

Security Issues and Countermeasures Across the Full Lifecycle of Scientific Papers

Authors: Wang Yun, Wu Bingchao, Guan Bei, Yongji Wang

Date: 2022-11-13T00:00:00+00:00

Abstract

Purpose: To review and summarize the entire lifecycle of scientific paper publication, explore security issues and solutions throughout the lifecycle, and provide reference and guidance for strengthening the protection of confidential information in scientific papers; **Methods:** From the perspective of the entire lifecycle of scientific papers, analyze potential security issues in five stages: author topic selection and planning, author institution review, editorial office manuscript processing, scientific paper archiving, and scientific paper circulation, and provide constructive suggestions and countermeasures for these issues; **Results:** To achieve the goal of ensuring security throughout the entire lifecycle of scientific papers, authors need to enhance information security awareness, institutions should define security and confidentiality classification levels, editorial offices should cultivate reviewers who possess both professional expertise and confidentiality awareness, and improve scientific paper storage technologies and digital watermarking technologies; **Conclusion:** With the networking of scientific papers comes an increase in information leakage issues; analyzing security issues throughout the entire lifecycle of scientific papers and exploring corresponding countermeasures can effectively prevent the leakage of sensitive information and intelligence in scientific fields.

Full Text

Security Issues and Countermeasures Throughout the Entire Life Cycle of Scientific Papers

Wang Yun¹, **Wu Bingchao**², **Guan Bei**², **Wang Yongji**^{2 1} Dalian Tax Cadre Institute, State Taxation Administration ² Institute of Software, Chinese Academy of Sciences

Abstract

[Objective] To summarize the entire publication life cycle of scientific papers, examine the security issues and solutions throughout this cycle, and provide reference for strengthening the protection of classified information in scientific papers. **[Methods]** From the perspective of the whole life cycle of scientific papers, this study analyzes potential security issues across five stages—author topic selection and planning, institutional review, editorial manuscript processing, paper archiving, and paper dissemination—and proposes constructive recommendations and countermeasures. **[Results]** To ensure security throughout the entire life cycle of scientific papers, authors must enhance information security awareness, institutions should establish classification levels for confidentiality, editorial departments need to cultivate reviewers with both professional expertise and security consciousness, and storage technologies and digital watermarking techniques must be improved. **[Conclusion]** As scientific papers become increasingly networked, information leakage incidents are on the rise. Analyzing security issues throughout the entire life cycle and exploring corresponding countermeasures can effectively prevent the disclosure of sensitive information and intelligence in scientific and technological fields.

Keywords: scientific papers; whole life cycle of scientific papers; security countermeasures for scientific papers

The internet era is driving the development of scientific and technological revolutions, with knowledge, information, intellectual value, and talent allocation becoming the innovative sources of this information revolution. In this context, academic resources such as ACM and IEEE journals and conferences continue to emerge, leading to a surge in the number of published scientific papers. Since the 1990s, the rapid development of the internet has transformed lifestyles, enabling researchers to fully leverage their strengths and publish their latest findings online. This networkization of scientific papers has brought unprecedented changes to information dissemination pathways, efficiency, and scope, but it has also increased the probability and risk of information leakage. For instance, Alibaba's "Taobao" once suffered a data breach where a software developer used a custom web crawler to extract over 1.1 billion user records. Of particular concern, current internet-based academic journal retrieval systems contain the vast majority of scientific papers from natural and social sciences. While these platforms provide essential database support for scientific verification and novelty searches, they also pose confidentiality risks. As Tang Di et al. [1] point out, overseas intelligence agencies exploit journal databases for intelligence collection, obtaining sensitive information from publicly published scientific papers. Therefore, strengthening confidentiality safeguards during the publication process is urgent. Qin Xiaoxue et al. [2] note that the confidentiality challenges posed by scientific journals on the internet have long made them primary targets for foreign intelligence infiltration and information theft. Since the US-China trade friction, technological competition has intensified, with various "chokepoint" technologies such as photolithography machines and industrial software facing

restrictions.

