Secure and Trustworthy Cyberinfrastructure for IoT and Microelectronics (SaTC 2026)

IEEE Houston Section

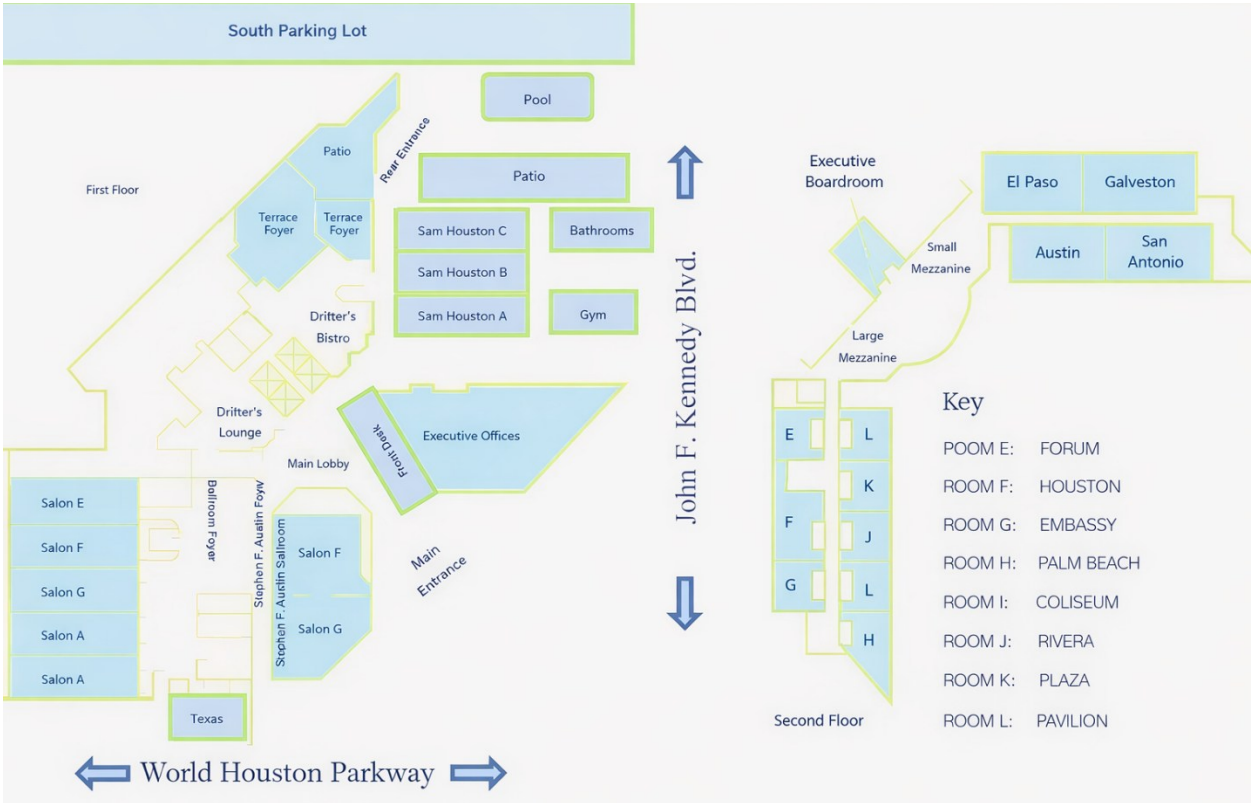
IEEE DAYTON

CONTENTS

Detailed Agendas	Page(s)
Day 1: Tuesday (March 24)	10 – 33
Day 2: Wednesday (March 25)	34 – 54
Day 1 (online): Tuesday (March 24)	56 – 69
Day 2 (online): Wednesday (March 25)	70 – 83
Day 3 (online only): Thursday (March 26)	84 - 97

Conference Link: https://www.satcconf.com
Registration Link: https://www.satcconf.com/author.html#registration

Venue Floor Plan



CHAIR'S MESSAGE

Welcome to the 2nd IEEE Conference on Secure and Trustworthy Cyberinfrastructure for IoT and Microelectronics

SaTC 2026

It is with great pleasure that I welcome you to the second IEEE Conference on Secure and Trustworthy Cyberinfrastructure for IoT and Microelectronics (SaTC 2026) here in Housten, Texas. As we witness the rapid evolution of these transformative technologies, ensuring their security and integrity is of paramount importance. This conference serves as an invaluable forum for the exchange of pioneering ideas, critical challenges, and collaborative exploration aimed at strengthening the cyberinfrastructure that supports IoT and microelectronics. I encourage everyone to immerse yourself in the sessions, explore novel ideas, share your insights, and contribute to shaping the future of secure, resilient systems. I extend my sincere gratitude for your participation and eagerly anticipate the profound discussions that will unveil the forthcoming breakthroughs in our field.

Warm regards,
Fathi Amsaad, General Chair

SPONSORS/SUPPORT

Industry Partners

Academic Partners

Speakers from Academia, Industry and Government.


GRAND VALLEY
STATE UNIVERSITY


THE OHIO STATE
UNIVERSITY


DEARBORN


LSU
LOUISIANA STATE UNIVERSITY


VCU


EASTERN
MICHIGAN UNIVERSITY

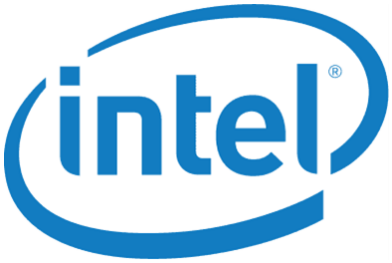

TAYLOR'S
UNIVERSITY
Wisdom · Integrity · Excellence


RICKERT
ARENO
ENGINEERING


Sandia
National
Laboratories


semi


Meta


intel


CYBERPRO
GLOBAL


RIVERSIDE RESEARCH


IEEE
Houston Section


amazon
web services


AFIT
Air Force Institute of Technology


1804
OHIO
UNIVERSITY


Research


FIU
FLORIDA
INTERNATIONAL
UNIVERSITY


NM
STATE
UNIVERSITY


MTSU
MIDDLE TENNESSEE STATE UNIVERSITY.


KU
THE UNIVERSITY OF
KANSAS


WILBERFORCE
UNIVERSITY


1848
THE UNIVERSITY of
MISSISSIPPI


Southern
Illinois
University
CARBONDALE


OHIO
NORTHERN
UNIVERSITY


EMBRY-RIDDLE
Aeronautical University
DAYTONA BEACH, FLORIDA


TEXAS TECH
UNIVERSITY


UT
THE UNIVERSITY OF
TOLEDO


WESTERN NEW ENGLAND
UNIVERSITY
WNE


PRAIRIE VIEW A&M UNIVERSITY
TEACHING
RESEARCH
SERVICE
PVAMU
1876

Opening Keynote

Day 1 - Tuesday March 24, 2026

08:30 AM – 09:10 AM

Plenary Session I
Opening Keynote

The Future of Semiconductor Innovation: GenAI in Design and Security

Session Chair:

Dr. Akshay Kulkarni, Prairie View A&M University

Presenter/Speaker:

Dr. Mark M. Tehranipoor, University of Florida

Abstract: Designing functionally correct, high-performance, and provably secure system-on-chips (SoCs) has become a strategic imperative for modern computing infrastructure. However, escalating complexity, heterogeneous integration, and evolving security threats are pushing traditional design and verification methodologies beyond their practical limits. The emergence of large language models (LLMs) offers a transformative opportunity for SoC automation. Beyond code generation, LLMs enable architectural reasoning, specification refinement, vulnerability analysis, and design-space exploration. Yet chip design is inherently multidisciplinary and iterative, requiring more than a single monolithic model. An agentic paradigm-where specialized AI agents collaborate within a coordinated framework-enables modular reasoning, cross-layer verification, and adaptive security validation across the SoC lifecycle. This keynote introduces a multi-agent intelligent assistant system designed to automate and augment SoC design and security verification. By integrating synthesis, threat modeling, formal reasoning, runtime monitoring, and hardware-software co-verification, this framework moves us toward self-optimizing, security-aware, and continuously verified silicon-redefining how next-generation microelectronic systems are conceived, built, and trusted.

Speaker Bio: Mark M. Tehranipoor is the Distinguished Professor, Intel Charles E. Young Preeminence Endowed Chair Professor, and Sachio Semmoto Chair in the Department of Electrical and Computer Engineering at the University of Florida. His research spans GenAI security, hardware security and trust, supply chain security, IoT security, and VLSI design, test, and reliability. He holds 50+ issued/pending patents and has authored 20 books and 700+ conference and journal publications. His honors include 25 best paper awards and nominations, the NSF CAREER Award, the AFOSR MURI Award, the IEEE Computer Society Meritorious Service Award, Outstanding Contribution Award, TTTC Bob Madge Innovation Award, and the 2026 Taylor Booth Education Award. He also received the University of Florida Innovation of the Year and teacher/scholar of the year awards. He co-founded IEEE HOST, IEEE AsianHOST, and PAINE, and has served in major leadership roles for numerous IEEE and ACM conferences. He is a founding co-Editor-in-Chief of the Journal on Hardware and Systems Security and has served as editor or associate editor for several leading journals. Dr. Tehranipoor also served as a founding director of the Florida Institute for Cybersecurity Research and other centers focused on microelectronics security. He is a Fellow of the IEEE, ACM, National Academy of Inventors, AAIA, AIIA, and ASEMFL, a Golden Core Member of the IEEE Computer Society, and a member of ACM SIGDA.

Invited Talks

Day 1 - Tuesday March 24, 2026

09:10 AM – 09:30 AM

Plenary Session I

Invited Talk

VERIFY-CPS: Validation and Evaluation for Resilient and Integrity-Focused Cyber-Physical Systems

Session Chair:
Dr. Akshay Kulkarni, Prairie View A&M University

Presenter/Speaker:
Dr. Darryl K. Ahner, Professor and Dean of College of Engineering and Computer Science, Wright State University

Abstract: As defense and critical infrastructure systems increasingly integrate cyber, physical, and autonomous components, ensuring these systems are trusted, resilient, and mission-ready requires rigorous test, evaluation, and validation (TEVV) methodologies. Traditional testing approaches are insufficient for cyber-physical systems operating under uncertainty, adaptive threats, and dynamic operational conditions. This talk focuses on the role of testbeds, operational experimentation, and data-driven evaluation frameworks in assessing the performance, reliability, and cyber resilience of trusted cyber-physical systems. Drawing on experience across Department of Defense test and evaluation organizations and academic research environments, it highlights how stochastic modeling, simulation, and analytics can be used to characterize system behavior, quantify risk, and validate performance across realistic mission scenarios. The presentation emphasizes the importance of integrated test architectures that combine cyber testing, physical system evaluation, and operational validation to support trusted autonomy and mission assurance in contested environments.

Speaker Bio: Darryl K. Ahner, Ph.D. is the Dean of the College of Engineering and Computer Science at Wright State University, a role he assumed in July 2023. Prior to joining Wright State, he served as Dean for Research at the Air Force Institute of Technology (AFIT) at Wright-Patterson Air Force Base, where he led the Office of Research and Sponsored Programs and managed a $36 million research portfolio. Dr. Ahner is a professor of stochastic operations research and has held senior leadership roles across defense and academic institutions, including Director of the Office of the Secretary of Defense Scientific Test and Analysis Techniques within the Test and Evaluation Center of Excellence, Director of the Center for Operational Analysis, faculty member at the U.S. Military Academy at West Point, and Director of Research at the U.S. Army Research Center at the Naval Postgraduate School. In 2021, he received the Secretary of Defense Medal for Exceptional Civilian Service for his contributions to workforce development and national security research. His research focuses on test and evaluation optimization, autonomous and cyber-physical systems, reliability, stochastic modeling, simulation, and defense analytics. He has authored many peer-reviewed journal articles, conference proceedings, and several book chapters. He earned a B.S. in Mechanical Engineering (Aerospace) from the U.S. Military Academy at West Point, served 22 years in the U.S. Army, and holds a Ph.D. in Systems Engineering from Boston University, along with advanced degrees from Rensselaer Polytechnic Institute and a graduate certificate from AFIT.

Invited Talks

Day 1 - Tuesday March 24, 2026

09:30 AM – 09:50 AM

Plenary Session I

Invited Talk

Embedded and Hardware-Centric Cybersecurity: Trust, Vulnerabilities, and National Security Applications

Session Chair:

Dr. Akshay Kulkarni, Prairie View A&M University

Presenter/Speaker:

Dr. Paul Simon, Senior Cyber Security Research Engineer, Riverside Research

Abstract: As embedded systems and hardware platforms increasingly underpin mission-critical defense, aerospace, and consumer technologies, cybersecurity must extend beyond software protections to address vulnerabilities at the hardware layer. This talk will explore emerging threats and assurance challenges in embedded and hardware-focused security, drawing from experience across government, defense, and commercial sectors. The presentation will examine practical methodologies for cyber vulnerability assessment of weapon systems and embedded devices, microelectronics trust and assurance validation, and hardware-centric attack surfaces, including reverse engineering and system-level exploitation. Emphasis will be placed on real-world security validation strategies and lessons learned from both defense research environments and large-scale commercial device security programs. By connecting applied research, national security applications, and hardware system design considerations, this talk highlights the evolving landscape of hardware-rooted cybersecurity risks and the need for integrated assurance approaches across the system lifecycle.

Speaker Bio: Dr. Paul Simon is a Senior Cyber Security Research Engineer at Riverside Research in Dayton, Ohio, where he conducts advanced cybersecurity research with an emphasis on embedded systems and hardware-focused security. His work centers on microelectronics trust, system assurance, vulnerability analysis, and secure hardware design for high-consequence and mission-critical systems. Prior to joining Riverside Research in 2025, Dr. Simon served as a Senior Hardware Security Engineer at Amazon (Device & Services Security), where he was part of a specialized team focused on securing consumer devices and services at scale. Before Amazon, Dr. Simon supported multiple government and defense-related programs in and around the Air Force Institute of Technology (AFIT) and the Air Force Research Laboratory (AFRL) through roles at HII Technical Solutions and Applied Research Solutions. His work included cyber vulnerability assessments of weapon systems, microelectronics trust and assurance validation, reverse engineering, hardware system design, and cybersecurity research for embedded devices. Dr. Simon earned his Bachelor of Science (1997) and Master of Science (2011) degrees in Electrical Engineering from the University of Dayton. He received his Ph.D. in Electrical Engineering from the Air Force Institute of Technology (AFIT) in 2022. He has been a member of IEEE for over 15 years.

09:50 AM – 10:10 AM	**Coffee Break & Networking Opportunity**

Keynote Presentation

Day 1 - Tuesday March 24, 2026

10:10 AM – 10:40

Plenary Session II

Keynote Presentation

Thrusting the Quantum Computer: Security Threats from Side-channel Leakage to PUFs and Trojans

Session Chair:
Dr. Bayley King, Riverside Research

Presenter/Speaker:
Dr. Selçuk Köse, University of Rochester

Abstract: Superconducting digital electronics provide the classical control and readout infrastructure for many quantum computing platforms, operating in close proximity to superconducting qubits at cryogenic temperatures. This talk will begin with an overview of superconducting digital logic and the physical realization of superconducting qubits, establishing the hardware foundations of contemporary quantum computing systems. After reviewing key operating principles, the focus will shift to the interface circuits that connect superconducting digital controllers to qubit and readout subsystems. These interface circuits define critical security boundaries by translating ultrafast superconducting signals into accessible electrical quantities. The talk will examine side-channel leakage mechanisms arising from superconducting digital control and interface circuitry, followed by a discussion of hardware Trojans that may be embedded within the digital control and readout stack. Recent work on physical unclonable functions (PUFs) implemented in superconducting digital control circuits will also be presented as a hardware-rooted approach to device identification and authentication. Looking ahead, this talk argues that hardware trust must be treated as a fundamental design requirement in superconducting quantum computing systems. As these platforms scale, security considerations will increasingly influence the co-design of qubits, superconducting digital logic, and interface circuits, shaping how reliable and trustworthy quantum computers are ultimately built.

Speaker Bio: Dr. Selçuk Köse received his PhD degree in Electrical and Computer Engineering from the University of Rochester in 2012. After spending nearly seven years at the University of South Florida (USF), he joined the Department of Electrical and Computer Engineering at the University of Rochester where he is currently a Professor. He previously worked at TUBITAK, NXP semiconductor, Intel corporation, and Eastman Kodak. Dr. Köse is a recipient of the NSF CAREER award (2014), USF College of Engineering Outstanding Junior Research Achievement Award (2014), USF Outstanding Faculty Award (2016), Cisco Research Award (2015, 2016, and 2017) and USF Outstanding Research Achievement Award (2017). His research interests include VLSI circuit design, hardware security, cryogenic electronics, and quantum computing. His research has been funded by NSF, DARPA, Department of Energy, SRC, Cisco, Intel, and TSMC.

Invited Talk

Day 1 - Tuesday March 24, 2026

10:40 AM – 11:00 AM

Plenary Session II
Invited Talk

AI in Cybersecurity
Session Chair:
Dr. Bayley King, Riverside Research

Presenter/Speaker:
Dr. Thangaraj Petchiappan, Vice Chair, IEEE Houston Section / CTO, SIMS-iLink Digital

Abstract: AI continues to reshape how businesses operate, it is also transforming the threat landscape just as rapidly. The future of cybersecurity lies in anticipation, automation, and resilience, where human judgment and AI-driven intelligence work together to stay ahead of evolving risks.

Speaker Bio: Thangaraj Petchiappan Chief Technology Officer at SIMS-iLink Digital, has helped many Fortune 500 clients and industries innovate and transform for the digital future. He is dedicated to enhancing infrastructure automation and integrating advanced cybersecurity solutions, continually driving improvements in platforms and processes. He plays a pivotal role in leading the development of innovative solutions that demonstrate the potential of new and emerging technologies such as AI and ML. Thangaraj mentors team members, advises them on how to apply AI in Cybersecurity based on real-world experience, and helps them grow professionally by improving their skills. Thangaraj and his team are at the forefront of innovation in cybersecurity, creating cutting-edge solutions that use AI to combat cyber threats. They harness the power of natural language processing, computer vision, deep learning, and graph analytics to build tools for phishing detection, malware analysis, threat intelligence, and network security monitoring.

Terrace

Keynote Presentation

Day 1 - Tuesday March 24, 2026

11:00 AM – 11:30 AM

Plenary Session II
Keynote Presentation

AI and Edge Computing: Emerging Security Challenges in the New Era

Session Chair:

Dr. Bayley King, Riverside Research

Presenter/Speaker:

Dr. Sandip Ray, Warren B. Nelms Endowed Professor, University of Florida

Abstract: The Internet of Things (IoT) era began roughly a decade ago, when the number of smart, connected devices surpassed the global human population. Today, billions of such systems interact across applications of unprecedented scale and diversity, including smart homes, biomedical devices, autonomous vehicles, and smart cities. This growth is expected to accelerate into the trillions over the coming decade, making IoT one of the fastest-growing technological sectors in history. At this scale, ensuring that these systems operate safely, reliably, securely, and as intended is critical to modern life. Yet traditional approaches to system architecture and design are often insufficient for the demands of the IoT era. Key challenges arise from the complex interplay among reliability, energy efficiency, security, software enablement, validation, in-field configurability, and other design constraints. Addressing these issues requires fundamentally new, cross-disciplinary approaches spanning computer architecture, hardware/software co-design, verification, and machine learning, while also drawing from fields such as mechanical engineering, biomedical engineering, and device physics. This talk will examine the architectural and design challenges involved in enabling efficient, reliable, and trustworthy computing in the IoT regime. It will further highlight a major shift in computing paradigms: the movement from owned and cloud-based infrastructure toward edge computing, where AI is increasingly deployed on highly personalized and intimate data. Particular attention will be given to safety and security challenges in edge AI accelerators, including emerging vulnerabilities introduced by this transition, along with recent results in both offensive and defensive security.

Speaker Bio: Dr. Sandip Ray is the Warren B. Nelms Endowed Professor in the Department of Electrical and Computer Engineering at the University of Florida. His research focuses on correct, dependable, secure, and trustworthy computing, spanning specification, synthesis, architecture, and validation, with applications in IoT, autonomous vehicles, smart homes, and intelligent implants. Before joining UF, he was a Senior Principal Engineer at NXP Semiconductors, leading R&D on security architecture and validation for automotive and IoT hardware platforms, and previously a Research Scientist at Intel Strategic CAD Labs, where he led research on validation technologies, design-for-security, and design-for-debug for SoC designs. His work has also influenced companies such as AMD, Galois, IBM, Microsoft, and Collins. Dr. Ray is the author of three books and more than 120 publications, and has delivered over 60 invited and keynote talks. He has served in major leadership roles across numerous international conferences, including as program committee member, track chair, and program chair, and has contributed as guest editor and associate editor for several leading journals. He earned his Ph.D. from the University of Texas at Austin and is a Senior Member of IEEE.

Terrace

Luncheon Keynote

Day 1 - Tuesday March 24, 2026

11:45 AM – 12:15 PM

Luncheon Keynote

Keynote Presentation

Building Translational Innovation Ecosystems: From Discovery to Real World Impact

Session Chair:

Dr. Osama Fakron, Purdue University Fort Wayne

Presenter/Speaker:

Dr. Samir Iqbal, Associate Dean of Research, Grand Valley State University

Abstract: Translating research discoveries into real world impact requires intentional ecosystems that connect invention, innovation, and implementation. As technology advances rapidly across disciplines, academic, industry, and community partners must work collaboratively to ensure that emerging knowledge is transformed into solutions that address societal, economic, and workforce challenges. This keynote explores strategies for strengthening translational research pipelines by focusing on partnership formation, proposal competitiveness, and structured commercialization pathways that support sustainable innovation. Drawing from experience managing national funding programs that advance applied research and entrepreneurial science, this presentation will highlight approaches for bridging the gap between foundational research and deployment ready technology. Special attention will be given to test bed models, collaborative networks, and funding mechanisms that enable researchers and innovators to move ideas from concept to application. The session is intended to benefit academic and professional audiences by providing insights into building multidisciplinary partnerships, strengthening translational research capacity, and enhancing the broader societal and economic value of scientific and technological advances.

Speaker Bio: Dr. Samir Iqbal is a researcher in nanotechnology, biosensing, and biomedical image analytics. He served as one of the founding Program Directors of the NSF Technology, Innovation, and Partnerships (TIP) Directorate, which focuses on advancing use inspired research, innovation ecosystems, workforce development, and pathways that connect academic discovery to societal impact. He earned his PhD from Purdue University.

11:30 AM – 13:00 PM	**Lunch Buffet Open & Networking Opportunity**

Day 1 - Tuesday March 24, 2026

PANEL DISCUSSION 13:00 PM – 14:15

Industry & National Lab Research Panel: Advances and Challenges in Trusted Microelectronics, IT/OT, Side-Channel, and Digital Assurance for Secure Systems Engineering

MODERATOR:	Dr. Matthew Areno (CTO, Rickert-Areno Engineering, LLC Co-Chair for the Secure Edge/IoT working group, MMEC)
This panel explores the latest developments in trusted microelectronics, cybersecurity for critical systems engineering, IT/OT integration, side-channel vulnerabilities, and digital assurance. The discussion will highlight strategies for protecting critical infrastructure in the Department of Defense, the Air Force, and industry. Panelists will address emerging threats, mitigation techniques, and practical applications in IoT and microelectronic systems, emphasizing reliability, trust, and security in high-risk environments.	

Panelists:

Dr. Bayley King (Riverside Research)

Panelist Bio: Dr. Bayley King is a Senior Research Scientist at Riverside Research, where he works at the intersection of hardware security, embedded systems, and data science, supporting national security-focused research and development. He works as a capture manager, principal investigator and program manager for Microelectronic strategy and technology development. He currently serves as an Adjunct Professor in the Department of Computer Science and Engineering at Wright State University and is also an Adjunct Professor of Computer Science at the University of Dayton. Prior to joining Riverside Research, Dr. King completed his Ph.D. in Computer Science and Engineering at the University of Cincinnati, where he conducted research in machine learning and security-focused computing for the Air Force Research Lab. His work spans hardware assurance, secure embedded systems, and applied AI, with publications including research on securing third-party HDL IP and security-related data-driven methods.

Dr. William (Will) Zortman (Sandia National Laboratory)

Panelist Bio: William (Will) Zortman is the Digital Assurance for High Consequence Systems (DAHCS) Campaign Manager for Sandia National Laboratories' Laboratory Directed Research and Development Office. The DAHCS Mission Campaign is fundamental and developmental research focused on integrating digital assurance into the discipline of systems engineering so that systems engineers, program managers and risk acceptors can make engineering trade-offs between digital risk and other system risks.

Dr. Darren Pulsipher (Intel)

Panelist Bio: Darren Pulsipher is the Chief Enterprise Architect for Public Sector at Intel, where he focuses on secure digital transformation across government, critical infrastructure, and mission-critical environments. He is also the Chairman of the Open Digital Transformation Forum at The Open Group, where he leads global efforts to advance architecture-driven approaches to digital transformation, governance, and cybersecurity. Dr. Pulsipher's work centers on the secure convergence of Information Technology (IT) and Operational Technology (OT) systems. He specializes in addressing architectural, cultural, and governance challenges created by misaligned taxonomies, competing operational drivers such as uptime, safety, and security, and long-standing organizational separation between IT and OT domains. His research and practice emphasize treating cybersecurity as an architectural discipline, applying People, Process, and Technology principles—grounded in the GEAR model—to enable resilient convergence while preserving the operational individuality required in cyber-physical systems.

Dr. Paul Simon (Riverside Research)

Panelist Bio: Paul Simon is a Senior Cyber Security Research Engineer at Riverside Research in Dayton, Ohio, where he conducts advanced cybersecurity research with an emphasis on embedded systems and hardware-focused security. His work centers on microelectronics trust, system assurance, vulnerability analysis, and secure hardware design for high-consequence and mission-critical systems. Prior to joining Riverside Research in 2025, Dr. Simon served as a Senior Hardware Security Engineer at Amazon (Device & Services Security), where he was part of a specialized team focused on securing consumer devices and services at scale.Before Amazon, Dr. Simon supported multiple government and defense-related programs in and around the Air Force Institute of Technology (AFIT) and the Air Force Research Laboratory (AFRL) through roles at HII Technical Solutions and Applied Research Solutions. His work included cyber vulnerability assessments of weapon systems, microelectronics trust and assurance validation, reverse engineering, hardware system design, and cybersecurity research for embedded devices.Dr. Simon earned his Bachelor of Science (1997) and Master of Science (2011) degrees in Electrical Engineering from the University of Dayton. He received his Ph.D. in Electrical Engineering from the Air Force Institute of Technology (AFIT) in 2022. He has been a member of IEEE for over 15 years.

