Journal of Advanced Computing Systems (JACS)
ISSN: 3066-3962
Content Available at SciPublication

AI-Powered Role-Based Access Control (RBAC): Automating Policy Enforcement in Enterprise Environments

Rajendra Muppalaneni[1], Anil Chowdary Inaganti[2], Nischal Ravichandran[3], Sai Rama Krishna Nersu[4],
Lead Software Developer[1], Workday Techno Functional Lead[2], Senior Identity Access Management Engineer[3], Software Developer[4],
muppalanenirajendra@gmail.com[1], anilchowdaryinaganti@gmail.com[2], nischalravichandran@gmail.com[3], sai.tech359@gmail.com[4]
DOI: 10.69987/JACS.2025.50201

Keywords

Role-Based Access Control, GDPR, HIPAA, zero-trust, enterprise security, dynamic role adjustment, user behavior monitoring.

Abstract

The growing complexity of modern cloud infrastructures has made traditional methods of managing access control increasingly inadequate. Role-Based Access Control (RBAC) has been a widely adopted method to manage user permissions; however, as organizations scale, managing these roles manually becomes more difficult, leading to security vulnerabilities and operational inefficiencies. To address these challenges, AI-powered RBAC systems are being integrated into enterprise environments. By leveraging machine learning algorithms and advanced analytics, these AI-driven systems automate role assignments, continuously monitor user behavior, and dynamically adjust access controls in real-time. This approach improves policy enforcement, reduces the risk of privilege creep, enhances security, and ensures compliance with regulatory standards such as GDPR and HIPAA. AI-powered RBAC not only optimizes access management but also adapts to evolving business needs, ensuring secure and efficient access to critical resources. This article explores the methodology, benefits, and real-world applications of AI-powered RBAC systems and examines the future trends in access control management driven by AI.

1. Introduction

The rapid pace of digital transformation across industries has led to a significant shift toward cloud-based services and applications. As organizations increasingly rely on the cloud for storing and processing data, managing applications, and delivering services, the complexity of IT environments continues to grow. With this digital shift, organizations are also faced with heightened concerns about data security, compliance, and the management of access to sensitive resources. As a result, there is a greater need for robust, scalable access control mechanisms that ensure the right people have access to the right resources at the right time [1].

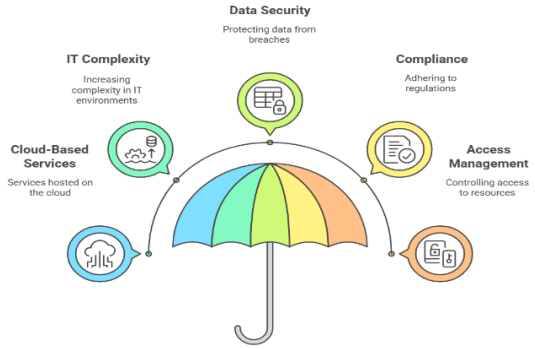

Figure 1: Navigating Digital Transformation

One of the most widely adopted methods for managing access to resources in enterprise environments is Role-Based Access Control (RBAC). RBAC helps organizations define specific roles within the organization and then assign permissions to those roles based on job functions. This ensures that users and systems have access only to the resources they need to perform their duties, and limits unnecessary exposure of sensitive information. While RBAC has long been a reliable method for managing access control, the increasing scale and complexity of modern IT infrastructures make manually managing these policies increasingly difficult. The growing number of users, cloud services, and applications can overwhelm traditional RBAC approaches, resulting in misconfigurations, permission errors, and potential security vulnerabilities [2],[3].

To address these challenges and enhance the efficiency of policy enforcement, organizations are increasingly turning to AI-powered RBAC systems. These systems utilize advanced technologies like machine learning (ML) and analytics to automate and optimize access control management. By leveraging AI, RBAC systems are able to dynamically adjust user roles and permissions in real-time based on changing user behavior, organizational needs, and security requirements. AI can analyze vast amounts of data generated by user activities, system behaviors, and resource interactions to ensure that access controls remain accurate, compliant, and adaptive to evolving business needs.

Figure 2: Evaluating RBAC Effectiveness and Complexity

AI-powered RBAC systems improve the overall efficiency of policy enforcement by reducing the administrative burden of manually defining, assigning, and adjusting roles. They also provide a more granular, adaptive approach to role management by continuously learning from user interactions and adjusting access controls based on context. This dynamic nature helps reduce the risk of human error, enhances security by promptly detecting unauthorized access attempts, and ensures compliance with a wide range of regulatory standards, including GDPR, HIPAA, SOX, and PCI-DSS. Additionally, the ability to automate role assignment and policy enforcement reduces the risk of privilege creep (the accumulation of excessive permissions over time), which is a common issue in large organizations [4].

