2026 Silicon Valley Cybersecurity Conference (SVCC 2026)

San Jose, California, USA
10-12 June 2026

IEEE Catalog Number: CFP26DI5-POD
ISBN: 979-8-3195-0665-8

IEEE
Advancing Technology for Humanity

Copyright © 2026, IEEE

All Rights Reserved

Copyright and Reprint Permissions:

Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

*** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.

IEEE Catalog Number:	CFP26DI5-POD
ISBN (Print-On-Demand):	979-8-3195-0665-8
ISBN (Online):	979-8-3195-0664-1

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA

Phone:	(845) 758-0400
Fax:	(845) 758-2633
E-mail:	curran@proceedings.com
Web:	www.proceedings.com



TABLE OF CONTENTS

Enhancing Anomaly Resilience in Research Networks: A Large-Scale Forecasting Benchmark for Dynamic Security Baselining 1
Mohammad Arafath Uddin Shariff, Byrav Ramamurthy

Reducing Cognitive Load in Packet Analysis: a Plain-Language Translation Framework for Novice Security Analysts 9
Jhaell Jimenez, Yoohwan Kim, Ju-Yeon Jo

Integrating Post-Quantum Cryptography Into a CDN-Style PKI: Design, Trade-Offs, and an Experimental Baseline 19
Katrina Parsom, Yoohwan Kim, Ju-Yeon Jo

Are You Aware of Shadow Ai? Governai for Addressing Emerging Risks 27
Syed Huzaifa Bin Afzal, Justin Bowman, Yu-Tien Renee Chian, Ayush Singh, Wenjun Fan

Evaluating Website Fingerprinting Resistance Under VPN Tunneling 35
Mohammed Ameenuddin Farooqui, Joshua Honig, Mohammed Abuhamad, Eric Chan-Tin

IoT-CyberAgent: An Intelligent Multi-Agent Cyber Threat Detection and Response System for IoT Networks 42
Potri Abhisri Barama, Michelle Kim, Younghee Park

Secure Smart Home: Federated Learning with LLM-Based Recommendations and Differential Privacy 50
Sadia Asif Malik, Ahsan Altaf, Adeel Anjum, Muazzam A. Khan Khattak, Awais Ahmad Goutham Reddy Alavalapati, Sunshin Lee

Uncovering Weaknesses in Autonomous Driving: A Formal Approach to Adversarial Scenario Generation and Falsification 58
Carlos O. Hernandez, Luis Burbano, Diego Ortiz Barbosa, Alvaro A. Cardenas, Younghee Park

A Study of Large Language Model Performance for Phishing URL Detection and Explainability for User-Centric Security 68
Jaishnoor Kaur, Eugene Vuong, Hongmin Li

PhishLite: A Client-Side Phishing Detection Utilizing URL and Web Content 76
Viona Widodo, Hayato Yamana

Tor for Cryptocurrency: Enhancing Mining Rewards While Preserving Anonymity 84
Nazmus Sakib, Kelei Zhang, Simeon Wuthier, Wenjun Fan, Sang-Yoon Chang

Risk-Driven Secure Software Engineering (RDSSE) 92
Neha Prakash, Madhushree Kumari

Supervised Learning Approaches for Intrusion Detection Systems for Smart Grid Substation Networks 102
Sowmya Bandari, Venkat Sai Suman Lamba Karanam, Byrav Ramamurthy

Evaluating X.509 Certificate Performance of NIST PQC Round 2 Additional Digital Signatures 108
Amrutvyasa Ramasamy, Sanketh Chapaneri, Manohar Raavi

When Accuracy Is Not Enough: Evaluating Explainable Vulnerability Detection Beyond Accuracy 113
Fabion Walden, Mengjun Xie

Prompt-Language Leakage from LLM-Generated Data via Membership Inference on Downstream LSTMs 123
Kevin Jin, Amith Kamath Belman

A Tsetlin Machine-Driven Intrusion Detection System for Next-Generation IoMT Security 131
Rahul Jaiswal, Per-Arne Andersen, Linga Reddy Cenkeramaddi, Lei Jiao, Ole-Christoffer Granmo

Hybrid Quantum-Classical Layer-7 Traffic Classification: Methodology and Evaluation 139
Simone Mainardi, Kaushal Bansal, Prabhat Singh

Enhancing Cybersecurity Incident Response Efficiency Through Autonomous Agentic AI: Design, Implementation, and Evaluation with Wazuh SIEM 147
Mohamad Nour Shahin, Ruslan Damindarov

