



L OVELY
P ROFESSIONAL
U NIVERSITY

Transforming Education Transforming India

NAAC
GRADE **A++**

International Conference on
**ARTIFICIAL INTELLIGENCE
IN INFORMATION SECURITY**



Organized by
Research and Development Cell, Lovely Professional University, Punjab



LOVELY PROFESSIONAL UNIVERSITY

Lovely Professional University (LPU) is a multi-faculty research-oriented institution with hi-tech campus offering more than 200 professional programmes. LPU campus is a complete world in itself having students from all states of India and more than 40+ countries of the world. LPU is a world class institution with internationally benchmarked curricula, innovative pedagogy focused on experiential learning, cutting edge research, 450+ foreign tie-ups, well qualified faculty with industry exposure, outstanding sports & cultural facilities, excellent residential facilities, In-campus shopping mall, hospital, banks, postal services etc. The University is ranked high on various parameters by Government Bodies and other credible organisations. LPU receives Highest Grade A++ with 3.68 score on 4 Point Scale by NAAC (National Assessment & Accreditation Council), an Autonomous Institution of the University Grants Commission (UGC), Ministry of Education, Govt. of India. The Times Higher Education World University Rankings 2025 has ranked LPU amongst Top 10 Universities in India Including all Government (even IITs & NITs), & Private Institutions, and many more.

ABOUT THE CONFERENCE

The International Conference on AI in Information Security will bring together researchers, practitioners, and industry leaders to explore how artificial intelligence is transforming the security landscape. This event will focus on the dual aspects of AI in information security: how it can enhance security measures and how it itself must be secured and governed. As AI technologies continue to evolve, their potential to strengthen security is vast. From improving threat detection and response times to enhancing data privacy and anomaly detection, AI has become a powerful tool in safeguarding digital systems. However, with the increasing integration of AI into security infrastructure, concerns about its vulnerabilities are also growing. The conference will address how AI systems can be protected from misuse and adversarial attacks, ensuring they are transparent, accountable, and resilient.

The conference will bring together thought leaders to share insights on the latest AI-driven security innovations, explore real-world applications, and discuss the challenges of securing AI itself. Key topics will include AI-based threat intelligence, ethical considerations in AI security, the governance of AI technologies, and the potential risks associated with AI in cybersecurity. By providing a platform for knowledge exchange and collaboration, the conference aims to bridge the gap between theoretical research and practical application. It will encourage partnerships across industries and academia, helping to shape the future of AI-driven security solutions and establishing best practices for securing AI technologies. The event will serve as a critical step in advancing both the capabilities of AI in information security and the necessary safeguards to protect it.

CONFERENCE TRACKS AND TOPICS

Track 1: Network Security: Intrusion detection, anomaly detection, malware analysis, AI-driven threat intelligence, secure network protocols, cloud/edge/IoT security, adversarial traffic analysis, AI-assisted red-team operations.

Track 2: Information Security: AI-based data protection, cryptography and key management, IAM, digital forensics, privacy-preserving ML, secure data pipelines, risk modelling, automated incident response.

Track 3: Software Security: Vulnerability detection using AI, automated code review, secure DevOps, secure SDLC, fuzzing, static/dynamic analysis, supply-chain security, GenAI security risks in coding tools.

Track 4: Security of AI: Adversarial ML, model extraction/inversion, data poisoning, watermarking, secure training pipelines, LLM robustness, federated learning security, trustworthy AI deployment.

Track 5: AI, explainability, bias and fairness audits, governance frameworks, regulatory compliance (EU AI Act, IndiaAI), societal impacts, accountability mechanisms

Track 6: AI-driven defense security using predictive intelligence, autonomous systems, cyber defense, SIGINT, and explainable AI.

KEYNOTE SPEAKERS



Prof. Farshad Badie

The Dean,
Faculty of Computer
Science and Informatics
Berlin School of Business
and Innovation (BSBI),
Germany



Richard Blech

Founder and CEO,
XSOC CORP,
United States of America



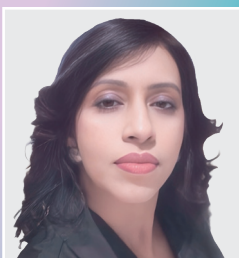
Megha Pandey

Network Engineer,
Wipro, India



Prof. Atta Ur Rahman Khan

Professor,
Ajman University



Dr. Shravani Shahapure

Associate Director,
Cyber and Emerging Technologies
Deloitte Touche Tohmatsu
India LLP



