SaTC International Conference

# Secure and Trustworthy Cyberinfrastructure for IoT and Microelectronics (SaTC 2025)

Holiday Inn Dayton

2800 Presidential Drive Fairborn, OH 45324

IEEE DAYTON

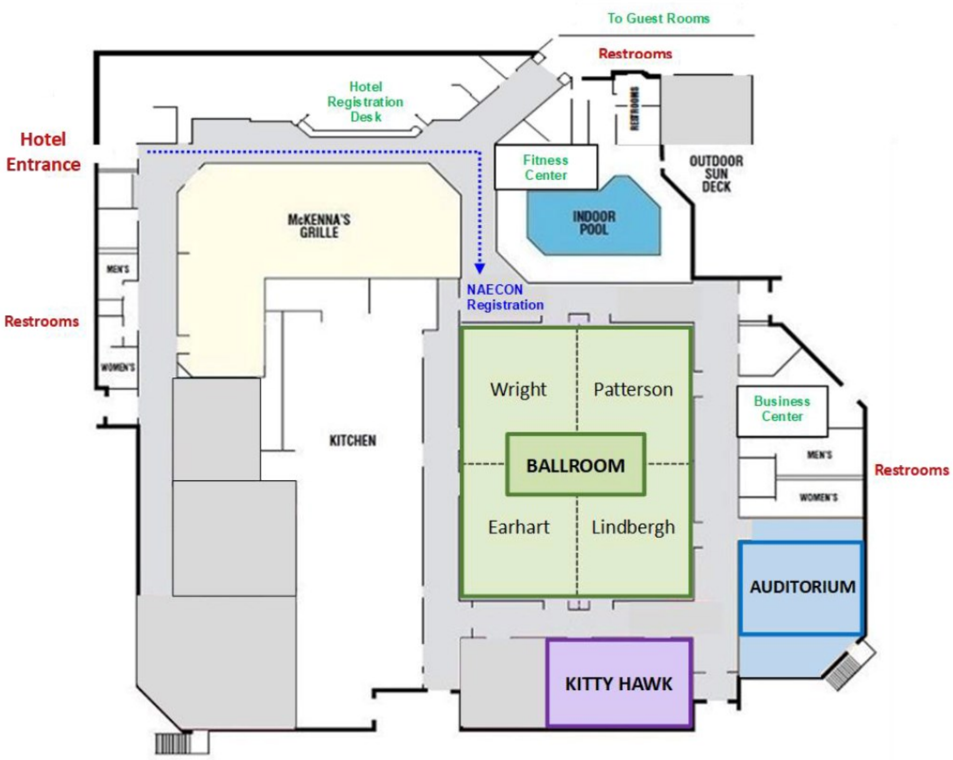
DAYTON, OH EST. 1943

THE CENTER OF AEROSPACE INNOVATION

# CONTENTS

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

## Venue Floor Plan



## WIFI ACCESS CODE (Holiday Inn): FBNPD

# CHAIR’S MESSAGE

## Welcome to the 1st IEE Conference on Secure and Trustworthy Cyberinfrastructure for IoT and Microelectronics

## SaTC 2025

It is with great pleasure that I welcome you to the inauguration of the first IEEE Conference on Secure and Trustworthy Cyberinfrastructure for IoT and Microelectronics (SaTC 2025) here in Dayton, Ohio. 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

WRIGHT STATE UNIVERSITY
ESTABLISHED 1967

**“We empower all students to excel in their lives and chosen careers through integrated learning, research, innovation, and experience.”**

**To be a diverse, inclusive university that positively transforms the educational, economic, and social fabric of the communities Wright State University serves.**

**ACADEMIC DEANS**

**DARRYL K. AHNER,**
Ph.D. Engineering and Computer Science

**SUBHASHINI GANAPATHY,**
Ph.D. Graduate Programs and Honors Studies

**DONALD H. HOPKINS, JR., M.B.A.**
Raj Soin College of Business (interim)

**AY E AHIN, Ph.D.**
Science and Mathematics

**GARY SCHMIDT, Ph.D.**
Liberal Arts

**MARTY SEXTON, Ph.D., RN, FNAP**
Health, Education, and Human Services (interim)

**GREGORY TOUSSAINT, M.D.**
Boonshoft School of Medicine (interim)

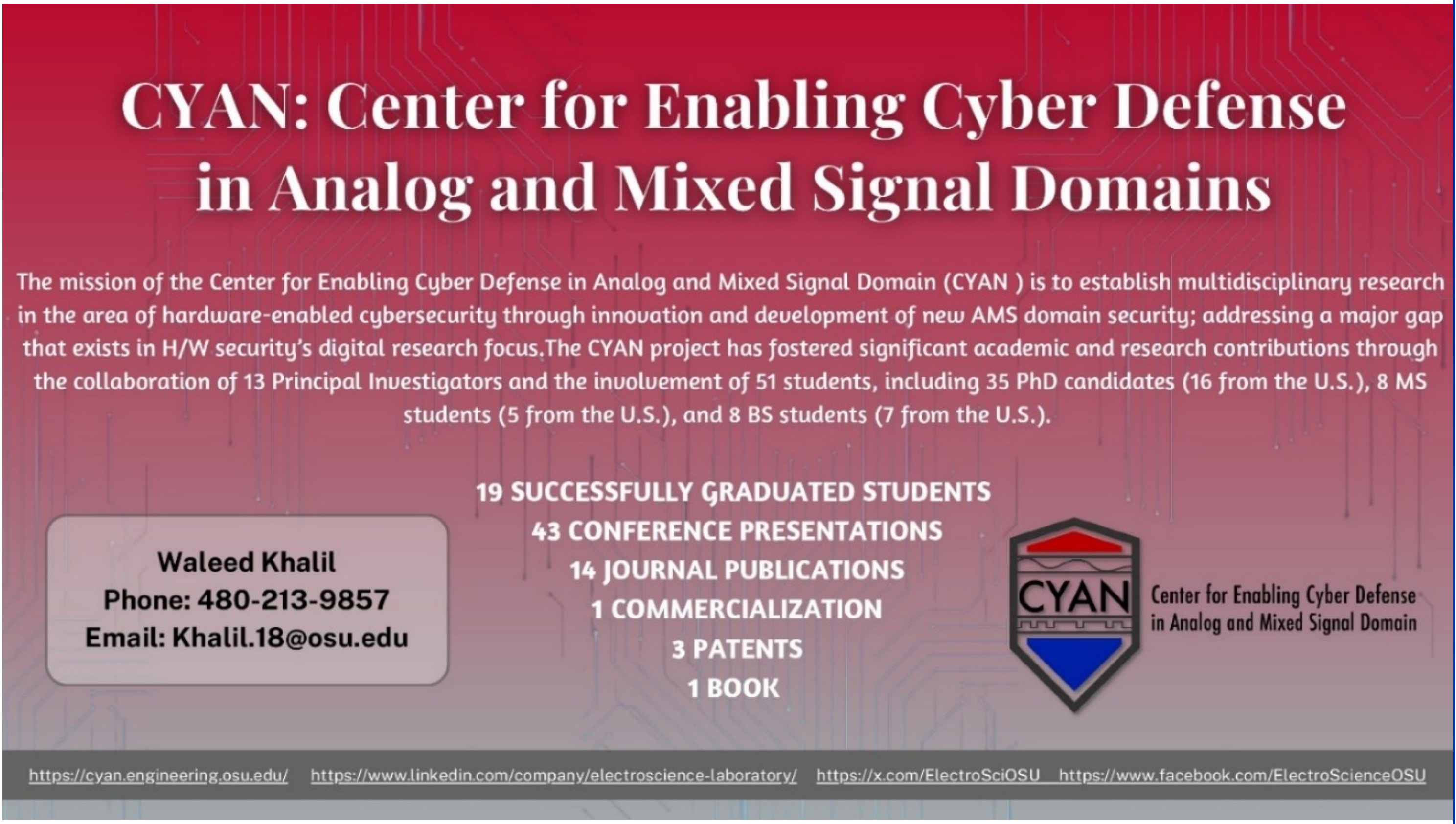
**More Than 11K Students**
**2 campuses (Dayton and Lake)**
**14: 1 ; Student-to-Faculty Ratio**
**Minority Strudents Enrollment (26%)**
**International Strudents from 72 countries (14%)**
**169 Graduate Programs and 177 Undergraduate programs**

## MIDWEST MICROELECTRONICS CONSORTIUM

MMEC leads the acceleration of microelectronic technologies and delivers solutions to establish a trusted and resilient domestic supply chain. The MMEC is the premier collaborative, public-private ecosystem, that engages broadly across innovative partners in industry, academia and government to rapidly advance defense and commercial applications. This unique environment empowers members to discover new technologies, share capabilities, develop a skilled workforce and launch groundbreaking innovation into scalable commercial production for the benefit of National Security and economic dominance.

**Leigh Drinkard**
(509)990-4036
LDrinkard@mmeconsortium.org
**Karsten Olson**
(509)869-2846
KOlson@mmeconsortium.org

MMEC™
ACCELERATE : COLLABORATE : EXECUTE



# CYAN: Center for Enabling Cyber Defense in Analog and Mixed Signal Domains

The mission of the Center for Enabling Cyber Defense in Analog and Mixed Signal Domain (CYAN ) is to establish multidisciplinary research in the area of hardware-enabled cybersecurity through innovation and development of new AMS domain security; addressing a major gap that exists in H/W security's digital research focus.The CYAN project has fostered significant academic and research contributions through the collaboration of 13 Principal Investigators and the involvement of 51 students, including 35 PhD candidates (16 from the U.S.), 8 MS students (5 from the U.S.), and 8 BS students (7 from the U.S.).

Waleed Khalil
Phone: 480-213-9857
Email: Khalil.18@osu.edu

19 SUCCESSFULLY GRADUATED STUDENTS
43 CONFERENCE PRESENTATIONS
14 JOURNAL PUBLICATIONS
1 COMMERCIALIZATION
3 PATENTS
1 BOOK

CYAN
Center for Enabling Cyber Defense
in Analog and Mixed Signal Domain

https://cyan.engineering.osu.edu/ https://www.linkedin.com/company/electroscience-laboratory/ https://x.com/ElectroSciOSU https://www.facebook.com/ElectroScienceOSU

# CORE PARTNERSHIP/ATTENDANCE: ACADEMIC INSTITUTIONS, GOVERNMENT, AND INVITED SPEAKERS

AFRL
THE AIR FORCE RESEARCH LABORATORY
LEAD | DISCOVER | DEVELOP | DELIVER

Ansys
POWERING INNOVATION THAT DRIVES HUMAN ADVANCEMENT™

Ohio™
CyberOhio

NSTXL
NATIONAL SECURITY TECHNOLOGY ACCELERATOR

NATIONAL CENTERS OF ACADEMIC EXCELLENCE
IN CYBERSECURITY

CINSER@CSU
CENTER FOR INFORMATION & SECURITY EDUCATION AND RESEARCH
CHICAGO STATE UNIVERSITY

TAYLOR'S
UNIVERSITY
Wisdom · Integrity · Excellence

EXPEDIENT
TECHNOLOGY SOLUTIONS, LLC

Parallax
ADVANCED RESEARCH

OHIO
NORTHERN
UNIVERSITY

O
THE OHIO STATE
UNIVERSITY

MICROELECTRONICS
COMMONS
BRIDGING THE GAP FROM LAB TO FAB
Microelectronics Commons

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

NSF

MMEC™
MIDWEST MICROELECTRONICS CONSORTIUM

# OPENING REMARK

Day 1 - Tuesday February 25, 2025

**08:05 AM – 08:15 AM**

**Welcome Notes, Opening Remarks, and Overview of the IEEE and SaTC Conference Vision**

*Session Chair*:

Dr. Tara Salman, Texas Tech University

Prof. Waleed Khalil, Ohio State University

*Presenter*: Dr. Fathi Amsaad, Wright State University

**ABSTRACT:** Professor Fathi Amsaad welcomes attendees to the 1st IEEE Conference on Secure and Trustworthy Cyberinfrastructure for IoT and Microelectronics (SaTC 2025). This session will provide an overview of the conference's key objectives, including fostering interdisciplinary discussions on securing emerging technologies and enhancing trust across systems. Professor Amsaad will emphasize the importance of collaboration between academia, industry, and government in addressing the critical challenges of assured supply chain security, microelectronics, and IoT applications.

**BIOGRAPHY:** Dr. Fathi Amsaad is an Assistant Professor in the Department of Computer Science and Engineering (CSE) with a joint appointment in the Department of Biomedical, Industrial, and Human Factors Engineering (BIHFE) at Wright State University. He earned his Ph.D. in Engineering with a specialization in Computer Science and Engineering from the University of Toledo in 2017. Dr. Amsaad directs the Semiconductor Microelectronics Security, Assurance, Resilience, and Trust (SMART) Cybersecurity Research Lab at the Joshi Research Center. His research focuses on Cyber and Physical System Security, particularly Hardware-Oriented Security and Trust (HOST). His expertise includes microelectronic circuit protection, cryptographic hardware security, secure SoC design, additive manufacturing security, counterfeit detection, hardware side-channel attack countermeasures, and zero-trust security for COTS components.

Ballroom

# OPENING REMARK

Day 1 - Tuesday February 25, 2025

**08:15 AM – 08:30 AM**

**Welcome Notes, Opening Remarks, and Overview of the IEEE and SaTC Conference Vision**

*Session Chair*:
Dr. Tara Salman, Texas Tech University
Prof. Waleed Khalil, Ohio State University

*Presenter*: Prof. Guru Subramanyam, University of Dayton

**ABSTRACT:** The Dayton Section of IEEE welcomes all conference delegates and presents an overview of its mission, initiatives, and planned activities for the year. Key events and programs are highlighted, emphasizing their role in fostering collaboration, innovation, and professional development within the engineering community.

**BIOGRAPHY:** Dr. Guru Subramanyam is currently a Professor of Electrical and Computer Engineering at the University of Dayton. He has published over 175 refereed journals and conference papers in the area of electronic materials and devices. His current research involves oxide thin films for reconfigurable RF/microwave circuits, and sensors. He has been collaborating with Air Force Research Laboratory (AFRL) in these areas since 2000. His work to date has been funded by NASA, AFRL, AFOSR, NSF, and DARPA. Professor Subramanyam won the 2008 Alumni award for Scholarship at the University of Dayton, and 2007 IEEE Harrell Noble Award from the IEEE Dayton Section. In 2013, University of Dayton opened the Center of Excellence for Thin-film Research and Surface Engineering (CETRASE) under his leadership. He is currently the Chair of the IEEE Dayton section, and Region 2 Coordinator for the IEEE Microwave Theory and Technology Society (MTTS).

# OPENING REMARK

Day 1 - Tuesday February 25, 2025

**08:30 AM – 08:45 AM**

**Welcome Notes, Opening Remarks, and Overview of the IEEE and SaTC Conference Vision**

*Session Chair*:

Dr. Tara Salman, Texas Tech University

Prof. Waleed Khalil, Ohio State University

*Presenter*: Ms. Felicia N Reinhart

**ABSTRACT:** This presentation provides an overview of IEEE Region 2 within the broader organizational structure of IEEE and the responsibilities of the Region Director. Key priorities for 2025, upcoming regional events, and opportunities for member engagement will be discussed.

**BIOGRAPHY:** Felicia currently serves on the IEEE Board of Directors which is the largest technical professional society in the world dedicated to advancing technology for the benefit of humanity. As a director, she also oversees Region 2, one of the 10 Regions that span the globe. Her role also includes serving on the IEEE Board of Directors, the IEEE Member and Geographic Activities Board, and the IEEE-USA Board. Felicia retired in 2024 after a 32-year career that included 18 years at the Air Force Research Laboratory (AFRL) and her retirement from active duty in the US Air Force in 2005. She started out in the AFRL Information Directorate working on distributed collaborative systems, then moved on to the AFRL Sensors Directorate where her research included developing cyber protections for avionics systems. She concluded her career as a security research engineer developing technology tools and solutions for the Department of Defense security & intelligence community. Her diversified experience included managing a $10M state-of-the-art lab supporting multiple in-house research missions and to her last focus on managing a multimillion-dollar digital transformation effort to serve the Air Force Security community enterprise. She received her B.S. in Computer Engineering from the University of Central Florida (summa cum laude) and her M.S. in Computer Engineering from the Air Force Institute of Technology. She lives in Beavercreek, OH with her dog, Bixby.

Ballroom

# OPENING REMARK

Day 1 - Tuesday February 25, 2025

**08:45 AM – 09:00 AM**

**Welcome Notes, Opening Remarks, and Overview of the IEEE and SaTC Conference Vision**

*Session Chair*:

Dr. Tara Salman, Texas Tech University

Prof. Waleed Khalil, Ohio State University

*Presenter*: Dr. Darryl K. Ahner, Wright State University

**ABSTRACT:** The College of Engineering and Computer Science at Wright State University welcomes all conference attendees and highlights its commitment to research, innovation, and workforce development. This session provides an overview of the college's initiatives, including its focus on assured microelectronics research and its role in advancing security and trust in emerging technologies.

**BIOGRAPHY:** Dr. Darryl K. Ahner is the Dean of the College of Engineering and Computer Science at Wright State University. He holds a Ph.D. in Systems Engineering from Boston University and has two master's degrees from Rensselaer Polytechnic Institute. Before joining Wright State, he served as the Dean for Research at the Air Force Institute of Technology (AFIT) and was the founding Director of the OSD Scientific Test and Analysis Techniques in Test and Evaluation Center of Excellence. His research focuses on stochastic models, dynamic programming, military operations research, and complex system modeling. He has secured over $7.8 million in research funding, authored 75 technical articles, and received multiple awards, including the OSD Medal for Exceptional Civilian Service and the ITEA Allen R. Matthews Award.

# KEYNOTE PRESENTATIONS

Day 1 - Tuesday February 25, 2025

**09:05 AM – 09:45 AM**

**Fueling transformation for Security, Trust, and Assurance – No Excuses!**

*Session Chair*: Prof. Waleed Khalil, Ohio State University

*Presenter*: Dr. Mathew Casto, CTO, Midwest Microelectronics Consortium (MMEC), Inc.

**ABSTRACT:** Microelectronics are critical to all aspects of modern life and imperative for national security.  As the technology and its producing sources grow more complex, the products and systems that consume microelectronics, and especially those with long life applications, are at an increasing risk of cyber-physical vulnerabilities, IP theft, diminishing sources, counterfeit issues, and obsolescence. Developing a sustainable innovation ecosystem for trusted and assured semiconductor and microelectronic supply chains can be catalyzed with an emphasis on the first principles of innovation, focused by a "No-Excuse" roadmap. This talked will explore the challenges and opportunities in developing such an ecosystem, including the mechanisms to incentivize collaboration between academia, industry, and government across commercial and defense sectors to build market differentiating products and resilient systems.

**BIOGRAPHY:** Dr. Matthew Casto is the Chief Technology Officer of The Midwest Microelectronics Consortium (MMEC), where he leads technological innovation and directs product research and development from the laboratory to commercialization. Dr. Casto holds B.S. and M.S. degrees in Electrical Engineering from Wright State University and a Ph.D. in Electrical and Computer Engineering from The Ohio State University. He joined MMEC in 2023, after serving over 20 years in various technical leadership roles within the Department of Defense (DoD), including as Director of the DoD Trusted and Assured Microelectronics (T&AM) Program and Senior Strategic Advisor for Microelectronics Innovation at the U.S. Air Force. Dr. Casto also led sensor and countermeasure technology development for airman and guardians at the Air Force Research Laboratory, and most recently led the delivery of high-volume smart, secure access control products as CTO and SVP of Engineering and Manufacturing at the Genie Company. He has authored over 50 publications, patents, and invited talks and was inducted into the IEEE Hardware Oriented Security and Trust (HOST) Hall of Fame in 2020. He is also a 2025 recipient of the Presidential Early Career Award for Scientists and Engineers (PECASE).

# INVITED TALK

Day 1 - Tuesday February 25, 2025

**09:45 AM – 10:00 AM**

**Breaking Barriers - Accelerating Semiconductor Growth**

*Session Chair*: Prof. Waleed Khalil, Ohio State University

*Presenter*: Mr. Salman Nasir, Director, National Center for the Advancement of Semiconductor Technology

**Abstract:** Our world faces significant challenges that also present remarkable opportunities for technological advancements. Semiconductors are crucial in addressing global needs in energy, healthcare, automotive technologies, and communications. This keynote explores how innovations in semiconductor technology, such as advanced model architectures and system partitioning, can drive sustainable growth and energy efficiency. The need for co-optimization across the system stack—while maintaining rigorous security standards—is essential to ensure both performance and resilience. The National Semiconductor Technology Center (NSTC) will play a vital role in fostering collaboration and ensuring that the U.S. remains a leader in technological innovation.

