Enhancement of Security Mechanisms for an Open Information Platform Supporting the Publication of Scientific Research

Roman Moroz[1]

[1] *Lviv Polytechnic National University, Bandery St. 12, 79013 Lviv, Ukraine*

Abstract

A review of recent publications revealed limitations of current open publication systems in access control, data and metadata protection, and integration with external services. Threats were clarified and attack vectors classified to systematize risks originating from both internal and external environments, including unauthorized user actions, content modification, breaches in the review process, and infrastructure vulnerabilities. An integrated security model for the communication subsystems of the publication platform was developed to enhance security mechanisms, including the combination of RBAC and ABAC models for differentiated access control, the use of multi-level encryption and key management systems, UEBA algorithms for anomaly detection, and authentication protocols to ensure data integrity.

Keywords

Access management, metadata control, information protection, user activity auditing, authentication, ethical standards, publication workflow

Introduction

Contemporary scientific communication increasingly relies on open digital infrastructures that support the complete publication workflow, from manuscript submission to dissemination of published materials. Such platforms integrate editorial management, peer review organization, archive formation, and interoperability with international identifiers and services, facilitating interaction among a large number of users with different roles and ensuring compatibility with external systems, including identification registries, bibliometric databases, and long-term data preservation systems. The use of cloud technologies and modular architectures makes these platforms accessible to the broader scientific community, while simultaneously imposing additional requirements for ensuring data security, process integrity, confidentiality, availability, and protection against cyber threats.

Review of recent publications

In recent years, there has been a marked increase in attention to open information platforms that support the entire cycle of scientific publications. Studies emphasize the need to integrate access management, metadata control, and information protection mechanisms, as these platforms interact with a large number of users and store substantial volumes of data, including manuscripts, reviews, and analytical results [1]. Recent works have examined various approaches to securing user interactions, focusing on role models and access policies that combine classical RBAC (role-based access control) and ABAC (attribute-based access control), enabling differentiation of user privileges based on context, publication stage, and object characteristics [2]. Research indicates that this combination reduces the risk of unauthorized access to manuscripts and reviews while maintaining flexibility for editorial and reviewer procedures [3]. Certain studies highlight privacy and confidentiality protection through pseudonymization, metadata access control, and visibility

restrictions according to user roles. Issues of review anonymity and prevention of deanonymization are considered essential for upholding ethical standards and ensuring equal conditions for authors and reviewers [4]. Furthermore, investigations underline the necessity of auditing user actions and tracking metadata changes to prevent manipulation and ensure the integrity of the publication process [5].

A separate body of research focuses on the protection of data and metadata at the infrastructure level. These studies examine encryption technologies, key management systems, version control methods, and mechanisms for ensuring document immutability. Findings indicate that the implementation of multi-level encryption and authentication protocols enhances data security during storage and transmission, reducing the likelihood of unauthorized access or information loss [3]. Scientific works also address the integration of platforms with external services such as ORCID and DOI registries and plagiarism detection systems. Research demonstrates that interaction with these services requires standardized data exchange protocols and authentication mechanisms to maintain data integrity and reliability [1]. Additionally, existing studies describe approaches for monitoring and detecting anomalies in user behavior and publication processes. The use of analytics, UEBA (user and entity behavior analytics) algorithms, and integrated logging enables the identification of suspicious activities indicative of access policy violations or attempts to modify manuscripts and reviews [6].

The review of recent studies has shown that existing publication support platforms implement basic mechanisms for access control and data preservation; however, gaps remain in providing comprehensive protection of the review process, metadata management, and integration with external services. In particular, methods for monitoring user actions are insufficiently developed, complicating the detection of unauthorized modifications to manuscripts and reviews. Support for context-based differentiated access is also limited, increasing the risk of data manipulation at various stages of the publication workflow. Identified gaps in review anonymity standards and metadata integrity control emphasize the need to integrate new security mechanisms that ensure both data protection and process transparency. This includes the extension of access policies, enhancement of authentication protocols, and implementation of analytical tools for monitoring anomalous user behavior.

Rationale for the Relevance of Enhancing Security Mechanisms of a Publication Platform

Publication platforms operate within cloud and hybrid infrastructures, necessitating the implementation of comprehensive security mechanisms at multiple levels. Threats include unauthorized access to manuscripts and reviews, identifier substitution, compromise of integration services, vulnerabilities in containerized environments, and misuse during the review process. Particular attention should be given to the security of the data flow administration chain, which determines the reliability of the entire platform. The enhancement of security mechanisms in open publication platforms is increasingly relevant in the context of growing volumes of digital scientific data, the complexity of user interactions, and integration processes with external services. The timeliness of this research is motivated by the need to develop approaches that combine access control, metadata protection, and process monitoring without imposing excessive constraints on the efficiency of the publication workflow. Under these conditions, the formation of a cybersecurity architecture capable of addressing the specificities of scientific

communication, ensuring compliance with privacy requirements, and maintaining process stability over the long term becomes critical. The present study aims to align access models, threat analysis methodologies, and countermeasure mechanisms within a unified system that adheres to the principles of open science and the requirements of contemporary communication infrastructures.