Prof. NK Goyal

President, CSAI
President, CMAI Association
of India & Chairman
Emeritus TEMA



Dr. Ch. A. S Murty

Sc 'G', CISO and Centre Head
(C-DAC Kolkata) Centre for
Development of Advanced
Computing (C-DAC) A Scientific
Society of Ministry of Electronics
and Information Technology
(MeitY) Government of India

ORGANIZING COMMITTEE

Chief Patron

Dr. Ashok Kumar Mittal
Honourable Chancellor, LPU

Patron

Mrs. Rashmi Mittal
Worthy Pro Chancellor, LPU

General Chair

Prof. Lovi Raj Gupta
Pro-Vice Chancellor, LPU

Prof. Monica Gulati
Research & Development
Cell, LPU

General Co-Chair

Prof. Atul Thakur
Research & Development
Cell, LPU

Program Chair

Prof. Rahul Saha
School of Computer
Science & Engineering,
Research & Development
Cell, LPU

Prof. Gulshan Kumar
School of Computer
Science & Engineering,
Research & Development
Cell, LPU

Program Co-Chair

Dr. Shravani Sahapure
Big4, India

Dr. Archana Chhabra
School of Computer
Science and Engineering,
LPU

Dr. Harpreet Kaur
School of Computer
Science and Engineering,
LPU

Dr. Chetna
School of Computer
Science and Engineering,
LPU

International Chair

Prof. Atta Ur Rahman Khan
Ajman University,
United Arab Emirates

Dr. Farshad Badie
Berlin School of Business
and Innovation, Germany

Richard Blech
XSOC Corporation,
United States of America

Publication Chair

Dr. Anand Nayyar
Duy Tan University,
Vitenam

Dr. Weiwei Jiang
Beijing University of Posts
and Telecommunications,
China

Dr. Shravani Shahpure
Big4, India

Registration & Finance Chair

Prof. Ramandeep Singh
Research & Development
Cell, LPU

Dr. Chetna
School of Computer
Science & Engineering, LPU

Local Arrangement Chair

Prof. Devendra K. Pandey
Research & Development
Cell, LPU

Mr. Balpreet Singh
Research & Development
Cell, LPU

Technical Chair

Dr. Anand Nayyar
Duy Tan University, Vietnam

Dr. Leila Bayoudhi
University of Monastir, Tunisia

Prof. Tai Hoon Kim
Chonnam National University,
South Korea

Plenary Session Chair

Dr. Sushil Kumar Singh
Marwadi University,
Gujarat, India

Dr. Leila Bayoudhi
University of Monastir, Tunisia

Dr. Ramesh Kumar Thakur
National Institute of Technology,
Bhopal, India

Dr. Souvik Das
National Institute of Technology,
Rourkela, India

Dr. Prateek Agrawal
Rungta International Skills
University, Bhilai, India

Dr Ankit Kumar Jain
National Institute of Technology,
Kurukshetra, India

Dr Himanshu Nandanwar
Motilal Nehru National Institute
of Technology Allahabad, India

Dr. Achyut Shankar
Benette University India and
University of Johannesburg,
South Africa

Dr. Tawseef Ayoub Shaikh
National Institute of Technology
Srinagar, Jammu & Kashmir, India

Dr. T P Sharma
National Institute of Technology
Hamirpur, Jammu & Kashmir, India

Hospitality Chair

Mr. Akshay Kumar
Research & Development
Cell, LPU

Technical Arrangement

Dr. Rohan Kumar
Research and Development
Cell, LPU

Dr. Jaisukh Paul Singh
Research and Development
Cell, LPU

Mr. Ayush Baliyan,
Research and Development
Cell, LPU

Collaboration & Guest Facilitation

Prof. Reji Thomas
Research and Development
Cell, LPU

Dr. Abhinay Thakur
Research and Development
Cell, LPU

Media & Publicity Chair

Mr. Balwinder Singh
Web Designer,
Division of Infotech, LPU

TIMELINE OF SUBMISSIONS (TENTATIVE)

