ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Enhancing Role-Based Access Control through Artificial Intelligence and Machine Learning

Vamsy Priya Anne

Department of Computer Information Systems, Grand Valley State University, USA

ABSTRACT

In this research paper, an attempt has been made to discuss the implementation of AI & ML to improve the existing RBAC systems. Having used a qualitative research approach, the study evaluates the secondary materials from scholarly articles and industrial white papers found in Google Scholar and ProQuest. The research shows that AI and ML may improve RBAC by dynamically changing responsibilities, identifying dangers, and reducing false alarms. AI enables predictive analysis to avoid security risks and analytical power to oppose and adapt to working situations. AI and RBAC integration improve security and system responsiveness by standardizing the working process. The paper recommends more research on algorithms and ethics, as well as industry-specific solutions. These enhancements should make RBAC more versatile, efficient, and secure for allowing and controlling access levels in varied organizational situations.

***Corresponding author**

Vamsy Priya Anne, Department of Computer Information Systems, Grand Valley State University, USA.

Received: February 05, 2024; **Accepted:** February 09, 2024; **Published:** February 12, 2024

Keywords: Role-Based Access Control (RBAC), Artificial Intelligence (AI), Machine Learning (ML), Cybersecurity, Access Control Systems

Introduction

Background

Knowing the historical evolution of RBAC since the beginning of the use of this method in the 90s gives a rich understanding of the improvements made to this model. Originally intended to implement information access control based on the organizational position of a user, RBAC has evolved into a key method for effectively regulating permissions and preventing intrusion. However, with such complex and dynamic systems prevailing more prominently in digital environments, a system like RBAC that is centralized and hierarchical has its issues related to flexibility, scalability and real-time risk analysis.

This is the case because the new advancement of AI and ML in RBAC systems can solve these challenges. By incorporating a learning mechanism, AI and ML will allow the access controls to adjust the facets of security based on the real-time data that is obtained rather than having to rely on conventional roles and permissions [1].

Aim Objectives and Research Questions

Research Aim

This study aims to find out how on the use of AI and in particular, ML as enhancement on conventional RBAC systems.

Research Objectives

- To explore the existing and potential integration of the AI technologies in the current and future research on RBAC.
- To understand the challenges and issues faced by current RBAC systems that integrate AI and ML.
- To evaluate the competence of different ML algorithms to give proper response in case of unauthorized access attempts.
- To evaluate the impact of integrating AI on the RBAC on system security and the extent to which users adhere to the new rules.

Research Questions

- What are the main limitations of traditional RBAC systems in handling modern cybersecurity threats?
- How can AI and ML contribute to the evolution of RBAC frameworks?
- What are the potential risks and benefits of integrating AI into RBAC systems?
- How does the implementation of ML in RBAC influence operational efficiency and security responsiveness?

Research Rationale

This work is informed by the fact that such environments are becoming more dynamic and need better protection. Some of the drawbacks of implementing the traditional RBAC solutions include the following, which does not address dynamic access needs or new risks factors [2]. AI and ML in RBAC may alter access control from rigid and predetermined ones to dynamic systems that can take splitting decisions within a few seconds for the protection of the system [3]. This paper will depict an assessment of the strengths and weaknesses of this integration to determine the impact on cybersecurity.

Literature Review

RBAC systems play a good role in the management of user privileges whereby privileges are subjected to roles within an organization making it secure in different sectors [4]. However, the use of static RBAC has the following disadvantages that make it incompatible with a dynamic cybersecurity business environment [5]. The integration of Artificial Intelligence (AI) and Machine Learning (ML) into cybersecurity, including RBAC systems, provides substantial improvements in several key areas:

According to Hamdan & Talluri, 59% of cybersecurity specialists stated that improved threat detection was the primary strength of artificial intelligence in information technology and cybersecurity [6,7].

Next in line, 57% of respondents assert that enhanced vulnerability management is an essential benefit of AI [8]. This technology has been found to be efficient in sorting big data to look for suspicious activities, improving on time, precision and cost factors of security management [9].