**Speaker Bio**: Mr. Salman Nasir is the Director of the Program Management Office at Natcast, overseeing R&D programs. Previously, he was the Programs & Site Lead at Battelle's Dayton facility, managing Microelectronics Security Research and Hardware Assurance programs. He has over a decade of R&D experience particularly in microelectronic hardware, RF communication, EO/IR sensors, high-performance computing, image processing, and compound semiconductor devices. Mr. Nasir holds an MBA, an MS in Electrical Engineering, and a BS in Electrical Engineering. Mr. Nasir is a certified PMP® and Six Sigma Black Belt, with multiple industry and DoD awards, including the Defense Manufacturing Technology Achievement Award.

| 10:00 AM – 10:10 AM | Coffee Break |
|---|---|

Ballroom

## Day 1 - Tuesday February 25, 2025

## REGULAR SESSION 1: PAPER PRESENTATIONS (10:10 AM – 11:30 AM)

| | |
|---|---|
| SESSION CHAIRS: | Dr. Love Kumar Sah, *Assistant Professor of Electrical & Computer Engineering, Western New England University* |

For the Online Session please Use the Link below:
https://meet.google.com/vzf-odhq-vgq

or scan the QR Code

| **Session 1: Hardware Design, Side-Channel Analysis and PUF-based Security & Trust** | |
|---|---|
| 10:10 AM - 10:30 AM<br>Paper 1 (online) | **iPUF: A Novel Security-by-Design Paradigm to Mitigate Data Manipulation and External Attacks in Cyber-Physical Systems**<br>*Authors*: Seema Aarella, Sameer Agarwal, Saraju Mohanty, and Elias Kougianos<br>*Abstract*: Fault Injection attack is a type of side-channel attack on the Physical Unclonable Function (PUF) module that can induce faults in the PUF response by manipulating the PUF circuit behavior through voltage glitches, laser attacks, temperature manipulations, or any other attacks potentially leading to information loss or security system failure. This type of attack exposes the physical characteristics of PUFs that can be analyzed to predict or compromise the unique challenge response pairs (CRPs) reducing the security and reliability of the PUF. Mitigation strategies against such attacks typically include adding noise to the PUF output, using error-correcting codes, or enhanced cryptographic protocols that obscure physical side-channel attacks. In this research, we propose a Generative Adversarial Network (GAN) based security model, that monitors the PUF behavior and detects the variations in PUF response. The model can detect glitches in the PUF response and generate alerts to take mitigation measures. |
| 10:30 AM – 10:50 AM<br>Paper 42 | **Hardware based Obfuscation for Secure and Trusted System: A Comprehensive Study**<br>*Authors*: Khaled Saleh, Fathi Amsaad, Omar Darwish<br>*Abstract*: Hardware obfuscation techniques aim to pro tect integrated circuits (ICs) from reverse engineering and intellectual property theft by making their designs harder to understand. This survey explores various types of hardware obfuscation, such as logic locking, camouflage, and layout camouflaging, assessing their effectiveness and usability. It examines their purpose in safeguarding ICs against unauthorized access, highlighting challenges and advancements in implementing these techniques in modern semiconductor design. Hardware obfuscation techniques are used to strengthen the security of integrated circuits (ICs) by making their designs more complicated and hard to analyze, consequently preventing reverse engineering and intellectual property theft. The review looks at different forms of hardware obfuscation, including logic locking, camouflage, and layout camouflaging, evaluating their efficacy and usability. The article explores the role of securing integrated circuits (ICs) from unauthorized access, focusing on the problems and improvements in integrating these strategies in contemporary semiconductor architecture. |

| | |
|---|---|
| 10:50 AM – 11:10 AM<br>Paper 81 | **Design and Implementation of Approximate Multiplier Using Approximate 4-2 Compressors and Approximate Half Adders**<br>*Authors*: Lakshmi Sowjanya Koneru, Sneha Ramagiri, Dr.Prakash Kodali<br>*Abstract*: In real-time Advanced computing applications such as image processing, neural networks and digital signal pro- cessing (DSP), Approximate multipliers are designed to provide acceptable results while conserving power, hardware resources and improving speed with bounded inaccuracies. In this paper we design an Approximate Multiplier using Approximate compressor and Approximate Half Adders to gain less power consumption for approximate computing. The experimental results indicate 89.47% decrease in area, 86.82% decrease in power and 48.057% decrease in the area delay for proposed 8x8 multiplier compared to exact multiplier. The accuracy percentage for the proposed multiplier is 77.5%. The proposed design is coded in Verilog HDL and simulated using Xilinx VIVADO tool. |
| 11:10 AM – 11:30 AM<br>Paper 148 (online) | **Vulnerability Analysis Employing Generative Adversarial Network Model of a Ring Oscillator Physical Unclonable Function**<br>*Author*: Talha Hussain Syed, Akshay Raghavendra Kulkarni, and Mohammed Niamat<br>*Abstract:* Physical Unclonable Functions (PUFs) are critical to authentication and assurance of integrated circuits (ICs), by leveraging inherent manufacturing process variations in the semiconductor chips to generate unique Challenge-Response Pairs (CRPs). This research investigates the susceptibility of FPGA based Ring Oscillator Physical Unclonable Function (ROPUF) by predicting its CRPs using machine learning models and Generative Artificial Intelligence (Gen-AI). An essential component of this research is identifying potential security risks to prevent the incorporation of vulnerable components into secure applications. In this paper, we consider a plausible scenario where an adversary illicitly acquires 5% of the CRP dataset, and a Generative Adversarial Network (GAN) is used to generate synthetic CRPs that are subsequently added to augment the training dataset by 35%. With this augmented data, machine learning models demonstrate a notable improvement in predictive accuracy. Decision Tree (DT) prediction accuracy increases from 60.17% to 67.15%, K-Nearest Neighbors (KNN) from 64.67% to 72.17%, Random Forest Classifier (RF) from 67.83% to 75.74%, and Extreme Gradient Boosting (XGB) from 73.83% to 83.41%. This enhanced predictive capability reveals that machine learning models even with partial datasets augmented using GAN models can predict the original CRPs with increased accuracy. |

## Day 1 - Tuesday February 25, 2025

## REGULAR SESSION 2: PAPER PRESENTATIONS (10:10 AM – 11:25 AM)

| | |
|---|---|
| SESSION CHAIRS: | Dr. Rafiul Kabir, *Assistant Professor of Computer Engineering, Central Michigan University* |

For the Online Session please Use the Link below: https://meet.google.com/fmw-vhoa-amw

or scan the QR Code

| **Session 2: Exploration of Automotive and Safety and Security** | |
|---|---|
| 10:10 AM - 10:35 AM<br>Paper 164 (online) | **HEMA: A Hands-on Exploration Platform for MEMS Sensor Attacks**<br>*Authors*: Bhagawat Baanav Yedla Ravi, Md Rafiul Kabir, Sandip Ray<br>Abstract: Automotive safety and security are paramount in the rapidly advancing landscape of vehicular technology. Building safe and secure vehicles demands a profound understanding of automotive systems, particularly in safety and security. Traditional learning approaches, such as reading materials or observing demonstrations, often fail to provide the practical, handson experience essential for developing this expertise. For novice users, gaining access to automotive-grade systems and mastering their associated hardware and software can be challenging and overwhelming. In this paper, we present a novel, affordable, and flexible exploration platform, HEMA, that enables users to gain practical, hands-on insights into the security compromises of micro-electromechanical systems (MEMS) sensors, a critical component in modern ADAS systems. Furthermore, we discuss the unique challenges and design considerations involved in creating such a platform, emphasizing its role in enhancing the understanding of automotive safety and security. This framework serves as an invaluable resource for educators, researchers, and practitioners striving to build expertise in the field. |
| 10:35 AM – 11:00 AM<br>Paper 170 (online) | **TinyML-Enabled Intrusion Detection for Securing Eletric vehicle Supply Equipment (EVSE)**<br>*Authors*: Sunil Thapa, Sushil Poudel; Mohmoud Abouyoussef<br>Abstract: Electric Vehicles (EVs) and Electric Vehicle Supply Equipments (EVSEs) are vulnerable to cybersecurity threats like malware injections, unauthorized access, denial-of-service (DoS) attacks, distributed denial-of-service (DDoS) attacks, and man-in-the-middle (MITM) attacks, all of which can compromise their functionality and security. While Machine Learning (ML) effectively addresses cybersecurity threats, implementing traditional ML solutions in EVSE is challenging due to resource limitations, requiring lightweight and efficient solution to ensure effective threat detection and mitigation. Tiny Machine Learning (TinyML) is an emerging solution that opens up the possibility of running ML models on resource-constrained devices, making it ideal for implementing Intrusion Detection Systems (IDS) in EVSE charger units. This paper explores the potential of TinyML as an effective solution for enhancing EVSE cybersecurity. The proposed TinyML model is evaluated using the Hardware |

| | |
|---|---|
| | Performance Counter (HPC) and Network data sources of CICEVSE2024 dataset, achieving accuracies of 98.72% and 99.84%, F1-scores of 98.65% and 99.83%, recall scores of 98.72% and 99.84%, and precision scores of 98.88% and 99.84%, respectively. |
| 11:00 AM – 11:25 AM<br>Paper 206 (Online) | **An AI-Spatial Analysis of Traffic Crash Severity in Proximity to High Schools in Ann Arbor, Michigan**<br>*Authors*: Lina Ahmed, Tehetna Hailu, Omar Darwish, Suleiman Ashur *<br>Abstract: This study investigates the use of Artificial Intelligence (AI) and spatial analysis to predict traffic crash severity near high schools in Ann Arbor, Michigan. Given the unique challenges of high pedestrian activity, student drivers, and congested traffic during school hours, this research employs a machine learning model and SHAP, an AI Explainability algorithm, to analyze factors influencing crash severity. The primary objective is to identify key contributors to crash severity, including weather conditions, road classifications, speed limits, and crash times. Data imbalances are addressed through techniques like Synthetic Minority Oversampling (SMOTE) to enhance model performance. Spatial analysis was performed using Geographic Information Systems (GIS) data, evaluating the impact of proximity to schools and traffic conditions on crash severity. Results indicate that road type, pedestrian presence, and other contextual factors significantly affect crash severity, with certain areas near schools identified as high-risk zones. This study highlights the potential of AI-driven models combined with spatial analysis to inform traffic safety interventions and policy development in school zones. |

## Day 1 - Tuesday February 25, 2025

## REGULAR SESSION 3: PAPER PRESENTATIONS (10:10 AM – 11:30 AM)

| | |
|---|---|
| SESSION CHAIRS: | Dr. Akshay Kulkarni, *Assistant Professor, Prairie View A&M University*<br>Dr. Mohammed Niamat, *Professor of Electrical Engineering and Computer Science, University of Toledo* |

For the Online Session please Use the Link below: https://meet.google.com/ger-nwyc-bqf

or scan the QR Code

| **Session 3: Energy-Efficient Wireless Protocols for IoT** | |
|---|---|
| 10:10 AM – 10:35AM | **Optimizing Resource Allocation for 5G-IoT Networks Using Machine Learning Techniques** |
| Paper 51 (Online) | *Authors*: Sara Kengesbayeva*, Abdul Razaque, Nurzhigit Smailov, Zhuldyz Kalpeyeva, Uskenbayeva Raissa Kabievna<br>*Abstract*: The development of smart devices and the enhancement of the 5G network pose a challenge in the management of resources especially in the dynamic and high-density networks. This paper proposes a machine learning approach for the optimization of resource allocation for 5G Internet-of-things (IoT) networks. The framework integrates real-time data processing, dynamic routing and edge computing for the improvement of the network throughput and quality of service (QoS). The suggested methods have been developed and evaluated in MATLAB simulations have shown important enhancements in latency, bandwidth and energy efficiency. Through the overcoming the limitations of the conventional methods, this research offers the solutions for the resource allocation problem in the 5G-IoT networks which are scalable, adaptive and efficient. |
| 10:35 AM – 11:00 AM | **A TDMA Algorithm for Multi-Hop Energy Harvesting Wireless Sensor Networks: Restricted Tree Topology** |
| Paper 153 | *Authors*: Alexander Burkholder, Tanner Patterson, Ahmed Ammar*, Khalid Al-Olimat<br>*Abstract*: This paper proposes a time-division multiple access (TDMA) algorithm for energy-harvesting wireless sensor networks (WSNs) with a restricted tree topology. The proposed algorithm supports various transmission scenarios, including single-hop, dual-hop, and multi-hop transmissions. It allows a sensor node to synchronize either with a synchronization packet from the base station or a packet from a neighboring node within its communication range, while effectively addressing clock drift issues. The results demonstrate that the proposed algorithm performs comparably to state-of-the-art algorithm, but with a shorter time synchronization interval, as it does not perform individual synchronization of branches. In addition, the results indicate that the time synchronization interval depends on the clock drift rate, which varies across nodes. |

| | |
|---|---|
| 11:00 AM – 11:25 AM | **Network Layer Attack Performance Measurement in Wireless Sensor Network Using Parallel Computing** |
| Paper 160 | *Authors: Sufian Al majmaie*, Mithun Kumar PK, Fathi Amsaad*<br>*Abstract*: Efficient execution of computationally complex operations in edge environments requires decomposition into concurrent sub-computations. One significant application of parallel computation is in Wireless Sensor Networks (WSNs), for whom extending network life is paramount for reliable performance. Efficient techniques for distributing tasks have a key role in minimizing computation and consumption of energy. This research proposes a parallel routing mechanism for WSNs for enhancing system performance, particularly in cases of network layer attack scenarios. Malicious nodes were installed and incorporated in a proposed algorithm for testing its performance. There is no mechanism in use that tests network layer attack scenarios in parallel computation for a specific observation period, even when WSNs have high volumes of metadata and data to manage. The scheme was analyzed under Black Hole, Gray Hole, and Sybil attack environments, with key performance factors including Packet Delivery Fraction (PDF), Normalized Routing Load (NRL), and Throughput measured. Results exhibit significant computation time savings with parallel processing compared to sequential computation. With one attack and 49 ordinary nodes, file tracking attained 171.8MB, growing exponentially to 735.2MB with four attack nodes. With multi-core architectures (2, 4, and 8 cores), proposed parallel processing outpaces sequential approaches with performance improvement of over four times. Results confirm that parallel computation enables real-time attack detection, network robustness, and efficiency in WSNs with high-density sensors. |
| **11:30 AM – 1:00 PM** | **LUNCH BUFFET OPEN (ROOM: BALLROOM)** |
| **11:30 AM – 12:10 PM** | **BREAK AND NETWORKING OPPORTUNITY-I** |

Ballroom

# LUNCHEON KEYNOTE PRESENTATION

Day 1 - Tuesday February 25, 2025

**12:10 PM – 12:45 PM**

**Hardware Side-Channel and Non-Destructive Techniques for Trusted Microelectronics**
*Session Chair:* Mr. Aaron Miller, Galois, Inc
*Presenter:* Mr. P. Len Orlando III, Senior Business Development Executive at ANSYS

**Abstract:** Mr. P. Len Orlando III will discuss the critical role of side-channel analysis in securing microelectronics, especially in the Federal, Aerospace, and Defense sectors. Drawing from his extensive experience at the Air Force Research Laboratory and Ansys, he will examine how side-channel vulnerabilities affect the security and trust of semiconductor systems. The session will explore Ansys' efforts to develop advanced tools for side-channel analysis, leveraging Electronic Design Automation (EDA) technologies and scalable cloud solutions to enhance hardware security. Mr. Orlando will provide insights into cutting-edge research aimed at protecting hardware from side-channel attacks, highlighting the technical advancements and practical applications in the semiconductor field.

**Session Chair Bio**: Mr. P. Len Orlando III is a Senior Business Development Executive at Ansys, within the Ansys Government Initiatives (AGI) business unit. He joined Ansys in January 2023 to lead semiconductor efforts focused on the Federal, Aerospace, and Defense marketplace. Prior to joining Ansys, Mr. Orlando served 21 years as a Senior Scientist at the Air Force Research Laboratory, Sensors Directorate. He holds a B.S. degree in Electrical and Computer Engineering from The Ohio State University and an M.S. degree in Electrical Engineering from the University of Dayton. His career spans several diverse areas, including trust and assurance, RF MMIC and AMS design, EDA infrastructure, and scalable cloud deployment.

| | |
|---|---|
| **12:45 PM – 1:00 PM** | **BREAK AND PANEL SETUP** |

# PANEL DISCUSSION

Day 1 - Tuesday February 25, 2025

**13:00 PM – 14:10 PM**

**Software/Hardware Co-Design Solutions: Assured and Trusted Microelectronics, IoT Security, and Side Channel Analysis**

MODERATOR:

Mr. Len Orlando III
(Senior Business Development Executive, Ansys)

**Panel Overview:** This panel brings together leading experts from industry and top academic institutions in the U.S. specializing in assured and trusted systems. The discussion will focus on the critical challenges and advancements in assured and trusted microelectronics, IoT security, and side-channel analysis, emphasizing their role in developing secure and high-performance software/hardware co-design solutions. Panelists will explore ASIC and AI-driven co-design architectures, heterogeneous system integration, reconfigurable computing, and mixed-signal security, addressing emerging vulnerabilities in modern embedded systems. Additionally, the panel will highlight strategies for mitigating side-channel threats and enhancing system confidentiality, integrity, and availability, ensuring resilience in microelectronics. Experts will also examine key design trade-offs, power efficiency, and real-time constraints, providing insights into the future of co-optimized hardware/software security solutions.

## Panelists:

Dr. Waleed Khalil, Professor and Associate Director of the Electro Science Laboratory, Ohio State University

Panelist Bio: Dr. Waleed Khalil is a Professor of Electrical and Computer Engineering at The Ohio State University and Associate Director of the Electro Science Laboratory. He founded the Circuit Laboratory for Advanced Sensors and Systems (CLASS) and co-leads the CYAN Center of Excellence. Before joining OSU, he spent 16 years at Intel in wireless and wireline communications. His research focuses on integrated circuits, hardware security, and heterogeneous chip integration. He holds 19 patents, has published over 120 papers, and is currently serving as General Co-chair for the IEEE International Symposium on Hardware Oriented Security and Trust (HOST)

# PANEL DISCUSSION

Day 1 - Tuesday February 25, 2025

**13:00 PM – 14:10 PM**

**Software/Hardware Co-Design Solutions: Assured and Trusted Microelectronics, IoT Security, and Side Channel Analysis**

Panelists (Continued):

Dr. Richard Ott, Technical Director, Air Force Institute of Technology (AFIT)

Panelist Bio: Dr. Richard Ott is the Technical Director of the Digital Innovation and Integration Center of Excellence (DIICE) at the Air Force Institute of Technology, where he is responsible for guiding the development and execution of the center's strategic vision, ensuring technical quality of projects and programs, and fostering collaboration across various Air Force organizations, joint services, and OSD. Though his role spans a broad portfolio, he has as keen interest in ensuring secure and assured systems and works to apply Digital Materiel Management approaches to advance cyber physical applications. Before assuming this role, Dr. Ott spent time as the Assistant Chief Scientist at the Sensors Directorate of the Air Force Research Laboratory. Earlier during his tenure at AFRL, he was the Air Force Verification and Validation Lead for OSD's Trusted Electronics program, leading research on methods to improve microelectronic counterfeit detection and supply chain assurance – where he led the JFAC ASSESS Working Group, evaluating second order effect system capability and working to link measured observables to their physical origin. Dr. Ott earned a Bachelor of Arts in Physics from Ohio Wesleyan University, followed by a Master's in Mechanical Engineering from the University of Akron, a Ph.D. in Mechanical Engineering from Utah State University, and he has completed Air War College. He has over 30 peer reviewed publications, proceedings, or patents, and has delivered visionary and keynote talks on several occasions, as well as authored numerous technical reports, test plans, and test reports throughout his career.

# PANEL DISCUSSION

Day 1 - Tuesday February 25, 2025

**13:00 PM – 14:10 PM**

**Software/Hardware Co-Design Solutions: Assured and Trusted Microelectronics, IoT Security, and Side Channel Analysis**

Panelists (Continued):

Dr. Matthew Areno, CEO and co-owner, Rickert-Areno Engineering and Consulting

Panelist Bio: Dr. Matthew Areno is the CTO of Rickert-Areno Engineering, LLC and Chief Solutions Architecture for CloudTank. He completed his bachelor's and master's degrees at Utah State University in 2007 and began his career at Sandia National Laboratories, focusing on vulnerability assessment and reverse engineering of embedded systems using ARM-core processors. He also earned a PhD from the University of New Mexico, where his dissertation explored enhancing embedded system security with PUF-enhanced cryptographic units. Dr. Areno then joined Raytheon Cyber Security Innovations as Chief Architect, specializing in anti-tamper solutions and establishing trust in Commercial-off-the-Shelf (COTS) equipment. In 2019, he moved to Intel, where he held roles such as Senior Director of Security Assurance and Cryptography, Chief Security Architect, and Anti-Tamper Lead. He serves on the Board of Advisors for Augusta University School of Computer and Cyber Sciences, as co-chair of the Secure Edge Working Group under the Midwest ME-Commons Consortium, and on the Editorial Board for the Journal of Hardware and Systems Security.

