Deep Science Publishing
https://doi.org/10.70593/978-93-49307-51-3_5

DeepScience
Open Access Books

Chapter 5

Conclusion and future directions for machine learning enhanced Identity and Access Management (IAM) systems

Esther Chinwe Eze

University of North Texas, United States

5.0 Conclusion

This section presents a summary of the key findings and conclusions obtained during the implementation of the project. The findings and conclusions are based on all the essential activities and tasks that contributed to the successful outcome of the project. It also documents a reflection of some of the lessons learned during the project as well as the achievements and further research work. The project aims to utilize ML capabilities in the Identity and access management process to make it more efficient, and resilient to IAM attacks. The project commenced by analysing the requirements of the system which was gathered at the investigation stage. Afterward, a careful design process was carried out. The implementation of the project followed after the design and all the requirements were converted to a working process. Coding for ML was done using the R programming language. Evaluation and results of the four (4) classifiers were presented. From the activities involved in the design, implementation, evaluation, and results above, It is safe to state that the aim and objectives including the functional and non-functional requirements of the project were met having carried out each process successfully.

5.1 Reflection

In retrospect, a project of this nature is quite tasking and requires extra effort and relevant knowledge. However, the project was quite interesting, carrying out the project to the end required extensive study and research as well as the application of relevant computing skills. Much effort and time were required to solve the challenges that were faced from the start of the project (investigation stage) to the implementation stage**.**

5.2 Legal, Ethical, Social and Professional Risk

The undertaking of this project was conducted with careful consideration of ethical and related issues. No legal and ethical issues arose during this project. The IAM dataset used was generated by the researcher to mimic real-life data, however, the data was anonymized so no personal or sensitive details were included. Likewise, all development tools used; R studio, R, WEKA, excel, and WSO2 server are open source software that are free and available for use and do not require any license to be used. Therefore, no licensing issues were faced during the project.

5.3 Recommendation and Further Work

The project was designed and implemented according to the expected requirements, however, there is still room for improvement and enhancement. Further research work in this area can extend the functionalities of the selected algorithm thereby making room for optimum results. Although the Random Forest (RF) model gave the highest accuracy of 100% it is still not at its best and improvements must be made. To improve the accuracy of the RF model, the number of trees had to be increased, and also the quality of the dataset can increase the accuracy of the model thereby making it reliable and fit for IAM attack detection. Conclusively, there is a promising opportunity for AI to assist in addressing some of the security issues faced by traditional IAM. However, this project only focused on the user authentication and privilege aspect of IAM, and a conclusion is based on simulated activities of users with limited resources. In the future, the application of skills, resources, and more experiments can be applied to explore the vast capabilities of IAM to achieve more innovative solutions.

References

Aboukadri, S., Ouaddah, A., & Mezrioui, A. (2024). Machine learning in identity and access management systems: Survey and deep dive. Computers & Security, 139(103729), 103729. https://doi.org/10.1016/j.cose.2024.103729

Banday, M. T., & Mehraj, S. (2017). Directory services for identity and access management in cloud computing. 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT).

Biscoe, C. (2017). Verizon's 2017 Data Breach Investigations Report. IT Governance UK Blog; IT Governance. https://www.itgovernance.co.uk/blog/verizons-2017-data-breach-investigations-report

Cloudflare. (2021). What is a phishing attack. Cloudflare.com. https://www.cloudflare.com/es-la/learning/access-management/phishing-attack.

De Groot, J. (2019). What is Identity and Access Management (IAM)? Digitalguardian.com. https://digitalguardian.com/blog/what-identity-and-access-management-iam

Fajar, P. (2020). Brute force attack demonstration with hydra. Steemit. https://steemit.com/technology/@fajar.purnama/brute-force-attack-demonstration-with-hydra

Fisher, N. (2018). 5 identity attacks that exploit your Broken Authentication. Okta.com. https://www.okta.com/blog/2018/03/5-identity-attacks-that-exploit-your-broken-authentication/

Ganesh The Awesome. (2020). What is identity and access management and why it's important for modern companies. GlobalDots. https://www.globaldots.com/resources/blog/what-is-identity-and-access-management-and-why-its-important-for-modern-companies/

George. (2023). Cyber security strategy: How to stay ahead of new threats. Cybersecurity UK 🛡️ | Stygian Cyber Security | Safeguarding Your Digital World 🖥️. https://stygian.co.uk/cyber-security-strategy/

Identity Management Institute. (2022). Key characteristics of identity and access management solutions. Identity Management Institute®; Identity Management Institute. https://identitymanagementinstitute.org/key-characteristics-of-identity-and-access-management-solutions/

Indu, I., Anand, P. M. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering Science and Technology an International Journal, 21(4), 574–588. https://doi.org/10.1016/j.jestch.2018.05.010

Jason, B. (2016). How to Use Machine Learning Algorithms in Weka. Machinelearningmastery.com. https://machinelearningmastery.com/use-machine-learning-algorithms-weka/

LogonBox. (2017). Artificial Intelligence – is it the Answer for Identity Management? LogonBox; LogonBox Ltd. https://www.logonbox.com/content/artificial-intelligence-answer-identity-management/

Mayuri, D., & Sridevi, K. (2017). Identity and access management: concept, challenges, solutions. International Journal of Latest Trends in Engineering and Technology, 8(1). https://doi.org/10.21172/1.81.039

Miller, D. (2020). What is Identity Access Management? Varonis.com. https://www.varonis.com/blog/what-is-iam/

Mohr, F., & van Rijn, J. N. (2022). Learning curves for decision making in supervised machine learning: A survey. In arXiv [cs.LG]. http://arxiv.org/abs/2201.12150

Phil, S., & Gittlen, S. (2020). What is Identity and Access Management? Guide to IAM. Search Security; TechTarget. https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system

Porwal, U., & Mukund, S. (2018). Credit card fraud detection in e-commerce: An outlier detection approach. In arXiv [cs.LG]. http://arxiv.org/abs/1811.02196

Sampath, D. (2022). Application of Machine Learning in models. Royal Book Publishing.

Strom, D. (2021). What is IAM? Identity and access management explained. CSO Online. https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html

Thakur, M. A., Parvat, T. J., & Walunj, V. S. (2021). Data security using directory server in identity and access management system. In ICT Analysis and Applications (pp. 73–84). Springer Singapore.

The Hacker News. (2024). China-linked hackers compromise ISP to deploy malicious software updates. The Hacker News. https://thehackernews.com/2024/08/china-linked-hackers-compromise-isp-to.html

WSO. (2021). Identity Server Documentation. Wso2.com. https://is.docs.wso2.com/en/latest/get-started/overview/

Wu, Y., Wei, D., & Feng, J. (2020). Network attacks detection methods based on deep learning techniques: A survey. Security and Communication Networks, 2020, 1–17. https://doi.org/10.1155/2020/8872923

Xu, X., Liu, Q., Zhang, X., Zhang, J., Qi, L., & Dou, W. (2019). A blockchain-powered crowdsourcing method with privacy preservation in mobile environment. IEEE Transactions on Computational Social Systems, 6(6), 1407–1419. https://doi.org/10.1109/tcss.2019.2909137