1. The Whole Life Cycle of Scientific Papers

The whole life cycle concept is a management philosophy and theory that has emerged from practical exploration, with different interpretations across various domains. The publication of scientific papers constitutes a complete chain that forms the entire life cycle of scientific paper publication.

1.1 Concept of Whole Life Cycle

The whole life cycle is a transactional concept and theory that arises from practical exploration. In different fields, it has different interpretations. As Li Manyi et al. [3] research indicates, whole life cycle management thinking applies to scientific review mechanisms and confidentiality review mechanisms. For example, the software life cycle (SLC) encompasses requirements analysis, design, coding, debugging, testing, acceptance, operation, and eventual decommissioning. Similarly, the whole life cycle of intelligent manufacturing enterprises extends from product design data to end-of-use, establishing a product life cycle management platform that enables innovative customized production models across different stages such as product and process design and integrated enterprise financial management, thereby accelerating healthy enterprise development.

Corresponding Author: Wang Yongji²

[Figure 1: see original paper] The Whole Life Cycle of Scientific Papers

1.2 The Whole Life Cycle of Scientific Papers

The publication of scientific papers forms a complete chain that constitutes the entire life cycle of scientific paper publication. This life cycle comprises five stages: author topic selection and planning, institutional review, editorial manuscript processing, paper archiving, and paper dissemination, as illustrated in Figure 1.

In the first stage, authors should first understand laws and regulations regarding the scope of state secrets and classification levels in relevant fields when planning topics, ultimately determining the direction of their research. In the second stage, since scientific papers involve cutting-edge fields of scientific and technological production, the author's institution must review whether the achievements exceed academic research boundaries, properly classify the confidentiality level of scientific achievements and key technologies, and conduct thorough confidentiality reviews to ensure information security. Editorial departments play a crucial role in paper security review. Editorial staff and reviewers must strengthen their confidentiality awareness and prevent leakage of confidential information through strict editorial systems. The editorial review process specifically includes four stages: drafting appointments, receipt, initial review, and external review, as proposed by Gao Yi et al. [4]. In the fourth stage,

with internet development, information storage carriers for scientific papers have rapidly shifted from traditional paper documents to electronic documents, network databases, and electronic journals. These data storage media enable rapid information transmission but suffer from weak classified carrier management, insufficient technical protection capabilities, and high risk of loss of control. In the fifth stage, the final scientific achievements will be incorporated into internet-based academic journal retrieval systems for extensive promotion and exchange. These platforms provide retrieval, reading, and downloading services for academic literature and dissertations, and must prevent internal personnel from downloading papers and privately disseminating them to hostile forces, which would cause leakage of core confidential information.

2. Security Issues Throughout the Life Cycle of Scientific Papers

Security issues permeate all five stages of the scientific paper life cycle. According to the characteristics of these security issues, risks must be identified in advance during life cycle management, and potential information security risks must be analyzed.

2.1 Author Topic Selection and Planning Stage

Potential information security issues at this stage include authors' limited knowledge of confidentiality requirements for their research topics and the leakage of classified information during writing. First, authors often have insufficient understanding of the confidentiality requirements for their research topics. Before writing, their confidentiality awareness is weak, and they fail to conduct confidentiality assessments according to institutional regulations, instead relying on personal judgment. Second, due to pressure from career advancement, degree defenses, performance evaluations, and assessments, authors may overly describe key technical parameters, technical solutions, and implementation paths involving classified scientific achievements to increase acceptance rates.

2.2 Institutional Review Stage

Potential information security issues during institutional review include inadequate classification work and insufficient enforcement of confidentiality review systems. First, a reasonable classification system is critical to effective paper review. The foundation of proper classification work involves specifying detailed classification catalogs and their granularity to safeguard national security and interests. Second, although institutions have established confidentiality review bodies, they often lack reviewers with both confidentiality knowledge and scientific research expertise, causing confidentiality review systems to become mere formalities that fail to effectively fulfill their responsibilities.