Mr. Aaron Miller, Strategy and Technology Transition Leader, Galois Inc.

Panelist Bio: Aaron Miller is the Strategy and Technology Transition Leader at Galois, specializing in secure systems, systems engineering, and digital transformation with a software focus. He co-founded two startups—Tangram Flex, a component-oriented engineering company, and Niobium Microsystems, a silicon design company specializing in high-assurance cryptographic and model-based designs. With a background in systems engineering and a master's degree from the University of Dayton, Aaron is dedicated to advancing methodologies for building high-quality, cost-effective systems. At Galois, he collaborates with leading researchers worldwide to identify, develop, and transition cutting-edge technologies that enhance the security and reliability of software and cyber-physical systems. His expertise bridges research, industry, and government, driving innovation in hardware/software co-design and system trustworthiness.

| **2:10 PM – 2:20 PM** | **COFFEE BREAK** |
|---|---|

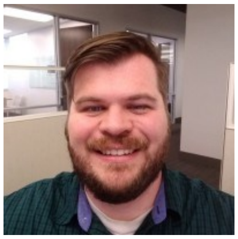
Ballroom

# INVITED TALK

Day 1 - Tuesday February 25, 2025

**14:20 PM – 15:20 PM**

Session Chair: Mr. Dominic Mohrhardt , *Air Force Life Cycle Management Center (AFLCMC) KC-46*
*Presenter:* Prof. Kenneth M. Hopkinson, *Chair Computer Science Department, Airforce Institute of Technology (AFIT)*
*Presenter:* Dr. Matt Areno, *Senior Principal Security Architect Engineer at Intel*



**Session Chair Bio:** Dominic Mohrhardt is a senior computer and electrical engineer, curtly a Ph.D. student at Wright State University, researching hardware security and trust in the SMART Lab under the supervision of Dr. Amsaad. He is also with the Air Force Life Cycle Management Center (AFLCMC) KC-46 program, contributing to critical aerospace and defense systems. With industry experience at Milwaukee Tool, VadaTech Inc., and JCM Global, he has worked on advanced electronic systems, including FPGA-based designs, motor drives, and wireless communication. Specializing in RISC and ARM architectures, EMC compliance, and power electronics, Dominic bridges hardware and software through innovative co-design methodologies, driving advancements in trusted microelectronics for defense and commercial applications.

## Speakers:

Prof. Kenneth M. Hopkinson **(14:30 PM - 15:00 PM)**

**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.

Ballroom

# INVITED TALK

Day 1 - Tuesday February 25, 2025

**14:20 PM – 15:20 PM**

**Speakers (Continued):**

Dr. Matt Areno **(15:00 PM - 15:20 PM)**

**Abstract:** Innovation vs Security: The Perpetual Tug-of-War. The last few decades have exemplified the continuous struggle between fostering and sustaining innovation while ensuring secure deployment and runtime. Security has often been seen as being diametrically opposed to convenience. Let's face it, how often do we see an Instagram reel or social media post about how wicked-cool or ingenious some new piece of technology is versus posts about how secure that technology is? And when we do see those posts about security, it is typically from the creator of the technology and not by its users. Recognizing the world of electronics is at an inflection point with the advances of artificial intelligence and post quantum computing, it is imperative that we overcome this perceived conflict between innovation and security at a time when our cyberinfrastructure is under its greatest threat in history. If we fail, our critical infrastructure won't be far behind.

**Speaker Bio:** Dr Matthew Areno is the CEO and co-owner of Rickert-Areno Engineering and Consulting. Dr. Areno completed his bachelor's and master's degrees at Utah State University in 2007 and took a position with Sandia National Laboratories. At Sandia, he focused on vulnerability assessment and reverse engineering of embedded systems primarily utilizing ARM-core processors. During this time, he also completed his PhD at the University of New Mexico with dissertation work on strengthening embedded system security through the use of PUF-enhanced cryptographic units. In 2013, Dr. Areno took a position with Raytheon Cyber Security Innovations in Austin, TX; he served as a Chief Architect for a number of anti-tamper solutions, with specific expertise in establishing trust in COTS equipment. In 2019, he joined Intel where he served as a Senior Principal Engineer and had roles including the Senior Director of Security Assurance and Cryptography, Chief Security Architect, and Anti-Tamper Lead. Dr Areno serves on the Board of Advisors for Augusta University School of Computer and Cyber Sciences, as the co-chair of the Secure Edge Working Group under the Midwest ME-Commons Consortium, and on the Editorial Board for the Journal of Hardware and Systems Security. And if you're still awake at this point, Geaux Tigers!

| **3:20 PM – 3:30 PM** | **COFFEE BREAK** |
|---|---|

Ballroom

## Day 1 - Tuesday February 25, 2025

## REGULAR SESSION 4: PAPER PRESENTATIONS (15:30 PM – 16:50 PM)

| | |
|---|---|
| SESSION CHAIRS: | Dr. Ahmed Ammar, *Assistant Professor of Electrical & Computer Engineering, Ohio Northern University*<br>Dr. Moussa Ayyash, *Professor of Computer Science, Chicago State University* |

For the Online Session please Use the Link below: https://meet.google.com/vzf-odhq-vgq

or scan the QR Code

| **Session 4: Trustworthy AI and Cyber-Physical Security in Smart Cities and IIoT** | |
|---|---|
| 15:30 PM – 15:50 PM<br>Paper 114 | **Securing AI-Driven ECG Classification with Robust Defense Against Boundary Attacks**<br>*Authors*: Ucchwas Talukder Utsha, Tara Salman, Bashir I. Morshed<br>*Abstract*: Machine learning based electrocardiogram (ECG) classification systems are essential for cardiac monitoring but remain vulnerable to adversarial attacks, which can compromise patient safety. This study investigates the vulnerability of a Convolutional Neural Network (CNN) trained on the MIT-BIH Arrhythmia Dataset under adversarial attacks. We specifically focus on boundary attacks, which are black-box adversarial attacks that perturb ECG signals to induce misclassifications without requiring access to the model's internal architecture or parameters. To mitigate these attacks, the paper employs adversarial training as a defense mechanism by retraining the model with adversarial examples to improve its robustness. Our experimental results demonstrate that the attack success rate decreases from 88.00% on smaller subsets (100 samples) to 69.97% on larger subsets (10,000 samples), highlighting the importance of dataset size and diversity in evaluating model vulnerability. After applying adversarial training, the retrained model achieved significant resilience, reducing the attack success rate to 11.39% on newly generated unseen adversarial signals while maintaining a clean signal accuracy of 94.57%. These results demonstrate the effectiveness of the proposed defense mechanism against blackbox attacks. The defense-enhanced model can be integrated into real-time cardiac monitoring systems to ensure accurate beat classification, improving patient safety and reducing the risk of misdiagnosis from adversarial attacks. |
| 15:50 PM – 16:10 PM<br>Paper 151 | **Mitigating Gradient Inversion Attacks in Energy Theft using Hierarchical Federated Learning**<br>*Authors*: Syeda Sanjana Sahid, Tara Salman; Mohamed Baza<br>*Abstract*: Energy theft in smart grids is a widespread challenge that impacts utility providers and consumers. The advancement of machine learning (ML) combined with the amount of data produced by smart grids can help resolve the problem by building efficient ML models to detect such attacks. However, preserving data privacy in energy theft detection remains a crucial challenge. Federated Learning (FL) can enable distributed learning by sharing local data. However, FL is still vulnerable to gradient inversion attacks, where an adversary can reconstruct private data from shared gradient updates. This paper is the first to address gradient inversion attacks for numerical datasets and propose hierarchical federated learning (HFL) to mitigate such attacks in energy theft detection applications. HFL introduces a hierarchical structure with intermediate edge nodes that aggregate client gradients before passing them to the server. This structure limits direct communication between clients and servers, reducing attack surfaces and enhancing data privacy. The approach investigates the effectiveness of HFL against gradient inversion attacks, focusing on iDLG (Improved Deep Leakage from Gradients). Our evaluation demonstrates that HFL balances model accuracy and privacy, significantly lowering the attack success rate at the server by 342 times compared to traditional FL. |

| | |
|---|---|
| 16:10 PM – 16:30 PM<br>Paper 16 (online) | **Improving Transparency and Privacy in Financial Fraud Detection with Explainable AI and Federated Learning**<br>*Authors*: Nimit Bhardwaj |

| | |
|---|---|
| | *Abstract*: The pervasive issue of fraudulent transactions presents a considerable challenge for financial institutions globally. Developing innovative fraud detection systems is critical to maintaining customer confidence. However, several factors complicate the creating of effective and efficient fraud detection systems. Notably, fraudulent transactions are infrequent, resulting in imbalanced transaction datasets where legitimate transactions vastly outnumber instances of fraud. This data imbalance can concede the performance of fraud detection. Additionally, stringent data privacy regulations prevent the sharing of customer data, hindering the development of high-performing centralized models. Furthermore, fraud detection mechanisms must remain transparent to avoid impairing the user experience. This research proposes an approach utilizing Federated Learning (FL) with Explainable Artificial Intelligence (XAI) to overcome these obstacles. FL allows financial organizations to train fraud detection models collaboratively without requiring direct data sharing. So, customer confidentiality and data privacy are never compromised. Simultaneously, the incorporation of XAI guarantees that the model's predictions are interpretable by human experts. Experimental evaluations using real-time transaction datasets consistently demonstrate that the FL-based fraud detection system performs well. This study establishes the potential of FL as a reliable, privacy-preserving tool in combating fraud. |
| 16:30 PM – 16:50 PM<br>Paper 5 (online) | **FedSecure: A Robust Federated Learning Framework for Adaptive Anomaly Detection and Poisoning Attack Mitigation in IoMT**<br>*Authors*: Fawaz Alruwaili *, Saraju Mohanty, Elias Kougianos<br>*Abstract*: Federated learning (FL) is a valuable solution for training models on distributed data with maintaining privacy. However, FL also introduces new security threats such as, poisoning attacks, where learning process can be compromised by malicious clients. While many studies have addressed FL security, data diversity is not considered in many of these studies, which reduces their generalization in real-world applications. In this paper, we propose FedSecure, an adaptive and decentralized anomaly detection framework to mitigate poisoning attacks within Internet of Medical Things (IoMT). FedSecure integrates deep learning models (Bi-LSTM autoencoder and a DNN classifier) to capture complex patterns. FedSecure is tested on diverse real-world datasets, achieving accuracies of 95.4% for Bi-LSTM and 99.96% for DNN. Experimental results show FedSecure ability in detecting and mitigating poisoning attacks which enhances FL security in real-world IoMT environments. |

## Day 1 - Tuesday February 25, 2025
## REGULAR SESSION 5: PAPER PRESENTATIONS (15:30 PM – 16:45 PM)

| | |
|---|---|
| SESSION CHAIRS: | Dr. Ahmed Oun, *Assistant Professor of Electrical Engineering and Computer Science, Ohio University*<br>Dr. Love Kumar Sah, *Assistant Professor of Electrical & Computer Engineering, Western New England University* |

For the Online Session please Use the Link below: https://meet.google.com/fmw-vhoa-amw or scan the QR Code

| Session 5: Security and Privacy-Aware Schemes for Internet of Things (IoTs) | |
|---|---|
| 15:30 PM – 15:50 PM<br>Paper 49 | **Trojan Threats in Quantum Computing Hardware: SFQ Control and Readout Vulnerabilities**<br>*Authors*: Ayisat Adedokun *, Selçuk Köse, Yerzhan Mustafa<br>*Abstract*: The frequency-sensitive properties of superconducting systems render them susceptible to malicious attacks which pose significant risks to quantum computing hardware. A novel single flux quantum (SFQ)-based hardware Trojan, termed as pulse-interleaved Trojan (PI-Trojan), designed to exploit these vulnerabilities is proposed in this paper.<br>Embedded within a frequency divider circuit, the PI-Trojan is evaluated for its threat potential at both low and high frequencies.<br>The Trojan is designed to remain inactive during standard low-frequency testing and to be selectively activated at higher operational frequencies, specifically targeting qubit control and readout operations.<br>Extensive simulations demonstrate the PI-Trojan ability to disrupt clock signals, which can potentially destabilize qubit synchronization, and compromise data integrity, emphasizing the urgent need for a robust security framework to protect superconducting quantum systems from such covert threats. |
| 15:50 PM – 16:10 PM<br>Paper 14 (online) | **SecFarm: An IoT Application Framework to Aid Farmers with a Secured Farm System**<br>*Authors*: Mahdi Shamsa<br>*Abstract*: TAs humans, we coexist alongside animals on our planet. Depending on this truth; adapting to them is essential for several reasons. Some people obtain their sustenance from Livestock, preserving our lives, etc. Agricultural products are crucial for humanity, and their preservation is a fundamental human responsibility. Animals are one of the threats to crop production. In this phase, it is forbidden to kill, harm, or imprison them. Simultaneously managing crops and animals is one of the most challenging jobs farmers undertake. Monitoring crop growth on the farm and protecting them from animals is an addressed issue in this paper. A system has been developed to aid farmers in safeguarding crops and preventing animal-related losses. The proposed approach is capable of deterring animals from crops without inflicting harm or damage. The proposed system utilizes You Only Look Once version 5 (YOLOv5) along with a high-quality dataset to facilitate the classification of hazardous objects detected by the camera. |

| | |
|---|---|
| 16:10 PM – 16:30 PM<br>Paper 58 (online) | **Adversarial Vulnerabilities in OCC-based Intrusion Detection Systems for IoT Security**<br>*Authors*: Mohamed Baza<br>*Abstract*: The rapid expansion of Internet of Things (IoT) technologies has transformed interactions between physical and digital systems, driving advancements in smart cities, healthcare, and industrial automation. However, the distributed nature of IoT devices and the vast volumes of data they generate make them prime targets for cyber threats. Intrusion Detection Systems (IDS), enhanced by machine learning, are vital for identifying and mitigating these threats. This paper examines evasion attacks within a one-class classification (OCC) framework, a machine learning technique for anomaly detection, focusing on adversarial attacks like the Fast Gradient Sign Method (FGSM) and Projected Gradient Descent (PGD). The study explores vulnerabilities in OCC models within IoT systems, including autoencoders and support vector machines (SVM). Experimental results reveal a significant drop in model performance due to adversarial perturbations, highlighting the need for more robust defenses in OCC-based IDS for IoT security. |
| 16:30 PM – 16:50 PM<br>Paper 116 | **Fuzzy Logic based Zero Trust Architecture for Security of AMI in Smart Grids**<br>*Authors: Hrishav Bhattarai*, Akshay Kulkarni, Mohammed Niamat*<br>*Abstract: The shift from traditional power grids to smart grids (SG) has made delivering electricity more efficient and sustainable, but it has also brought new cybersecurity challenges, especially in the Advanced Metering Infrastructure (AMI) ecosystem, which collects, sends, and analyzes energy and data across a network of users and devices. However, AMI systems are vulnerable to unauthorized access and data breaches, risking energy theft and service disruptions due to their distributed and interconnected nature. This paper introduces a novel trust score based Zero Trust Architecture (ZTA) using fuzzy logic to secure AMI, employing a flexible security model that goes beyond traditional fixed-rule approaches. In this approach, fuzzy logic is used to calculate trust scores based on a range of factors, including but not limited to user activity, device details, and the timing of access. Each of these factors help shape a trust score that reflects how safe and trustworthy each access attempt is. Access is only granted if both, the overall trust score, and specific individual scores meet certain set levels. This ensures that unauthorized access is blocked even if some factors look safe while others do not. The simulation results show how this model can protect AMI by stopping unauthorized access and keeping the data secure. This fuzzy logic based ZTA provides a flexible and smarter method for securing smart grid networks against growing cyber threats and helps keep smart grid networks safe as they evolve.* |

Kitty Hawk

## Day 1 - Tuesday February 25, 2025

## REGULAR SESSION 6: PAPER PRESENTATIONS (15:30 PM – 16:50 PM)

| | |
|---|---|
| SESSION CHAIRS: | Dr. Tara Salman, *Assistant Professor of Computer Science, Texas Tech University*<br>Dr. Akshay Kulkarni, Assistant Professor, Prairie View A&M University |

For the Online Session please Use the Link below:
https://meet.google.com/ger-nwyc-bqf

or scan the QR Code

| **Session 6: Emerging Technologies and Applications in Secure and Intelligent Systems** | |
|---|---|
| 15:50 PM – 16:10 PM | **Bio-powered IoT nodes: Low-power systems in remote Environments** |
| Paper 156 | *Authors*: Anwar Elhadad*<br>*Abstract*: The widespread adoption of Internet of Things (IoT) networks is hindered by the lack of reliable and sustainable power sources. Traditional batteries are expensive, environmentally harmful, and impractical for many applications, particularly in remote environments. While energy harvesting techniques offer alternatives, they often face challenges related to integration, safety, and inconsistent performance. This research presents a successful integration of a miniaturized, microbial fuel cell (MFC) array powered by photosynthetic electrogenic bacteria. Our MFC array enabled us to effectively power a long-range LORA wireless system for data transmission over distances of approximately 750 meters. The compact and environmentally friendly design of our MFC array allows for seamless integration into remote ecosystems, providing a sustainable and reliable energy source for IoT nodes in such environments. This innovation has the potential to unlock the full potential of IoT networks in various applications, including environmental monitoring and underwater exploration. |

| | |
|---|---|
| 16:10 PM – 16:30 PM | **Gaussian process as feature selection method for regression tasks: comparison with classic methods** |
| Paper 38 | *Authors*: Abdul Razaque*, Ajmal Khan, Kazhimulin Diyas |
| | *Abstract*: Feature selection is a crucial stage in the development of machine learning models, especially for regression issues where extraneous or duplicated information may compromise the model's interpretability and accuracy. In this study, we analyze and compare the efficacy of several feature selection techniques, with a focus on a novel use of Gaussian Processes (GPs), a technique frequently used for hyperparameter optimization, for feature selection. This is opposed with traditional feature selection algorithms that have been extensively utilized in regression modeling, such as Principal Component Analysis (PCA), Least Absolute Shrinkage and Selection Operator (LASSO), and Recursive Feature Elimination (RFE). The main research topic is: How well do various feature selection strategies work for regression problems, especially when contrasting Gaussian Processes with conventional approaches? We test each method's performance with regards to model intelligibility, computational expediency, prediction correctness, and feature significance on a number of datasets of regression. In addition, we explore the importance of feature selection not only for improving the models' performance in the high-dimensional noisy or irrelevant dataset but also for their robustness in generalization.<br/>By means of a number of tests, we show that whereas conventional techniques such as RFE and LASSO are effective in some situations, Gaussian Processes provide a versatile, probabilistic strategy that can surpass existing techniques in terms of striking a balance between model complexity and performance. |
| 16:30 PM – 16:50 PM | **Adaptive Morphological Operations for Space Debris and Satellite Tracking with AI-Powered Multi-Resolution Data Fusion** |
| Paper 169 | *Authors:* Mithun Kumar Pk, Soham Roy, Fathi Amsaad*, Darryl Ahner |
| | *Abstract:* Space situational awareness (SSA) faces critical challenges due to the exponential growth of satellites and space debris, creating an urgent need for enhanced tracking capabilities. This research addresses the limitations of current tracking systems using electro-optical image fusion by introducing an innovative framework combining adaptive filtering, multiresolution data fusion, and morphological operations. We propose a Vertical and Horizontal Adaptive Median (VHADMED) filter to reduce sensor noise while preserving object features, coupled with an AI-powered multi-resolution data fusion approach that integrates information. Additionally, the proposed adaptive morphological operations enhance object detection and tracking capabilities through dynamic structural elements. Experimental results show that the VHADMED filter reduces noise by 98% while maintaining edge integrity, and the multi-resolution fusion framework improves object detection accuracy by 97%. The system successfully tracks 99.9% of identified space objects across consecutive frames but the existing research's accuracy is 97.76% based on CNN-based model, demonstrating significant advancement in debris and satellite tracking for enhanced space traffic management. |

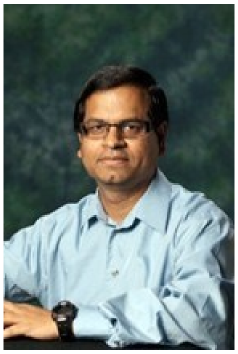
Ballroom

# INVITED TALK

Day 1 - Tuesday February 25, 2025

**16:50 PM – 17:20 PM**

**Cyberfortifying CPS through Security-by-Design**
*Session Chair:* Dr. Love Kumar Sah (Western New England University)
*Presenter:* Prof. Saraju Mohanty (University of North Texas)



**Abstract**: Smart cities use one or multiple smart systems (or components) including smart healthcare, smart agriculture, and smart energy, and hence is a system of systems. The various systems of the smart cities are essentially cyber-physical systems (CPS) made of 3Cs (Computation, Communications, and Control). While connectivity is the key for IoT-enabled CPS, it brings in various forms of cyber-attacks on its devices, systems, and data. The existing cybersecurity solutions have serious resources, energy and latency overheads making them impossible for use in CPScomponents like medical devices, smart cars, and UAVs. Blockchain based solutions is being explored in almost every application in smart cities. However, blockchains have significant energy, latency, and scalability issues and not suitable for resource constrained frameworks. This talk will present broad perspectives of the vast multifaceted forms of cybersecurity attacks and secure/security by design (SbD) solutions in CPS. SbD advocate making cybersecurity as a requirement right in the design phase so that retrofitting would not be needed. The talk will present SbD driven cybersecurity solutions for CPS or IoT usingthe hardware security primitive Physical Unclonable Function (PUF). The talk will address many questions about SbD including: (1) What are the challenges of cybersecurity? (2) What is SbD?(3) What are the 7 principles of SbD? (4) What is Hardware-Assisted Security (HAS)? (5) How SbD can be used for IoT/CPS? (6) What are specific examples SbD deployment in CPS?

