Computer Fraud and Security
ISSN (online): 1873-7056

Role-Based Access Control and Conditional Access Policies in Microsoft 365 for Secure Academic Collaboration

Kishore Thota

Systems Architect and Principal Consultant (Independent Researcher)

Exotic IT Services Corporation, Toronto, Canada

University of Bridgeport, Bridgeport, Connecticut, USA

Hi-Link Technology Group, New York, USA

Email: kishorethota563@gmail.com

ORCID: 0009-0006-3107-4717

Abstract

Academic institutions are depending more and more on cloud-based collaboration tools like Microsoft 365 in the age of digital transformation to support administrative, teaching, and research tasks. In order to ensure safe academic collaboration among 10 Indian higher education institutions, this study examined the application and effects of Conditional Access Policies (CAP) and Role-Based Access Control (RBAC) within Microsoft 365. The study evaluated the degree of awareness, policy deployment procedures, and perceived results among IT administrators, academics, and administrative staff using a mixed-methods approach that included questionnaires, interviews, and system configuration checks. IT staff demonstrated a high degree of awareness and policy enforcement, according to the results, however faculty members had little knowledge of security controls, which frequently caused usability issues. Advanced restrictions like device compliance standards were less often adopted, although the majority of institutions had already put in place basic RBAC and CAP features like role groups and Multi-Factor Authentication. Users recognized notable gains in data security and system credibility, notwithstanding certain perceived barriers to collaboration effectiveness. The study came to the conclusion that attaining security and collaboration in academic settings requires a well-rounded approach that includes user training, inclusive policy formulation, and adaptive access controls.

Keywords: Microsoft 365, Role-Based Access Control, Conditional Access Policies, Academic Collaboration, Cloud Security, Higher Education, Data Governance, Multi-Factor Authentication.

1. INTRODUCTION

The use of cloud-based systems has become crucial in the quickly changing higher education scene in order to facilitate digital administration, research cooperation, and distant learning. Academic institutions throughout the world have adopted Microsoft 365, a top suite of productivity and communication tools, because of its scalability, integration capabilities, and support for collaborative work settings. But there are also serious issues with data privacy, access control, and information security that arise from our growing reliance on digital infrastructure.

From student records and administrative files to research results and intellectual property, academic institutions handle sensitive data. A growing emphasis on putting strong security measures in place inside systems like Microsoft 365 is a result of the necessity to guarantee that only authorized personnel have access to particular types of data. Conditional Access Policies (CAP) and Role-Based Access Control (RBAC) are two of the most important techniques in this situation. By allowing organizations to allocate rights according to user roles, RBAC makes sure that users can only access the things they are permitted to use. By implementing dynamic access rules based on contextual variables including device compliance, user location, risk levels, and authentication strength, CAP further improves security.

Despite the strength of these features, there are particular difficulties in using them successfully in educational settings. Academic institutions, in contrast to business settings, frequently involve a variety of user groups, such as researchers, faculty, students, and outside collaborators, all of whom have varying access needs. Thus, it is crucial to strike a balance between security and usability. Furthermore, the uniform implementation of access

regulations may be impacted by differences in the technological literacy and knowledge of administrative and faculty personnel.

In order to determine how well RBAC and CAP secure academic collaboration without sacrificing usability, this study looked at how these features have been applied in Microsoft 365 in Indian educational institutions. The study evaluated awareness levels, real-world deployment strategies, perceived advantages, and typical obstacles, providing valuable information on how to accomplish safe, role-aware, and flexible digital collaboration in the classroom.

2. LITERATURE REVIEW

Uddin, Islam, and Al-Nemrat (2019) suggested a dynamic access control paradigm that combined authorization procedures with task-role-based access control. In order to improve security and operational efficiency, their study focused on flexibility in modifying access rights in response to real-time task assignments. In academic institutions, where user tasks frequently alternate between teaching, research, and administrative duties, this strategy proved especially pertinent. Institutions were able to better match access credentials with functional responsibilities in Microsoft 365 settings thanks to the dynamic nature of their model.

