IEEE Region 4
Serving IEEE Members in all or parts of Illinois, Indiana, Iowa, Michigan, Minnesota Nebraska, North and South Dakota, Ohio, and Wisconsin

Contents

Directors Column

As I begin my term as Region 4 Director, I would like to take this opportunity to thank outgoing Region Director Vickie Ozburn for her hard work in re-energizing Region 4 after the Covid Pandemic. I would also like to thank her for her diligence in preparing me to follow in her footsteps. During the past few months Vickie and I have spent a lot of time reviewing Region 4 operations and looking for ways to make the Region more efficient and responsive to the needs of the members.

The Region 4 ExCom has traditionally been a loose group of committees. This is not always the most efficient way to operate. Sometimes answers were delayed and good ideas had to fight their way to the top for review. To speed up communications and vet ideas more efficiently, the ExCom is being broken into six groups: Region Management, Section Support, Region Support, Professional Activities, Outreach, and member Communications. Questions and comments will still start in the appropriate Region Committee, but the Group chair will have the authority to manage the group and ensure answers are obtained on a timelier basis and common problems are worked out. We do not want either answers or good ideas to get lost in volume.

Though membership is trending up after the stagnation of the pandemic, we need to make a concerted effort to increase our membership. The best way to do this is by interesting and inclusive programs which will attract new members and retain the members we already have. The list of virtual meetings which is distributed weekly is done with the purpose of including members who might not be able to attend an in-person meeting by virtue of distance or timing. This is a great way to explore the offerings of the various societies. One benefit that came from the pandemic is the expansion of virtual offerings. For those members who do not live close to meetings and presentations, this is a great way to stay involved. Even for those who are close, work or other responsibilities might interfere with attending the in-person meetings. If your society does not have a chapter in your area, there may be critical mass to start a chapter and create even more activity.

Region 4 pioneered Virtual Senior Member Reference panels during the pandemic. This is being continued as a service to those who don't live close to chapter meetings, don't belong to a society, or have commitments which preclude finding references.

Region 4 is implementing some new programs designed to create interest in both the Academic and Industry Communities. Region 4 has had an active Industry Activities Committee for some time now. The Committee is being expanded to address the emerging Quantum and Artificial Intelligence areas and reinforced IEEE's Commitment to Sustainability. In the coming months we hope to strengthen our ties to local industry by adding an ambassador program. A new Region 4 Committee is being formed, Academic Engagement Committee, to engage researchers active at Region 4 Universities and to catalog the work being done locally. The purpose of this committee is not to start student branches, although they may be involved if they are

interested, but to support the academic work of the academics in the Region. Following the lead of the Department of Defense, many government agencies, private industry, and foundations are now requiring responses to bid requests and grant proposals have representation by both Industry and Academia in order to be considered. The last part of this new endeavor is a Relationship Management committee which is charged with seeking out funding opportunities for bid fulfillment and grants. Working as a team, Industry, Academia, and Relationship groups will seek to bring additional funding to the region and make IEEE the go to partner for winning bids and grant proposals.

Another area where all of IEEE, not just Region 4, is focusing attention is that of Students and Young Professionals. Serving on an IEEE Committee or in Committee leadership is an excellent way for Students and Young Professionals to gain valuable experience in being a productive employee in a way that does not impact future performance evaluations or compensation. IEEE is a safe space to learn the things that normal course work does not cover. Things like planning, budgeting, working with diverse personalities can be learned in a safe space. IEEE is the place to prepare leaders of industry and academia without repercussions. Committee chairs have been tasked with recruiting Young Professionals or graduating seniors to participate in committee leadership. IEEE can be considered a “management training” program to take Young Professionals and Students from the halls of academia to the offices of industry.

These are more ambitious goals and Region 4 will need more committee chairs, support/vice chairs and committee members to accomplish them. Members who are interested in becoming part of the management team, should complete the interest form on the Region 4 website.

More initiatives will be rolled out in the coming months and the support of all members is appreciated.

Thank you in advance for your support.

Connie Kelly, ckelly@core.com

Editors Corner

In this issue:

Presenting the first 2025 Q1 and beginning of the year edition! Thank you to all contributors and keep them coming!

Among some of the technical content rich and detailed-oriented highlights are the articles by AI for Health Equity by Vijay Viradia; Rethink Risk by Shamila Chandariah (note these are two have been regularly contributing in many past issues to the R4 newsletter as well). We hope that will inspire more budding tech authors to come forward.

Hearty congratulations are due to all the recently R4 awardees. Time and bandwidth permitting – we will try to feature them in future editions of the newsletter, asking them to describe their work and share a little bit about themselves.

And don't forget to check out the, our very own Region 4 sponsored EIT 2025 conference! New to the newsletter is the announcement for the annual Cedar Rapids Professional Development Conference, aka ProCon 2025.

In January 2025, we had a joint meeting with Region 6 – you will find a brief report by our past R4 Director on that event.

A renewed call for volunteers appears as well as IEEE nominations.

We also welcome Aurenice Oliveira as our new R4 WiE Chair.

Previous editions in this series may be found on the Region 4 website. Click on the "Newsletter" button in the top left column. Comments, newsletter submissions, articles of interest and suggestions may be sent via email to the editor: sharan.kalwani@ieee.org

Microsoft Word format is preferred but we can work with ODT as well. Where possible use the Arial font in point size of 10 and single spacing. Images can be in either *JPEG, GIF, PNG or similar formats.*

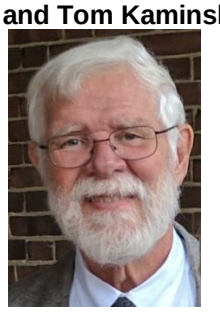
We try to complete the newsletter layout a week before publication, to allow time for review and corrections. If you have an article or notice, please submit it as early as possible. We publish once every quarter.

The newsletter relies on the contributions of our members and officers, so please do not be shy. If you have something that should be shared with the rest of the region, we want to give you that opportunity. The next deadline will be around the end April 2025 (well after Tax Day, good way to relieve some of the stress with a little creative and news sharing content).

Sharan Kalwani,
Editor, Region 4 Newsletter and Enthusiastic IEEE volunteer
Chair, IEEE Southeastern Michigan Section (2022-2025)

Medium Section Report

Medium Sections News, Dec 2024
By Co-Chairs Hamid Vakilzadian and Tom Kaminski



The medium sections of Region 4 are Calumet, Madison, Nebraska, Northeastern Wisconsin, and West Michigan, with a membership of 500. These sections are very active in serving their local membership and attending Area and Region Committee Meetings to implement new strategies and activities to better serve their members. The following is brief information on the activities of the medium sections, mainly from the fourth quarter of 2024.

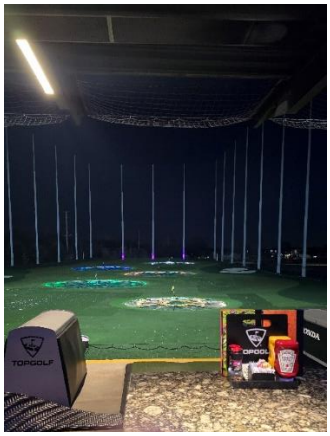
Summary of 2024 Events of Medium Sections

Section	Technical	Administrative	Other (Social, Humanitarian, Professional)
Calumet	**5**	**N/A**	**3**
Madison	**6**	**13**	**3**
Nebraska	**6**	**13**	**6**
NE Wisconsin	**8**	**4**	**3**
Western Michigan	**8**	**5**	**2**

IEEE Calumet Section
Chair – Greg Whelan and Vice-Chairman David Jenson

Event #1: Top Golf Social Outing
Date: December 8, 2024
Number of attendees: 22

The Calumet Section on a yearly basis has a social outing in December to celebrate the holidays open to members and their families and friends. As with all of our meetings, we do this jointly with the Calumet Chapter of the ISPE. This year we went to Top Golf in Naperville. This was our third year at Top Golf and each year we have more people attending. In 2025, Top Golf is opening a new facility in Tinley Park, which is closer to us, and hopefully, we will see an increase in attendance again. This always has good reviews and always proves to be a fun time for everyone.



Event #2: Robotics and Valparaiso University Mechatronics Program.
Date: November 7, 2025
Number of Attendees: 48

The Calumet Section has an annual meeting in November with the Valparaiso University Student Section. It is held jointly with the Calumet Chapter of the ISPE. This year we had the Merrillville High School Robotics Team attend the meeting and demo their robot and explain the Robotics Program they are part of. Also in attendance was representation from the Valparaiso University Robotics Football Team. These two demos and explanations were very fun to watch. They were followed by a presentation about the Valparaiso University Mechatronics Program. This presentation was a great partner to the robotics teams demos as it showed the students where the robotics can lead them.