2.3 Editorial Manuscript Processing Stage

Editorial processing includes four sub-stages: drafting appointments, receipt, initial review, and external review, each with potential information security issues. During the solicitation stage, some editorial departments include disclaimers in their calls for papers, reminding authors to ensure submissions do not involve confidentiality issues, yet fail to establish confidentiality clauses or require confidentiality review certificates as stipulated. During receipt, manuscripts transmitted over networks may be attacked by spyware, trojans, and network sniffing, leading to confidential information leakage. During initial review, editorial staff often have unreasonable quantity and knowledge structures, making them unable to detect leaks due to insufficient expertise. During external review, there is risk of confusing confidential content with professional technical information, potentially sending classified information to external reviewers and causing leaks.

2.4 Scientific Paper Archiving Stage

Potential information security issues during network database archiving include virus attacks and security vulnerabilities. First, with the development of cloud computing and big data technologies, network databases continuously suffer virus attacks during operation. Malicious actors implant trojans to disrupt computer network code, interfere with normal database operations, and steal scientific paper data, resulting in leaks. Second, no computer network database is completely secure in internet environments. Hackers discover program vulnerabilities during database applications, illegally invade storage addresses, steal and modify scientific paper data, causing loss of research achievement information or experimental data and leading to leakage of classified information.

2.5 Scientific Paper Circulation Stage

Potential security issues during dissemination include authors' rights infringement and leakage traceability problems. First, as final scientific achievements are incorporated into internet-based academic journal retrieval systems for extensive promotion and exchange, the document format of scientific papers makes it easy to extract core data using conversion software, infringing upon authors' rights during circulation. Second, while journal retrieval platforms provide retrieval and downloading services for academic literature and dissertations, scientific papers should have restricted public access, exchange, and usage scopes within certain timeframes. Internal personnel must be prevented from downloading papers and privately disseminating them to hostile forces, which would cause leakage of domestic core confidential information.

3. Countermeasures for Information Security Issues Throughout the Life Cycle

Establishing a monitoring mechanism for the entire life cycle of scientific papers enables process management and effective defense against and proactive response to information security issues across the five stages.

3.1 Author Topic Selection and Planning Stage

First, authors should strengthen self-review and enhance confidentiality awareness by regularly participating in confidentiality education activities organized by their institutions, adhering to the principle of not publishing classified content or only publishing it after declassification, thereby eliminating leakage incidents at the source. Second, during topic selection, authors should avoid sensitive themes such as national defense technology development and weapons research, minimize the use of classified project documents and charts, and strictly prohibit direct publication of classified achievements.

3.2 Institutional Review Stage

First, institutions should improve classification work and implement a dedicated responsibility system for scientific paper confidentiality review. Based on detailed purpose descriptions, institutions must establish specialized confidentiality organizations and standardize review processes. Confidentiality review specialists must master confidentiality laws and regulations while also possessing expertise in scientific paper technologies. Second, institutions should strengthen confidentiality knowledge education. Since confidentiality review directly relates to national security and interests, institutions must enhance publicity efforts to build the first “firewall” of confidentiality prevention, strengthening confidentiality knowledge learning based on authors’ positions, enhancing awareness of scientific achievement protection, and disseminating confidentiality concepts for scientific information.

3.3 Editorial Manuscript Processing Stage

First, during solicitation, papers involving state secrets or national defense information require confidentiality review. Editorial departments must explicitly specify confidentiality review requirements and content guidelines, actively implementing confidentiality systems. Second, during receipt, network database security can be enhanced through cryptographic keys. As Lu Jianlan et al. [5] indicate, keys establish contractual relationships between databases and users. Scientific paper databases can use physical, digital signature, or biometric password forms to provide network passwords, enabling point-to-point secure information transmission and rapidly completing registration verification, thereby significantly improving security. Third, during initial review, a two-stage manual review process plus AI-enabled review can be adopted. The two-stage manual review employs an “initial review + expert review” model to screen

confidential content, followed by expert determination. AI-assisted review utilizes artificial intelligence to automatically identify or redact sensitive information. Fourth, during external review, confidentiality review and academic review should be separated, with authors removing classified content before submission to external reviewers, and an “external reviewer certification system” should be implemented to prevent reviewers from leaking confidential information.

