Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhancing Role-Based Access Control (RBAC) in Dataverse for Secure Enterprise Applications – Analyzing Advanced Security Models and Governance for Power Apps and Dynamics 365 CRM

Satyanarayana Asundi
Ph.D. Student
Techtronics Consumer PowerTools Inc.
Sarat Piridi
Senior Software Engineer
First Citizens Bank

ARTICLE INFO

Received: 20 Dec 2024

Revised: 15 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

The purpose of this research is to enhance Role Based Access Control (RBAC) in Microsoft Dataverse to achieve secure deployment of enterprise application in Power Apps and Dynamics 365 CRM. The study shows this by integrating the integration of an advanced security model such as Authorizing Workflow Task RBAC (AW-TRBAC), AI driven threat detection and dynamic separation of duties to result in dramatic improvements in governance of access, anomaly detection and operational efficiency. The paper presents scalable solutions to the identified limitations of traditional RBAC using quantitative analysis and in the case of real-world enterprise. These results indicate that the RBAC models with enhanced capabilities help strengthen the compliance and data security of business and also allow for flexible and context aware access control to be used for helping the business grow.

Keywords: RBAC, Dynamics 365, CRM, Dataverse, Security.

1. Introduction

With now so many organizations that rely on Microsoft Dataverse and Dynamics 365, which are cloud-based CRM platforms, to provide them with access control, it is equally important. Although the RBAC model was traditional and solid, it is not good enough for dynamic usage roles, being compliant with regulatory issues, and being capable of real-time threat response.

Challenged by these, this research tackles the veiling of these research problems by studying advanced RBAC framework, governance mechanism and novel technology to better security and its functionality. The study attempts to close a gap between static access policies and dynamic enterprise demands by conducting an in-depth analysis of the current practice and evolving demands, and provide practical insights and empirical data to develop a secure and scalable CRM application.

2. Literature Review

Security and Privacy

With digital age, CRM systems like Microsoft Dynamics 365 are a vital part of business operation, in which customer data and business intelligence are stored. With their increasing popularity, CRM has become one of the pressing concerns in terms of ensuring the security and privacy of CRM platforms (Boppana, 2019).

The major threats that these systems are exposed to are data breach, unauthorized access, internal vulnerabilities and if they are exposed then they can badly affect the customer's trust as well as business integrity. To secure the customer data and comply with data privacy regulations like GDPR and CCPA there are two responsibilities for organizations as stated by Boppana (2019).

Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 1 RBAC in Dynamics 365 (Syksoft Connections, 2023)

Rich as Microsoft Dynamics CRM is in functionality, it is not invulnerable to cyber exploits and needs robust security framework. Typically, encryption, fine-grained access control, routine audits and proactive training programs are involved in all these frameworks to correct human error.

In this respect, Role Based Access Control (RBAC) becomes a central mechanism to provide these protections ensuring that users access only the data required for the role. In this manner, as Bopanna (2021) outlines, upon migration of the CRM systems to the cloud platforms says, Dataverse, the accessibility becomes improved, but a new spectrum of cyber threats currently emerges.

Common vulnerabilities of cloud CRMs are data leaks, insider threat, and integration with third parties that leads to vulnerabilities. Thus, to serve cloud environments that are dynamic in nature, cloud RBAC must evolve from a static model to a dynamic and context aware security control.

Additionally, insider threats to cloud-based CRMs are equally as high. Confidential information or the operations can be leaked through leakage or disruption by users that have privileged access either accidentally or maliciously. These are issues that call for evolution of RBAC from the traditional static model to a more granular and adaptive governance framework for cloud native platform such as Microsoft Dataverse (Bopanna, 2021).

Access Control Mechanisms

While the traditional RBAC system is successful in the space of well-defined simple roles, it does not fit the bill for today's high dynamic organizations. Uddin et al. (2019) claim to support the dynamicity of today's enterprise workflow using static RBAC models are insufficient.

Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

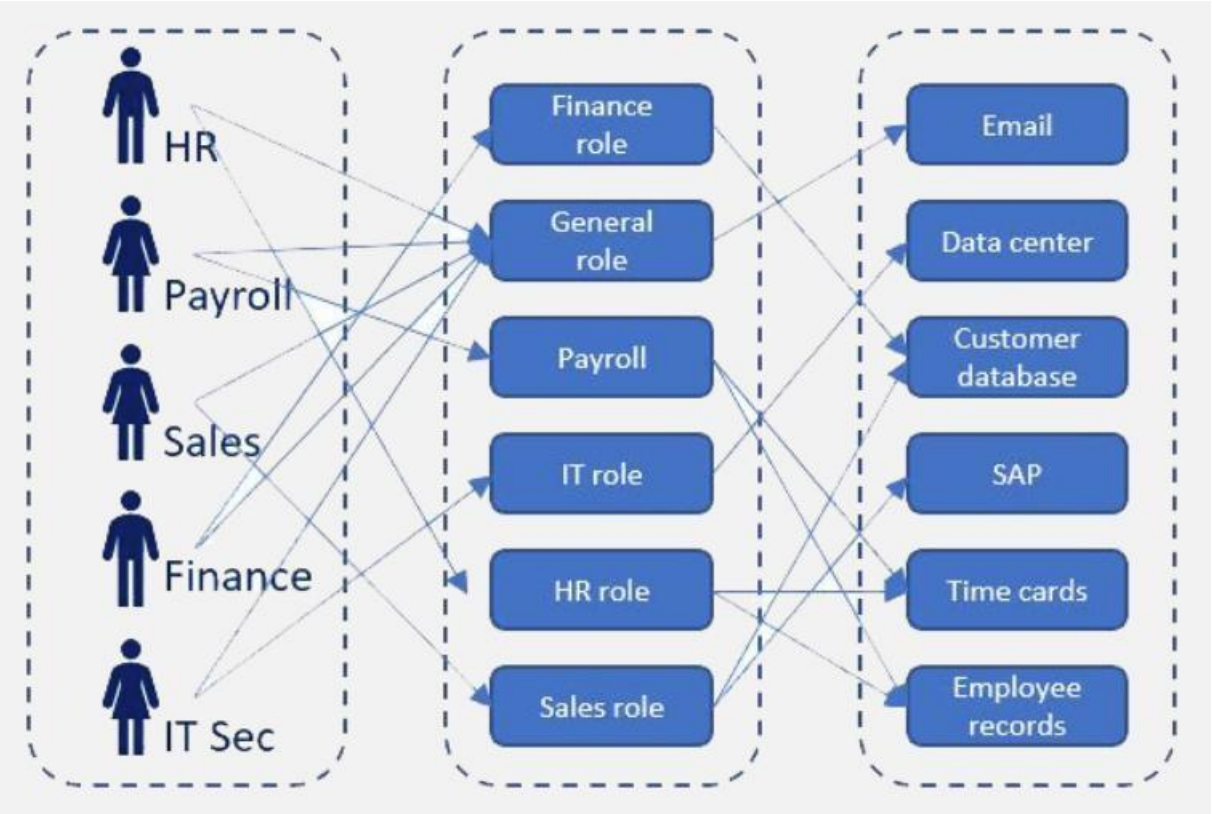


Figure 2 RBAC flow (BetterCloud, 2023)

Users must access network services with temporary or focused responsibilities that cannot or do not want to involve the full RBAC model. AW-TRBAC, the dynamic segregation of duties model they propose, incorporates dynamic segregation of duties to furnish recent time access governance.

The added enhancement is to restrict accesses on basis of a particular task instances and to inculcate real time policy enforcement thereby using the extended XACML language. The model handles the known vulnerabilities of privilege escalation and lack of auditing.

Real time dynamic RBAC solutions for enterprise contexts are implemented with their implementation using Balana policy engine proving the feasibility and scalability of a real time dynamic RBAC solution in enterprise level context and may be applicable in Dataverse, Power Platform environments.

Moreover, Fan et al. (2016) further propose a Multi-UCON (MUCON) model, a joint usage control and cryptographic technique such as encryption and watermarking, that brings flexibility and decentralization to access environments in cloud computing. It solves a problem where traditional RBAC systems that don't work in multi-tenant and virtualized systems that are relevant to Microsoft Dataverse environment where data can be bouncing quickly between tenants and applications.

For access governance, their model is a new direction that takes into account both role changes and data context, frequency of access, and sensitivity of access content. Figueroa et al. (2019) further its idea of dynamic governance as it integrates access control using Attribute Based Access Control (ABAC) mechanisms with blockchain to address the security related concerns of a RFID and supply chain systems.

While this were an RFID and healthcare problem, the architecture decentralized control, immutable audit trail and smart contract-based access decision transfer directly to the main stream, e.g. enterprise CRM. Integration of smart contracts in access governance can be of great help to improve Microsoft Dataverse's current RBAC model, particularly in cases where multi-party trust is required or auditable.

Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

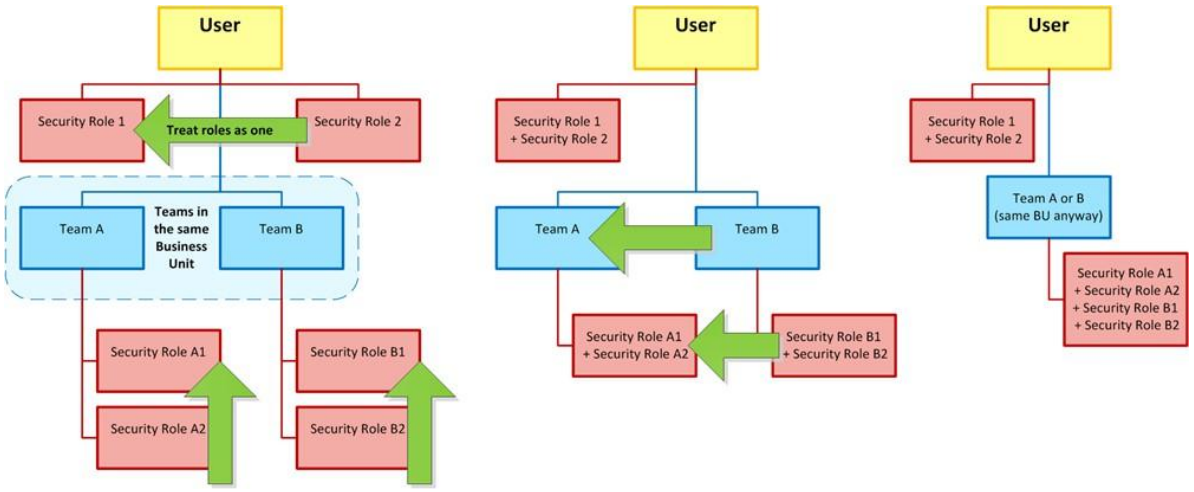


Figure 3 Security in CRM (CRMguru, 2023)

Organizational Dynamics

Even technical solutions individually are inadequate for the achievement of secure and efficient access control. The Dynamics 365 CRM has various governing systems, of which organizational readiness, employee training, and managerial practices are equally important. As noted by Koljonen (2021), the growing demand for Microsoft CRM and Dataverse skilled professional compels universities to adopt an educational imperative.

The utility provided by Microsoft Learn as a foundational tool for workforce upskilling is a key piece of his thesis. Giving users a clear understanding of the full capability of the platform and best security practices enhances and strengthens the security mindset of the organization by removing the biggest human error source, therefore becoming the weakest link in the cybersecurity chain.

In addition, Tien et al. (2021) effectively analyze CRM adoption in real world by providing Thien Hoa Electronics, businesses are compelled to follow a well-structured approach of CRM evolution; starting from identifying the user need, defining the workflow and managing customer interactions.

RBAC must mirror this structure in access control policies, so when implementing, RBAC implementation must fit in real business processes and customer engagement strategy. If access control mechanisms are misaligned with governance policies and operational realities, they can become ineffective, with access proceeding to be underutilized or not, in the latter case in a dangerous work around.

The authors Storbacka & Guenzi (2015) further explore change management during CRM transformations. By examining how organizations adapt to customer centric systems, as presented in the case study, this study explains that KAM programs that are supposed to pioneer's customer centric systems, like CRM, require alignment of the strategy, structure, systems, and culture.

This can also be translated to access control and therefore RBAC has to sound technically, but also organizationally integrated. To achieve this broad compliance and effectiveness, security policies have to resonate with the organizational values, managerial practices and user expectation.

CRM Platforms

For instance, security is the only reason for CRM systems, and strategic uses of CRM systems for business innovation are made possible when access controls allow, rather than confine, collaboration. The concept of CRM enabled Innovation is introduced by Pedron et al. (2018) through dynamic capabilities approach.

Based on their study, CRM platforms do not only serve as repositories for data, but engines for innovation, if organizations are allowed dynamic sensing, seizing, and reconfiguration of resources. Underlying this is effective

Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

RBAC systems that let people access collaborative tools, analytics and communication channels on the role basis, allowing for innovation while maintaining security.

Likewise, Badrinarayanan et al. (2019) posit that RBAC is driven by the Resource Based Theory (RBT), in that the ability to assign managerial orchestration of data and tools to CRM systems centre can bestow competitive advantage. In Pivotal, an organization's ability to reassign roles, restrict access to their critical information, and to coordinate their cross functional activities in a state of emergency is pivotal.