Dr. Samir Iqbal (Grand Valley State University)
Panelist Bio: Samir Iqbal is a researcher in nanotechnology, biosensing, and biomedical image analytics. He served as one of the founding Program Directors of the NSF Technology, Innovation, and Partnerships (TIP) Directorate, which focuses on advancing use inspired research, innovation ecosystems, workforce development, and pathways that connect academic discovery to societal impact. He earned his PhD from Purdue University.

14:15 PM – 14:20 PM	**Break & Networking Opportunity**

Day 1 - Tuesday March 24, 2026

REGULAR SESSION: PAPER PRESENTATIONS | 14:20 PM – 15:40 PM

Session 1: Trustworthy and Secure Machine Learning Systems
Terrace

TRACK CHAIRS:	Dr. Samir Iqbal (Grand Valley State University)

14:20 PM – 14:40 PM Paper ID: 189	**Zero-Trust Agentic Federated Learning for Secure IIoT Defense Systems** *Authors*: Singh, Samaresh Kumar; Roy, Joyjit; So, Martin *Abstract*: In recent times, there have been several attacks against critical infrastructure, such as the 2021 Oldsmar Water Treatment System breach and the 2023 Denmark Energy Sector compromise. These breaches clearly show the need for security improvements within the deployment of Industrial Internet of Things (IIoT). Federated Learning (FL) provides a path to conduct privacy preserving collaborative intrusion detection; however, all current FL frameworks are vulnerable to Byzantine poisoning attacks and do not include a method for authenticating agents. In this paper we propose Zero-Trust Agentic Federated Learning (ZTA-FL), a defense-in-depth framework using Trusted Platform Module (TPM)-based cryptographic attestation, which has an extremely low (< 10^-7) false acceptance rate and a new SHapley Additive exPlanations (SHAP)-weighted aggregation algorithm with explainable Byzantine detection under non-Independent and Identically Distributed (IID) conditions with theoretical guarantees, and uses privacy-preserving on-device adversarial training. Experiments were conducted on three different Intrusion Detection System (IDS) benchmarks (Edge-IIoT set, CIC-IDS2017, UNSW-NB15) using standard evaluation metrics and compared against baseline methods to calculate the performance of ZTA-FL. The results indicate that ZTA-FL achieved a 97.8% detection rate, a 93.2% detection rate when subjected to 30% Byzantine attacks (an improvement over FLAME of 3.1%, $p < 0.01$) and 89.3% adversarial robustness, while reducing the communication overhead by 34%. This paper also includes theoretical analysis, failure mode characterization, and open-source code for reproducibility.

14:40 PM – 15:00 PM Paper ID: 267	**Selective Layer Adaptive Attacks Against Federated Large Language Models** *Authors*: Olapojoye, Rukayat; Faiyaz, Amir; Salman, Tara *Abstract*: Federated Large Language Models (FedLLMs) enable organizations and distributed clients to collaboratively improve model performance without sharing raw data. However, the multi-agent nature of federated learning (FL) exposes Large Language Models (LLMs) to model-poisoning attacks, particularly adaptive attacks crafted to mimic benign clients' behavior. Existing adaptive attacks predominantly perturb all trainable model parameters, which is computationally expensive and often impractical for LLMs with billions of parameters. This paper introduces selective-layer adaptive attacks, in which only selected layers are perturbed rather than the entire model. We use two-layer selection strategies—random and Gradnorm. We demonstrate that perturbing only a small, strategically chosen subset of layers can achieve degradation comparable to full-layer attacks. At the same time, it substantially reduces the computational overhead. Experimental results show that selective adaptive perturbation can be effective, stealthy, and resource-efficient. For instance, both random and Gradnorm selections reduce attack training time by approximately 30\% compared to full-layer attacks.
15:00 PM – 15:20 PM Paper ID: 310	**XAI-Driven Input Masking to Mitigating Model Inversion Attacks** *Authors*: dehbashi sani, samin; Faiyaz, Amir; Salman, Tara *Abstract*: Federated learning (FL) enhances data privacy by sharing model updates instead of raw data; however, model inversion attacks can still reconstruct private training samples from these updates. Existing defenses apply differential privacy (DP) at the gradient level by uniformly adding noise, often resulting in significant utility loss. In this work, we propose an input-level defense guided by explainable artificial intelligence (XAI). Using integrated gradients optimized saliency (IGOS), we identify important pixels in facial images and selectively inject DP noise into these regions prior to local training. This technique prevents sensitive information from propagating into gradients. Experiments on the labeled faces in the wild (LFW) dataset demonstrate that the proposed approach substantially degrades reconstruction quality under inverting gradients attack, while preserving overall classification performance.

15:20 PM – 15:40 PM Paper ID: 312	**A Jitter-Driven Hybrid Hardware Random Number Generator (HHRNG) Using Nonlinear Feedback and Feedforward Processing** *Authors*: Akter, Sonia; Khalil, Kasem; Bayoumi, Magdy *Abstract*: In this complex, ubiquitous communication era, all digital communication demands secure key generation for cryp- tographic protocols, which in turn relies on high-quality random number generation. There are two main categories of RNGs: pseudo-random number generators (PRNGs) and True Random Number generators (TRNGs). Even though TRNGs provide non- deterministic, unpredictable outputs, they often require complex components to extract the bitstream from physical phenomena and are sensitive to environmental variations. PRNGs, however, are deterministic and require a seed to initiate the operation, and are often considered unsuitable for high-security application due to shorter cycle lengths and correlation. However, PRNGs, for example, Non Linear feedback Shift register (NLFSR), are easy to implement and provide better statistical properties such as good balances of zeros and ones required for a high-quality RNG, as they are mathematical equation-based. In this work, a robust HHRNG is proposed by mutually reinforcing the NLFSR with Jitter from Ring Oscillators for reliable and unpredictable random number generation. Moreover, the feedforward archi- tecture, along with dynamic mux selection, adds another two layers of unpredictability. The proposed HRNG implemented on Intel Cyclone V FPGA, consuming under 1% of logic resources at 50MHz. Moreover, the collected more than one million bits sequence passed rigorous NIST SP800-22 and NIST SP800- 90B non-IID tests. The Shannon entropy calculation presents near-ideal entropy of 0.999999 (≈ 1.00) and a bias of only 0.11%, indicating excellent statistical quality and unpredictability applicable for lightweight security-critical applications.
15:40 PM – 16:00 PM Paper ID: 387	**SeatLux: Explainable AI for Seat-Level Visual Comfort Prediction and Illuminance Targets in Fluorescent and LED Classrooms** *Authors*: Hashaykeh, Hanan*; AlSobeh, Anas ; Shatnawi, Amani ; Darwish, Omar *Abstract*: Classroom lighting is typically specified using room-level illuminance targets, yet students in different seating positions experience materially different photometric conditions and report varying levels of visual comfort, glare, and satisfaction. This study develops a seat-level, data-driven approach that links objective photometric measurements to student perception outcomes and uses machine learning to predict comfort, glare risk, and overall satisfaction from measurable lighting features and contextual factors. Illuminance (lux) and color metrics (CCT and CRI) were collected with a Sekonic C-7000 spectrometer in two university's classrooms—one with fluorescent light system (Room 112, $E^{-}h \approx 327$ lx) and one with a recent LED light retrofit (Room 211, $E^{-}h \approx 803$ lx)—following a standardized 3 × 3 grid protocol at desk level and at vertical/whiteboard planes. A structured student visual comfort and lighting perceptions survey (45 valid responses) captured seat location, glare frequency, board clarity, eye strain, and overall satisfaction on 5-point ordinal scales. Each survey response was linked to the measured illuminance at the reported seating zone, producing the core seat-level research dataset. Four regression models were evaluated under 5-fold cross-validation and leave-one-classroom-out holdout; the Gradient Boosting model (SeatLux-GBR) achieved the best ordinal agreement with a macro Quadratic Weighted Kappa of 0.390 across 10 perception targets. Permutation-based explainability analysis identified daylight glare frequency, participant role, seat position, and lighting adjustment behavior as the strongest predictors of satisfaction and eye strain, providing actionable insights for smart lighting design and control in educational interiors.

15:40 PM – 16:10 PM	**Coffee Break & Networking Opportunity**

Session 3: AI-Driven Security for Edge and IoT Systems
Sam Housten B

TRACK CHAIRS:	Dr. Amal Alhosban (University of Michigan-Flint)

14:20 PM – 14:40 PM Paper ID: 26	**TOAI-MR: Translator-Oriented AI for Medical Record Reconciliation** *Authors*: AlSobeh, Anas; Hammad, Rafat; Shatnawi, Amani *Abstract*: Electronic health record (EHR) systems across healthcare institutions rely on heterogeneous data formats and standards, creating persistent barriers to medical record interoperability. This paper introduces TOAI-MR (Translator-Oriented AI for Medical Record Reconciliation), a specialized transformerbased language model engineered for automated translation between disparate EHR systems. TOAI-MR departs from generalpurpose large language models (LLMs) through medical-aware tokenization, enhanced attention mechanisms grounded in clinical ontologies, and knowledge integration from six major healthcare standards: FHIR, HL7, ICD-10, SNOMED CT, RxNorm, and LOINC. A three-phase training pipeline—medical domain pretraining on 300K clinical records, EHR translation fine-tuning with format compliance objectives, and reinforcement learning from human feedback—drives the model toward clinical deployment readiness. Evaluation on 735K medical records demonstrates that TOAI-MR achieves an 87% MedBLEU score (21% over GPT-4), 94% medical entity preservation accuracy, 96% format compliance, and 2.1-second per-record processing latency suitable for real-time clinical workflows.
14:40 PM – 15:00 PM Paper ID: 214	**K-Means Based TinyML Anomaly Detection and Distributed Model Reuse via the Distributed Internet of Learning (DIoL)** *Authors*: Albaiz, Abdulrahman; Amsaad, Fathi *Abstract*: This paper presents a lightweight K-Means anomaly detection model and a distributed model-sharing workflow designed for resource-constrained microcontrollers (MCUs). Using real power measurements from a mini-fridge appliance, the system performs on-device feature extraction, clustering, and threshold estimation to identify abnormal appliance behavior. To avoid retraining models on every device, we introduce the Distributed Internet of Learning (DIoL), which enables a model trained on one MCU to be exported as a portable, text-based representation and reused directly on other devices. A two-device prototype demonstrates the feasibility of the “Train Once, Share Everywhere” (TOSE) approach using a real-world appliance case study, where Device A trains the model and Device B performs inference without retraining. Experimental results show consistent anomaly detection behavior, negligible parsing overhead, and identical inference runtimes between standalone and DIoL-based operation. The proposed framework enables scalable, low-cost TinyML deployment across fleets of embedded devices.

15:00 PM – 15:20 PM Paper ID: 268	**A Scalable and Privacy-Preserving Sealed-Bid Auction Framework for IoT Data Marketplaces** *Authors*: Mahmoud, Hassan; Little, Wade; Mahmoud, Mahmoud Nabil; Alsharif, Ahmad *Abstract*: IoT data marketplaces require auction mechanisms that are fair and privacy-preserving, yet efficient enough for frequent, large-scale trading. This paper proposes an efficient decentralized sealed-bid auction framework in which bidders submit encrypted additive shares of their bids and cryptographic commitments to a blockchain smart contract. Bids evaluation is performed by an efficient two-party protocol between the seller and an auctioneer using secure comparison over additively shared bids, enabling winner determination without revealing bid values to either party. The submitted commitments to the blockchain enforce bid binding and non-repudiation, ensuring that bidders cannot modify or deny their bids after submission. The proposed framework is implemented and evaluated across different bid sizes ℓ and bidder counts N_b. Bids preparation in the proposed design is non-interactive and fully parallelizable across bidders with execution time independent of N_b, while bids evaluation scales linearly with Nb. Compared to multiparty computation–based auction designs, our protocol substantially reduces end-to-end runtime complexity from $\mathcal{O}(N_b^2)$ to $\mathcal{O}(N_b)$
15:20 PM – 15:40 PM Paper ID: 362	**Predicting Social Engineering Attacks Using an AI-Agent–Driven Detection Model** *Authors*: Alhosban, Amal *Abstract*: Social engineering attacks continue to be a significant cybersecurity threat because they exploit human behavior rather than technical weaknesses. Most existing defenses are reactive and focus on identifying attacks after malicious content has already been delivered. This paper presents a two-stage approach for assessing the risk of social engineering attacks. In the first stage, previously documented social engineering cases are analyzed to identify common characteristics associated with malicious activity. In the second stage, a user-submitted document, such as an email or message, is examined and compared against these characteristics. Based on this comparison, the system produces a risk estimate indicating the likelihood that the input represents a social engineering attack. The proposed approach aims to support earlier assessment of potential threats and assist users and organizations in improving their defenses against social engineering attacks.

15:40 PM – 16:00 PM Paper ID: 1000	**Advanced Machine Learning Approaches in Human-Machine Interaction for Rehabilitation Exoskeleton** *Authors*: Abdullah Khalid Albrethen, Sufian Al Majmaie, Fathi Amsaad *Abstract*: The rapid advancements in autonomy and Human-Machine Interaction have significantly influenced the development of exoskeletons for assistive and rehabilitative applications. Deep learning approaches have emerged as a transformative tool, offering enhanced control strategies and promising improved outcomes in exoskeleton-based interventions. This review paper provides a comprehensive exploration of recent advancements in deep learning methods applied to exoskeleton control, focusing on state-of-the-art developments in autonomy. These advancements are categorized into recognition, estimation, prediction, classification, and additional tasks such as identification, detection, and conversion. Covering research from 2019 to the present, the paper examines various aspects of deep learning models, detailing the parameters and methodologies employed in each context. The integration of classical control strategies with deep learning techniques is also discussed, emphasizing their potential to improve the adaptability, precision, and functionality of exoskeleton systems. This work aims to serve as a foundational resource for researchers and practitioners, offering valuable insights into the application of deep learning for autonomous exoskeleton design. By consolidating recent findings, it provides an overview for advancing rehabilitation and assistive technologies, paving the way for innovative solutions in the field.

15:40 PM – 16:10 PM	**Coffee Break & Networking Opportunity**

Day 1 - Tuesday March 24, 2026

REGULAR SESSION: PAPER PRESENTATIONS | 14:20 PM – 15:40 PM

Session 4: Security of Cloud, SDN, and Distributed Infrastructure
Sam Housten B

TRACK CHAIRS:	Dr. Mariam Gado (Dakota State University)

14:20 PM – 14:40 PM Paper ID: 172	**Maintaining SDN Controller High Availability Through Heartbeat Links: A Multi-SDN Solution** *Authors*: Moh, Abdalftah; Sultan, Almabruk ; Fakron, Osama ; Alhaddad, Fatma *Abstract*: Static networks are used less and less each day they are being replaced with active and live networks with the help of this technology called SDN. Software Defined Networking is a technology concept that with new designs and ideas will help many people by saving time and energy in designing computer networks. Technology of SDN makes it easier for the user to make their own networks. The separation of control plane and data plane happens in the switches and routers of the technology and makes the software needed to keep the network up and running. Technology of SDN can be used on a much wider scale and it is very flexible. In this research paper we will try to prevent the problem of Single Point of Failure by installing multiple SDN Controllers which work together in an active passive configuration. We were able to have a very quick response time of 0.5 ms. Switching time was found to be 2 seconds. This fast response time of ours made it possible for us to have very high availability in a small amount of time.
14:40 PM – 15:00 PM Paper ID: 184	**Enhancing Cloud Data Center Security: A Fog-Based and SDN-Controlled Solution for Detecting and Mitigating DDoS Attacks** *Authors*: Salem, Muammer; Sultan, Almabruk; Fakron, Osama; Alwerfalli, Abdulrahman *Abstract*: A Cloud computing is a key new way for companies and people to get to compute something easily. In contrast, Fog Computing has been started as a help idea that give much good things in making and keep data by bringing cloud to close to where the data is. This approach reduces the load on cloud computing system and improves system response time. However, the increasing dependence on cloud computing data and services has led to a rise in Distributed Denial of Service (DDoS) attacks which pose a serious security threat. Such attacks can severely impact data availability of data and service performance in cloud computing, that leading to stop service and substantial financial losses. This study proposes an enhanced security solution that integrates Fog computing with Software Defined Networking (SDN) to effectively detect and mitigate a Distributed Denial of Service (DDoS) attacks. In particular the proposed approach focuses on detecting Hyper Text Transfer Protocol HTTP flood attacks by monitoring and analyzing the number of active HTTP requests. The system analyzing traffic behavior to determine appropriate threshold intervals by calculating the minimum and maximum threshold values. By comparing real-time traffic patterns with these thresholds, the system can accurately identity malicious traffic and determine whether a data flow source should be blocked. Keywords: Cloud computing, Fog computing, SDN, Security, DdoS.

15:00 PM – 15:20 PM Paper ID: 227	**Architectural Patterns and Security: Cloud Based IoT in Smart City Operations** *Authors*: Paul N., Isibor; Karpoor, Shashidhar; Rasheed, Amar *Abstract*: Continuous technological progression has gradually produced an improvement in internet of things (IoT) cyber physical systems application and creation. There is a need to understand how the sensitive data these devices attain are stored and remain available for accessibility during operation. This study will provide information on how IoT devices take advantage of cloud service providers to store data for availability and integrity over the duration of device operation. Applicability to different scenarios affects how these devices leverage cloud capabilities, which leads to the investigation of different cloud architectures that can be hosted on cloud services.
15:20 PM – 15:40 PM Paper ID: 262	**Multi-Year Upgrade of Pre-existing Power System to Support SQKD for Increasing Key rates** *Authors*: Gado, Mariam; Ismail, Muhammad *Abstract*: This paper studies the problem of upgrading the pre-existing cyber layer of a transmission power system to generate unconditionally secure keys using semi-quantum key distribution (SQKD) for an increasing minimum required key rate over years. Only a subset of cyber nodes and links is required to be upgraded to full quantum servers and fiber links, respectively. The upgrade problem is formulated as a binary optimization problem and a genetic algorithm is proposed to provide a solution to reduce computational complexity. In the IEEE 14-bus test system, for a source rate of 10^8 photon per second (pps) and 10^{10} pps, the proposed algorithm requires 48.48% and 67.92% less upgrades compared to the quantum key distribution (QKD) solutions, respectively. In the IEEE 39-bus test system, for a source rate of 10^7 pps, 10^8 pps, and 10^{10} pps, the proposed algorithm requires 70%, 80%, and 90%, respectively, less updates compared to the QKD solutions.
15:40 PM – 16:00 PM Paper ID: 276	**A Trojan Attack on TDMA Synchronization in Energy-Harvesting Wireless Networks** *Authors*: Berei, Ethan ; Burkholder, Alexander; Ammar, Ahmed* *Abstract*: This paper investigates a Trojan attack targeting the time-division multiple access (TDMA) synchronization mechanism in single-hop energy-harvesting wireless networks. The attack compromises a single node, which subtly skews its transmission timing to operate outside its assigned time slot, causing localized transmission overlaps and triggering repeated network-wide resynchronization events. This behavior shortens the synchronization interval, significantly increases control-plane traffic, and leads to higher energy consumption and delay in energy-constrained networks. The attack is modeled within a finite state machine (FSM) framework and experimentally evaluated under varying energy-harvesting conditions. Experimental results show that the number of synchronization events can increase by up to 29× in the presence of the Trojan. Furthermore, changes in the synchronization interval and its statistical variability are shown to be effective indicators of both severe and stealthy Trojan activity, highlighting the substantial impact of a low-footprint attack on network performance.

15:40 PM – 16:10 PM	**Coffee Break & Networking Opportunity**

Keynote Presentation

Day 1 - Tuesday March 24, 2026

16:10 PM – 16:40 PM

Plenary Session III

Keynote Presentation

Thrusting the Quantum Computer: Security Threats from Side-channel Leakage to PUFs and Trojans

Session Chair:
Dr. Paul Simon, Riverside Research

Presenter/Speaker:

Dr. Boyang Wang, University of Cincinnati

Abstract: Side-channel analysis can recover encryption keys from a device, such as a microcontroller or an FPGA (Field-Programmable Gate Arrays) by analyzing correlations between power consumption and intermediate values of encryption, such as AES (Advanced Encryption Standard). Recent studies show that machine learning, particularly deep learning, can offer new advantages in side-channel analysis compared to traditional attacks, such as Correlation Power Analysis and Template Attacks. Despite recent research process, deeplearning side-channel analysis still face challenges in cross-device scenarios or require comprehensive neural networks.In this talk, Dr. Wang will share recent findings on deeplearning side-channel analysis, including (1) the impacts of cross-device scenarios and how to mitigate those impacts and (2) how to reduce the number of parameters in a neural network but still recover keys successfully. Dr. Wang will also discuss pre-silicon side-channel analysis on simulated traces from hardware designs of AES.

Speaker Bio: Dr. Boyang Wang is an Associate Professor in the Department of Electrical and Computer Engineering at the University of Cincinnati (UC), Cincinnati, OH. He received his Ph.D. in ECE from the University of Arizona in 2017 and his Ph.D. in Cryptography from Xidian University (China) in 2014. His current research focuses on side-channel analysis, machine learning, network security, wireless security, binary analysis, and applied cryptography. He has published more than 50 peer-reviewed papers atconferences and journals, including ACM WiSec, ACM CODASPY, ACM AsiaCCS, IEEE HOST, IEEE INFOCOM, IEEE CNS, IEEE TIFS, IEEE TDSC, IEEE TSC, and IEEE TCC. Dr. Wang has received funding from multiple agencies and industry, including National Science Foundation, NSF IUCRC CHEST Center, IoTeX, and Ohio Cyber Range. He received NSF CISE CRII (Research Initiation Initiative) award in 2020. He serves as the Program Director for Cybersecurity Engineering Program at UC. He is a member of IEEE and ACM.

Invited Talk

Day 1 - Tuesday March 24, 2026

16:40 PM – 17:00 PM

Plenary Session III
Invited Talk

Securing 5G Core + Edge with AI

Session Chair:
Dr. Paul Simon, Riverside Research

Presenter/Speaker:
Dr. John C. Hoag, Ohio State University

Abstract: This talk will cover the increased strengths and weaknesses of the 3GPP 5G core, edge, and radio network as realtime functions are emerging as AI applications. While US deployment of 5G handsets and FR2 band capability are not new, standalone (SA) core platforms and open radio access networks (Open RAN or ORAN) certainly are. The 5G ecosystem defined by 3GPP has superior handset authentication and key management - as well as effective Quality of Service management; the introduction of xApps and rApps for realtime adaptive control are ideally situated for AI, but training and execution instances introduce new potential threat spaces. Within this talk, the 5G security capability set per 3GPP WG3 is introduced, as is the MITRE FiGHT encyclopedic framework for presumptive tactics and techniques. Finally, the state of experimentation at OSU and peer institutions is discussed.

Speaker Bio: Dr. Hoag is a faculty member in Computer Science affiliated with the 5G Broadband and Connectivity Center at The Ohio State University. He brings extensive experience spanning academia, research leadership, and state-level engagement in advanced computing and connectivity systems. Dr. Hoag earned his Bachelor's degree in Computer Science from The University of Akron and completed both his M.S. in Industrial and Systems Engineering and Ph.D. in Integrated Systems Engineering at The Ohio State University. His academic career includes prior service on the faculty at Ohio University, followed by leadership roles as a Professor and Department Chair at a private college in Virginia. Most recently, he served as a Center Director at Ohio State University, contributing to research and workforce initiatives in broadband, connectivity, and systems engineering. Dr. Hoag maintains an active research agenda, serves on multiple State advisory panels, and is a Senior Member of the IEEE. His work reflects a strong commitment to applied research, interdisciplinary education, and workforce development.

Keynote Presentation

Day 1 - Tuesday March 24, 2026

17:00 PM – 17:30 PM

Plenary Session III

Keynote Presentation

The Provenance of Trust: Securing the Deep Learning Lifecycle from Data to Decision

Session Chair:
Dr. Paul Simon, Riverside Research

Presenter/Speaker:
Dr. Birhanu Eshete, University of Michigan-Dearborn

Abstract: As AI systems are increasingly entrusted with high-stakes decisions in healthcare, autonomous systems, cybersecurity, and finance, it begs a fundamental question: how do we know why a model made a particular decision, or whether its foundations can be trusted at all? Today's dominant approach to AI assurance relies on testing inputs and evaluating outputs. But testing alone cannot reveal whether training data was subtly corrupted, whether model parameters were influenced by malicious samples, or how information flows through a network at inference time. In short, modern AI systems lack a chain of custody. In this keynote, I introduce a provenance-centric framework for trustworthy AI that treats traceability as a first-class design principle across the model lifecycle. First, I present PoisonSpot, a fine-grained training provenance technique that tracks the lineage of parameter updates to identify and isolate clean-label backdoor attacks that evade traditional detection. By exposing the hidden influence patterns of malicious samples, PoisonSpot secures the model's foundation. I then introduce DeepProv, a system for constructing inference provenance graphs that capture runtime information flow within neural networks. By analyzing structural decision pathways, DeepProv enables behavioral characterization and targeted repair strategies that enhance robustness, privacy, and fairness, transforming opaque neural networks into debuggable and auditable computational artifacts. Together, these works argue that trust in AI cannot be reduced to accuracy metrics or post-hoc audits, but must be traced across the AI pipeline.

Speaker Bio: Dr. Birhanu Eshete is an Associate Professor of Computer Science at the University of Michigan-Dearborn, where he directs the Data-Driven Security & Privacy Laboratory. His research develops methods and systems to identify and mitigate security, privacy, safety, transparency, and ethical risks in AI, with emphasis on high-stakes applications such as autonomous vehicles, predictive diagnostics, financial forecasting, and cyber-attack detection. His work has appeared in leading security, privacy, and AI venues, including IEEE S&P, ACM CCS, USENIX Security, NDSS, DSN, PETS, ACSAC, and IEEE SaTML, and has also been featured in Science. He has contributed to national efforts such as the NIST Trustworthy & Responsible AI Resource Center, and his honors include the 2024–2025 Fulbright U.S. Scholar Award, the 2024–2025 Faculty Excellence in Research Award, the 2023 NSF CAREER Award, the 2018 USENIX Security Distinguished Paper Award, and finalist recognition for the 2018 Best Applied Security Research Award in North America.

