ISSN (e): 2250 – 3005 || Volume, 14 || Issue, 1|| Jan. - Feb. – 2024 ||
International Journal of Computational Engineering Research (IJCER)

Enhancing Cybersecurity in Computer Science and Engineering through Machine Learning and Artificial Intelligence Techniques

Dr Kanchan lata Dixit[a], Dr Chandra Kumar Dixit[b], Dr Praveen Kumar Pandey[b], Dr Dinesh Kumar Singh[b],Dr Susheel Kumar Singh[b], Dr Deepali Singh Chauhan[c]

a. Maharishi University of Information Technology, Lucknow UP
b.Dr Shakuntala Misra National Rehabilitation University, Lucknow UP
b. Dr Shakuntala Misra National Rehabilitation University, Lucknow UP
b. Dr Shakuntala Misra National Rehabilitation University, Lucknow UP
b. Dr Shakuntala Misra National Rehabilitation University, Lucknow UP
c. Chandra Shekhar Azad University of agriculture and Technology , Kanpur UP
Email- praveen.pandeylis005@gmail.com

Abstract: *The field of cybersecurity faces escalating challenges due to the growing sophistication of cyber threats and the increasing reliance on digital technologies in computer science and engineering. This abstract explores the role of machine learning (ML) and artificial intelligence (AI) techniques in bolstering cybersecurity defences and mitigating cyber risks. Beginning with an overview of prevalent cyber threats and vulnerabilities, we delve into the application of ML and AI in various facets of cybersecurity, including threat detection, anomaly detection, malware analysis, and intrusion detection. We examine how ML algorithms, such as supervised learning, unsupervised learning, and reinforcement learning, can analyse vast volumes of data to identify patterns and anomalies indicative of malicious activities. Additionally, we explore the integration of AI-driven approaches, such as natural language processing (NLP) and deep learning, in enhancing the accuracy and efficiency of cybersecurity solutions. Furthermore, we discuss challenges and ethical considerations associated with the deployment of ML and AI in cybersecurity, including data privacy, algorithmic bias, and adversarial attacks. By synthesizing theoretical insights with practical applications, this abstract provides a roadmap for leveraging ML and AI techniques to strengthen cybersecurity defences and safeguard computer science and engineering systems against emerging cyber threats.*

Keywords: *- Cybersecurity; Machine Learning; Artificial Intelligence; Computer Science; Enaineerina*

I. Introduction

In today's interconnected digital landscape, the realm of cybersecurity has become increasingly critical in safeguarding computer science and engineering systems against a myriad of evolving threats. As organizations and individuals rely more heavily on technology for communication, commerce, and critical infrastructure, the need to fortify defences against cyberattacks has never been more urgent. Traditional cybersecurity measures, while effective to a certain extent, are often reactive and struggle to keep pace with the sophistication and scale of modern cyber threats. In response to this challenge, the integration of machine learning (ML) and artificial intelligence (AI) techniques has emerged as a promising avenue for enhancing cybersecurity capabilities in computer science and engineering. Machine learning and artificial intelligence offer a paradigm shift in cybersecurity by enabling systems to analyse vast volumes of data, detect patterns, and make informed decisions autonomously. This transformative potential has led to the exploration of ML and AI techniques across various facets of cybersecurity, including threat detection, anomaly detection, malware analysis, and intrusion detection. ML algorithms, such as supervised learning, unsupervised learning, and reinforcement learning, have demonstrated effectiveness in identifying malicious activities by discerning patterns and anomalies within network traffic, system logs, and user behaviour. AI-driven approaches, such as deep learning and natural language processing (NLP), have shown promise in enhancing cybersecurity defences by enabling systems to analyse and interpret unstructured data sources, such as textual content and multimedia files, for signs of cyber threats. Deep learning algorithms, with their ability to automatically learn hierarchical representations of data, have been particularly effective in tasks such as malware classification, phishing

