PST2025 Preliminary Program			
27 AUGUST 2025 (ADT Time)			
8:00 – 16:00	Conference On-Site Registration		
8:30 – 8:45	Welcome Speeches -- Dr. Ali Ghorbani and Dr. Rongxing Lu		
8:45 – 9:45	Invited Talk 1 (in-person) -- Dr. Sébastien Gambs		
9:45 – 10:15	Morning Break and Poster Presentations		
10:15 – 11:55	In-Person Session PS1	In-Person Session PS2	Online Session OS1
11:55 – 13:00	Lunch		
13:00 – 14:00	Invited Talk 2 (online) -- Dr. Lingyu Wang		
14:00 – 15:40	In-Person Session PS3	In-Person Session PS4	Online Session OS2
15:40 – 16:10	Afternoon Break and Poster Presentations		
16:10 – 17:30	In-person CIC Cybersecurity 4MT Competition		Online Session OS3
18:30 – 21:00	Banquet		
28 AUGUST 2025			
8:00 – 12:00	Conference On-Site Registration		
8:00 – 8:45	Networking		
8:45 – 9:45	Invited Talk 3 (in-person) -- Dr. Roozbeh Razavi-Far		
9:45 – 10:15	Morning Break and Poster Presentations		
10:15 – 11:55	In-Person Session PS5	In-Person Session PS6	Online Session OS4
11:55 – 13:00	Lunch		
13:00 – 14:40	In-Person Session PS7	In-Person Session PS8	Online Session OS5
14:40 – 15:10	Afternoon Break and Poster Presentations		
15:10 – 16:30	In-Person Session PS9		Online Session OS6
16:30 – 16:50	Closing		

*Posters will be displayed during both days (27th and 28th). Poster presenters are expected to be at the poster display area during the refreshment breaks.

27 AUGUST 2025

27 AUGUST 2025, 10:15 – 11:55

In-Person Session PS1: Malware Detection with Machine Learning

Room: Aitken Room

Chair: Mahdi Rabbani

- **Paper ID 7**: Using Counterfactuals for Explainable Android Malware Detection
  Authors: Maryam Tanha, Winston Zhao, Aaron Hunter, Ashkan Jangodaz
- **Paper ID 107**: TOM-Net: Few-Shot IoT Malware Classification via Open-Set Aware Transductive Meta-Learning
  Authors: Man-Ying Chen, Tao Ban, Shin-Ming Cheng, Takeshi Takahashi
- **Paper ID 109**: Evaluating Efficient Patch-Based Backdoor Attacks in Satellite Image Classification Systems
  Authors: Ghazal Rahmanian, Pooria Madani

- **Paper ID 130**: A Per-Bag Suspicion-Based Bagging Strategy for Fighting Poisoning Attacks in Classification
  Authors: Aghoghomena Akasukpe, Tomi Adeyemi, Pooria Madani, Li Yang, Miguel Vargas Martin
- **Paper ID 133:** Harnessing Language Models to Analyze Android App Permission Fidelity
  Authors: Yunik Tamrakar, Ritwik Banerjee, Ethan Myers, Lorenzo De Carli, Indrakshi Ray

27 AUGUST 2025, 10:15 – 11:55

In-Person Session PS2: Privacy-Preserving Data and Image Processing

Room: J. Harper Kent Auditorium

Chair: Sara Miller

- **Paper ID 40**: CONTEXT-AWARE LOCATION DE-IDENTIFICATION USING DENOISING DIFFUSION
  Authors: Md Shopon, Marina Gavrilova
- **Paper ID 99**: Private Function Evaluation using CKKS-based Homomorphic Encrypted LookUp Tables
  Authors: Haoyun Zhu, Takuya Suzuki, Hayato Yamana
- **Paper ID 151**: Privacy-Preserving Image Learning Across Trust Boundaries
  Authors: Atsuko Miyaji, Tomoshi Yagishita, Yuki Hyohdoh