DAP-L: A Database-Agnostic, Identity-Preserving Streaming Protocol for LLM Agents 154
Chiranjeevisantosh Madugundi, Sabitha Muppuri, Manjunath Mitikiri

Enhancing Automotive Intrusion Detection: A Generalized Feature Engineering Pipeline for Diverse Architectures 159
Adam Mejia, Ashutosh Mane, Kristina Bathan, Younghee Park

MALCDF: A Distributed Multi-Agent LLM Framework for Cyber Defense 165
Arth Bhardwaj, Sia Godika, Yuvam Loonker

Security Analysis of Distributed Virtual Reality and Physiological Sensor (VR-PHY) Systems 172
Rashmi Elavazhagan, Taanish Alam, Lea Christy Y. Wiranatha, Yen H. Nguyen, Abdullah Siddiqui Amir M. B. Khan, Nathan Lee, Mohammad Husain

A Comparative Analysis of LLMS for BOM Processing 180
Michelle Buslon, Sean Breckling, Yoohwan Kim, Ju-Yeon Jo

A Comparative Analysis of Global AI Safety Perspectives: Toward an Integrated Cybersecurity-Oriented AI Safety Framework 188
Young B. Choi, Paul C. Hong

Poster: DART - Data Augmentation of Rare ATT&CK Techniques Using LLM Agents 191
Taya Ambrose, Sergio Valderrama, Álvaro Cárdenas, Younghee Park

Poster: The IPv6 Blind Spot: Security Assessment of Dual-Stack VPN Vulnerabilities 194
Jeevan Reji, Sanjith Velusamy

Poster: The UNICORN Framework: A Multi-Dimensional Methodology for Evaluating Guardrail Robustness in Enterprise Large Language Model Assistants 197
Rupinder Pal Singh

Poster: Exploring the Minimization of Perturbations in Adversarial Example Generation Against ML-Based NIDS 201
Christopher Yoeurng, Aras Janusonis, Jason Jelincic, Dongfeng Fang

Usability and Trust in Cloud Encryption: Experimental Evaluation of AWS and Related Cloud Platforms 204
Aahana Sharma, Antoine Si, Mohammad Iftekhar Husain

Poster: Rethinking Intrusion Detection Evaluation: The Impact of Cross-Scenario Leakage 208
Zahra Ghausi, Nina Tkachuk, Kevin Davood, Bryant Hipolito, Esteban Verdin, Kaiman Zeng

Poster: From Assistants to Actors: Deconstructing the Security Implications of Autonomous AI Agents 211
Akanksha Pathak

POSTER: Fine-Tuning Large Language Models via Reinforcement Learning with Verifiable Rewards for Congestion Control 215
Shanaya Varkey, Shaunak Galvankar, Sean Choi

Least Significant Bit Steganography Detection and Analysis Using Large Language Models for Digital Forensics 218
Arjun Sudheer, Jason Kim, Younghee Park

Poster: Towards Transparent NIDS: An xLSTM-Based Explainable Architecture 221
Aayush Joshi, Dongfeng Fang

Next-Generation Cloud Security: A Bibliometric and Technical Analysis of Machine Learning and Deep Learning Approaches 224
Natasha Saini

Designing Secure Generative AI for Global Supply Chains Governance-by-Design for Trustworthy Deployment 227
Paul C. Hong, Young B. Choi, David W. Hwang

Enhancing Implicit Neural Representation-Based Steganography Using Adaptive Perturbation and Adversarial Training 229
Kanza Fatima, Nan-I Wu, Cheng-Ying Yang, Min-Shinag Hwang, Chenyi Yang

Poster: Reinforcement Learning-Based Strategies for Improving CAPTCHAs 232
Meghana Indukuri, Eman Naseerkhan, Joshua Rose, Martin Tran, Younghee Park

Poster: A Lightweight and Scalable Python Framework for Early Anomaly Detection in Security Event Logs 235
Gulnara Chunareva

Autonomous Detection Engineering: From Threat Research to Detection Authoring 238
Fatih Bulut, Anjali Mangal

One Engine to Rule Them All 239
Akshay Pratinav, Chaitanya Bhatt

Using Identity Data to Reduce Security Risk 240
Neha Prakash

When AI Agents Fail in Production: Security Lessons for Builders 241
Venkata Sai Kishore Modalavalasa

Identity-Centric AI: Detecting Lateral Movement Through Risk-Aware Identity Graphs 242
Krupa Pratap Brahmkstri