Figure 3: AI Powered RBAC Cycle

In this article, we will explore how AI enhances traditional RBAC systems and how its integration transforms access control policies. We will examine the benefits of AI-powered RBAC, including increased security, streamlined policy enforcement, and improved compliance management. Moreover, we will discuss the role of machine learning in continuously adapting to changing user needs and threat landscapes, and how this technology is shaping the future of enterprise security frameworks. Ultimately, the article aims to provide a comprehensive understanding of how AI-driven RBAC systems are revolutionizing access management in modern organizations, making them more agile, secure, and compliant in a rapidly evolving digital world.

The implementation of AI-powered Role-Based Access Control (RBAC) systems involves several key steps, which enable organizations to automate access management while improving the accuracy, efficiency, and security of role assignment and policy enforcement. The methodology for integrating AI into RBAC can be broken down into three main phases: defining roles and access control policies, enforcing policies using AI, and utilizing machine learning for continuous improvement. Each of these phases works together to create a dynamic and adaptive access control system that evolves with the organization's needs and external threats.

2. Methodology

Figure 4: AI Powered RBAC Hierarchy

2.1 Defining Roles and Access Control Policies

The first step in implementing an AI-powered RBAC system is defining roles within the organization. Traditional RBAC systems typically require administrators to manually assign roles based on predefined job functions, such as "Admin," "Manager," "HR," or "Engineer." Each role is associated with a specific set of permissions that dictate the level of access to resources, applications, and data. These permissions are determined based on the needs of the business, security protocols, and regulatory compliance requirements.

In an AI-powered RBAC system, this role definition process can be significantly enhanced through automation. AI systems can analyze large datasets, including historical user behavior, access patterns, and organizational structures, to automatically assign roles based on real-time insights. For instance, AI can observe a user's behavior and determine which systems, data, or applications they access most frequently. It can then recommend a suitable role based on these activities, ensuring that employees are granted access only to the resources necessary for their job functions. This data-driven approach reduces the manual effort involved in role assignment and ensures that roles are dynamically adjusted to reflect users' evolving responsibilities and activities [5].

Furthermore, AI can help organizations align access policies with regulatory standards, such as GDPR, HIPAA, and SOC 2, by ensuring that sensitive data access is restricted to users with specific roles that align with compliance requirements. As organizations scale, the ability to automate this process becomes increasingly valuable in maintaining a streamlined and compliant access control system.

2.2 AI-Driven Policy Enforcement

Once roles and access policies have been defined, the next step is enforcing these policies across the organization's systems using AI-driven automation. AI-powered RBAC systems continuously monitor user activity and behavior in real-time to ensure that users only access the data and systems they are authorized to use based on their roles. By automating policy enforcement, AI ensures that security policies are consistently applied, reducing the risk of human error or intentional breaches [6].

One key feature of AI-driven policy enforcement is the ability to detect and prevent violations in real-time. For example, if an employee attempts to access sensitive financial data outside their designated role, the AI system can immediately flag or block the request, preventing unauthorized access. The AI can also trigger an alert to notify security teams of the potential breach, enabling a rapid response. In some cases, the system can automatically adjust the user's role to reflect their current task or responsibilities, dynamically updating access permissions as needed. This dynamic role adjustment ensures that access control policies remain relevant and secure at all times [7].

Moreover, AI systems can handle complex, multi-layered access control policies that are often difficult to manage manually. In large organizations, employees may require different levels of access across multiple systems or departments. AI can intelligently allocate permissions and enforce policies across these systems, ensuring that access is tailored to each user's role and responsibilities, while also maintaining the principle of least privilege. This ensures that users only have access to the minimum necessary resources to perform their duties, reducing the risk of unnecessary exposure to sensitive data.

AI-driven policy enforcement also includes automated audits. The system can regularly check and validate that access control policies are being adhered to, providing automated reports and logs that facilitate audits and compliance checks. This is particularly valuable for organizations operating under strict regulatory frameworks, as it simplifies the process of demonstrating compliance and helps identify any areas of potential risk or non-compliance.

2.3 Machine Learning for Continuous Improvement

Machine learning (ML) plays a crucial role in continuously improving AI-powered RBAC systems by enabling them to learn from user behaviors, access patterns, and evolving organizational structures. Over time, as the system gathers more data, machine learning algorithms can refine access control policies and improve their accuracy and effectiveness. This continuous learning process allows AI to adapt to changing business needs, ensuring that access controls remain relevant, efficient, and secure [8].

One key advantage of machine learning in RBAC is the ability to detect anomalies in user behavior that could signal potential security threats [9]. For example, if an employee who typically accesses HR data suddenly begins accessing financial reports or customer records, the machine learning model can flag this behavior as an anomaly. Based on historical data and past incidents, the system can determine whether this access is legitimate or whether it poses a security risk. If the access is deemed suspicious, the AI system can automatically alert security personnel, trigger a review, or take corrective actions, such as temporarily revoking access or prompting multi-factor authentication (MFA) verification.