Servos and Osborn [11] carried out an extensive analysis of attribute-based access control (ABAC) systems, emphasizing both recent developments and unresolved research issues. Their results showed that ABAC was still underutilized because of its complexity in real-world implementation, despite its strength in handling fine-grained access decisions based on user, object, and environmental attributes. Although Microsoft 365's conditional access controls, which enforce access based on geography or device compliance, reflect similar attribute-based reasoning, the complexity of ABAC may make it more difficult to implement in academic contexts than RBAC.

Ouaddah, Abou Elkalam, and Ait Ouahman (2016) presented FairAccess, an access control architecture for Internet of Things (IoT) ecosystems built on the blockchain. Their study offered important insights into decentralized access control mechanisms that guaranteed transparency, traceability, and resistance to manipulation, even though it did not specifically target academic collaboration. Future advancements in safe academic data sharing, especially in multi-institution collaborative research collaborations, may be influenced by the ideas covered in FairAccess, such as decentralized trust and policy immutability.

Tabrizchi and Kuchaki Rafsanjani (2020) provided a thorough analysis of cloud computing security challenges, highlighting important problems such insider threats, data breaches, identity management, and access control. Their research highlighted how crucial it is to use adaptive access control systems and layered security architectures in order to reduce risks in multi-tenant cloud settings such as Microsoft 365. In line with the need for RBAC and conditional access restrictions in education, the survey highlighted the risk of cloud systems lacking appropriate role and context-aware access setups.

Sun [12] centered on cloud computing data security and privacy, providing an overview of mitigating techniques and a classification of common threats. According to the survey, access management is still a crucial component of any cloud security strategy, particularly when managing sensitive institutional data and personally identifiable information (PII). Context-sensitive access controls, such as conditional access policies, which dynamically impose authentication and compliance checks based on user behavior and environmental circumstances, were encouraged by the research.

RESEARCH METHODOLOGY

Research Design

This study used a mixed-methods research design, combining qualitative and quantitative techniques to provide a comprehensive understanding of how academic institutions implement Conditional Access Policies (CAP) and Role-Based Access Control (RBAC) in Microsoft 365 environments. Data triangulation was made possible by the mixed-methods approach, which enhanced the findings' dependability, depth, and trustworthiness. Through a combination of narrative insights and statistical research, the study sought to document the human experiences as well as the technical execution of policy implementation.

2.1. Population and Sampling

The study focused on academics, system security officers, and IT administrators in Indian higher education institutions that have implemented Microsoft 365 for academic collaboration. Ten organizations recognized for their proactive use of cloud-based tools and digital security procedures were chosen using a purposive sample technique. For the purpose of gathering data via surveys and interviews, a total of 60 participants were found and enlisted among these institutions. To guarantee balanced viewpoints, this comprised 40 teaching or administrative workers and 20 IT/security staff.

2.2. Data Collection Methods

Surveys

IT staff and faculty personnel were given a structured questionnaire to gauge their knowledge, happiness, and use of Microsoft 365's RBAC and CAP features. In order to quantify respondents' attitudes and experiences statistically, the questionnaire had a number of Likert-scale items, with 1 denoting "strongly disagree" and 5 denoting "strongly agree." Over the course of three weeks, the survey was circulated and gathered electronically.

Semi-Structured Interviews

IT administrators and security personnel participated in semi-structured interviews to examine more complex viewpoints. Finding practical difficulties, decision-making techniques, and institutional approaches to the enforcement of access control policies were the main topics of the interviews. Each virtual session lasted between thirty and forty-five minutes. Informed consent was obtained before the interviews were taped, and they were transcribed for qualitative analysis.

System Configuration Review

To verify survey and interview data with real-world deployment procedures, a thorough examination of anonymized Microsoft 365 tenant configurations was conducted. Audit logs, conditional access settings, role assignment hierarchies, and compliance setups were all analyzed throughout this evaluation. Institutions offered sanitized datasets that represented actual operational circumstances but did not include personal identification.

2.3. Data Analysis Techniques

In order to find common trends and variances across various institutions and user roles, quantitative data gathered through surveys were analyzed using cross-tabulation and descriptive statistics (means, percentages).

NVivo software was used to process the semi-structured interviews' qualitative data. Recurring themes including "ease of configuration," "user resistance," "collaboration disruptions," and "compliance efficiency" were found using a thematic coding technique.

