ICISS

International Conference on Information Systems Security (ICISS 2025)
IIT Indore, Indore, Madhya Pradesh, India
16th – 20th December 2025

ICISS 2025 Technical Program

DAY 1 PROGRAM – TUESDAY, DECEMBER 16

Time (IST)	Event
09:00 – 09:30	Registration and Welcoming Participants
09:30 – 11:30	**TUTORIAL 1: Federated Learning: Architecture, Threat Landscape, and Defence Mechanisms** **Speakers:** Prof. Rajiv Ranjan (Newcastle University, UK), Dr. Devki Nandan Jha (Newcastle University, UK), Dr. Tejal Shah (Newcastle University, UK)
11:30 – 11:45	TEA BREAK
11:45 – 13:00	**TUTORIAL 1** (Prof. Rajiv Ranjan's Team)
13:00 – 14:00	LUNCH
14:00 – 16:15	**TUTORIAL 2: Vajra-Sandbox: A Robust Framework for Malware Execution and Analysis** **Speakers:** Dr. Manjesh Kumar Hanawal (IIT Bombay), Mr. Atul Kabra (ReliaQuest, Bengaluru), Mr. Prakhar Paliwal (IIT Bombay)
16:15 – 16:30	TEA BREAK
16:30 – 17:30	**TUTORIAL 2** (Dr. Manjesh Kumar Hanawal's Team)

DAY 2 PROGRAM – WEDNESDAY, DECEMBER 17

Time (IST)		Event
09:00 – 09:30		Registration
09:30 – 10:30		**Conference Inauguration**
10:30 – 11:30		**KEYNOTE 1:** Practical Resilient Efficient Quantum Key Distribution **Speaker:** Prof. Pranab Sen (TIFR, Mumbai)
11:30 – 11:45		TEA BREAK
11:45 – 13:00	**Paper Presentation Session 1: AI/ML Security**	
	11:45 – 12:05	**Curriculum Learning with Image Transformation and Explainable AI for Improved Network Intrusion Detection** Sathwik Narkedimilli, Pavan Kumar, Raghavendra Ramachandra
	12:05 – 12:25	**MazeNet: Protecting DNN Models on Public Cloud Platforms with TEEs** Kripa Shanker, Vivek Kumar, Aditya Kanade, Vinod Ganapathy
	12:25 – 12:45	**Automation and Risk: Transformers Models Reshape Secrecy Information Management** Wellington Fernandes Silvano, Maurício Konrath, Lucas Mayr, Ricardo Felipe Custódio
	12:45 – 13:00	**The Hidden Risks of LLM-Generated Web Application Code: A Security-Centric Evaluation of Code Generation Capabilities in Large Language Models** Swaroop Dora, Deven Lunkad, Naziya Aslam, Subramanian Venkatesan, Sandeep Kumar Shukla
13:00 – 14:00		LUNCH
14:00 – 15:15	**Paper Presentation Session 2: Applied Cryptography**	
	14:00 – 14:20	**Randomness Efficient Algorithms for Estimating Average Gate Fidelity via k-wise Classical and Quantum Independence** Pranab Sen, Aditya Nema
	14:20 – 14:40	**Cryptanalysis of Two Outsourced Ciphertext-Policy Attribute-Based Encryption Schemes** Koshalesh Meher, Y Sreenivasa Rao
	14:40 – 15:00	**Dynamic Key-Constant Aggregate Encryption (DKCAE) for Secure Data Sharing in Contemporary Computing** Inarat Hussain, Devrikh Jatav, Gaurav Pareek, Purushothama BR
	15:00 – 15:15	**DoPQM: Devices Oriented Post-Quantum Cryptographic Migration Strategies for an Enterprise Network** Amit Bhowmick, Divyesh Saglani, Lakshmi Padmaja Maddali, Akhila Rayala, Meena Singh Dilip Thakur, Rajan M A

15:15 – 16:15		**INVITED TALK:** Reverse Engineering Industrial Control Devices **Speaker:** Dr. Nils Ole Tippenhauer (CISPA, Germany)
16:15 – 16:30		TEA BREAK
16:30 – 17:00	**Paper Presentation Session 3: AI/ML Security**	
	16:30 – 16:45	**Frequency-Aware Deepfake Detection: Transformers vs. CNNs** Aditi Panda, Srijit Kundu, Tanusree Ghosh, Ruchira Naskar
	16:45 – 17:00	**A Secure Federated Learning using Differential Privacy Mondrian Clustering** Rojalini Tripathy, Paladri Pranitha, B U Tejonath, Padmalochan Bera

DAY 3 PROGRAM – THURSDAY, DECEMBER 18

Time (IST)		Event
09:00 – 09:30		Registration
09:30 – 10:30		**KEYNOTE 2:** AI Agentic Security: Safeguarding the Next Generation of Autonomous Systems **Speaker:** Prof. Elisa Bertino (Purdue University)
10:30 – 11:30	**Paper Presentation Session 4: Security & Privacy**	
	10:30 – 10:50	**SoK: Evaluation of Methods for Privacy Preserving Edge Video Analytics** Arun Joseph, Vinod Ganapathy
	10:50 – 11:10	**Privacy-Preserving Fair Text Summarization Using Federated Learning** Aman Lachhiramka, Nibhrant Vaishnav, Dheeraj Kumar
	11:10 – 11:30	**Uncovering Security Weaknesses in srsRAN withCodeQL: A Static Analysis Approach forNext-Gen RAN Systems** Garrepelly Manideep, Sriram Sankaran, Altaf Shaik
11:30 – 11:45		TEA BREAK
11:45 – 13:00	**Paper Presentation Session 5: Threat Detection**	
	11:45 – 12:05	**Adversarial Attack on CryptoEyes from INFOCOM 2021** Jashwanth Kadarum, Imtiyazuddin Shaik, Srinivas Vivek
	12:05 – 12:25	**Cyber Warfare During Operation Sindoor: Malware Campaign Analysis and Detection Framework** Prakhar Paliwal, Atul Kabra, Manjesh Kumar Hanawal
	12:25 – 12:45	**SAAT: Stealthy Adversarial Attack on IDS in Cyber Physical Systems using Control Logic Induction** Tanmoy Kanti Das, Rajneesh Kumar Pandey