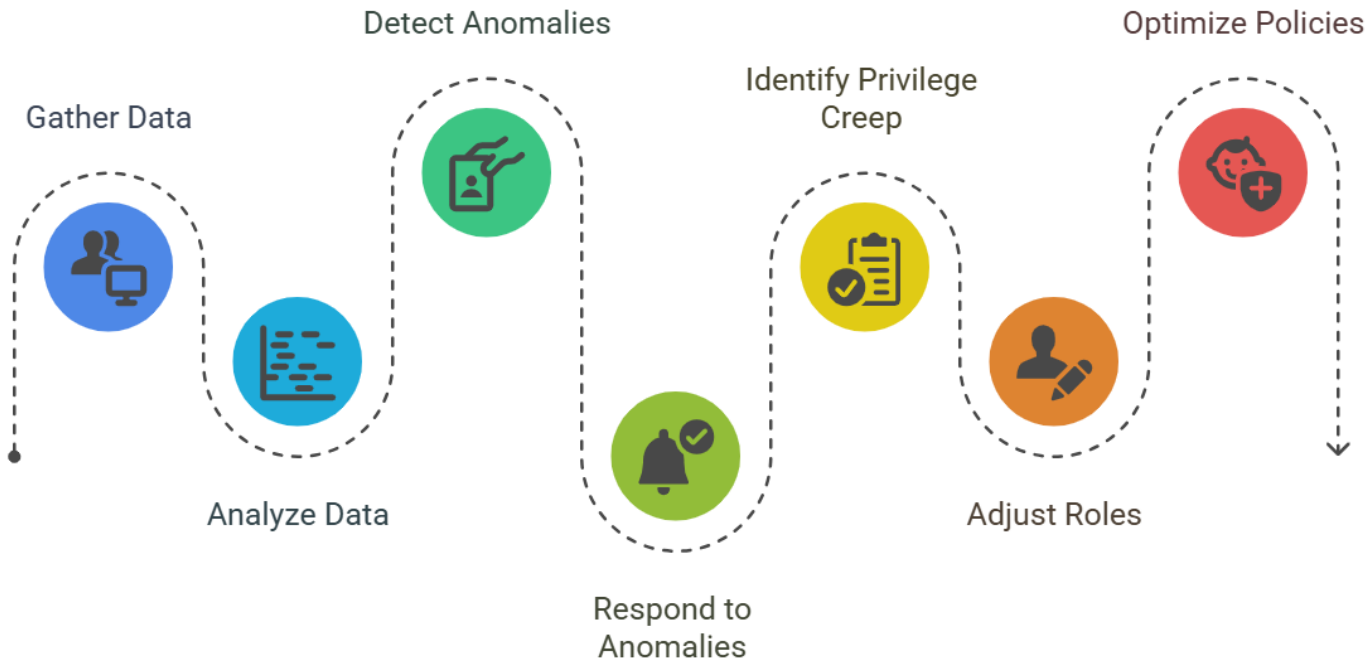

Figure 5: Machine Learning Process in RBAC Systems

Machine learning algorithms also help identify patterns of privilege creep, a phenomenon where users accumulate excessive permissions over time due to role changes or new project assignments. These permissions often remain unchecked, leading to unnecessary access to sensitive data. AI can proactively monitor for this issue and automatically adjust roles or revoke unnecessary privileges, helping to maintain the principle of least privilege and reduce the risk of data breaches [10].

In addition, machine learning models improve access policy optimization by analyzing how users interact with cloud services and applications. By identifying trends and understanding the context of each user's role, AI can propose adjustments to role definitions or access control policies. For example, if an employee's role evolves over time or their access requirements change based on a new project, the AI system can update their access permissions accordingly, ensuring that they have access to the right resources at the right time. This adaptive approach helps organizations scale efficiently while maintaining tight security controls.

3. Key Benefits of AI-Powered RBAC

AI-powered Role-Based Access Control (RBAC) systems offer significant advantages to organizations by enhancing access management, reducing the risk of data breaches, improving operational efficiency, and ensuring regulatory compliance. By leveraging advanced AI and machine learning algorithms, these systems enable organizations to manage user access dynamically, adapt to evolving business needs, and prevent unauthorized access to critical resources. Below are some of the key benefits of AI-powered RBAC:

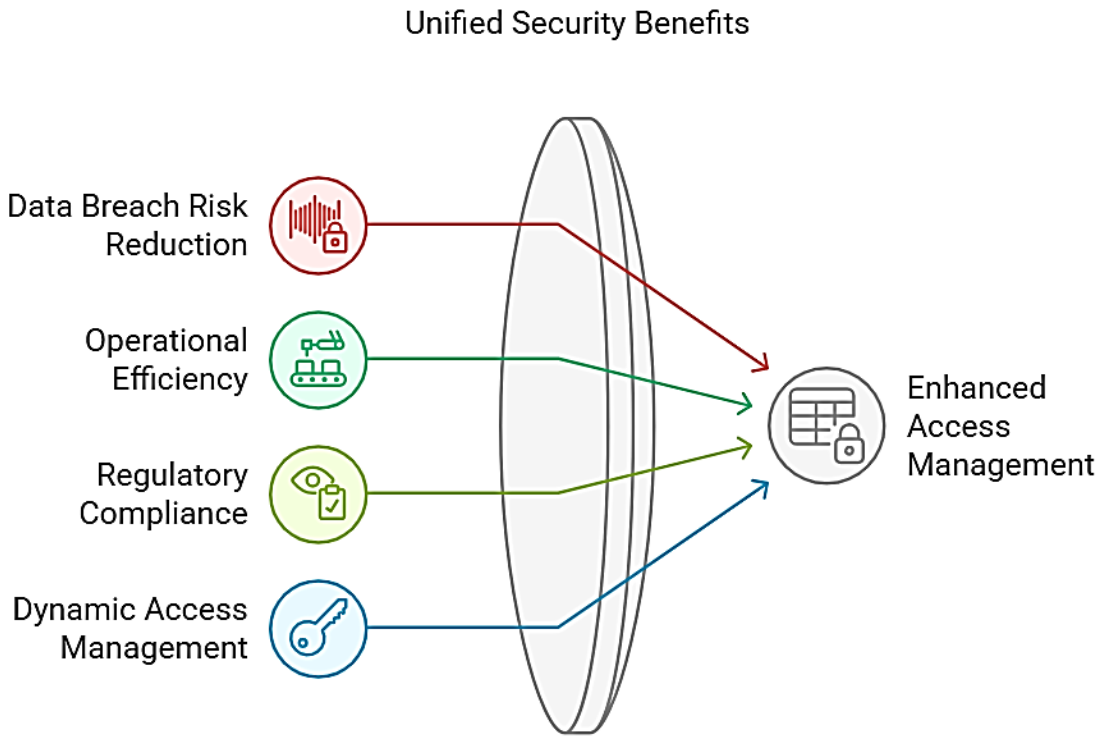

Figure 6: Unified Security Benefits

3.1 Improved Security and Risk Management

One of the most significant advantages of integrating AI into RBAC systems is the improvement in security. In traditional RBAC systems, administrators assign roles and permissions manually, which is prone to human error and oversight. By automating role assignments and continuously monitoring user behavior, AI ensures that only authorized individuals have access to sensitive data and systems, significantly reducing the risk of unauthorized access [11].

AI enhances security by monitoring user access in real-time and detecting abnormal or suspicious access patterns that may indicate potential threats. For example, if an employee attempts to access data or systems outside their usual scope of work—such as sensitive files not relevant to their role—the AI system can flag this as anomalous behavior. This anomaly detection can be crucial in identifying insider threats or external attacks, which might otherwise go unnoticed until damage occurs. Upon detecting suspicious activity, AI can take immediate corrective action, such as blocking the user's access, sending alerts to security teams, or even triggering automated security protocols (e.g., locking accounts or prompting multi-factor authentication) [12].

Additionally, AI-powered RBAC helps mitigate the risk of privilege creep, a common issue in organizations where employees accumulate excessive permissions over time due to role changes, project assignments, or promotions. This unchecked accumulation of access rights can create security vulnerabilities, as users may gain access to resources they no longer require, increasing the potential attack surface. AI systems can proactively detect privilege creep by continuously assessing user access and ensuring that permissions are appropriately adjusted to reflect users' current job functions. This dynamic permission adjustment ensures that users have the minimum necessary access, in line with the least privilege principle, which is fundamental to strong security practices [13].

3.2 Greater Efficiency in Policy Enforcement

One of the key challenges of traditional RBAC systems is the manual and time-consuming process of managing

roles, permissions, and access control policies, particularly in large organizations. As businesses scale and employees come and go, manually assigning and updating roles can become overwhelming and prone to errors. AI-powered RBAC significantly improves efficiency by automating much of the role assignment and policy enforcement processes, reducing administrative overhead and streamlining access management [14].

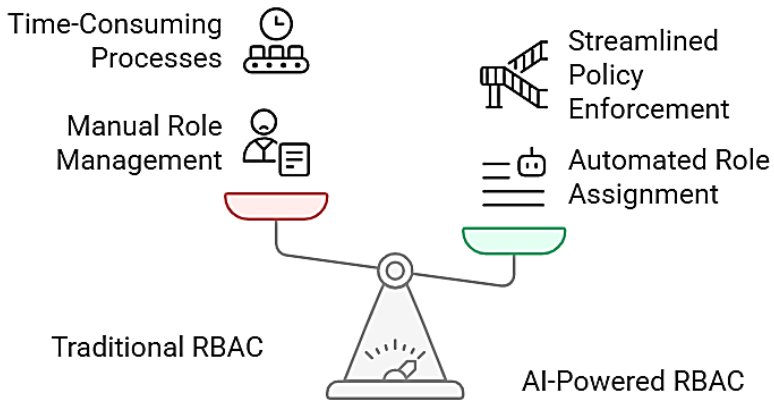

Figure 7: Traditional Vs AI Powered RBAC

AI systems can automatically analyze vast amounts of data to determine which roles and permissions are most appropriate for each user, based on their behavior, organizational function, and job requirements. For instance, when a new employee joins, AI can quickly assess their position within the organization and recommend an appropriate role based on historical data and job-related patterns. As employees change roles, move to different departments, or take on new responsibilities, AI can dynamically adjust their access levels accordingly. This real-time adjustment not only enhances operational efficiency but also reduces the risk of errors associated with manual role assignments [15].