Research into enhancing RBAC through AI and ML demonstrates significant potential for making these systems more dynamic and responsive: It has been postulated that ML algorithms can be integrated with RBAC systems to forecast users' future access requirements in an attempt to alleviate the stress of updating and improving system security [10]. Utilizing neural networks in context of RBAC helps identify discrepancies in access patterns in real time, enhancing the system's effectiveness in preventing unauthorized access [11].

AI and ML implementation has downsides, too. Cyberattacks may employ security technology for phishing, malware, and deepfake assaults. Due to its dual-use nature, cybersecurity measures must be constantly updated to avoid abuse [12]. Therefore, AI and ML are revolutionizing RBAC systems by helping organizations identify threats, manage vulnerabilities, and react to security issues. However, these technologies introduce new dangers and problems, therefore cybersecurity must be updated to offer effective protection in a continuously changing technological environment [13].

Methodology

The approach used in this research is the qualitative one that is involved in the secondary data collection to assess how AI and ML can improve RBAC systems. This work is underpinned by the previous research and analysis of articles and white papers to evaluate the adoption of AI and ML to RBAC [14].

Data Collection

Journal articles and white papers are the most suitable for this research because they offer theoretical frameworks and real-world scenarios on the use of AI and ML in strengthening RBAC systems in cybersecurity. These documents are found in credible academic databases including Google Scholar and ProQuest among others. Secondary data is collected because large volumes of data are required to meet the research needs [15].

Some of the constraints associated with the use of the primary data in the research include the following: These platforms are essential in sourcing a wide array of resources encompassing the latest studies, the classical literature, and industry reports addressing breakthroughs and application of AI/ML in access control systems.

Analysis Technique

This paper will be discussed advantages, challenges as well as risks which are correlated with incorporation of AI and ML into the RBAC systems. Specifically, this study will analyse how AI and ML increase threat detection as well as access control. It will also explore the key threats and risks associated with incorporation of these technologies into security architecture, as well as access the risk associated with.

Tools and Techniques

Other than Google Scholar and ProQuest, the research will incorporate other tools based on artificial intelligence to extract information. They include software that can process and analyze huge volumes of data such as Python libraries (e. g. Importantly, they used programming languages such as Python with its libraries like Pandas for data manipulation and SciKit-Learn for machine learning applications). These tools will help in proper sorting, categorization and consequently analysis of the collected data to get insights [16].

Ethical Considerations

Since this study exclusively uses secondary data, it is important to maintain the highest level of ethical standard on methodology, and the norm in the academic world is to give credit where credit is due. Every source used will be properly cited and the author's work will be respected and protected as applicable. Further on, the influence of bias will be minimized as the research data and information from different and varied sources and points of view will be incorporated in the research paper.

Findings

Learning and artificial intelligence technologies have shown a positive evolution of prediction and prevention of illegitimate access in Role Based Access Control systems. Based on the literature review, the following positive impacts of AI and ML have been earmarked for contributing to the improvement of RBAC security measures [17].

Enhanced Prediction and Detection Capabilities

Thus, AI and ML are essential for transforming RBAC systems into dynamic security threat models. These solutions enable organizations discern between regular and malicious traffic patterns or intrusion attempts before they compromise security. Therefore, ML algorithms can find abnormalities to regular categories by mining large volumes of access data and user behavior. It strengthens security and saves time and effort manually screening for threats [18].

Dynamic Role Adjustments and Access Control

It's amazing that ML algorithms can automatically regulate user access privileges based on data analysis. This flexibility is a huge advance over the initial RBAC method, which employed roles that may not match the business or security context. AI might allow IT business management modifications based on personnel traits. Over-privileged access in stiff RBAC models is reduced.