3.4 Scientific Paper Archiving Stage

First, install firewalls and security software. While antivirus software only prevents virus intrusion, firewalls are essential for defending against hacker attacks. As a blocking point, firewalls significantly enhance database security by filtering insecure services, reducing risks of theft, destruction, and tampering, and improving protection capabilities. Second, adopt database encryption methods. Data encryption uses key-based technologies to protect information, where scientific papers are encrypted with keys and can only be decrypted with the same keys. This ensures that hackers and intruders only see garbled data. Additionally, secure keys and access authentication mechanisms establish contractual relationships between databases and users, enabling point-to-point transmission.

3.5 Scientific Paper Circulation Stage

First, scientifically define data property rights for scientific papers. According to the Civil Code of the People’s Republic of China, intellectual property rights are rights legally enjoyed by right holders over works and trademarks. While data information generally cannot serve as intellectual property objects, data rights in scientific papers represent a new field of intellectual property protection. Zhang Junhong et al. [6] note that “Liu Shijin, a member of the National Committee of the Chinese People’s Political Consultative Conference, proposed at this year’s National People’s Congress that to maintain the bottom line of data property rights protection and data security, initial and value-added data property rights should be scientifically defined, and the legitimate rights of various property rights in different circulation links should be equally protected.” Second, adopt blockchain-based circulation methods for scientific papers. Shi Guanbin et al. [7] indicate that blockchain technology ensures documents cannot be tampered with or forged at any stage by constructing a “judicial alliance chain,” making them original evidence. By building an underlying trusted alliance chain network, scientific papers form blockchain transaction information during resource retrieval, online reading, and downloading services, thereby thoroughly solving authors’ rights and leakage traceability issues [8,9].

In summary, as internet popularization increases the probability and risk of information leakage in networked scientific papers, improving monitoring systems throughout the entire life cycle is essential. Editorial departments should organize experts to inspect and supervise information security throughout the life cycle, standardizing operations in each link and recording original research data. Staff at all stages must strictly review confidential information and follow estab-

lished regulations, with editorial departments arranging supervisors for regular inspections. Additionally, monitoring tools for the entire life cycle should be developed. Addressing limited staff energy and expertise, AI-enabled monitoring tools can be created to automatically detect non-compliant operations and provide recommendations according to regulations.

References

- [1] Tang Di, Xia Xuelian. Confidentiality Issues and Countermeasures in the Process of Scientific Paper Publication[J]. Secrecy Science and Technology, 2015(01): 62-64.
- [2] Qin Xiaoxue. Analysis of Leakage Risks and Confidentiality Management Countermeasures for Scientific Journals[J]. Publishing and Printing, 2021(02): 67-71.
- [3] Li Manyi. Reflections on the Confidentiality Review Mechanism for Manuscripts Throughout Their Life Cycle in Scientific Journals[J]. Acta Editologica, 2014(S1): 12-13.
- [4] Gao Yi, Wang Yanxiu, Zhang Guihong, Jiang Mei. Discussion on How to Do a Good Job in Confidentiality Work for Scientific Journals[J]. Public Communication of Science & Technology, 2020, 12(24): 26-28.
- [5] Lu Jianlan. Research on Security Issues of Computer Network Databases[J]. Electronic Test, 2021(14): 133-134.
- [6] Zhang Junhong. Liu Shijin, Member of the National Committee of the Chinese People's Political Consultative Conference: Balancing Data Security and Circulation[J]. Economy, 2022(04): 36.
- [7] Shi Guanbin, Chen Quanzhen. On the Advantages of Blockchain-Based Electronic Data Preservation and Judicial Review Paths[J]. Journal of Southwest Minzu University (Humanities and Social Sciences Edition), 2021(01): 67-73.
- [8] Zhao Jingwu. From Confidentiality to Security: Theoretical Logic and System Construction of Data Destruction Obligations[J]. SJTU Law Review, 2022(02): 28-41.
- [9] Dai Ni. Scientific Journals Should Strengthen Confidentiality Work[J]. Acta Editologica, 2022, 34(03): 244-248.

Note: Figure translations are in progress. See original paper for figures.

Source: ChinaXiv –Machine translation. Verify with original.