Event	Duration (hh:mm:ss)	Start	End	Details
Day 1 (December 17, 2024)				
Opening Remarks (30 mins)	00:30:00	09:00:00	09:30:00	Patron, Local Chair, PC Chairs, General Chair
Keynote 1 Chair: Vishwas Patil (50 mins)	00:50:00	09:30:00	10:20:00	**Scams in the Cryptocurrency Market** *Alessandro Mei, Sapienza University of Rome*
Tea break	00:10:00	10:20:00	10:30:00	--
Session 1 **Systems Security** Chair: TBA (80 mins)	01:20:00	10:30:00	11:50:00	**Microarchitectural Security of Firecracker VMM for Serverless Cloud Platforms** (Weissman, Zane, Tiemann, Thore, Eisenbarth, Thomas, Sunar, Berk) **An OS support for Tamper-resistant Software Execution Using Empty Interruptions** (Kato, Souma, Koyanagi, Yui, Ukezono, Tomoaki) **S-RFUP: Secure Remote Firmware Update Protocol** (Podder, Rakesh, Rios, Tyler, Ray, Indrajit, Raman, Presanna, Righi, Stefano) **Securing Virtual Reality Apps Inter-Process Communication** (Falebita, Oluwatosin, Ray, Indrakshi, Abdelgawad, Mahmoud, Anspach, Evan)
Tea break	00:10:00	11:50:00	12:00:00	--
Invited Talk 1 Chair: Vishwas Patil (30 mins)	00:30:00	12:00:00	12:30:00	**Large Language Models: Are Guarded Models Safe?** *Atul Prakash, University of Michigan*
Lunch break	01:00:00	12:30:00	13:30:00	*Venue: TBA*
Session 2 **Network Security** Chair: TBA (55 mins)	00:55:00	13:30:00	14:25:00	**Securing the Web: Analysis of HTTP Security Headers in Popular Global Websites** (Kishnani, Urvashi, Das, Sanchari) **BP-MAP: A Secure and Convenient Mutual Authentication Protocol** (Narumanchi, Harika, Maddali, Lakshmi Padmaja, N, Narendra Kumar) **Effects of Soft-Domain Transferand Named Entity Informationon Deception Detection** (Triplett, Steven, Verma, Rakesh, Minami, Simon)
Break	00:05:00	14:25:00	14:30:00	--
Keynote 2 Chair: Ram Krishnan (50 mins)	00:50:00	14:30:00	15:20:00	**Security Tai Chi: The Art of Building and Attacking Secure Computing Systems** *Ahmad-Reza Sadeghi, TU Darmstadt*
Tea break	00:10:00	15:20:00	15:30:00	--

Event	Duration (hh:mm:ss)	Start	End	Details
Session 3 **Network Security* & Attacks** Chair: TBA (90 mins)	01:30:00	15:30:00	17:00:00	***Countering Subscription Concealed Identifier (SUCI)-Catchers in Cellular Communications** (Parkin, Julian, Tripunitara, Mahesh) **Paving the Way: Advancing V2X Safety Through Innovative Attack Generation and Analysis Framework (V2X-SAF)** (Tomar, Shubham, Tripathi, Meenakshi, Yadav, Harsh, Singh, Amarbir) **From Traits to Threats: Learning Risk Indicators of Malicious Insider using Psychometric Data** (Nanamou, N'Famoussa Kounon, Neal, Christopher , Boulahia-Cuppens, Nora, Cuppens, Frédéric, Bkakria, Anis) **Identifying Insecure Network Configurations through Attack Modeling and Explainable AI** (Thomas, Blessy, M Thampi, Sabu, Mukherjee, Preetam) **QIris: Quantum Implementation of Rainbow Table Attacks** (Jun Quan , Lee, Jia Ye, Tan, GEOK LING, GOH, Balachandran, Vivek)
Business Meeting^^	00:20:00	17:00:00	17:20:00	All are invited to attend. ^^(post meeting, participants will travel to Chokhi Dhani for Conference Dinner)
Day 2 (December 18, 2024)				
Keynote 3 Chair: Ram Krishnan (50 mins)	00:50:00	09:30:00	10:20:00	**Data Security and Privacy in Emerging Scenarios** *Pierangela Samarati, University of Milan*
Tea break	00:10:00	10:20:00	10:30:00	
Session 4a **Privacy & Usability** Chair: TBA (60 mins)	01:00:00	10:30:00	11:30:00	**Web Privacy Perceptions Amongst Indian Users** (Kancherla, Gayatri Priyadarsini, Dey, Aditi, Saroj, Prakriti, Bichhawat, Abhishek, Saxena, Anshika, Saxena, Anshika) **Making EULA Great Again: A Novel Nudge Mechanism to Improve Readability, User Attention and Awareness** (Bin Zahid, Shamim, Ghosh Bristy, Aishwarya, Hasan Oli, Md Musfikur, Fahim, Md , Ahmed Rumee, Sarker, Zaber, Moinul Islam) **A Decoupling Mechanism for Transaction Privacy** (Patil, Vishwas, Shyamasundar, RK)