**Speaker Bio**: Dr. Saraju Mohanty is a Professor at the University of North Texas. Prof. Mohanty's research is in "Smart Electronic Systems" which has been funded by NSF, SRC, US Air Force, IUSSTF, and Mission Innovation. He has over 20 years of research experience on security and protection of media, hardware, and systems. He introduced the Secure Digital Camera (SDC) in 2004 with built-in security features designed using HardwareAssisted Security (HAS) or Security by Design (SbD) principle. He is widely credited as the designer for the first digital watermarking chip in 2004 and first the low-power digital watermarking chip in 2006. He has authored 550 research articles, 5 books, and 10granted and pending patents. His Google Scholar h-index is 59 and i10-index is 282 with 16,000 citations. He is a recipient of 21 best paper awards, Fulbright Specialist Award in 2021, IEEE Consumer Electronics Society Outstanding Service Award in 2020, and the PROSE Award for Best Textbook in Physical Sciences and Mathematics category in 2016. He has delivered 31 keynotes and served on 15 panels at various International Conferences. He has been serving on the editorial board of several peer-reviewed international journals, including IEEE Transactions on Bigdata, IEEE Transactions on CAD as well as EiC of IEEE Consumer Electronics Magazine. He is the steering committee chair/vice-chair for the IEEE International Symposium on Smart Electronic Systems (iSES), the IEEE-CS Symposium on VLSI (ISVLSI), and the OITS International Conference on Information Technology (OCIT). He has supervised 3 post-doctoral researchers, 17 Ph.D. dissertations, 28 M.S. theses, and 41 undergraduate-research projects.

Ballroom

# INVITED TALK

Day 1 - Tuesday February 25, 2025

**17:20 PM – 17:50 PM**

**Advancing Cybersecurity and AI for Secure Microelectronics: A Global Perspective**

*Session Chair:* Dr. Love Kumar Sah (Western New England University)

*Presenter:* Prof. Noor Zaman Jhanjhi (Taylor's University)

**Abstract**: This talk explores the integration of Artificial Intelligence (AI) and Cybersecurity in securing microelectronics, with a focus on the emerging challenges in IoT and edge computing systems. It will cover innovative AI-driven solutions for enhancing the security, resilience, and trustworthiness of microelectronic systems and supply chains. The discussion will also address the role of AI in identifying and mitigating evolving threats, and the significance of interdisciplinary collaboration in strengthening digital infrastructures. Key global research trends and the transformative potential of these technologies in ensuring secure and trusted systems will also be highlighted.

**Speaker Bio**: Prof. Dr. Noor Zaman Jhanjhi is a highly esteemed Senior Professor of Computer Science, specializing in Artificial Intelligence and Cybersecurity. He currently holds the position of Professor at the School of Computer Science at Taylor's University, Malaysia, and serves as the Program Director for Postgraduate Research Degree Programmes as well as the Director of Research Center. With a career marked by academic leadership and groundbreaking research, Prof. Jhanjhi has been pivotal in advancing research and education in computer science. Recognized globally, Prof. Jhanjhi has been ranked among the world's top 2% research scientists for three consecutive years (2022, 2023, and 2024). In Malaysia, he is ranked among the top three computer science researchers and was honored with the Outstanding Faculty Member award by MDEC Malaysia in 2022, as well as the Vice Chancellor's Best Research Citations Award from Taylor's University in 2023. His impressive academic portfolio includes over 70 research books edited or authored with prestigious publishers such as Springer, Elsevier, Taylor & Francis, Wiley, and IGI Global USA. His research has garnered more than 1000 points in impact factor, reflecting the depth and breadth of his contributions to the field. A dedicated mentor, Prof. Jhanjhi has supervised and co-supervised 38 postgraduate students to successful graduation and has served as an external examiner for over 60 Ph.D. and Master's theses globally. In addition to his academic accomplishments, Prof. Jhanjhi holds Associate Editor and Editorial Board positions with several high-ranking journals, including PeerJ Computer Science, CMC Computers, Materials & Continua, and Frontiers in Communication and Networks. He was also recognized as an Outstanding Associate Editor for IEEE ACCESS. His contributions to research and innovation are further demonstrated by his successful management of over 40 internationally funded research grants.

A sought-after keynote speaker, Prof. Jhanjhi has delivered over 70 invited talks at international conferences and has chaired numerous sessions. His commitment to academic excellence and accreditation extends to his involvement with ABET, NCAAA, and NCEAC over the past decade.

| | | |
|---|---|---|
| **16:50 PM – 18:30 PM** | **Sa1TC Reception & Networking Opportunity** | Ballroom/Foyer |

End of Day 1

# KEYNOTE PRESENTATIONS

Day 2 - Wednesday February 26, 2025

**08:20 AM – 09:00 AM**

**Hardware Security 2.0 (and the Unmistakable Role of Generative AI)**
*Session Chair:* Prof. Moussa Ayyash, Chicago State University
*Presenter:* Prof. Swarup Bhunia (IEEE Fellow), University of Florida

**Session Chair Bio**: Dr. Moussa Ayyash is a Professor in the Department of Computing, Information, and Mathematical Sciences and Technology at Chicago State University, where he also serves as the Director of the Center of Information and Security Education and Research (CINSER). He holds a B.S., M.S., and Ph.D. in Electrical and Computer Engineering. Dr. Ayyash's research interests encompass a broad range of areas, including digital and data communication, wireless networking, visible light communications, network security, artificial intelligence (AI), the Internet of Things (IoT), and interference mitigation. His work focuses on advancing communication systems and security, as well as developing innovative solutions to mitigate interference in modern wireless networks and IoT applications.

Ballroom

# KEYNOTE PRESENTATIONS

Day 2 - Wednesday February 26, 2025

**08:20 AM – 09:00 AM**

**Hardware Security 2.0: An AI-Enabled Future**
*Session Chair:* Prof. Moussa Ayyash, Chicago State University
*Presenter:* Prof. Swarup Bhunia (IEEE Fellow), University of Florida

**Abstract**: With the emergence of the Internet of Things (IoT) regime that promises exciting new applications from smart cities to connected autonomous vehicles, security of edge devices has come to the forefront of the system design process. Recent discoveries and reports on numerous security attacks on microchips and circuits violate the well-regarded concept of hardware trust anchors. Current business models and the supply chain eco-system for microelectronics give rise to unprecedented security issues and accentuate the need for secure, trustworthy hardware. It has prompted system designers to develop novel security primitives, design-for-security, and test/validation solutions to achieve secure hardware for diverse IoT applications. Emerging security issues and countermeasures have also led to interesting interplay between security and verification. Verification of hardware for security and trust has become an integral part of the system design flow. The talk will cover a spectrum of challenges associated with hardware security and describe emerging solutions in creating secure trustworthy hardware that can enable IoT security for the mass. It will outline the need and challenges for verification of an electronic design's security properties and the motivation for learning-guided security design and verification. Finally, it will outline how AI-driven assurance of hardware, specifically the usage of generative AI, is creating a promising new paradigm of hardware-centric IoT security.

**Speaker Bio**: Dr. Swarup Bhunia is currently a preeminence professor of cybersecurity and Semmoto Endowed Professor of Internet of Things (IoT) at University of Florida. He serves as the Director of the Warren B. Nelms Institute for the Connected World. Earlier, he was appointed as the T. and A. Schroeder associate professor of Electrical Engineering and Computer Science at Case Western Reserve University. He has over twenty years of research and development experience with 10 authored/edited books and over 300 publications in peer-reviewed journals and premier conferences and ten authored/edited books. His research interests include hardware security and trust, adaptive nanocomputing and novel test methodologies. Dr. Bhunia received IBM Faculty Award, National Science Foundation career development award, Semiconductor Research Corporation Inventor Recognition Award, IEEE HOST Hall of Fame award, University of Florida Research Foundation Professorship Award, SRC technical excellence award as a team member, and several best paper awards/nominations. He is co-founding editor-in-chief of a Springer journal on hardware and systems security. Dr. Bhunia received his PhD from Purdue University on energy-efficient and robust electronics. He is a Fellow of the IEEE.

Ballroom

# KEYNOTE PRESENTATIONS

Day 2 - Wednesday February 26, 2025

**09:00 AM – 09:40 AM**

**Transforming AI through Neuromorphic Engineering: Bridging the Gap between Artificial Intelligence and Hardware**

*Session Chair:* Prof. Moussa Ayyash, Chicago State University

*Presenter:* Dr. Steven D. Harbour (Parallax Advanced Research)

**Abstract**: In his keynote, Dr. Harbour will discuss the emerging field of neuromorphic engineering and its role in shaping the future of AI hardware. He will explore how neuromorphic systems—designed to replicate the neural networks of the human brain—are pushing the boundaries of AI, offering novel solutions to current challenges in speed, energy consumption, and scalability. With insights into the latest research and practical applications, attendees will gain a deeper understanding of how AI hardware can evolve to support more efficient, adaptive, and robust AI technologies.

**Speaker Bio**: Dr. Steven Harbour is the Director of AI Hardware Research at the Center of Excellence, Parallax Advanced Research, where he leads groundbreaking projects in AI-driven computing, including the development of BRAIN, a cutting-edge neuromorphic chip. With over 30 years of expertise, his work spans neuromorphic engineering, microchip design, artificial intelligence (AI) and machine learning (ML), cybersecurity, human-autonomy teaming, avionics, and autonomous systems. Dr. Harbour has authored over 50 publications on nanotechnology, nanoscale architectures, and AI-integrated microcircuit design, particularly focusing on Spiking Neural Networks (SNN). His extensive career includes over 20 years in AI algorithms, hardware development, image sensor processing, and chip design for both commercial and defense applications. Previously, he served as the Global Hawk Chief of Avionics Engineering and Modernization Programs, supporting the Air Force Research Laboratory and the Air Force Life Cycle Management Center. A former USAF fighter flight test pilot, Dr. Harbour has logged over 5,000 flight hours across multiple aircraft, including the F-16, F-4, B-52, and MIG-29. He holds a Ph.D. in Neuroscience with specializations in neuromorphic computing, AI, and ML, along with advanced degrees in aerospace engineering, mathematics, and electrical engineering. In addition to his research leadership at Parallax Advanced Research, he teaches at the University of Dayton and Sinclair College, contributing to the next generation of AI and aerospace professionals.

| | |
|---|---|
| **09:40 AM – 10:20 AM** | **BREAK AND NETWORKING OPPORTUNITY-III** |

## Day 2 - Wednesday February 26, 2025

## REGULAR SESSION 7: PAPER PRESENTATIONS (10:20 AM – 11:40 AM)

| | |
|---|---|
| SESSION CHAIR | Dr. Ahmmed Oun, *Assistant Professor of Electrical Engineering and Computer Science, Ohio University* |

For the Online Session please Use the Link below: https://meet.google.com/vzf-odhq-vgq or scan the QR Code

| **Session 7: Future Trends in IoT Systems Security and Trusted Microelectronics** | |
|---|---|
| 10:20 AM – 10:40 AM<br>Paper 135 | **A Cloud Computing-Enabled ESP32-CAM System for Real-Time Object Recognition with Feedback**<br>*Authors*: Sayed Nowroz, Nermeen Saleh, Fathi Amsaad*, Mohamed Ibrahem<br>*Abstract*: Real-time and low-cost Internet of Things (IoT) devices with competent object recognition capabilities have always been a matter of interest in the industry. Such solutions have a wide variety of applications in smart surveillance, healthcare, industrial automation, etc. Multidisciplinary skills are required to design and build such systems securely and reliably. This paper proposes a hybrid architecture that leverages cloud computing to complement the capabilities of lightweight edge devices. In this system, the ESP32-CAM, a popular microcontroller with WiFi capabilities integrated with a camera sensor, captures high resolution images and streams them as integer buffers using the Message Queuing Telemetry Transport (MQTT) protocol for low power, efficient and secure communication. The image data are processed in the cloud using the AWS infrastructure, where a Single Shot MultiBox Detector (SSD) object detection model trained on the Common Objects in Context (COCO) dataset identifies objects on the sensor images with HD quality. Based on detection, we provide in-circuit feedback by manipulating General Purpose Input/Output (GPIO) pins which opens the door for pragmatic solutions, capable of both sensing and action execution. Performance analysis demonstrates the system's scalability, achieving an average latency of 5.1 seconds and an object detection accuracy of 81.25%. This work underscores the potential of integrating edge devices with cloud platforms to enhance the computational capabilities of IoT systems. Future efforts will aim to refine response latency, strengthen data security, and broaden the framework's applications in complex IoT environments. |
| 10:40 AM – 11:00 AM<br>Paper 37 | **IoT-Driven Energy Monitoring Framework: Enhancing Efficiency, Sustainability, and Real-Time Optimization**<br>*Authors*: Ajmal Khan, Gulnara Bektemyssova, Abdul Razaque, Anar Beketova, Hari Mohan Rai , Meer Jaro Khan<br>*Abstract*: Energy waste is a critical issue, driving up utility costs and harming the environment. Traditional energy monitoring systems are passive, lacking real-time optimization, which leads to unattended energy consumption and inefficiency. This article introduces IoT-based energy meters (IoTEM) to provide a real-time approach to energy management, offering actionable insights and enabling immediate adjustments. By monitoring energy usage at the appliance level, these smart meters help users identify inefficiencies, reduce costs, and improve energy efficiency. Despite their benefits, IoT energy meters face challenges, such as data privacy concerns and the complexity of managing large-scale systems. This paper examines IoT energy metering systems, addressing their potential to improve energy management performance, modernizing outdated infrastructure, and reducing environmental impacts. |

| | |
|---|---|
| 11:00 AM – 11:20 AM<br>Paper 112 (online) | **Quantum preprocessing for Internet of Things edge computing security devices**<br>*Authors*: Tiffany Cheng, Shoshana Sugerman, Colin Farley, Brian Callahan*<br>*Abstract*: Quantum preprocessing has the potential for significantly reducing computing power and storage space needed for tiny devices, such as Internet of Things devices, to satisfactorily operate as security devices such as an Intrusion Detection System. This paper proposes a quantum process to facilitate selecting important features and combinations from the NSL-KDD dataset. The quantum algorithm utilities the Grover's algorithm along with the Pearson correlation coefficient for the oracle creation and Grover diffusion process. The selected features are then evaluated based on quantum and domain specific knowledge, the presence of quantum inaccuracy and resource requirements. In application, having the knowledge of important features can avoid utilizing the entire dataset while training on a classical computer, optimizing efficiency and resource usage, further enabling the capability of IoT devices to operate IDS systems. |
| 11:10 AM – 11:40 AM<br>Paper 196 (online) | **A Novel Framework against Reverse Engineering and Cloning in Untrusted Multi-tenant Cloud FPGA**<br>*Author*: Muhammed Kawser Ahmed*<br>*Abstract*: The integration of Field-Programmable Gate Arrays (FPGAs) in cloud architectures meets the demand for enhanced performance and scalability. FPGAs offer dynamic reconfiguration, enabling tailored hardware acceleration while minimizing power consumption. Major cloud providers like Amazon, Huawei, Microsoft, and Alibaba are incorporating FPGA-based cloud acceleration services. However, this integration introduces security challenges. In cloud FPGA deployment, cloud FPGA providers (CFPs) conduct extensive Design Rule Checks (DRC) to identify malicious circuits based on oscillation. These malicious circuits have been accused of launching remote power side channel, denial of service (DoS), and remote fault injection attacks. The attackers exploit the Power Distribution Network (PDN) of the FPGA boards, causing excessive voltage drops that can compromise the security and integrity of the designs on the board and attacks are often successful due to the shared nature of the PDN network. However, providing untrusted cloud FPGA providers with access to tenant design bitstreams also raises concerns about data confidentiality and integrity. Similar to attackers, having access to a tenant's design can lead to intellectual property theft, cloning, and reverse engineering. Furthermore, current Trusted Execution Environment (TEE)- based isolation techniques cannot guarantee prevention against these attacks, as they do not consider the CFP as a malicious entity. Additionally, many of the proposed methods come with significant implementation overhead. In this context, we propose an optimized obfuscation-based security model that provides protection against reverse engineering, cloning, and piracy. Importantly, our solution imposes minimal overhead, outperforming other suggested approaches in terms of efficiency and, in some cases, even reducing overall operational overhead. |

Auditorium

## Day 2 - Wednesday February 26, 2025

## REGULAR SESSION 8: PAPER PRESENTATIONS (10:20 AM – 11:35 AM)

SESSION CHAIRS: Dr. Akshay Kulkarni, *Assistant Professor, Prairie View A&M University*

For the Online Session please Use the Link below: https://meet.google.com/fmw-vhoa-amw

or scan the QR Code

| **Session 8: Robust AI Models for IoT Security** | |
|---|---|
| 10:20 AM – 10:40 AM<br>Paper 52 | **SAG-ERC: Securing Attack-Graph-based Systems through Node Embedding, Ranking, and Clustering**<br>*Authors*: Mohammad Al-Eiadeh, Mustafa Abdallah*<br>*Abstract*: Securing interdependent systems (where a successful attack on an asset can lead to the compromise of other assets in the system) is a challenging task. This paper introduces a security framework for these interdependent systems managed by a single defender. Using attack graphs to model vulnerabilities, we propose a resource allocation strategy that prioritizes edges through in-degree nodes. We apply a random walk embedding algorithm to project nodes into feature vectors, followed by KMeans clustering to group similar nodes and calculate the severity risk of each cluster. We also use TrustRank algorithm to evaluate asset influence. Resources are then allocated based on normalized cluster risks and node ranking scores. Our method outperforms existing resource allocation algorithms across four real-world systems, supported by statistical validation. The implementation source code is available for further development. |
| 10:40 AM – 11:00 AM<br>Paper 36 (online) | **AI and Machine learning for 6G-enabled IoT**<br>*Authors*: Daniil Buzinov, Abdul Razaque, Gulnara Bektemyssova, Anar Beketova, Mohsin Ali Farhad<br>*Abstract*: Artificial intelligence (AI), machine learning (ML), and 6G networks may transform the Internet of Things. 6G networks provide minimal device latency and accommodate substantial data throughput. It also addresses network support issues inside the extensive IoT ecosystem. AI and ML enable 6G-enabled IoT platforms to allocate resources, comprehend context, and execute intelligent decisions for predictive maintenance and security. Nevertheless, energy efficiency, data confidentiality, and device interoperability pose challenges as systems become increasingly intricate and interconnected. This article advocates the systematic application of AI and ML to enhance the performance of 6G IoT networks. We illustrate how AI-driven network management may enhance connectivity, operational costs, and real-time decision-making in smart cities, healthcare, and industrial automation. This study investigates the role of federated learning and edge computing in addressing energy and privacy challenges within extensively distributed IoT systems. This paper presents a foundational reference model to inspire research that addresses gaps and integrates the global landscape, focusing on the dependable, efficient, and intelligent utilization of 6G-enabled IoT systems |

| | |
|---|---|
| 11:00 AM – 11:20 AM<br>Paper 29 | **Hybrid Graphical Password Authentication System Using Intuitive Approach**<br>*Authors*: Abdul Razaque*, Andas Arslan, Alikhan Sabitov, Ajmal Khan<br>*Abstract*: Developing an authentication system that achieves both a high level of security and an intuitive, user-friendly interface remains a complex and challenging task. The main challenge lies in balancing two critical factors: security, which often requires complex and less user-friendly methods, and usability, which demands a system that users can easily understand and interact with. This balance is difficult to achieve because improving one aspect frequently compromises the other, making it challenging to design an authentication system that excels in both areas. In this paper, we propose a graphical authentication system that enhances the security and usability of existing authentication schemes. This improvement is achieved by integrating a variety of mechanisms in a novel way to address the weaknesses of current security systems. These mechanisms include multistep authentication, the use of the drawmetric mechanism for password creation to improve memorability, the concept of a one-time password (OTP) with random selection of password elements, random placement of password elements at different stages, assignment of random numbers to password elements, the use of the password hashing algorithm, called bcrypt, which employs a salted method and iterative process, as well as the generation of JSON Web Tokens for secure data transmission and verification. The authentication system described in this article presents a new perspective on existing graphical password implementation mechanisms. By rethinking existing approaches, it opens up new possibilities for innovation in security techniques. |
| 11:20 AM – 11:40 AM<br>Paper 181 (Online) | **SlangLLM: Dynamic Detection and Contextual Filtering of Slang in NLP Applications**<br>*Authors:* Anas AlSobeh*, Laksh Patel<br>*Abstract:* The inherent speed at which slang evolves and its context-dependent nature make it difficult for Large Language Models (LLMs) to detect poisonous terms They often miss harmful slang and struggle to detect benign uses of such terms. We present SlangLLM, a flexible framework that tackles these limitations, accomplishing this by combining frequency-based scoring, part-of-speech (PoS) weighting, and crowd-sourced definitions from Urban Dictionary. Dependency relations and semantic similarity ensure contextual filtering to identify toxic prompts correctly. Leveraging a new "slang poison level" metric, SlangLLM both quantifies toxicity and infers prompt permissibility. Experiments show that it is effective at guarding LLMs against poisonous slang prompts, significantly improving over baseline methods for slang-based toxicity while still allowing safe usage. This research contributes to ethical AI practices by improving the resilience of LLMs in conversational and content moderation scenarios. SlangLLM can serve as a preventative measure, used by law enforcement, to avert crime by analyzing social media accurately. |