The results of system configuration reviews were contrasted with a compliance checklist derived from the National Institute of Standards and Technology's (NIST) Cybersecurity Framework and Microsoft's RBAC/CAP best practices. This served as a standard by which to measure the institutional maturity of the application of access control policies.

3. RESULTS AND DISCUSSION

The results of the surveys, interviews, and system configuration assessments carried out at 10 Indian higher education institutions are shown in this section. The outcomes show the degree of implementation of Microsoft 365's Conditional Access Policies (CAP) and Role-Based Access Control (RBAC), the difficulties encountered, and the perceived efficacy by administrators and users. These results are interpreted in light of the study's goals and the body of research on safe academic cooperation.

3.1. Awareness and Adoption Levels of RBAC and CAP

Survey responses revealed a moderate to high level of awareness among IT administrators regarding RBAC and CAP features in Microsoft 365. Faculty awareness, however, remained limited. Table 1 summarizes the levels of awareness reported across different user roles.

Table 1: Awareness of RBAC and CAP by User Role

User Role	High Awareness (%)	Moderate Awareness (%)	Low Awareness (%)
IT Administrators	80%	15%	5%
Security Officers	70%	25%	5%
Faculty Members	25%	40%	35%
Administrative Staff	30%	50%	20%

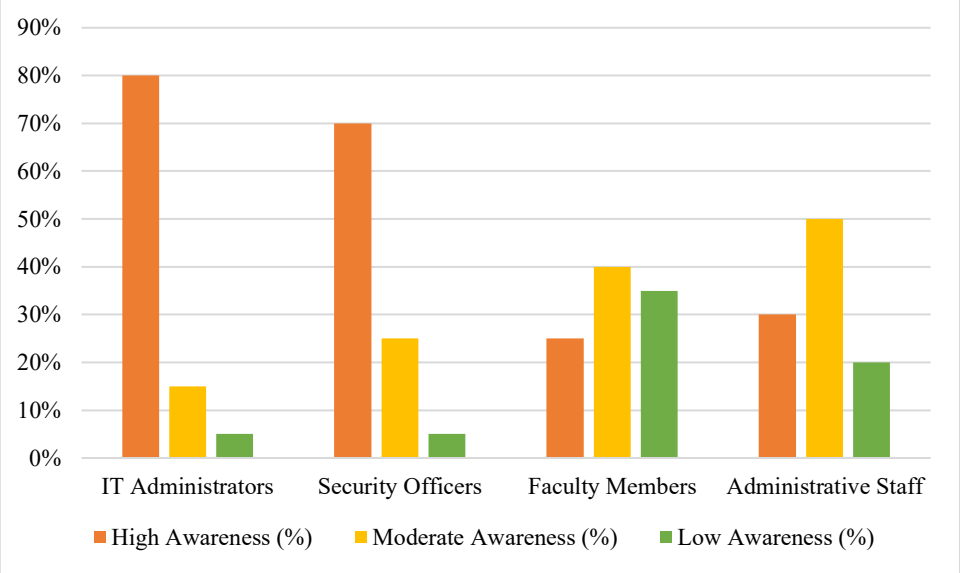

Figure 1: Awareness of RBAC and CAP by User Role

The data makes clear that security professionals and IT managers were well-versed in access control systems. Faculty and administrative personnel, on the other hand, were less knowledgeable and frequently relied on administrator settings or defaults rather than actively participating in the implementation of policies. This indicated a potential training gap for end users that could impede full system optimization.

3.2. Implementation Practices and Policy Enforcement

Configuration reviews and interviews indicated varied levels of RBAC and CAP implementation. Institutions with dedicated security teams demonstrated stricter adherence to best practices. Table 2 illustrates the implementation frequency of key security policies across the ten institutions studied.