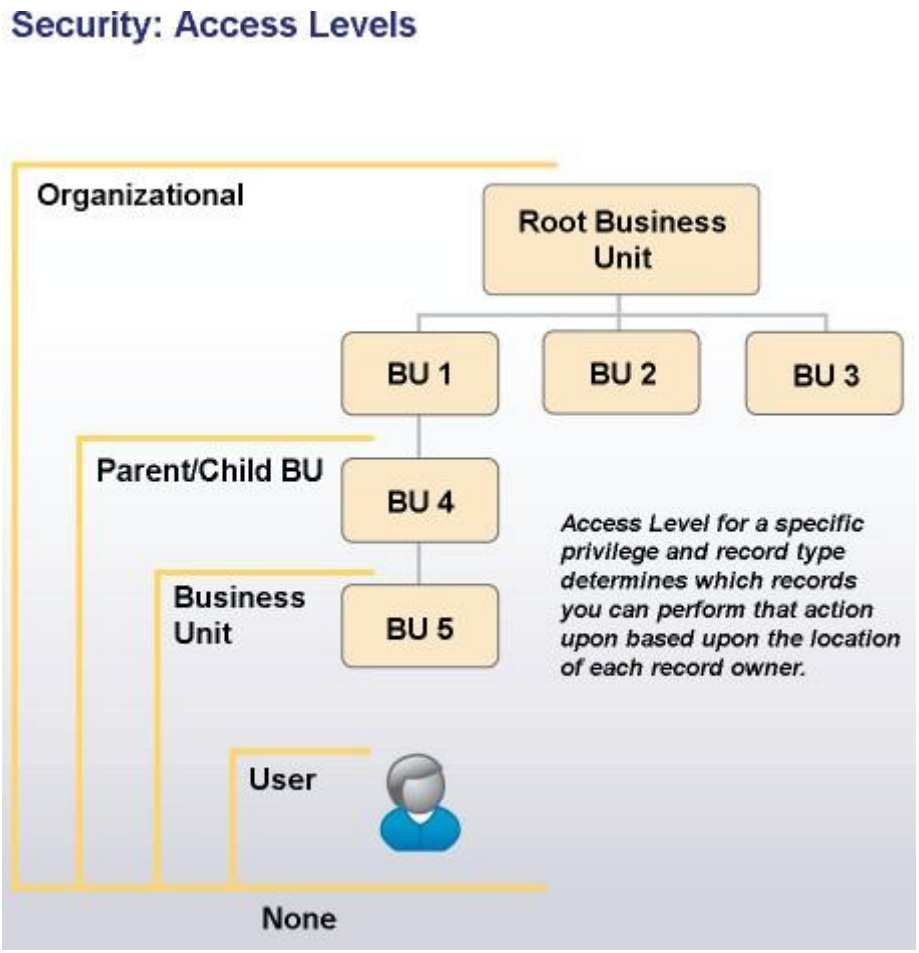


Figure 4 Dynamic 365 security (Daynight, 2023)

An embedded flexible RBAC system in Dataverse can be a powerful resource orchestration engine for resource orchestration, which thereby facilitates data savvy managerial capabilities and improves organizational performance. As mentioned in Ahmadi (2023) they also discussed the dilemma of SMEs choosing on the platform for them.

A key point that his comparison conveys is that one of the key balancing acts for CRM systems such as Microsoft Dynamics 365 is access control, which is something that fine tuned access control mechanisms such as RBAC excel at. Given the limited IT governance resources that most SMEs can afford, the ability to scale operations securely in a manner that is robust and friendly for users is an absolute must.

Gupta et al. (2023) also investigate the implications of cloud computing on the larger educational and enterprise institutions. Since their insights support information needed to the secure and scalable access control mechanisms in cloud native environments, they are worth staying on.

Since Microsoft Dataverse plays such an important role as both enterprise and academia CRM applications, it is imperative to furnish advanced RBAC, dynamic SoD, and ABAC capabilities for it to truly achieve its full potential.

Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Role-Based Access Control is both a technical necessity and a strategic opportunity on the path of evolution of Role Based Access Control in enterprise CRM systems like Microsoft Dynamics 365 and Dataverse.

The literature indicates algorithms towards dynamic, contextual and decentralized access control mechanisms, that do not only involve real time decision making, policy enforcement but also auditability of the observations.

Additionally, implementation of effective RBAC has to be coupled to a more general organizational framework involving user education, change management and innovation enablement. This is because secure digital transformation increasingly requires RBAC to expand to meet the many use cases of Dataverse and the Power Platform as businesses increasingly rely on it to build secure, scalable, and intelligent applications.