Conference Dates:
September 10-11, 2026

Last Date of Paper Submission:
June 30, 2026

**Registration
Last Date:**
August 30, 2026

Paper Acceptance Notification:
July 15, 2026

Camera Ready Submission End Date:
August 15, 2026

TECHNICAL PARTNER



PUBLICATION PARTNER



PROGRAM COMMITTEE

Alti Adel	Ferhat Abbas SETIF-1 University, Algeria
Bestoun S. Ahmed	Karlstads Universitet, Sweden
Nauman Bin Ali	Blekinge Institute of Technology, Sweden
Domenico Amalfitano	University Federico II of Naples, Italy
Davide Ancona	Università di Genova, Italy
Marco Antônio Araújo	Federal University of Juiz de Fora, Brazil
Francesca Arcelli Fontana	University of Milano-Bicocca, Italy
Saïd Assar	Institut Mines-Telecom Business School, France
Issa Atoum	Philadelphia University, Jordan
Deepika Badampudi	Blekinge Institute of Technology, Sweden
Doo-Hwan Bae	Korea Advanced Institute of Science and Technology, Republic of Korea
Marcio de Oliveira Barros	Universidade Federal do Estado do Rio de Janeiro - UNIRIO, Brazil
Davide Basile	ISTI CNR Pisa, Italy
Lorenzo Bettini	DISIA, Univ. Firenze, Italy
Saurabh Bilgaiyan	KIIT Deemed to be University, India
Iuliana Maria Bocicor	Babes-Bolyai University, Romania
Boyan Bontchev	Sofia University "St. Kliment Ohridski", Bulgaria
Fernando Brito e Abreu	ISTAR/ISCTE-IUL, Portugal
Bernd Bruegge	Technical University Munich, Germany
Ralf Bruns	Hannover University of Applied Sciences and Arts, Germany
Alessio Bucaioni	Maelardalen University, Sweden
Alena Buchalceva	University of Economics, Czechia
Ahmet E. Cakir	Ergonomic Institut, Germany
Carlos Cares	Universidad de La Frontera, Chile
Eric Cariou	Lab-STICC, University of Brest, France

Josep Maria Carmona Leyva	Independent Researcher, Spain
Juan Manuel Carrillo-de-Gea	Dept. Informatics and Systems, University of Murcia, Spain
Marcos Lordello Chaim	University of São Paulo, Brazil
Allaoua Chaoui	University Constantine 2 - Abdelhamid Mehri, Algeria
Anis Charfi	CMU, Qatar
Grigoreta-Sofia Cojocar	Babes Bolyai University, Romania
Lucas Cordeiro	University of Manchester, United Kingdom
Agostino Cortesi	Università Ca' Foscari di Venezia, Italy
Heitor Costa	Federal University of Lavras, Brazil
Michael John Decker	Bowling Green State University, United States
Giuseppe Destefanis	Brunel University London, United Kingdom
Marcos Didonet Del Fabro	Universite Paris-Saclay, CEA List, France
Hércules Antonio do Prado	Catholic University of Brasília, Brazil
Sophie Ebersold	IRIT, France
Mahmoud El Hamlaoui	ENSIAS, UM5R, Morocco
Vladimir Estivill-Castro	Universitat Pompeu Fabra, Spain
Carles Farré	Universitat Politècnica de Catalunya, Spain
Shukor Sanim M. Fauzi	Universiti Teknologi MARA, Malaysia
Maria João Ferreira	Universidade Portucalense, Portugal
Massimo Ficco	University of Salerno, Italy
Eduardo Figueiredo	Federal University of Minas Gerais, Brazil
Tarik Fissaa	Computer Science, INPT, Morocco
Samuel Fricker	University of Applied Sciences Northwestern Switzerland FHNW, Switzerland
Ilenia Fronza	Free University of Bolzano - Bozen, Italy
José A. Galindo	University of Seville, Spain
Stéphane Galland	Université de Technologie de Belfort Montbéliard, France
Cigdem Gencel Ambrosini	Independent Researcher, Italy
Nicolas Gold	University College London, United Kingdom
Elena Gómez-Martínez	Universidad Complutense de Madrid, Spain
Tony Gorschek	BTH, Sweden
Gregor Grambow	Hochschule Aalen, Germany
Yann-Gaël Guéhéneuc	Concordia University, Canada
Hatim Hafiddi	INPT, Morocco
G. W. Hamilton	Dublin City University, Ireland
Bogumiła Hnatkowska	Independent Researcher, Poland
Ralph Hoch	TU Wien
Helena Holmström Olsson	Malmo University, Sweden
Ludovico Iovino	Gran Sasso Science institute, Italy
Takashi Ishio	Future University of Hakodate, Japan
Mirjana Ivanovic	University of Novi Sad, Serbia
Dayang N. A. Jawawi	University of Technology Malaysia, Malaysia
George Kakarontzas	Digital Systems Department, University of Thessaly, Greece
Mohamad Kassab	Pennsylvania State University, United States



L OVELY
P ROFESSIONAL
U NIVERSITY

Transforming Education Transforming India

LOVELY PROFESSIONAL UNIVERSITY (LPU)

Jalandhar-Delhi, G.T. Road, Phagwara, Punjab (INDIA) -144411.

ThinkBIG