## Day 2 - Wednesday February 26, 2025

## REGULAR SESSION 9: PAPER PRESENTATIONS (10:20 AM – 11:35 AM)

| | |
|---|---|
| SESSION CHAIRS: | Dr. Suleiman Ashur, *Professor of Civil Engineering and Construction Management, Eastern Michigan University*<br>Dr. Omar Darwish, *Assistant Professor of Information Security and Applied Computing, Eastern Michigan University*<br>Dr. Anas Alsobeh, *Assistant Professor, Program Coordinator Information Technology (ITEC) Program, Southern Illinois University* |

For the Online Session please Use the Link below:
https://meet.google.com/ger-nwyc-bqf

or scan the QR Code

| **Session 9: AI-Driven Threat Analysis for IoT Software Security** | |
|---|---|
| 10:20 AM – 10:40 AM<br>Paper 161 | **Severity Assessment of Cardiac Arrhythmias Through Synchronized ECG-to-Audio Time Series Analysis**<br>*Authors*: Mithun Kumar Pk, Fathi Amsaad, Darryl Ahner *<br>*Abstract*: The rapid assessment of cardiac arrhythmias remains critical in emergency healthcare settings, where traditional ECG interpretation methods often require specialized expertise and considerable time. Although contemporary research has advanced considerably in detecting cardiac arrhythmias, there remains a critical gap in automated systems capable of quantifying the severity levels of rhythm disorders, especially in cases of atrial and ventricular fibrillation. This investigation presents a pioneering approach to quantify arrhythmia severity through automated feature extraction from sonified ECG signals. Our methodology employs a novel integration of spectral, temporal, peak distances, and wavelet-based features dynamically extracted from acoustically transformed ECG signals. The investigated model automatically processes these multi-domain features to evaluate the physiological impact of different arrhythmia types, focusing specifically on the severity gradation of atrial and ventricular fibrillation. Experimental results demonstrate superior performance compared to contemporary arrhythmia detection methods, achieving high accuracy in both identification and severity classification tasks. This research introduces a new paradigm in cardiac rhythm analysis by providing quantitative severity assessment capabilities previously unavailable in automated systems. |
| 10:40 PM – 11:00 AM<br>Paper 137 | **Experimental Analysis of Fine-Tuned Drone Detection YOLO Models**<br>*Authors*: Sara Acikkol Dogan*, Jonathan Walatkiewicz, Samir Tout, Omar Darwish, and Ourania Spantidi<br>*Abstract*: The increasing usage of recreational drones poses significant challenges for radar-based detection, primarily due to their small size and resemblance to birds. To help tackle such challenges, this study experimented with You Only Look Once (YOLO) object detection models to identify drones versus birds in a curated and balanced dataset. All model training, validation, and testing showed high detection metric values, with a mean average precision (mAP50) close to 0.98. Although our findings exhibited strong performance, they also led us to uncover deficiencies in our chosen dataset and model training, such as data leakage and overfitting. We addressed these through building an external dataset and fine-tuning select hyperparameters, respectively. We present our results, which showed modest, yet promising improvements, along with a few lessons learned that will provide value to other researchers exploring similar studies. |

|  |  |
|---|---|
| 11:00 AM – 11:20 AM<br>Paper 55 (online) | **File Type Classification based on Data Fragments from Compressed Archives for Digital Forensics**<br>*Authors*: Mohammed Salman*<br>*Abstract*: This paper presents a novel deep learning approach to classifying file types based on file fragments from compressed archive files for digital forensics such as analyzing IoT traffic. Existing solutions do not classify files in compressed archives. The proposed DL model implements and optimizes a modified Conv2D Inception network with two sets of filters FGA and FGB combined with kernel density estimation (KDE). Our experiment results demonstrate that the modified Inception network with filter FGA and KDE using Gaussian and Epanechnikov kernels achieves a classification accuracy of 72.54% and 73.18%, respectively. The Epanechnikov kernel with filter FGB improves the system performance and attains an accuracy of 75.24%. |
| 11:20 AM – 11:45 AM<br>Paper 155 (online) | **Criminal Email Detection Using Innovative Large Language Models and Data Augmentation**<br>*Author*: Levi Pittman, Mohamed Ibrahem*, Mahmoud Abyoussef<br>*Abstract*: The increasing use of email as a communication tool has provided new opportunities for criminals to coordinate illegal activities. In response, law enforcement agencies have turned to advanced technologies to analyze email content and identify potential criminal behavior. Traditional methods for criminal detection often rely on known offenders, with some approaches using feature extraction and natural language processing (NLP) techniques to examine communication. However, with the recent advancements in large language models (LLMs), these tools have become significantly more powerful and versatile. This paper explores the use of LLMs to detect criminal content in emails. We demonstrate that LLMs offer improved accuracy in identifying emails that contain criminal information, thereby enhancing user protection. To evaluate the effectiveness of LLMs, we tested several models to classify criminal emails and addressed the challenge of imbalanced datasets using multiple data augmentation techniques. The results are compared to existing literature, illustrating the impact of LLMs and data augmentation in improving the classification of criminal emails. |

|  |  |
|---|---|
| **11:35 AM – 1:00 PM** | **LUNCH BUFFET OPEN** |

Ballroom

# LUNCHEON KEYNOTE PRESENTATIONS

Day 2 - Wednesday February 26, 2025

**12:10 PM – 12:45 PM**

**When Machines Misbehave – The Emerging Science of AI Forensics**
*Session Chair:* Mr. Eric Parsley (Expedient Technology Solutions, LLC)
*Presenter:* 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.

| | |
|---|---|
| 12:45 PM – 13:00 PM | COFFEE BREAK |

# PANEL DISCUSSION

Day 2 - Wednesday February 26, 2025

**13:00 PM – 14:10 PM**

**Cybersecurity and Microelectronics Workforce Development Panel**
(BALLROOM)

| | | |
|---|---|---|
| MODERATOR: | | Dr. John Hoag (University of Akron) |

**Panel Overview**: The Cybersecurity and Microelectronics Workforce Development Panel aims to address the growing need for a skilled workforce in cybersecurity and microelectronics in the US, particularly in state of Ohio, AF, defense, academic, government, and industry sectors. The panel will explore strategies to strengthen and diversify the talent pipeline through collaborations between government, academia, and industry, focusing on developing resilient and qualified professionals. Key discussions will cover workforce development initiatives, the importance of training programs, and the creation of sustainable partnerships to meet the evolving demands of microelectronics and cybersecurity in critical applications.

**Panelists:**

Mr. Kirk M. Herath

Panelist Bio: Kirk Herath is the Cybersecurity Strategic Advisor to Ohio Governor Mike DeWine and Lt. Governor Jon Husted, as well as Chairman of CyberOhio. He leads efforts to strengthen the state's cybersecurity, support local governments in cyber preparedness, and develop a modern cyber workforce. He is also an Adjunct Professor of Law at Ohio State’s Moritz School of Law and Cleveland State’s Cleveland-Marshall Law School. Previously, he spent 32 years at Nationwide as VP, Associate General Counsel, and Chief Privacy Officer. He is a past president of the International Association of Privacy Professionals and served on the DHS Data Privacy and Integrity Advisory Committee (2005–2011). He is admitted to the Ohio Bar.

# PANEL DISCUSSION

Day 2 - Wednesday February 26, 2025

**13:00 PM – 14:10 PM**

**Cybersecurity and Microelectronics Workforce Development Panel**
(BALLROOM)

| | |
|---|---|
| MODERATOR: | Dr. John Hoag (University of Akron) |

**Panelists (Continued):**

Karen Manzo, Executive Vice President of Development, SOCHE (Southwestern Ohio Council for Higher Education)

Panelist Bio: Karen Manzo is the Senior Vice-President of Finance and Contracts at the Strategic Ohio Council for Higher Education (SOCHE). Karen received her BS in Business Administration in Finance from the University of Dayton. Karen also furthered her education at Wright State University majoring in Accounting. Karen has risen through the ranks at SOCHE working there since 2013. Her expertise is financial accounting, preparing contracts and assisting with the Work Force Development side of SOCHE.

Hayley Atwater

Panelist Bio: Hayley Atwater is currently serving as the Microelectronics Commons Development Subject Matter Expert at the Office of the Under Secretary for Defense for Research and Engineering, a role she has held since October 2023. In this position, Hayley is responsible for shaping and implementing initiatives that aim to develop a resilient and diverse workforce to meet the growing demands of the microelectronics and semiconductor industries, with a particular focus on defense applications. With a background as a Materials Engineer with the US Army since 2018, Hayley brings valuable experience in both engineering and workforce development. Prior to her current position, she worked as a Teaching Assistant at Alfred University and completed an internship with the US Army in 2016. She holds a bachelor's degree in Material Science Engineering from Alfred University, where she was involved in extracurricular activities such as the Karamo's Honors Fraternity and the Women's Lacrosse Team.

# PANEL DISCUSSION

Day 2 - Wednesday February 26, 2025

**13:00 PM – 14:10 PM**

**Cybersecurity and Microelectronics Workforce Development Panel**
(BALLROOM)

| | |
|---|---|
| MODERATOR: | Dr. John Hoag (University of Akron) |

**Panelists (Continued):**

Jessica Falcon

Panelist Bio: Jessica Falcon is the Director of Workforce Development for the Midwest Microelectronics Consortium (MMEC), leading partnerships among industry, government, and academia to build a sustainable workforce. With a passion for workforce development, she drives awareness and implementation of MMEC initiatives, helping partners cultivate a strong and diverse talent pipeline. Jessica began her career in federal service in 2009 while earning her B.A. in Psychology, later joining the Air Force Research Lab as a testing technician. She advanced to Lead Instructional Systems Developer and Chief of Standards and Evaluations, overseeing curriculum development for programs training 6,000 students annually. With 14 years of experience supporting military and civilian trainees, she is a dedicated educator and leader. Jessica holds an M.S. and Ed.D. in Education and is committed to fostering collaboration and innovation to shape MMEC’s future workforce.

| | |
|---|---|
| 12:45 PM – 13:00 PM | COFFEE BREAK |

Ballroom

# INVITED TALK

Day 2 - Wednesday February 26, 2025

**14:30 PM – 15:00 PM**

**The Need for Software-Hardware Co-Design in Secure ASICs and Accelerators**
*Session Chair:* Mr. Dominic Mohrhardt (AFLCMC)
*Presenter:* Dr. Samir Tout (Eastern Michigan University)

**Abstract**: With increased development in connected and autonomous vehicles, smart mobility solutions, and IoT integration, security has become very crucial for these systems. Dr. Tout will give a very engaging talk on the challenges and solutions related to the cybersecurity of mobility and autonomy systems. He will share his experience in Mobility and Autonomy Cybersecurity (MAC) Research and outline the emerging threats and vulnerabilities in this domain. He will discuss artificial intelligence and machine learning for anomaly detection and predictive analytics, sharing insights from some of his funded projects and experience including the NSF-funded SaTC research related to these emerging areas of research. The session will emphasize main directions of activity on protection of the critical mobility infrastructure, stimulation of creativity in secure system design, and improvement of industry standards. Attendees will gain valuable knowledge and actionable ideas for addressing cybersecurity challenges in the ever-evolving mobility and autonomy landscape.

**Speaker Bio**: Dr. Samir Tout is a full professor at the School of Information Security & Applied Computing at Eastern Michigan University. His main research interests are in the realm of cybersecurity, mobility, artificial intelligence and machine learning. He was awarded a collaborative SaTC NSF grant in 2014 in integrated smart grid analytics for anomaly detection, which he successfully concluded in 2018. He published in various venues, he is a TEDx speaker and has multiple industry cybersecurity certifications. Dr. Tout has served as a consultant for several OEMs and Tier-x suppliers and supported their cybersecurity programs. He has served as a reviewer for journals, conferences, NSF proposals and he currently serves on multiple cybersecurity standards committees. Dr. Tout built a Mobility and Autonomy Cybersecurity lab, which has been a training platform for many EMU students. He earned his Ph.D. from Nova Southeastern University, and his masters/bachelor's degrees from the University of Western Ontario.

Ballroom

# INVITED TALK

Day 2 - Wednesday February 26, 2025

**15:00 PM – 15:30 PM**

**The Need for Software-Hardware Co-Design in Secure ASICs and Accelerators**
*Session Chair:* Mr. Dominic Mohrhardt (AFLCMC)
*Presenter:* Aaron Miller (Galois Inc.)

**Abstract**: The increasing complexity of secure ASIC and accelerator design demands a fundamental shift in how engineers approach hardware/software integration. In this talk, Aaron Miller will explore the necessity of digital-first, component-oriented engineering methodologies tailored for secure semiconductor development. He will discuss how ASIC designers must clearly define security assumptions, adopt rigorous verification techniques, and align with evolving industry standards to ensure resilience against emerging threats. Emphasizing formal methods and secure-by-design principles, Aaron will outline pathways to enhance system trustworthiness, streamline design cycles, and reduce lifecycle costs. His insights will highlight how co-design strategies can drive innovation in high-assurance silicon, enabling more secure and efficient computing architectures.

**Speaker Bio**: Aaron Miller is the Strategy and Technology Transition Leader at Galois, specializing in secure systems, systems engineering, and digital transformation with a software focus. He co-founded two startups—Tangram Flex, a component-oriented engineering company, and Niobium Microsystems, a silicon design company specializing in high-assurance cryptographic and model-based designs. With a background in systems engineering and a master's degree from the University of Dayton, Aaron is dedicated to advancing methodologies for building high-quality, cost-effective systems. At Galois, he collaborates with leading researchers worldwide to identify, develop, and transition cutting-edge technologies that enhance the security and reliability of software and cyber-physical systems. His expertise bridges research, industry, and government, driving innovation in hardware/software co-design and system trustworthiness.

| | |
|---|---|
| 15:30 AM – 16:00 AM | BREAK AND NETWORKING OPPORTUNITY-IV |

# EVENING TECHNICAL SESSIONS

Day 2 - Wednesday February 26, 2025

**16:00 PM – 18:00 PM**

**SaTC Exhibition & Poster Session I**
SATC RECEPTION and NETWORKING OPPORTUNITY-II
(BALLROOM/FOYER)

| | |
|---|---|
| SESSION CHAIRS: | Dr. Ahmed Ammar, *Assistant Professor of Electrical & Computer Engineering, Ohio Northern University*<br>Dr. Ahmmed Oun, *Assistant Professor of Electrical Engineering and Computer Science, Ohio University* |

Poster Session I: (16:00 PM – 18:00 PM)

| Poster Number | Paper ID | Title | Authors |
|---|---|---|---|
| Poster 1 | 171 | Enhancing IoT Intrusion Detection Systems through Adversarial Training | Karma Gurung, Ashutosh Ghimire, Fathi Amsaad* |
| Poster 2 | 134 | Automation of Industrial Electropolishing using Real-Time IoT-Based Control | Nermeen Saleh, Fathi Amsaad, Mohamed Ibrahem, Hugh Salehi |
| Poster 3 | 136 | PUF-Based Hardware Security for Trusted Internet of Drones: Challenges and Future Directions | Sufian Al majmaie, Niraj Prasad Bhatta, Pratik Pandurang Kharat, Fathi Amsaad * |
| Poster 4 | 146 | Foundation Models in Digital Pathology Imaging: Pioneering Next-Generation AI for Healthcare Transformation | Md Ariful Islam Mozumder, Rashadul Islam, Imtiage Sami, Arfatul Sumiraj, Kim Hee Cheol |
| Poster 5 | 144 | Intrusion Detection in IoT Networks Using Hyperdimensional Computing: A Case Study on the NSL-KDD Dataset | Ghazal Ghajari, Elaheh Ghajari, Hossein Mohammadi, Fathi Amsaad |
| Poster 6 | 143 | Network Anomaly Detection for IoT Using Hyperdimensional Computing on NSL-KDD | Ghazal Ghajari, Ashutosh Ghimire, Elaheh Ghajari, Fathi Amsaad |
| Poster 7 | 122 | Intrusion Detection in IoT: A Comprehensive Review of Techniques, Challenges, and Future Directions | Kanchon Gharami, Micah Parrilla, Harkiran Kaur Bhullar, William A. Davis, Shafika Showkat Moni |

|  |  |  |  |
|---|---|---|---|
| Poster 8 | 23 | Kidney Stone Detection in Ultrasound Imaging: Addressing Noise and Image Segmentation | Adithya Vardhan Redd Tummala, Ashutosh Ghimire, Fathi Amsaad |
| Poster 9 | 21 | Adaptive Ensemble Learning for Real-Time Financial Fraud Detection: A Lightweight Approach | Ashutosh Ghimire, Vishnu Vardhan Baligodugula, Fathi Amsaad |

**Immediately following the Poster Session, please join us for the**

SaTC Dinner & Networking Opportunity

(18:00 PM – 20:00 PM)

# EVENING SESSIONS

Day 2 - Wednesday February 26, 2025

**16:00 PM – 18:00 PM**

**Secure Edge Working Group Meeting**
(KITTY HAWK)

| **Description** |
|---|
| The MMEC Secure Edge Working Group meeting brings together MMEC working group members and U.S. Government (USG) stakeholders to collaborate on advancing mission-driven security solutions. The working group aims to leverage MMEC capabilities to support device innovations, architectures, IP techniques, and COTS devices, enabling composable high-performance/low SWAP-C architectures over the near (3-year), mid (5-year), and far (10-year) term.<br>This meeting will serve as a platform for engaging key stakeholders, exchanging insights, and fostering innovation in secure edge computing. Additionally, it provides an opportunity to introduce the working group and MMEC to interested parties, allowing them to gain a deeper understanding of its objectives and sign up for future participation. |

**Immediately following the Group Meeting, please join us for the**

SaTC Dinner & Networking Opportunity
(18:00 PM – 20:00 PM)

# MICROELECTRONICS COMMONS UPDATING KEYNOTE

Day 3 - Thursday February 27, 2025

**08:20 AM – 08:30 AM**

**Enlightening Talk-I**
*Session Chair*: Dr. Matthew Casto, CTO, MMC
*Presenter*: Ms. Stephanie Lin, Microelectronics Commons at NSTXL

**Abstract**: The Department of Defense's (DoD) Microelectronics Commons, a $2 billion initiative under the CHIPS and Science Act, is transforming domestic semiconductor innovation and production by accelerating the transition from research to manufacturing. As Vice President of NSTXL and Chair of the Commons Hub Board, Stephanie provides strategic leadership to ensure effective collaboration across all eight Hubs. Her expertise in microelectronics policy, hardware assurance, and anti-tamper technologies has been instrumental in shaping national defense strategies. This session will highlight key advancements in microelectronics security, policy considerations, and the role of public-private partnerships in strengthening the U.S. semiconductor ecosystem.

**Speakers Bio**: Stephanie serves as the Vice President at the National Security Technology Accelerator (NSTXL) overseeing the execution of the Microelectronics Commons, the $2B DoD program established by the CHIPS and Science Act. She also serves as the Chair to the Commons Hub Board, comprising members of all eight Hubs. Before this role, she supported various senior leaders within the Office of the Secretary of Defense for several years in anti-tamper, hardware assurance, and microelectronics policy. She also led policy and Congressional activities for the Defense Microelectronics Cross-Functional Team and supported the Trusted and Assured Microelectronics (T&AM) Program. She holds degrees in electrical and computer engineering.