Event #3: PNW Robotics & Power Laboratory Tour
Date: January 29, 2024
Number of Attendees: 27

Re-connecting with the Purdue NW student chapter an annual joint meeting was initiated. A complete tour of the robotics & power laboratories was completed on Jan. 29th 2024. The capabilities and options available at each lab were reviewed. In addition, several senior design presentations were given on their respective research topics.

Event #4: Power Equipment Fundamentals
Date: April 19th, 2024
Number of Attendees: 30

This was a joint event between the PNW student chapter, the Valparaiso University student chapter, and the Calumet section. We gathered at the NISPCO Service Center in Valparaiso, IN, to introduce the students to the theory and operation of various devices utilized on the power grid.

A synopsis of the devices and theory covered are as follows:

SCADA - a presentation by a member of the Communication & control team related to the operation of SCADA

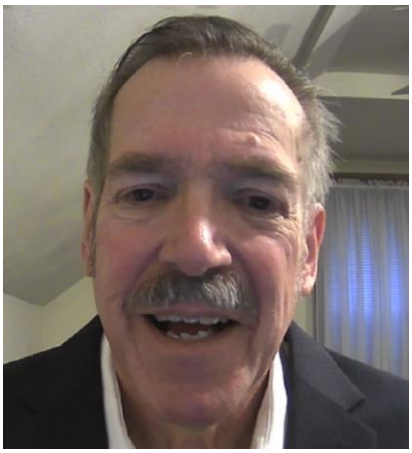
Mobile Substation – fundamental elements, including protection and control, for a full distribution substation mounted on a trailer.

Transformer – Components and function of a power transformer, focusing on the devices ensuring operation.

DA Viper – controllable vacuum reclosing device with a corresponding relay that is normally pole-mounted out in the field. The purpose is for grid reliability in the case of a fault detected downstream of the device, to function as a smart interrupting device that can further be controlled, locally or remotely.

Protective Relay Operation & Purpose – A member from System Protection along with the colleague Protection & Control group who works with this devices presented the purpose, function, and theory behind the protective relay. The focus here was primarily on the relay as an Intelligent Electronic Device.

IEEE Madison Section



Mike Stemper, Madison Section Chair

AI Events

In 2024, we held two events that featured AI topics. The first event, “Building and using Small Language Models,” was co-hosted by the IEEE CN and the MadAI Meetup Group. We look forward to having other meetings jointly with the MadAI Meetup Group.

On November 8, IEEE-MSN hosted IEEE Distinguished Lecturer Karen Haigh, who spoke on "Cognitive Electronic Warfare". Despite having to vie for parking with the throngs going to a UW volleyball match, 18 members and guests attended, probably due to the novel nature of the topic.

Student Raspberry Pi Pico Workshop

To forge better relationships with Engineering Students at the University of Wisconsin, the Madison IEEE Section and the University of Wisconsin IEEE Student Branch co-hosted two Workshops on successive days on the use of the Raspberry Pi Pico for engineering projects. Students were asked to bring their own laptops to load the software development tools for Micro Python and Arduino Development Tools. Students who attended were provided with Raspberry Pi Picos with a short color-changing LED string and a USB cable. If they were an IEEE member, or joined IEEE, they were allowed to take the devices home. About 40 students attended the workshop.

NWS Visit Report

Visit to National Weather Service (NWS) Lincoln, Illinois

On October 29, 2024, several members of the IEEE Central Illinois Section visited the National Weather Service (NWS) office in Lincoln, Illinois. This event was organized by the Section Chair Brady Mayes and Technical Committee Chair Dinup Sukumaran.

The National Weather Service (NWS) office in Lincoln, Illinois, is responsible for providing weather forecasts and warnings for a large portion of central and eastern Illinois. This includes major cities like Bloomington-Normal, Champaign-Urbana, Decatur, Springfield, and Peoria. This office in Lincoln is one of the 122 local offices in United States.

This event provided a unique opportunity for IEEE members and guests to gain firsthand insights into the operations of a crucial government agency responsible for weather forecasting, warnings, and climate monitoring. The one-hour visit began with a warm welcome from the NWS staff followed by an insightful half-hour presentation by an NWS expert. The presentation covered a range of topics, including

- A comprehensive overview of the NWS's mission, responsibilities, and the critical role it plays in public safety.
- A deep dive into the state-of-the-art technology like the doppler radar system they use to track storms and precipitation, satellite imagery to monitor large scale weather patterns and computer models to predict future weather conditions.
- Range of services provided by NWS- Short-term and long-term weather forecasts for specific locations; timely warnings for severe weather events like tornadoes, thunderstorms, and floods; historical climate data and future climate projections and information on river levels and flood risks.
- Collaborative Efforts: The NWS works closely with various agencies and organizations to ensure effective communication and coordination during severe weather events.

Following the presentation, attendees embarked on a guided tour of the NWS facility where we got to see the monitoring station, computer aided modeling tools, local Doppler Radar and weather balloon launch station.

The IEEE Central Illinois Section's visit to the NWS office was a successful endeavor. The event provided a valuable learning experience for all attendees, fostering a deeper understanding of the complex work involved in weather forecasting and emergency response. The IEEE Central Illinois Section is grateful to NWS for hosting this informative and inspiring event.

Contributed by
Dinup Sukumaran
Technical Committee Chair, SSCS Section Chapter Chair
Central Illinois Section of the IEEE, Region 4

Attendees in front of NWS Lincoln, IL

Local Doppler Radar

Rethinking Risk

Rethinking Risk : The Impact of Climate Change on Financial Models in Insurance and Banking

Author: Sharmila Devi Chandariah, Senior Technical Lead in Financial Services, SMIEEE, Policy Administration System & GenAI Expert

Introduction:

Climate change has transitioned from a theoretical concern to a pressing reality, altering financial services landscape. The increasing frequency and severity of climate-related disasters have revealed significant vulnerabilities in traditional financial models, compelling insurers and bankers to confront escalating risks. This evolving landscape necessitates not only adaptation but also innovative approaches within these sectors. Here we explore how the insurance and banking industries are responding to climate risks and the strategies that are fostering financial ecosystem.

The Evolving Risk Landscape:

To understand the implications of climate change, it is crucial to recognize the diverse risks it introduces. Physical risks encompass natural disasters such as hurricanes, floods, wildfires, and rising sea levels, which endanger assets worldwide. For instance, 2023 saw over $100 billion in insured losses due to natural disasters, highlighting the increasing unpredictability of environmental changes. Transition risks arise as economies shift towards green energy; industries reliant on fossil fuels face declining valuations. Additionally, regulatory measures like carbon taxes and net-zero commitments further intensify these risks. Also, liability risks emerge for companies cascading financial repercussions for insurers and lenders.

Impacts on the Insurance Industry:

The insurance sector is at forefront managing the financial uncertainties brought about by climate change. Traditional actuarial models often struggle to account for the non-linear impacts of climate change; thus, insurers are increasingly turning to advanced climate simulations and geospatial analytics to enhance their catastrophe modeling precision. Collaborations with firms such as RMS and AIR Worldwide exemplify this shift towards more accurate risk assessment. Moreover, parametric insurance has emerged as an innovative solution that triggers payouts based on predefined conditions—such as specific rainfall levels or wind speeds—allowing for quicker claims resolution and addressing gaps in conventional models. To cope with rising claims, insurers are adjusting premiums and revising coverage in high-risk areas, which poses affordability challenges for policyholders. Additionally, insurers are proactively funding initiatives aimed at risk mitigation, such as wildfire prevention programs, and incentivizing policyholders to adopt climate-resilient building practices.

Impacts on Banking and Financial Services

Banks face significant challenges in adapting their financial models to accommodate the realities of changing climate. Credit risk management is increasingly impacted by physical risks in vulnerable regions and transition risks that threaten the stability of carbon-intensive industries. As a result, climate risk assessments have become integral to credit evaluations. The rise of green financing and sustainable investments reflects a broader shift towards sustainability within the banking sector. Banking Institutions are committed billions to sustainable financing initiatives by 2030, signaling a strong move towards environmentally responsible investment practices. Furthermore, regulatory bodies now mandate climate stress tests for banks, enabling them to model potential losses under various climate scenarios and devise appropriate mitigation strategies. Increased regulatory supervision has also become a hallmark of this transition; institutions such as the European Central Bank and the Federal Reserve require robust disclosures regarding climate risk, promoting transparency and accountability across the financial sector.