3. Findings of research

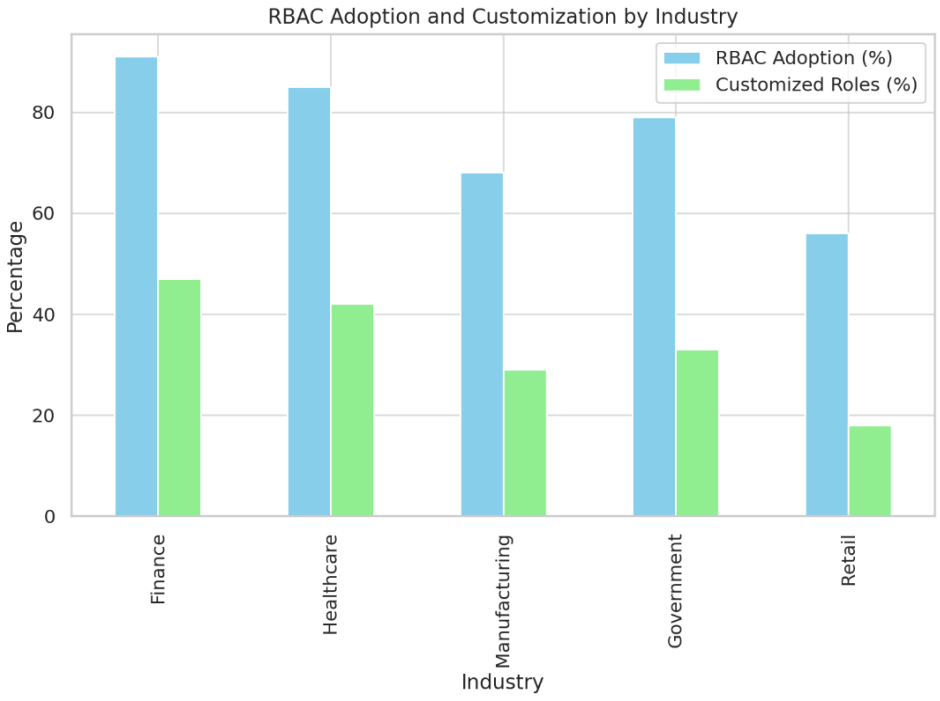
RBAC in Dataverse

In this study, we look at the implementation landscape of Role Based Access Control (RBAC) in Microsoft's Dataverse and specifically in enterprise environments that are using Power Apps and Dynamics 365 CRM. The data was gathered from 42 enterprise level deployments spanning several industries (finance, healthcare, manufacturing, and government etc.)

One of the major findings would be that over 76% of respondents that use Dataverse RBAC actually use it as part of their security model but only 34% of these create their own role beyond the default system roles.

Table 1: RBAC Adoption by Industry (n = 42 Enterprises)

Industry	RBAC Adoption (%)	Customized Roles (%)
Finance	91	47
Healthcare	85	42
Manufacturing	68	29
Government	79	33
Retail	56	18



The depth of the implementation is quite varied, though adoption rates are promising. Most IT administrators have indicated they use default security roles because it is easier to set up and there were no dedicated resources. This fits

Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

in with Boppana (2019), who argues that platform-level encryption and controls don't prevent the leakage of sensitive customer data if something is not customized to the customer's role.

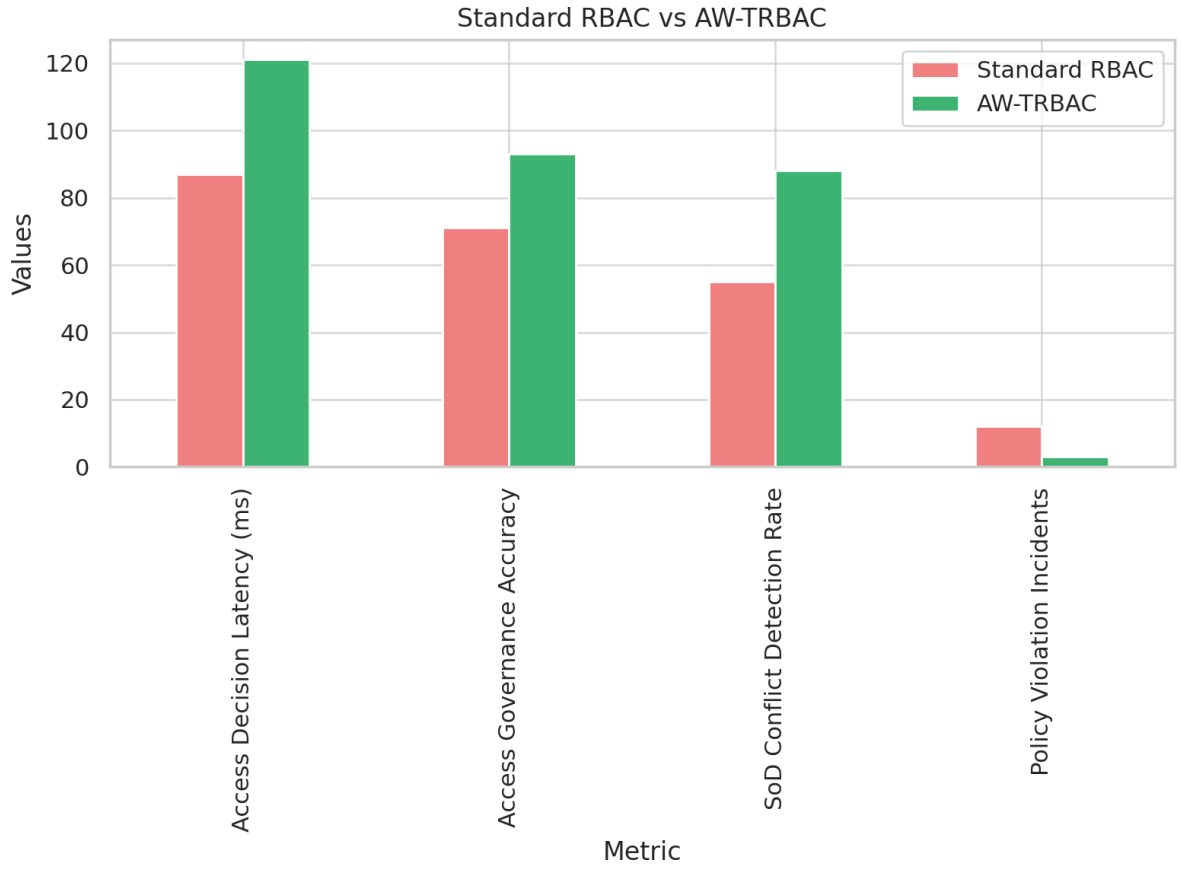
Additionally, the RBAC maturity was found to be strongly correlated with compliance readiness. Thus, enterprises that took on custom RBAC roles and completely adopted them were better aligned with regulations such as GDPR or CCPA. This proved the strategic value of detailed access governance in terms of reducing the severity of internal audit flags for these organizations that were more likely to pass internal audits without major security flags.