Ballroom

# MICROELECTRONICS COMMONS UPDATING KEYNOTE

Day 3 - Thursday February 27, 2025

**08:30 AM – 08:40 AM**

**Enlightening Talk-II**
*Session Chair*: Dr. Matt Casto, CTO, MMC
*Presenter*: Dr. Wayne Churaman, DEVCOM Army Research Lab/DoD Microelectronics Commons

**Abstract**: Dr. Wayne Churaman will provide a comprehensive overview of the evolving landscape of secure microelectronics and IoT. With increasing threats to semiconductor supply chains and embedded systems, ensuring the security and trustworthiness of next-generation microelectronics is more critical than ever. Attendees will gain insights into government, industry, and academic collaborations, as well as strategies for mitigating risks in microelectronics. The keynote will also emphasize the importance of building a skilled workforce, fostering R&D in secure electronics, and addressing future challenges in semiconductor security. This session is essential for professionals, researchers, and policymakers looking to stay ahead in the rapidly evolving field of cybersecurity and microelectronics.

**Speakers Bio**: Dr. Churaman is serving as the Microelectronics Commons Technical Execution Area (CTEA) Lead for Secure Edge/Internet of Things (IoT). His role includes providing technical oversight and programmatic management of Commons Hub activities and funding within the Secure Edge/IoT portfolio. He is responsible for the development of technical execution plans, as well as developing and maintaining technical roadmaps in coordination with the Microelectronic Commons Board of Service Executives (BSE) and engaging with stakeholders to ensure technology readiness level (TRL)/manufacturing readiness level (MRL) maturation for the projects aligned with his technical execution area. Dr. Churaman sits at DEVCOM Army Research Laboratory, where he is an Electronics Engineer in the Electromagnetic Spectrum Sciences Directorate. His background is in secure packaging and novel security solutions for microelectronics. Dr. Churaman received his M.S. in Electrical Engineering, and his Ph.D. in Mechanical Engineering from the University of Maryland at College Park in 2010 and 2019 respectively, where his research focused on the development of a novel micro-actuator for enhanced locomotion of an autonomous robotic platform. His work has resulted in over 24 career journal papers and proceedings, and 509 citations in the highly specialized field of physical hardware security for microelectronics.

# MICROELECTRONICS COMMONS UPDATING KEYNOTE

Day 3 - Thursday February 27, 2025

**08:40 AM – 08:50 AM**

**Enlightening Talk-III**

*Session Chair*: Dr. Matt Casto, CTO, MMC

*Presenters*: Dr. Erin Gawron-Hyla, DEVCOM Army Research Lab/DoD Microelectronics Commons

**Abstract**: Dr. Gawron-Hyla will explore the strategic importance of workforce development in the rapidly evolving field of secure and trusted microelectronics. She will highlight key initiatives, industry-government partnerships, and innovative training programs designed to bridge skill gaps and enhance the DoD's microelectronics ecosystem. Her talk will provide insights into fostering a highly skilled, adaptable workforce to meet the challenges of emerging technologies and national security needs.

**Speakers Bio**: Dr. Gawron-Hyla is serving as the Microelectronics Commons Technical Execution Area Lead for Workforce Development. Her role includes guidance and oversight of Hub workforce development portfolios and metrics, as well as coordination of microelectronics workforce development efforts with other DoD programs and government agencies. Dr. Gawron-Hyla sits at DEVCOM Army Research Laboratory where she is a Research Chemist in the Electromagnetic Spectrum Sciences Division. Her background as a materials chemist led to supporting research efforts in materials development for microelectronics integration. Prior to her work at DEVCOM ARL, Dr. Gawron-Hyla taught high school chemistry and served as science department chair at Heritage High School in Conyers, GA. Dr. Gawron-Hyla received her B.S. in Chemistry and Mathematics from Rose-Hulman Institute of Technology as part of the first class of women, and her M.S. in Science Education from Purdue University. She also holds a Ph.D. in Chemistry from Georgia Tech and completed a Post Doctoral fellowship at the University of Calgary in Alberta, Canada.

Ballroom

# KEYNOTE PRESENTATIONS

Day 3 - Thursday February 27, 2025

**09:00 AM – 09:40 AM**

**Advancing Workforce Development and Innovation in Microelectronics, Cybersecurity, and Emerging Technologies**

*Session Chair:* Mr. Kirk Herath, Cybersecurity Advisor to Ohio Governor

*Presenter:* Mr. Mike Duffey, Chancellor, Ohio Department of Higher Education

**Abstract**: Mr. Mike Duffey, Chancellor of the Ohio Department of Higher Education, will deliver a keynote address on Thursday, February 26, from 9:00 to 9:40 a.m. His presentation will explore workforce development with a focus on microelectronics, semiconductors, IoT, cybersecurity, and secure and assured systems. Additionally, he will discuss funding opportunities for research and development, emphasizing strategies to enhance industry-academic collaboration and drive innovation in these critical technological areas.

**Speaker Bio**: Appointed as the 11th Chancellor of the Ohio Department of Higher Education in January 2024, Mr. Mike Duffey oversees Ohio's two-year and four-year colleges, universities, and technical centers. Prior to this role, he served as Senior Vice Chancellor for five years, contributing to policies on tuition guarantees, student debt relief, and support for innovation. From 2011 to 2019, Mr. Duffey was a member of the Ohio House of Representatives, chairing the Higher Education and Workforce Committee and co-sponsoring legislation that established JobsOhio. He holds a Master of Business Administration from The Ohio State University and a bachelor's degree in political science from the University of Michigan. Residing in Worthington with his wife, Lindsay, and their two children, he is committed to advancing higher education in Ohio.

| | |
|---|---|
| **09:40 AM – 10:00 AM** | **COFFEE BREAK & PREPERATION FOR THE PANEL (3) DISCUSSION** |

# PANEL DISCUSSION

Day 3 - Thursday February 27, 2025

**10:00 AM – 11:00 AM**

**AF/Industry Trusted and Assured Microelectronics Panel**
(BALLROOM)

MODERATOR:

Mr. Kevin McCamey
(Resilient Microelectronics, Sensors Directorate, AFRL)

**Moderator Bio**: Mr. Kevin McCamey Program Manager, Resilient Microelectronics, Sensors Directorate Kevin McCamey is Senior Program Manager for Trusted Microelectronics at the Sensors Directorate, Air Force Research Laboratory. Trusted Microelectronics program is a diverse portfolio for development and validation of integrated components for assured design, verification and validation, trusted packaging and reliability of microelectronics to ensure trusted microelectronics meet specific mission requirements of Air Force and Space Force weapon systems. Mr. McCamey was previously the Deputy Division Chief for the Advanced Programs Division of the Sensors Directorate leading Combat Identification, Multi-mode sensor development, and rapid technology demonstrations for the directorate. He held a variety of technical leadership, program management, and supervisory positions in AFRL and industry including program manager on the software development for the Space Based Infrared System, and Base Realignment and Closure lead for the Sensors Directorate mission consolidation of 2 remote sites to Wright-Patterson. Kevin holds a BS and MS in Electrical Engineering and an MBA from the University of Dayton and MS in National Resource Strategy from the National Defense University.

**Panel Overview**: The AF/Industry Trusted and Assured Microelectronics Panel will explore critical challenges and advancements in securing microelectronics for defense and commercial applications. As microelectronics form the backbone of modern military and aerospace systems, ensuring their trust, integrity, and resilience is paramount. This panel brings together leading experts from government, industry, and research institutions to discuss strategies for safeguarding the microelectronics supply chain, mitigating security risks, and advancing secure design methodologies. Key Topics of Discussion: 1) Ensuring trusted and assured microelectronics for mission-critical applications, 2) Addressing vulnerabilities in the supply chain and lifecycle management, 3) Advances in secure design, verification, validation, and packaging, 4) The role of autonomous systems, AI, and synthetic aperture radar, 4) (SAR) technologies in microelectronics security, and 5) Industry's role in supporting hardware security, embedded system trust, and cyber resilience.

# PANEL DISCUSSION

Day 3 - Thursday February 27, 2025

**10:00 AM – 11:00 AM**

**AF/Industry Trusted and Assured Microelectronics Panel**
(BALLROOM)

| | |
|---|---|
| MODERATOR: | Mr. Kevin McCamey<br>(Resilient Microelectronics, Sensors Directorate, AFRL) |

**Panelists:**

Edmund Zelnio, Director, Autonomy Technology Research Center, Sensors Directorate, AFRL

**Panelist Bio**: Edmund Zelnio is currently the director of the Autonomy Technology Research Center in AFRL, a Sensors Directorate summer intern program. Ed's 49-year career with the Air Force Research Laboratory (AFRL) includes numerous technical and leadership roles in automated exploitation of imaging sensors, primarily addressing synthetic aperture radar. He is a former division chief and technical advisor of the Automatic Target Recognition Division of the Sensors Directorate in AFRL and has served in an advisory capacity to the Department of Defense and the intelligence community. He has served as the chair of the SPIE Algorithms for Synthetic Aperture Radar Imagery conference for the past 29 years. He is the recipient of the 53rd Department of Defense Distinguished Civilian Service Award and is an AFRL Fellow. Ed a BS in Electrical Engineering from Bradley University and post-graduate doctoral studies at The Ohio State University in electromagnetics and Wright State University in signal processing.

Christopher Bozada, Principal Integrator, Aerospace Components and Subsystems Division, AFRL

**Panelist Bio**: Chris Bozada serves as the Principal Integrator for AFRL's Sensors Directorate's Aerospace Components and Subsystems Division. He ensures the division technology program appropriately invests in enabling electronics / optoelectronics materials and devices and RF/EO subsystems for sensing, electronic warfare and communications across the electromagnetic spectrum. The division is the Sensors Directorate's lead for trusted and assured electronics for supply chain, sustainment and access to the measurably secure electronics. Chris has a MS in Electrical Engineering from the University of Dayton, a BS in Electrical Engineering from the University of Missouri-Columbia, and a BS in Chemical Engineering from Stanford University. Chris is also an AFRL Fellow.

# PANEL DISCUSSION

Day 3 - Thursday February 27, 2025

**10:00 AM – 11:00 AM**

**AF/Industry Trusted and Assured Microelectronics Panel**
(BALLROOM)

| | |
|---|---|
| MODERATOR: | Mr. Kevin McCamey<br>(Resilient Microelectronics, Sensors Directorate, AFRL) |

**Panelists (Continued):**

Dr. Paul M. Simon, PhD, Senior Hardware Security Engineer, Device & Services Security, Amazon

**Panelist Bio**: Dr. Simon is a member of a small team of hardware security experts on Amazon focusing on the security of consumer devices and services. He also coordinated Amazon joining the Industry Advisory Board (IAB) for the Center for Hardware and Embedded Systems Security and Trust (CHEST) consortium. Prior to joining Amazon in 2022, Dr. Simon worked for several government contractors in and around AFIT and AFRL performing cyber vulnerability assessments of weapon systems, micro-electronics trust and assurance validation and research, and various other research to include reverse engineering, hardware system design, and cyber security of embedded devices. Dr. Simon received his bachelor's (1997) and masters (2011) degrees in electrical engineering from University of Dayton, and received his PhD in electrical engineering from AFIT.

Jarod Patton

**Panelist Bio**: Panelist Bio: Jarod Patto is a Principal at Booz Allen Hamilton, a global leader in cybersecurity, defense, and technology consulting. With extensive experience in strategic advisory, digital transformation, and emerging technologies, he plays a key role in helping government and private sector organizations enhance their security posture and operational resilience. As a leader in Booz Allen's defense and intelligence sector, Mr. Patto has contributed to advanced cybersecurity solutions, AI-driven analytics, and critical infrastructure protection. His work involves collaborating with federal agencies, military branches, and enterprise clients to address complex security challenges in an evolving digital landscape.

| | |
|---|---|
| **11:00 AM – 11:15 AM** | **COFFEE BREAK & PREPERATION FOR THE REGULAR SESSION DISCUSSION (4)** |

Ballroom

## Day 3 - Thursday February 27, 2025

## REGULAR SESSION 10: PAPER PRESENTATIONS (11:15 AM – 12:30 PM)

| | |
|---|---|
| SESSION CHAIRS: | Dr. Ahsan Mian, *Professor of Mechanical & Materials Engineering, Wright State University* |
| | Dr. Daniel Young, *Professor of Mechanical & Materials Engineering, Wright State University* |

For the Online Session please Use the Link below:
https://meet.google.com/vzf-odhq-vgq

or scan the QR Code

| **Session 10: Additive Approaches to Electronic Manufacturing and Trust** | |
|---|---|
| 11:15 AM – 11:40 AM<br>Paper 130 | **Processing and Characterization of Functional Ink Material for Flexible Hybrid Electronics**<br>*Authors*: Arashdeep Singh, Ahsan Mian<br>*Abstract*: Inkjet printing provides a straightforward approach for creating flexible hybrid electronics devices of the next generation. This study focuses on the complex connections between materials, processes, and resulting properties, especially focusing on emerging functional materials such as nanomaterials, polymers, and composites. As such, we processed, printed and characterized the conductive (Nano silver) and dielectric (polyimide and polyimide/BaTiO3 nanocomposite) ink-based materials for heterogeneous integration and sensor applications. The ceramic/polymer dielectric composite material was considered for further improvement in dielectric properties of the material. After processing and inkjet printing of the materials, they were characterized by high-resolution imaging and elemental identification using SEM and EDX, respectively. |

| | |
|---|---|
| 11:40 AM – 12:05 PM<br>Paper 8 (online) | **InoculLedger: A Secure and Scalable Distributed Ledger for Efficient Vaccine Supply Chain Management**<br>*Authors*: Faisal Alamri, Anand Kumar Bapatla, Venkata K. V. V. Bathalapalli, Saraju P. Mohanty∗, Elias Kougianos<br>*Abstract*: The Vaccine Supply Chain (VSC) is a crucial component of the Healthcare Cyber-Physical System (H-CPS), enabling seamless coordination among various entities to ensure the timely delivery of safe and effective vaccines. Given the extensive number of interactions and the stringent requirements for monitoring environmental parameters, the VSC features a highly complex architecture with intricate operational dynamics. This complexity, coupled with the reliance on multiple centralized systems, often results in lack of transparency, making it challenging to monitor the vaccine movement withing the supply chain network as well as recording the temperature excursions.<br>To address these challenges, we propose a novel blockchain-based system that provides a transparent and secure mechanism for storing and accessing vaccine records. By leveraging the IOTA Tangle data structure, our system meets the high throughput demands of the application while ensuring data integrity and scalability. A proof-of-concept implementation was developed and analyzed to evaluate its scalability and adaptability for real-world deployment, demonstrating its potential to revolutionize the VSC by enhancing transparency and efficiency. |
| 12:15 PM – 12:35 PM<br>Paper 178 (online) | **Future Possibilities of Using Additive Manufacturing to Produce Shape Memory Metals in Embedded Systems and Actuators**<br>*Author*: Celebi, Ahu; Elahinia, Mohammad; Behvar, Alireza; Mohajerani, Shiva ; Al Gamal, Anwar; Sojoodi, Mahyar<br>*Abstract*: Shape memory alloys (SMAs) have become revolutionary materials as a result of their distinctive characteristics, including superelasticity, high energy density, and shape memory effect. The fabrication and application landscape of SMAs have been revolutionized by the integration of Additive Manufacturing (AM) technologies, which has allowed for the precise control of microstructure, functionality, and complex geometries. This synergy has unleashed a vast amount of potential for advanced applications in embedded systems and actuators, particularly in the aerospace, robotics, and biomedical sectors, where precision and adaptability are essential. Despite their transformative potential, the widespread adoption of these technologies is still hindered by challenges such as high production costs, material optimization, and manufacturing consistency. This review emphasizes the most recent developments in AM-fabricated SMAs, with a particular emphasis on their utilization in morphing structures, sensors, and actuators. Key advancements include the investigation of adaptive control systems, multifunctional composite designs, and self-sensing capabilities that facilitate the integration of SMA-based components into embedded technologies. Furthermore, the paper discusses the unique ways in which AM addresses long-standing SMA fabrication challenges, including the ability to achieve application-specific properties, minimize defects, and facilitate complex designs. This paper provides a critical perspective on the future of SMAs in emerging technologies by synthesizing recent research and industrial trends, thereby delineating strategies for interdisciplinary collaboration. By means of these developments, AM is on the brink of expediting the adoption of SMAs, which will ultimately lead to the development of high-performance actuators, intelligent robotics, and next-generation adaptive devices, thereby redefining the potential of engineering and technology. |

## Day 3 - Thursday February 27, 2025
## REGULAR SESSION 11: PAPER PRESENTATIONS (11:15 AM – 12:30 PM)

SESSION CHAIRS: Dr. Ahmmed Oun, *Assistant Professor at Prairie View A&M University*

For the Online Session please Use the Link below:
https://meet.google.com/fmw-vhoa-amw

or scan the QR Code

| **Session 11: AI Approaches for Detecting Anomalies in IoT Devices** | |
|---|---|
| 11:15 AM – 11:35 AM<br>Paper 3 | **Identifying the Origins of Business Data Breaches through CTC Detection**<br>*Authors*: Gayle Frisbie, Omar Darwish, Anas AlSobeh, Abdallah Al-shorman<br>*Abstract*: The frequency of cybersecurity events and data breaches escalates, resulting in substantial financial liabilities for businesses. Contemporary organizations rely heavily on network connections to facilitate efficient operations in diverse locations. Covert timing channels (CTCs) represent a sophisticated cyber threat that involves the covert addition of private data to regular network traffic. This creates hidden communication paths that are difficult to spot. This study proposes a novel approach for detecting CTCs using machine learning (ML), significantly advancing the state-of-the-art in data breach detection and information leakage through CTC. Our method uses a special combination of Unicode transformation and machine learning to improve the ability to detect by looking at data about the time between packets. In particular, our findings indicate that the Gradient Boost Classification model yields an accuracy rate ranging from 73% to 78%, while the Random Forest model (RF) also exhibits significant accuracy. |
| 11:35 AM – 11:55 AM<br>Paper 18 | **Enhancing Cybersecurity in Critical Infrastructure with LLM-Assisted Explainable IoT Systems**<br>*Authors*: Ashutosh Ghimire, Ghazal Ghajari, Karma Gurung, Love Kumar Sah, Fathi Amsaad<br>*Abstract*: Ensuring the security of critical infrastructure has become increasingly vital with the proliferation of Internet of Things (IoT) systems. However, the heterogeneous nature of IoT data and the lack of human-comprehensible insights from anomaly detection models remain significant challenges. This paper presents a hybrid framework that combines numerical anomaly detection using Autoencoders with Large Language Models (LLMs) for enhanced preprocessing and interpretability. Two preprocessing approaches are implemented: a traditional method utilizing Principal Component Analysis (PCA) to reduce dimensionality and an LLM-assisted method where GPT-4 dynamically recommends feature selection, transformation, and encoding strategies.<br/>Experimental results on the KDDCup99 10% corrected dataset demonstrate that the LLM-assisted preprocessing pipeline significantly improves anomaly detection performance. The macro-average F1 score increased from 0.49 in the traditional PCA-based approach to 0.98 with LLM-driven insights. Additionally, the LLM generates natural language explanations for detected anomalies, providing contextual insights into their causes and implications. This framework highlights the synergy between numerical AI models and LLMs, delivering an accurate, interpretable, and efficient solution for IoT cybersecurity in critical infrastructure. |
| 11:55 AM – 12:15 PM | **AI-Enhanced Security Framework for QR Codes** |

| | |
|---|---|
| Paper 27 | *Authors*: Abdul Razaque, Mukhammedali Zhursinbek, Vyacheslav Khan, Ajmal Khan, Zhuldyz Kalpeyeva<br>*Abstract*: This research article examines potential security vulnerabilities related to the use of QR codes (rapid response code) in various industries.<br>The relevance of the topic of this article is that in the modern world QR codes are becoming more popular for payment, access to websites and information exchange, which are also becoming a target for intruders. Due to the lack of encryption, the ease with which fake QR codes can be generated, and the inability to verify the location of the source, both ordinary users and businesses are exposed to serious risks.<br>This article examines the most common threats associated with the use of QR codes, using examples of phishing attacks, malware infections and data leaks. It stresses that poor data protection and lack of encryption can lead to unauthorized access to personal and financial information. It also examines how fake QR codes, which are often posted in public places, can lead users to malicious websites, leading to identity theft and financial losses. Based on a detailed analysis of these risks, the document argues that in order to solve this problem, it is necessary to pay more attention to the security of QR codes in order to maintain confidence in this widely used technology. |
| 12:15 AM – 12:35 PM<br>Paper 142 | ***Detecting Hardware Trojans: Deep Learning Solutions Combining PUF Metrics and Side-Channel Observations***<br>*Authors:* Muskan Saraf*, Akshay Kulkarni, Mohammed Niamat<br>*Abstract:* This study presents a deep learning-based framework for detecting hardware Trojans in integrated circuits (ICs) using Side-Channel Analysis (SCA) and Challenge-Response Pairs (CRPs) from Ring Oscillator Physical Unclonable Functions (ROPUFs). A Trojan-infected ROPUF is implemented on an Artix-7 FPGA using VHDL in the AMD Xilinx Vivado Design Suite. Power, voltage, and current traces are collected using Keysight DC power analyzers under Trojan-active and Trojaninactive states to assess the impact of Trojan circuits. The study employs advanced Deep Learning Algorithms (DLAs), including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Deep Clustering Networks (DCN), to analyze subtle variations in the collected datasets. Experimental results demonstrate that LSTM and RNN models achieve the best performance, excelling in both CRP and SCA datasets with superior precision, recall, and F1 scores. Specifically, the LSTM model achieves an accuracy of 87% when combining CRP and SCA datasets, indicating its effectiveness in identifying Trojan-induced anomalies. This research highlights the reliability of DL models in enhancing hardware security and providing an efficient detection mechanism for malicious intrusions. |