Emerging Innovations and Technologies

The integration of innovative technologies is reshaping how both insurance and banking sectors approach climate risk management. Artificial intelligence (AI) and machine learning tools provide granular insights into climate risks, enhancing predictive modeling capabilities. For example, insurers are utilizing AI to anticipate wildfire paths or flood impacts, refining their underwriting practices accordingly. Startups in sustainable InsurTech and FinTech are driving innovation in environmental, social, and governance (ESG) evaluation platforms that help institutions align their investments with sustainability goals.

Challenges in Addressing Climate Risk

Despite these advancements, there are several challenges that remains effectively addressing climate risk. Data limitations, insufficient historical data on extreme weather events hampers predictive accuracy. Varying regional regulations create further hurdles for global institutions to manage effectively. Affordability challenges emerge as higher premiums and loan costs place critical financial services out of reach for vulnerable populations. Furthermore, balancing short-term profitability with climate mitigation strategies demands a shift in organizational culture and operations.

Call to Action: Collaboration is Key

Addressing climate risks requires a collaborative effort among various stakeholders. Insurers and banks should work together to develop bundled products that address both financial and environmental risks effectively. Governments can offer incentives for green investments and resilience measures that support these initiatives. Technology leaders are called upon to innovate solutions that fill existing data gaps and enhance capabilities across the industry.

Conclusion

Navigating climate change effectively can be achieved by financial models within insurance and banking getting evolved significantly. Through the adoption of technology, promotion of innovation, and cultivation of cross-sector partnerships, these industries can pave the path to a more resilient and sustainable future.

Author Bio:

Sharmila Devi Chandariah is a Senior Technical Lead with over a decade of extensive experience in the fintech industry, particularly focusing on the banking and insurance sectors. As a Senior Member of IEEE, she has demonstrated exceptional leadership and technical expertise throughout her career. Her specialization includes developing various web applications and transforming Policy Administration Systems for the U.S. Property & Casualty Insurance. Leveraging her Guidewire Certified ACE credentials, Sharmila excels in delivering innovative solutions tailored to the unique needs of insurance clients, particularly through her expertise in Policy Administration. Sharmila's contributions to the field have been recognized with the Star Associate Award, awarded for her pivotal role in developing the Transient Schema for the Policy Migration tool. This solution significantly enhanced the speed and accuracy of data migration from legacy systems to new Policy Administration Systems. Driven by a passion for integrating advanced technologies into insurance applications, Sharmila actively applies Machine Learning, Deep Learning, and Natural Language Processing (NLP) to tackle current business challenges. Her work in Generative AI has led to the development of various innovative solutions, including Test to SQL generation, knowledge management, and Splunk integration, resulting in considerable cost savings for her clients. This showcases her ability to merge technical prowess with practical business applications. In addition to her technical roles, Sharmila has recently been invited to serve on the advisory board of a startup focused on leveraging technology to enhance insurance processes. In this capacity, she will provide strategic insights and guidance on product development and market positioning. As the Innovation Lead at her current organization, Sharmila reviews and provides feedback on innovative solutions proposed by her peers, ensuring they align with client needs and can be effectively implemented. Her commitment to excellence and innovation positions her as a key person in advancing technology within the fintech landscape.

R4 Awards: 2024

Announcing the 2024 IEEE Region 4 Award Recipients

The 2024 IEEE Region 4 award winners have been selected!

From left to right, M Butt, A Chin, J Walz, S Lasassmeh, J Trevathan, N Minuta, P Hamari

M. Majid Butt received the Outstanding Professional Award with citation, "In recognition of exemplary contributions to the field of wireless communications and networks"

Dr. Alvin Chin received the Outstanding Service Award with citation, "For outstanding leadership and initiative in forming new Local Groups and conference sponsorships to benefit members throughout the Region"

John Walz received the Industry Engagement Award with citation, "In recognition of sustained contributions to the IEC including new initiatives that created significant synergies between IEEE and Region 4 industries"

Suha Lasassmeh received the Women in Engineering Award with citation, "For advancing WIE goals through impactful service, mentorship, and advocacy, inspiring young women in engineering and promoting women in the profession"

Jonathan Trevathan, Ph.D. received the Young Professional Achievement Award with citation, "In recognition of creating an innovative streaming solution for IEEE events and initiating unique activities to engage young professionals in the community"

Nathnael Minuta received the Outstanding Student Award with citation, "In recognition of exemplary academic achievement, student leadership, and dedication to community service"

Dr. Puteri S. Megat Hamari received the Student Branch Counselor Award with citation, "For dedication, vision, and mentorship advancing both service to the community and IEEE's goals"

Organization awards were also selected.

The **Calumet Section** received the Outstanding Section Award for medium sized sections with citation, "For exemplary leadership and service to their members."

The **Cedar Rapids Section WIE Affinity Group** received the Outstanding Affinity Group Award with citation, "In recognition of social, professional, and technical events to further the professional development of their members"

The **Milwaukee Section EMC Chapter** received the Outstanding Chapter Award with citation, "For sustained leadership and contributions to the EMC Society bringing engagement and education throughout the Region"

The **Minnesota State University Student Branch** received the Outstanding Student Branch Award with citation, "For exceptional commitment to advancing technology through impactful events, student-led initiatives, and community outreach programs"

Membership Growth Awards were received by **Central Illinois** (large), **Nebraska** (medium), and **Iowa-Illinois** (small) Sections in recognition of exceeding 2024 membership growth goals.

Membership Retention Awards were selected. The awards go to **Central Iowa** (small), **Nebraska** (medium), and **Central Indiana** (large) Sections in recognition of attaining the highest membership retention in 2024.

Congratulations to all Individual and Organization award recipients!

The Region 4 Awards and Recognition program is designed to encourage, recognize, and reward excellence in promoting the interests of IEEE as reflected in the operations of the Region and its Operating Unit activities.

Each award has a unique mission and criteria—and offers the opportunity to honor distinguished colleagues. For more information see the Region 4 Awards and Recognition web site at:
https://r4.ieee.org/committees/awards/

Steve Kerchberger
Chair, Region 4 Awards and Recognition Committee

Strategic Plan 2025-2030

New R4 WiE Chair

Introduction as the New Chair for IEEE Region 4 Women in Engineering (WIE)
I am honored to introduce myself as the new Chair of IEEE Women in Engineering (WIE) for our region. Having been an active IEEE member since 2000, I have had the privilege of serving in various roles within the organization, and I am excited to continue contributing to IEEE's mission, particularly in advancing the role of women in the engineering profession.

My primary goal as Chair of WIE is to create and support initiatives that focus on the professional development of women in engineering. Through sharing experiences, fostering collaboration, and providing networking opportunities, I aim to bring women in our field closer together, creating an empowering environment for all.

A key focus will be helping women develop leadership skills and building a pipeline of future leaders in our industry. In addition, I will prioritize supporting and sustaining women leaders in all career stages. I strongly believe in enhancing leadership skills, expanding knowledge of the technology landscape, and helping women make meaningful connections that will further their careers.

As an advocate for the next generation of engineers, I am also deeply committed to supporting students. I believe in the importance of mentorship and providing opportunities for students to grow in their technical careers, as well as connecting them to the resources and networks they need to succeed. In recognition of my passion for mentoring and fostering student growth, I was recently honored with the IEEE MGA Outstanding Student Branch Counselor Award. This recognition inspires me to continue my work supporting students and young professionals as they embark on their engineering journeys.

I look forward to working with each of you as we move forward in this journey, and I encourage you to get involved, share your insights, and help us make WIE a source of support and inspiration for all women in engineering. Thank you for your continued dedication to advancing our profession. Together, we can create lasting change and foster an environment where we can all thrive.

Kind regards,
Aurenice Oliveira, PhD
Chair, IEEE Region 4 Women in Engineering (WIE)
IEEE Member since 2000

Contact Info:
oliveira@mtu.edu

Zero Trust & Cloud

Zero Trust in Multi-Cloud Environments: A Framework for Consistent Policy Enforcement

Author: Gaurav Shekhar
Sr. Group Application Manager / Enterprise Architect, USA.

Abstract
The proliferation of multi-cloud environments has introduced complexities in managing security policies and enforcing consistent protection against evolving cyber threats. Zero Trust Architecture (ZTA) has emerged as a crucial framework to address these challenges. This paper discusses the importance of ZTA in multi-cloud settings, outlining its benefits, advantages, and potential disadvantages. It explores how consistent policy enforcement can safeguard cloud environments from cyber threats and how Zero Trust principles can minimize attack surfaces. Furthermore, the study highlights ZTA's role in mitigating ransomware attacks and reducing vendor risks, ultimately presenting a robust approach for securing multi-cloud ecosystems.