27 AUGUST 2025, 10:15 – 11:55

Online Session OS1: Anomaly Detection and Vulnerability Analysis

Room: Chancellor's Room

Chair: Mohammad Jafari Dehkordi

- **Paper ID 75**: Exploring Clustering Algorithms for Anomaly Detection in Electric Vehicle Charging Stations Infrastructure using OCPP
  Authors: Chris Tchassem, Yendoubé Kombate, Pierre-Martin Tardif
- **Paper ID 93**: Legal Retrieval Augmented Generation with Structured Retrieval and Iterative Refinement
  Authors: Chaitanya Dhananjay Jadhav, Chang Liu, Jun Zhao
- **Paper ID 136**: Characterizing Event-themed Malicious Web Campaigns: A Case Study on War-Themed Websites
  Authors: Maraz Mia, Mir Mehedi Ahsan Pritom, Tariqul Islam, Shouhuai Xu
- **Paper ID 149**: TFVDFuzzer: Transformer-based Fuzzing Framework for Vulnerability Detection in Modbus Protocol
  Authors: Ahmed Reda Aldysty, Nour Moustafa, Erandi Lakshika
- **Paper ID 154**: Database Systems Examination and Digital Forensics Tool: the Progress and Limitations
  Authors: Oluwasola Mary Adedayo

27 AUGUST 2025, 14:00 – 15:40

In-Person Session PS3: Cryptographic Techniques and Secure Systems

Room: Aitken Room

Chair: Vikas Chouhan

- **Paper ID 2**: A Static Analysis of Popular C Packages in Linux
  Authors: Jukka Ruohonen, Krzysztof Sierszecki, Mubashrah Saddiqa
- **Paper ID 50**: CHOO-PIR: Hint-Based Private Information Retrieval with Commodity Servers
  Authors: Kittiphop Phalakarn, Ryuya Hayashi
- **Paper ID 114**: Empirical Evaluation and Reclassification of Cryptographic Algorithms for Energy-Efficient Secure Communication in Medical IoT Devices
  Authors: Sidra Anwar, Jonathan Anderson
- **Paper ID 116**: Comparing Client- & Server-Side AEAD Encryption in Software-Defined Storage Systems
  Authors: David Mohren, Minh Tien Truong, Brett Kelly, Kenneth Kent
- **Paper ID 158**: Securing Android Inter-Process Communication (IPC) Using NGAC
  Authors: Jason Simental, Elmaddin Azizli, Mahmoud Abdelgawad, Indrakshi Ray

27 AUGUST 2025, 14:00 – 15:40

In-Person Session PS4: Intrusion Detection and Threat Mitigation

Room: J. Harper Kent Auditorium

Chair: Hossein Shokouhinejad

- **Paper ID 74**: Cyber Threat Mitigation with Knowledge-Infused Reinforcement Learning and LLM-Guided Policies
  Authors: Md. Shamim Towhid, Shahrear Iqbal, Euclides Neto, Nashid Shahriar, Scott Buffett, Madeena Sultana, Adrian Taylor
- **Paper ID 78**: On Feature Selection for Botnet Detection using Adaptive Exploration in Binary Particle Swarm Optimization Algorithm
  Authors: Syed Tehjeebuzzaman, Mustafa Siam-Ur-Rafique, Ashikur Rahman, Abderrahmane Leshob, Raqeebir Rab
- **Paper ID 111**: Exploring the Impact of Feature Selection on Non-Stationary Intrusion Detection Models in IoT Networks
  Authors: Muaan Ur Rehman, Hayretdin Bahsi, Rajesh Kalakoti
- **Paper ID 121**: Semantic and Graph-Based Unsupervised Learning for Insider Threat Detection Using User Activity Sequences
  Authors: Neda Moghadam, Christopher Neal, Sara Imene.Boucetta, Frederic Cuppens, Nora Boulahia-Cuppens