# MORNING TECHNICAL SESSIONS

Day 3 - Thursday February 27, 2025

**11:15 AM – 12:35 PM**

**SaTC Exhibition & Poster Session II**
(BALLROOM/FOYER)

SESSION CHAIRS: Dr. Suleiman Ashur, *Professor of Civil Engineering and Construction Management, Eastern Michigan University*

Poster Session II: 11:15 PM – 12:35 PM

| Poster Number | Paper ID | Title | Authors |
|---|---|---|---|
| Poster 1 | 15 | Leveraging Advanced AI for Real-Time Sign Language Detection and Translation: A Pioneering Approach to Bridging Communicative Gaps and Promoting Societal Inclusivity | Sk. Md. Towfikul Islam Siam, Maher Ali Rusho, Md. Saad Bin Sayed, Md. Mofazzal Hossen, Sumiya Sultana, Mehedi Hasan Refat, Ahmed Haque Dhrubo*, Mohammad Abdul Qayum |
| Poster 2 | 159 | Robust Server Room Monitoring with SIGFOX IoT Gateway and Adaptive Gated Recurrent Units | Mani Rupak Gurram, Mithun Kumar Pk, Fathi Amsaad* |
| Poster 3 | 105 | Predictive Analytics for Sepsis Using Time-Series Data and Recurrent Neural Networks | Sara A Althubiti, Farzeen Ashfaq * |
| Poster 4 | 161 | Severity Assessment of Cardiac Arrhythmias Through | Mithun Kumar Pk, Fathi Amsaad, Darryl Ahner |
| Poster 5 | 141 | Factors Influencing Student Adoption of ChatGPT in Higher Education: A Technology Acceptance Model-Based Survey | Jonathan Walatkiewicz, Abdallah Al Shorman, Omar Darwish, Robert Carpenter |
| Poster 6 | 162 | Securing IoT/Edge Computing Infrastructure for Smart Agriculture: Challenges and Solutions | Niraj Prasad Bhatta, Fathi Amsaad, Sufian Al Majmaie |
| Poster 7 | 167 | Secure and Privacy-Preserving AI: A Zero Trust Architecture for Federated Machine Learning | Al Amin Hossain, Mithun Kumar PK, Fathi Amsaad, Darryl Ahner |
| Poster 8 | 177 | The Art of Obfuscation: A Comprehensive Survey of Software Protection Techniques | Khaled Saleh, Love Kumar Sah, Fathi Amsaad |

|  |  |  |  |
|---|---|---|---|
| Poster 9 | 197 | Parrot Anafi Ai Drone Configuration for Programmable Flight | Jonathan Walatkiewicz, Abdullah Al Shomar, Sara Acikkol Dogan, Samir Tout, Omar Darwish |

|  |  |
|---|---|
| **12:00 PM – 13:30 PM** | **LUNCH BUFFET OPEN** |

Ballroom

# WORKSHOP

Day 3 - Thursday February 27, 2025

**11:15 AM – 12:35 AM**

**Cybersecurity in Aerospace: Protecting Critical Systems in a Connected World**
*Collaborator*: Mr. David Haase (Relite IT)
*Collaborator:* Mr. Eric Parsley (Expedient Technology Solutions, LLC)

**David Haase Bio**: David Haase is the owner of Relite IT, a managed service provider offering solutions including IT consulting, computer networking, computer repair, backup & recovery systems, and more. He is passionate about helping businesses and individuals with their IT needs, offering both refurbished and new computer sales and services. David is also an international director for Sewing Centers for Women in Pakistan, where he manages resources and establishes strategic goals to empower women. His experience also includes roles such as Assistant Chief Flight Instructor at Aviation Sales, Inc. and adjunct faculty at Sinclair Community College. He holds an Associate of Arts and Sciences (AAS) degree in Aeronautics/Aviation/Aerospace Science from Sinclair Community College.

**Mr. Eric Parsley Bio**: Eric Parsley is a vCISO with over 13 years of experience in IT and cybersecurity, specializing in cybersecurity program development and implementation, business continuity planning, and incident response strategy. Currently, he serves as the vCISO at Expedient Technology Solutions LLC, where he helps clients better protect themselves from cyber threats, security risks, and business disruptions. He is also a Ph.D. student in Computer Engineering at Wright State University, further advancing his expertise in cybersecurity and technology. In addition to his cybersecurity roles, Eric has worked in various technical positions, including systems security administration and cybersecurity engineering. He holds multiple certifications, including CISSP, CISM, CRISC, CCP, and CCA, and has contributed significantly to the development of cybersecurity strategies and solutions.

Ballroom

# LUNCHEON KEYNOTE PRESENTATIONS

Day 3 - Thursday February 27, 2025

**12:40 PM – 13:20 PM**

**Cybersecurity Leadership in a Rapidly Evolving Threat Landscape**
*Session Chair:* Mr. Eric Parsley (Expedient Technology Solutions, LLC)
*Presenter:* Mr. Don Boian (OCRI, Former NSA)

**Abstract:**

With decades of experience in cybersecurity, intelligence, and risk management, Don Boian will provide critical insights into the evolving cybersecurity landscape, risk management strategies, and leadership in securing organizations against modern threats. Drawing from his extensive background in both government intelligence operations and private-sector cybersecurity, Mr. Boian will discuss the challenges organizations face in building resilient security programs, navigating regulatory compliance, and adapting to emerging cyber threats. His talk will also emphasize the role of security executives in shaping national cybersecurity policies and fostering collaboration between public and private sectors to strengthen the overall security ecosystem.

**Bio:**

Don Boian is an accomplished technology leader and award-winning information security expert with extensive experience in both the public and private sectors. He currently serves as the Chief Information Security Officer (CISO) of Hound Labs, a biotech startup in the San Francisco Bay Area. Previously, he was the Security Outreach Director and CISO of Huntington National Bank, where he led security and risk management initiatives. Before transitioning to the private sector, Mr. Boian spent 30 years with the National Security Agency (NSA), where he retired as a Defense Intelligence Senior Executive. His leadership roles included Associate Deputy Director for TechSIGINT and Ground Capabilities, Chief Mission Control Capabilities, Technical Director for the Chief of Operations (J3) at USCYBERCOM, and Director of Operations for TAO (Tailored Access Operations). His expertise spans both offensive and defensive cyber operations, making him a key figure in national cybersecurity efforts. Mr. Boian is highly active in the cybersecurity community, serving on the board of the National Technology Security Coalition (NTSC) and leading its Strategic Direction Committee, where he collaborates with lawmakers to shape effective cybersecurity policies. He is also a cybersecurity consultant for the U.S. Department of Energy.

His contributions have been recognized with numerous awards, including the Chairman Joint Civilian Service Commendation Award, Dr. Louis Tordella Award, Meritorious Civilian Service Award, and the National Intelligence Meritorious Unit Citation. Mr. Boian holds an MS in Electronic Engineering from Johns Hopkins University and a BS in Electrical Engineering from The Ohio State University.

# INVITED TALK

Day 3 - Thursday February 27, 2025

**13:30 PM – 13:50 PM**

**Trust in AI/ML: A User-Centered Perspective**
*Session Chair:* Mr. Dominic Mohrhardt (AFLCMC)
*Presenter:* Dr. Gene M. Alarcon (AFRL)

**Abstract**:
Dr. Gene M. Alarcon will provide an insightful discussion on trust in artificial intelligence and machine learning (AI/ML) from a user perspective. Drawing on his expertise in industrial-organizational psychology, Dr. Alarcon will explore the psychological and behavioral factors that influence trust in AI/ML systems. His talk will cover key considerations such as interpersonal trust, human-AI interactions, personality influences, and the challenges of fostering user confidence in AI-driven technologies. Attendees will gain a deeper understanding of how trust is developed, maintained, and potentially eroded in AI applications, particularly in high-stakes environments such as defense and security.

**Speaker Bio**: Gene M. Alarcon is a senior research psychologist in the Air Force Research Laboratory at Wright Patterson Air Force Base, Ohio. He earned his PhD in industrial organizational psychology from Wright State University in 2009. His research interests include interpersonal trust, trust in technology, personality and artificial intelligence / machine learning.

Ballroom

# INVITED TALK

Day 3 - Thursday February 27, 2025

**13:50 PM – 14:10 PM**

**Empowering Cybersecurity Through Training, Leadership, and Innovation**

*Session Chair:* Mr. Dominic Mohrhardt (AFLCMC)
*Presenter:* Ms. Connie Matthews Reynolds (ReynCon Educational Services & Cybersecurity Training)

**Abstract:**
This invited talk will focus on the evolving cybersecurity landscape, the importance of skills development, and strategies for strengthening organizational security through training and leadership. As cyber threats continue to grow in complexity, organizations must adopt **proactive security measures, invest in workforce training, and foster a culture of continuous learning**. The session will highlight key **industry trends, challenges in securing digital assets, and best practices for building resilient cybersecurity programs**. Additionally, it will explore the role of **leadership in driving security awareness, bridging the cybersecurity skills gap, and implementing innovative training solutions** to prepare professionals for emerging threats in an increasingly digital world.

**Speaker Bio**: Connie Matthews Reynolds is the Founder and CEO of ReynCon, a cybersecurity training and consulting provider. She is a passionate cybersecurity expert who has worked in the industry for over 19 years. ReynCon focuses on training and development in InfoSec/Cybersecurity domains. They work with companies to build comprehensive programs that drive positive change in the business and upskill their teams. Connie is a trailblazer in the Ohio tech industry and was recently named among 11 recipients of Verizon's inaugural Ohio Trailblazers Award. She was named a finalist for the Cyber Security Woman of The World and Cyber Security Woman Volunteer of the World (2023). Connie currently serves as the President of Central Ohio ISSA, Co-Chair of the Leadership Team of ISSA International, and Advisor for Netskope, Breach Siren, and Accelerating Angels.

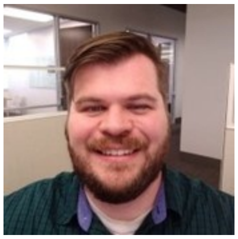
# INVITED TALK

Day 3 - Thursday February 27, 2025

**14:10 PM – 14:30 PM**

**A Radically Transparent Computer Without Complex VLSI**
*Session Chair:* Mr. Dominic Mohrhardt (AFLCMC)
*Presenter:* Dr. Marc Abel (Wright State University)

**ABSTRACT:** Foreign adversaries have colonized America's computers from at least 1986. Four decades later, online safety is the largest failure in the history of human engineering. Radical stewardship in cybersecurity would bring radical progress, but responsibility for losses will need to flow from the bottom up. The buck stops with victims, who must accept all blame for cyberattacks. Only then will people at risk properly vet the products and vendors they select. A leading challenge in stewardship is balancing the opaque, proprietary nature of VLSI complex logic with the owner's need for complete control. Since these aspects are incompatible and owner control is essential, it's necessary to offer computer designs that avoid complex VLSI entirely. One such architecture, Dauug|36, is being developed at Wright State University to deliver 36-bit computing, preemptive multitasking, paged virtual memory, and hundreds of opcodes, all without using a single microprocessor or anything like one.



**Speaker Bio**: Marc Abel is an engineer-scientist specializing in technology that supports civil rights, economic security, and geopolitical stability. He holds a 1991 B.S. in Engineering and Applied Science (focused on computer science) from Caltech, and a 2022 Ph.D. in Computer Science and Engineering from Wright State University. Marc is the sole inventor, architect, implementer, maintainer, documenter, and promoter of the Dauug|36 open-source minicomputer for critical infrastructure. He is the original and still only author of Dauug|36's firmware, designer and implementer of Dauug|36's assembly language and assemblers, writer of several related software tools, especially open-source electronic design automation and simulation tools, and the sole author of Osmin, a real-time operating system (RTOS) kernel for the architecture. He is the writer of 200,000 words of system documentation, including his dissertation and its online continuation called The Dauug House.

| | |
|---|---|
| 14:30 PM – 14:50 PM | COFFEE BREAK & PANEL SETUP |

# PANEL DISCUSSION

Day 3 - Thursday February 27, 2025

**14:50 PM – 16:35 PM**

## Empowering Innovation: Leveraging HBCU Expertise in Cybersecurity, Microelectronics, Semiconductors, and Beyond Panel

(BALLROOM)

| | | |
|---|---|---|
| MODERATOR: | | Dr. Steven Bibyk<br>(Ohio State University) |

**Moderator Bio**: Steven Bibyk’s research interests include, trust and assurance of secure electronic systems, rapid prototyping of embedded systems, reincarnating art and technology pieces for education of innovation and inventing. His teaching interests are all types of electronics and embedded systems, informal learning in prototyping activities such as student projects, competitions, and maker contests. While at The Ohio State University, Dr. Bibyk has also worked in the following positions: (1) National Research Council Fellow, Summer Faculty at Air Force Research Labs, (2) Research Scientist, Space Electronics Division, NASA Glenn Research Center and the Ohio Aerospace Inst. (3) Senior Scientist for the Micrys Corp., Columbus Ohio, (4) Extensive consulting with government and industry design groups in setting up integrated circuit design facilities, (5) STEP Faculty Mentor for the STEPmaker program.

**Panel Overview**: This panel will highlight the contributions of Historically Black Colleges and Universities (HBCUs) in microelectronics and related fields, emphasizing their partnerships with non-HBCUs and industry with key discussion topics including: 1) HBCU Research Excellence in Microelectronics: Showcasing cutting-edge research projects led by HBCUs, focusing on innovation in microelectronics, semiconductors, nanoengineering and materials science. 2) Cross-Disciplinary Collaborative Initiatives and Industry Partnerships: Exploring successful collaborations between HBCUs, non-HBCUs, and industry partners that drive innovation and offer practical opportunities for student engagement in STEM research and internships, while including the underrepresented minorities and females to ensure equity in future workforce preparation. 3) Advancing Diversity in Technology Fields: Discussing HBCU contributions in expanding diversity within STEM, including pathways that prepare underrepresented students for careers in microelectronics, computer engineering, and data science

# PANEL DISCUSSION

Day 3 - Thursday February 27, 2025

**14:50 PM – 16:35 PM**

**Empowering Innovation: Leveraging HBCU Expertise in Cybersecurity, Microelectronics, Semiconductors, and Beyond Panel**
(BALLROOM)

| | |
|---|---|
| MODERATOR: | Dr. Steven Bibyk<br>(Ohio State University) |

**Panelists**:

Dr. Mohammadreza Hadizadeh

**Panelist Bio**: Dr. Mohammadreza Hadizadeh is a distinguished theoretical and computational physicist who earned his Ph.D. in Physics in 2008. He currently serves as an Associate Professor of Physics and the Director of the Semiconductor Education and Research Program at Central State University. Dr. Hadizadeh's research expertise encompasses the theoretical and computational study of quantum few-body systems and two-dimensional semiconductor materials. Throughout his career, Dr. Hadizadeh has spearheaded numerous research and educational initiatives. He currently leads two major semiconductor consortia: the first, funded by Intel, collaborates with six higher education institutions across Ohio, and the second, funded by the National Science Foundation, partners with seven HBCUs. These consortia focus on developing technical workforce training, education, and research programs, with a special emphasis on supporting women and underrepresented minorities in the field. Dr. Hadizadeh is an active contributor to the scientific community, serving on the editorial boards of Scientific Reports and PLOS One. He has published over 60 journal articles and delivered more than 60 scientific presentations. His outstanding achievements have been recognized with the Central State University President's Award for exceptional success in securing significant external grants and the Faculty Excellence in Research Award.

s

# PANEL DISCUSSION

Day 3 - Thursday February 27, 2025

**14:50 PM – 16:35 PM**

**Empowering Innovation: Leveraging HBCU Expertise in Cybersecurity, Microelectronics, Semiconductors, and Beyond Panel**
(BALLROOM)

| | |
|---|---|
| MODERATOR: | Dr. Steven Bibyk<br>(Ohio State University) |

**Panelists (Continued)**:

Dr. Michael L. Curry

**Panelist Bio**: Dr. Michael L. Curry is a Professor and Graduate Program Coordinator in the Department of Nanoengineering at the Joint School of Nanoscience and Nanoengineering, North Carolina A&T State University (NC A&T). He earned his Ph.D. in Analytical Chemistry from the University of Alabama in 2004 and his B.S. in Chemistry from the University of West Alabama in 1999. Over the past 15+ years, Dr. Curry has established himself as a leading HBCU professor, researcher, and inventor, having mentored numerous undergraduate and graduate students. His research primarily focuses on developing biorenewable materials to replace synthetic polymers, thus mitigating climate change impacts. Dr. Curry's contributions to science include over 60 peer-reviewed publications, two U.S. patents, three pending patent applications, and more than 200 technical presentations. His work has been cited over 1300 times and led to the foundation of a startup specializing in sustainable biobased materials. He has also played a pivotal role in securing substantial grant funding for multidisciplinary research centers, enhancing research and educational capabilities at HBCUs. His dedication to STEM education and diversity has been recognized widely, earning him accolades such as the NC A&T Inaugural Faculty Fellow for the Center for Excellence in Entrepreneurship and Innovation, the 2025 American Chemical Society Stanley C. Israel Award for advancing diversity in chemical sciences, and several others. Dr. Curry's editorial work and organization of a special issue in the American Chemical Society Accounts of Chemical Research highlight the innovation at HBCUs, underscoring his impact on the chemical sciences landscape.

# PANEL DISCUSSION

Day 3 - Thursday February 27, 2025

**14:50 PM – 16:35 PM**

**Empowering Innovation: Leveraging HBCU Expertise in Cybersecurity, Microelectronics, Semiconductors, and Beyond Panel**
(BALLROOM)

| | |
|---|---|
| MODERATOR: | Dr. Steven Bibyk<br>(Ohio State University) |

**Panelists (Continued)**:

Dr. Suxia Cui

**Panelist Bio**: Dr. Suxia Cui is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University (PVAMU). She received her B.S. and M.S. degrees in Electrical Engineering from Beijing University of Technology, China, in 1999. In 2003, she joined PVAMU as an assistant professor after earning her Ph.D. in Computer Engineering from Mississippi State University, Starkville, MS. Dr. Cui's research interests include machine learning, computer vision, cybersecurity, and computing education. Her work has received funding from organizations, including the National Science Foundation, the U.S. Department of Agriculture, the Department of Defense, and the Department of Education. Additionally, Dr. Cui serves as an ACCESS campus champion, where she actively promotes high-performance computing research and education at PVAMU. She is a senior member of IEEE and an active member of professional organizations such as HKN, ACM, ASEE, and SPIE.

Dr. George White

**Panelist Bio**: Dr. White is the Senior Director of Strategic Partnerships at Georgia Tech, driving innovation collaborations with corporations, government, academia, national labs, and HBCUs. He has co-chaired key research initiatives in AI, Hypersonics, Biomanufacturing, Additive Manufacturing, Quantum Computing, and Trusted Electronics. A serial entrepreneur, Dr. White founded and sold Jacket Micro Devices and Innovative Packaging Solutions, raising over $22M in startup capital. With 30+ patents and 100+ publications, he has helped secure $700M+ in research funding. He holds a B.A. in Physics from Hampton University and an M.S. & Ph.D. in Metallurgical Engineering from the University of Illinois at Urbana-Champaign.