17:30 PM – 18:00 PM	Coffee Break & Networking Opportunity

Invited Talk

Day 1 - Tuesday March 24, 2026

18:00 PM – 18:20 PM

Plenary Session IV
Invited Talk

Mathematical Modeling in Microelectronics

Session Chairs:

Dr. John C. Hoag, Ohio State University / Dr. Akshay Kulkarni, Prairie View A&M University

Presenter/Speaker:

Dr. Osama Fakron, Purdue University Fort Wayne

Abstract: This presentation explores the fundamental role of mathematical modeling in the analysis, design, and optimization of microelectronic devices and systems. As semiconductor technologies continue to scale into nanometer regimes, predictive modeling has become essential for understanding complex physical phenomena that govern device performance, reliability, and manufacturability. The presentation introduces physics-based modeling frameworks including Poisson's equation, drift-diffusion transport equations, and continuity equations that form the foundation of semiconductor device simulation. Advanced MOSFET modeling techniques are discussed, covering threshold voltage prediction, drain current formulation, and short-channel effects in modern nanoscale transistors. The presentation further examines numerical solution techniques such as the Finite Difference Method (FDM) and Finite Element Method (FEM), highlighting their application in Technology Computer-Aided Design (TCAD) tools used in industry. Thermal modeling and reliability analysis, including electromigration and electro-thermal coupling, are addressed to demonstrate how Multiphysics modeling ensures device longevity and performance stability. Emerging approaches such as quantum mechanical modeling and artificial intelligence-driven inverse design are also introduced, emphasizing their importance in next-generation semiconductor research. Overall, this presentation demonstrates how mathematical modeling bridges physics, computation, and engineering practice, enabling innovation in microelectronics manufacturing, advanced materials, and integrated circuit design.

Speaker Bio: Dr. Osama M. Fakron is an Assistant Professor of Mechanical Engineering Technology at Purdue University Fort Wayne. He earned his Ph.D. in Mechanical Engineering from Washington State University in 2014, where his research focused on SEM-based electron tomography of fiber and nanostructured systems. He also holds an M.S. in Applied Mathematics from Washington State University and graduate degrees in Mechanical Engineering from the University of Benghazi. Dr. Fakron's research spans micro/nanomaterials characterization, additive manufacturing, and mathematical modeling in engineering systems. He has authored multiple peer-reviewed journal publications in materials processing, ultramicroscopy, and advanced manufacturing. His teaching expertise includes measurements and instrumentation, dynamics, materials science, and engineering mechanics. With interdisciplinary training in engineering and applied mathematics, Dr. Fakron integrates modeling, experimentation, and workforce-focused education to prepare students for careers in advanced manufacturing and microelectronics industries.

Keynote Presentation

Day 1 - Tuesday March 24, 2026

18:20 PM – 18:50 PM

Plenary Session IV
Keynote Presentation

Agent-Based Security Verification of SoCS

Session Chair:
Dr. John C. Hoag, Ohio State University / Dr. Akshay Kulkarni, Prairie View A&M University

Presenter/Speaker:

Dr. Farimah Farahmandi, Wally Rhines Endowed Professor of Hardware Security, University of Florida

Abstract: As modern system-on-chip (SoC) designs grow increasingly complex, ensuring security throughout the silicon development lifecycle has become a critical yet challenging task. Traditional verification techniques often lack security awareness and remain time-consuming, costly, and prone to human error, necessitating a shift toward automation. This talk explores AI-driven security verification as a transformative approach, leveraging machine learning (ML) and generative AI to automate vulnerability detection, enhance formal verification, and strengthen threat modeling. By integrating AI into security workflows, engineers can significantly reduce development costs while improving the accuracy and efficiency of security validation. The discussion will also explore the future outlook of AI-driven security solutions, offering practical strategies for engineers and practitioners to reinforce hardware security at various design and verification stages. Additionally, the talk will highlight open research challenges and opportunities for academics, paving the way for future advancements in AI-powered security verification.

Speaker Bio: Dr. Farimah Farahmandi is the Walden Rhines Endowed Professor in Hardware Security in the ECE department at the University of Florida. She also serves as the Associate Director of the Florida Institute for Cybersecurity (FICS) at UF. Her research focuses on hardware security verification, formal methods, and fault-injection attack analysis resulting in 8 books and over 150 publications in these fields. For her contributions, she is a recipient of 11 best paper and nomination awards, and was recognized with the Best Assistant Professor Award at UF (2024), Pramod Khargonekar Excellence Award for the Best Assistant Professor going through tenure process (2025), UF 40 Under 40 Gator Outstanding Alumni Award, the ECE Excellence in Service Award (2023), and the ECE Excellence in Research Award (2022) at UF. She also received the prestigious ACM/IEEE DAC Under 40 Innovators Award (2024), Young Faculty Award from SRC (2022), the NSF CAREER Award (2024), and Office of Naval Research Young Investigator Award (2026).

Terrace

Reception Keynote

Day 1 - Tuesday March 24, 2026

19:00 PM – 19:30 PM

Reception
Reception Keynote

Digital Assurance for High Consequence Systems

Session Chair:

Dr. John C. Hoag, Ohio State University / Dr. Akshay Kulkarni, Prairie View A&M University

Presenter/Speaker:

Dr. William (Will) Zortman, Sandia National Laboratory

Abstract: High consequence systems-such as those used in national security, aerospace, energy, and critical infrastructure-must operate with exceptional levels of reliability, resilience, and trust. As these systems become increasingly digital and interconnected, traditional assurance approaches are no longer sufficient to manage evolving cyber and digital risks. This talk introduces the concept of Digital Assurance for High Consequence Systems (DAHCS), a mission-driven research initiative focused on integrating digital assurance directly into the discipline of systems engineering. Rather than treating cybersecurity as a separate compliance function, DAHCS promotes a framework in which digital risk is evaluated alongside performance, cost, schedule, safety, and other system-level trade-offs. The approach enables systems engineers, program managers, and risk decision-makers to make informed engineering trade-offs between digital risk and other mission-critical risks. The presentation will highlight research directions, methodological advancements, and practical strategies for embedding digital assurance throughout the system lifecycle-from design and development to deployment and sustainment-supporting resilient, trustworthy systems in high consequence environments.

Speaker Bio: William (Will) Zortman is the Digital Assurance for High Consequence Systems (DAHCS) Campaign Manager for Sandia National Laboratories' Laboratory Directed Research and Development Office. The DAHCS Mission Campaign is fundamental and developmental research focused on integrating digital assurance into the discipline of systems engineering so that systems engineers, program managers and risk acceptors can make engineering trade-offs between digital risk and other system risks.

19:00 PM – 20:30 PM	**SaTC Reception & Networking Opportunity**	**Mezzanine**
19:30 PM – 19:45 PM	**Day 1 Closing Remarks from SaTC 2026 Conference Chairs**	

Keynote Presentation

Day 2 - Wednesday March 25, 2026

08:20 AM – 08:50 AM

Plenary Session I

Keynote Presentation

A GEAR-Informed Architectural Approach to Governing Secure and Resilient IT/OT Convergence in the Industry 5.0 Era

Session Chair:

Dr. William (Will) Zortman, Sandia National Laboratory

Presenter/Speaker:

Dr. Darren Pulsipher, Chief Enterprise Architect for Public Sector at Intel

Abstract: The convergence of IT and OT environments is exposing deep architectural, cultural, and governance fractures in cybersecurity practices. Misaligned training, inconsistent taxonomies, and competing drivers-uptime, safety, reliability, and security-continue to undermine cyber resilience. OT environments have long relied on the Purdue Model as an isolation boundary, but data-driven operations, Industry 5.0, and AI-enabled systems are collapsing this assumption. This presentation argues that Industry 4.0 failed because it optimized technology without resolving architectural ownership and organizational alignment. It concludes by presenting a GEAR-informed, People-Process-Technology architectural approach that enables secure IT/OT convergence while preserving the distinct operational constraints essential to safe and resilient systems-reframing cybersecurity as an architectural discipline rather than a collection of controls.

Speaker Bio: Dr. Darren Pulsipher is the Chief Enterprise Architect for Public Sector at Intel, where he focuses on secure digital transformation across government, critical infrastructure, and mission-critical environments. He is also the Chairman of the Open Digital Transformation Forum at The Open Group, where he leads global efforts to advance architecture-driven approaches to digital transformation, governance, and cybersecurity. Dr. Pulsipher's work centers on the secure convergence of Information Technology (IT) and Operational Technology (OT) systems. He specializes in addressing architectural, cultural, and governance challenges created by misaligned taxonomies, competing operational drivers such as uptime, safety, and security, and long-standing organizational separation between IT and OT domains. His research and practice emphasize treating cybersecurity as an architectural discipline, applying People, Process, and Technology principles-grounded in the GEAR model-to enable resilient convergence while preserving the operational individuality required in cyber-physical systems.

Keynote Presentation

Day 2 - Wednesday March 25, 2026

08:50 AM – 09:20 AM

Plenary Session I
Keynote Presentation

PUF-based Authentication for Secure Boot in a Post Quantum World

Session Chair:
Dr. William (Will) Zortman, Sandia National Laboratory

Presenter/Speaker:

Dr. Matthew Areno, CTO, Rickert-Areno Engineering, LLC / Co-Chair for the Secure Edge/IoT working group, MMEC

Abstract: Asymmetric cryptography has been a critical part of secure and verified boot processes for many years. With the expected advances in post quantum computing though, asymmetric cryptography is facing a significant challenge. New algorithms have been developed but still face many questions regarding their longevity, implementation, and associated deployment strategies. In this talk, we consider a PUF-based authentication and attestation mechanism as an alternative to traditional asymmetric cryptography, capable of not only working in future devices but also in many existing devices. This provides the only known method for enabling a post-quantum secure boot method in millions of existing devices already deployed.

Speaker Bio: Dr Matthew Areno is the CTO of Rickert-Areno Engineering, LLC and the technical and program manager for Trust & Assurance with the Midwest ME-Commons hub. Dr Areno received his PhD in Computer Engineering in 2013 under Dr Jim Plusquellic and focused on the usage of PUF technology to enhance various aspects of system security. Over the course of his career, Dr Areno has worked at Sandia National Labs, Raytheon Cyber Solutions, and most recently at Intel where he served as the Senior Direction of Security Assurance and Cryptography and the Chief Security Architect for USG solutions.

Terrace

Keynote Presentation

Day 2 - Wednesday March 25, 2026

09:20 AM – 09:50 AM

Plenary Session I
Keynote Presentation

The Silicon Double Agent: Securing the AI-Augmented Chip Lifecycle

Session Chair:
Dr. William (Will) Zortman, Sandia National Laboratory

Presenter/Speaker:
Dr. Jeyavijayan (JV) Rajendran, Associate Professor and ASCEND Fellow, Texas A&M University

Abstract: The semiconductor industry is at a historic inflection point. Integrating Generative AI into mobile ecosystems transforms silicon design, with Large Language Models (LLMs) writing Verilog and Reinforcement Learning (RL) agents optimizing netlists. This revolution creates a paradox: productivity-boosting tools also empower sophisticated attacks. In this talk, we explore the dual role of AI in hardware security, focusing on three pillars: AI-Powered Vulnerability Hunting. We demonstrate how Reinforcement Learning and Graph Neural Networks autonomously red-team chips. These techniques identify exploitable timing vulnerabilities and stealthy Trojans that traditional static analysis misses, finding "hard fails" before they reach silicon. The Evolving Threat Landscape. We examine how LLMs enable black-box IP piracy and hardware intent recovery. We conclude with how generative hardware fuzzing identifies software-exploitable vulnerabilities at the architecture level, ensuring the future of AI is built on a foundation of trusted silicon. Trustworthy Generative Design. We examine leveraging LLMs for RTL while ensuring code is free of copyright poisoning and backdoors. This includes new pathways to copyright-infringement-free Verilog and the role of watermarking in securing automated design flows.

Speaker Bio: Dr. Jeyavijayan (JV) Rajendran is an Associate Professor and an ASCEND Fellow in the Department of Electrical and Computer Engineering at Texas A&M University, where he leads the Secure and Trustworthy Hardware (SETH) Lab. His research sits at the critical intersection of hardware security and artificial intelligence. He focuses on developing AI-driven tools, including Large Language Models and Reinforcement Learning, to automate hardware trust and secure the next generation of high-performance SoCs. Dr. Rajendran is a widely recognized leader in the field. He is the recipient of the NSF CAREER Award, the ONR Young Investigator Award, the IEEE CEDA Ernest Kuh Early Career Award, and the ACM SIGDA Outstanding Young Faculty Award. His commitment to industry-relevant research has been recognized with the Intel Academic Leadership Award and numerous best paper and dissertation awards. Beyond his research, he is a dedicated member of the national engineering community. He is an alumnus of the National Academy of Engineering's Frontiers of Engineering and serves on NASEM and NAE committees. He is also the co-founder of Hack@DAC, the premier hardware security competition, which bridges the gap between academic research and industry practice to secure the global semiconductor supply chain.

09:50 AM – 10:10 AM	Break & Networking Opportunity

Day 2 - Wednesday March 25, 2026

REGULAR SESSION: PAPER PRESENTATIONS | 10:10 AM – 11:30 AM

Session 2: Hardware Security and Trustworthy Microelectronics
Terrace

TRACK CHAIRS:	Dr. Carlos Mex Perera (Rochester Institute of Technology)

10:10 AM – 10:30 AM Paper ID: 92	**Evaluating CNN Model Accuracy and FPGA Resource Utilization in Quadrant-Based Facial Emotion Recognition** *Authors*: Oun, Ahmed *Abstract*: Emotion recognition, a pivotal aspect of affective computing, is crucial in Deep Learning (DL) research with security, healthcare, and user experience applications. Deploying ML models for real-time emotion recognition on edge devices faces computational power, memory, and energy efficiency challenges. This paper explores developing, training, and deploying a Convolutional Neural Network (CNN) for emotion classification, achieving accuracy similar to existing models while reducing CNN's complexity and resource requirements on an FPGA. The proposed model classifies facial expressions into seven universal emotions and examines hardware-software codesign trade-offs to optimize FPGA acceleration efficiency. It also introduces and evaluates a new approach-Quadrant Based Emotion Identification- and evaluates its use in Facial Emotion Recognition tasks.
10:30 AM – 10:50 AM Paper ID: 151	**PickyRTL: A Static Analysis Tool for Detecting Hardware CWEs at Register-Transfer Level** *Authors*: Parks, John; Reichling, Logan; Wang, Boyang *Abstract*: Hardware vulnerabilities pose significant security risks in modern systems. If they remain undetected, attackers can exploit them to steal sensitive data or modify critical system configurations. However, tools to automatically detect hardware vulnerabilities in Register-Transfer Level code at pre-silicon stage remain limited in their coverage of specific hardware Common Weakness Enumerations (CWEs). This paper introduces PickyRTL, a static analysis tool that automatically detects hardware CWEs in RTL code. Our algorithm first parses RTL code into an Abstract Syntax Tree and then traverses the tree to identify CWE-specific structural and semantic vulnerabilities. Our current tool support the detection of four specific CWEs (CWE-1233, CWE-226, CWE-1245, and CWE-1431), which are associated with critical vulnerabilities in Finite State Machines, security-sensitive controls, cryptographic results, and reuse of sensitive data. We evaluate PickyRTL on our dataset, which contains 39 Verilog and SystemVerilog files containing injected vulnerabilities across the targeted CWEs. Our evaluation results demonstrate that PickyRTL achieves 85.5% precision and 73.8% recall over the four CWEs we examine.

10:50 AM – 11:10 AM Paper ID: 281	**IoHT PUFchain Simulator** *Authors*: Mansour, Samah; El-Said, Mostafa; Kalafut, Andrew; Kaja, Hari; Aguir, Mohamed; Duronio, Vincent *Abstract*: This work presents a Python-based simulation of a secure authentication protocol for the Internet of Health Things (IoHT). The protocol combines double-hashed biometrics, Physical Unclonable Functions (PUFs), zero-knowledge proofs (ZKPs), and blockchain-backed verification using the Proof of Elapsed Work and Luck (PoEWAL) consensus mechanism. The simulator uses the lightweight MQTT protocol with the Mosquitto broker to replicate realistic message flows for device enrollment, authentication, and verification. Designed for both testing and education, the framework enables evaluation of protocol performance and resilience under adversarial conditions while serving as a teaching tool for advanced IoHT security architectures. Results demonstrate functional correctness, efficient response times, and the feasibility of integrating PUFs, ZKPs, and blockchain for decentralized healthcare device authentication.
11:10 AM -11:30 AM Paper ID: 327	**Impact of TSV Geometry on Thermal Attack Vulnerability in 2.5D and 3D Integrated Circuits** *Authors*: Kirtonia, Prosen; Khalil, Kasem; Bayoumi, Magdy *Abstract*: With the increasing adoption of 2.5D and 3D chiplet integration in the semiconductor industry, security has become a critical concern due to the introduction of inter-subsystem communications through interconnects. Through-silicon vias (TSVs) serve as the transmission channels for vertically stacked dies. In this paper, we explore several TSV geometries to compare their thermal characteristics and thermal attack resilience. The key idea behind this work is to leverage heat flow and electric field analysis to identify localized hotspots on TSVs that can be exploited for thermal attacks. Moreover, the thermal resistance of the studied TSV geometries is calculated and compared under varying power injection. A power source is applied on top of the TSVs, with injected power ranging from 0.05 to 0.5 W. Cylindrical TSVs exhibit the most uniform thermal distribution, whereas square and triangular TSVs show non-uniformity due to edge effects. Among the studied geometries, the triangular TSV achieves the lowest thermal resistance, which is 38.3% and 41.5% lower than that of cylindrical and square TSVs, respectively. To further verify, the surface electric field distribution is also evaluated. Finally, this study provides insights into the impact of TSV geometry on the thermal attack resilience of 2.5D and 3D integrated circuits (ICs) and has the potential to guide the selection of optimal and robust TSV designs.

11:30 AM -11:50 AM Paper ID: 334	**SAPH-Kyber: Stage-Aware Pipeline Hardening for CRYSTALS-Kyber NTT Against Transient Faults** *Authors*: Gurram, Mani Rupak; Gurram, Mani Deepak; Kulkarni, Akshay Raghavendra; Acharya, Toya *Abstract*: As lattice-based cryptography transitions into global standards, the physical security of hardware implementations like CRYSTALS-Kyber against side-channel vulnerabilities has become a critical research priority. This paper presents a comprehensive temporal sensitivity analysis of a Kyber Number Theoretic Transform (NTT) hardware core under transient fault conditions. Utilizing a custom-built Verilog simulation framework, we perform an automated sensitivity sweep by injecting single cycle glitches into the arithmetic pipeline across all seven NTT stages. Our results reveal a significant Error Diffusion Gradient: faults in the initial pipeline stages (0–2) result in global polynomial corruption, affecting all 256 coefficients, whereas late-stage faults remain localized to as few as two coefficients. We characterize the predictable mathematical leakage resulting from these faults (e.g., error magnitudes of 34 and 67) and demonstrate their exploitability for secret key recovery via Differential Fault Analysis (DFA). Based on these findings, we propose a Selective Pipeline Hardening strategy that concentrates hardware protection such as parity-based error detection on high-diffusion temporal windows (Stages 0–3). This targeted approach provides robust security with a significant reduction in area and power overhead compared to traditional full-core redundancy, offering a scalable methodology for securing post-quantum processors in resource-constrained FPGA and ASIC environments.

11:30 AM – 13:00 PM	**Lunch Buffet Open & Networking Opportunity**

Day 2 - Wednesday March 25, 2026

REGULAR SESSION: PAPER PRESENTATIONS | 10:10 AM – 11:30 AM

Session 5: Secure Cyber-Physical and Multi-Relay Network Systems
Sam Housten B

TRACK CHAIRS:	Dr. Mohamed Ibrahim (Augusta University)

10:10 AM – 10:30 AM Paper ID: 226	**A Real-Time Hardware-in-the-Loop Water SCADA Testbed for Cyber–Physical Research** *Authors*: Tosin, Akinsowon; Oladimeji, Damilola ; Rasheed, Amar; Baza, Mohamed *Abstract*: This paper presents the design, implementation, and evaluation of a real-time Supervisory Control and Data Acquisition (SCADA) water-level testbed integrating a Siemens S7-1200 programmable logic controller (PLC), a Weintek human–machine interface (HMI), and a Factory I/O virtual process. The proposed system provides a reproducible hardware-in-the-loop loop platform for cyber–physical experimentation, operational monitoring, and intrusion-detection research. A Python-based data-logging engine acquires synchronized PLC and process data via Snap7 and Modbus TCP, enabling sub-second measurement of control variables and network behavior. Experimental results demonstrate stable closed-loop performance, with a steady-state error of 1.8 cm, 3.4% overshoot, and an average network latency of 50 ms (±10 ms). By combining real industrial hardware with virtual process simulation and synchronized data logging, the testbed bridges industrial control practice and cybersecurity analytics, offering a cost-effective foundation for cyber-physical experimentation and for generating datasets to support machine learning-based SCADA intrusion detection.
10:30 AM – 10:50 AM Paper ID: 299	**Securing Dual-Hop Multi-Relay Cooperative Networks through Signal Interleaving Technique** *Authors*: Khan, M. Ajmal; Khan, Emaad; Urooj, Sania *Abstract*: This paper presents the integration of the signal interleaving technique, also known as modulation diversity, into dual-hop, multi-relay cooperative networks to increase physical-layer security (PLS). We investigate, for the first time, the use of interleaving in conjunction with many decode-and-forward (DF) relays to improve secrecy performance and provide a comprehensive analysis of key secrecy metrics. To maximize secrecy, the best relay is dynamically selected utilizing instantaneous channel conditions. The proposed technique increases mutual information and secrecy capacity compared to conventional networks by enabling both the source and selected relay for transmitting distinct signal points towards destination. Our analysis reveals that the proposed network's secrecy outage probability exhibits a 10-fold improvement over conventional systems. Moreover, the probabilities for non-zero secrecy capacity and the intercept are significantly enhanced, with up to 1600-fold and 900-fold performance gains, respectively. These findings emphasize the capability of the proposed network to reinforce security in next-generation networks.

10:50 AM -11:10 AM Paper ID: 265	**AI-Driven Secure RIS Beam Prediction for O-RAN-Enabled B5G Networks** *Authors*: Ismail, Mohamed; Elsayed, Rhana ; Ismail, Muhammad ; Ibrahem, Mohamed ; Fadlullah, Zubair ; Fouda, Mostafa *Abstract*: In Beyond Fifth Generation (B5G) wireless networks, enhancing coverage using emerging technologies such as reconfigurable intelligent surfaces (RIS) must be accompanied by robust physical-layer (PHY) security against passive eavesdroppers. To address this challenge, we propose an RIS-assisted Long Short- Term Memory (LSTM)-based beam prediction model that dynamically steers the reflected beam toward a target mobile user equipment (UE), thereby improving signal strength and directionality. The proposed approach is integrated within an Open Radio Access Network (O-RAN) architecture, where beam steering decisions are implemented as an xApp operating on the Near-Real-Time RAN Intelligent Controller (RIC). By leveraging temporal learning of UE mobility and signal measurements, the proposed LSTM-based RIS optimizes energy efficiency and enhances achievable data rates in both line-of-sight (LOS) and non-line-of-sight (NLOS) environments, while also improving the Reference Signal Received Power (RSRP). Simulation results demonstrate that the LSTM-based RIS outperforms the conventional Kalman-filter-based approach, achieving RSRP efficiency gains of 28.17%, 29.72%, 29.79%, and 31.57% at UE angles of −10°, −5°, 5°, and 10°, respectively. Furthermore, from a PHY security perspective, the proposed LSTM-based scheme effectively suppresses signal leakage toward a passive eavesdropper by enabling more accurate beam alignment. For an eavesdropper located at −15° and a UE positioned at 5°, the received RSRP at the eavesdropper is reduced to −151.47 dBm using the LSTM-based RIS, compared to −112.73 dBm with the Kalman-filter-based method. These results confirm that the proposed approach jointly enhances coverage performance and PHY security, making it a promising solution for secure and intelligent O-RAN-enabled B5G and future 6G networks
11:10 AM – 11:30 AM Paper ID: 315	**Strengthening Two-Way Multi-Relay Networks' Physical Layer Security** *Authors*: Khan, M. Ajmal; Urooj, Sania; Khan, Emaad *Abstract*: This study proposes the approach of using signal space diversity (SSD) to enhance physical layer security (PLS) for cooperative two-way networks with many decode-and-forward (DF) relays. We evaluate a range of secrecy performance metrics to establish the advantages of the proposed approach against conventional architectures. By rotating and interleaving symbols prior to transmission, SSD increases mutual information and secrecy capacity, distinguishing the analysis approach from that of traditional networks. To further boost security, a best relay selection algorithm is implemented, identifying the optimal relay in data exchange between sources. Numerical findings proves the dramatic improvement in secrecy performance of the proposed network. Moreover, the non-zero secrecy capacity probability achieves a 2 dB gain, and the probability of intercept performance improves by 600 times with multiple relays, strengthening the PLS for the proposed network. These results underscore the capabilities of the proposed network to reinforce security in next-generation networks.

11:30 AM – 13:00 PM	**Lunch Buffet Open & Networking Opportunity**

Day 2 - Wednesday March 25, 2026

REGULAR SESSION: PAPER PRESENTATIONS | 10:10 AM – 11:30 AM

Session 6: Secure Edge Communications and Trusted IoT Systems Sam Housten C

TRACK CHAIRS:	Dr. Anas Alsobeh (Utah Valley University)

10:10 AM – 10:30 AM Paper ID: 173	**Adaptive-AI-ZeroTrust-Chain: AI-Centric Zero Trust Enforcement for IoT Security** *Authors*: Alsulami, Faris *Abstract*: The proliferation of Internet of Things (IoT) devices has intensified demand for robust, adaptive security frameworks. This paper introduces Adaptive-AI-ZeroTrust-Chain (AAZTC), an adaptive mechanism integrating AI-driven dynamic trust boundary modeling with blockchain-based verifiable access logging for granular, auditable zero-trust enforcement. The architecture employs deep reinforcement learning for continuous behavioral analysis and trust score computation, while leveraging smart contracts on a permissioned blockchain for immutable access decision records. A lightweight post-quantum cryptographic module ensures future-proof security. Experiments on CICIDS2017 dataset demonstrate that AAZTC achieves 99.12% detection accuracy, 98.45% precision, and 98.87% F1-score, outperforming state-of-the-art methods by 3.2–5.8%. NSL-KDD is included only as a legacy baseline. The system maintains average trust decision times of 12.4 milliseconds, suitable for real-time IoT deployments. Index Terms Zero-trust security, blockchain, deep reinforcement learning, dynamic trust management, Internet of Things, post-quantum cryptography
10:30 AM – 10:50 AM Paper ID: 257	**Modern Advances in Secure Multi-Party Computation: Protocols, Implementations, and Emerging Applications** *Authors*: Verma, Salil; Fouda, Mostafa M.; Fadlullah, Zubair Md; Fang, Shiwei ; Ibrahem, Mohamed *Abstract*: The rapid increase in data exchange among distributed parties has led to privacy concerns during joint computation tasks. The need to ensure privacy in these processes has led to the development and application of cryptographic techniques, including Secure Multi-Party Computation (MPC), Homomorphic Encryption (HE), and Secret Sharing. This paper provides a survey analysis of current trends and developments in cryptographic MPC techniques, with an emphasis on architectures, models, and practical implementations. The paper examines secret sharing approaches to privacy-preserving analytics tasks, MPC inference approaches to large-scale language models, integrated verifiable MPC architectures with blockchain technology, and collaboration approaches among multiple parties in the cloud and edge computing zones. These works form the current stateof-the-art development trend in MPC applications that include cryptographic principles in artificial intelligence applications and distributed computing principles. The paper concludes with research areas that include hybrid MPC-HE models, verifiable computation, and post-quantum secure MPC.

