DeepScience

Artificial Intelligence-Assisted Identity and Access Management

Esther Chinwe Eze

Artificial Intelligence-Assisted Identity and Access Management

Esther Chinwe Eze

University of North Texas, United States

DeepScience

Published, marketed, and distributed by:

Deep Science Publishing
USA | UK | India | Turkey
Reg. No. MH-33-0523625
www.deepscienceresearch.com
editor@deepscienceresearch.com
WhatsApp: +91 7977171947

ISBN: 978-93-49307-70-4

E-ISBN: 978-93-49307-51-3

https://doi.org/10.70593/978-93-49307-51-3

Citation: Eze, E. C. (2025). *Artificial Intelligence-Assisted Identity and Access Management*. Deep Science Publishing. https://doi.org/10.70593/978-93-49307-51-3

The publishers, authors, and editors are not responsible for errors or omissions, or for any consequences arising from the application of the information presented in this book, and make no warranty, express or implied, regarding the content of this publication. Although the publisher, authors, and editors have made every effort to ensure that the content is not misleading or false, they do not represent or warrant that the information-particularly regarding verification by third parties-has been verified. The publisher is neutral with regard to jurisdictional claims in published maps and institutional affiliations. The authors and publishers have made every effort to contact all copyright holders of the material reproduced in this publication and apologize to anyone we may have been unable to reach. If any copyright material has not been acknowledged, please write to us so we can correct it in a future reprint.

Preface

As businesses come to appreciate the need for Identity and Access Management (IAM) to protect their environments, they ensure that only permitted users can access sensitive data and systems. Growing companies need robust IAM solutions that enable them to handle user authentication, permissions, and access control more effectively, therefore underlining their need. Still, security breaches have been a major headache, even with the advances in IAM technologies. Cybercriminals are constantly improving their techniques to bypass conventional IAM policies, which has resulted in many security incidents and data breaches. Dealing with these security issues offers a promising solution by integrating Artificial Intelligence (AI) and Machine Learning (ML). By helping IAM systems recognize possible attacks that traditional methods could miss, AI and ML technologies provide sophisticated features for spotting unusual behavior patterns. Once an IAM attack is underway, these tools may help better identify unauthorized access, privilege escalation, and other suspect behavior. Machine learning algorithms are particularly well suited for this task as they can constantly learn and adjust from information, enhancing their precision over time. This study investigates the use of ML algorithms to improve the security of IAM systems, concentrating mainly on identifying attacks aimed at IAM servers, including OpenIAM and WSO2. Using Python code and WEKA, the study applies and experiments with different machine learning approaches, such as classification algorithms that can discern atypical behavioral patterns that point to IAM assaults. The research seeks to raise the detection rate of these assaults using machine learning, therefore giving another level of security for IAM systems. The study measures the performance of the suggested solution and its ability to spot possible risks using thorough dataset development, training, and validation of the models. The results of this study underline how combining IAM systems with machine learning could provide more reactive, real-time protection from emerging threats. Although challenges, including data constraints and the difficulty of feature selection, still exist, the findings indicate that artificial intelligence and machine learning might greatly strengthen the resilience of IAM systems. Further investigation could refine the models for even higher precision and broaden their use to other security situations, thereby adding to the larger field of cybersecurity.

Esther Chinwe Eze

Contents