Moreover, AI's ability to continuously monitor user activities and adjust roles and permissions in real-time enables organizations to manage complex access policies across a wide range of users and systems. This capability is particularly beneficial in large-scale organizations or those with rapidly changing roles and responsibilities. As the organization grows, AI-powered RBAC can scale effortlessly, handling the increased volume of users and access control requirements without requiring additional administrative resources. This leads to faster onboarding, role changes, and streamlined management of access controls, ensuring that security and policy enforcement are never compromised as the organization expands.

3.3 Enhanced Compliance and Auditability

Compliance with regulatory standards such as GDPR, HIPAA, SOX, and PCI-DSS is a critical concern for organizations, particularly those handling sensitive data. Ensuring that users have access only to the data they are authorized to view and interact with is a key component of maintaining compliance. AI-powered RBAC systems help organizations meet these regulatory requirements by automating the enforcement of access control policies and ensuring that only the appropriate individuals have access to sensitive information [16], [17].

AI models can continuously monitor access to sensitive data, automatically ensuring that users only access information aligned with their roles. This not only ensures compliance but also reduces the risk of human error in assigning permissions. In cases of non-compliance or unauthorized access attempts, AI systems can automatically detect and respond to potential violations by taking corrective actions such as restricting access or notifying security teams for further investigation. Additionally, AI-powered RBAC systems can generate automated audit trails, providing an auditable record of who accessed what data, when, and why—essential for compliance reporting and periodic security reviews [18].

Furthermore, regulatory environments and business needs are constantly evolving. AI-powered RBAC systems can stay up-to-date with these changes by

automatically adjusting policies to comply with new laws, standards, or organizational requirements. For instance, if a new data privacy regulation is introduced, AI can automatically reassign roles and adjust permissions to ensure compliance without requiring manual intervention. This proactive approach significantly reduces the administrative burden on compliance teams and helps organizations avoid costly fines or penalties associated with non-compliance.

3.4 Scalability and Adaptability

One of the standout benefits of AI-powered RBAC systems is their scalability and adaptability, which are essential for organizations that need to manage growing and dynamic user bases. Traditional RBAC systems can become cumbersome as organizations expand, especially when roles and permissions must be manually updated to reflect changes in users' responsibilities. As the number of users increases, the risk of errors also rises, leading to potential security vulnerabilities [19].

AI-powered RBAC systems are inherently scalable because they rely on machine learning algorithms and data-driven insights to manage access controls dynamically. AI can quickly adapt to changes in user behavior, organizational structure, or business needs, automatically adjusting roles and permissions as required. Whether the organization is onboarding new employees, reorganizing teams, or expanding into new markets, AI can easily accommodate these changes without the need for manual role updates or extensive administrative effort [20].

Moreover, AI-powered RBAC systems are adaptable to new security threats or compliance requirements. As the threat landscape evolves or as new regulatory standards are introduced, AI models can adjust access control policies to reflect these changes in real-time. For example, AI systems can detect emerging security risks based on user behavior patterns and adjust roles or permissions accordingly to prevent unauthorized access. This adaptability ensures that RBAC remains relevant and responsive to the ever-changing environment in which the organization operates.

4. Real-World Applications and Case Studies

To understand the practical impact of AI-powered RBAC in real-world scenarios, it is essential to look at how organizations in various industries have successfully implemented these systems. Through these case studies, we can see how AI-driven RBAC systems streamline access control, improve security, and ensure compliance with regulatory standards, all while reducing the administrative burden typically associated with manual role management.

4.1 Case Study Analysis

Global Healthcare Provider – Securing Sensitive Patient Data [22],[23].

A large global healthcare provider faced significant challenges in managing access to its sensitive patient data. The organization had to comply with strict healthcare regulations such as HIPAA (Health Insurance Portability and Accountability Act) while ensuring that only authorized medical staff and employees could access patient records. With thousands of employees across multiple departments and a large, diverse user base, manually managing role assignments and access permissions was cumbersome, prone to errors, and time-consuming.

