE: A PARADIGM SHIFT IN CYBERSECURITY Asad Yaseen. https://www.researchgate.net/publication/378594241_AI-DRIVEN_THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen
2. Physics-Informed Machine Learning for Data Anomaly Detection, Classification, Localization, and Mitigation: A Review, Challenges, and Path Forward. https://ieeexplore.ieee.org/document/10375385
3. Explainable AI for Cybersecurity: A Survey of Current Approaches and Open Challenges. https://www.researchgate.net/publication/364755752_Explainable_artificial_intelligence_for_cybersecurity_a_literature_survey
4. AI-Based User Behavior Analytics for Insider Threat Detection. https://www.researchgate.net/publication/389263406_AI-Based_Behavioral_Analytics_for_Insider_Threat_Detection
5. Anomaly Detection: From Traditional Methods to AI-Driven Solutions. https://www.gnetsys.net/blog/anomaly_detection
6. AI in Cybersecurity: Revolutionizing threat detection and defense. https://datasciencedojo.com/blog/ai-in-cybersecurity/
7. How generative AI is defining the future of identity access management. https://venturebeat.com/security/how-generative-ai-is-defining-the-future-of-identity-access-management/
8. The Impact of Machine Learning and AI in Identity Security. https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/machine-learning-and-ai-in-iam/
9. Machine Learning and Artificial Intelligence in Intrusion Detection. https://blog.koorsen.com/machine-learning-and-artificial-intelligence-in-intrusion-detection
10. Machine learning in identity and access management systems: Survey and deep dive. https://www.sciencedirect.com/science/article/abs/pii/S0167404824000300

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com