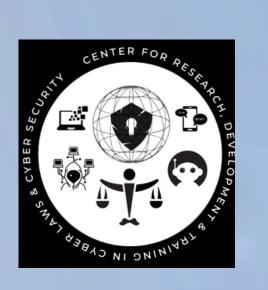# TAMIL NADU
NATIONAL LAW UNIVERSITY
TIRUCHIRAPPALLI

CENTRE FOR RESEARCH, DEVELOPMENT AND TRAINING
IN
CYBER LAWS AND CYBER SECURITY
(CRDT-CLCS)

NATIONAL CONFERENCE
ON
CYBER CRIMES
AND
ARTIFICIAL INTELLIGENCE

21ST SEPTEMBER, 2024
SATURDAY

cyberlawcenter@tnnlu.ac.in

Tamil Nadu National Law University, Tiruchirappalli.

ABOUT THE TAMIL NADU NATIONAL LAW UNIVERSITY

The Tamil Nadu National Law University (TNNLU) was established by the Government of Tamil Nadu by an Act of the State Legislature (Act No. 9 of 2012) to provide quality legal education at the global level.

TNNLU's Mission is to achieve global recognition as an institution of eminence and excellence in all spheres of legal education, rooted in an interdisciplinary approach to the study of law, such that the graduates of TNNLU will be independent, critical thinkers, and socially responsible human beings.

TNNLU offers two undergraduate programs, viz, B.A. LL.B., (Hons.) and B.Com. LL.B., (Hons.); three One-year LLM programmes, viz, Corporate and Securities Laws, Intellectual Property Laws and Natural Resources Law; and Ph.D. Programme in Law.

TNNLU is included in the approved list of universities by the UGC and Centre for Legal Education recognized by the Bar Council of India. TNNLU is a member of the Shastri Indo- Canadian Institute and it is a permanent member of the Indian Academy of Social Sciences. TNNLU is also an empaneled institution with the Competition Commission of India.

ABOUT CRDT-CLCS

The Centre for Research, Development, and Training in Cyber Laws and Cyber Security (CRDT-CLCS), funded by the Tamil Nadu Government was set up in 2022 with the aim to create awareness, conduct research and provides training related to dealing with cybercrimes, cyber contraventions and cyber security amongst Internet users, in general, and in the State of Tamil Nadu in particular, with an objective to prevent cybercrimes, misuse of technology and better enforcement of cyber laws.

The Centre carries out the Cyber Jagrukta (Security) Awareness Diwas, a monthly awareness program to promote cyber security and better internet practices. As part of the Diwas, the Centre has circulated brochures on "Biggest Data Breaches in India", and "An Understanding on Digisex, Sextortion and Revenge Porn".

The Centre has conducted three National Level Webinars on "Cyber Crimes against women and children – Legal response" in November 2022; on "Online Gaming: the risks, privacy and cyber security- a social legal conundrum" in April 2023; and on 'Legal Dimensions of Cyber crimes in Cyber Space with special reference to vulnerable victims' in October 2023. The Centre has organized a National Level Essay Writing Competition on Artificial Intelligence and Cyber Law in India in January 2023.

The Centre frequently circulates videos on Cyberspace terms translated from English to Tamil named "Inaiyaveli Mozhi Arivom" (Letz learn Cyberspace terms). It also conducts cyber awareness events through cyber fests at the TNNLU in 2023 and 2024. The Centre has its own newsletter named 'Data Monitor'.

ABOUT THE CONFERENCE

Artificial intelligence (AI) refers to a machine's ability to combine computers, datasets and sets of instructions to perform tasks that usually require human intelligence, such as reasoning, learning, decision-making and problem-solving. AI is already shaping almost every domain worldwide, and the trend is expanding rapidly. This cutting-edge technology, which has undergone various improvements, has influenced every industry and reshaped its processes and operations by propelling innovations. AI has made network security, anti-malware and fraud-detection software more formidable by spotting anomalies quicker than the human brain.

However, like any other technological advancement, AI poses a massive risk and an array of complex challenges in cybersecurity. The major cyber threats leveraging AI include brute force, denial of service, AI-generated deepfakes and social engineering attacks. The risks of artificial intelligence to cybersecurity are expected to increase rapidly with AI tools becoming cheaper and more accessible. Intelligence agencies across the world are grappling with the rise of potential security problems tied to algorithms that can generate human-sounding interactions, Large Language Models (LLMs) such as OpenAI's ChatGPT, which businesses are incorporating into a wide range of services, including sales and customer care. As the popularity of AI chatbots continues to grow, it is essential to take necessary precautions to safeguard against fraudulent activities.