To address this challenge, the healthcare provider implemented an AI-powered RBAC system. The AI system automated role assignments by analyzing historical user data, identifying user behaviors, and automatically assigning roles based on job functions. For example, doctors and nurses were automatically granted access to patient records, while administrative staff were given access to non-sensitive patient information. The AI system continuously monitored user access patterns, analyzing login times, system usage, and the types of data accessed. By monitoring these behaviors in real time, the system could automatically detect any suspicious activity, such as unauthorized access attempts, and immediately block or flag the attempts for further investigation.

Furthermore, the AI-powered RBAC system automatically adjusted access levels based on users' changing roles or responsibilities. If a staff member changed departments or was reassigned to a new project, the system would automatically update their access rights accordingly. This automation ensured that the healthcare provider stayed compliant with HIPAA and other healthcare regulations, while also improving the organization's overall security posture. The result was improved compliance, enhanced data security, and a significant reduction in administrative effort associated with managing access control.

Multinational Financial Institution – Streamlining Access Control Across Global Operations [23], [24].

In another example, a multinational financial institution integrated an AI-powered RBAC system to streamline access control across its vast global network. The institution needed a robust system to manage access to its critical financial systems, which housed sensitive client data, transaction records, and financial reports. Compliance with industry regulations such as SOX (Sarbanes-Oxley Act) and PCI-DSS (Payment Card

Industry Data Security Standard) was essential, as the organization handled highly sensitive information that required strict access management and security controls.

By deploying AI-driven RBAC, the institution was able to automate the assignment of roles and permissions based on job functions, user activity, and region. AI models continuously monitored user actions, ensuring that employees only accessed financial data relevant to their roles. For example, financial analysts were given access to financial reports, but were restricted from accessing sensitive client data unless it was necessary for their job function.

The system also helped mitigate the risk of unauthorized access and privilege escalation, where users inadvertently gained access to resources beyond their responsibilities over time. The AI system dynamically adjusted user roles based on real-time job changes, promotions, or department transfers, ensuring that employees retained the minimum necessary access for their duties. Additionally, it automatically flagged and blocked any unauthorized access attempts, providing security teams with real-time alerts for further investigation.

5. Future Trends and Developments

As AI, machine learning, and other emerging technologies continue to evolve, the capabilities of AI-powered RBAC systems will only improve. The future of access control management will be shaped by advances in AI algorithms, integration with new security models, and the growing demand for zero-trust security frameworks. Below are some key future trends and developments that will drive the evolution of AI-powered RBAC systems:

5.1 Evolution of AI Capabilities

AI algorithms will continue to evolve, enabling even more sophisticated access management capabilities. Future AI-powered RBAC systems will be able to handle even more complex and nuanced decision-making processes, based on a deeper analysis of contextual information. For example, AI will be able to analyze not just user behavior but also environmental factors such as time of day, location, device type, and other contextual parameters to determine the risk associated with granting access to a resource [25].

Adaptive AI will also become more prevalent, continuously refining role assignments based on changing user activities and patterns. The system will learn from user behaviors over time and be able to predict future access needs with increasing accuracy. This will allow organizations to better anticipate user needs and grant or revoke access proactively, before issues arise [26].

5.2 Integration with Zero-Trust Security Models

One of the key emerging trends in cybersecurity is the adoption of the zero-trust security model. Zero-trust is based on the principle that no user or device—whether inside or outside the network—is inherently trusted. Instead, access to resources is granted only after rigorous verification and continuous monitoring. AI-powered RBAC systems will play a crucial role in enforcing zero-trust policies by ensuring that user roles and permissions are constantly evaluated and adjusted based on dynamic risk factors [27].

AI will enable real-time risk-based access controls, automatically adjusting permissions and enforcing stricter policies in high-risk scenarios. For example, if a user is logging in from an unusual location or device, AI can automatically request additional authentication steps, such as multi-factor authentication (MFA), before granting access. Similarly, AI can limit access to sensitive resources based on contextual factors, such as the user's role, location, or behavior. This tight integration between AI and zero-trust frameworks will allow organizations to create a more resilient and adaptive security infrastructure [28],[29].

5.3 Seamless Integration with Identity and Access Management (IAM) Systems

AI-powered RBAC systems will also increasingly integrate with Identity and Access Management (IAM) solutions. IAM systems are already widely used to manage user identities, authentication, and authorization. By integrating AI-driven RBAC with IAM systems, organizations can create a more unified and automated approach to managing user access and roles across all applications, databases, and network resources [30],[31].

This integration will enable more granular control over who can access what resources and when. AI will provide continuous monitoring of access and adapt roles based on real-time data from IAM systems, ensuring that users are granted the appropriate access level based on their verified identity, job function, and risk assessment. Furthermore, AI-enhanced IAM systems will provide organizations with powerful tools for compliance management and auditability, ensuring that all access activities are logged, monitored, and compliant with regulatory requirements.

5.4 AI-Driven Threat Detection and Prevention

As AI models become more advanced, they will not only improve access control management but will also enhance threat detection and prevention capabilities. AI-powered RBAC systems will analyze user behaviors and system interactions to detect potential threats before they escalate into breaches [32][33]. This proactive

approach to security will allow organizations to respond to potential threats more quickly and effectively, preventing damage before it occurs.