In simple terms a zero-trust environment does not make any assumptions about the trustworthiness of users. Instead, it uses a "least privilege" approach in which users are only given the least privilege access that they need to do their job and no more. This approach can help organizations improve their cybersecurity posture by making it more difficult for attackers to access sensitive data. It also simplifies security management by eliminating the need to manage complex firewall rules.

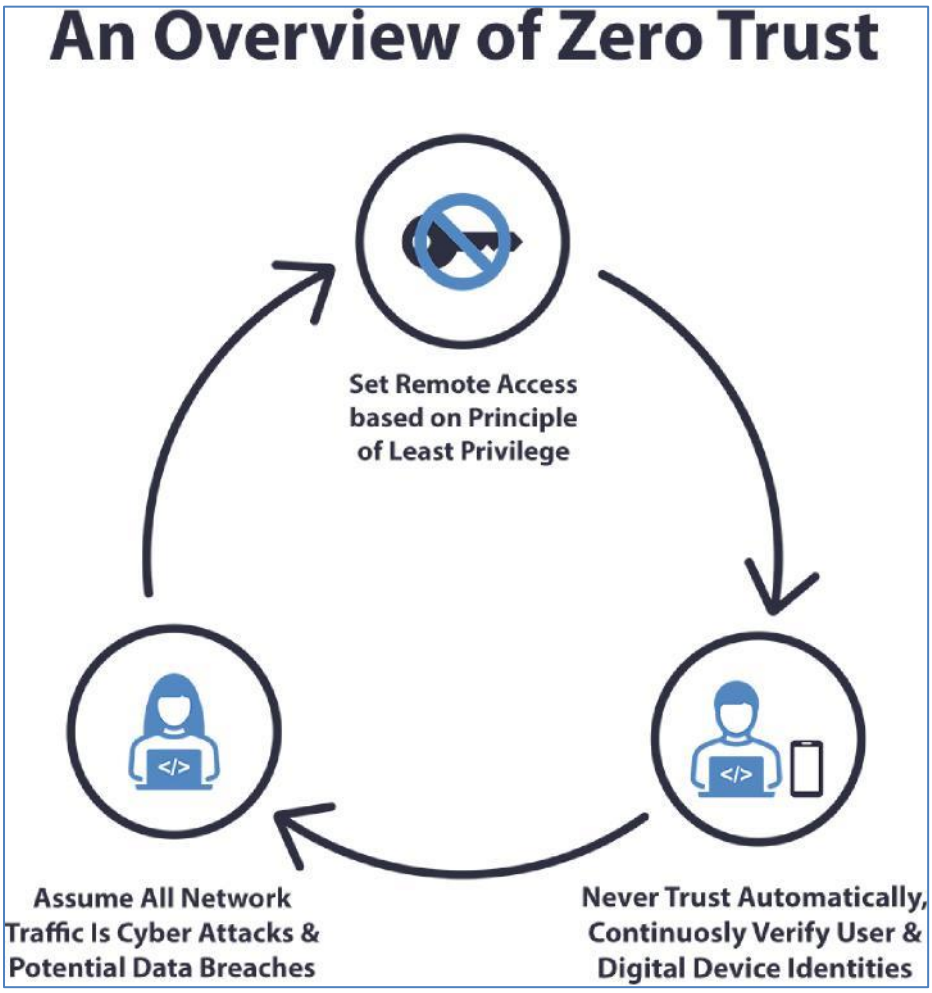
In contrast, in a traditional trust-based environment, organizations typically have perimeter-based security that relies on firewalls and other security controls to keep the bad guys out. Zero-trust environments are often considered more secure than traditional trust-based ones, but some tradeoffs must be considered. For example, zero-trust environments can require more effort to set up and manage and may not be compatible with all legacy applications.

Keywords: Zero Trust Security, Automation, Software Development, Security, Least Privilege, Multi Cloud Security, MicroSegmentation

1. Introduction

As organizations increasingly adopt multi-cloud strategies to leverage diverse capabilities and services, ensuring robust security across these platforms has become paramount. Traditional perimeter-based security models are inadequate in such dynamic environments, where data and workloads are distributed across multiple cloud service providers. Zero Trust Architecture (ZTA) offers a paradigm shift by enforcing a "never trust, always verify" approach, focusing on continuous validation of user and device identity, granular access controls, and comprehensive monitoring.

This paper investigates the application of ZTA in multi-cloud environments, emphasizing the importance of consistent policy enforcement. It examines how adopting ZTA can address vulnerabilities, reduce the attack surface, and enhance protection against sophisticated threats such as ransomware. The study also evaluates potential disadvantages and provides insights into mitigating vendor risks within a multi-cloud context.



2. Literature Survey - The Evolution of Enterprise Security: From Perimeter to Zero Trust

The concept of Zero Trust was first introduced by Forrester Research in 2010, emphasizing the need for granular access controls and identity verification. Studies have demonstrated that traditional security models struggle to adapt to multi-cloud architectures due to fragmented policies and inconsistent enforcement mechanisms.

2.1 Pre-2004: The Era of Perimeter-Based Security
For decades, enterprise security relied on the perimeter-based approach, modeled after a "castle and moat" philosophy. Organizations built strong external defenses—firewalls, intrusion detection systems, and access controls—to protect internal resources.

Within this model, anyone inside the perimeter (e.g., employees, devices on internal networks) was implicitly trusted, while external entities were viewed as untrusted. This approach worked well in environments where resources were centralized in on-premises data centers, and access was primarily through local office networks.

However, the early 21st century brought a seismic shift:
- **Cloud Adoption**: Enterprises began moving their infrastructure, applications, and data to cloud platforms.
- **Decentralization**: Workforces became more distributed, with employees working from remote locations and using personal devices.
- **Evolving Threats**: Cyberattacks grew more sophisticated, often exploiting implicit trust within internal networks.

These changes made traditional perimeter defenses inadequate, as threats could easily bypass them once inside.

2.2 2004: The Foundations of Zero Trust – Deperimeterization
In 2004, the Jericho Forum, an international consortium of security professionals, foresaw the limitations of perimeter-based defenses. They introduced the concept of **deperimeterization**, advocating for security models that no longer depended on a defined boundary.

Key principles of de-perimeterization included:
- **Data-Centric Security**: Protecting data itself, regardless of where it resides.
- **Encryption**: Ensuring data is encrypted in transit and at rest.
- **Identity-Based Controls**: Authenticating users and devices based on their identity rather than their location.

This forward-thinking approach recognized the growing mobility of users and data, laying the groundwork for the Zero Trust philosophy.

2.3 2010: The Birth of "Zero Trust"
John Kindervag, then a principal analyst at Forrester Research, coined the term **Zero Trust** in 2010. He formalized it as a response to the inherent weaknesses of perimeter-based security. Kindervag's core assertion was simple yet revolutionary:

"Trust is a vulnerability."

Rather than granting implicit trust to users or devices within the network, Zero Trust assumes that every interaction is potentially malicious. It enforces strict identity verification and access controls at every point, regardless of the user's location or device.

2.4 The Shift to Zero Trust: Why It Matters

The traditional perimeter-based approach became ineffective in addressing modern challenges:

1. **Remote Work**: Employees accessing corporate resources from home or public networks increased the attack surface.
2. **Cloud Computing**: Data and applications moved outside the physical network perimeter, making it harder to enforce consistent protections.
3. **BYOD (Bring Your Own Device)**: The proliferation of personal devices accessing enterprise networks introduced unmanaged endpoints.
4. **Sophisticated Threats**: Attackers increasingly exploited lateral movement within networks, abusing the implicit trust granted to "insiders."

Zero Trust addressed these gaps by adopting the principle of **least privilege access**:

- Users and devices are granted the minimum permissions necessary to perform their tasks.
- Access is verified continuously, using real-time context such as user identity, device health, location, and behavior.