Table 2: Implementation of Key Microsoft 365 Security Policies

Security Policy	Institutions Implemented (n=10)	Implementation Rate (%)
Role-Based Access Groups Configured	9	90%
Conditional Access for Location	7	70%
MFA (Multi-Factor Authentication)	8	80%
Device Compliance-Based Access	6	60%
Session Timeout Policies	5	50%

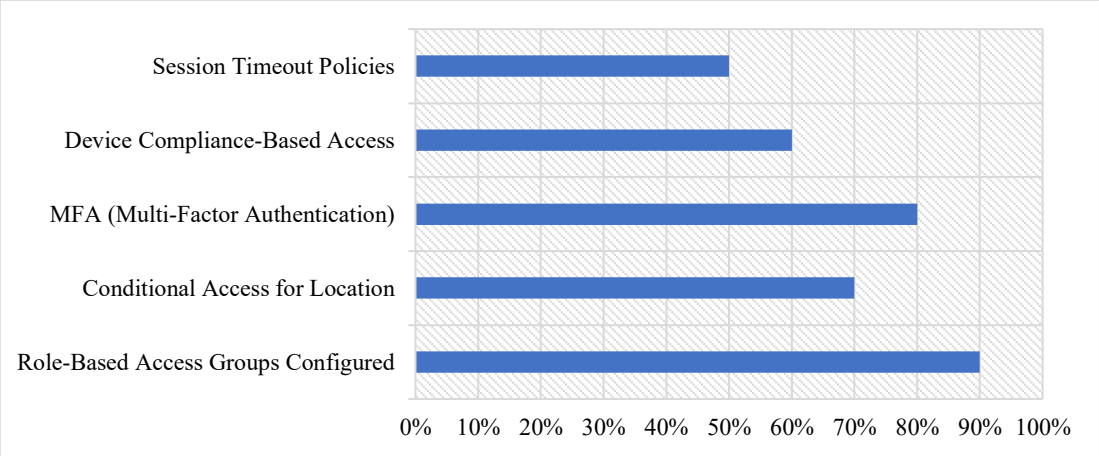

Figure 2: Implementation of Key Microsoft 365 Security Policies

According to the data, the majority of universities have implemented MFA protocols and simple RBAC structures. Advanced CAPs, such as session timeout limits and device compliance, were applied less frequently, nonetheless. Institutions stated that obstacles to complete deployment included issues including user reluctance, technological difficulty, and license restrictions.

3.3. Perceived Impact on Collaboration and Security

Survey and interview feedback suggested that security policies improved trust in data handling and user accountability, though occasional disruptions in access and user experience were reported. Table 3 reflects user perceptions of how the implemented policies affected collaboration.

Table 3: Perceived Impact of RBAC and CAP on Academic Collaboration

Perceived Impact	IT Admins (%)	Faculty (%)	Admin Staff (%)
Improved Data Security	100%	65%	75%
Reduced Unauthorized Access	95%	55%	60%
Hindered Collaboration Efficiency	20%	45%	30%
Increased Trust in System Use	90%	70%	80%

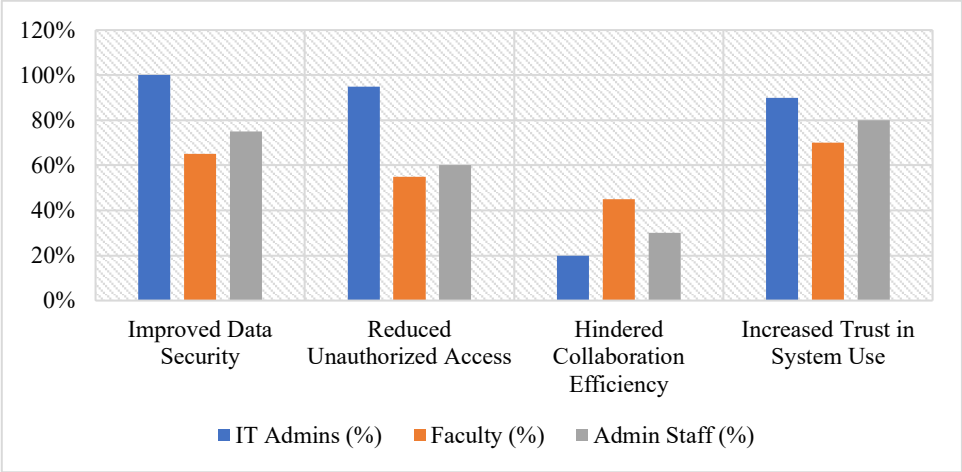

Figure 3: Perceived Impact of RBAC and CAP on Academic Collaboration

Nearly half of the faculty members said that policy enforcement, particularly with regard to CAPs, was a hindrance to smooth collaboration, even though all IT administrators agreed that data security had improved and dangers

had decreased. These issues frequently had to do with device compliance enforcement, VPN limitations, or timeouts. The significance of inclusive policy formulation is demonstrated by the lower number of unfavorable experiences reported by institutions that included academics in access design decisions.

