2026 IEEE 12th Conference on Big Data Security on Cloud (BigDataSecurity 2026)

New York City, New York, USA
8-10 May 2026

IEEE Catalog Number: CFP26E88-POD
ISBN: 979-8-3195-3237-4

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:	CFP26E88-POD
ISBN (Print-On-Demand):	979-8-3195-3237-4
ISBN (Online):	979-8-3195-3236-7

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

A Four-Axis Systematization of AI and Cybersecurity in the Era of Large Language Models 1
Mashiat Amin Farin, Bhavani Thuraisingham

Deep Continual Learning: Survey of Method and Application 13
Yigong Wang, Zhuoyi Wang, Mufan Sang, Bhavani Thuraisingham, Latifur Khan

AI for Cyber and Cyber for AI: How AI and Cyber Benefit Each Other 24
Bhavani Thuraisingham

Semantic Policy Regulation Mapping for IoT Cybersecurity Compliance 34
Silambarasan Palanisamy, Lavanya Elluri, Meenakshi Dakuru, Gunjan Batra

Architectural Security Risks in Edge-Assisted LoRaWAN Data Pipelines 42
Sheikh Tareq Ahmed, Josemaria Chukwuemeka Osuorah, Annamalai Annamalai, Toya Acharya

TinyML Enabled Passwordless Web Authentication Using On-Device Biometric Inference on Resource Constrained Hardware 48
Yogeswar Reddy Thota, Jay Kamleshbhai Pandya

Query-Based Fingerprinting of Text-to-Image Large Language Models 54
Saketh Ram Josyabhatla, Junggab Son, Daeyoung Kim

Secured Prediction: Password Guessability Analysis Using Gradient Boosting Machines 60
Shivani Pakala, Junggab Son, Daeyoung Kim

A Stability Testing Framework for Machine Learning in Honeypot Traffic Classification 66
Nayam Ahmed, Kamran Uddin, Junggab Son, Daeyoung Kim

Policy-Driven Federated Big Data Analytics with Verifiable Privacy Guarantees in Multi-Cloud Environments 72
Varun Raj

Adaptive Provenance Control: Control-Plane-Driven Security for Big Data Pipelines in Elastic Cloud Environments 78
Varun Raj

Control-Plane-Mediated Defense Against Data Poisoning in Large-Scale Distributed Learning Systems 84
Varun Raj

TRACE: Tamper-Resistant Accountability and Cryptographic Evidence for Multi-Agent AI Systems 90
Bharathwaj Vijayakumar, Sahana Karamutti Varadaraju, Lathish Balaji Baskaran

A Systematic Evaluation of Recurrent Architectures for Binary Solar Flare Prediction from Multivariate Time Series 96
Syed Abrab Mahmood, Ruizhe Ma

An AE-GNN-Based Clinical Decision Support System for Multi-View ERCP Pathological Classification 104
XiaoGuang Wang, Meng Wan, Rongqiang Cao, Fang Liu, Jianjiang Li

High-Performance Implementation of Crystals-Dilithium using DSP-Free NTTs on FPGA 112
Junxin Chen, Jianning Pan, Chen Chen, Hua Guo, Bo Li, Wenmao Liu, Xiyong Zhang

FASTI: Fast and Accurate Secure Transformer Inference 119
Zirui Gong, Hua Guo, Jiarong Huo, Weixin Liu, Yong Ma

Virtual Reorganization with Partition Synopses for Dynamic Trajectory Partition Optimization 126
Wentao Guan, Min Chen

SYNAPSE: Privacy-Constrained Diagnosis-Aware Exercise Recommendation with Synthetic Data 132
Chunyu Guo, Xuezheng Liu, Miao Hu, Di Wu, Chuxuan Zeng, Liang Du

Energy-Aware Scheduling Algorithm Based on Weighted Energy Pre-allocation 138
Yanghao Yu

An Efficient Proof-of-Learning Framework for Distributed and Secure Blockchains 145
Weihang Cao, Mustafa Doger, Sennur Ulukus

AI-Driven Zero-Trust Access Enforcement in Poly-Cloud Ecosystems 151
Venumadhav Venkata Kalluru

Zero Trust Data Engineering: A Reference Architecture for Serverless, FedRAMP-High Healthcare Pipelines 157
Tristan McKinnon

Quantum-Enhanced Secure Data Handling: A Hybrid Architecture with BB84-Based Encryption and Cloud-Native Orchestration 160
Anibal Calle-Zuniga, Jorge Freire-Tamayo, Jonathan Pibaque-Ponce, Kevin Atauchi-Dominguez Ricardo Cajo, Washington Velasquez

Urban Travel Hotspot Identification Based on Multi-Density Adaptive Trajectory Clustering 166
Huan Liu, Min Chen

A Hardware–Software Co-Design Optimization Framework for Edge-Oriented DETR-Based Object Detection 172
Xianglong Zeng, Qiming Zhao, Ningyuan Yu, Wei Hu

TGN-GCL: Enabling Temporal Contrastive Learning with Dynamic Task Graphs for Accurate Evaluation of Network-on-Chips Performance 178
Linying Wu, Jihe Wang, Jinshuai Wei, Zhiyu Sun, Yuanhua Xiao, Danghui Wang