2.5 Core Principles of Zero Trust

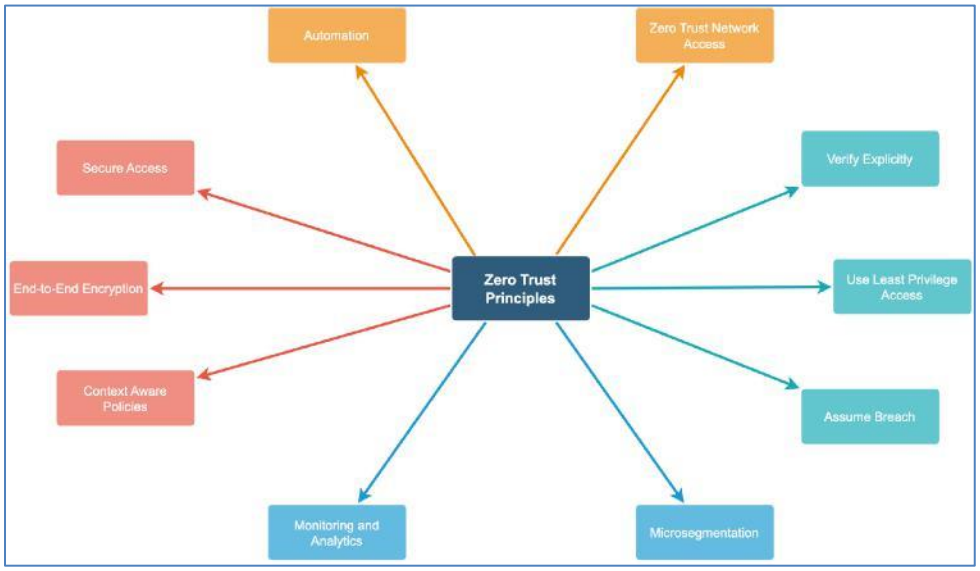
Zero Trust is built on several foundational pillars:

1. **Verify Explicitly**
   - Always authenticate and authorize access using all available data points, such as user identity, device health, location, and behavior.
   - Implement strong authentication mechanisms like Multi-Factor Authentication (MFA) and continuous verification to minimize risks.
2. **Use Least Privilege Access**
   - Grant users and devices the minimum level of access necessary to perform their tasks.
   - Regularly review and adjust permissions to ensure access aligns with business needs and security policies.
   - Enforce just-in-time (JIT) and just-enough-access (JEA) controls to reduce exposure.
3. **Assume Breach**
   - Design systems under the assumption that an attacker may already be inside the network.
   - Employ segmentation to minimize lateral movement, limiting the scope of potential damage.
   - Continuously monitor and log activity to detect and respond to anomalies in real time.
4. **Microsegmentation**
   - Divide the network into smaller, secure zones to isolate workloads and applications.
   - Implement granular access controls within these segments to reduce the attack surface.

5. **Continuous Monitoring and Analytics**
   - Utilize real-time data collection and analysis to detect potential threats and unauthorized access.
   - Leverage AI and machine learning for behavior analytics and anomaly detection.
6. **Context-Aware Policies**
   - Apply dynamic access policies based on contextual factors such as device posture, geolocation, and time of access.
   - Adapt security controls based on the current risk level of the interaction.
7. **End-to-End Encryption**
   - Ensure data is encrypted at rest and in transit, reducing exposure to interception or tampering.
   - Implement data integrity measures to prevent unauthorized modifications.
8. **Secure Access to All Resources**
   - Apply consistent security controls across all environments, including on-premises, cloud, and hybrid setups.
   - Protect all endpoints, applications, and APIs with a uniform security strategy.
9. **Automation and Orchestration**

- Use automated tools to enforce policies, respond to threats, and maintain compliance with minimal manual intervention.
- Integrate security workflows across diverse systems for seamless policy enforcement.

10. **Zero Trust Network Access (ZTNA)**
- Replace traditional VPNs with ZTNA solutions that verify each connection individually, ensuring secure access to specific applications without exposing the broader network.



2.6 Key Technologies Enabling Zero Trust

The implementation of Zero Trust often relies on:

Identity and Access Management (IAM): Centralized user authentication and authorization.

- **Multi-Factor Authentication (MFA)**: Adding layers of verification to prevent unauthorized access.
- **Microsegmentation**: Dividing networks into smaller zones to limit the spread of threats.
- **Endpoint Detection and Response (EDR)**: Monitoring and responding to suspicious activity on devices.
- **Cloud Access Security Brokers (CASBs)**: Ensuring secure access to cloud applications.

2.7 Zero Trust in Practice

Adopting Zero Trust requires cultural, procedural, and technological shifts:

- **Cultural Change**: Organizations must move away from legacy trust models and embrace the idea of continuous verification.
- **Continuous Monitoring**: Real-time analysis of user behavior and device health to detect anomalies.
- **Policy Enforcement**: Automated policies based on context, ensuring consistent security across on-premises and cloud environments.

2.6 Key Technologies Enabling Zero Trust

The implementation of Zero Trust often relies on:

Identity and Access Management (IAM): Centralized user authentication and authorization.

- **Multi-Factor Authentication (MFA)**: Adding layers of verification to prevent unauthorized access.
- **Microsegmentation**: Dividing networks into smaller zones to limit the spread of threats.
- **Endpoint Detection and Response (EDR)**: Monitoring and responding to suspicious activity on devices.
- **Cloud Access Security Brokers (CASBs)**: Ensuring secure access to cloud applications.

2.7 Zero Trust in Practice

Adopting Zero Trust requires cultural, procedural, and technological shifts:

- **Cultural Change**: Organizations must move away from legacy trust models and embrace the idea of continuous verification.
- **Continuous Monitoring**: Real-time analysis of user behavior and device health to detect anomalies.
- **Policy Enforcement**: Automated policies based on context, ensuring consistent security across on-premises and cloud environments.

2.8 The Future of Zero Trust

As organizations increasingly adopt hybrid work models and multi-cloud strategies, Zero Trust continues to evolve. Emerging technologies like AI and machine learning are enhancing the ability to detect threats and enforce policies dynamically.

By shifting the focus from "trusted" networks to context-aware access and continuous validation, Zero Trust represents the modern standard for enterprise security.

2.9 Key Research Contributions:

1. **Sharma et al. (2021):** Explored ZTA's effectiveness in mitigating insider threats, showcasing its ability to limit unauthorized access and reduce the impact of malicious actions within organizations.
2. **Lee et al. (2022):** Investigated ZTA's application in securing distributed workloads, emphasizing micro-segmentation and continuous monitoring to counteract lateral movement within cloud environments.
3. **NIST SP 800-207 (2020):** Provided foundational guidance on implementing ZTA, outlining principles like least privilege and identity-based access controls.

2.10 Industry Practices:

- **Microsoft Azure (2023):** Highlighted ZTA's application in multi-cloud environments, offering insights into tools and services designed for consistent policy enforcement.
- **Google Cloud and AWS:** Documented their respective ZTA models, emphasizing interoperability and vendor-agnostic frameworks for unified security.

Despite these advancements, challenges persist in implementing ZTA across multi-cloud environments. Fragmented security policies and lack of standardization remain critical barriers, necessitating a structured and comprehensive framework.

3. Methodology

The proposed framework integrates Zero Trust principles with policy enforcement mechanisms to secure multi-cloud environments. The methodology comprises six core components:

3.1 Identity-Centric Access Controls

Identity is the cornerstone of ZTA. Authentication and authorization are enforced through:

- **Multi-Factor Authentication (MFA):** Ensuring users verify their identity through multiple channels.
- **Identity as a Service (IDaaS):** Centralized identity management tools like Azure AD and Okta.

Example Code: Configuring MFA in Azure AD:

```
Connect-AzureAD
Set-MsolUser -UserPrincipalName "user@example.com"
-StrongAuthenticationRequirements @({"RelyingParty":"*", "State":
"Enabled", "Method":"OneWaySMS"})
```

3.2 Dynamic Policy Enforcement

Dynamic policies are enforced using centralized policy engines, incorporating:

- **Risk-Based Access Control (RBAC):** Adjusting access based on real-time threat analysis.
- **Tools:** Azure Policy, AWS Organizations, and Terraform.

Example Policy Definition (Terraform):

```
resource "azurerm_policy_definition" "example" {
  name         = "deny-public-storage"
  display_name = "Deny Public Storage Accounts"
  policy_type  = "BuiltIn"
  mode         = "Indexed"
  policy_rule = jsonencode({
    "if": {
      "field": "Microsoft.Storage/storageAccounts/publicNetworkAccess",
      "equals": "Enabled"
    },
    "then": {
      "effect": "Deny"
    }
  })
}
```

3.3 Micro-Segmentation

Breaking down the network into smaller, isolated segments limits lateral movement.

Tools:

- VMware NSX for micro-segmentation.
- AWS Security Groups for controlling inbound and outbound traffic.

Example: Configuring security groups in AWS:

```
aws ec2 create-security-group --group-name "microsegment"
--description "Micro-segment group"
aws ec2 authorize-security-group-ingress --group-name "microsegment"
--protocol tcp --port 22 --cidr 203.0.113.0/24
```

3.4 Continuous Monitoring

Continuous monitoring ensures prompt detection of anomalies using:

- **Security Information and Event Management (SIEM):** Tools like Splunk and Azure Sentinel.
- **Behavioral Analytics:** Leveraging AI/ML to identify deviations.

