UTTAR PRADESH STATE INSTITUTE OF FORENSIC SCIENCE, LUCKNOW

ALL INDIA COUNCIL FOR TECHNICAL EDUCATION

CYBERVIDYAPEETH FOUNDATION, FARIDABAD

CALL FOR PAPERS

Dimension of Cyber warfare, Multilateral Legal Frameworks, Forensics & Strategic Countermeasures

Venue: UPSIFS, Lucknow
Dates: March 17-18, 2025

साइबर वेद मंथन
CYBER VEDA MANTHAN

powered by

PIVOT
Detect. Defend. Disrupt.

Youth 4 Nation

Overview

The UPSIFS, in collaboration with Cybervidyapeeth Foundation, proudly announces a national-level conference focused on Cyber Warfare & Countermeasures. This prestigious event aims to bring together researchers, academicians, and professionals from across India to share their innovative research findings and practical experiences in critical areas of national security. The conference represents a unique opportunity for participants to contribute to India's cybersecurity landscape while gaining recognition from the highest levels of government, including the Ministry of Defense. Selected papers will be published in a conference proceedings book, creating a lasting impact on the field and providing valuable references for future research endeavors.

Conference Themes

1. OSINT - Open Source Intelligence

The landscape of open-source intelligence has transformed dramatically with the proliferation of digital information sources. This track invites papers exploring innovative methodologies for collecting, analyzing, and utilizing publicly available information for intelligence purposes. Submissions should address challenges in data verification, source credibility assessment, automation of OSINT processes, legal and ethical considerations in OSINT operations, integration of OSINT with traditional intelligence sources, and development of new tools and frameworks for OSINT analysis. Research papers demonstrating practical applications in national security, corporate intelligence, or law enforcement contexts are particularly encouraged. All submissions must include a working prototype or proof-of-concept implementation with supporting code documentation.

2. Cognitive Warfare and Countermeasures

In an era where information warfare has become increasingly sophisticated, understanding and countering cognitive warfare is crucial for national security. This track seeks papers examining the psychological and technological aspects of cognitive warfare, including influence operations, perception manipulation, and psychological resilience. Submissions should explore advanced countermeasures against cognitive attacks, methods for detecting and analyzing influence campaigns, strategies for building societal resilience against information warfare, and frameworks for protecting critical national infrastructure from cognitive threats. Papers investigating the role of artificial intelligence in both conducting and defending against cognitive warfare are especially welcome. Each submission must include a practical demonstration through a prototype system with accompanying source code.

3. Detecting Bots on Social Media

The proliferation of automated accounts on social media platforms presents significant challenges to information integrity and social discourse. This track invites research papers focusing on innovative approaches to bot detection, classification, and mitigation on social media platforms. Submissions should address advanced machine learning techniques for bot detection, behavioral analysis methods, network pattern recognition, real-time monitoring systems, and scalable solutions for large-scale bot detection. Papers should also consider the evolution of bot behavior, challenges in distinguishing sophisticated bots from human users, and strategies for maintaining detection effectiveness against emerging bot technologies. All submissions must include a functional prototype with implementation code demonstrating the proposed detection methods.

4. Deepfake Detection

As deepfake technology becomes increasingly sophisticated, the need for reliable detection methods grows more crucial. This track welcomes papers exploring cutting-edge approaches to deepfake detection across various media types. Submissions should address advanced neural network architectures for deepfake detection, forensic analysis techniques, temporal inconsistency detection, biometric verification methods, and real-time detection systems. Papers should also consider the challenges of detecting novel deepfake generation methods, maintaining detection accuracy across different media qualities, and developing robust solutions that can adapt to evolving deepfake technologies. Each submission must include a working prototype implementation with source code demonstrating the detection capabilities.

5. Cryptocurrency Investigation

The growing adoption of cryptocurrencies has created new challenges for financial investigation and security. This track seeks papers examining advanced methods for investigating cryptocurrency transactions and related criminal activities. Submissions should address blockchain analysis techniques, transaction tracking methodologies, identification of suspicious patterns, wallet clustering approaches, and tools for investigating crypto-related crimes. Papers exploring the integration of traditional financial investigation methods with blockchain analysis, regulatory compliance frameworks, and international cooperation in cryptocurrency investigations are particularly encouraged. All submissions must include a functional prototype tool with supporting code documentation demonstrating the proposed investigation techniques.

Paper Requirements

Technical Specifications

- Word count must be between 3,000 and 5,000 words
- Each submission must include:
  - Detailed methodology and research findings
  - Prototype or proof-of-concept implementation
  - Source code with documentation
  - Testing results and performance analysis
  - Deployment instructions and requirements
- Code submissions should be well-documented and follow industry best practices
- Prototype demonstrations should be reproducible and include clear setup instructions

Awards and Recognition Prizes

For each of the five themes, three outstanding papers will be awarded substantial cash prizes:

- First Prize: INR 75,000
- Second Prize: INR 50,000
- Third Prize: INR 25,000

Special Recognition

All selected participants will receive certificates from the Minister of Defense, Government of India, during a special ceremony. This recognition represents a significant achievement in participants' academic and professional careers, acknowledging their contribution to national security research and development.

Submission Guidelines

Paper Format and Standards

Papers must adhere to the following requirements:

- Strict compliance with IEEE conference paper format
- Original research work not previously published or under review elsewhere
- Word count between 3,000 and 5,000 words
- Use of IEEE template with standard formatting (10-point font, double column)
- Proper citations and references following IEEE style
- Plagiarism check certification must be submitted along with the paper
- Prototype implementation with source code
- Technical documentation and deployment guidelines

Submission Process

Papers must be submitted through the official conference portal following these steps:

- Registration and payment of participation fee (INR 5,000 per submission)
- Submission of full paper in PDF format
- Submission of prototype code and documentation
- Submission of plagiarism report
- Author declaration form
- Copyright transfer form
- All submissions must be completed by the specified deadline

Important Dates

- Call for Papers Launch: January 26, 2025
- Full Paper Submission Deadline: March 5, 2025
- Notification of Acceptance: March 7, 2025
- Camera-Ready Submission: March 10, 2025
- Conference Dates: 17-18 March, 2025

Eligibility and Participation

The conference is open to all Indian nationals, including:

- Academic researchers and faculty members
- Industry professionals
- Government organization employees
- Research scholars and postgraduate students
- Independent researchers and consultants
- Students

Contact Information

For any queries regarding paper submission or conference details, please contact:

- Email: cyberveda@upsifs.ac.in
- Contact Whatsapp: +91 89397 32808 | Mobile: +91 97111 47900
- Website: https://cybervedmanthan.in/

Publication

All accepted papers will be:

- Published in the conference proceedings book with ISBN
- Published as a conference book
- Made available through the conference digital library

Note

- All submitted papers will undergo a rigorous peer-review process
- The decisions of the review committee will be final
- Participation certificates will be issued only to authors who present their papers at the conference
- Authors of selected papers may be invited to extend their work for publication in partner journals
- Prototype implementations must be functional and well-documented
- Code submissions will be evaluated for quality and reproducibility

cyberveda@upsifs.ac.in | business@pivotsec.in | mentor@cybervidyapeeth.in | info@abhedi.com
cybervedmanthan.in | pivotsec.in | cybervidyapeeth.in | abhedi.com

contact@youth4nation.in | Whatsapp: +91 89397 32808
youth4nation.in | Mobile: +91 97111 47900