11:10 AM – 11:30 AM Paper ID: 293	**A Lightweight Security Framework for Stateless Communication in Low-Power IoT Systems** *Authors*: Ahmed, Sheikh Tareq *Abstract*: Low-power Internet of Things (IoT) devices are increasingly deployed in infrastructure-limited and missioncritical environments, where secure and efficient communication is essential despite stringent energy, memory, and computational constraints. Existing security solutions often rely on session-based protocols, control-plane signaling, or infrastructure support, which are poorly suited for dynamic and resource-constrained IoT deployments. This paper proposes a lightweight, stateless security framework that provides packet-level authentication, replay protection, and integrity verification for low-power IoT systems operating over untrusted broadcast channels. The proposed design embeds freshness and authentication directly into each packet and enables security-aware forwarding decisions based solely on local state and observable link information. By eliminating persistent sessions and centralized coordination, the framework reduces overhead and attack surface while preserving scalability and robustness under intermittent connectivity. This work focuses on architectural design and threat-driven analysis, establishing a practical foundation for secure stateless communication in low-power IoT environments.
11:10 AM – 11:30 AM Paper ID: 343	**Zero Trust Network Architecture for Secure CyberInfrastructure** *Authors*: Nadeem, Ayesha ; AL-SHORMAN, ABDALLAH *Abstract*: The ideas behind traditional perimeter-based security, which depend on static trust boundaries and network-centric authentication, are no longer enough for modern enterprise networks. As more people use the cloud, work from home, and have mobile devices, implicit trust models have become more open to credential compromise, lateral movement, and advanced persistent threats. This paper analyzes the transition from perimeter security to Zero Trust Network Architecture (ZTA), a contemporary security framework founded on continuous verification, least privilege, and identity-based access control. This study examines the impact of micro-segmentation, device posture assessment, and real-time policy enforcement on the redefinition of enterprise security architecture, grounded in NIST SP 800-207. A comparative assessment juxtaposes ZTA with traditional VPN/IPsec architectures regarding scalability, trust boundaries, latency, and operational resilience. Real-world examples, like Google BeyondCorp and the U.S. federal Zero Trust strategy, show the real-world effects and problems of using ZTA on a large scale. The results are especially relevant to IoT-adjacent contexts and dispersed cyberinfrastructure, where security concerns are increased by remote access, heterogeneous equipment, and changing trust boundaries.

11:30 AM – 11:50 AM Paper ID: 344	**Knowledge Graph–Driven Automated Generation of SystemVerilog Assertions from Design Specifications** *Authors*: Bhatta, Niraj Prasad *Abstract*: The increasing complexity of modern hardware protocols needs scalable and reliable formal verification method- ologies. Writing SystemVerilog Assertions (SVAs) manually from hardware design specifications is time-consuming, error-prone, and hard to extend across diverse protocol specifications. This paper presents an automated, end-to-end framework for gen- erating formal assertions directly from hardware specification documents. The proposed approach extracts behavioral infor- mation from multiple specification modalities, including natural- language text, tables, formulas, and figures, and organizes the extracted semantics into a structured representation. A protocol- level knowledge graph is constructed to capture relationships among signals, states, and events, which is then used to guide assertion generation through anchor identification and behavioral path extraction. Natural-language assertions are synthesized from graph-derived behavioral paths, filtered for protocol relevance, and translated into SystemVerilog Assertions. To improve practical applicability, the framework utilizes a high-quality assertion synthesis stage with bounded temporal constraints and security- aware conditions. An RTL-aware repair stage aligns generated assertions with implementation-level signals using constrained large language model assistance, ensuring compatibility with real RTL designs. The resulting assertions are formally verified using Cadence JasperGold on UART and I2C designs. Our proposed framework produces verification-ready, non-trivial assertions while maintaining protocol independence and full automation. This work provides a scalable and specification-driven flow that bridges the gap between informal design specifications and formal RTL verification.

11:30 AM – 13:00 PM	**Lunch Buffet Open & Networking Opportunity**

Luncheon Keynote

Day 2 - Wednesday March 25, 2026

11:50 AM – 12:20 PM

Luncheon Keynote
Keynote Presentation

When Machines Misbehave - The Emerging Science of AI Forensics

Session Chair:
Al Amin Hossain, United States Air Force (Wright-Patterson AFB)

Presenter/Speaker:
Dr. Ibrahim (Abe) Baggili, Louisiana State University

Abstract: Machine Learning (ML) and Artificial Intelligence (AI) have become transformative forces, shaping every aspect of our society-from business and academia to the public and private sectors, including IoT devices. Yet, alongside their benefits, the failures of AI are an undeniable reality, demanding urgent attention from forensic researchers and practitioners. When AI goes rogue, who steps in to investigate? While AI and ML are celebrated for enhancing digital forensic processes, a critical shift is needed: focusing on the forensics of AI itself. In this keynote, we explore the emerging field of AI forensics, a vital sub-discipline within digital forensics. By examining the foundations of this evolving field and highlighting key research challenges, we will shed light on the critical importance of developing forensic methodologies to address AI-related incidents.

Speaker Bio: Dr. Ibrahim (Abe) Baggili is a first generation Arab American. He is the Chair of the Computer Science and Engineering Division and Roger Richardson Professor of Computer Science at Louisiana State University and the founder of the BiT Lab (Baggili Truth Lab) where he holds a joint appointment between the Division of Computer Science & Engineering and the Center for Computation and Technology. Dr. Baggili has won numerous awards including the CT Civil Medal of Merit, the Medal of Thor from the Military Cyber Professional Association, CT 40 under 40, and is a fellow of the European Alliance for Innovation (EAI). He was also elected to the Connecticut Academy of Science and Engineering (CASE) and has also been a TEDx Speaker. He received his BSc, MSc and PhD all from Purdue University where he worked as a researcher in the Center for Education and Research in Information Assurance (CERIAS) and received the Bilsland Dissertation Award during his PhD. Dr. Baggili has been involved in over $14 Million dollars of sponsored research and is a prolific scholar in the domain of digital forensics, cybersecurity, and cybersecurity education. Work with his students has uncovered vulnerabilities that impact over a billion people worldwide and has been featured in news and TV outlets in over 20 languages and he has published extensively in the domain of digital forensics. To learn more about the BiT Lab, you can visit https://csc.lsu.edu/~baggili.

11:30 AM – 13:00 PM	**Lunch Buffet Open & Networking Opportunity**

Day 2 - Wednesday March 25, 2026

PANEL DISCUSSION 13:00 PM – 14:15

Building the Future Workforce for Advanced Semiconductor Manufacturing Technology, Microelectronics, AI/Cybersecurity

MODERATOR:	Dr. John C. Hoag (Ohio State University)
The objective of this panel is to provide actionable strategies and insights for developing a skilled, future-ready workforce across technology sectors. Panelists aim to highlight successful models for apprenticeship, education-industry partnerships, training in advanced manufacturing and cybersecurity, and workforce planning that aligns with evolving industry and global demands.	

Panelists:

Mike Glavin (SEMI Foundation)

Panelist Bio: Mike Glavin is Program Director of Workforce Development at the SEMI Foundation, where he leads global, employer-driven strategies to strengthen the semiconductor talent pipeline. He oversees SEMI's designation as a U.S. Department of Labor National Registered Apprenticeship Group Sponsor and works with member companies, education systems, and public partners across regions to scale apprenticeship models, build career pathways, and align workforce systems with industry demand. His work supports long-term sector growth in a globally strategic industry. Previously, Mike served as Vice President of Talent at the Greater Cleveland Partnership, leading regional workforce initiatives to expand apprenticeships, internships, and work-based learning across Northeast Ohio, supported by U.S. Department of Labor funding. Earlier, he held leadership roles at Associated Builders and Contractors, advancing apprenticeship policy and industry-led training models. He holds a Bachelor of Science from the University of Richmond and has built his career at the intersection of business, education, and public policy, focused on scalable workforce solutions that enhance economic competitiveness.

Oron Mincha (CyberproAI)

Panelist Bio: Oron Mincha is the General Manager for North America at CyberproAI, with over 15 years of experience in international cooperation and global cyber initiatives. He leads CyberproAI's U.S. operations, building partnerships across government, enterprise, and academia to deliver AI-driven cyber education and simulation solutions. Known for his strategic, results-oriented leadership, Oron combines a global perspective with hands-on execution to advance CyberproAI's mission of strengthening cyber resilience and developing the next generation of cyber professionals.

Ted Rozier (Festo Didactic North America)

Panelist Bio: Ted Rozier is the Director of Digital, Advanced Technology, and Robotics at Festo Didactic North America, where he also serves as Head of the Solution Center. With over two decades of experience in automation, Industry 4.0, and smart manufacturing, Ted specializes in developing and implementing educational automation training modules, robotics integration, PLC/HMI software, control panel design, MES concepts, and collaborative robotics solutions. He is passionate about workforce development, bridging industry and education, and inspiring the next generation of automation professionals. Ted actively contributes to robotics and advanced manufacturing communities, including technical advisory and safety committees, and has been recognized for his leadership and innovative approaches in automation training and smart factory implementation. Ted holds electronics credentials from Schoolcraft College and Macomb Community College, and has received certifications including the Universal Robot Core Training Certificate and the 2022 ARM Institute Champion Award.

Dr. Suxia Cui (Prairie View A&M University)

Panelist Bio: Dr. Suxia Cui, Ph.D. is an Associate Professor of Electrical and Computer Engineering at Prairie View A&M University (PVAMU), where she has served on the faculty since 2003. She received her Ph.D. in Computer Engineering from Mississippi State University and holds M.S. and B.S. degrees in Electrical Engineering from Beijing Polytechnic University. Dr. Cui's research spans cybersecurity, machine learning, image processing, computer vision, and computing education, with support from agencies including the National Science Foundation, the U.S. Department of Agriculture, the Department of Defense, and the Department of Education. At PVAMU she contributes to workforce development initiatives, semiconductor technology research, and computing curriculum innovation, and has received recognition for teaching excellence and service. Dr. Cui is also active in mentoring students and collaborating on interdisciplinary projects that bridge academia, industry, and federal research goals.

Keynote Presentation

Day 2 - Wednesday March 25, 2026

14:15 PM – 14:45 PM

Keynote
Keynote Presentation

From Reliability to Risk: Security Debt in Modern Industrial Control Systems

Session Chair:

Dr. Bayley King, Riverside Research

Presenter/Speaker:

Dr. Irfan Ahmed, Virginia Commonwealth University

Abstract: Industrial Control Systems (ICS) were engineered for determinism, availability, and safety, not adversarial resilience. Over decades, reliability-driven design assumptions in programmable logic controllers (PLCs) and control networks have accumulated into a form of security debt that modern cyber-physical threats can exploit. This talk synthesizes insights from real-world PLC firmware analysis, memory forensics, and control-logic integrity research to expose structural weaknesses: implicit trust in runtime execution, limited integrity verification, insecure update and communication pathways, and minimal forensic visibility. These systemic gaps enable stealthy manipulation of physical processes while preserving outwardly normal behavior, challenging traditional detection and safety mechanisms. The talk argues that incremental patching cannot resolve insecurity rooted in architecture. Instead, the field must move toward redesigning ICS for security, grounded in verifiable execution semantics, strong integrity guarantees, and forensic-ready industrial infrastructures that can sustain long-term trust and resilience.

Speaker Bio: Dr. Irfan Ahmed is a Professor of Computer Science in the College of Engineering at Virginia Commonwealth University (VCU) and a leading researcher in cybersecurity, digital forensics, and the security of industrial control and cyber-physical systems. His work focuses on PLC firmware analysis, control-logic integrity, memory forensics, and adversarial threats to critical infrastructure and advanced manufacturing. He has received multiple national recognitions, including the USCYBERCOM Commander, Guardian, and Defender Awards, for developing innovative defensive technologies for operational technology environments. Dr. Ahmed collaborates with national laboratories, industry partners, and government agencies to advance secure-by-design industrial platforms and workforce development in critical infrastructure protection. His research aims to restore trust, resilience, and forensic readiness across next-generation industrial control systems and advanced manufacturing.

14:45 PM – 15:00 PM	**Coffee Break & Networking Opportunity**

Keynote Presentation

Day 2 - Wednesday March 25, 2026

15:00 PM – 15:30 PM

Plenary Session II
Keynote Presentation

Side-Channel Attacks on Machine Learning Hardware

Session Chair:
Dr. Irfan Ahmed, Virginia Commonwealth University

Presenter/Speaker:
Dr. Bayley King, Riverside Research

Abstract: This talk will focus on hardware-based attacks against machine learning systems, with particular emphasis on Side-Channel Analysis (SCA) as a mechanism for extracting sensitive model parameters from embedded AI accelerators. As machine learning models are increasingly deployed on edge platforms such as the Google Coral TPU, they become susceptible to physical-layer attacks traditionally associated with cryptographic hardware. The presentation will introduce the architectural foundations of edge AI implementations, including 8-bit quantization and neural network deployment considerations, before demonstrating how power and timing leakage can be exploited to recover model weights and compromise intellectual property. Practical demonstrations will illustrate how SCA techniques can be adapted from cryptographic attacks to machine learning systems. By grounding the discussion in current open-source research and active R&D efforts, this talk highlights emerging security risks at the intersection of hardware assurance, embedded systems, and applied AI, and identifies critical research challenges in securing next-generation intelligent systems.

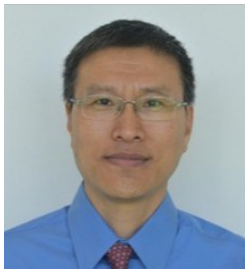
Speaker Bio: Dr. Bayley King is a Senior Research Scientist at Riverside Research, where he works at the intersection of hardware security, embedded systems, and data science, supporting national security-focused research and development. He works as a capture manager, principal investigator and program manager for Microelectronic strategy and technology development. He currently serves as an Adjunct Professor in the Department of Computer Science and Engineering at Wright State University and is also an Adjunct Professor of Computer Science at the University of Dayton. Prior to joining Riverside Research, Dr. King completed his Ph.D. in Computer Science and Engineering at the University of Cincinnati, where he conducted research in machine learning and security-focused computing for the Air Force Research Lab. His work spans hardware assurance, secure embedded systems, and applied AI, with publications including research on securing third-party HDL IP and security-related data-driven methods.

Invited Talk

Day 2 - Wednesday March 25, 2026

15:30 PM – 15:50 PM

Plenary Session II
Invited Talk



Analog In-Memory Inference across Vision and Language for Edge Intelligence

Session Chairs:

Dr. Irfan Ahmed, Virginia Commonwealth University

Presenter/Speaker:

Dr. Lijun Qian, Prairie View A&M University

Abstract: Analog in-memory computing (AIMC) is a promising compute paradigm to improve speed and power efficiency of neural network inference beyond the limits of conventional von Neumann-based architectures. However, AIMC introduces fundamental challenges such as noisy computations and there lacks a comprehensive understanding of how analog inference generalizes across task domains, precision settings, and architectural scales, and how core design parameters such as cell bits, ADC resolution, and tile size jointly influence model reliability and efficiency. In this talk, we start with benchmarking inference performance of pretrained deep learning models on AIMC simulators. We conduct a comprehensive evaluation of analog inference across both vision and language tasks using three state-of-the-art simulators-CrossSim, AIHWKIT, and MemTorch. Then we systematically quantify how cell precision, ADC resolution, and crossbar tile size influence model accuracy, stability, and efficiency under realistic non-idealities. Results demonstrate that analog inference can achieve within 2-5% of digital baselines when parameters are tuned regarding to layer sensitivity and workload structure. Furthermore, we derive task-aware design guidelines recommendations for vision models and transformer-based NLP tasks based on our findings.

Speaker Bio: Dr. Lijun Qian is Texas A&M University System Regents Professor and AT&T Endowed Professor in the Department of Electrical and Computer Engineering at Prairie View A&M University (PVAMU). He is also the Director of the Center of Excellence in Research and Education for Big Military Data Intelligence (CREDIT Center). He received BE from Tsinghua University, MS from Technion-Israel Institute of Technology, and PhD from Rutgers University. Before joining PVAMU, he was with Bell-Labs Research in Murray Hill, New Jersey. He was a visiting professor of Aalto University, Finland. He led the CREDIT Center to win the first place in the AI tracks at Sea challenge organized by the US Navy, and the first place in the IEEE CyberC Big Data Competition organized by the IEEE Big Data Initiative. He received Best Paper Award in IEEE CAMAD 2025, AIxHEART 2025, IEEE RoboCom 2023, and IEEE Globecom 2017. His research interests are in the areas of big data processing, artificial intelligence, quantum information science and quantum machine learning, wireless communications and mobile networks, network security and intrusion detection, and computational and systems biology.

Invited Talk

Day 2 - Wednesday March 25, 2026

15:50 PM – 16:10 PM

Plenary Session II
Invited Talk

Securing AI with Zero Trust

Session Chairs:

Dr. Irfan Ahmed, Virginia Commonwealth University

Presenter/Speaker:

Al Amin Hossain, United States Air Force (Wright-Patterson AFB)

Abstract: The widespread adoption of artificial intelligence (AI) across mission-critical systems, Internet of Things (IoT) environments, and microelectronics-enabled infrastructures has substantially expanded the cyber-attack surface. Traditional perimeter-based security models are no longer adequate to protect modern AI systems that are highly distributed, data-centric, and continuously evolving. Zero Trust Architecture (ZTA), grounded in the principle of "never trust, always verify," offers a robust, adaptive security paradigm to address these challenges. Accordingly, it is essential to examine the role of Zero Trust as a foundational enabler of secure and trustworthy AI technologies. Our study analyzes the application of Zero Trust principles to AI-enabled enterprise systems, cloud-native platforms, and large language models (LLMs) across the AI lifecycle, including data ingestion, model training, inference, and deployment. Emphasis is placed on least-privilege access, continuous verification, micro-segmentation, and data integrity. The spectacular findings demonstrate that integrating Zero Trust into AI architectures enhances system resilience, mitigates adversarial threats, and enables secure AI deployment within IoT and microelectronics-driven environments.

Speaker Bio: Al Amin Hossain is a DoD SMART Scholar and Computer Scientist with the United States Air Force at Wright-Patterson Air Force Base in Dayton, Ohio. He currently serves as a Lead Computer Scientist supporting the Air Force Life Cycle Management Center (AFLCMC), where he leads technical strategy, planning, and execution for mission-critical modernization efforts, including enterprise logistics and sustainment systems. His work spans Zero Trust and secure AI, low-code/no-code application development (Appian), robotic process automation (RPA) (UiPath, Automation Anywhere), and modernization of enterprise platforms to improve interoperability, scalability, and compliance with DoD standards. He has led multiple RPA and Generative AI initiatives that reduce manual workload and improve operational efficiency, and has contributed to major acquisition and engineering documentation aligned with complex program requirements. He is also pursuing a Ph.D. in Computer Engineering at Wright State University (2023-2027), with research interests at the intersection of AI and cybersecurity. He has received recognition for his research contributions, including a Best Paper Award at IEEE ICAMAC 2025 (Dubai, UAE) for work exploring Zero Trust approaches in modern AI.

Invited Talk

Day 2 - Wednesday March 25, 2026

16:10 PM – 16:30 PM

Plenary Session II
Invited Talk

Auditable AI for Cyber Risk Assessment

Session Chairs:
Dr. Irfan Ahmed, Virginia Commonwealth University

Presenter/Speaker:
Afroz Mohammed, MSB Insurance Agency, Inc

Abstract: Artificial intelligence is increasingly embedded in cybersecurity and risk assessment workflows, influencing how organizations detect, prioritize, and respond to cyber threats. As AI-driven systems become more operationally significant, challenges related to trust, explainability, governance, and auditability have emerged as critical concerns, particularly in regulated and high-assurance environments. This invited talk examines the intersection of artificial intelligence and cybersecurity from an industry perspective, focusing on how AI-enabled risk assessment systems can be designed to support secure, accountable, and auditable operations. Drawing on real-world experience in regulated enterprise environments, including property and casualty insurance, the talk highlights where AI adds value in identifying and prioritizing cyber risk signals while preserving human oversight and control mechanisms. Common failure modes, governance gaps, and assurance challenges are discussed to illustrate why accuracy alone is insufficient for building trustworthy AI in cybersecurity contexts.

Speaker Bio: Mr. Afroz Mohammed is an analytics and risk professional specializing in the application of artificial intelligence to cybersecurity and risk assessment challenges in regulated industries. His work focuses on designing AI-enabled risk frameworks that integrate machine learning insights with governance, explainability, and auditability requirements. Afroz has extensive industry experience in property and casualty insurance, where AI systems are increasingly used to support cyber risk evaluation, operational decision-making, and regulatory compliance. His research on AI-driven risk assessment frameworks has been submitted for peer review with IEEE, and he regularly presents to professional audiences on the practical implications of trustworthy AI, governance, and assurance. Afroz's perspective bridges applied AI research with real-world cybersecurity and enterprise risk operations.

Invited Talk

Day 2 - Wednesday March 25, 2026

16:30 PM – 16:50 PM

Plenary Session II

Invited Talk

Building the Semiconductor Talent Pipeline: How SEMI Foundation Is Aligning the Ecosystem from Discovery to Workforce

Session Chairs:

Dr. Irfan Ahmed, Virginia Commonwealth University

Presenter/Speaker:

Mike Glavin, SEMI Foundation

Abstract: As the semiconductor industry continues to grow, the challenge is no longer simply raising awareness of careers in the field. The real challenge is helping individuals successfully progress from initial exposure to meaningful participation in the workforce. Too often, workforce efforts operate as isolated programs rather than as part of a coordinated pathway. In this session, the SEMI Foundation will highlight how its portfolio of student engagement, career exploration, training, and apprenticeship initiatives works together to support the semiconductor talent pipeline. Underpinning these efforts is the Beyond Awareness framework, an operating model that helps map how individuals move from discovery and curiosity to exploration, training, and ultimately workforce entry. Participants will see how this framework helps connect SEMI Foundation programs across the talent journey, strengthen handoffs between experiences, and provide a clearer way to understand workforce impact. By aligning industry, education, and workforce partners around a shared structure, the SEMI Foundation is helping the semiconductor ecosystem build a more visible, coordinated, and scalable pathway from awareness to careers.

Speaker Bio: Mike Glavin is Program Director of Workforce Development at the SEMI Foundation, where he leads global, employer-driven strategies to strengthen the semiconductor talent pipeline. He oversees SEMI's designation as a U.S. Department of Labor National Registered Apprenticeship Group Sponsor and works with member companies, education systems, and public partners across regions to scale apprenticeship models, build career pathways, and align workforce systems with industry demand. His work supports long-term sector growth in a globally strategic industry. Previously, Mike served as Vice President of Talent at the Greater Cleveland Partnership, leading regional workforce initiatives to expand apprenticeships, internships, and work-based learning across Northeast Ohio, supported by U.S. Department of Labor funding. Earlier, he held leadership roles at Associated Builders and Contractors, advancing apprenticeship policy and industry-led training models. He holds a Bachelor of Science from the University of Richmond and has built his career at the intersection of business, education, and public policy, focused on scalable workforce solutions that enhance economic competitiveness.

Day 2 - Wednesday March 25, 2026

EVENING TECHNICAL SESSIONS (15:00 PM – 16:00 PM)

SaTC Exhibition & Poster Session I
(Sam Housten B)

TRACK CHAIRS:	[Track chair Name] [Track chair affiliation] [Track chair 2 Name] [Track chair 2 affiliation]

Poster Session I: (15:00 PM – 16:00 PM)			
Poster Number	Paper ID	Title	Authors
1	75	Theoretical Analysis of Fidelity and Interpretability Trade-offs in Explainable Artificial Intelligence	Koppanati, Kavyasri; Jakkula, Akshitha; Khan, Muhammad Zubair; Copus,Belinda
2	91	A Conceptual Framework for Multiplayer Mixed Reality Training with Biometric Feedback	Gurung, Karma; Karki, Dhiran; Ghimire, Ashutosh; Amsaad, Fathi
3	213	Fully Autonomous Z-Score–Based TinyML Anomaly Detection on Resource-Constrained MCUs Using Power Side-Channel Data	Albaiz, Abdulrahman; Amsaad, Fathi
4	229	Hybrid Spiking Convolutional Neural Network (H-SCNN) on AudioMNIST	Oliver, Ludvig; Hopkinson, Kenneth
5	232	StressSnap: Data-Driven Modeling of Physiological Parameters for Wearable Stress Monitoring	Krista, Chandrika Mani; Bapatla, Anand Kumar; Khan, Muhammad; Rachakonda, Laavanya
6	249	Secure and Privacy-Preserving Frameworks for IoMT: A Survey of Cryptographic and Blockchain-Enabled Approaches	Abdelraouf, Hussien; Eltoukhy, Ahmed T. ; Fouda, Mostafa M.; Fadlullah, Zubair Md ; Ibrahem, Mohamed
7	254	DeepEdge+Location: A Location-Based Task Orchestrator for Edge Computing	Kyerematen-Boateng, Hubert; Josyula, Darsana; Casbeer, David
8	272	Financial IoT Smishing Detection: Challenges, Gaps, and Research Roadmap	Jurkuch, Abit; Mahgoub, Imadeldin
9	311	Counterfeit RF Fingerprint Detection Using an Autoencoder-Based Approach	Mex Perera, Carlos
10	324	The IoMT Security Trilemma: A Systematic Review of Privacy, Utility, and Resource Efficiency in Federated Edge Learning	Mansour, Samah; Louati, Mahmoud; Kammoun, Islem

Day 2 - Wednesday March 25, 2026

EVENING TECHNICAL SESSIONS (16:00 PM – 17:00 PM)

SaTC Exhibition & Poster Session II (Sam Housten B)

TRACK CHAIRS:	[Track chair Name] [Track chair affiliation] [Track chair 2 Name] [Track chair 2 affiliation]

Poster Session II: (16:00 PM – 17:00 PM)			
Poster Number	Paper ID	Title	Authors
11	333	Pre-ISP Adversarial Patch Detection in RAW Bayer Space for Trustworthy IoT Vision	Anusuya Sijapati (Wright state university)*; Bibek Maharjan (Tribhuvan University); Fathi Amsaad (Wright State University)
12	386	LLM-Assisted Side-Channel Leakage Analysis of AES Power Traces	Sufian Al majmaie; Niraj Prasad Bhatta; Fathi Amsaad
13	1001	Deterministic Integration of MoS2-Graphene Heterostructures for Future Chip-Scale 2D Electronics	Mustafa Ali
14	1002	Side-channel Analysis for Hardware Trojan Detection	Iain White
15	1003	Hardening Serverless Applications via Graph Reachability: Detection and Remediation of Over-Permissioned Policies	Fawaz Abdulwahab
16	1004	Contactless Backdoors: EM-Triggered Payload Insertion in AES-128 FPGA Bitstreams	Christopher Josiah Stance

17:15 PM – 17:30 PM	**Day 2 Closing Remarks from SaTC 2026 Conference Chairs**

Online Sessions

Day 1 - Tuesday March 24, 2026

Online Session: Paper Presentations | 10:00 AM – 12:00 AM

Online Session 1: Assured IoT/Edge Systems, Hardware Trust, and Embedded Security
Room Link: https://meet.google.com/fij-icdz-rrx

TRACK CHAIRS:	Dr. Mohamed El-Hadedy Aly (California State Polytechnic University, Pomona)

10:00 AM – 10:15 AM Paper ID: 22	**Trusted RAN-Edge Digital Twin Framework for Next-Generation IoT Security** *Authors*: Patel, Saurabh *Abstract*: We present a lightweight digital twin framework for the RAN edge that detects security threats using only RF key performance indicators (KPIs). Unlike traditional architectures requiring full network state, our approach combines KPI-only modeling (RSSI, RSRP, SINR, BLER) with HMACSHA256 synchronization and a hybrid anomaly detection engine (statistical rules plus a 3-layer neural network). Evaluation on 100–5000 simulated devices demonstrates effective detection of spoofing (F1=0.92) and KPI manipulation (F1=0.90) with 2–5 second latency and an 8.4% false positive rate. Scalability analysis on Raspberry Pi 4B hardware confirms the framework maintains acceptable performance (62% CPU, 891 MB RAM) up to 500 devices per node, validating its suitability for resource constrained 6G edge deployments.
10:15 AM – 10:30 AM Paper ID: 180	**SecureHLSMem: Memory-Safety Enforcement for High-Level Synthesis of Accelerators** *Authors*: Haque Gazi, Md Mahfuzul; Hossain, M Shifat; Hussain, Arif; Jha, Sumit Kumar; Ahmed, Md Rubel *Abstract*: High-Level Synthesis (HLS) compiles C/C++ kernels into RTL for FPGA and SoC accelerators, but unsafe C/C++ memory semantics, such as out-of-bounds accesses, null dereferences, and overflowed indices, can be synthesized into hardware without any runtime exception mechanism. These violations cause silent data corruption, invalid control-state transitions, or unsafe memory-mapped transactions during FPGA execution. This paper presents SecureHLSMem, an end-to-end memory-safety framework for HLS that combines (i)~lightweight compile-time hazard detection, (ii)~a synthesizable bounds-checking unit (BCU) that enforces spatial safety at runtime, and (iii)~a dynamic sanitization mode that records violations for diagnosis in simulation and on FPGAs. Across representative DSP and ML kernels with seeded vulnerabilities, SecureHLSMem detects all injected hazards and prevents silent corruption, incurring only 2--4\% LUT overhead on average with no observed frequency degradation.