For instance, AI can detect when a user's behavior deviates from established patterns—such as accessing a large amount of data in an unusual manner—and flag it for investigation. It can also use predictive analytics to forecast potential threats and adjust user roles and permissions accordingly, minimizing the risk of a security breach.

Conclusion

AI-powered Role-Based Access Control (RBAC) represents a significant leap forward in access management, combining automation, machine learning, and real-time monitoring to improve security, operational efficiency, and compliance. By dynamically adjusting roles and permissions based on contextual data and user behavior, these systems ensure that only authorized individuals can access sensitive resources, significantly reducing the risk of unauthorized access and data breaches. Furthermore, the automation of policy enforcement reduces the administrative burden and ensures that access controls remain agile and responsive to changing organizational needs. Real-world applications in industries such as healthcare and finance demonstrate the tangible benefits of AI-driven RBAC, including enhanced compliance with regulations and better risk management. Looking ahead, the integration of AI with emerging security models, such as zero-trust frameworks, will further strengthen the resilience and adaptability of access control systems. As AI continues to evolve, organizations will benefit from more sophisticated, scalable, and secure solutions for managing access in an increasingly complex digital landscape.

References:

[1] Bhatt, S., Pham, T., Gupta, M., Benson, J., Park, J., & Sandhu, R. (2021). Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future. IEEE Access, 9, 107200-107223. https://doi.org/10.1109/ACCESS.2021.3101218.

[2] Ferraiolo, D., Cugini, J., & Kuhn, D. (2014). Role-Based Access Control (RBAC) : Features and Motivations.

[3] Butt, A., Mahmood, T., Saba, T., Bahaj, S., Alamri, F., Iqbal, M., & Khan, A. (2023). An Optimized Role-Based Access Control Using Trust Mechanism in E-Health Cloud Environment. IEEE Access, 11, 138813-138826. https://doi.org/10.1109/ACCESS.2023.3335984.

[4] Shin, S., Park, M., Kim, T., & Yang, H. (2024). Architecture for Enhancing Communication Security with RBAC IoT Protocol-Based Microgrids. Sensors (Basel, Switzerland), 24. https://doi.org/10.3390/s24186000.

[5] Ghazal, R., Malik, A., Qadeer, N., Raza, B., Shahid, A., & Alquhayz, H. (2020). Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments. IEEE Access, 8, 12253-12267. https://doi.org/10.1109/ACCESS.2020.2965333.

[6] Cheminod, M., Durante, L., Seno, L., Valenza, F., & Valenzano, A. (2019). A comprehensive approach to the automatic refinement and verification of access control policies. Comput. Secur., 80, 186-199. https://doi.org/10.1016/J.COSE.2018.09.013.

[7] Bhattacharya, S., & Raman, R. (2023). Speed Violation Detection and Enforcement with CNN and IoT Integration. 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), 1-5. https://doi.org/10.1109/SMARTGENCON60755.2023.10441950.

[8] Arora, S., Khare, P., & Gupta, S. (2024). A Machine Learning for Role Based Access Control: Optimizing Role Management and Permission Management. 2024 First International Conference on Pioneering Developments in Computer Science & Digital Technologies (IC2SDT), 158-163. https://doi.org/10.1109/IC2SDT62152.2024.10696236.

[9] K. K. R. Yanamala, "AI and the Future of Cognitive Decision-Making in HR," Applied Research in Artificial Intelligence and Cloud Computing, vol. 6, no. 9, pp. 31–46, Sep. 2023.

[10] Mehmood, M., Amin, R., Muslam, M., Xie, J., & Aldabbas, H. (2023). Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning. IEEE Access, 11, 46561-46576. https://doi.org/10.1109/ACCESS.2023.3273895.

[11] Ribalta, C., Geraud-Stewart, R., Sergeeva, A., & Lenzini, G. (2024). A systematic literature review on the impact of AI models on the security of code generation. Frontiers in Big Data, 7. https://doi.org/10.3389/fdata.2024.1386720.

[12] Avhad, K., Jadhav, V., Kurhade, S., & Raut, P. (2024). Real-Time Surveillance with AI: A Comprehensive Approach to Security and Monitoring. International Journal of Advanced Research in Science, Communication and

Technology. https://doi.org/10.48175/ijarsct-19681.

[13] Currey, J., McKinstry, R., Dadgar, A., & Gritter, M. (2020). Informed Privilege-Complexity Trade-Offs in RBAC Configuration. Proceedings of the 25th ACM Symposium on Access Control Models and Technologies. https://doi.org/10.1145/3381991.3395597.

[14] K. K. R. Yanamala, "Dynamic bias mitigation for multimodal AI in recruitment ensuring fairness and equity in hiring practices," JAMM, vol. 6, no. 2, pp. 51–61, Dec. 2022.