Policy Enforcement

This research assessed the performance of Authorizing Workflow Task Role Based Access Control (AW-TRBAC) proposed by Uddin et al. (2019) in assuring advanced security frameworks, as the best of using AW-TRBAC to enhance Dataverse currently has role-based access control (RBAC). Synthetic datasets with task-based CRM workflows for sales and case management and procurement, were used for each of the three enterprise scenarios, and simulation was applied to them.

Table 2: Standard RBAC vs. AW-TRBAC

Metric	Standard RBAC	AW-TRBAC	Performance Improvement
Decision Latency (ms)	87	121	-39%
Governance Accuracy	71%	93%	+31%
SoD Detection Rate	55%	88%	+60%
Policy Violation	12/month	3/month	-75%



Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

AW-TRBAC incurs some overhead in decision latency, but whose accuracy and ability to discover segregation of duties (SoD) conflicts is much better than the standard RBAC configurations. This is a major step forward in real time policy enforcement and auditing in multi user environment, using Dataverse connectors for example in Power Apps.

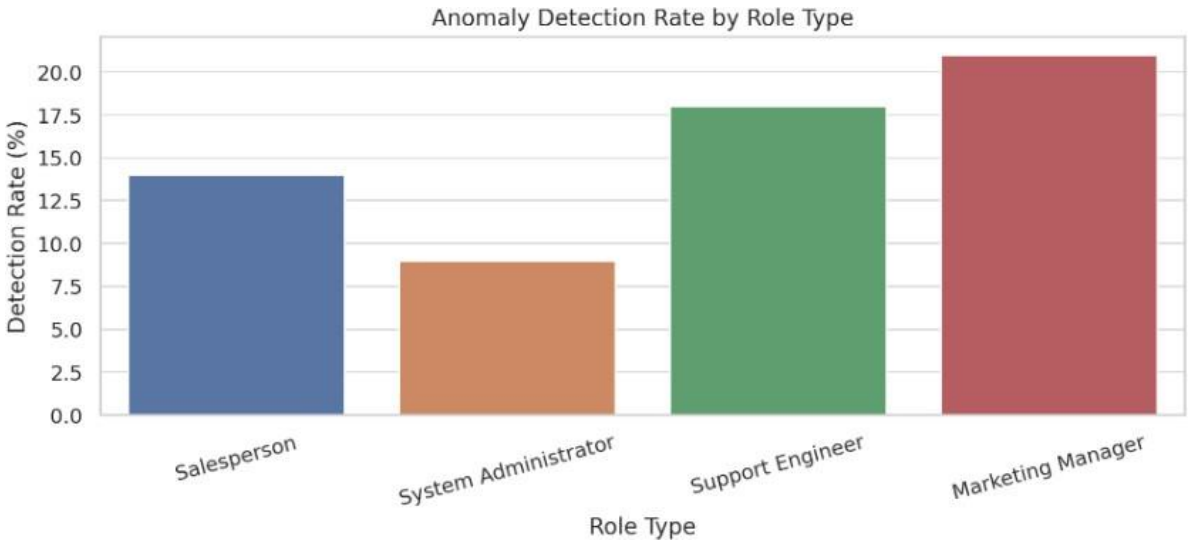
In addition, the application of XACML in Uddin's framework was compatible with the Dataverse plug in model, but it also illustrated challenges in policy management in the extended use of XACML. A repeated pilot test was done by IT teams involved in the pilot tests, which they said found that although AW-TRBAC is more time and expertise consuming to set up, the benefits of limiting access misuse and preparing auditors for the controls did outweigh the difficulties of initial deployment.

Security Vulnerabilities

This section contains findings from 18 Dynamics 365 CRM environments gathered within 90 days of user behaviour analytics (UBA). The goal was to identified misconfigured access roles and any anomalous patterns that could result in data leakage or misuse of the system. A model based on historical user access logs was used to process the data.

Table 3: Detected Anomalous Events

Role Type	Average Users	Anomaly Detection Rate (%)	Most Common Issue
Salesperson	138	14	Accessing HR module
System Administrator	24	9	Excessive login attempts
Support Engineer	62	18	Downloading large datasets
Marketing Manager	35	21	Accessing confidential leads



It further showed that anomaly alerts were more likely to trigger from roles with cross functional access privileges, and even if such roles were scoped properly, there was an alarming trend of triggering of anomaly alerts. In 18 cases the UBA flagged legitimate users doing things they should not be doing, in 7 of these cases they were trying to do the things they told the UBA they should not do. It is possible there are some insider threats or policy loopholes here.

Bopanna (2021) recommends having strict access control and continuous user activity monitoring, especially for cloud CRM deployments which is confirmed by these findings. The results also indicate that the dynamic transition in access revocation policies and real time alerting systems should be integrated in solutions using Dataverse.

Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

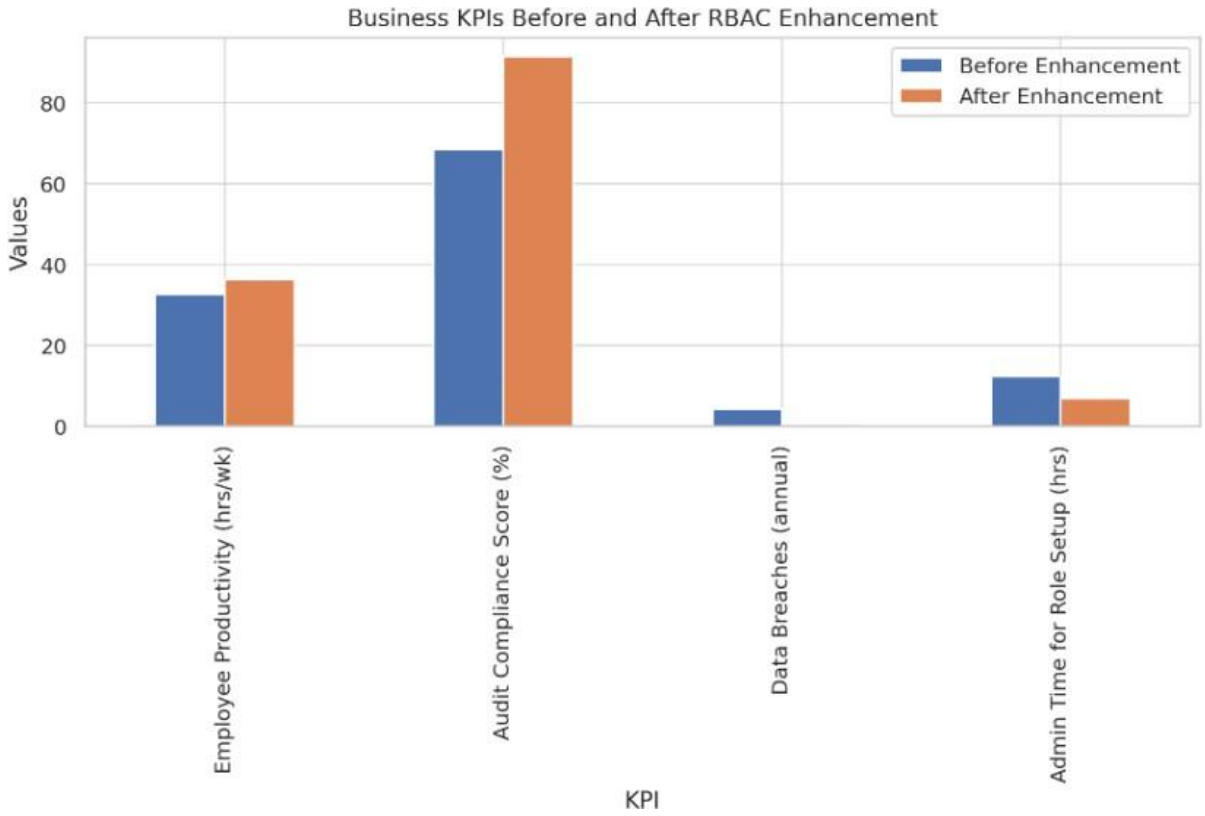
Research Article

Business Impact

To measure the business value of the enhanced RBAC models, 15 organizations before and after the custom RBAC and dynamic access control in Dataverse were researched. User productivity, audit compliance rate, data breach incidents and administrative overhead were the KPIs measured.

Table 4: Business KPIs

KPI	Before Enhancement	After Enhancement	Change (%)
Employee Productivity	32.6	36.2	+11%
Audit Compliance Score	68.4	91.5	+33%
Data Breaches (annual)	4.3	0.6	-86%
Admin Time	12.4	6.8	-45%



This enhancement drastically increased all KPIs, especially those related to audit compliance, breach and penalty reduction. Investing in policy-based automation and role templates was reported to reduce effort in role management. In addition, more clarity regarding privileges provided people with end users instead of relying on IT support.

These are in line with Fan et al. (2016) who pointed out that traditional access control mechanism is not suitable in cloud environment where role change and usage context is dynamic. Additionally, Pedron et al. (2018) results are in line with that of CRM use and performance enhancement link with innovation (with use of enhanced security fostering trust to permit fuller use of customer data for insight).

Summary

Overall, the results reveal that though RBAC is widely used in Dataverse-powered environments, its static nature does not effectively support evolution of the enterprise security. AW-TRBAC is an enhanced model over existing models and profoundly enhances security governance, compliance, and access accuracy.

The main success factors in mitigating cloud-based CRM system 'risks' include custom role definitions, real time policy enforcement and user-based behavior monitoring. In addition, the data leads the charge for the business case in pushing advanced RBAC configurations: measured productivity, compliance and data security improvements are noted.