Example: Integrating Azure Sentinel with continuous monitoring:

```
Connect-AzAccount
Set-AzSentinel -WorkspaceName "SecurityWorkspace"
-ResourceGroupName "ResourceGroup"
```

3.5 Ransomware Mitigation Techniques

Mitigation strategies include:

- **Immutable Backups:** Preventing backup tampering.
- **Encryption:** Ensuring sensitive data is unreadable without keys.
- **Incident Response:** Automated responses to ransomware detections.

3.6 Vendor Risk Management

Third-party risks are minimized through:

- **Audits:** Regularly evaluating vendor compliance.
- **Contractual Requirements:** Mandating adherence to ZTA principles.
- **Continuous Assessment:** Monitoring vendors for emerging risks.

4. Results and Discussion

4.1 Advantages of ZTA in Multi-Cloud Environments

1. **Improved Security Posture:** ZTA reduces risks by enforcing strict identity-based access.
2. **Minimized Attack Surface:** Micro-segmentation and least privilege principles limit entry points.
3. **Ransomware Resilience:** Immutable backups and encryption ensure data integrity.
4. **Vendor Risk Reduction:** Unified security policies mitigate third-party risks.

4.2 Challenges in Adopting ZTA

1. **Complexity:** Deploying ZTA across multi-cloud environments requires expertise.
2. **Performance Overheads:** Continuous monitoring impacts system performance.
3. **Cost Implications:** Investments in tools and expertise are significant.

Case Study: Implementation of ZTA in a healthcare organization:

- **Challenge:** Fragmented security policies across AWS and Azure.
- **Solution:** Centralized policy engine and micro-segmentation.
- **Outcome:** 40% reduction in unauthorized access incidents.

5. Conclusion

The adoption of multi-cloud environments has fundamentally transformed how organizations manage and secure their IT infrastructure. Traditional perimeter-based security models are no longer effective in addressing the complexities of distributed architectures, dynamic workloads, and an increasingly sophisticated threat landscape.

In response to these challenges, the Zero Trust framework has emerged as a robust security paradigm, emphasizing continuous verification, least privilege access, and the principle of "never trust, always verify."

Implementing Zero Trust in multi-cloud environments requires a cohesive strategy that ensures consistent policy enforcement across diverse platforms and services. Organizations must leverage identity and access management (IAM), microsegmentation, and real-time monitoring to maintain granular control over user and device interactions. Additionally, adopting a unified security policy framework allows for streamlined governance and compliance, even in heterogeneous cloud ecosystems.

While the transition to Zero Trust demands significant cultural, technical, and operational shifts, the benefits far outweigh the challenges. By embedding security into every layer of the infrastructure and enforcing contextual, identity-driven access policies, organizations can mitigate risks and build resilience against evolving cyber threats.

In conclusion, Zero Trust is not merely a security strategy but a foundational framework for securing multi-cloud environments. Its principles of continuous verification and adaptive security are essential for navigating the complexities of modern enterprise IT, ensuring that organizations can achieve their goals without compromising on security. The future of multi-cloud security lies in embracing Zero Trust as a strategic enabler for innovation and business continuity.

5. References

1. Forrester Research. (2010). "The Zero Trust Model of Information Security."
2. Sharma, P., & Gupta, R. (2021). "Zero Trust in Cloud Computing: Mitigating Insider Threats." Journal of Cloud Security, 14(3), 45-56.
3. Lee, J., & Park, S. (2022). "Securing Distributed Workloads with Zero Trust." International Journal of Cybersecurity, 9(1), 78-90.
4. National Institute of Standards and Technology (NIST). (2020). "Zero Trust Architecture." SP 800-207.
5. Microsoft Azure. (2023). "Zero Trust in Multi-Cloud Environments." White Paper.
6. Google Cloud. (2022). "Adopting Zero Trust for Multi-Cloud Strategies."
7. Amazon Web Services (AWS). (2022). "Implementing Zero Trust in Cloud-Native Applications."

Author Bio:

Gaurav Shekhar is working as Vice President - Technology in the 5th largest bank in USA. With over a 18+ years in the software realm, he has honed a passion for melding the art of Managing/Architecting and coding with the precision of cloud technologies, data science, and machine learning. He is not just an Architect or Engineer; I'm a strategist who bridges the gap between complex technical processes and tangible business outcomes.

Throughout his journey, he has steered multifaceted projects from ideation to fruition, consistently exceeding both timelines and expectations. His penchant for innovation is evident in the architectures envisioned and the culture of standardization and automation he has championed. He is skilled in directing technical projects from start to end, preparing and executing strategic plans and control structures for projects, and ensuring successful completion within time. He has been recognized for innovative solutions, architecture vision, and inner-sourcing open-source culture of standardization and automation. Navigating the entire lifecycle of software development, from requirement analysis to maintenance, is second nature to him. No industry is foreign, and no challenge is too daunting. His track record displays impeccable system architecture, design, and a relentless commitment to client satisfaction.

Volunteer Call

Thank you for being an IEEE member and a member of IEEE Region 4. As a Member of IEEE you automatically become a member of your local IEEE Section, this allows you to share technical, professional, and personal interest with others in the worldwide member community of IEEE.

Are you looking for a way to get more involved within your local IEEE Section or Region 4? **If so**, **We want you!** Do you want to help guide programs or project ideas or maybe take part in a micro volunteering activity? So you may ask what is micro volunteering.

Micro Volunteering: Making a Difference in a Matter of Minutes.
Micro-volunteering describes a volunteer, or team of volunteers, completing small tasks that make up a larger project. These short, infrequent volunteer opportunities are often called "microvolunteering," which allows people to volunteer for specific tasks that can be completed in a short window of time. We want to make volunteering for IEEE fun and easy.

One of the objectives for Region 4 is to recruit and provide leadership and volunteering opportunities to our members. In order to accomplish this, we will send in regular intervals a Form to seek Volunteering and Leadership interest for our members.

Please let us know and we'll be happy to help out and find a spot just for you. We request you to please fill out the following form to express your interest:
https://docs.google.com/forms/d/19k46v6NsE1TwwR4Bky4MgNvdIKRN46LJ9x2x3pOuioM

ProCon 2025

ProCon is back.

The Annual IEEE Cedar Rapids Professional Development Conference, ProCon 2025, is a one-day, two-track regional event for engineers and other professionals, to be held April 1, 2025, at the Kirkwood Convention Center. Annual IEEE Cedar Rapids Professional Development Conference, ProCon 2025 : vTools Events | vTools IEEE

Date: 01 Apr 2025
Time: 08:00 AM to 04:30 PM
Location: Cedar Rapids, IA

Speakers
Mary Ellen Randall - 2025 IEEE President-Elect
Tarek Lahdiri - Region 4 Director-Elect
Courtney Smock and Jackie Pelland - Slingshot25 Professional Training and Coaching

Time	Track 1	Track 2
8:00 - 8:30	Registration	
8:30-10:00	Keys to Successful Team Building Mary Ellen Randall	
10:00-10:15	Break	
10:15-11:45	Move With a Purpose! Mary Ellen Randall	Fundamentals of Project Management and the SAFe AGILE Process Tarek Lahdhiri
11:45-1:15	Luncheon	
1:15-2:45	Accountability - Putting yourself on the Hook Sling Shot 25	Fundamentals of Project Management and the SAFe AGILE Process - continued
2:45-3:00	Break	
3:00-4:30	You're Just Not That Big a Deal Sling Shot 25	

IEEE Nominations Call

Are you ready to make a significant impact in the world of technology? The IEEE is seeking dedicated professionals to step up and lead the way!

As the world's largest technical professional organization, IEEE relies on the commitment and expertise of its volunteer members to drive innovation and shape the future. We are excited to announce that nominations are now open for various leadership positions, including:

- 2027 IEEE President-Elect (who will serve as President in 2028)
- 2026 IEEE Secretary
- 2026 IEEE Treasurer
- 2026 IEEE Vice President, Educational Activities
- 2026 IEEE Vice President, Publication Services and Products
- 2026 IEEE Committee, Vice Chairs, and Members

This is your opportunity to contribute to the growth and direction of IEEE, collaborate with like-minded professionals, and help advance technology for the benefit of humanity.

We encourage all qualified candidates to nominate themselves or a deserving colleague. Please note that a strong track record of leadership and relevant accomplishments within and outside of IEEE can increase the likelihood of recommendation, especially for high-level roles.