10:30 AM – 10:45 AM Paper ID: 233	**Stealthy Merker Memory Attacks on Siemens S7 Programmable Logic Controllers** *Authors*: Suwal, Anup; SUN, WEIQING; Evans, William *Abstract*: Industrial control systems (ICS) now routinely connect field devices, programmable logic controllers (PLCs), and supervisory networks, leaving safety-critical operations vulnerable to remote attacks. We examine a particular threat to Siemens S7 PLCs: runtime memory manipulation that targets process values and operator displays without modifying the control logic. Attackers can alter Data Blocks and Merker memory to skew the process behavior and falsify HMI readings while the user program remains unchanged. We implemented and tested three memory attacks on a lab water-tank controller to assess their effects and detection challenges. The findings reveal that carefully crafted memory-only attacks, especially those focused on Merker regions, can evade standard program-integrity checks and basic write-pattern monitoring.
10:45 AM – 11:00 AM Paper ID: 234	**AquaScope: A Secure, Edge-Native Framework for Real-Time Aquatic Habitat Monitoring** *Authors*: Rachakonda, Laavanya; Madewell, Matthew; Tarra, Aditya; Serrano, Hector *Abstract*: The escalating volatility of global freshwater ecosystems needs real-time, trustworthy monitoring infrastructures. Traditional Cloud-Centric IoT architectures suffer from latency and vulnerability to adversarial data poisoning at the unattended edge. AquaScope, a resilient, edge-native framework for secure environmental sensing, is presented to address these challenges. This system integrates a multi-variate sensor array with a lightweight Edge Security Kernel that executes a temporal anomaly detection algorithm. By shifting the computational burden of the Habitat Suitability Index (HSI) from the cloud to the edge, AquaScope ensures data integrity and operational continuity during network partitions. Experimental evaluation confirms the system's ability to autonomously filter sensor spoofing attacks with negligible latency (< 20 ms) while maintaining high predictive accuracy for aquatic species presence.

11:00 AM – 11:15 AM Paper ID: 255	**Unsupervised Module Boundary Identification in FPGA Netlists using Structural Graph Hashing** *Authors*: Nathamuni Venkatesan, Aparajithan; Vemuri, Ranga; Emmert, John *Abstract*: FPGA reverse engineering enables intellectual property theft, hardware trojan insertion, and vulnerability analysis by reconstructing high-level designs from synthesized netlists. Existing approaches struggle with optimization-induced structural transformations that obscure module boundaries. We present an unsupervised algorithm that reconstructs RTL module boundaries from primitive-level FPGA netlists using structural fingerprinting via Weisfeiler-Leman graph hashing, locality-sensitive hashing for candidate generation, and DBSCAN clustering. Our approach targets datapath-intensive designs with repeated computational modules (DSP, arithmetic, signal processing cores). Evaluation across six OpenCores DSP designs and 24 designoptimization combinations demonstrates 97.3% mean module family identification accuracy under hierarchy-preserved synthesis for forward-dataflow architectures (cascade filters, CORDIC, transform circuits). CORDIC designs maintain 99.7-100% accuracy with minimal variation (0.0% std dev) across synthesis optimization levels, while transform circuits achieve 88.5-96.7%. Under realistic default synthesis configuration, CORDIC designs maintain 97.7-100% accuracy, transform circuits achieve 79.9-80.4%, cascade filters 89%, and feedback systems 31%, revealing which computational patterns survive aggressive synthesisinduced structural transformation. The work provides insights for IP protection and enables architectural reconnaissance for security analysis.
11:15 AM – 11:30 AM Paper ID: 264	**Physical Evaluation of Naturalistic Adversarial Patches for Camera-Based Traffic-Sign Detection** *Authors*: D'Urso, Brianna ; Sakib, Tahmid Hasan ; Hasan, Syed Rafay *Abstract*: This paper studies how well Naturalistic Adversarial Patches (NAPs) transfer to a physical traffic sign setting when the detector is trained on customized dataset for autonomous vehicle (AV) environment. We construct a composite dataset, CompGTSRB (which is customized dataset for AV environment), by pasting traffic sign instances from the German Traffic Sign Recognition Benchmark (GTSRB) onto undistorted backgrounds captured from the target platform. CompGTSRB is used to train YOLOv5 model and generate patches using a Generative Adversarial Network (GAN) with latent space optimization, following existing NAP methods. We carried out a series of experiments on our Quanser QCar testbed utilizing the front CSI camera provided in QCar. Across configurations, NAPs reduce the detector's STOP class confidence. Different configurations includes distance, patch sizes, and patch placement. These results along with a detailed step-by-step methodology indicate the utility of CompGTSRB dataset and the proposed systematic physical protocols for credible patch evaluation. The research further motivate reseaching the defenses that address localized patch corruption in embedded perception pipelines.

11:30 AM – 11:45 AM Paper ID: 278	**Hardware Trojan Detection through Electro-optical Frequency Mapping Combined with Test Patterns** *Authors*: Farhan, Mohammad; Shen, Haoting *Abstract*: Due to the high cost of establishing and maintaining semiconductor manufacturing plants, today, most integrated circuit (IC) chip designers rely on fabless operations and offshore fabrication from third-party foundries. Unfortunately, the foundries may be in-line with potential adversaries that can perform malicious modifications to the original design during the fabrication, which are known as hardware Trojans. Various hardware Trojan detection techniques have been reported. However, the detection based on invasive imaging technique is efficacious but damages the tested chip, while the non-invasive detection based on electrical testing and/or side-channel analyses have challenges with stealthy hardware Trojans. In this paper, we propose a non-invasive hardware Trojan detection technique that is designed to capture the gate-level difference between the original layout design and the fabricated IC chip. The proposed technique combines electrical testing and electro-optical frequency mapping to track the optical behavior of logic gates during switching, with coverage up to 100% within a reasonable time frame. A comparison will be performed between the original design and the fabricated chip to detect the suspicious modifications, where no "golden chip" is required.
11:45 AM – 12:00 AM Paper ID: 282	**NEITH: Networked Evidence Integrity for Telemetry Hashing** *Authors*: El-Hadedy, Mohamed *Abstract*: Autonomous platforms rely on high-rate multi-sensor telemetry (e.g., Global Navigation Satellite System (GNSS) and LiDAR) for safety, accountability, and post-incident reconstruction, yet disputes often reduce to a basic question: what data was actually retained. This paper presents NEITH, a lightweight window-commitment contract that makes retention externally checkable without trusted storage or full log replication. NEITH partitions time into windows of length Δ. Within each window, each ingested chunk is mapped to a leaf position from ingestion-observable metadata (sensor identifier and per-window index) and aggregated with standard hash functions and extendable-output functions (XOFs) in a Merkle-style tree, yielding one constant-size root Rt (32 bytes) per window. Later, a verifier checks retention claims from the published roots and a short inclusion proof (Rt, c, π); an optional order rule also makes within-window reordering detectable. NEITH runs on a small edge Kubernetes cluster and is evaluated with u-blox GNSS and Youyeetoo LiDAR streams plus bursty synthetic producers. Over 32 consecutive windows (Δ = 10 s), the system emits one root per window and stays aligned to the window schedule. Microbenchmarks on 8 KiB leaves show that widely used tree-hash designs sustain 5–26 MB/s under 1/8/32 concurrent connections, whereas a reference Python ASCON-XOF baseline costs approximately 760 ms per 8 KiB leaf, indicating when the no-stutter timing bound cannot be met on this software stack. Overall, window commitments provide a practical integrity layer for verifiable telemetry retention on resource-constrained cyber-physical pipelines.

Day 1 - Tuesday March 24, 2026

Online Session: Paper Presentations | 10:00 AM – 12:00 AM

Online Session 2: Network and Communication Security, Authentication, and Quantum-Safe IoT

Room Link: https://meet.google.com/yxy-yekw-fvo

TRACK CHAIRS:	Dr. Robert Joseph Hayek (Argonne National Laboratory)

10:00 AM – 10:15 AM Paper ID: 28	**Optimizing Task Scheduling in Fog Computing with Deadline Awareness** *Authors*: Sirjani, Mohammad Sadegh; Ahmad, Mohammad; Mousavi, Amir; Nourbakhsh, Erfan; Nguyen, Khoa; *Abstract*: The rise of Internet of Things (IoT) devices has led to the development of numerous time-sensitive applications that require quick responses and low latency. Fog computing has emerged as a solution for processing these IoT applications, but it faces challenges such as resource allocation and job scheduling. Therefore, it is crucial to determine how to assign and schedule tasks on Fog nodes. This work aims to schedule tasks in IoT while minimizing the total energy consumption of nodes and enhancing the Quality of Service (QoS) requirements of IoT tasks, taking into account task deadlines. This paper classifies Fog nodes into two categories based on their traffic level: low and high. It schedules short-deadline tasks on low-traffic nodes using an Improved Golden Eagle Optimization (IGEO) algorithm, an enhancement that utilizes genetic operators for discretization. Long-deadline tasks are processed on high-traffic nodes using reinforcement learning (RL). This combined approach is called the Reinforcement Improved Golden Eagle Optimization (RIGEO) algorithm. Experimental results demonstrate that RIGEO achieves up to a 29% reduction in energy consumption, up to an 86% improvement in response time, and up to a 19% reduction in deadline violations compared to state-of-the-art algorithms.
10:15 AM – 10:30 AM Paper ID: 162	**Securing IoT Devices in the Quantum Era: AI-Based Detection with Hybrid Post-Quantum Encryption** *Authors*: yaaqub, zina; Sarmad, Maryam *Abstract*: With the advancement of quantum computing, the long-term security of IoT systems is increasingly challenged, particularly due to the vulnerability of traditional public-key cryptography. This study integrates artificial intelligence (AI) with a hybrid strategy that involves Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) to address this challenge. Incoming traffic from the TON-IoT dataset is processed by AI using XGBoost, Random Forest, and One-Class SVM as anomaly-detection filters. Only traffic classified as normal is forwarded to the encryption phase. Post-quantum key establishment is performed using Kyber-512, and the resulting shared secret is combined with simulated BB84-based QKD key material via a key-derivation function (KDF) to derive a 256-bit session key, which is then used with AES-256-GCM for authenticated IoT data encryption. Experimental results demonstrate that the hybrid algorithm, along with the AI, can effectively improve IoT security. Upon optimization of the parameter β (=1.0), the Delivery Purity is 0.92, the Data Delivery rate is 0.80, and the Secure Delivery Fβ score is 0.94 compared to Delivery Purity of 0.77, Delivery Rate of 1.0, and Secure Delivery Fβ score of 0.87, respectively, without AI.

10:30 AM – 10:45 AM Paper ID: 165	**PQ-MQTT: A Hybrid Post-Quantum Secure Communication Protocol for MQTT-Based IoT Networks** *Authors*: Saleem, Sohaib; Umran, Samir M.; Abduljabbar, Zaid Ameen; Perazzo, Pericle; Saleem, Uzair *Abstract*: The proliferation of Internet of Things (IoT) devices that use the Message Queuing Telemetry Transport (MQTT) protocol poses significant security challenges in the emerging quantum computing era. Current Transport Layer Security (TLS) implementations rely on classical cryptographic algorithms vulnerable to Shor's algorithm. This paper proposes PQ-MQTT, a hybrid post-quantum secure communication protocol that integrates ML-KEM-768 with X25519 for key encapsulation and a lightweight session-key derivation mechanism optimized for resource-constrained IoT publishers. We present a formal security analysis under the Quantum Random Oracle Model (QROM), demonstrating resilience against store-now-decrypt-later attacks. Experimental evaluation on the Raspberry Pi 4, ESP32, and Arduino Nano 33 platforms shows that PQ-MQTT achieves handshake latencies of 127.3ms, 412.7ms, and 1,847.2ms, respectively, with 18.2KB of additional memory overhead. A comparative analysis of pure post-quantum and classical TLS implementations shows energy reductions of 23.5%-40.5% relative to pure PQC, achieved through our hybrid optimization approach, while maintaining 94.2% throughput efficiency.
10:45 AM – 11:00 AM Paper ID: 182	**Hybrid Harris Hawks–Grey Wolf Optimizer in Ad Hoc networks: An In-depth Analysis of Structure, Performance and Limitations** *Authors*: AL-Asadi, Hamid *Abstract*: Based on the growing complexity of dynamic ad hoc networks like MANETs, VANETs, WSNs, and FANETs, new types of hybrid metaheuristics such as the Hybrid Harris Hawks-Grey Wolf Optimizer (HHGWO) will make it possible for networks designed using a new smart structure. Nature-based metaheuristic algorithms like the Grey Wolf Optimizer (GWO) and Harris Hawks Optimizer (HHO) should be and can be hybridized for improved network optimization. Mostly theoretical at this stage, HHGWO has been tested ONLY within very specific, simplified test environments. As a result, there has been no consistent framework for evaluation of real-world performance, different kinds of challenges, and/or limits on time and resources. This is especially true when assessing HHGWO for core optimization on critical issues of energy preservation and topological balance, within highly dynamic, uncertain environments, particularly hard network setups. This research perspective has the potential to temper HHGWO as a pure theoretical construct, and as a real designed intelligence capable of autonomous network management

11:00 AM – 11:15 AM Paper ID: 202	**An Improved SMS Security Technique to Avoid Plaintext and Dictionary Attacks** *Authors*: Zam Zam Mirza, Qurat Ul Ain ; Ashraf, Humaira; Kanwal, Rimsha ; Jhanjhi, NZ. *Abstract*: In the era of flourishing digital communication and the unprecedented surge in mobile device usage, securing message transmission has become paramount. The prevalence of short messaging services (SMS) intensifies the demand for robust security measures to safeguard the privacy of smartphone users. ”Security” is a crucial component in this kind of circumstance. Encryption is one method that’s frequently utilized to offer security. It protects the original raw data from in-trusion and plays a crucial function when private data is moving via the network. This research introduces an innovative approach to DNA Cryptography, leveraging a dynamic DNA sequence table to enhance security in SMS communications. The proposed Efficient Cryptographic Scheme for SMS (ECSS) algorithm employs DNA molecules and strands to encrypt information, ensuring a high level of confidentiality for texts received on Android smartphones. ECSS cryptography focuses on preserving the secrecy of data transfer over networks. The paper explores the nuances of DNA Crypto, distinguishing it from classical cryptography and elucidating the process of DNA Data encryption. An Androidbased application is developed to implement the proposed technique, demonstrating consistent encryption results where the length of the message remains unchanged after decryption. The security solution exhibits potential for significantly enhancing mobile communication security. The study also presents experimental results, including received text message accuracy, cipher text, average encryption time, and average decryption time. The findings reveal an average encryption and decryption speed of approximately 0.011 and 0.037 seconds, respectively, effectively thwarting plaintext and dictionary attacks.
11:15 AM – 11:30 AM Paper ID: 204	**Adaptive Quality of Experience Optimization in Wireless Multimedia Sensor Networks: A Cross-Layer Analytical Approach** *Authors*: AL-Asadi, Hamid *Abstract*: The paper introduces a cross-layer analytical model of the optimization of the Quality of Experience (QoE) in the Wireless Multimedia Sensor Networks (WMSNs). The proposed strategy combines parameters at the physical, network and application layers to enforce dynamic adjustment of the multimedia transmission when conditions in the network change. The model allows real-time regulation of the encoding rate and the routing path by taking into account the joint influence of such factors as the packet loss, delay, jitter, and perceptual video quality to attain increased satisfaction of end-users. The model incorporates a real-time adaptive control mechanism that continuously adjusts video bitrate, routing decisions, and transmission power based on ongoing QoE estimation. Lightweight feedback loops operating across the physical, network, and application layers, enabling the system to react instantly to variations in channel quality, delay, and packet loss, govern these adjustments. The analytical controller applies gradient-based update rules to maintain optimal QoE while respecting energy constraints, ensuring efficient and perceptually aware multimedia delivery. Findings of the simulation show that the adaptive mechanism can greatly enhance the QoE measures with energy efficiency and network stability as compared to the conventional QoS-based schemes. The results indicate that user-centric design is significant in the design of intelligent WMSN systems in multimedia applications.

11:30 AM – 11:45 AM Paper ID: 274	**Stateless Per-Packet IoT Authentication Framework Using Machine Learning** *Authors*: El-Said, Mostafa; Sherman, Nate *Abstract*: Securing Internet of Things (IoT) devices remains a critical challenge due to constrained device resources, limited authentication mechanisms, and the lack of IoT-specific security datasets. This paper presents a stateless, per-packet authentication framework that integrates traditional TCP state validation with machine learning (ML) based classification, implemented using Microsoft Azure cloud services. A synthetic IoT network traffic generator was developed to address the scarcity of public datasets, enabling large-scale model training and controlled experimentation. Using Azure Machine Learning AutoML, a Voting Ensemble model achieved 96.9% accuracy when trained on 200,000 simulated packets. The trained model was deployed within a real-time Azure pipeline incorporating IoT Central, Event Hubs, Azure Functions, and SQL Database services. Due to cloud resource constraints, live evaluation was conducted on approximately 450 packets, during which 64.4% of traffic was filtered by TCP state validation prior to ML inference, demonstrating the effectiveness of multilayered security triage. Although latency was elevated because of non-production Azure components, the results validate the feasibility of combining lightweight protocol validation with machine learning to enhance IoT authentication. Beyond research contributions, the proposed framework provides a realistic, scalable environment testbed suitable for research and teaching cloud-based IoT and cybersecurity concepts.
11:45 AM – 12:00 AM Paper ID: 303	**Post-Quantum Authentication for Resource-Constrained IoT: A Comparative Study of Hash-Based Signatures on RP2350** *Authors*: Wimal, Kesara; Cullen, Gary; Greaney, Paul *Abstract*: The emergence of quantum computing threatens classical cryptographic systems protecting IoT infrastructure. This study addresses the challenge of implementing post-quantum authentication on resource-constrained devices by evaluating hash-based signature schemes on the RP2350 microcontroller. Three authentication approaches are implemented and benchmarked: HMAC-SHA256 (classical baseline), Lamport one-time signatures, and Winternitz one-time signatures with Merkle trees. All implementations integrate Physical Unclonable Functions (PUF) for hardware-rooted key derivation, eliminating persistent key storage vulnerabilities. Experimental evaluation across three Raspberry Pi Pico 2 W devices measures key generation time, signing latency, verification overhead, memory consumption, and transmission size under realistic temperature sensor workloads. Results demonstrate that Winternitz signatures achieve post-quantum security with 2.1KB signatures and 55-183ms signing time, representing 74% size reduction and 3× performance improvement over Lamport while maintaining equivalent security. A hybrid authentication model is proposed, combining Winternitz signatures for periodic device authentication with HMAC for continuous sensor data transmission, balancing post-quantum security with operational efficiency. This work provides the first comprehensive performance characterisation of hash-based signatures on RP2350, offering practical guidance for IoT developers transitioning to post-quantum cryptography in resource-constrained environments.

Day 1 - Tuesday March 24, 2026

Online Session: Paper Presentations | 10:00 AM – 12:00 AM

Online Session 3: Distributed and Cloud Systems Security, Privacy, and Data Integrity
Room Link: https://meet.google.com/koq-bocg-evb

TRACK CHAIRS:	Dr. Anand Bapatla (University of Central Missouri)

10:00 AM – 10:15 AM Paper ID: 35	**Federated Learning and Generative AI for Privacy-Preserving FinTech Cybersecurity** *Authors*: Venkatachalam, Prakasam *Abstract*: FinTech ecosystems—including digital banking, mobile wallets, cryptocurrency platforms, and wealth management systems—have created unparalleled attack surfaces for professional cybercriminals. Privacy risks, computational latency constraints, and scalability issues hinder traditional centralised cybersecurity systems' ability to safeguard FinTech applications. This paper introduces a FinTech-specific Adaptive Threat Intelligence Framework that merges Federated Learning (FL) and Generative Adversarial Networks (GANs) to provide decentralised, privacy-preserving, and real-time defence against evolving cyber threats. The proposed framework allows distributed FinTech nodes to collaborate on model training without exposing sensitive customer or transaction data. At the same time, conditional GANs generate synthetic fraud and cyberattack scenarios to improve anomaly detection. Extensive testing on benchmark datasets shows outstanding performance (92% accuracy, 90% precision, 91% recall, 1.4 seconds latency) with strong privacy guarantees ($\varepsilon < 1.0$). This framework addresses the particular cybersecurity needs of FinTech infrastructure with a scalable, regulation-compliant, and resilient solution.
10:15 AM – 10:30 AM Paper ID: 36	**Neural Representation Learning and Privacy-Preserving Cloud–Edge Collaboration for Next-Generation Financial Wealth Management Platforms** *Authors*: Venkatachalam, Prakasam *Abstract*: Wealth management must be innovative, private, and transparent as financial ecosystems become more complicated. NeuroWealth, a neural representation and privacy-aware framework for next-generation financial systems, integrates graph neural networks (GNNs), transformer-based temporal learning, and federated cloud–edge collaboration. To provide accurate, adaptable, and explainable investment suggestions, the system records relational and temporal relationships among people, institutions, and goods. NeuroWealth solves new client and product cold-start issues with meta-learning (MAML) and content-collaborative embeddings. The methodology ensures GDPR and MiFID II model interpretability and compliance via SHAP-based explainability and counterfactual reasoning. Federated learning (FL) with differential privacy (DP) protects sensitive financial data while retaining usefulness. Experiments on actual and synthetic datasets show 17.6% improvement in NDCG, 31% reduction in cold-start error, and 0.84–0.92 compliance with essential regulations in terms of explainability. Live benchmarks show 120 ms latency and 15,000 requests/sec throughput, showing NeuroWealth's large-scale viability. The platform provides scalable, safe, and interpretable AI for personalised financial wealth management

10:30 AM – 10:45 AM Paper ID: 179	**Blockchain-Based Document Verification System Using Ethereum Smart Contracts and Cryptographic Hashing** *Authors*: Islam Khan, Md. Mazenul; Nafi, Akib Sadman; Ullah, Kazi Refat; Hossain, Jonayed; Haque Dhrubo, Ahmed Faizul; Pramanik, Souvik; Qayum, Mohammad Abdul *Abstract*: In this paper, we presented an e-Registry prototype that builds on the decentralized and tamper-evident nature of Ethereum to authenticate digital documents. The system is a gas-efficient Smart Contract on the Ethereum blockchain that stores SHA-256 hashes of documents, so your sensitive files are secure with us, but we don't know what they are! Accessible through a web-based user interface using MetaMask for transaction signing and the Web Crypto API for client- side hashing of documents offers an intuitive privacy-preserving process. Finally, system diagnostics and security reports can be generated using Python-based tools and hashed to store on the blockchain for validation. Running on the Ethereum Sepolia testnet, the system provides practical efficiency, with transaction fees of 0.0005-0.001 SepoliaETH and verification delay less than 3 seconds. This provides an alternative to traditional centralized verification systems that suffer from single points of failure, lack of transparency, and reliance on third-party services by offering a secure and tamper-resistant decentralized proof of existence for digital files.
10:45 AM – 11:00 AM Paper ID: 220	**A Hybrid PQC-Enabled Attribute and Data Encryption Pipeline for Next-Generation Metaverse Platforms** *Authors*: Malik, Javairia; Ashraf, Humaira ; Jhanjhi, Nz ; Ihsan, Uswa *Abstract*: The metaverse requires secure, low-latency, and finegrained access control mechanisms capable of supporting realtime communication and high-volume immersive data. Conventional Ciphertext-Policy Attribute-Based Encryption (CP-ABE) schemes are unsuitable for these environments because their computational overhead grows with the number of attributes and policy complexity, leading to unacceptable latency for resourceconstrained VR/AR devices. To address this challenge, this paper proposes a hybrid post-quantum CP-ABE framework that encrypts only a compact AES session key under attribute-based policies, while large metaverse data objects are protected using AES-GCM. This design ensures that CP-ABE operations remain lightweight and independent of payload size, enabling efficient real-time data sharing.The framework incorporates a dual-plane architecture consisting of a Quantum-Resilient Control Plane which utilizes Kyber Key Encapsulation Mechanisms (KEM) for secure channel establishment and Dilithium signatures for identity assurance and a Low-Latency Data Plane, where avatars execute only symmetric-key operations. Heavy CP-ABE decryption tasks are delegated to a dedicated Decryptor Peer (DP), substantially reducing client-side computation and improving scalability across diverse metaverse scenarios.An evaluation of the proposed approach demonstrates that CP-ABE latency remains nearly constant across attribute sets ranging from 2 to 2000, while AES-GCM maintains stable performance regardless of policy size.Overall, the proposed framework offers quantum-resilient security, fine-grained attribute enforcement, and low-latency performance, establishing a practical and scalable solution for secure real-time metaverse communication