Identification of Threats and Attack Vectors in a Publication Platform

The analysis of threat models and attack vectors constitutes a necessary prerequisite for enhancing the security mechanisms of communication systems and cloud infrastructure within an open information platform for publication support. This approach entails the identification of all key platform components, including user interfaces, manuscript submission and review processes, administrative functions, metadata management, and integration with external services. The threat model defines potential sources of risk, such as unauthorized access, content manipulation, abuse of user roles and privileges, compromise of metadata integrity, and anomalous behavior that deviates from established procedures. Within the publication platform, the threat model provides a framework for understanding how different system elements interact with both external and internal sources of potential risk. Threats emerge at the intersection of user roles, content processing workflows, and technical infrastructure components. The functions of authors, reviewers, editors, and administrators determine not only data access rights but also potential avenues for undesired actions affecting the integrity of manuscripts and metadata. Unauthorized content modifications may result from both external attacks and internal procedural violations, highlighting the need for differentiated control mechanisms. Interaction with external services, including identification systems and plagiarism detection databases, introduces additional vectors affecting data, where any inaccuracy or error in information exchange may compromise the publication support process.

Therefore, the proposed integrated security model for the communication subsystems of the publication platform is presented as a three-tier structure reflecting the interaction of users, publication support processes, and protective mechanisms (Figure). The first tier comprises user roles and external services, including authors, reviewers, editors, administrators, as well as integrated systems such as ORCID, DOI, plagiarism detection services, and archives. Each element is considered a potential source of threats, including unauthorized account access, content manipulation, role abuse, data leakage during integration with external services, and internal anomalies in user behavior. The second tier encompasses the primary publication support processes, including manuscript submission, peer review, editorial verification, publication, and integration with external systems. Interaction arrows from actors to processes illustrate potential impacts on specific operations and points where threats may manifest. The third tier represents protective mechanisms applied to processes as barriers or frameworks. These include RBAC and ABAC for differentiated access control and management of roles and attributes, UEBA for detecting hidden and internal anomalies, and authentication protocols alongside data integrity measures to prevent metadata or content tampering.

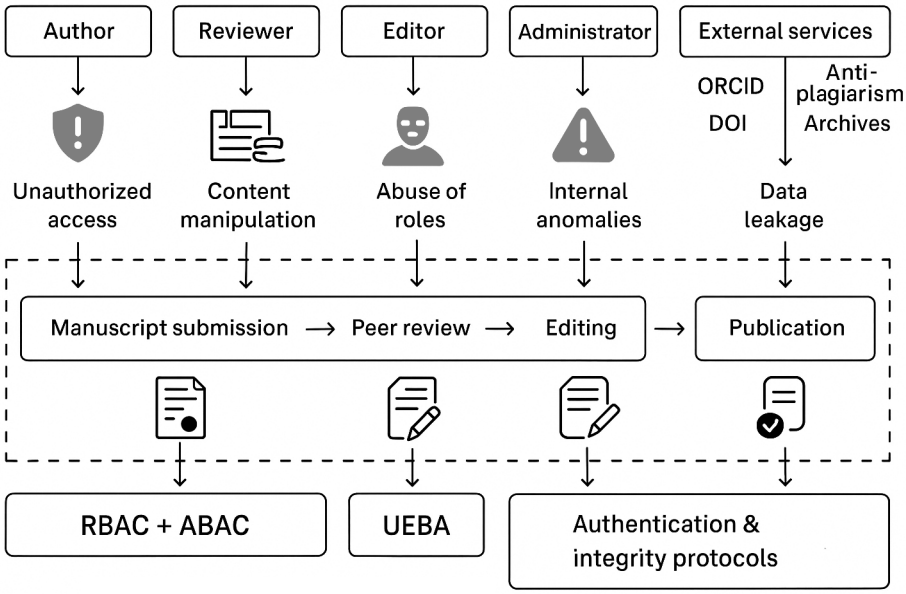

Figure : Integrated security model of communication subsystems in a publication platform. Developed by the author.