To learn more about the positions, eligibility requirements, and nomination process, please visit our Guidelines for Nominating Candidates.

Don't miss this unique chance to make a lasting impact on the global professional community. Join us in our mission to advance technology for the benefit of humanity.

Submit your nominations today and help shape the future of IEEE!

If you have any questions about the application or nomination process, please contact: nominations@ieee.org or visit the IEEE Nominations page

R4+R6 Joint Meeting Report

Successful Region 4 & 6 Joint Meeting

Region 4 held its annual face-to-face meeting in San Francisco with Region 6 at the Embassy Suites San Francisco Waterfront hotel. There were 140 volunteers and 32 guests in attendance.

Guest speakers included 2025 IEEE President Kathleen Kramer, 2024 IEEE Past President Tom Coughlin, 2026 IEEE President-Elect Mary Ellen Randall, and IEEE USA President Tim Lee.

Other special guests included Region 2 Director-Elect Philip Gonski, Region 7 Director Tom Murad, Region 8 Director Mike Hinchey, MGA President Antonio Luque, and Region 1 Director Bala Prasanna.

Friday afternoon started the event with various training sessions covering vTools, OU Analytics, ConCur, and NextGen Banking. Antonio led a discussion on volunteer paths in MGA and the IEEE, while Howard and Sevada led a discussion on membership elevation. The day ended with an evening reception at the hotel.

Saturday started with a welcome from Region 4 Director Connie Kelly and Region 6 Director Joseph Wie.

Next up was presentations from Kathleen and Tim, followed by a Fireside Chat with all our invited guests.

We held both Regions Award Ceremonies (photo above) and hosted a HKN Professional Induction Ceremony. New inductees included Avery Lu, Gaurav Kishor Deshmukh, Jeffery Pawlan, Kenneth Lin, Michelle Thompson, Wendy Al-Kukdad, and Yiran Chen.

Saturday afternoon was filled with carousel breakouts on a variety of topics, wrapping up with an evening reception and group dinner.

The meeting wrapped up Sunday with each Region hosting a Region meeting and then joining for an update on Future Directions, attendee feedback and closing remarks. Fun was had by all!

EIT 2025

ANNOUNCEMENT and CALL FOR PAPERS
2025 IEEE INTERNATIONAL CONFERENCE on ELECTRO/INFORMATION TECHNOLOGY (EIT)
May 29-31, 2025
Valparaiso University
Valparaiso, IN 46383-6493 USA

http://www.eit-conference.org/eit2025

The 2025 IEEE International Conference on Electro/Information Technology (EIT) sponsored by IEEE Region 4 and hosted by Valparaiso University, is committed to advancing research and fostering innovation in the fields of electrical and computer engineering. Our mission is to provide a dynamic forum where academic researchers, industry professionals, and students discuss the latest developments, exchange ideas, and collaborate on emerging technologies. The conference aims to inspire innovation through rigorous presentations, enlightening workshops, and open dialog. Topics of interest include but are not limited to:

Robotics and Mechatronics	Wireless communications and Networking
Intelligent Systems and Multi-agent Systems	Ad Hoc and Sensor Networks
Control Systems and System Identification	Internet of Things
Reconfigurable and Embedded Systems	Artificial Intelligence and Machine Learning
Power Systems and Power Electronics	Cybersecurity
Solid State, Consumer and Automotive Electronics	Computer Vision
Electronic Design Automation	Signal/Image and Video Processing
Biomedical Applications, Telemedicine	Distributed Data Fusion and Mining
Biometrics and Bioinformatics	Cloud, Mobile, and Distributed Computing
Nanotechnology	Software Engineering & Middleware Architecture
Micro Electromechanical Systems	Entrepreneurial Minded Learning
Electric Vehicles	Engineering Education

Important dates:

- Notification of acceptance: March 28, 2025
- Early registration deadline: April 11, 2025
- Final manuscript (PDF) due: May 2, 2025

For more information, ideas for organizing/chairing sessions, industry participation, tutorials, professional activities sessions, please contact: Dr. Sami Khorbotly or Dr. Hossein Mousavinezhad.

Note: Typical papers will be 4-6 pages, IEEE journal 2-column format, papers more than 6 pages will be charged a fee.

AI for Health Equity

AI for Health Equity: A Practical Approach to Bridging Disparities *by Vijay Varadia*

Introduction

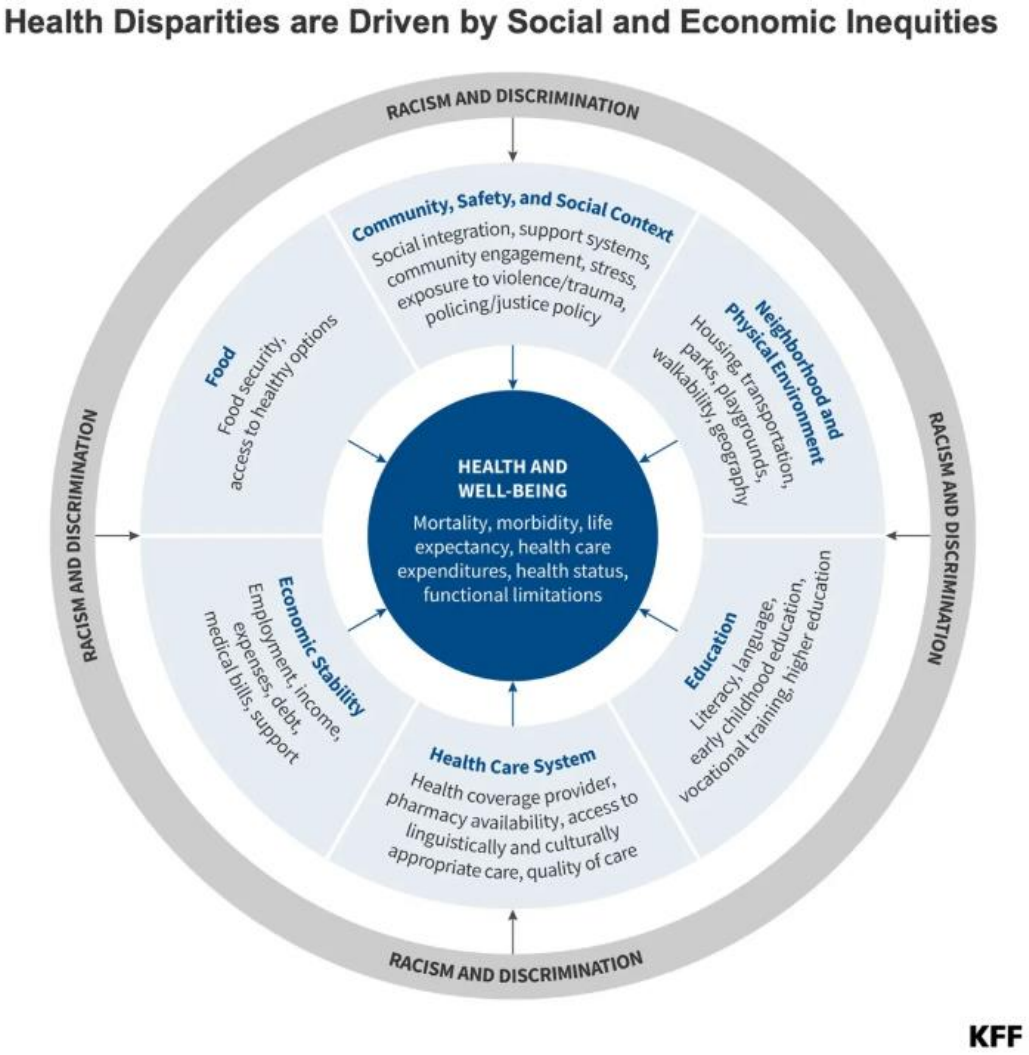
Health equity is the principle ***that everyone should have a fair and just opportunity to attain their highest level of health.*** However, disparities in healthcare access, quality, and outcomes persist due to socioeconomic, geographic, and systemic factors. Historically, these inequities have disproportionately affected marginalized communities, leading to poorer health outcomes and higher mortality rates.

Artificial Intelligence (AI) is emerging as a powerful tool to address these disparities by enabling data-driven decision-making, improving early disease detection, and personalizing patient care. From predictive analytics identifying high-risk populations to AI-driven telehealth solutions expanding access to underserved areas, the technology holds immense potential to bridge the healthcare gap. This blog explores how AI can be leveraged to promote health equity, highlighting real-world applications, challenges, and strategies for responsible deployment.

