#

#

##

**International Conference on Computational Intelligence and Information Retrieval**

***Organized by***

***Sister Nivedita University (SNU), India***

*Technically Sponsored by:*

**Scientific Innovation Research Group (SIRG), Egypt**

**Scientific Research Group in Egypt (SRGE), Egypt**

**CI2S lab, Argentina**

**Date: 24th – 25th April 2025 (Hybrid Mode)**

##  \*\*\*\*\*\*\*\*\*\*\*\*\*\* CALL FOR PAPERS \*\*\*\*\*\*\*\*\*\*\*\*\*\*

 **SPECIAL SESSION**

**Natural Language Processing for Cybersecurity (NLPC)**

### SESSION ORGANIZERS:

###

|  |  |  |
| --- | --- | --- |
| A person smiling for a picture  Description automatically generated |  | A person wearing a black head scarf  Description automatically generated |
| Dr. Punam KumariAssociate Professor, ASET, Amity University Bengaluru, India.pkumari@blr.amity.edu | Dr. Rajat BhardwajAssociate Professor, ASET, Amity University Bengaluru, India.rajatbhardwaj.x@gmail.com | Dr. Abeer A. Aljohani Department of Computer Science, Applied College, Taibah University, Medina 42353, Saudi Arabia; aahjohani@taibahu.edu.sa |

**SESSION DESCRIPTION:**

This session will explore the intersection of Natural Language Processing (NLP) and cybersecurity, focusing on innovative techniques and applications to tackle modern cyber threats. Participants will delve into how NLP can enhance the detection and prevention of phishing attacks, malware analysis, and social engineering by analyzing and understanding textual data.

**RECOMMENDED TOPICS:**

Topics to be discussed in this special session include (but are not limited to) the following:

1. Phishing and Social Engineering Detection
	* NLP techniques to identify phishing emails and messages.
	* Automated detection of social engineering attacks through text analysis.
2. Threat Intelligence Extraction
	* Mining threat intelligence from unstructured text sources (e.g., blogs, reports, forums).
	* NLP for automated parsing and summarization of cybersecurity threat data.
3. Malware Communication Analysis
* NLP-based approaches for detecting malicious command-and-control communications.
* Decoding obfuscated text used in malware payloads.
1. Sentiment and Behavioral Analysis
* cybercriminals using sentiment analysis and linguistic patterns.
* Identifying intent and tone in cyber threat communications.
1. Real-Time Language Processing
* Real-time NLP applications for detecting and responding to emerging threats.
* Challenges in multilingual and low-resource language detection for cyber threats.
1. Automated Security Policy Generation
* Using NLP to generate and manage security policies from textual data.
* Semantic analysis for refining rule-based cybersecurity systems.
1. NLP for Dark Web Monitoring
* Text mining techniques for tracking and analyzing dark web activities.
* Language-specific challenges in monitoring hidden services.
1. Adversarial NLP in Cybersecurity
* Understanding and mitigating adversarial attacks on NLP-based systems.
* Building robust NLP models against evasion techniques.
1. Chatbot and Social Media Threats
* Identifying malicious chatbot activities and impersonation through text analysis.
* NLP for detecting misinformation and threats on social media platforms.
1. Cross-Linguistic Threat Detection
* NLP methods for detecting cyber threats across multiple languages.
* Leveraging machine translation and multilingual models for cybersecurity.
1. Forensic Linguistics in Cybersecurity
* NLP for forensic analysis of cyber threats and attack attribution.
* Linguistic fingerprinting to trace threat actors.
1. Legal and Ethical Considerations
* Ethical implications of using NLP in cybersecurity monitoring.
* Privacy-preserving methods for text-based threat analysis

**PUBLICATION AND SUBMISSION PROCEDURE**

The conference aims at carrying out double-blind review process. The papers submitted by the authors will be assessed based on their technical suitability, the scope of work, plagiarism, novelty, clarity, completeness, relevance, significance, and research contribution. The conference proceedings will be published in AIP Web of Science, Scopus series.

**NOTE: While submitting the paper in this special session, please specify International Conference on Cyber Analytics and Information Retrieval at the top (above paper title) of the first page of your paper.**

# \* \* \* \* \* \*