11:00 AM – 11:15 AM Paper ID: 300	**Secure, Smart, Automated, and Privacy-Preserving Cybersecurity Policy Compliance Framework for Sensitive Data Protection** *Authors*: Owusu-Tweneboah, Jemima ; Altarawneh, Amani *Abstract*: Cybersecurity regulatory and compliance frameworks such as NIST SP~800-53 Rev.~5, the HIPAA Security Rule, and the GDPR define essential security and privacy obligations for healthcare information systems and their supporting infrastructures. Despite their critical role, compliance assurance in healthcare is predominantly manual and centered on periodic, point-in-time assessments, relying on human interpretation of regulatory requirements and fragmented evidence collection. As healthcare ecosystems evolve toward distributed systems and extensive third-party participation, there is a growing need for compliance mechanisms that enable continuous assurance, verifiable accountability, and privacy-preserving enforcement across organizational boundaries. This paper proposes SSAP-CPCF, a Secure, Smart, Automated, and Privacy-Preserving Cybersecurity Policy Compliance Framework that integrates permissioned blockchain orchestration, LLM-assisted regulatory interpretation with human validation, and zero-knowledge proof–based verification. The framework explicitly encodes regulatory authority, assessor oversight, and multi-party approval into its protocol design, ensuring that automation enforces, rather than replaces, governance structures. SSAP-CPCF treats compliance as an enforceable system property by binding assessments to vendor-declared obligations and enforcing approval and oversight requirements at the ledger level, ensuring integrity, auditability, and separation of authority. A prototype implemented on a multi-organization Hyperledger Fabric network demonstrates the feasibility of privacy-preserving, ledger-enforced compliance automation in realistic multi-stakeholder settings.
11:15 AM – 11:30 AM Paper ID: 338	**Practical Secure ECG Abnormality Queries by Cloud-Assisted for Biosignal-based Monitoring** *Authors*: To, Ngoc M.; Dinh, Minh N.; Kumar, Dinesh; Tran, Viet Xuan Phuong *Abstract*: With the advancement of cloud-connected wearable electrocardiogram (ECG) devices, continuous monitoring of cardiovascular health has been enabled at scale but also introduces significant privacy and security risks. These generate vast amounts of sensitive data such as critical cardiac biomarkers, but current transmission and storage methods often leave them unprotected. This can be misused by third parties to infer hidden abnormalities, creating risks for employment or insurance discrimination and targeted persuasion. While there are cryptographic solutions, they tend to compromise clinical usability or computational efficiency, making them impractical for real-time applications on edge devices. There is an urgent need for a light-weight query-driven encryptor to ensure the privacy of the ECG data. This paper presents a practical design for securely and easily querying cloud-stored encrypted data. The proposed system enables authorised users, such as clinicians, to perform encrypted searches for specific cardiac abnormalities without decrypting patient records. Our method ensures privacy throughout computation and transmission while supporting meaningful clinical analytics. To demonstrate real-world feasibility, the framework is implemented in a distributed edge–cloud setting, with an ultra-low-power Arduino Nano 33 IoT device acting as the ECG data source and a cloud server performing encrypted query processing. Experimental evaluation shows that the proposed approach achieves accurate query matching with minimal latency and low computational overhead, making it suitable for continuous monitoring and scalable deployment. This work contributes a practical solution for privacy-preserving analytics in distributed healthcare systems, bridging the gap between cryptographic security and deployable cloud-based medical monitoring.

11:30 AM – 11:45 AM Paper ID: 360	**Secure and Scalable IoT Data Sharing with Dynamic Group Management via Re-Encryption** *Authors*: Zhang, Bowu *Abstract*: Despite its growing popularity, the Internet of Things (IoT) poses significant challenges to data security and user privacy. These challenges stem from ubiquitous data access, device heterogeneity, and, most critically, the lack of effective security mechanisms such as robust encryption and access control. Existing IoT security solutions often suffer from low efficiency and limited scalability, making them unsuitable for deployment across large-scale IoT networks with constrained computational resources. To address these issues, we propose a new secure data collection and sharing scheme tailored for IoT applications. Specifically, we leverage Partially Homomorphic Encryption (PHE) to strengthen data security by supporting secure temporal data association. Furthermore, we design flexible data sharing mechanisms, including group-based sharing that utilizes re-encryption to efficiently handle dynamic membership changes within IoT groups. Our analysis demonstrates that the proposed scheme not only offers strong cryptographic guarantees for both data collection and sharing but also achieves high efficiency in managing dynamic group keys, making it well-suited for resource-constrained IoT environments.
11:45 AM – 12:00 AM Paper ID: 382	**Cloud Reliability Analysis via Log-Based Anomaly Detection: An End-to-End Evaluation on HDFS** *Authors*: Thomas Kidu, Vignesh R. Babu, Alex Zhu *Abstract*: Modern cloud systems generate high-velocity log streams across distributed services that provide fine-grained signals for reliability monitoring and incident triage, yet manual monitoring and rule-based alerting do not scale and often miss emerging failure modes. This paper evaluates log-based anomaly detection for cloud reliability on the Hadoop Distributed File System (HDFS) dataset using a practical, reproducible pipeline built on structured LogHub artifacts. We compare unsupervised count-based baselines (Isolation Forest and an autoencoder) with a sequence-aware DeepLog-inspired model that fuses ordered event sequences and event-count statistics using bidirectional LSTM layers under heavy class imbalance. We also present an interactive monitoring dashboard that surfaces anomaly predictions and reliability-oriented summaries. On 575,061 HDFS block traces with 29 event templates, the final model reaches Precision 0.965, Recall 0.999, and F1 0.982 on the held-out test split.

Invited Talk

Room Link: https://meet.google.com/fij-icdz-rrx

Day 1 - Tuesday March 24, 2026

13:00 PM – 13:30 PM

Plenary Session I
Invited Talk

Neuromorphic Microelectronics for Enabling Secure Edge Intelligence

Session Chairs:
Dr. Omar Darwish, Eastern Michigan University

Presenter/Speaker:
Dr. Steven Harbour, Director of AI Hardware Research, Parallax Advanced Research

Abstract: As artificial intelligence transitions from cloud-based systems to edge-deployed autonomous platforms, traditional computing architectures face significant limitations in power efficiency, adaptability, and resilience. Neuromorphic hardware, inspired by biological neural systems, offers a transformative approach to enabling real-time cognition, ultra-low-power computation, and mission-resilient AI at the edge. This presentation explores the development of neuromorphic microchips based on Spiking Neural Networks (SNNs) and nanoscale circuit architectures designed to support trusted, secure, and adaptive AI systems. Emphasis is placed on hardware-software co-design, energy-efficient processing, and architectural innovations that enable robust operation in contested and high-consequence environments. Applications across aerospace, ISR, autonomous systems, and human-autonomy teaming are discussed, along with the technical challenges of scaling neuromorphic solutions for defense and commercial deployment. The findings highlight how next-generation AI hardware can enhance system resilience, reduce latency, and enable secure, trustworthy autonomous capabilities in microelectronics-driven environments.

Speaker Bio: Dr. Steven D. Harbour is the Director of AI Hardware Research at Parallax Advanced Research, where he leads advanced neuromorphic computing and artificial intelligence hardware initiatives within the Center of Excellence. With more than 30 years of experience in aerospace engineering, microelectronics, and defense research, he brings deep technical leadership across neuromorphic engineering, microchip design, AI/ML hardware acceleration, cybersecurity, human-autonomy teaming, avionics, and autonomous systems. He serves as Principal Investigator of the BRAIN program, a cutting-edge neuromorphic chip effort focused on nanoscale architectures and Spiking Neural Network (SNN)-based microcircuit design for resilient, low-power AI hardware. Dr. Harbour has authored over 50 publications in nanotechnology, nanoscale systems, and AI-enabled hardware design. Previously, he served as Global Hawk Chief of Avionics Engineering, supporting the Air Force Research Laboratory Sensors Directorate and the Air Force Life Cycle Management Center at Wright-Patterson Air Force Base. A former USAF fighter flight test pilot with over 5,000 flight hours in multiple aircraft platforms, he combines operational aviation experience with advanced research leadership. He holds a Ph.D. in Neuroscience (Neuromorphics, AI/ML), an M.S. in Aerospace Engineering & Mathematics, and a B.S. in Electrical Engineering, and also teaches at the University of Dayton and Sinclair College.

Invited Talk

Room Link: https://meet.google.com/fij-icdz-rrx

Day 1 - Tuesday March 24, 2026

13:30 PM – 14:00 PM

Plenary Session I
Invited Talk

AI in Energy Management

Session Chairs:

Dr. Omar Darwish, Eastern Michigan University

Presenter/Speaker:

Dr. Antonio Sanfilippo, CTO, AgriTech Forward Inc. / Editor-in-Chief, Green Technology, Resilience, and Sustainability Journal

Abstract: As energy systems grow in complexity due to the increasing integration of renewable energy and the electrification of transportation, Artificial Intelligence (AI) and digitalization have arisen as the prime technologies to address emerging challenges. Machine learning, multi-agent simulations, optimization and game theory methods are being successfully applied to a number of energy management tasks, with the support of robotics, Internet of Things (IoT) and cloud/edge computing technologies. The goal of this talk is to provide a venue for a deep dive into the AI and digitalization ecosystem for energy management through a review of the state-of-the-art and the identification of future directions.

Speaker Bio: With over three decades of experience, Dr. Sanfilippo specializes in advancing sustainable AI solutions in renewable energy, food resilience, homeland security, and healthcare. Currently, he is Chief Technology Officer at AgriTech Forward Inc. and serves as the Editor-in-Chief for Springer Nature's Green Technology Resilience and Sustainability journal. From 2014 through 2025, he was Chief Scientist at Qatar Environment and Energy Research Institute, where he led the energy management program. Under his leadership, the Program established renewable energy and smart grid capabilities that have become national benchmarks, including a large network of solar monitoring stations and a 100 kWp microgrid testbed. Prior to QEERI, Dr. Sanfilippo was Chief Scientist at the Pacific Northwest National Laboratory in the US, where he was awarded the Laboratory Director's Award for Exceptional Scientific Achievement. He led multidisciplinary research projects for various government agencies (DHS, NIH, DOE, NSF) and directed an advanced laboratory research initiative on predictive analytics focused on security, energy and environment applications. Dr. Sanfilippo has also held positions as Research Director in the private sector, Senior Consultant at the European Commission, and Research Supervisor and Group Manager at SHARP Laboratories of Europe. He conducted his early research in Computational Linguistics at the University of Cambridge, and the University of Edinburgh where he completed his PhD in Cognitive Science. He holds 9 patents and has over 200 publications.

Day 1 End

Day 2 - Wednesday March 25, 2026

Online Session: Paper Presentations | 08:30 AM – 10:30 AM

Online Session 4: Trustworthy AI for Threat Detection, Malware Analysis, and Cyber Defense

Room Link: https://meet.google.com/fij-icdz-rrx

TRACK CHAIRS:	Dr. Faris Alsulami (University of Jeddah)

08:30 AM – 08:45 AM Paper ID: 32	**Hybrid Deep Learning Models For Detecting Anomalous Behavior in Peer-To-Peer Payment Systems** *Authors*: Selvam, Muthu *Abstract*: The rising use of real-time peer-to-peer (P2P) payment technologies like RTP, Zelle, and ACH has increased banking industry fraud efforts that are nuanced, fast-evolving, and hard to intercept using standard rule-based systems. This research introduces a hybrid deep learning system that detects P2P payment transaction abnormalities using CNNs and LSTM networks. The model detects fraud by learning spatial patterns from transaction data and temporal relationships in sequential behaviour. The system outperformed traditional methods by 8.6% in detection accuracy and 23% in inference time on real-world financial datasets with 94.2% precision and 92.8% recall. Experimental results show statistically significant increases in detection and inference efficiency over competing baselines. Results suggest real-time financial systems are feasible, but large-scale production validation is needed. The framework supports scalable adaptive fraud detection in current digital payment infrastructures.
08:45 AM – 09:00 AM Paper ID: 190	**Hybrid Ransomware Detection Model Using Dynamic Behavioral** *Authors*: Faisal Saeed, Muhammad ; Tahir, Sidra ; Sarwar, Sumaira *Abstract*: Ransomware are one of the biggest challenges to the cybersecurity. This malware is continuously evolving using advanced obfuscation and signature- evasion techniques. The traditional methods become ineffective to detect this continuously evolving malware. This research proposes a hybrid two-stage ransomware detection framework which uses dynamic behavioral analysis with the deep learning models to improve accuracy and adaptability. In the first stage, it dynamically analyzes system-level behavioral data like API call sequences, registry modifications and file system activities using Bidirectional LSTM- based sequence autoencoder (BiLSTM-AE). In the second stage, a Deep Neural Network (DNN) learns the temporal and semantic patterns in these behaviors to differentiate between the legitimate software programs and malware. This hybrid-framework is de- signed to minimize false negatives and keeping the false positives at a very low level for the early and reliable detection of the malware. The model is trained in a sandbox environment with the diverse dataset of both ransomware and normalware samples. This study develops an automated, strong and intelligent solution which could keep up with the evolving ransomware environment.

09:00 AM – 09:15 AM Paper ID: 260	**Zero-Shot Network Intrusion Detection Using Semantic Learning and CVAE Augmentation** *Authors*: Hasan, Kamrul; Mansour, Samah; Ogamba, Hilda *Abstract*: Detecting previously unseen cyber attacks remains a significant challenge for conventional intrusion detection systems, which depend heavily on labeled training data and often struggle to generalize to emerging threats. To address this limitation, this work introduces a zero-shot network intrusion detection framework that integrates a semantic bottleneck with Condi- tional Variational Autoencoder (CVAE)–based data augmentation to facilitate knowledge transfer across heterogeneous attack types. The framework is evaluated using a leave-one-out cross- validation protocol on the UNSW-NB15 dataset and demonstrates consistently strong binary detection performance across multiple attack categories, with detection rates exceeding ninety percent for all classes. The ensemble-based architecture maintains high recall while exhibiting a comparatively elevated false positive rate, highlighting the importance of decision threshold calibration for real-world deployment scenarios. Ablation analyses further validate the contribution of each architectural component. The semantic bottleneck enhances abstract feature representation and generalization, k-nearest neighbor refinement improves prototype alignment, and CVAE-based augmentation enriches the train- ing distribution with semantically consistent synthetic samples. The use of multiple random restarts promotes optimization stability, while ensemble voting increases robustness through model diversity. Collectively, these findings demonstrate that the combination of semantic learning and generative augmentation provides an effective and resilient approach to zero-shot detection of previously unseen cyber attacks.
09:15 AM – 09:30 AM Paper ID: 277	**Query-free Adversarial Malware Generation Using Conditional Denoising Diffusion** *Authors*: Mahmoud, Hassan; Yasar, Samin; Khan, Muhammad Jahanzeb; Mahmoud, Mahmoud Nabil; Alsharif, Ahmad *Abstract*: Machine learning-based malware detection systems are vulnerable to adversarial attacks. Most existing attack methods require repeated queries, confidence score feedback, or knowledge of the detection model, which limits their practicality in real-world scenarios. This paper introduces a novel framework for generating adversarial malware without requiring any access to the detector. The proposed approach leverages conditional denoising diffusion probabilistic models (DDPMs) and operates solely on mathematical representations of malware features. The method incrementally modifies malicious software features to resemble those of benign programs through a sequential process, while preserving core malicious functionality via rule-based constraints. The framework is evaluated on three prevalent static malware feature types: byte histograms, imported APIs, and ASCII strings. Experimental results on large-scale datasets demonstrate that diffusion-based generation outperforms GAN-based methods for sparse binary features, achieving higher evasion rates for API imports 66.9% and ASCII strings 34.7%, while GANs remain more effective for byte histogram features. These findings demonstrate that diffusion models offer a practical and robust alternative for query-free adversarial malware generation and highlight the importance of feature-aware attack strategies.

09:30 AM – 09:45 AM Paper ID: 329	**A Predictive Cyber Threat Detection for IoT Systems Leveraging on Twitter-Based Threat Intelligence** *Authors*: Dzamesi, Lily; Yeboah, Foster; Yeboah, Jones; Nyarko-Boateng, Owusu *Abstract*: The Command and Control (C2) infrastructure remains a critical enabler of cyberattacks, supporting activities such as malware propagation, ransomware operations, and large-scale data exfiltration. As cyber threats continue to evolve, there is a growing need for predictive approaches that can identify emerging threats before they fully materialize. This study explores the use of Twitter as a source of real-time threat intelligence to support predictive cyber threat detection in IoT systems. Using a dataset collected from publicly available Twitter feeds, the study examines reported C2 servers by analyzing key attributes including IP addresses, domain names, communication protocols, geographic distribution, and user engagement indicators such as retweets and likes. The findings highlight notable patterns in the regional and protocol-level distribution of C2 infrastructure, as well as relationships between social media engagement and subsequent detection by antivirus vendors. These observations demonstrate the potential of social media driven intelligence to complement traditional security mechanisms and enhance early warning capabilities for IoT environments. Overall, the study contributes to cybersecurity research by providing empirical insights into C2 server characteristics and illustrating how Twitter-based threat intelligence can support more proactive and informed cyber defense strategies.
09:45 AM – 10:00 AM Paper ID: 340	**Proactive Approaches to Vulnerability Assessment and Mitigation** *Authors*: Albrechjt, Ethan ; Howard, Dan ; Vallejo, Diego ; Hewison, Graham ; Khan Mohd, Tauheed *Abstract*: As technology becomes more relied on in daily operations, the risks associated with software vulnerabilities such as data breaches, system failures, and financial losses have grown significantly. Traditional tools for detecting vulnerabilities, such as static and dynamic analysis, are quickly becoming inadequate due to the rapid pace of software development and the growing complexity of applications. This paper investigates new methods for identifying and categorizing vulnerabilities, focusing on the potential of machine learning and artificial intelligence to improve detection. These technologies can analyze large volumes of data and uncover patterns that might otherwise go unnoticed, helping to predict future vulnerabilities. In addition, our research highlights the challenges in patch management, highlighting the importance of automation in reducing human error and speeding up the deployment of patches. By exploring innovative tools and developing efficient workflows for vulnerability discovery and patching, this research aims to provide organizations with more effective strategies for minimizing security risks. The goal is to improve vulnerability management and help organizations better protect their systems from cyber threats.

10:00 AM – 10:15 AM Paper ID: 373	**A Universal Machine-Learning-Based Framework for Detecting and Preventing File Inclusion Attacks in PHP Web Applications** *Authors*: Khan, Fawad; Oluoch, Jared; Niamat, Mohammed *Abstract*: The purpose of this study is to investigate File Inclusion Attacks conducted through interactive PHP web applications. In addition to examining the nature of these attacks, this study aims to develop a framework for their detection and prevention. The proposed framework involves the design of a specialized Web Application Firewall (WAF) that is primarily limited to File Inclusion Attacks. The objective of this firewall is to identify and prevent File Inclusion Attacks using machine learning (ML) techniques. The firewall also provides additional capabilities, including retraining support and a limited form of static analysis. This study further compares the performance of the proposed machine learning-based firewall with that of a conventional rule-based firewall system, namely ModSecurity.
10:15 AM – 10:30 AM Paper ID: 383	**Integrating Machine Learning and Deep Learning for Robust and Privacy-Preserving Intrusion Detection: A Unified Framework and Experimental Study** *Authors*: Maha Ali Hussein, Sundos A. Hameed Alazawi, Haider K. Hoomod *Abstract*: While trendy Intrusion Detection Systems (IDS) are widely used inside the industry, they're missing in several regions: they do now not shield in opposition to state-of-the-art attackers that use deception, they're now not powerful in detecting and responding to the maximum superior styles of assaults, and they do not protect personally identifiable statistics. In this research, the authors present a blended method using Machine Learning (ML) and Deep Learning (DL) techniques. Their approach combines CNN (Convolutional Neural Networks) and BiLSTM (Bidirectional Long Short-Term Memory) networks, each of which might be known for picking up complicated styles in streams of facts with conventional classifiers which can make the final hazard identification. The team additionally tested their schooling method for resiliency against adverse inputs in this example, inputs that have been subtly altered to throw off detection. The reviews cover the Fast Gradient Sign Method which tests if predictions can still be trusted when they are being stressed. Besides that, they offer a general assessment that the technique is effective in real, world scenarios measured by standard benchmarks and the newly developed, hybrid method keeps its high, performance level even when running under privacy settings and being attacked by adversaries. The main argument for the new method is that it beats the performance of individual machine learning or deep learning systems at detecting rare and sophisticated attacks and, at the same time, it is a smart detection and tough protection tradeoff.

Day 2 - Wednesday March 25, 2026

Online Session: Paper Presentations | 08:30 AM – 10:30 AM

Online Session 5: Trustworthy LLMs, Vision-Language Models, and Explainable AI
Room Link: https://meet.google.com/yxy-yekw-fvo

TRACK CHAIRS:	Dr. Yousef Fazea Alnadesh (Marshall University)

08:30 AM – 08:45 AM Paper ID: 60	**Harnessing Vision Language Models for Negation Sensitivity in Visual Question Answering** *Authors*: Roy, Sourav; Alam, Fardin; Ali, Yeash Zuddan; Sahariyar, Hussain Md.; Alam, Md. Nahin; Haque Dhrubo, Ahmed Faizul; Qayum, Mohammad Abdul *Abstract*: Negation flips the meaning of a question, yet many vision language models (VLMs) still answer as if the prompt were positive. We present a simple, reproducible pipeline that measures negation sensitivity in yes / no Visual Question Answering (VQA) using BLIP and CLIP. We parse questions, create rule based negated counterparts, and evaluate paired original and negated (Questions and Answers) for the same image so that wording, not content, drives differences. On a validation set of N =1181 pairs, BLIP achieves Affirmative and Negation accuracies of 0.484, 0.516 while CLIP achieves 0.516, 0.484 on (Epoch:1, Learning rate for BLIP 1e-4 and for CLIP 2e-4) respectively. A small combined (Avg.) negation differential (Δ = −0.015) suggests reduced affirmation bias compared with common baselines. We include model comparisons, qualitative results per-sample, and clear reporting to support reuse.
08:45 AM – 09:00 AM Paper ID: 147	**Leveraging Vision-Language Models for Movie Genre Prediction: A Comparative Analysis of BLIP, CLIP, ViLT, and FLaVA** *Authors*: Abyad, Shak Mohammad; Khalil, Md. Ibrahim; Antu, S.M. Riaz Rahman; Pramanik, Souvik; Dhrubo, Ahmed Faizul Haque; Sajjad, Mohsin; Qayum, Mohammad Abdul *Abstract*: Movie genre classification is a multimodal task which needs to simultaneously comprehend the visual content and text summaries. In this paper, we compare four state-of- the-art Vision–Language Models (VLMs), e.g. BLIP, CLIP, ViLT and FLAVA, using a large-scale movie genre dataset that we curated. These models are representative examples of various multimodal learning paradigms, including contrastive learning, vision–language bootstrapping, transformer-based feature align- ment and unified multimodal fusion. Our results demonstrate that the best overall accuracy is achieved by CLIP 96% and FLAVA 97% , while BLIP shows a more homogeneous behavior across different genres. ViLT is closer to scoring textual models, probably for some semantic overlap and visual confusion between genres. The results may suggest the obvious pros of contrastive and fusion-based approaches in order to reinforce that fine- grained interaction information still the most important task. This study sheds light on the performance and limitations of VLMs in movie genre prediction, which can be helpful to guide future work on multimodal media analysis, content understand- ing and recommendation system applications.

09:00 AM – 09:15 AM Paper ID: 193	**A BART-Enhanced Hybrid Framework for Multi-Document Summarization** *Authors*: Ihsan, Uswa ; Jhanjhi, Nz ; Ashraf, Humaira ; Malik, Javairia *Abstract*: In the modern information age, the internet hosts vast quantities of textual data spread across numerous documents, making it difficult for users to extract relevant and concise information efficiently. Multi-document summarization aims to generate compact summaries that retain key information while minimizing redundancy. However, many existing MDS approaches still struggle with redundancy and limited accuracy. This study introduces an efficient hybrid multi-document summarization framework based on the pre-trained BART model. The proposed method integrates clustering and ranking techniques, including K-Means, Gaussian Mixture Model, centroid computation, and cosine similarity, to improve sentence selection and ensure more coherent summaries. Experiments conducted on the DUC2004 dataset demonstrate that the proposed approach outperforms existing methods, achieving higher F1, Precision, and Recall scores of 0.13269, 0.11875, and 0.15034, respectively, while reducing textual redundancy by 97%. The results indicate that integrating BART with hybrid clustering techniques effectively enhances summary informativeness and readability, offering a promising direction for future advancements in multi-document summarization
09:15 AM – 09:30 AM Paper ID: 198	**A Hybrid Stylometric and Transformer-Based Framework for Detecting AI-Generated Text** *Authors*: Kanwal, Rimsha; Zam Zam Mirza, Qurat Ul Ain ; Ashraf, Humaira; Jhanjhi, NZ. *Abstract*: The fast development of big models of language applications (LLMs) like ChatGPT, GPT-4, Claude, or Gemini has changed digital content development positively but has at the same time increased the difficulties in determining whether a certain text has been written by a human being or is produced by an artificial intelligence (AI). Online information, academic writing, and journalism take the risk of being compromised because of the indistinction between these two types of writing. In this paper, the hybrid architecture that combines stylometric and transformer-based embeddings is introduced to detect AIgenerated text correctly, particularly news and educational fields. The framework takes advantage of classic linguistic properties sentence length, frequency of punctuation, richness of lexicon and burstiness with the semantic representations based on the TF-IDF embeddings and BERT embeddings. Logistic Regression and Random Forest are the two supervised classifiers that were trained and tested with mixed datasets of human and AIgenerated texts. Experimental findings show that the Random Forest model was better in precision and robust and its average accuracy of 90% was higher than that of Logistic Regression (87%) with different samples. The proposed solution is effective because it can bridge the gap between interpretability and high performance, using both stylometric and semantic features. A comparative study with the current models in the GPTZero, GLTR and DetectGPT platforms shows better adaptability and automation, and this system is applicable to content verifiers, academic integrity systems, and news authenticity, which are used to examine the system. The future directions of the model include improvements to be multilingual data and multimodal detection (text and visual cues).