[15] Budhwar, P., Malik, A., Thedushika, M., Silva, D., & Thevisuthan, P. (2022). Artificial intelligence – challenges and opportunities for international HRM: a review and research agenda. The International Journal of Human Resource Management, 33, 1065 - 1097. https://doi.org/10.1080/09585192.2022.2035161.

[16] Aberkane, A., Poels, G., & Broucke, S. (2021). Exploring Automated GDPR-Compliance in Requirements Engineering: A Systematic Mapping Study. IEEE Access, 9, 66542-66559. https://doi.org/10.1109/ACCESS.2021.3076921.

[17] Adeyelu, O., Ugochukwu, C., & Shonibare, M. (2024). AUTOMATING FINANCIAL REGULATORY COMPLIANCE WITH AI: A REVIEW AND APPLICATION SCENARIOS. Finance & Accounting Research Journal. https://doi.org/10.51594/farj.v6i4.1035.

[18] Fragkos, G., Johnson, J., & Tsiropoulou, E. (2022). Dynamic Role-Based Access Control Policy for Smart Grid Applications: An Offline Deep Reinforcement Learning Approach. IEEE Transactions on Human-Machine Systems, 52, 761-773. https://doi.org/10.1109/thms.2022.3163185.

[19] Chatterjee, S. (2024). Unveiling Innovations in Event Management Systems: A Comparative Study. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. https://doi.org/10.55041/ijsrem36321.

[20] M, A., Wahab, A., & Idris, M. (2024). Adaptable and Dynamic Access Control Decision-Enforcement Approach Based on Multilayer Hybrid Deep Learning Techniques in BYOD Environment. Computers, Materials & Continua. https://doi.org/10.32604/cmc.2024.055287.

[21] Dagher, G., Mohler, J., Milojkovic, M., & Marella, P. (2018). Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology. Sustainable Cities and Society, 39, 283-297. https://doi.org/10.1016/J.SCS.2018.02.014.

[22] Martínez, A., Pérez, M., & Ruiz-Martínez, A. (2023). A Comprehensive Model for Securing Sensitive Patient Data in a Clinical Scenario. IEEE Access, 11, 137083-137098. https://doi.org/10.1109/ACCESS.2023.3338170.

[23] Pochu, S., Nersu, S. R. K., & Kathram, S. R. (2024). Enhancing Cloud Security with Automated Service Mesh Implementations in DevOps Pipelines. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 7(01), 90-103.

[24] Mcinnes, J. (1971). Financial Control Systems for Multinational Operations: An Empirical Investigation. Journal of International Business Studies, 2, 11-28. https://doi.org/10.1057/PALGRAVE.JIBS.8490734.

[25] Hung, L., Doll, T., Barbosu, M., Luque, A., & Wang, D. (2012). An enhancement of the Role-Based Access Control model to facilitate information access management in context of team collaboration and workflow. Journal of biomedical informatics, 45 6, 1084-107 . https://doi.org/10.1016/j.jbi.2012.06.001.

[26] Zhang, L., Yu, Z., Wu, S., Zhu, H., & Sheng, Y. (2024). Adaptive Collaboration With Training Plan Considering Role Correlation. IEEE Transactions on Computational Social Systems, 11, 25-37. https://doi.org/10.1109/TCSS.2022.3204052.

[27] Wang, Z., Yu, X., Xue, P., Qu, Y., & Ju, L. (2023). Research on Medical Security System Based on Zero Trust. Sensors (Basel, Switzerland), 23. https://doi.org/10.3390/s23073774.

[28] Arora, S., & Tewari, A. (2023). Zero trust architecture in IAM with AI integration. International Journal of Science and Research Archive. https://doi.org/10.30574/ijsra.2023.8.2.0163.

[29] Alomari, M., Khan, H., Khan, S., Al-Maadid, A., Abu-Shawish, Z., & Hammami, H. (2021). Systematic Analysis of Artificial Intelligence-Based Platforms for Identifying Governance and Access Control. Security and Communication Networks. https://doi.org/10.1155/2021/8686469.

[30] Sharma, S. (2024). AI-Enhanced Cyber Threat Detection and Response Systems. Shodh Sagar Journal of Artificial Intelligence and Machine

Learning. https://doi.org/10.36676/ssjaiml.v1.i2.14.

[31] Pochu, S., & Nersu, S. R. K. (2024). Securing Agile Development: A Framework for Integrating Security into the Software Lifecycle. Bulletin of Engineering Science and Technology, 1(03), 77-88.

[32] kumar Karne, V., Mandaloju, N., Srinivas, N., & Engineer, S. V. N. S. C. Business & Social Sciences.

[33] Pochu, S., Nersu, S. R. K., & Kathram, S. R. (2024). Multi-Cloud DevOps Strategies: A Framework for Agility and Cost Optimization. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 7(01), 104-119.