Tea break	00:15:00	11:30:00	11:45:00	
Session 4b **Privacy & Usability** Chair: TBA (45 mins)	00:45:00	11:45:00	12:30:00	**Enabling Privacy in IT Service Operations** (Gupta, Rohit, Kumar, Rishabh, Mondal, Sutapa, Gharote, Mangesh, Lodha, Sachin) **Privacy-Preserving Photo Sharing: An SSI Use Case** (Shehu, Sadiq, Fraser, Ashley, Frymann, Nick, Haynes, Paul, Schneider, Steve) **Zone Recovery Attack on a Secure Privacy-Preserving Ride-Matching Protocol** (Murthy, Shyam, Upadhyaya, Santosh Kumar, Vivek, Srinivas)
Lunch break	01:00:00	12:30:00	13:30:00	
Session 5 **AI Security** Chair: TBA (60 mins)	01:00:00	13:30:00	14:30:00	**Protecting ownership of trained DNN models with Zero-Knowledge Proofs** (Sato, Shungo, Tanaka, Hidema) **MALAI: ML-based Attack on Learning With Error problem** (Suma Sri, Mandru, Yadav, Chakka Srikanth, Sanyashi, Tikaram, Singh, Virendra) **Patch based backdoor attack on Deep Neural Networks** (manna, debasmita, Tripathy, Somanath)
Keynote 4 Chair: Ram Krishnan (50 mins)	00:50:00	14:30:00	15:20:00	**Biometrics and AI: Challenges and Opportunities** *Vincenzo Piuri, University of Milan*

Event	Duration (hh:mm:ss)	Start	End	Details
Tea break	00:10:00	15:20:00	15:30:00	
Invited Talk 2 Chair: Vishwas Patil (30 mins)	00:30:00	15:30:00	16:00:00	**Towards Regulated, Private and Robust Central Bank Digital Currency** *Kari Kostiainen, ETH Zurich*
Session 6 **Malware & Vulnerability Detection** Chair: Saurabh Sharma (60 mins)	01:00:00	16:00:00	17:00:00	**Insights from Running 24 Static Analysis Tools on Open Source Software Repositories [ONLINE]** (Hashmat, Fabiha, Alwaleed Aljaali, Zeyad, Shen, Mingjie, Machiry, Aravind) **REMEDII: Robust Malware Detection with Iterative and Intelligent Adversarial Training using GANs** (Gupta, Sanchit, Kumar, Vireshwar) **Semantics-Based Static Vulnerability Detection of Solidity Using Abstract Interpretation** (Kushwaha, Maitri, Mukherjee, Arnab, Pandey, Aishwarya, Halder, Raju)
Session 7 **PhD Forum** **Lightening Talks** (60 mins)	01:00:00	17:00:00	18:00:00	**PhD Forum presentations** Lightning Talks (5 mins each)
Day 3 (December 19, 2024)				
Invited Talk 3 Chair: TBA (30 mins)	00:30:00	09:30:00	10:00:00	**The Multifaceted Role of Cryptographic Primitives in XRPL R&D** *Aanchal Malhotra, Ripple*
Session 8 **Industry/Demo Papers** Chair: TBA (60 mins)	01:00:00	10:00:00	11:00:00	**Integrating Crypto-Based Payment Systems for Data Marketplaces: Enhancing Efficiency, Security, and User Autonomy** (Walunj, Vipul, Dutta, Jyotirmoy, Rajaraman, Vasanth, Sharma, Abhay) **Ontologies for WAF configurations: when knowledge-graphs help troubleshooting** (Wiaux, Bastien, Bertrand Van Ouytsel, Charles-Henry, Legay, Axel, Stern, Marc) **IntelliSOAR: Intelligent Alert Enrichment using Security Orchestration Automation and Response (SOAR)** (Dwivedi, Surabhi, Rajendran, Balaji, P V, Akshay, Akshaya, Acha, Ampatt, Praveen, Sudarsan, Sithu D) **InTrust: An Asset Monitoring, Analysis and Vulnerability Assessment system for Zero Trust Network** (Muraleedharan, Rajendra Neve, Hrishikesh, Sarkar, Samar, Rajendran, Balaji)
Invited Talk 4 Chair: TBA (30 mins)	00:30:00	11:00:00	11:30:00	**Modeling and Security Analysis of Attacks on Machine Learning Systems** *Anoop Singhal, NIST*
Research Opportunities Track (30 mins)	00:30:00	11:30:00	12:00:00	Announcement from the Sponsors & others on internships, research initiatives, and collaboration opportunities
ICISS-2024 Closing Remarks (30 mins)	00:30:00	12:00:00	12:30:00	TPC Co-chairs, Local Organising Committee
Lunch	01:00:00	12:30:00	13:30:00	