Anomalous user behavior, including unusual system requests, attempts to circumvent established access policies, or modifications to metadata, represents internal attack vectors that cannot be detected without analyzing action sequences and comparing them to expected usage patterns. Each manuscript processing stage, from submission to publication, includes points where interference or unauthorized changes may affect the accuracy and reliability of information. Identifying these points allows for the delineation of threat categories and the development of tools that regulate user access and actions while maintaining the efficiency of the publication workflow.

Thus, attack vectors are formed as a combination of user capabilities, technological vulnerabilities, and external integrations, creating a multi-level network of interdependencies. Intrusions through accounts, content substitution or modification, interference with the review process, and breaches of metadata integrity occur not in isolation but within an interconnected context, where a single action can trigger cascading effects across multiple platform components. Detecting and identifying these interrelationships provides a foundation for developing comprehensive control procedures that integrate user behavior monitoring, context-sensitive access rights, and authentication mechanisms adaptable to system actions.

The integration of analytical tools for detecting anomalous behavior while ensuring data integrity enables the deployment of protective mechanisms without disrupting the publication workflow. This approach establishes a foundation for the resilient operation of the platform, where each system component and every integration with external services is assessed in terms of potential threats and corresponding measures to mitigate their impact. The development and application of the presented threat and attack vector model create conditions for implementing security measures that ensure the integrity, availability, and reliability of information within the publication platform, while maintaining the efficiency and flexibility of processes at all stages of scientific material handling.

Conclusions

Thus, the presented security model for the communication subsystems of the publication platform integrates differentiated access management, monitoring of anomalous behavior, and protection of information integrity across all stages of the publication process. It combines user roles and external services as potential sources of threats with publication support processes, enabling the detection and localization of risks related to unauthorized access, content manipulation, role abuse, data leakage, and internal anomalies. Novel features of the model include the use of RBAC and ABAC to implement differentiated access control based on roles and attributes, UEBA for detecting hidden and internal anomalies in user behavior, and authentication protocols along with data integrity measures to prevent tampering of metadata and content.

The research results indicate the relevance of enhancing security mechanisms in publication platforms through the combined use of RBAC and ABAC access models for differentiated user rights control based on context and publication cycle stage, multi-level encryption and key management systems for data protection during storage and transmission, analytical tools and algorithms. The implementation of the proposed approaches will contribute to enhancing the reliability, resilience, and trustworthiness of digital publication support platforms for scientific research, while ensuring compliance with current privacy requirements and integration with international scientific infrastructure services. The model's structure enables a proper realization of the interconnection between users, processes, and security mechanisms, demonstrating the target measures applied for access control, monitoring of anomalous behavior, and protection of information integrity throughout the publication support process. It establishes a methodological foundation for the further development of comprehensive cybersecurity strategies for open publication platforms, allowing the integration of data security, process transparency, and publication workflow efficiency, which is essential in the context of contemporary scientific communication and the advancement of open science.

Declaration on Generative AI

During the preparation of this work, the author used X-GPT-4 for grammar and spelling check of domain-specific terminology in English. After using this tool, the author reviewed and edited the content as needed and takes full responsibility for the publication's content.

References

[1] Paseri, L. (2023). Open science and data protection: Engaging scientific and legal contexts. Journal of Open Access to Law, 11(1), 1-18. https://doi.org/10.63567/1bnsyb91

[2] Mahmood Rajpoot, Q., Jensen, C. D., & Krishnan, R. (2015). Attributes enhanced role-based access control model. In S. Fischer-Huebner & C. Lambrinoudakis (Eds.), Proceedings of the 12th International Conference on Trust, Privacy and Security in Digital Business (TrustBus'15) (pp. 3-17). Springer. https://doi.org/10.1007/978-3-319-22906-5_1

[3] Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). Guide to attribute based access control (ABAC) definition and considerations (NIST Special Publication 800-162). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-162

[4] Payer, M., Huang, L., Gong, N. Z., Borgolte, K., & Frank, M. (2015). What you submit is who you are: A multimodal approach for deanonymizing scientific publications. IEEE Transactions on Information Forensics and Security, 10(1), 200–212. https://doi.org/10.1109/TIFS.2014.2368355

[5] Berti Suman, A., & Pierce, R. (2018). Challenges for citizen science and the EU open science agenda under the GDPR. European Data Protection Law Review, 4(3), 284-295. https://doi.org/10.21552/edpl/2018/3/7

[6] Landauer, M., Skopik, F., Höld, G., & Wurzenberger, M. (2022). A user and entity behavior analytics log data set for anomaly detection in cloud computing. In 2022 IEEE International Conference on Big Data (Big Data), Dec. 17 2022 to Dec. 20 2022, Osaka, Japan (pp. 4285-4294). https://doi.org/10.1109/BigData55660.2022.10020672