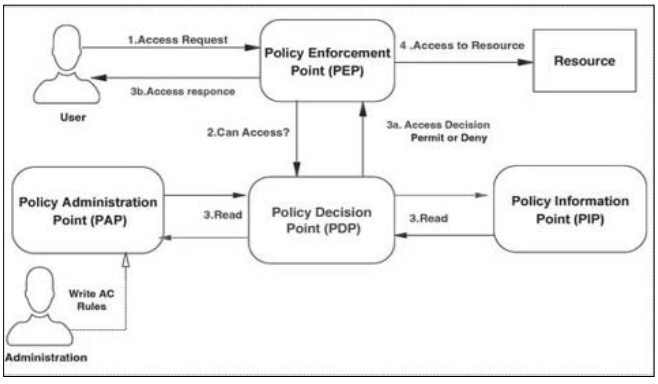

Figure 1: Role of Access control through AI and ML

Preventive Security Measures

AI and ML can help RBAC systems execute preventative security actions. Deep learning models may prevent or detect security threats from user access behaviors. These systems may also use fresh data to suggest access control changes before security problems arise. The AI may also simulate various security conditions using machine learning and deep learning to understand how access control settings influence the system and push admins to choose the proper RBAC settings.

Reduced False Positives and Improved Response Times

AI in the RBAC model reduces threat detection false positives. Access events may be better differentiable by the machine learning algorithms utilizing the context rather than usual AI-based techniques. This reduces cases of false positives that disrupt operations and allows analysts to focus on real threats. AI-integrated systems can independently respond to threats and give back response time.

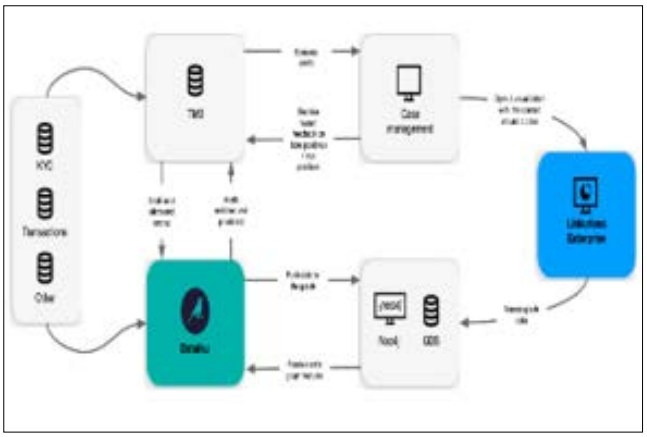

Figure 2: Strategies for Reduced False Positives

Discussion

The integration of AI with standard RBAC systems means that security is now intelligent and dynamic based on the environment. It has considerable implications in respect of personnel operations and measures of protection in organizations. The incorporation of AI in the RBAC systems enhances its capability of protecting the prospective threats. Machine Learning, is subfield of artificial intelligence and can analyze lots of data and can look for patterns which can make security logic more proactive. AI integrated RBAC systems not only control access rights but also effectively mitigate these attacks before they occur by being able to predict such events [19].

From an operation point of view, AI greatly reduces the number of efforts in managing access controls. AI automates role assignment and adjustments, saving staff time administering and upgrading RBAC systems. Such an approach lets system administrators focus on more essential tasks and avoid mundane labor.

Conclusion and Recommendations

The incorporation of AI and ML into the RBAC model has brought very positive results since it improved the security and functionality of the systems. AI and ML help to create more effective and higher-level controls that can adapt to user conduct patterns as well as new risks that may emerge. The primary advantages include higher detection rates, meaning that possible security threats will be identified as early as possible, and adaptive access controls which guarantee that the protection measures are as relevant to the organization and the user roles as possible [20].

Recommendations for Future Research

Future research may involve working on the further optimization of the algorithms used to decrease the number of false positives as well as increasing the effectiveness of threats identification. Moreover, it is necessary to further analyses the ethical consequences of integrating AI into access control, including privacy violations and different types of bias in algorithmic decision-making [7].

Practical Applications in Industry

It is recommended that Industries should consider a pilot run of the proposed AI-enhanced RBAC system in different organizations, thus gauging its efficiency and suitability for large-scale adoption. Formulating guidelines to incorporate these technologies in RBAC systems also within specific industry sectors may also help organizations adapt these advanced solutions to industry-specific issues, strengthen security measures if needed without infringing on privacy and legal standards [21].