09:30 AM – 09:45 AM Paper ID: 228	**Benchmarking the Effectiveness of AI-Driven Red Teaming Across Safety-Aligned Language Models** *Authors*: Hasan, Kamrul; Malicha, Joyce *Abstract*: Large language models (LLMs) have advanced rapidly, yet even safety-aligned models remain vulnerable to adversarial prompts that bypass safeguards and induce harmful outputs. Conventional red teaming methods, including static test- ing and gradient-based attacks, are limited by either insufficient adaptability or restrictive access assumptions. In this work, we benchmark an autonomous AI-driven evolutionary red teaming system that iteratively generates, evaluates, and refines prompts to uncover safety vulnerabilities in 7-billion-parameter aligned LLMs. Using Qwen-7B-Instruct as a prompt-mutation agent, the AI-driven method achieves a 47.0% method-level Attack Success Rate (ASR), matching the GCG baseline (47.0%) and exceeding static prompting (33.5%). We evaluate four open-source models (Gemma-7B, Llama-2-7B-Chat, Vicuna-7B, Mistral-7B) using the AdvBench harmful behaviors benchmark and a dual-stage evaluation framework (Llama-Guard-3 classification and Beaver- 7B severity scoring), achieving a 0% false positive rate on 200 benign prompts. Results show substantial cross-model robustness variation (14.7% to 64.0% overall ASR; 4.4x spread), indicating that safety performance is strongly model-dependent even at similar scale. These findings show that adaptive black-box red teaming is competitive with strong gradient-based baselines and useful for scalable safety auditing.
09:45 AM – 10:00 AM Paper ID: 266	**Evaluating Explainable AI Fidelity in Lightweight Vision Transformers Using Transfer Learning** *Authors*: Phelps, Drew; Hasan, Syed Rafay; Altarawneh, Amani *Abstract*: Explainable artificial intelligence is increasingly used to support trust and analysis in vision models deployed on resource constrained devices. Lightweight Vision Transformers differ substantially in architecture, capacity, and tokenization, which can influence both predictive performance and the quality of explanation guided regions. This paper evaluates explanation effectiveness across multiple edge oriented Vision Transformer architectures using two retraining based frameworks, fine tuned fidelity and geometric remove and retrain. By comparing models under sufficiency and necessity based retraining assumptions, we analyze how architectural differences affect classification accuracy and explanation behavior. Across both evaluation paradigms, TinyViT demonstrates the most consistent explanation effectiveness, showing stronger robustness and recovery under region removal and higher sufficiency when inference is constrained to explanation-guided regions, whereas DeiT-Tiny and SHViT exhibit larger degradation under the same masking budget.

10:00 AM – 10:15 AM Paper ID: 328	**AI-Assisted Forensic Triage of Multilingual Online Gaming Chats Using Large Language Models** *Authors*: Johnson, Jerrold ; Ibrahem, Mohamed; Abouyoussef, Mahmoud *Abstract*: Online gaming platforms generate massive volumes of short, informal, and multilingual messages that increasingly appear in digital forensic investigations. Manual examination of such data is time-consuming and difficult to scale, motivating the need for automated triage mechanisms that assist investigators without replacing human judgment. This paper evaluates zero-shot large language models (LLMs) as decision-support tools for early-stage forensic triage of online gaming communication. Using real-world Discord messages from the publicly available DISCO dataset, we construct a forensic analysis pipeline incorporating multilingual preprocessing, a classical Term Frequency–Inverse Document Frequency (TF–IDF) with Logistic Regression baseline, zero-shot LLM classification, and human validation. On a 200-message human-annotated subset, GPT-4.1-mini achieved higher agreement with human judgments (accuracy 0.77) than the classical baseline (accuracy 0.655). A consistency analysis further indicates that repeated LLM runs agree on 72\% of evaluated messages, highlighting both practical utility and the continued need for human oversight. These findings suggest that LLMs can effectively support forensic triage by prioritizing potentially relevant messages while maintaining a human-centered investigative process.
10:15 AM – 10:30 AM Paper ID: 369	**AI-Augmented Debugging: Using LLMs and Execution Traces to Explain and Fix Software Failures** *Authors*: Devarajulu, Vishnupriya S *Abstract*: Fault localization and debugging are major bottlenecks in the current software development that requires massive developer time and resources. Conventional methods of debugging require the use of manual inspection of execution logs and stack traces, which leads to long detectability and higher cognitive load. The current paper outlines a new framework that combines large language models with the analysis of execution traces and symbolic execution methods to automatically detect, analyze, and provide solutions to the failures in software. The system processes logs, stack traces, and source code to generate probable root cause locations, natural language explanations, and fix recommendations. A Comprehensive evaluation using real-world crash datasets demonstrates that this approach achieves superior fault localization accuracy while reducing mean time to resolution by over 41.2% compared to conventional debugging tools.

Day 2 - Wednesday March 25, 2026

Online Session: Paper Presentations | 08:30 AM – 10:30 AM

Online Session 6: AI-Enabled Healthcare, Perception, and Intelligent Secure Systems
Room Link: https://meet.google.com/koq-bocg-evb

TRACK CHAIRS:	Dr. Laavanya Rachakonda (University of North Carolina Wilmington)

08:30 AM – 08:45 AM Paper ID: 30	**Compact Vision Transformers for BFMRX Bone-Fracture Detection** *Authors*: Hossain, Jonayed; Ullah, Kazi Refat; Nafi, Akib Sadman; Islam Khan, Md. Mazenul; Haque Dhrubo, Ahmed Faizul; Pramanik, Souvik; Qayum, Mohammad Abdul *Abstract*: In this work, we investigate the influence of transfer learning on compact vision backbones for bone fracture detection across multiple anatomical regions. We use the Bone Fracture Multi-Region X-ray (BFMRX) dataset (10,580 images) and eval- uate five backbones (DaViT-Tiny, MViT-v2-Tiny, TinyViT-5M, RepViT-m3, PiT-Ti) under both transfer learning and training from scratch. Transfer learning yielded better validation ac- curacy (98.28%–99.76%) and lower loss (0.0173–0.0527) com- pared to training from scratch (accuracy: 90.11%–98.31%, loss: 0.0504–0.3173). DaViT backbones performed best, with a minimal drop in performance when trained from scratch (1.45 pp) and tight training-validation gaps. MViT-v2 showed strong reliance on pre-training (99.52% → 90.11% without transfer). Overall, transfer learning proved essential for achieving reliability and efficiency in BFMRX, with DaViT providing the best post-transfer performance for deployment.
08:45 AM – 09:00 AM Paper ID: 98	**Outcome Prediction in Angioplasty Procedures Using ResNet18 and AlexNet** *Authors*: Rohith, K. S. ; Prabhu, M. Ramkumar ; Maqsood, Umair *Abstract*: In estimating outcomes in several angioplasty tech- niques, the use of deep neural has grown a lot, so in this study we used images from patients who underwent balloon angioplasty, drug-coated angioplasty. Images go through rigorous preprocessing to get clarity and optimal sharpness for deep learning analysis and we checked how well ResNet18 and AlexNet help in this angioplasty by using these images, also testing confirmed that ResNet18 demonstrated high confidence in distinguishing between the favorable and unfavorable procedural actions so this paper gives a critical examination of the ResNet18 model's performance across various angioplasty cases, detailing its strengths, limitations, influential factors, and provide the directions for future research.

09:00 AM – 09:15 AM Paper ID: 110	**Artificial Intelligence for Strengthening E-Prescription Security in Healthcare Networks** *Authors*: Paripally, Keerthi; Hossain, Gahangir *Abstract*: Electronic prescription or e-prescription systems have the benefit of transmitting prescriptions electronically through delivery to pharmacies by doctors, thereby preventing handwriting mistakes and enhancing patient safety. Artificial intelligence is on the rise in healthcare systems as they become more digital. AI could assist e prescribing by detecting mistakes, identifying suspicious trends and assisting in avoiding false or incorrect prescriptions. Meanwhile, the increased number of cyberattacks on healthcare networks has generated new security issues. There is a threat of hacking, unauthorized access, data leakage, altered prescriptions and this poses serious problems both to the patients and the healthcare giver. As much as AI can enhance security, it has the potential of introducing new threats when not well handled. The paper outlines the functionality of e prescription systems, security issues they are most likely to encounter and the impact of AI on the weaknesses and strengths of such systems. A basic enhanced AI security solution is suggested to assist in securing future eprescription systems.
09:15 AM – 09:30 AM Paper ID: 136	**Secure AI-Driven eConsent Platforms: Enhancing Trust, Compliance, and Participation in Clinical Research** *Authors*: Vinnakota, Jayasri; Raheem, Tayiba; Hossain, Gahangir *Abstract*: AI-enabled secure electronic informed consent (eConsent) tools are increasingly adopted in clinical trials to enhance patient awareness, accelerate participant recruitment, and enable remote access to research studies. These systems integrate advanced technologies such as audit trails, encryption, identity verification, and blockchain-based dynamic consent mechanisms to ensure transparency, security, and trust. The framework emphasizes compliance with critical regulatory and ethical standards, including HIPAA, GDPR, and ICH-GCP, to protect participant data privacy and maintain data integrity throughout the consent lifecycle. This work analyzes major security threats to eConsent systems—particularly data breaches and authentication vulnerabilities—and discusses effective mitigation strategies. Electronic informed consent exemplifies how digital transformation is reshaping clinical research, as eConsent platforms improve participant understanding, engagement, and oversight. Consequently, AI-enabled eConsent systems are progressively replacing traditional paper-based consent processes in modern clinical trials.

09:30 AM – 09:45 AM Paper ID: 200	**AI-Enabled Thermal Security System for Weapon Identification in Adverse Visibility** *Authors*: Zam Zam Mirza, Qurat Ul Ain; Kanwal, Rimsha ; Ashraf, Humaira ; Zaman Jhanjhi, Noor *Abstract*: Thermal imaging technology has been significant in security surveillance, particularly in offering images in less visibility. The success of its applications in military, security, medical and industrial applications is growing day by day out. Over the last few years research on thermal imaging technology as a means of detecting weapons and abnormal behavior identification has gained momentum slowly. To enhance the recognition effect, the integration of data based on multi-modes will form a major direction, that is, the combination of motion, emotion and object detection data. Though, the current thermal imaging analysis systems are based on either artificial judgment or mere image processing technology, and they lack intelligent analysis and recognition capability of concealed weapons and behavior of human beings in a complex environment. Thus, it is extremely practical importance to design an AI-based thermal imaging system which will be capable of weapons detection and ability to read abnormal behavior. The model can identify a weapon carrying person for a specific video or picture of a thermal image.
09:45 AM – 10:00 AM Paper ID: 252	**Bone Fracture Detection Using Vision Transformers: A Comparative Analysis of the Pooling-based Vision Transformer (PiT) and the Causal Transformer (CaFormer) Models** *Authors*: Munna, Atikul Islam; Khalil, Md. Ibrahim; Munna, Assaduzzaman; Halder, Arnob; Pramanik, Souvik; Haque Dhrubo, Ahmed Faizul; Qayum, Mohammad Abdul *Abstract*: Bone fracture detection in radiography remains a critical challenge in medical imaging, where minor fractures often elude both human experts and conventional deep learning models. This study introduces a novel comparative analysis of vision transformer architectures of Pooling-based Vision Transformer (PiT), Causal Transformer (CaFormer), ConvNeXt, XCiT, and HardCoReNAS to address the limitations of traditional convolutional networks in fracture diagnosis. Using a dataset of 4,083 annotated X-ray images (hand, leg, hip, shoulder), we evaluated model performance through rigorous augmentation, hyperparameter tuning, and cross-validation. Despite achieving 98.83% training accuracy, CaFormer demonstrates a generaliza- tion gap with 97.30% testing accuracy, while PiT outperforms all models with 97.51% testing accuracy despite lower training performance (97.90%). Our findings reveal a critical paradox: models excelling in training do not necessarily generalize better to unseen clinical data. Our work underscores the potential of vision transformers, particularly PiT, in automating fracture detection while highlighting the risks of overreliance on training metrics. Our study concludes with actionable insights to improve model robustness through dataset balancing and segmentation in future research.

10:00 AM – 10:15 AM Paper ID: 339	**Transforming Medical Devices Through Software Innovation** *Authors*: Needham, Cameron ; Lechner III, Joe ; Stojanovski, Kristijan ; Saleh, Zeinab ; Khan Mohd, Tauheed *Abstract*: This research paper aims to shed new light on how software assurance is applied to medical fields and also looks at when this is allowed or not. We will explore the critical areas of AI in medical devices, wearable technology, and discuss new government regulations on software and AI in medical devices. We will also talk about how we found these findings and how they impact society. We first examine new innovations and inventions in the field of medical devices and how software assurance is applied. The next sections will discuss how software can and is assisting with surgical operations such as 3D modeling and how robots can impact surgeries. We will also dive into how some new government regulations control how software can be applied in a medical setting. One of the last sections that this paper will discuss is wearable technology and how these devices can become vulnerable to cyber attacks.
10:15 AM – 10:30 AM Paper ID: 341	**Cybersecurity in Healthcare: Safeguarding Patient Data and Systems** *Authors*: Khan Mohd, Tauheed; Digna, Eric ; Ebrahim, Mohammad ; Zhao, Yihong ; Biesiada, Joseph *Abstract*: This study investigates cybersecurity vulnerabilities in healthcare organizations, specifically focusing on X-ray machine systems and their susceptibility to Remote Shell (rsh) service exploitation. Through a simulated environment designed to replicate an X-ray machine's server infrastructure, we analyze the exploitation of critical vulnerabilities CVE-2019-13543 and CVE-2019-13539, particularly examining how rsh misconfiguration can lead to system compromise. The research employs virtual machines running Ubuntu 18.04 LTS with Apache 2.2 and rsh services to simulate X-ray machine software configurations in a controlled laboratory setting. Our methodology includes vulnerability assessment and exploitation testing, demonstrating how attackers can bypass authentication and achieve privilege escalation through rsh vulnerabilities. Results reveal successful exploitation of these vulnerabilities, highlighting critical security implications for medical devices running outdated software versions and insecure services like rsh. The findings emphasize the necessity for healthcare organizations to maintain updated systems, implement proper security controls, and replace legacy services like rsh with more secure alternatives. This research contributes to understanding cybersecurity challenges in medical devices and provides insights for improving security measures in healthcare environments, where a single breach can cost up to 4.9 million and potentially impact patient safety.

Invited Talk

Room Link: https://meet.google.com/fij-icdz-rrx

Day 2 - Wednesday March 25, 2026

10:30 PM – 11:00 PM

Plenary Session I

Invited Talk

A GEAR-Informed Architectural Approach to Governing Secure and Resilient IT/OT Convergence in the Industry 5.0 Era

Session Chairs:

Khaled Saleh, Wright State University

Presenter/Speaker:

Dr. Noor Zaman Jhanjhi, Taylor's University

Abstract: [Abstract]

Speaker Bio: Dr. Noor Zaman Jhanjhi is a distinguished Senior Professor of Computer Science at Taylor's University, Malaysia, where he specializes in Artificial Intelligence and Cybersecurity. As the Director of the Research Center, Center for Intelligent Innovation CII, and Program Director for Postgraduate Research Degree Programmes, he plays a pivotal role in shaping academic excellence and driving cutting-edge research initiatives. Globally acclaimed for his scholarly contributions, Prof. Jhanjhi has been consistently ranked among the world's top 2% research scientists (2022, 2023, 2024, and 2025) and stands as one of Malaysia's top computer science researchers. He has been named amongst the top 0.05% of all scholars worldwide according to the 2025 ScholarGPS rankings. His exceptional work has earned him prestigious accolades, including the Outstanding Faculty Member Award (MDEC Malaysia, 2022) and the Vice Chancellor's Best Research Citations Award (Taylor's University, 2023). A prolific author and editor, Prof. Jhanjhi has published over 80 research books with leading publishers such as Springer, Elsevier, IGI Global, Bentham, IET, and Wiley, etc., amassing 1,000+ impact factor points. His mentorship spans 45 postgraduate completions, and he has examined 70+ Ph.D. and Master's theses worldwide. As an Editor-in-Chief, Associate Editor, and Editorial Board member for top-tier journals (PeerJ Computer Science, IEEE Access, CMC Computers), he advances scholarly discourse. His leadership extends to securing 40+ international research grants, underscoring his influence in innovation. A dynamic keynote speaker, Prof. Jhanjhi, has delivered 100+ invited talks and chaired major conferences. His decade-long engagement with ABET, NCAAA, and NCEAC accreditation bodies highlights his dedication to global academic standards. Combining research brilliance, academic leadership, and a passion for mentorship, Prof. Jhanjhi continues to inspire the next generation of computer scientists while shaping the future of AI and cybersecurity.

Invited Talk

Room Link: https://meet.google.com/fij-icdz-rrx

Day 2 - Wednesday March 25, 2026

11:00 PM – 11:30 PM

Plenary Session I

Invited Talk

Assurance and Reliability in Advanced AI Technologies: A Foundation for Trusted Microelectronics

Session Chairs:

Khaled Saleh, Wright State University

Presenter/Speaker:

Dr. Darpan Verma, Device Engineer, Intel

Abstract: Advances in microelectronics, heterogeneous integration, and AI enabled hardware have intensified the need for robust mechanisms that ensure assurance, reliability, and trust across device lifecycles. As fabrication processes grow more complex and supply chains expand, semiconductor technologies face heightened risks related to performance variability, reliability degradation, and potential hardware manipulation-concerns strongly emphasizing deep dives in secure, trustworthy microelectronics infrastructures. This talk outlines how combining rigorous device level reliability analysis with assurance practices strengthens the foundation of trusted microelectronics. Drawing from real examples of compromised hardware in communication systems and demonstrated hardware Trojan insertions, the talk illustrates vulnerabilities that can emerge without strong assurance principles. By integrating reliability engineering, electrical characterization, and supply chain trust concepts, this session offers a unified perspective on building predictable, secure, and resilient microelectronic systems that support next generation IoT, edge, and critical infrastructure technologies.

Speaker Bio: Dr. Darpan Verma is a device engineer at Intel, specializing in device characterization, electrical reliability analysis, and the interaction between fabrication processes and device performance. His work focuses on translating experimental electrical and structural measurements into engineering insights that guide the development of advanced logic and memory technologies. He earned his Ph.D. in Materials Science and Engineering from The Ohio State University, where he investigated wide bandgap (GaN, beta-Ga2O3) and 2D semiconductor devices. His doctoral research included developing a photocurrent based electric field mapping methodology that enabled direct visualization of electric field distribution by using Frankz-Keldysh Effect, thus opening pathways to analyze reliability limits and breakdown mechanisms in power and optoelectronic devices without breaking or damaging them in the process. Before his Ph.D., Dr. Verma taught undergraduate electronics courses and mentored students, and he remains passionate about supporting early career researchers and engineers as they navigate technical and professional development paths.

Day 2 End

Day 3 - Thursday March 26, 2026

Online Session: Paper Presentations | 08:30 AM – 10:30 AM

Online Session 7: Human-Centered, Explainable, and Applied Trustworthy AI
Room Link: https://meet.google.com/fij-icdz-rrx

TRACK CHAIRS:	Dr. Kamrul Hasan (Grand Valley State University)

08:30 AM – 08:45 AM Paper ID: 31	**Human-Centered AI in Banking: Designing Adaptive Systems for Secure and Personalized Financial Engagements** *Authors*: Selvam, Muthu *Abstract*: This article presents the Human-Centered Adaptive AI Framework for intelligent financial systems that prioritise users' agency, privacy, transparency, and customisation. Behavioural profiling, adaptive personalisation, explainable artificial intelligence (XAI), and trust and privacy assurance create a responsive and ethical user experience tailored to each person's financial behaviours and goals. Federated learning and consent-driven data usage protect sensitive data while adapting. The system uses SHAP, LIME, and dynamic user interfaces depending on the knowledge and goal to make AI decisions understandable. An integrated examination of user surveys, prototype testing, and quantitative metrics showed improvements in trust perception, target completion rates, data-sharing compliance, and support efficiency. These studies show that human-centered design inside AI systems may make financial technology safer, more transparent, and more user-friendly.
08:45 AM – 09:00 AM Paper ID: 74	**Predicting Student Academic Performance Using Machine Learning Techniques** *Authors*: Sailaja Pulagam, Reshma Sai Aishwarya Artham, Muhammad Zubair Khan, Belinda Copus *Abstract*: Accurately predicting student academic performance is a key objective in educational data mining and learning analytics, as early identification of at-risk students enables timely and targeted academic interventions. In this study, we investigate the problem of final grade prediction using the UCI Student Performance dataset and formulate it as a supervised regression task. Four widely adopted regression models—Linear Regression, Random Forest, XGBoost, and Support Vector Regression (SVR)—are implemented and evaluated under a consistent pre processing and validation framework. Experimental results show that ensemble tree-based models, particularly Random Forest, achieve superior generalization performance, attaining a test R2 of 0.83 and the lowest root mean squared error (RMSE). Beyond predictive accuracy, this work emphasizes model interpretability by analyzing feature importance to identify the academic and behavioral factors that most strongly influence final outcomes. Prior-period grades emerge as the dominant predictors, while attendance, study time, and previous failures provide additional explanatory power. Rather than introducing a new algorithm, this paper provides an interpretable and deployment-oriented empirical baseline for AI-based academic decision-support systems. The findings demonstrate how transparent machine learning models can support early-warning frameworks within institutional analytics workflows, balancing predictive performance with practical usability.

09:00 AM – 09:15 AM Paper ID: 76	**Fake News Detection Using Machine Learning Techniques** *Authors*: Veerati, Meghana Reddy; Sriramula, Anvitha; Khan, Muhammad Zubair; Bapatla, Anand Kumar *Abstract*: This paper presents a supervised machine learning approach for detecting fake news articles using text-based features. The study utilizes the "Fake and Real News Dataset" from Kaggle and implements three traditional machine learning classifiers: Logistic Regression, Linear Support Vector Machine (SVM), and Random Forest. Text preprocessing includes lowercasing, tokenization, stopword removal, and term frequency-inverse document frequency (TF-IDF) vectorization. On a heldout test set, Logistic Regression, Linear SVM, and Random Forest achieve accuracies of 98.64%, 99.48%, and 99.84%, respectively. The results demonstrate that TF–IDF based traditional machine learning models-especially Random Forest and Linear SVM are highly effective for fake news detection, providing competitive performance compared to more complex approaches reported in the literature.
09:15 AM – 09:30 AM Paper ID: 109	**Improving Rating Accuracy in a Comparative Study of Web and Android Platforms Using a Quantitative Survey of Chef Booking Applications** *Authors*: Ganesh, Vunnam ; Vindhya A, Shri ; Azeem Khan, Abdul *Abstract*: The research project revolves around improving rating precision in a person-alized application for booking chefs to cook at home, called BookAChef. To improve the preciseness of ratings and customer satisfaction in this paper, we analyze the dependability of the rating systems on web and Android plat-forms. We achieve our objectives with user input analysis, optimization techniques, and performance testing. Materials and Methods: This study will consider two applications: an Android application, N = 15, and a Web appli-cation, N = 15. This implies that the sample size for the study will be N = 30. Sample size calculations are carried out using G Power to achieve a statistical power of 80%. This was also in agreement with rating accuracy assessment in the BookAChef app through user text message summaries. Results: The rating accuracy of the Android application is 85.2667%, while the online ap-plication has a rating accuracy of 90.6000%. However, the p=0.028 significance gives a result of p¿0.05, meaning there is no significant statistical difference between the two groups within the data. Conclusion: Based on the comparison, web applications have received higher ratings than Android ap-plications.

09:30 AM – 09:45 AM Paper ID: 181	**Advancing Sentiment Analysis with BERT: A Comparative Evaluation Against Machine Learning and Deep Learning Techniques** *Authors*: Chowdhury, Saif Mahmood;Ratul, Tashfin Rahat; Rahman, Arif; Tanvir, K.M. Farhan; Chowdhury, Ashfaqur Rahman; Sayed, Md. Saad Bin; Antu, S.M. Riaz Rahman; Haque Dhrubo, Ahmed Faizul; Pramanik, Souvik; Sajjad, Mohsin; Qayum, Mohammad Abdul *Abstract*: Sentiment analysis is crucial in understanding public opinion, monitoring brand reputation, and informing decision- making processes across industries. With the growing influence of social media on various sectors, accurate sentiment analysis can offer real-time insights into user behavior and market trends. However, traditional machine learning and some deep learning models often struggle to capture the nuanced and context- dependent nature of short and noisy text data found on platforms like Twitter. This research addresses the gap by leveraging a Bidi- rectional Encoder Representations from Transformers (BERT) for sentiment analysis and comparing its performance against traditional machine learning and other state-of-the-art deep learning models. In this study, we implement and evaluate BERT alongside models such as Logistic Regression, Random Forest, CNN, and LSTMs on a comprehensive Twitter dataset of 416,809 examples in English. The BERT model achieves statistically significant improvements with accuracy, precision, recall, and an F1-score of 94%. This represents a 2% improvement over the next best performing model (CNN) and a 12% improvement over the traditional Naive Bayes model, demonstrating its superior capability to understand context and semantics. The experiments are conducted on the aforementioned Twitter dataset, ensuring the robustness and generalizability of the findings. The proposed approach holds immense real-world applicability in domains like customer feedback analysis, political sentiment tracking, and disaster response management. By providing a reliable method for sentiment detection, this work bridges the gap between research advancements and practical implementation, enabling organizations to derive actionable insights from social media data with highly competitive accuracy.
09:45 AM – 10:00 AM Paper ID: 326	**Explainable AI Models for Transparent and Ethical Customer Relationship Management Decision** *Authors*: Kukar, Sourabh *Abstract*: Customer Churn is a severe problem of banking institutions, which directly affects profitability and sustainability. To solve this problem, this paper offers an explainable artificial intelligence (XAI)-based framework of transparent and ethical customer relationship management (CRM) decision-making, namely, churn prediction. The data-processing, feature engineering, and class balancing based on SMOTE, as well as machine learning models in the form of the ensemble, were used with the help of the Bank Turnover (Churn Modelling) dataset. While comparing the Random Forest, Logistic Regression. The experimental results indicate that ensemble models are better than traditional methods, where Gradient Boosting has the highest ROC-AUC of 86.14% and XGBoost has the highest accuracy of 84.25%. To increase transparency, several XAI methods, such as, partial dependence plot, permutation feature importance, and decision path analysis and individual conditional expectation plot were utilized. These results indicate that behavioral and demographic characteristics are the major sources of churn, which allow reliable, interpretable, and practical CRM strategies.