ABOUT THE CONFERENCE

In India, National Crime Record Bureau (NCRB) data for 2022 reveals a concerning surge in cybercrimes across the country, with a 24.4% increase compared to the previous year. The Data from cybersecurity firm CheckPoint Research shows during the first quarter of 2023, India's average weekly attacks increased by 18% when compared to the corresponding period in 2022, with every organisation facing a minimum of 2,108 weekly attacks. However, the number of bot attacks has risen by 48% in the second quarter as against the first one and nine out of 10 websites encountered a bot attack, according to the State of Application Security Q2 report by Indusface (an application security software-as-a-service company). The misuse of AI is a growing concern. AI is a double-edged sword, bringing both opportunities and risks. Cybercriminals are increasingly leveraging AI-powered tools to conduct sophisticated attacks. A recent series of crimes assisted by AI, ranging from voice scams and financial frauds to celebrity deepfakes, has set off fresh concerns over technologies that run on AI and how they can abet criminal activities, in new form and scale.

There appears to be an emerging realisation that AI-enabled crimes are no longer part of an imagined dystopia; they are now real and warrant an informed response. As AI continues to advance, it is crucial for policymakers to stay one step ahead, developing proactive strategies to mitigate the potential risks associated with AI-driven cybercrimes. This one-day national conference aims to understand and facilitate discussion in these areas by inviting paper presentations on the themes mentioned. Further, it aims to conduct a panel discussion by inviting eminent scholars in the field.

OBJECTIVES OF THE CONFERENCE

1. To facilitate a platform for discussion on areas mentioned in the themes.
2. To sensitise the stakeholders on evolving cybercrimes in the age of AI.
3. To assess and analyse the implications of AI in context of cyber crimes.
4. To examine the ethical and legal concerns of cybercrimes in the age of AI.

THEME FOR THE CONFERENCE

THEME-I

- CYBER CRIMES IN METAVERSE
  - VIRTUAL CRIMES IN METAVERSE AGAINST VULNERABLE GROUPS- GROOMING, RADICALISATION AND CYBER ATTACKS;
  - METAVERSE ASSETS AND METAVERSE ENVIRONMENT;
  - CYBER WARFARE AND CYBER TERRORISM;
  - HUMAN RIGHTS, CONSTITUTIONAL, AND POLITICAL CHALLENGES IN METAVERSE;
  - CYBER CRIMES IN METAVERSE AND CYBER SECURITY MEASURES;

THEME-II

- CYBER CRIMES IN EXTENDED REALITY (XR)
  - ONLINE SAFETY FOR CHILDREN AND WOMEN FROM XR CRIMES;
  - PROTECTION OF YOUTH FROM XR ONLINE GAMING PLATFORMS;
  - EXTENDED REALITY AND CYBER SECURITY;
  - SECURITY AND PRIVACY CONCERNS OF VIRTUAL REALITY (VR), MIXED REALITY (MR) AND AUGMENTED REALITY (AR);
  - PRIVACY CONCERNS AND CYBER SECURITY ASPECTS;

THEME-III

- CYBER CRIMES RELATED TO ARTIFICIAL INTELLIGENCE (AI) AND ROBOTICS
  - AI-POWERED ROBOTS AND CYBER CRIMES;
  - MACHINE LEARNING (ML) AND CYBER CRIMES;
  - DIGISEXUALS AND CYBER CRIMES;
  - BRAIN-COMPUTER INTERFACE (BCI) - ETHICAL AND LEGAL IMPLICATIONS;
  - LIABILITY AND PRIVACY CONCERNS;

THEMES

THEME-IV
- CYBER CRIMES AND CYBER SECURITY CHALLENGES
  - AI AND CYBER SECURITY TO PREVENT CYBER CRIMES;
  - CYBER CRIMES IN SECTORS INCLUDING HEALTHCARE, E-COMMERCE, BANKING AND FINANCIAL SERVICES, EDUCATION SECTOR ETC., AND THEIR CYBER SECURITY ASPECTS;
  - DATA PROTECTION AND CYBER SECURITY CHALLENGES;
  - CYBER CRIMES AGAINST VULNERABLE GROUPS;
  - CYBER SECURITY CHALLENGES AND SOLUTIONS;

THEME-V
- LAW ENFORCEMENT AGENCIES AND CYBER CRIMES IN THE AGE OF AI
  - LEGAL CHALLENGES OF USE OF AI AS A TOOL IN FRAUD DETECTION;
  - ROLE OF POLICE IN CYBER CRIME INVESTIGATIONS AND CHALLENGES;
  - CYBER FORENSICS AND LEGAL IMPLICATIONS;
  - JURISDICTIONAL CHALLENGES ;
  - HUMAN RIGHTS AND POLITICAL CONCERNS FACED BY LAW ENFORCEMENT AGENCIES;

Note: The above-mentioned sub-themes are illustrative and not exhaustive and hence any submission pertinent to the provided themes may be taken into consideration.

PANEL DISCUSSION

A panel discussion as part of the conference will take place with resource persons expected to join from the legal academia, law enforcement officials, industry representatives and experts in the fields of cyber Laws, cyber security, and artificial intelligence.