References

1. Sekar M (2022) Machine learning for auditors: Automating fraud investigations through artificial intelligence. Springer https://link.springer.com/book/10.1007/978-1-4842-8051-5.
2. Kure HI, Islam S, Mouratidis H (2022) An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Comput Appl 34.
3. Grant R, Phene A (2022) The knowledge based view and global strategy: Past impact and future potential. Global Strategy Journal 12.
4. Akstinaite V, Garrard P, Sadler-Smith E (2022) Identifying Linguistic Markers of CEO Hubris: A Machine Learning Approach. British Journal of Management 33.
5. Ramamurthy V, Richa G, Baral SK (2022) Artificial Intelligence and Digital Diversity Inclusiveness in Corporate Restructuring. Nova https://novapublishers.com/shop/artificial-intelligence-and-digital-diversity-inclusiveness-in-corporate-restructuring/.
6. Hamdan AH, Arora P, Alareeni B, Hamdan RK (2022) Future of Organizations and Work After the 4th Industrial Revolution: The Role of Artificial Intelligence, Big Data, Automation, and Robotics. Springer 1037.
7. Sampath Talluri, Vamsy Priya Anne, Venkata Santosh Chadalavada (2023) Role-Based Access Control (RBAC) in A Centralized Identity and Access Management (IAM) System. International Journal of Information Technology (IJIT) 4: 88-95.
8. Visani F, Raffoni A, Costa E (2022) The quest for business value drivers: applying machine learning to performance management. Production Planning and Control 1127-1147.
9. Anshari, Hamdan M (2022) Understanding knowledge management and upskilling in Fourth Industrial Revolution: transformational shift and SECI model. VINE Journal of Information and Knowledge Management Systems 52.
10. Durairaj Ł Wróblewski, Sheela A, Hariharasudan A, Urbański M (2022) Random forest based power sustainability and cost optimization in smart grid. Production Engineering Archives 28: 82-92.
11. Kure HI, Islam S, Ghazanfar M, Raza A, Pasha M (2022) Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. Neural Comput Appl 34.
12. Hajli N, Saeed U, Tajvidi M, Shirazi F (2022) Social Bots and the Spread of Disinformation in Social Media: The Challenges of Artificial Intelligence. British Journal of Management 33.
13. Rahman M, Wahab SA, Latiff ASA (2022) Organizational sustainability: Issues, challenges and the future of Bangladesh pharmaceutical industry. Journal of Future Sustainability 2.
14. Hu J (2022) Assessing Students' Digital Reading Performance: An Educational Data Mining Approach. Routledge https://www.routledge.com/Assessing-Students-Digital-Reading-Performance-An-Educational-Data-Mining-Approach/HU/p/book/9781032403151?srsltid=AfmBOorRdISGGFC4Mzy9v6054msqT0C1mxLF9h2N_uVdDQ_AXTJGXY_l.
15. Fletcher G (2022) Management and Visualisation: Seeing Beyond the Strategic. Routledge https://www.taylorfrancis.com/books/oa-mono/10.4324/9781003304166/management-visualisation-gordon-fletcher.
16. Oluyisola OE, Bhalla S, Sgarbossa F, Strandhagen JO (2022) Designing and developing smart production planning and control systems in the industry 4.0 era: a methodology and case study.

J Intell Manuf 33.

17. Singh P (2022) Fundamentals and methods of machine and deep learning: Algorithms, tools, and applications. Wiley https://onlinelibrary.wiley.com/doi/book/10.1002/9781119821908.
18. Yan R, Wang S (2022) Applications of machine learning and data analytics models in maritime transportation. Applications of Machine Learning and Data Analytics Models in Maritime Transportation https://digital-library.theiet.org/doi/book/10.1049/pbtr038e?showtab=chapters.
19. Willard J, Jia X, Xu S, Steinbach M, Kumar V (2022) Integrating Scientific Knowledge with Machine Learning for Engineering and Environmental Systems. ACM Comput Surv 55.
20. Galán RA Carrasco, Latorre A (2022) Military Applications of Machine Learning: A Bibliometric Perspective. Mathematics 10.
21. Tiddi, Schlobach S (2022) Knowledge graphs as tools for explainable machine learning: A survey. Artif Intell 302.