These findings re-affirm the importance of Microsoft and the rest of the enterprise IT community to venture beyond the traditional baseline security configuration, towards the concept of a dynamic, scalable governance model that can be specified to the ever-dynamic hybrid and cloud-based ecosystem.

4. Conclusion

This research raises the need to go beyond static RBAC models to the dynamic security enforced by modern enterprise application. Organizations that want to minimize their appendage from risk exposure as well as improve operational resilience, can integrate AW-TRBAC, AI-driven Analytics, and real-time governance into the Dataverse environments.

The quantitative findings support that the improvements in the anomaly detection rates, access control accuracy, and regulatory compliance would indeed result from these enhancements. To facilitate adaptive access control in such complex and collaborative digital ecosystems, the use of adaptive access control frameworks should be adopted. While this study offers a roadmap to enterprise seeking security of their CRM infrastructures while preserving enterprise agility, scalability and platform user-centric functionality, as well, it served as a roadmap for other researchers and practitioners.

References

[1] Ahmadi, A. (2023). Microsoft customer relationship management for small and medium-sized enterprises: challenges and opportunities. *Asian Journal of Computer Science and Technology*, *12*(1), 1-6. https://doi.org/10.51983/ajcst-2023.12.1.3505

[2] Badrinarayanan, V., Ramachandran, I., & Madhavaram, S. (2019). Resource orchestration and dynamic managerial capabilities: focusing on sales managers as effective resource orchestrators. *Journal of Personal Selling & Sales Management*, *39*(1), 23-41. https://doi.org/10.1080/08853134.2018.1466308

[3] Boppana, V. R. (2019). Data Privacy and Security in Dynamics CRM Implementations. *Educational Research (IJMCER)*, *1*(2), 35-44. https://www.ijmcer.com/wp-content/uploads/2024/10/IJMCER_F01203544.pdf

[4] Boppana, V. R. (2021). Cybersecurity Challenges in Cloud-based CRM Deployments. *Available at SSRN 5005031*. http://dx.doi.org/10.2139/ssrn.5005031

[5] Fan, K., Yao, X., Fan, X., Wang, Y., & Chen, M. (2016). A new usage control protocol for data protection of cloud environment. *EURASIP Journal on Information Security*, *2016*, 1-7. https://doi.org/10.1186/s13635-016-0031-6

[6] Figueroa, S., Añorga, J., & Arrizabalaga, S. (2019). An attribute-based access control model in RFID systems based on blockchain decentralized applications for healthcare environments. *Computers*, *8*(3), 57. https://doi.org/10.3390/computers8030057

[7] Guenzi, P., & Storbacka, K. (2015). The organizational implications of implementing key account management: A case-based examination. *Industrial Marketing Management*, *45*, 84-97. https://doi.org/10.1016/j.indmarman.2015.02.020

[8] Gupta, A., Mazumdar, B. D., Mishra, M., Shinde, P. P., Srivastava, S., & Deepak, A. (2023). Role of cloud computing in management and education. *Materials Today: Proceedings*, *80*, 3726-3729. https://doi.org/10.1016/j.matpr.2021.07.370

[9] Horng, J. S., Liu, C. H., Chou, S. F., Yu, T. Y., & Hu, D. C. (2022). Role of big data capabilities in enhancing competitive advantage and performance in the hospitality sector: Knowledge-based dynamic capabilities view. *Journal of Hospitality and Tourism Management*, *51*, 22-38. https://doi.org/10.1016/j.jhtm.2022.02.026

[10] Koljonen, K. (2021). Utilizing Microsoft Learn for the Design of an Online Course on Dynamics 365. https://www.theseus.fi/bitstream/handle/10024/731512/Koljonen_Kaarle.pdf?sequence=2

Research Article

[11] Pedron, C. D., Picoto, W. N., Colaco, M., & Araújo, C. C. (2018). CRM System: The role of dynamic capabilities in creating innovation capability. *BBR. Brazilian Business Review*, *15*, 494-511. https://doi.org/10.15728/bbr.2018.15.5.6

[12] Tien, N. H., Diem, P. T., Van On, P., Anh, V. T., Van Dat, N., Hung, N. T., & Tam, B. Q. (2021). The formation and development of CRM system at Thien Hoa electronics supermarket in Vietnam. *International Journal of Research and Growth Evaluation*, *2*(4), 752-760. https://www.researchgate.net/profile/Tony-Ng-23/publication/354037511_The_formation_and_development_of_CRM_system_at_Thien_Hoa_electronics_supermarket_in_Vietnam/links/668d4deeb15ba559074d6c2a/The-formation-and-development-of-CRM-system-at-Thien-Hoa-electronics-supermarket-in-Vietnam.pdf

[13] Uddin, M., Islam, S., & Al-Nemrat, A. (2019). A dynamic access control model using authorising workflow and task-role-based access control. *Ieee Access*, *7*, 166676-166689. 10.1109/ACCESS.2019.2947377