Understanding Health Disparities

Health disparities refer to the ***differences in health outcomes and access to healthcare services among various population groups***, often driven by social, economic, and environmental factors. These disparities manifest across multiple dimensions:

- **Socioeconomic Status:** Individuals from lower-income households experience higher rates of chronic illnesses and have reduced access to quality healthcare services. For instance, adults with disabilities are four times as likely to report having fair or poor health compared to those without disabilities (40.3% vs. 9.9%). NCBI
- **Geography:** Rural populations often face limited access to healthcare facilities, leading to poorer health outcomes. Between 2015 and 2019, rural populations had higher rates of poverty and premature death than their urban counterparts. Rural Health Information Hub
- **Race and Ethnicity:** Significant health disparities exist among different racial and ethnic groups. In 2017, 10.6% of African Americans were uninsured compared to 5.9% of non-Hispanic whites. Additionally, 89.4% of African Americans had health care coverage in 2017 compared with 93.7% of white Americans. Center for American Progress
- **Maternal Mortality:** In 2023, Black women in the U.S. experienced maternal mortality rates nearly 3.5 times higher than white women during childbirth. AP News



https://www.kff.org/racial-equity-and-health-policy/issue-brief/disparities-in-health-and-health-care-5-key-question-and-answers/

These disparities highlight the need for targeted interventions to promote health equity and ensure that all individuals have the opportunity to achieve optimal health outcomes.

Health Equity Framework by CDC

The road to health equity includes successful health equity strategies, data practices to support advancement of health equity, and policies to improve population health.

https://www.cdc.gov/health-equity/what-is/paving-the-road-to-health-equity.html

- **Programs:** Health equity ensures all communities have access to essential healthcare resources. Public health programs integrate targeted initiatives, including preventive care and outreach efforts, to reduce disparities and improve overall health outcomes.
- **Measurement:** Advancing health equity requires high-quality data and accurate interpretation tools. Standardized metrics help track disparities, social determinants, and inequities, ensuring effective resource allocation and informed policy decisions at the national level.
- **Policy:** Equitable health policies must address diverse community needs. AI-driven insights help policymakers implement adaptable, bias-free policies that reduce disparities and create inclusive healthcare solutions for vulnerable populations.
- **Infrastructure:** A strong public health infrastructure is vital for sustainable health equity. AI enhances resource distribution, early disease detection, and system responsiveness, ensuring equitable healthcare access for underserved communities.

How AI can help in achieving the goals outlined in the "Road to Health Equity Framework by CDC"

1. Programs: Enhancing Public Health Initiatives with AI

AI can improve health programs by ensuring that **all population groups** have equal access to healthcare resources.

- **AI-Powered Predictive Analytics:** Helps identify high-risk populations for early intervention in chronic diseases, maternal health, and infectious disease outbreaks.
    - *Example:* AI models used by the CDC predict flu outbreaks and vaccine distribution needs for vulnerable communities.
- **AI-Driven Mobile Health (mHealth) Solutions:** AI-based mobile applications help underserved communities access healthcare services, appointment scheduling, and medication reminders.
    - *Example:* AI-powered telehealth platforms like Babylon Health provide affordable virtual consultations for low-income groups.

2. Measurement: Accurate Data for Health Disparities Analysis

AI enhances the collection, interpretation, and application of **health equity metrics** by analyzing large datasets with precision.

- **AI for Social Determinants of Health (SDOH) Analysis:** AI can analyze electronic health records (EHRs), census data, and social factors to detect patterns in health disparities.
    - *Example:* The PLACES project by the CDC leverages AI to map chronic disease burden at a local level, helping policymakers take action.
- **Natural Language Processing (NLP) for Health Equity Research:** AI can process unstructured data from medical notes, surveys, and social media to gain insights into health inequities.
    - *Example:* AI-driven text analysis can identify disparities in healthcare access by analyzing patient feedback in real-time.

3. Policy: Creating AI-Driven Equitable Health Policies

AI can help **design and evaluate policies** that are more responsive to the needs of marginalized communities.

- **Bias-Free AI Models for Policy Recommendations:** AI algorithms trained on diverse and representative datasets ensure that policy recommendations do not favor one demographic over another.
    - *Example:* AI models analyzing Medicaid and Medicare data can help policymakers optimize healthcare funding for underserved populations.
- **AI-Powered Simulation Models:** AI can simulate the impact of policy decisions on different populations, ensuring that interventions do not widen disparities.
    - *Example:* AI-driven simulations can predict how changes in health insurance policies impact different socioeconomic groups before they are implemented.

4. Infrastructure: Strengthening Public Health Systems with AI

AI can modernize the public health infrastructure to make it **more responsive, efficient, and inclusive**.

- **AI-Enabled Public Health Surveillance:** AI automates real-time disease tracking and identifies potential outbreaks faster than traditional methods.
    - *Example:* AI models helped predict and track COVID-19 spread, enabling quicker public health responses.
- **Automating Administrative Workflows:** AI reduces the administrative burden in healthcare settings, allowing more focus on patient care.
    - *Example:* AI-powered chatbots and automation tools reduce paperwork for Medicaid/Medicare applications in low-income communities.
- **AI for Workforce Optimization:** AI-driven tools help forecast healthcare workforce needs, ensuring that rural and underserved areas receive the right distribution of doctors, nurses, and specialists.

Challenges and Ethical Considerations

While AI holds immense promises for advancing health equity, several challenges and ethical concerns must be addressed to ensure fair and responsible implementation.

1. Bias in Training Data and AI Algorithms

AI models are only as unbiased as the data they are trained on. If datasets predominantly reflect certain demographics while underrepresenting others, the resulting algorithms may reinforce existing health disparities.

- Example: A study published in *Science* found that an AI model used in U.S. hospitals was less likely to refer Black patients for advanced care compared to white patients with similar health conditions.

2. Ensuring Transparency and Accountability

Healthcare AI models often operate as "black boxes," making it difficult for providers and patients to understand how decisions are made.

- Solution: Implementing explainable AI (XAI) techniques can improve transparency, allowing clinicians and regulators to scrutinize decision-making processes.

3. Overcoming Trust Barriers in AI Adoption

Many marginalized communities have historical distrust of healthcare systems, which can extend to AI-driven healthcare solutions.

- Approach: Engaging communities through participatory AI design, culturally competent AI applications, and clear patient education can build trust and improve adoption.

Addressing these challenges is critical to ensuring that AI contributes to health equity rather than exacerbating existing disparities.

Conclusion

AI has the potential to revolutionize healthcare by addressing systemic health disparities and improving access to quality care. From early disease detection to telemedicine and population health analytics, AI-driven solutions can bridge critical gaps in healthcare delivery. However, ethical deployment, bias mitigation, and community engagement are essential to ensure AI benefits all populations equitably.

Healthcare professionals, researchers, and policymakers must work collaboratively to implement responsible AI solutions that promote health equity. By leveraging AI thoughtfully, we can create a more inclusive and just healthcare system for the future.

About Author

Vijay Viradia (PMP, SAFe, CSM)
Project Management, Healthcare & AI Specialist
Menomonee Falls, WI, USA

Mob: +1 (262) 290-3160

LinkedIn | Blog | Website | Peer Reviews | Speaker

Vijay is a distinguished Digital Healthcare Transformation Leader, known for his unique blend of Healthcare IT, Cloud, AI, Data Analytics and Project Management expertise in delivering Large-Scale Healthcare IT solutions, and business acumen. He worked with Fortune 500 companies in delivering healthcare solutions. Vijay led the team of Architects, Business Analysts, Developers, and Operations staff for the implementation of the healthcare system.

Vijay has a strong interest in,

- Leveraging cloud, AI/ML, and microservices to transform healthcare systems through Agile, Lean and AI powered Project Management.
- Revolutionize Patient Outcomes through Emerging Technologies.
- Health Equity, healthcare needs in rural areas, and enhancing access to healthcare for all individuals.
- Improving patient & provider experiences, quality of care, and healthcare operations.

Web & Social Sites

Region 4 Website
https://r4.ieee.org/

Each of the sites below may be accessed through the Website:

R4 Event Calendar
https://r4.ieee.org/events/month/

R4 Facebook Page
https://www.facebook.com/R4.IEEE/

R4 LinkedIn Page
https://www.linkedin.com/company/ieeer4/

R4 Twitter
https://twitter.com/IEEER4

R4 Instagram
https://www.instagram.com/ieeer4/

R4 YouTube Channel
https://www.youtube.com/@IEEER4

R4 Newsletter:
https://r4.ieee.org/our-newsletter/

R4 Committee Members:
https://r4.ieee.org/committees/

Extra