# PANEL DISCUSSION

Day 3 - Thursday February 27, 2025

**14:50 PM – 16:35 PM**

**Empowering Innovation: Leveraging HBCU Expertise in Cybersecurity, Microelectronics, Semiconductors, and Beyond Panel**
(BALLROOM)

| | |
|---|---|
| MODERATOR: | Dr. Steven Bibyk<br>(Ohio State University) |

**Panelists (Continued)**:

Dr. Daniel Vrinceanu

**Panelist Bio**: Dr. Daniel Vrinceanu is a Professor of Physics at Texas Southern University (TSU) and Interim Associate Dean for Research and Outreach in the College of Science, Engineering, and Technology. A former International Physics Olympiad medalist, he earned his Ph.D. in Theoretical Atomic Physics from Georgia Tech, receiving the Sigma-Xi and APS Thesis Prize for his groundbreaking research. His expertise spans atomic and molecular physics, computational physics, and atmospheric science. His work on magnetized antihydrogen at the Harvard-Smithsonian Center revolutionized CERN data analysis, and his research at Los Alamos National Laboratory advanced plasma simulations. He now leads a DOE-funded atmospheric science program at TSU. As Director of TSU's High-Performance Computing Center, Dr. Vrinceanu applies computational and AI-driven methods to scientific challenges. A strong advocate for diversity in STEM, he plays a key role in the DOE's RENEW initiative, fostering graduate training in atmospheric sciences. His multidisciplinary research continues to push the frontiers of physics while mentoring the next generation of scientists.

| | |
|---|---|
| 16:35 PM – 17:35 PM | Closing Remarks from the SaTC Conference Chairs & Networking Opportunity |
| End of Day 3 | |

## Day 3 – Thursday February 27, 2025

## ONLINE SESSIONS-1

PAPER PRESENTATIONS (10:00 AM – 11:30 AM)

Online Sessions Google Meet Link-1

| | |
|---|---|
| SESSION CHAIR: | Dr. Akshay Kulkarni, *Assistant Professor at Prairie View A&M University* |

| ML Cybersecurity techniques for DevOps & Supply Chain applications | |
|---|---|
| **Paper ID** | **Title / Authors** |
| **47** | **Applying Artificial Intelligence to DevOps: A Study on AI-Driven Anomaly Detection and Predictive Maintenance in Cloud Environments**<br>*Authors:* Patel, Advait |
| **48** | **Systematic Literature Review of Cybersecurity Testbeds for Industrial Internet of Things.**<br>*Authors:* Taiwo Akinremi*, Joel Appiah, Amir Asadi, Opetunde Ibitoye, Hansinie Jayathilake, Hazem Said |
| **50** | **Prediction of Suicidal Tendencies in Adolescents Using Machine Learning Models and Artificial Intelligence**<br>*Authors:* Abdul Razaque*,Orazmukhamed Bekmurat, Ajmal Khan, Saule Amanzholova |
| **56** | **Optimizing Deep Feedforward Neural Networks for Effective Classification and Prediction of Cyber Incidents**<br>*Authors*: I, Ajitha ; A, Devi |
| **59** | **Exploratory Study on the Application of Artificial Intelligence Tools to Enhance Supply Chain Resilience**<br>*Authors:* Ibitoye, Opetunde; Asadi, Amir; Akinremi, Taiwo; Appiah, Joel; Jayathilake, Hansinie; Said, Hazem |
| **93** | **Categorization of IoT and Deep Learning-based Smart Waste Management detection and identification in cities**<br>*Author*: Saeed Almuflih , Ali ; Ayazuddin, Rizwan |
| **97** | **Leveraging Explainable Artificial Intelligence with Ensemble of Deep Learning Model for Predicting Customer Lifetime Value in the Fintech Sector**<br>*Author*: Pustokhina, Irina; Pustokhin, Denis ; Ashfaq, Farzeen |

## Day 3 – Thursday February 27, 2025

## ONLINE SESSIONS-2

PAPER PRESENTATIONS (10:00 AM – 11:30 AM)

Online Sessions Google Meet Link-2

| | |
|---|---|
| SESSION CHAIR: | Dr. Ahmed Ammar, *Assistant Professor of Electrical & Computer Engineering, Ohio Northern University* |

| Deep Learning & Gen AI for Life Critical Applications | |
|---|---|
| **Paper ID** | **Title / Authors** |
| **78** | **A Deep Learning Framework for Efficient Bone Cancer Detection and Classification**<br>*Authors*: Sagarika Saka, Santhosh Boddupalli, Farzeen Ashfaq * |
| **118** | **Data Engineering for Intelligent Systems and Generative AI: Architectures, Pipelines, and Strategy**<br>*Author*: Srinivas Murri* |
| **119** | **Advanced Automation Techniques for Ensuring Quality in AdTech Machine Learning and Data Pipelines**<br>*Author*: Naga Harini Kodey, Navadeep Vempati, Balaji Thadagamkandavel |
| **121** | **Advanced Machine Learning Models for Anti-Money Laundering (AML): Improving Detection Accuracy and Efficiency**<br>*Author*: Sagar Bharat Shah * |
| **125** | **Graph Contrastive Learning and GAN-based Fraud Detection in Imbalanced Graphs**<br>*Author*: Akhila Reddy Yadulla, Mounica Yenugula, Bhargavi Konda, Vinay Kumar Kasula, Chandra Mouli Madhav Kotteti, Sarath Babu Rakki |
| **127** | **MedDose: Redefining Medication Compliance Through an Intelligent AI and IoT-Driven System**<br>*Author*: Osmita Monzur Subonty, Md. Mahfuzur Rahman, Md. Abdur Rahman, Ahmed Haque Dhrubo, Farhana Sharmin, Mohammad Abdul Qayum |
| **33** | **Financial Status Analysis Using Credit Score Rating**<br>*Author*: Abdul Razaque*, Daulet Shynggys, Zhyldyz Kalpeyeva, Moldagulova Aiman Nickolayevna, Uskenbayeva Raissa Kabievna, Ajmal Khan |

## Day 3 – Thursday February 27, 2025

## ONLINE SESSIONS-3

PAPER PRESENTATIONS (10:00 AM – 11:30 AM)

Online Sessions Google Meet Link-3

| | |
|---|---|
| SESSION CHAIR: | Dr. Omar Darwish, *Assistant Professor of Information Security and Applied Computing, Eastern Michigan University* |

| **Performance & Evaluation of Cybersecurity Challenges using AI** | |
|---|---|
| **Paper ID** | **Title / Authors** |
| 104 | **Enhancing Precision Agriculture through Stacked Ensemble Model and Interpretability**<br>*Author*: Chitra Chitra, Preethi Raghuraman, Varsha Varsha, Manasa Mallavaram, Rizwan Ayaz |
| 108 | **Integrating Enhanced Learning to Rank into a Hybrid Deep Learning System for Optimized Recommendations**<br>*Author*: Naveen Kumar Navuri, Cvpr Prasad, Farzeen Ashfaq |
| 132 | **A Performance Evaluation of Post Quantum Digital Signatures for Proof of Stake Consensus**<br>*Author*: Tyler Judd, Suleyman Uludag |
| 139 | **A Comprehensive Survey of Model Extraction Attacks: Current Trends, Defenses, and Future Directions**<br>*Author*: Quazi Rian Hasnaine, Yaodan Cindy Hu, Mohamed I. Ibrahem, Mostafa M. Fouda. |
| 140 | **A Novel Attack Against Smart Grid Transformer Oil Temperature Prediction Systems**<br>*Author*: Alyaman Massarani, Mahmoud Badr, Mohamed Baza, Wassila Lalouani, Mohammad Hammoudeh, Amar Rasheed |
| 147 | **Evaluating the Efficacy of GPT-based Password Generation on Real World Data**<br>*Author*: Oguz Kagnici, Halil Bisgin, Suleyman Uludag |

## Day 3 – Thursday February 27, 2025

## ONLINE SESSIONS-4

PAPER PRESENTATIONS (11:40 AM – 13:20 AM)

**Online Sessions Google Meet Link-1**

| | |
|---|---|
| SESSION CHAIR: | Dr. Faezeh Soleimani, *Assistant Professor of Mathematical Sciences, Ball State University* |

| Next-Gen Security & Privacy Preservation for Smart Systems | |
|---|---|
| **Paper ID** | **Title / Authors** |
| 145 | **Advanced Encryption Techniques for Enhancing Data Security and Privacy in Cloud Environments**<br>*Author*: Parth Shah, Samarth Shah, Anurag Agrawal |
| 154 | **Privacy-Preserving Secure Framework for Intelligent Transportation Systems**<br>*Author*: Yuka Nagayoshi, Sharif Ullah, Bernard Chen, Mohamed Ibrahem, Mostafa Fouda, Mahmoud Abouyoussef |
| 157 | **Exploring Few-Shot Learning for CPS Anomaly Detection: A Path Toward Smart Grid Applications**<br>*Author*: Chowdhury Tasnuva Hazera, Mohamed Ibrahem, Mostafa Fouda |
| 172 | **hChain 4.0: A Permissioned Blockchain Framework for Secure, Privacy-Preserving, and Scalable EHR Management**<br>*Author*: Musharraf Alruwaill, Saraju Mohanty, Elias Kougianos |
| 175 | **A Quantum-Resistant Privacy-Preserving Framework for Consortium Blockchains Using Blind Signatures, Hierarchical Fully Homomorphic Encryption, and Zero-Knowledge Proofs**<br>*Author*: Bhargavi Konda, Akhila Reddy Yadulla , Vinay Kumar Kasula, Mounica Yenugula, Sarath Babu Rakki |
| 176 | **Adaptive Decision Tree With Random Forest Integration And Dimensionality Reduction For Efficient Botnet Forensics**<br>AUTHOR: Mohammed Abdulrazzaq, Ahmed Najm Obaid Alzubaidi, Abdullahi Abdu İbrahim |
| 200 | **Artificial Intelligence's Impact on the Banking Industry: Enhancing Security and Efficiency**<br>*Author*: Surendra Pandey, Bharat Bhushan, Pronaya Bhattacharya, Esraa Mohammed Alazzawi, Akhtar Jamil, Ravish Kumar Singh |
| 207 | **Enhancing Breast Cancer Detection in X-ray Imaging with Vision Transformers and CNNs Using Hybrid Edge-Aware Filtering**<br>*Author*: Esraa Mohammed Alazzawi, Mohammed Sadoon Hathal |

## Day 3 – Thursday February 27, 2025

## ONLINE SESSIONS-5

PAPER PRESENTATIONS (11:40 AM – 13:20 PM)

Online Sessions Google Meet Link-2

| | |
|---|---|
| SESSION CHAIR: | Dr. Wadhah Zeyad Tareq, *Assistant Professor, Istinye University, Turkey* |

| AI for Cybersecurity & Healthcare Applications | |
|---|---|
| **Paper ID** | **Title / Authors** |
| 150 | **Fine-Tuning LLaMA-3.2-3BIT on Bengali Hate Speech Dataset for Sentiment Classification**<br>AUTHOR: Abu Mukaddim Rahi, Mariam Binte Bashir, Maher Ali Rusho, Md Khurshid Jahan* |
| 182 | **Hybrid Deep Learning with Active Period Segmentation and Weighted Voting Ensemble for Intrusion Detection in IoT**<br>AUTHOR: Chitty Avula, Sathyanarayana Bachala |
| 186 | **Cluster based Personalized Recommender System to address Cold-Start Challenge**<br>*Author*: LNC. Prakash K, E. Pavithra, N. Nagalakshmi, V. Surya Narayana Reddy, S. Annapoorna, A. Chitty |
| 189 | **Machine Learning based Predictive Analysis of Obstructive Pulmonary Disease Progression using Chest X-Rays**<br>*Author*: Nagendra Kumar V. V, Rajeswari D, Farzeen Ashfaq |
| 202 | **Generative Artificial Intelligence(GenAI) models for Cyberbullying Detection and Prevention**<br>*Author*: Andleeb Khan, Bharat Bhushan, Parma Nand, Pronaya Bhattacharya |
| 204 | **Advancing Intrusion Detection in Software-Defined Networks**<br>*Author*: Atul Agrawal, Bharat Bhushan |
| 205 | **IoT Enabled Blue Force Tracker: The Warrior System for Enhanced Situational Awareness and Improved Tactical Decision Making**<br>*Author*: Priyanka Mane, Mandar Kolap, Rajesh Bharatiya, Madhuri Jadhavolap |
| 35 | **Hybrid Approach for Breast Cancer Detection Using CNNs and Real-Time Risk Assessment**<br>Author: Abdul Razaque*, Baurzhan Arabov, Gulfairus Kairedenova, Ajmal Khan |

## Day 3 – Thursday February 27, 2025

## ONLINE SESSIONS-6

PAPER PRESENTATIONS (11:40 AM – 13:20 AM)

Online Sessions Google Meet Link-3

| | |
|---|---|
| SESSION CHAIR: | Dr. Muhammed Davud, *Assistant Professor, Istinye University, Turkey* |

| Design & Development of AI Across Disciplines | |
|---|---|
| **Paper ID** | **Title / Authors** |
| **79** | **Developing Strategic Interventions in Enhancing English Language Proficiency of Engineering Students Using Deep Forest and Python**<br>*Author*: Medikonda Jayaranjan, Medikonda Jayaranjan, Farzeen Ashfaq |
| **80** | **Analyzing Greenspace Changes in Vijayawada (2019-2024) Using Remote Sensing and Machine Learning**<br>*Author*: Abhinaya Chalamalasetti, Raja Sravan Kumar Kovvali, Nandini Devi Rajulapati, Naga Nikshipta Vemuri, Farzeen Ashfaq |
| **13** | **healthMLsec: Machine Learning based Vulnerability Assessment in Health Systems: A Framework for Enhancing Cybersecurity and Patient Data**<br>*Author*: Omar Faruq Osama, Naresh Kshetri*, Mir Mehedi Rahman, Bishwo Prakash Pokharel |
| **92** | **Designing an Efficient Fertilizer Recommendation System with Bayesian Light GBM Processing and Mobile Net-Based Image Analysis**<br>*Author*: K. Anji Reddy, Ch. Nanda Sai Ram, V. Esther Jyothi, H. Pavan Venkata Sai Kumar, G. Bhavana, Rizwan Ayaz |
| **95** | **Gold Price Prediction Based on Stock Analysis Using CNN-Bidirectional LSTM**<br>*Author*: G.S.N.V. Sarvani, U. Kousalya, P. Sathwika, B.N. Ashok, Radhika Rani Chintala, Radha Mothukuri |
| **120** | **Evaluating Efficiency of Advanced Encryption Algorithms for Cloud Data Security**<br>*Author*: Himani Fnu, Srinivas Murri |
| **43** | **Efficient CSI Feedback for Large-Scale MIMO IoT Systems Using YOLOv8-Based Network**<br>*Author*: Rajesh, Daruvuri |

| Start | End | | SaTC 2025 AGENDA AT-A-GLANCE | | | |
|---|---|---|---|---|---|---|
| Day 1 – Tuesday February 25, 2025 | | | | | | Coffee Breaks: 1000 – 1010 & 1410 – 1420 & 1520 - 1530 |
| 07:30 | 17:00 | | Registration | | | BALLROOM FOYER |
| 07:30 | 08:30 | | Breakfast | | | BALLROOM FOYER |
| 08:05 | 09:05 | | Opening Remarks from the SaTC Conference Chairs | | | BALLROOM |
| 09:05 | 09:45 | | Keynote Talk<br>Session Chair: Prof. Waleed Khalil, Ohio State University<br>Speaker: Dr. Matthew Casto, CTO, MMEC Inc. | | | BALLROOM |
| 09:45 | 10:00 | | Invited Speaker<br>Mr. Dominic Mohrhardt (AFLCMC)<br>Salman Nasir (Director, Natcast) | | | BALLROOM |
| | | | Ballroom | Auditorium | Kitty Hawk | |
| 10:10 | 11:30 | | Side-Channel Analysis and Zero Trust Security | Exploration of Automotive Safety and Cybersecurity | Energy-Efficient Wireless Protocols for IoT | |
| 1130 | 1300 | | Lunch Buffet Open & Networking Opportunity | | | BALLROOM |
| 1210 | 1245 | | Luncheon Keynote<br>Mr. Aaron Miller, Galois, Inc.<br>Mr. P. Len Orlando III (ANSYS) | | | BALLROOM |
| 1300 | 1410 | | Software/Hardware Co-Design Solutions: Assured and Trusted Microelectronics, IoT Security, and Side Channel Analysis Panel | | | BALLROOM |
| 1420 | 1520 | | Invited Speakers<br>Mr. Dominic Mohrhardt (AFLCMC)<br>Prof. Kenneth M. Hopkinson (AFIT), Dr. Matt Areno (Intel) | | | BALLROOM |
| | | | Ballroom | Auditorium | Kitty Hawk | |
| 1530 | 1650 | | Trustworthy AI and Cyber-Physical Security in Smart Cities and IIoT | Security and Privacy-Aware Schemes for Internet of Things (IoTs) | Emerging Technologies and Applications in Secure and Intelligent Systems | |
| 1650 | 1750 | | Invited Speakers<br>Dr. Love Kumar Sah (Western New England University)<br>Prof. Saraju Mohanty (UNT), Prof. Noor Zaman Jhanjhi (Taylor’s U.) | | | Ballroom |
| 1700 | 1830 | | SaTC Reception & Networking Opportunity | | | Ballroom/Foyer |
| Day 2 – Wednesday February 26, 2025 | | | | | | Coffee Breaks: 1245 – 1300 & 1410 - 1430 |
| 0730 | 1700 | | Registration | | | BALLROOM FOYER |
| 0730 | 0830 | | Breakfast | | | |
| 0810 | 0820 | | Welcome and Overview of Day 2 Agenda | | | BALLROOM |
| 0820 | 0940 | | Keynote Talk<br>Prof. Moussa Ayyash, Chicago State University<br>Prof. Swarup Bhunia (IEEE Fellow), University of Florida,<br>Dr. Steven D. Harbour (Parallax Advanced Research) | | | BALLROOM |
| 0940 | 1020 | | Break & Networking Opportunity | | | |
| | | | Ballroom | Auditorium | Kitty Hawk | |
| 1020 | 1140 | | Future Trends in IoT Systems Security and Trusted Microelectronics | Robust AI Models for IoT Security | AI-Driven Threat Analysis for IoT Software Security | |
| 1130 | 1300 | | Lunch Buffet Open | | | BALLROOM |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| 1210 | 1245 | Luncheon Keynote<br>Mr. Eric Parsley (Expedient Technology Solutions, LLC)<br>Dr. Ibrahim (Abe) Baggili (Louisiana State University) |  |  | BALLROOM |
| 1300 | 1410 | Cybersecurity and Microelectronics Workforce Development Panel |  |  | BALLROOM |
| 1430 | 1520 | Invited Speakers<br>Mr. Dominic Mohrhardt (AFLCMC)<br>Dr. Samir Tout, Ph.D. (EMU), Mr. Aaron Miller (Galois Inc.) |  |  | BALLROOM |
| 1520 | 1600 | Break & Networking Opportunity |  |  |  |
|  |  | BALLROOM/FOYER | KITTY HAWK |  |  |
| 1600 | 1800 | SaTC Exhibition & Poster Session I | Secure Edge Working Group Meeting |  |  |
| 1800 | 2000 | Dinner & Networking Opportunity |  |  |  |
| Day 3 – Thursday February 27, 2025 |  |  |  |  | Coffee Breaks: 1430 – 1450 & 1615 - 1630 |
| 0730 | 1700 | Registration |  |  | BALLROOM FOYER |
| 0730 | 0830 | Breakfast |  |  |  |
| 0800 | 0815 | Welcome and Overview of Day 3 Agenda |  |  | BALLROOM |
| 0900 | 0940 | Microelectronics Commons Updating Keynote<br>Dr. Matt Casto, CTO, MMEC<br>Ms. Stephanie Lin (Microelectronics Commons at NSTXL),<br>Dr. Wayne Churaman (DEVCOM Army Research Lab/DoD Microelectronics Commons),<br>Dr. Erin Gawron-Hyla (DEVCOM Army Research Lab/DoD Microelectronics Commons) |  |  | BALLROOM |
| 0900 | 0940 | Keynote Talk<br>Mr. Kirk Herath (Ohio Governor's Office)<br>Mr. Mike Duffey (Ohio Department of Higher Education) |  |  | BALLROOM |
| 0940 | 1000 | Break & Preparation for Panel Discussion |  |  |  |
| 1000 | 1100 | AF/Industry Trusted and Assured Microelectronics Panel |  |  | BALLROOM |
| 1100 | 1115 | Break & Preparation for Regular Sessions |  |  |  |
|  |  | Ballroom | Auditorium | Kitty Hawk |  |
| 1115 | 1235 | Additive Approaches to Electronic Manufacturing and Trust | AI Approaches for Detecting Anomalies in IoT Devices | Poster Session II |  |
| 1115 | 1235 | Cybersecurity in Aerospace: Protecting Critical Systems in a Connected World Workshop |  |  |  |
| 1240 | 1800 | NCAE – National Pathways to Success (NPS) Program Cybersecurity Workshop |  |  |  |
| 1200 | 1330 | Lunch Buffet Open |  |  | BALLROOM |
| 1240 | 1320 | Luncheon Keynote<br>Mr. Eric Parsley (Expedient Technology Solutions, LLC)<br>Mr. Don Boian (OCRI, Formerly NSA) |  |  | BALLROOM |
| 1330 | 1430 | Invited Speakers<br>Mr. Dominic Mohrhardt (AFLCMC)<br>Dr. Gene M. Alarcon (AFRL), Ms. Connie Matthews Reynolds (ReynCon Educational Services & Cybersecurity Training), Dr. Marc Abel (WSU) |  |  | BALLROOM |
| 1450 | 1635 | Empowering Innovation: Leveraging HBCU Expertise in Cybersecurity, Microelectronics, Semiconductors, and Beyond Panel |  |  | BALLROOM |
| 1635 | 1735 | Closing Remarks from SaTC 2025 Conference Chairs |  |  | BALLROOM |
| End of Day 3 |  |  |  |  |  |