27 AUGUST 2025, 14:00 – 15:40

Online Session OS2: Privacy and Data Protection

Room: Chancellor’s Room

Chair: Mohammad Jafari Dehkordi

- **Paper ID 15**: A Model-Agnostic Framework for Privacy Risk Assessment of Machine Learning Models
  Authors: Le Wang, Sonal Allana, Xiaowei Sun, Liang Xue, Xiaodong Lin, Rozita Dara, Pulei Xiong
- **Paper ID 60**: Balancing Trade-offs: Adaptive Differential Privacy in Interpretable Machine Learning Models
  Authors: Farhin Farhad Riya, Shahinul Hoque, Yingyuan Yang, Jinyuan Sun, Olivera Kotevska
- **Paper ID 112**: Analysis of User-Generated Content to Unfold Privacy Concerns with CBDCs
  Authors: Arshpreet Singh, Mohamad Sadegh Sangari, Atefeh Mashatan
- **Paper ID 117**: DEDALUS & ICARUS: Image Privacy Classification Systems with Risk Oriented Explanations
  Authors: Hugo Rocha De Alba, Esma Aïmeur, Mohamed Loutis, Khulud Alqahtani
- **Paper ID 140**: A Longitudinal Look at GDPR Compliance
  Authors: Brian Kim, Yang Cao, K. Suzanne Barber

27 AUGUST 2025, 16:10 – 17:30

Online Session OS3

Room: Chancellor's Room

Chair: Mahdi Rabbani

- **Paper ID 94**: Beyond SSO: Mobile Money Authentication for Inclusive e-Government in Sub-Saharan Africa
  Authors: Oluwole Adewusi, Wallace Msagusa, Jean Pierre Imanirumva, Okemawo Obadofin, Jema Ndibwile
- **Paper ID 155**: Assessing Privacy Practices on Ontario Municipal Websites
  Authors: Adegboola David Adelabu, Yan Yan, Wenjing Zhang, Sampa Rauti, Ville Leppänen, Zuhaibuddin Bhutto, Wenthorpe
- **Paper ID 57**: Per-Attribute Privacy in Large Language Models Using Matrix-Variate Gaussian Mechanism
  Authors: Islam Monir, Gabriel Ghinita
- **Paper ID 61**: Trust-Aware Federated Defense Against Data Poisoning in ML-Driven IDS For CAVs
  Authors: Mahsa Tavasoli, Abdolhossein Sarrafzadeh penalizing, Ali Karimoddini, Milad Khaleghi, Tienake Phuapaiboon, Amauri Goines, Aiden Harris, Jason Griffith
- **Paper ID 120**: Probing AlphaFold's Input Attack Surface via Red-Teaming
  Authors: Tia Pope, Ahmad Patooghy
- **Paper ID 46**: Dynamic Decentralized Social Trust for Financial Inclusion with Regulatory Compliance
  Authors: Suzana Moreno, Alessandro Aldini, Seigneur Jean-Marc, Paul-Antoine Bisgambiglia

28 AUGUST 2025

28 AUGUST 2025, 10:15 – 11:55

In-Person Session PS5: Authentication and Trust Mechanisms

Room: Aitken Room

Chair: Vikas Chouhan

- **Paper ID 79**: "A Dynamic, Context-Aware Trust Model for Distributed Computing Environments"
  Authors: Divya Bansal, Sabrina Dhalla, Jaspal Kaur Saini
- **Paper ID 129**: Stateless Decentralized Authentication Using Segmented ZKPs for Microservices Architectures
  Authors: Vinh Quach, Ram Dantu, Sirisha Talapuru, Apurba Pokharel, Shakila Zaman
- **Paper ID 139**: Verify All: Establish Bidirectional and Provable Trustworthiness in Microservices Architecture
  Authors: Vinh Quach, Ram Dantu, Sirisha Talapuru, Indravadan Patel, Alexis Blackwell
- **Paper ID 157**: Formal Specification and Verification of Protection in Transit (PIT) Protocol Using UPPAAL
  Authors: Takwa Rhaimi, Hamed Aghayarzadeh, Rakesh Podder, Indrakshi Ray