ELIGIBILITY

The conference is open to all students across various disciplines, Ph.D. scholars, Academicians, Lawyers, Researchers, Policy Makers, Police Officers and Officials from various Departments, Representatives from Institutions, Social activists and NGOs.

REGISTRATION

Interested participants can register via the link provided below on or before 19th September 2024. Paper presenters can register once their abstracts are selected. Only 50 paper presenters slots are available. Accommodation will be provided on request basis for registrants and on payment of prescribed fee.
https://forms.gle/quA8HkMsdTyacDUZ7

Best Paper Presenter Award!

.

FEES

Paper Presentation

Students: Rs. 500

Academicians/ Advocates/ Industry Professionals/ Representatives from various departments/NGOs/others: Rs. 1000

Conference Participation/ observers only: Rs. 300

PAYMENT DETAILS

Account Name: TNNLU CONFERENCE SEMINAR AND WORKSHOPS

Account Number: 30030110042083

Bank: UCO Bank, TNNLS Branch

IFSC Code : UCBA0003003

REGISTRATION ON THE SUBJECT: 'CCAI NATIONAL CONFERENCE 2024'

TIMELINE OF CONFERENCE

- Deadline for abstract submissions: July 31, 2024
- Announcement of accepted abstracts: August 10, 2024
- Deadline for Full Paper Submission: September 01, 2024
- Intimation of Full Paper Acceptance: September 05, 2024
- Payment of fees & Registration of paper presenters: September 10, 2024
- Payment of fees & Registration for the observers/participants only: September 10, 2024
- Conference and Paper Presentation: September 21, 2024

SUBMISSION GUIDELINES

- Authors are invited to submit research papers on the above themes via e-mail to cyberlawcenter@tnnlu.ac.in with the subject '**Abstract Submission for CCAI Conference, TNNLU**'.

- An abstract of **300 words and 6 or 7 keywords** has to be submitted. The abstract must contain only the title of the paper.

- The name of the author(s), designation, institutional affiliation, e-mail address, postal address, and contact number must be sent in a **separate cover note** along with the abstract.

- Co-authorship is allowed up to a **maximum of 2 authors**.

- Authors whose abstracts have been submitted can submit the full papers of 3500 – 5000 words, including footnotes.

- Submissions should be original and unpublished works.

- If any submission is found plagiarized, it will be outrightly rejected.

- Full Paper submission should be submitted in a word document with the subject matter of '**Full Paper Submission for CCAI Conference, TNNLU**'.

- Acceptance of full papers will be intimated before the conference. Only accepted papers will be allowed to be presented.

- Authors must follow the Bluebook 21st edition citation style for the abstract and the full paper.

- **Formatting rules:**
  - Body Font – Times New Roman/Garamond
  - Body Font Size – 12, Size 14 can be used for Headings only
  - Line Spacing for the body – 1.5
  - Footnote font – Times New Roman/Garamond, Font Size – 10; Line Spacing -1.0
  - Page Margins – Normal
  - Page Size – A4; Orientation – Portrait
  - Page Nos. – Bottom/Top – Use Plain number

Disclaimer: The Organizing Committee reserves the right to modify and change the particulars of the conference whenever required.

CHIEF PATRON

PROF. (DR.) V. NAGARAJ
VICE-CHANCELLOR, TNNLU

PATRON

PROF. (DR.) S. M. BALAKRISHNAN

REGISTRAR, TNNLU

DIRECTOR OF THE CONFERENCE

MS. DEEPA MANICKAM
ASSISTANT PROFESSOR OF LAW
FACULTY-IN CHARGE
CENTRE FOR RESEARCH, DEVELOPMENT AND TRAINING IN
CYBER LAWS AND CYBER SECURITY (CRDT-CLCS), TNNLU.
DEEPAMANICKAM@TNNLU.AC.IN

FACULTY COORDINATORS

MR.NIDEESH KUMAR T.V. ,
ASST. PROF. OF LAW, TNNLU.

MS. VEDAVALLI. S,
ASST. PROF. OF LAW, TNNLU.

MS. DEEPIKA S,
ASST. PROF. OF LAW, TNNLU.

DR. PEERZADA SHAH FAISAL,
ASST. PROF. OF ECONOMICS,
TNNLU.

CONTACT:

CENTRE MAIL ID:
CYBERLAWCENTER@TNNLU.AC.IN

DIRECTOR OF THE CONFERENCE:
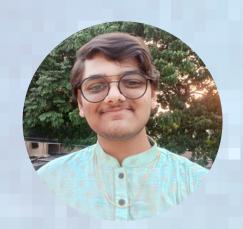MS. DEEPA MANICKAM
DEEPAMANICKAM@TNNLU.AC.IN

STUDENT COORDINATORS

MR GOKUL SHANKAR- 73053 35880

MR RAGHU DEVARAKONDA- 79016 95030