# Call for Papers: Special Issue on Applications of Natural Language Processing (NLP) in Software Security and Vulnerability Management

The International Journal of AI and Knowledge Engineering (IJAIKE) is pleased to announce a Special Issue on **"Applications of Natural Language Processing in Software Security and Vulnerability Management."** This special issue aims to bring together leading academic scientists, researchers, and practitioners to exchange and share their experiences and research results on all aspects of Natural Language Processing (NLP) applications in software security and vulnerability management.

**This call for papers is seeking** innovative contributions that explore the intersection of NLP and software security. We encourage submissions that offer new insights, research findings, and practical applications that enhance software security and vulnerability management using NLP techniques. Topics of interest include, but are not limited to:

**1. NLP for Automated Vulnerability Detection in Software**

- Utilizing NLP techniques to automatically detect and identify vulnerabilities in software code and systems.
- Development of models that analyze codebases to flag potential security issues.

**2. Text Analysis of Bug Reports and Security Advisories**

- Applying NLP to analyze bug reports, security advisories, and vulnerability databases.
- Techniques for extracting relevant information and trends from textual data.

**3. NLP-Based Threat Intelligence and Malware Analysis**

- Using NLP for analyzing threat intelligence reports, malware descriptions, and attack patterns.
- Development of systems that automatically categorize and assess threats based on textual information.

**4. LLM-Based Tools for Identifying Software Vulnerabilities**

- Leveraging large language models (LLMs) to identify and predict software vulnerabilities.
- Practical applications of LLMs in vulnerability assessment and mitigation.

**5. Patch Localization and Interpretability for Software Vulnerability Analysis**

- Research on NLP methods for identifying the precise location of vulnerabilities in code.
- Techniques for enhancing the interpretability of vulnerability analysis results.

**6. Large Dataset Development and Benchmarking for Software Vulnerabilities**

- Creation and benchmarking of large datasets for training and evaluating NLP models in software security.
- Methods for ensuring the quality and relevance of datasets used in vulnerability research.

**7. AI-Driven Code Review and Security Audits**

- Applying NLP and AI to automate code review processes and security audits.

- Techniques for integrating AI-driven insights into existing security workflows.

**8. Sentiment Analysis in Security Communities**

- Utilizing sentiment analysis to understand the dynamics of security communities and developer forums.
- Insights into how sentiment and discourse influence software security practices.

**9. NLP for Compliance and Legal Texts in Software Security**

- Analyzing compliance documents, legal texts, and regulatory frameworks using NLP.
- Ensuring software security practices align with legal and regulatory requirements.

**10. Case Studies and Real-World Applications**

- Documenting successful applications of NLP in software security and vulnerability management.
- Lessons learned and best practices from practical implementations.

The IJAIKE journal is an open-access publication managed by the Association for the Advancement of Knowledge Solutions (AAKS) in cooperation with the EurAsia Academic Publishing Group (EAPG).

## Submission Guidelines:

- Manuscripts should be submitted via the **Clarivate ScholarOne Manuscript Central Submission** portal at https://mc04.manuscriptcentral.com/jaike
- All submissions must be original and not under consideration for publication elsewhere,
- Papers will undergo a rigorous peer-review process to ensure high-quality contributions.

## Important Dates:

- **Submission Deadline**: 15th September, 2025
- **Notification of Acceptance**: 30th December, 2025
- **Publication Date**: June 2026

For any inquiries regarding this special issue, please contact the guest editors at:


**Mst Shapna Akter , Ph.D.**
Assistant Professor | Computer Science and Engineering,
Oakland University, Auburn Hills, Michigan, United States
https://www.linkedin.com/in/mst-shapna-akter-42bb15324/
Email:akter@oakland.edu

**Yao Qiang , Ph.D.**
Assistant Professor | Computer Science and Engineering,
Oakland University, Auburn Hills, Michigan, United States
https://qiangyao1988.github.io/
Email: qiang@oakland.edu


We look forward to receiving your valuable contributions and advancing the field of NLP in Software Security and Vulnerability Management together.