28 AUGUST 2025, 10:15 – 11:55

In-Person Session PS6: Federated Learning and Privacy Techniques

Room: J. Harper Kent Auditorium

Chair: Mahdi Rabbani

- **Paper ID 10**: Multilingual Phishing Email Detection Using Lightweight Federated Learning
  Authors: Dakota Staples, Hung Cao, Saqib Hakak, Paul Cook
- **Paper ID 24**: Privacy Preservation with Noise in Explainable AI
  Authors: Sonal Allana, Rozita Dara
- **Paper ID 45**: An Efficient and Privacy-Preserving AdaBoost Federated Learning Framework for AiP System
  Authors: Zhuliang Jia, Rongxing Lu, Mohammad Mamun, Suprio Ray
- **Paper ID 65**: SynQP: A Framework and Metrics for Evaluating the Quality and Privacy Risk of Synthetic Data
  Authors: Bing Hu, Yixin Li, Asma Bahamyirou, Helen Chen

28 AUGUST 2025, 10:15 – 11:55

Online Session OS4: Authentication and Access Control

Room: Chancellor's Room

Chair: Mohammad Jafari Dehkordi

- **Paper ID 125**: Short Training Techniques to Enhance Usability of System-Assigned PINs
  Authors: Israt Jui, Amirali Salehi-Abari, Julie Thorpe
- **Paper ID 148**: Securing Multi-Domain Systems: Intelligent ABAC Policy Learning for Cross-Domain Access Control
  Authors: Asmita Biswas, Barsha Mitra, Iqbal Gondal, Qiang Fu

- **Paper ID 153**: Enhancing Visual Speaker Authentication using Dynamic Lip Movement and Meta-Learning
  Authors: Pooja Pathare, Garima Bajwa
- **Paper ID 144**: Detecting Deepfakes using Temporal Consistency of Facial Expression Transitions
  Authors: Renjith Eettickal Chacko, Garima Bajwa
- **Paper ID 53**: Toward a Lexicon for Privacy, Security, and Trust: Analysing Digital Identity in Media using NLP
  Authors: Matthew Comb, Andrew Martin

28 AUGUST 2025, 13:00 – 14:40

In-Person Session PS7: Deception Detection and Fact-Checking

Room: Aitken Room

Chair: Hossein Shokouhinejad

- **Paper ID 37**: FactCellar: An Evidence-based Dataset for Automated Fact-Checking
  Authors: Arbaaz Dharmavaram, Farrukh Bin Rashid, Saqib Hakak
- **Paper ID 38**: An Intelligent Framework for Deceptive Review Detection Using Advanced Trust Vector Modeling
  Authors: Lily Dey, Md Shopon, Marina L Gavrilova
- **Paper ID 88**: From Birthday Cheers to Privacy Fears: Unraveling the Paradox of Social Media Celebrations in Nigeria
  Authors: Victor Yisa, Rita Orji
- **Paper ID 124**: LAID: Lightweight AI-Generated Image Detection in Spatial and Spectral Domains
  Authors: Nicholas Chivaran, Jianbing Ni
- **Paper ID 132**: Comparing Macro and Micro Approaches for Detecting Phishing Where It Spreads
  Authors: Mina Erfan, Paula Branco, Guy-Vincent Jourdan

28 AUGUST 2025, 13:00 – 14:40

In-Person Session PS8: Secure Infrastructure and Access Control

Room: J. Harper Kent Auditorium

Chair: Mohammad Jafari Dehkordi

- **Paper ID 64**: RF-RADS: A Robust Framework for Risk Assessment in Digital Substations
  Authors: Mahdi Abrishami, Kwasi Boakye-Boateng, Hossein Shokouhinejad, Emmanuel Dana Buedi, Kishore Sreedharan, Shabnam Saderi Oskouei
- **Paper ID 76**: Houdini: Benchmarking Container Security Confinement
  Authors: Huzaifa Patel, David Barrera, Anil Somayaji
- **Paper ID 104**: No Safety in Numbers: Traffic Analysis of Sealed-Sender Groups in Signal
  Authors: Eric Brigham, Nicholas Hopper