	12:45 – 13:00	**Genetic-LAD: A Hybrid Approach for Financial Fraud Detection** Nikhil Katiyar, Sneha Chauhan, Sugata Gangopadhyay, Aditi Kar Gangopadhyay
13:00 – 14:00		LUNCH
14:00 – 15:15	**Paper Presentation Session 6: Security & Privacy**	
	14:00 – 14:20	**Systematic Literature Review of Vulnerabilities and Defenses in VPNs, Tor, and Web Browsers** Neha Agarwal, Ethan Mackin, Faiza Tazi, Mayank Grover, Rutuja More, Sanchari Das
	14:20 – 14:35	**SANVector: SBERT-APTNet Vector framework for Cyber Threat Attack Attribution using diversified CTI Logs** Sougata Dolai, Annu Kumari, Mayank Agarwal
	14:35 – 14:50	**Self Learning Digital Twin for Kubernetes Security** Devnath N S, Adarsh Sasikumar, Aayushman Singh, Sriram Sankaran
	14:50 – 15:05	**Security and Privacy Assessment of U.S. and Non-U.S. Android E-Commerce Applications** Urvashi Kishnani, Sanchari Das
	15:05 – 15:15	Buffer / Transition Time
15:15 – 16:15		**PANEL DISCUSSION**
16:15 – 16:30		TEA BREAK
16:30 – 17:00	**Paper Presentation Session 7: Threat Detection**	
	16:30 – 16:45	**Enhancing Android Malware Detection with Federated Learning: A Privacy-Preserving Approach to Strengthen Cyber Resilience** Monalisa meena, Jyoti Gajrani, Meenakshi Tripathi, Dhruv Suthar, Chetan Rawat, Sweety Singhal
	16:45 – 17:00	**Security-Centric NWDAF Module for Threat Detection and Mitigation in 5G Core Networks** Lakshmi R. Nair, Adithya Anil, Preetam Mukherjee, Manuj Aggarwal

CONFERENCE BANQUET DINNER

DAY 4 PROGRAM – FRIDAY, DECEMBER 19

Time (IST)		Event
09:00 – 09:30		Registration
09:30 – 10:30		**PhD Forum Session 1**
10:30 – 11:30		**PhD Forum Session 2**
11:30 – 11:45		TEA BREAK
11:45 – 13:00		**PHD FORUM TALK:** Towards Developing Skills for Writing Great Papers and Giving Great Talks **Speaker:** Prof. Atul Prakash (University of Michigan, Ann Arbor)
13:00 – 14:00		LUNCH
14:00 – 15:15		**Paper Presentation Session 8: AI/ML Security**
	14:00 – 14:20	**NEXUS: Neuron Activation Scores Exploits for Unveiling Sensitive Attributes** Debasmita Manna, Somanath Tripathy
	14:20 – 14:40	**Attack Resilient Federated Learning Framework** Sushant Kumar, Kasturi Routray, Padmalochan Bera
	14:40 – 14:55	**An ML-Driven Adaptive Risk-Based Access Control for the Internet of Drones (IoD)** Jithu Vijay V P, Sabu M Thampi, Alwin Varghese T
	14:55 – 15:10	**Optimizing Machine Learning Based Access Control Administration Through Data Distillation** Mohammad Nur Nobi, Md Shohel Rana, Ram Krishnan
	15:10 – 15:15	Buffer / Transition Time
15:15 – 16:15		**KEYNOTE 3:** Smart Contracts, Dumb Mistakes: Understanding and Preventing DeFi Exploits **Speaker:** Prof. Christopher Kruegel (University of California, Santa Barbara)
16:15 – 16:30		TEA BREAK
16:30 – 17:00		**Paper Presentation Session 9: Security & Privacy**
	16:30 – 16:45	**Modular Analysis of Attack Graphs for Smart Grid Security** Smitha Rani, Preetam Mukherjee, Mathias Ekstedt
	16:45 – 17:00	**Adaptive MQTT Honeypots for IIoT Security Using Extended Mealy Machines** Saurabh Chamotra, Navdeep Singh, Piyali Dutta

DAY 5 PROGRAM – SATURDAY, DECEMBER 20

Time (IST)	Event
09:00 – 09:30	Registration
09:30 – 11:30	**DRDO Workshop Session** **Title:** NIGHUD (Network Information Gathering of Hidden Unseen Data)
11:30 – 11:45	TEA BREAK
11:45 – 13:00	**KEYNOTE 4:** Threat Modeling for Security of Machine Learning Systems **Speaker:** Dr. Anoop Singhal (NIST, Gaithersburg)
13:00 – 14:00	LUNCH
14:00 – 16:15	**CDAC Workshop Session** **Title:** Digital Trust for IoT Ecosystems: From Secure Identities to Quantum-Resilient Security
16:15 – 16:30	TEA BREAK
16:30 – 17:00	**Valedictory Session**