10:00 AM – 10:15 AM Paper ID: 391	**CTGAN-Augmented Stacked Ensemble of Machine and Deep Learning Models for Diabetes Prediction** *Authors*: Saeed, Muhammad Atif; Sasna, Shirin; Malik, Muhammad Atlas; Kumar, Vinod; Atiq, Azka; Jamil, Akhtar *Abstract*: Early prediction of type 2 diabetes enables timely intervention and may substantially reduce long-term complications and healthcare costs. This paper proposes a CTGAN-augmented stacked ensemble framework that integrates both ML and DL models for binary diabetes prediction on the widely used PIMA Indian Diabetes Dataset. The original dataset (768 records, eight numerical features) is cleaned using interquartile range (IQR)--based outlier clipping and scaled with Min--Max normalization. Class imbalance is addressed by generating realistic minority-class samples for only the training split using Conditional Tabular GAN (CTGAN). Three ML models (XGBoost, Random Forest, Decision Tree) and three DL architectures (Deep Neural Network, Deep & Cross Network, and TabNet) are tuned with Optuna for optimal hyperparameters. Their probabilistic outputs feed a two-level stacking scheme with Random Forest as level-1 meta-learner and XGBoost as level-2 meta-learner. The introduction of stacked ensemble learning substantially enhanced overall performance, with the two-stage stacking architecture consistently outperforming all individual models. On the held-out test set, the ML-based level-2 stacker achieved highest accuracy (0.931) and AUC-ROC (0.935), outperforming DL ensemble (Accuracy: 0.914, AUC-ROC: 0.927). Results confirm that well-tuned tree-based ensembles and hierarchical stacking offer a robust and generalizable strategy for small, structured clinical datasets.
10:15 AM – 10:30 AM Paper ID: 392	**Agentic Code Review: A Multi-Agent Framework with Meta-Cognitive Reflection and Human-in-the-Loop Alignment** *Authors*: Jamil, Akhtar; Saleem, Abdullah; Jamil, Akhtar; Ryan, Siddique Ahmad; Hameed, Alaa Ali; Fargetta, Georgia *Abstract*: Automated code review remains a persistent chal- lenge in software engineering. Traditional static analysis tools depend on rigid pattern matching and produce excessive false positives, while large language model (LLM)-based approaches frequently hallucinate findings that reference nonexistent code. This paper presents a multi-agent framework that addresses both limitations through orchestrated specialization and adversarial self-verification. The proposed system deploys four agents via LangGraph: a security specialist that combines Bandit static analysis with LLM-based contextual reasoning, a retrieval-augmented performance optimizer that grounds suggestions in historical pull request data, a meta-cognitive critic that validates all findings against the original source code to filter hallucina- tions, and a lead architect that synthesizes only verified results. A human-in-the-loop checkpoint ensures that critical decisions remain under expert oversight before final synthesis. Evaluation on deliberately vulnerable Python code samples demonstrates that the critic agent reduces false positives by 40% relative to a single-agent baseline, improves line-number accuracy from 67% to 92%, and lowers the hallucination rate from 32% to 18%. An ablation study confirms that the meta-cognitive verification layer contributes most significantly to these gains. These results indicate that adversarial self-verification within multi-agent ar- chitectures can meaningfully improve the reliability of LLM- driven code analysis for high-stakes software review tasks.

Day 3 - Thursday March 26, 2026

Online Session: Paper Presentations | 08:30 AM – 10:30 AM

Online Session 8: AI for Smart Environments, Manufacturing, and Autonomous Systems
Room Link: https://meet.google.com/yxy-yekw-fvo

TRACK CHAIRS:	Sreekanth Muktevi (YASH Technologies)

08:30 AM – 08:45 AM Paper ID: 4	**Performance Evaluation of Machine Learning Models for Real-Time Anomaly Detection in MQTT-Based IoT Networks** *Authors*: Alnadesh, Yousef *Abstract*: The swift growth of Internet of Things (IoT) devices and the adoption of the Message Queuing Telemetry Transport (MQTT) protocol have allowed for very efficient, lightweight communication in IoT networks, even in resource-constrained environments. Yet, as the number of devices grows and, with it, the amount of data traffic, we encounter increased risks: cyberattacks, data corruption, and system failures. This work presents a performance evaluation of four machine learning models, Random Forest (RF), Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Neural Networks (NN), for real-time anomaly detection in IoT networks that use MQTT as a communication protocol. The models were assessed along several dimensions: latency, detection accuracy, resource utilization, scalability, and robustness to noisy data. The Random Forest model achieved the highest accuracy (95.8%), with low latency (35 ms) and moderate resource utilization (45%). In contrast, Support Vector Machines (SVMs), while still achieving high accuracy (93.2%), had much poorer latency (180 ms) and were very resource-intensive, making them unsuitable for deployment on real-time resource-limited IoT devices. K-Nearest Neighbors (KNN) were even worse on all counts (89.8%, 250 ms). Neural Networks were better in accuracy (94%) but were still too resource-intensive (95% utilization) to be feasible for real-time effectuation on resource-limited IoT devices.
08:45 AM – 09:00 AM Paper ID: 15	**Engineering Spatiotemporal Forecasts at Scale: Dhaka Weather with state-of-the art Machine Learning models** *Authors*: Rijan, Tamim Ahmed; Katha, Navin Nawar; Raihan, Md. Toufique; Alam, Md. Nahin; Haque Dhrubo, Ahmed Faizul; Qayum, Mohammad Abdul *Abstract*: Accurate weather prediction is very important for climate adaptation as well as urban planning like Dhaka which is the one of the crowded city. We provide a reproducible dataset, consisting in 14,616 samples of hourly observations (Jan 2023–Aug 2024) from multiple stations and an end-to- end pipeline that goes through data ingestion, quality checks, feature engineering and model training. We compare LSTM with classical ML models (Decision Tree, Random Forest, Gradient Boosting, SVR, logistic regression, Naive Bayes) and ensemble methods. Ensemble learners like Gradient Boosting, Random Forest outperform individual models but LSTM captures tem- poral dependencies with R2 =0.826. Classification oriented tasks also manifest these patterns that deviate from usual classifiers, suggesting the necessity for the richer features or other formula- tions. We show here that the fusion of tree-based ensembles and deep sequence models is effective in predicting urban phenomena. The dataset and pipeline are production ready - they support feature stores, schedulers, CI/CD - and serve as strong baselines for further research in spatiotemporal modeling.

09:00 AM – 09:15 AM Paper ID: 131	**Intelligent Feature Selection for Semiconductor Manufacturing using a Hybrid Genetic Algorithm and Neural Network** *Authors*: Padmapriya, K. ; Kavitha, K. ; Bhimrao Mane, Manisha *Abstract*: When it comes to manufacturing processes, "Smart Manufacturing" refers to using optimization strategies that employ sophisticated analytics methodologies. Optimal and efficient methods of data management are becoming increasingly important as the number of Industrial Internet of Things (IIoT) sensors used in production processes continue to rise. Intelligent and effective automation is possible with the help of Machine Learning and Artificial Intelligence applied to production data. To make semiconductor production smarter, we undertake a thorough examination in this work using Deep Learning and Evolutionary Computing techniques. We provide an algorithm that can adapt to new situations in order to overcome obstacles and gain deeper insights into semiconductor production. This work describes in more detail how an intelligent feature selection algorithm may be developed by combining a Genetic Algorithm with a Neural Network. It aims to shed light on several aspects that enable firms to access effective predictive technologies and offer a cutting-edge solution for regulating industrial processes.
09:15 AM – 09:30 AM Paper ID: 133	**Macro-to-TWh: A Log-Stabilized Benchmark of 21 Supervised Regressors for Country-Level Primary Energy Consumption Prediction** *Authors*: Howlader, Jim; Bin Faruque, Abir; Islam, Maidul; Sahariyar, Hussain Md.; Shawon,Tithi, Afsana; Shauaib; Pramanik, Souvik; Haque Dhrubo, Ahmed Faizul; Qayum, Mohammad Abdul *Abstract*: Accurate estimation of national energy demand is essential for long-term planning, policy design, and sustainable development. This paper presents a comparative study of super- vised regression techniques for predicting country-wise primary energy consumption using macro-level indicators from a large-scale World Energy Consumption dataset (country–year records). After data cleaning and organization by country and year, missing values were handled through interpolation, and a log1p transformation was applied to reduce skewness and stabilize variance. Multiple regression models, including linear baselines and ensemble-based learners, were evaluated under a consistent train–test protocol using standard error metrics (R2, RMSE, MAE, and MAPE). Experimental results show that ensemble methods substantially outperform simpler regressors, confirming the non-linear relationship between the predictors and energy consumption. Among all evaluated models, Gradient Boosting achieved the best overall performance, delivering the highest coefficient of determination and the lowest prediction errors, while other ensemble strategies (e.g., voting and stacking) also produced competitive results. The findings suggest that boosting- based regressors offer a robust and practical approach for macro- level energy consumption estimation, and they provide a strong baseline for future work involving time-aware validation and richer explanatory features.

09:30 AM – 09:45 AM Paper ID: 221	**Voice- and Text-Based Tasking for Swarm Robotics: A Leader-Centric Coordination Framework** *Authors*: Zam Zam Mirza, Qurat Ul Ain; Kanwal, Rimsha ; Ashraf, Humaira ; Jhanjhi, NZ. *Abstract*: Natural language interfaces provide a promising future of simplifying human-swarm interaction by enabling the operator to make high-level commands without the use of lowlevel code or special control panels. Nevertheless, the implementation of multi-robot systems with linguistic communications will pose the difficulties in understanding the commands, real-time dispersing, and reliability of executing tasks simultaneously. In this paper, we give a leaderfollower swarm control architecture where a single leader robot is able to receive spoken or textual instructions and broadcast structured tasks to a group of follower robots via a simple messaging protocol. The system was simulated and tested in Webots with a four-robot system configuration with natural language parsing and pursuit-based and a particle swarm optimization (PSO) search behavior. The experimental data show that the quality of interpretation of the commands can always be high when it concerns the typical operation instructions, whereas the leader-swarm command propagation can have a latency of sub-seconds. The results show that battlefield navigation, formation and search testing can be carried out reliably by swarm agents with minimum positional drift and with stable acknowledgment reporting and this can prove that commands issued in a natural language can be commanded directly to swarm architectures with minimal effect on swarm coordination performance. The presented system supports the viability of the humanswarm-teaming concept and provides it with a basis in the scalable natural-language-powered robots of the future.
09:45 AM – 10:00 AM Paper ID: 263	**Passive On-Device BLE Interference Detection Using TinyML** *Authors*: Jozwik, Cameron; Zhu, Rui *Abstract*: Bluetooth Low Energy (BLE) is widely used in Personal Area Networks (PANs) and Internet of Things (IoT) systems, where operation in shared unlicensed spectrum exposes devices to radio-frequency interference arising from both benign coexistence and intentional disruption. In realistic deployments, such interference often manifests as stealthy behavior at the observation level, making it difficult to distinguish from naturally busy wireless environments. Due to strict resource constraints, most BLE devices lack on-device mechanisms to detect communication-layer disruptions in real time. This paper presents a passive, on-device BLE interference detection system implemented on an ESP32 microcontroller using TinyML. Without transmitting additional packets or modifying the BLE protocol, the system extracts lightweight statistical features from BLE scan windows, including RSSI distributions and activity indicators. A compact neural network is trained offline and deployed using TensorFlow Lite Micro, enabling real-time inference with sub-millisecond latency and minimal memory overhead. Experimental results show that embedded execution is reliable and efficient, while detection robustness is primarily constrained by environmental variability and data representativeness rather than model complexity or hardware limitations, particularly when distinguishing stealthy interference from naturally busy wireless conditions. These findings demonstrate that passive TinyML-based interference awareness is feasible on resource-constrained IoT devices and represents a practical building block for strengthening the security and resilience of BLE-based communication systems.

10:00 AM – 10:15 AM Paper ID: 322	**VPN Queue Performance Analysis Using Matrix Analytics Methods** *Authors*: Yusuf, Idris; Li, Wei *Abstract*: The post-COVID era has witnessed a significant increase in remote work policies, leading to the rapid adoption of Virtual Private Network (VPN) technology. Although VPNs are not a new technology, their widespread use has raised concerns regarding performance evaluation. In a typical VPN connection, users are first authenticated during Phase 1 before being permitted to send and receive data through a secured tunnel in Phase 2, which relies on the prior authentication stage. By modeling the VPN system as a two-phase service process within a single-server queue, this work establishes a theoretical framework for VPN performance analysis using the Matrix Analytic Method (MAM). Our analysis demonstrates that the VPN system can be characterized as a Level-Dependent Quasi Birth-Death (LDQBD) process. The corresponding infinitesimal generator matrix exhibits a block tridiagonal structure, where transitions are allowed only between neighboring states, and the block size increases with each level. Using MAM, we analyze the queueing system in steady state and derive the initial state probability vector. Based on this, several key VPN performance metrics are obtained. Numerical simulations are conducted to validate the theoretical results and confirm the accuracy of the proposed analytical model.
10:15 AM – 10:30 AM Paper ID: 366	**AI-Augmented Manufacturing Execution Systems for Precision Healthcare: A Scalable Framework for Smart Genomic and Proteomic Production** *Authors*: Nalluri, Satish; Bathini, Varun teja; Parasaram, Venkata Krishna Bharadwaj *Abstract*: The increased need to have precision healthcare requires intelligent and scalable manufacturing systems that could provide high-quality, traceability, and regulatory-compliant genomic and proteomic production. Traditional Manufacturing Execution System (MES) are generally weak in the analytical intelligence needed to handle heterogeneous process data and dynamic production conditions of the personalized healthcare manufacturing. To facilitate intelligent analytics on smart genomic and proteomic production environments, the paper suggests an AI-enhanced MES framework to facilitate such analytics. The proposed framework is evaluated by using a domain-inspired MES dataset that includes process parameters, quality indicators, operational metrics, cost attributes, and features of compliance. Preprocessing, scaling of features and balancing of classes SMOTE are used to improve the quality of data and learning strength. Extra Trees and Random Forest classifiers are the ensemble based supervised learning models that are used in predicating quality status in the MES environment. The experimental outcomes reveal that the Extra Trees model is more efficient than the Random Forest classifier, with an accuracy and F1-score of 95.21 and 95.25, respectively. The suggested AI-enabled MES system offers flexible and regulatory intelligent manufacturing in the precision healthcare domain.

Day 3 - Thursday March 26, 2026

Online Session: Paper Presentations | 08:30 AM – 10:15 AM

Online Session 9: Privacy-Preserving and Secure AI/ML: Surveys and Emerging Challenges
Room Link: https://meet.google.com/koq-bocg-evb

TRACK CHAIRS:	Dr. Sanjay Deshpande (Northwestern University)

08:30 AM – 08:45 AM Paper ID: 251	**A Systematic Survey on Cryptography-Driven Privacy in Machine Learning** *Authors*: Zidan, Arif Hassan ; Fouda, Mostafa M. ; Fadlullah , Zubair Md; Ibrahem, Mohamed *Abstract*: Machine Learning as a Service and Federated Learning have become key deployment models for deep neural networks, yet both raise critical privacy concerns: training data, client inputs, and proprietary models can be leaked through model queries, gradients, or aggregation protocols. Recent work shows that models remain vulnerable to membership inference, reconstruction, property inference, and model extraction attacks in realistic settings. In response, researchers increasingly explore cryptographic techniques—particularly approximate homomorphic encryption (HE) and secure multiparty computation (MPC) for privacy-preserving training and inference. This survey covers several representative lines of work. We begin by reviewing Cheon–Kim–Kim–Song (CKKS)-style HE-based Privacy Preserving Machine Learning (PPML) and its application to encrypted inference across tabular, text, image, and audio data. We then examine AutoFHE, which converts Rectified Linear Unit (ReLU)-based Convolutional Neural Networks (CNNs) into polynomial networks optimized for Residue Number System (RNS)-CKKS, balancing accuracy and latency. Next, we analyze PILLAR, ESPN, and HoneyBadger—systems co-designing polynomial activations with single-round MPC protocols for fast secure inference at nearReLU accuracy. Finally, we study ELSA, a two-server aggregation framework enforcing norm-bound updates while protecting client gradients against a malicious server. We compare all approaches across cryptographic primitives, threat models, performance, and applicability, concluding with open challenges and research directions.

08:45 AM – 09:00 AM Paper ID: 271	**Machine Learning for Usable Security: A Survey of User-Centered Approaches** *Authors*: Paul, Aney R.; Eishita, Farjana; Fouda, Mostafa M. *Abstract*: Usable security is where Human-Computer Interaction (HCI) meets cybersecurity. At this intersection, the design of a security system considers how the user thinks, acts, and makes decisions within it. The use of Machine Learning (ML) in usable security has become an effective approach to meeting the needs of both the security system and the user, providing stronger security and a more engaging experience. This survey provides a high-level overview of how recent developments in ML applied to usable security have advanced in four main areas: Authentication, Phishing Detection, Biometric Systems, and Privacy Configurations. We classify the various ML approaches developed in these areas, as well as identify several usability metrics, such as cognitive load, user acceptance, and task efficiency, and the impact of the various ML-based approaches on those metrics. Additionally, we discuss the trade-offs between model precision and system efficiency, with emphasis on the risks associated with false positives and false negatives in security contexts. The study outlines existing challenges, including the need for Explainable Artificial Intelligence (XAI), resilience against adversarial attacks, and ethical data management. Finally, we conclude with proposed future research directions toward the design of deployable, human-centered ML-based security systems.
09:00 AM – 09:15 AM Paper ID: 273	**Federated and Reinforcement Learning for Cyber Defense: A Comprehensive Survey of Emerging Intelligent Security Paradigms** *Authors*: Bajgai, Rishikesh; Ibrahem, Mohamed I.; Fadlullah, Zubair Md; Fouda, Mostafa *Abstract*: With a continuous increase in the use of digital platforms for day-to-day applications and the rapid rise in the complexity and frequency of cyber threats, intelligent, privacy-preserving defense mechanisms are increasingly used across critical domains, such as government, finance, defense, healthcare, and education. Conventional centralized machine learning (ML) methods have been effective to a certain extent. However, they involve sharing sensitive data during model training, thereby posing serious privacy and security risks. On the other hand, federated learning (FL) enables collaborative model development without sharing raw data. This helps ensure confidentiality in a distributed setting. Furthermore, reinforcement learning (RL) learns autonomously and adapts to develop defense strategies that effectively counter evolving cyberattack patterns. We focus on these two ML approaches for the cyber defense application, along with a combination of FL and RL (FL–RL). The paper examines the taxonomy for FL–RL-based cyber defense, system architectures, applications, common attacks, defense strategies, comparative analysis, and future research directions.

09:15 AM – 09:30 AM Paper ID: 332	**Applications and Limitations of Large Language Models in Digital Forensics: A survey** *Authors*: Ashton Saunders, Skyler ; Ibrahem, Mohamed; Abouyoussef, Mahmoud *Abstract*: Digital forensics (DF) plays a critical role in investigating and analyzing digital evidence across criminal and civil cases. Recent advances in Large Language Models (LLMs) have introduced new opportunities to support forensic workflows by automating or assisting tasks such as dataset generation, evidence extraction, analysis, reporting, and investigative support. Despite growing interest in this area, existing studies remain fragmented and lack a comprehensive examination of how LLMs are applied in digital forensics, as well as their associated limitations. This survey systematically reviews recent research on the use of LLMs in digital forensics, categorizing current applications and summarizing representative techniques and outcomes. In addition, the paper analyzes key challenges, including hallucinations, data privacy, explainability, performance cost, and legal admissibility, that currently limit real-world adoption. Finally, the survey outlines open research problems and future directions necessary to enable trustworthy and effective integration of LLMs into digital forensic investigations.
09:30 AM – 09:45 AM Paper ID: 361	**Defending Against Inference-Time Role Drift Attacks on Agentic AI in Healthcare** *Authors*: Fahim, Sanim Yousuf; Hossain, Mohammad Arif; Liu, Weiqi *Abstract*: Agentic artificial intelligence (AI) systems in clinical environments perform multi-step reasoning, tool invocation, and real-time actions over electronic health record (EHR) workflows. While healthcare systems commonly enforce credential- and API-layer role-based access control (RBAC), agentic architectures introduce an additional risk: semantic role manipulation at inference time, where natural-language interactions can steer an agent's tool-routing decisions toward unintended privileges when role context is inferred rather than cryptographically pinned. This paper formalizes Inference-Time Role Drift Attacks (IRDA), in which an adversary uses multi-turn coercion and paraphrasing to shift an agent's perceived operational role and trigger unauthorized tool requests. We propose a Role-Constrained Agentic Firewall (RCAF) that detects role drift using embedding-based consistency checks over multiple signals, including agent reasoning outputs, conversation context, and user messages, and blocks suspicious tool invocations. Using 100 synthetic patient profiles and 2800 attack episodes, IRDA achieves a 92% attack success rate against a baseline that authorizes tool access based on inferred roles. RCAF reduces successful unauthorized tool invocations to 0% at conservative thresholds while detecting drift in 92% of adversarial episodes; however, it also blocks legitimate escalation workflows, exposing a critical security–usability trade-off. We report ablations over embedding models (MiniLM vs. MPNet), detection signals, and threshold sweeps. Overall, the results show that credential-layer controls alone are insufficient when role inference drives tool authorization and that semantic-layer monitoring can mitigate IRDA but requires workflow-aware escalation handling.

09:45 AM – 10:00 AM Paper ID: 394	**Trojan Obfuscation vs. Detection: A Large-Scale Empirical Study of Evasion** *Authors*: Saleh, Khaled *Abstract*: We present a large-scale empirical study of how code obfuscation impacts Trojan detection. To our knowledge, no prior work has produced a Trojan-specific dataset with com- parable obfuscation variety. From 197 PE-based Trojan samples we generated 6,993 obfuscated variants using 45 techniques spanning packing, control-flow and data transformations, API- level evasion, encryption, and VM-based schemes. Variants were evaluated across six independent testing ecosystems (70+ en- gines). Obfuscation reduced mean Trojan detection from 73.84% to 22.30%—a drop of 51.54 pp—and 70.5% of variants achieved complete evasion (0% detection). Effects were consistent across platforms and highly significant ($t = 31.47$, $p < 0.0001$; Mann– Whitney $Z = -58.2$, $p < 0.0001$), with a very large effect (Cohen's $d = 1.76$) and low heterogeneity ($I2 = 8\%$). Cross- platform correlations ($r > 0.89$) suggest a systemic weakness in static/signature-driven Trojan detection. This work establishes a reproducible benchmark and methodological milestone for Trojan evasion research.
10:00 AM – 10:15 AM Paper ID: 395	**Trojan Attribution via Code Stylometry: Writing Behaviors and Coding Habits in Obfuscated Binaries** *Authors*: Saleh, Khaled *Abstract*: Attributing obfuscated Trojans to authors remains challenging because transformation obscures structure. We inves- tigate whether code authorship—inferred from writing behaviors and coding style—survives obfuscation in Trojan binaries. Using a survey-aligned taxonomy (lexical, syntactic, semantic), we run an attribution pipeline on 440 samples (224 original, 216 obfuscated) including Trojans from the Malware Analysis and Obfuscation Dataset. Findings: original samples decompile at 83.5%, obfuscated at 0%; byte n-grams reach 99.3%; lexical evidence dominates (2.42/3 avg) and drops sharply for obfuscated; coding habits (70.2% while vs. 14.8% for) survive compilation but vanish when decompilation fails. For obfuscated Trojans, only byte-level and lexical signals persist—syntactic and semantic collapse. We discuss implications for Trojan attribution under obfuscation.

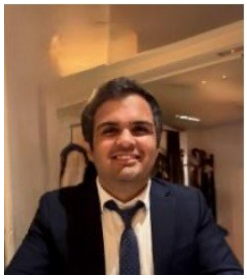
Invited Talk

Room Link: https://meet.google.com/fij-icdz-rrx

Day 3 - Thursday March 26, 2026

10:30 AM – 11:00 AM

Plenary Session I
Invited Talk



Micro-architectural Security in Heterogeneous System-on-Chips

Session Chairs:

Dr. Weiqi Liu, Auburn University at Montgomery

Presenter/Speaker:

Dr. Usman Ali, ASIC/SoC Micro-architectural and Security Engineer, Meta

Abstract: The integration of diverse, specialized processing units within high-performance Heterogeneous System-on-Chip (HSoC) architectures has significantly expanded the micro-architectural attack surface. As performance requirements necessitate the extensive sharing of hardware resources, components such as Network-on-Chip (NoC) fabrics, PCIe interconnects, and complex multi-level cache hierarchies have emerged as primary vectors for side-channel leakage and cross-domain exploitation. Centering on the inherent "security-performance trade-off" in modern silicon, this talk examines how resource contention and interconnect congestion can be leveraged to bypass traditional isolation boundaries and countermeasures for securing the next generation of energy-efficient, high-performance computing platforms.

Speaker Bio: Usman Ali, Ph.D. is a researcher and engineer in high-performance computer architectures and hardware security, with a focus on micro-architectural security in heterogeneous systems-on-chip (SoCs). His work investigates vulnerabilities in Network-on-Chip (NoC), interconnects (PCIe), memory subsystems, and cache hierarchies, and develops innovative defenses to secure high-performance computing platforms. Dr. Ali holds a Ph.D. in Electrical Engineering from the University of Connecticut and has published in top-tier hardware security and computer architecture venues, including IEEE HOST, SEED, and ICCD. His research advances the state of the art in secure, energy-efficient heterogeneous SoC designs, providing insights into both attacks and countermeasures. Dr. Ali's work bridges academia and industry, shaping secure and high-performance computing architectures that influence both research and practical systems design.

Invited Talk

Room Link: https://meet.google.com/fij-icdz-rrx

Day 3 - Thursday March 26, 2026

11:00 AM – 11:30 AM

Plenary Session I
Invited Talk

Assuring Trusted AI and Microelectronics for Critical Infrastructure Security

Session Chairs:

Dr. Weiqi Liu, Auburn University at Montgomery

Presenter/Speaker:

Prof. Kenneth M. Hopkinson, Air Force Institute of Technology (AFIT)

Abstract: This talk explores advances in AI and trusted microelectronics security for protecting critical infrastructure. Dr. Kenneth M. Hopkinson will highlight the role of cognitive radios, sensor fusion, and remote sensing technologies in securing essential critical systems like AF, military communication networks and power grids. The discussion will cover emerging cryptographic protocols and the integration of security solutions into assured and trusted systems and aerospace applications.

Speaker Bio: Dr. Kenneth M. Hopkinson is a Professor of Computer Science and Department Head of Electrical and Computer Engineering at the Air Force Institute of Technology (AFIT) in Dayton, Ohio. He is a Senior Member of the IEEE and ACM professional societies. Proficient in Networking, Security, Cryptography, Remote Sensing, Sensor Fusion, Critical Infrastructure Protection, and Space Applications, he has made significant research contributions that enhance national security and technological advancements.

Day 3 End