28 AUGUST 2025, 13:00 – 14:40

Online Session OS5: Cryptographic Methods and Security

Room: Chancellor’s Room

Chair: Vikas Chouhan

- **Paper ID 68**: Quantum Computing Threats to Management and Operational Safeguards of IEC 62351
  Authors: Brian Goncalves, Arash Mahari, Atefeh Mashatan, Reza Arani, Marthe Kassouf
- **Paper ID 82**: A Machine Learning-Based Framework for Assessing Cryptographic Indistinguishability of Lightweight Block Ciphers
  Authors: Jimmy Dani, Kalyan Nakka, Nitesh Saxena
- **Paper ID 87**: Encryption Struggles Persist: When Tech-Savvy Students Face Challenges with PGP in Thunderbird
  Authors: Md Imanul Huq, Ahmed Tanvir Mahdad, Nitesh Saxena
- **Paper ID 119**: GPU-Optimized Piecewise Linear Activations for Efficient and Secure Neural Networks
  Authors: Hiba Guerrouache, Menat Allah Fadoua Slama, Yacine Challal, Karima Benatchba
- **Paper ID 145**: Secret Sharing in 5G-MEC: Applicability for joint Security and Dependability
  Authors: Thilina Pathirana, Ruxandra F. Olimid

28 AUGUST 2025, 15:10 – 16:30

In-Person Session PS9: Network Security and Adversarial Attacks

Room: Aitken Room

Chair: Hossein Shokouhinejad

- **Paper ID 36**: RefPentester: A Knowledge-Informed Self-Reflective Penetration Testing Framework based on Large Language Models
  Authors: Hanzheng Dai, Yuanliang Li, Jun Yan, Zhibo Zhang
- **Paper ID 86**: DNS Profiler: Quantifying User Browsing Risk from DNS Traffic Patterns
  Authors: Mahdi Firoozjaei, Yaser Baseri, Qing Tan
- **Paper ID 48**: FragmentFool: Fragment-based Adversarial Perturbation for Graph Neural Network-based Vulnerability Detection
  Authors: Muhammad Fakhrur Rozi, Tao Ban, Seiichi Ozawa, Hiroaki Inoue, Takeshi Takahashi, Sajaad Dadkah
- **Paper ID 156**: Identifying and Addressing User-level Security Concerns in Smart Homes Using “Smaller” LLMs
  Authors: Hafijul Hoque Chowdhury, Riad Ahmed Anonto, Sourov Jajodia, Suryadipta Majumdar, Md. Shohrab Hossain

28 AUGUST 2025, 15:10 – 16:30

Online Session OS6: Trust and Verification

Room: Chancellor’s Room

Chair: Mahdi Rabbani

- **Paper ID 16**: TrollSleuth: Behavioral and Linguistic Fingerprinting of State-Sponsored Trolls
  Authors: Havva Alizadeh Noughabi, Fattane Zarrinkalam, Abbas Yazdinejad, Ali Dehghantanha
- **Paper ID 71**: Temporal-Spatial Feature Modification Attacks Against Machine Learning-Based Network Intrusion Detection Systems
  Authors: Eeshan Walia, Sohini Pillay, Christopher Yoeurng, Dongfeng Fang, Shengjie Xu
- **Paper ID 80:** G-STAR: A Threat Modeling Framework for General-Purpose AI Systems
  Authors: Pulei Xiong, Saeedeh Lohrasbi, Prini Kotian, Scott Buffett
- **Paper ID 103**: A Modeling and Static Analysis Approach for the Verification of Privacy and Safety Properties in Kotlin Android Apps
  Authors: Bara Nazzal, James Cordy, Manar Alalfi
- **Paper ID 131**: An Integer Programming Framework for ReBAC Policy Mining and Optimized Conformance Testing
  Authors: Padmavathi Iyer
- **Paper ID 122**: Detecting Ransomware Before It Bites: A Hybrid Model Approach for Early Ransomware Detection
  Authors: Sk Mahtab Uddin, Saqib Hakak, Miguel Garzón