General Observations

- Institutions with automated policy templates in Microsoft 365 reported higher consistency in policy enforcement.
- Lack of user-specific training emerged as a recurrent challenge in most academic settings.
- Smaller institutions without dedicated security teams had inconsistent implementations, sometimes relying on external consultants.

The findings indicated that while RBAC and CAP features in Microsoft 365 significantly strengthened data security in academic institutions, their effectiveness depended largely on user awareness, administrative planning, and policy customization. A balanced strategy involving security enforcement and usability support was essential for ensuring both safety and collaboration continuity.

4. CONCLUSION

According to the study, by lowering unauthorized access and enhancing data governance, the deployment of Role-Based Access Control (RBAC) and Conditional Access Policies (CAP) in Microsoft 365 greatly improved academic institutions' security posture. Collaboration was more efficient and smooth in institutions with well-organized access policies and greater user awareness. But the study also found that faculty members were not always aware of advanced CAP features, and that rigorous security configurations occasionally caused productivity delays. In order to guarantee safe and effective academic collaboration, the results underscored the necessity of a well-rounded strategy that combines strong security measures with user-centered design and training.

REFERENCES

[1] Alreshidi, E., Mourshed, M., & Rezgui, Y. (2018). Requirements for cloud-based BIM governance solutions to facilitate team collaboration in construction projects. Requirements engineering, 23(1), 1-31.

[2] Bernal Bernabe, J., Hernandez Ramos, J. L., & Skarmeta Gomez, A. F. (2016). TACIoT: multidimensional trust-aware access control system for the Internet of Things. Soft Computing, 20(5), 1763-1779.

[3] Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43-62.

[4] Correia, A. P., Liu, C., & Xu, F. (2020). Evaluating videoconferencing systems for the quality of the educational experience. Distance Education, 41(4), 429-452.

[5] Durairaj, M., & Manimaran, A. (2015). A study on security issues in cloud based e-learning. Indian Journal of Science and Technology, 8(8), 757-765.

[6] Ellcessor, E. (2016). Restricted access: Media, disability, and the politics of participation (Vol. 6). NYU Press.

[7] Fecher, B., Friesike, S., & Hebing, M. (2015). What drives academic data sharing?. PloS one, 10(2), e0118053.

[8] Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. Journal of Information privacy and security, 11(1), 38-54.

[9] Miao, Y., Liu, X., Choo, K. K. R., Deng, R. H., Li, J., Li, H., & Ma, J. (2019). Privacy-preserving attribute-based keyword search in shared multi-owner setting. IEEE Transactions on Dependable and Secure Computing, 18(3), 1080-1094.

[10] Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016). FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and communication networks, 9(18), 5943-5964.

[11] Servos, D., & Osborn, S. L. (2017). Current research and open problems in attribute-based access control. ACM Computing Surveys, 49(4), 1–45. https://doi.org/10.1145/3007204

[12] Sun, P. J. (2019). Privacy protection and data security in cloud computing: a survey, challenges, and solutions. Ieee Access, 7, 147420-147452.

[13] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: Issues, threats, and solutions. The Journal of Supercomputing, 76(12), 9493–9532. https://doi.org/10.1007/s11227-020-03213-1

[14] 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. https://doi.org/10.1109/ACCESS.2019.2947377

[15] Zhaofeng, M., Xiaochang, W., Jain, D. K., Khan, H., Hongmin, G., & Zhen, W. (2019). A blockchain-based trusted data management scheme in edge computing. IEEE Transactions on Industrial Informatics, 16(3), 2013-2021.

[16] Hu, V. C., Kuhn, D. R., & Ferraiolo, D. F. (2014). Attribute based access control (ABAC) definition and considerations (NIST SP 800-162). National Institute of Standards and Technology.

[17] Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richter, S., & Lefkovitz, N. (2017, update 2019). Digital Identity Guidelines: Authentication and Lifecycle Management (NIST SP 800-63B). National Institute of Standards and Technology.