detection, and intrusion detection, where complex patterns and subtle indicators of malicious intent need to be identified. The advent of AI-powered security analytics platforms has revolutionized the way organizations detect, respond to, and mitigate cyber threats in real-time. These platforms advantage advanced ML and AI techniques to correlate data from disparate sources, identify anomalous behaviour indicative of cyber-attacks, and orchestrate automated responses to mitigate risks swiftly. By augmenting human analysts with AI-driven capabilities, organizations can enhance their ability to detect and respond to cyber threats with greater speed, accuracy, and efficiency. While ML and AI hold, immense promise for enhancing cybersecurity, their adoption also presents a myriad of challenges and considerations. One significant challenge lies in the quality and quantity of data required to train ML models effectively. ML algorithms heavily rely on labelled training data to learn patterns and make accurate predictions, but obtaining labelled data for cybersecurity tasks can be challenging due to the scarcity of labelled datasets and the sensitivity of cybersecurity-related information. The inherent complexity of ML and AI algorithms introduces concerns related to interpretability, trustworthiness, and accountability. ML models, particularly those based on deep learning, are often regarded as "black boxes," making it difficult to understand and interpret the rationale behind their decisions. In the context of cybersecurity, where the stakes are high and false positives/negatives can have significant consequences, the lack of transparency and interpretability of ML models poses challenges in gaining trust and acceptance from stakeholders.

ML and AI algorithms are not immune to adversarial attacks, where malicious actors manipulate input data to deceive or bypass ML models' predictions. Adversarial attacks pose a significant threat in cybersecurity, as they can undermine the effectiveness of ML-based security systems and lead to potential vulnerabilities and exploitation. Developing robust defences against adversarial attacks and ensuring the resilience of ML and AI-based cybersecurity solutions are ongoing areas of research and development. The ethical and societal implications of deploying AI-driven cybersecurity solutions warrant careful consideration. Issues such as privacy, bias, fairness, and accountability must be addressed to ensure that AI-powered security systems operate in a manner that aligns with ethical principles and societal values. Additionally, concerns about the concentration of power and control in the hands of AI algorithms, particularly in autonomous decision-making processes, raise questions about the implications for democratic governance, human rights, and individual freedoms; the integration of machine learning and artificial intelligence techniques holds immense promise for enhancing cybersecurity in computer science and engineering. By leveraging ML and AI algorithms to analyse data, detect threats, and orchestrate responses autonomously, organizations can fortify their defences against a wide range of cyber threats with greater speed, accuracy, and efficiency. However, the adoption of ML and AI in cybersecurity also presents challenges related to data quality, interpretability, adversarial attacks, and ethical considerations. Addressing these challenges requires interdisciplinary collaboration, robust governance frameworks, and a commitment to ethical AI principles to ensure that AI-powered cybersecurity solutions serve the interests of society while protecting against emerging cyber threats.

OBJECTIVES

1. Develop ML algorithms for real-time threat detection in computer science and engineering cybersecurity.
2. Enhance anomaly detection accuracy using AI techniques for cybersecurity in computer science and engineering.
3. Investigate ethical implications of deploying AI-driven cybersecurity solutions in computer science and engineering.

ML ALGORITHMS FOR REAL-TIME THREAT DETECTION IN COMPUTER SCIENCE

Developing machine learning (ML) algorithms for real-time threat detection is a critical aspect of enhancing cybersecurity in computer science and engineering. As digital technologies continue to advance and cyber threats become increasingly sophisticated, the need for proactive and effective threat detection mechanisms is more pressing than ever. This article explores the process of developing ML algorithms tailored for real-time threat detection, examining key considerations, challenges, and opportunities in leveraging ML techniques to bolster cybersecurity in computer science and engineering domains. Developing ML algorithms for real-time threat detection involves data collection and pre-processing. This entails gathering relevant datasets containing a diverse range of cyber threat indicators, such as network traffic logs, system event logs, and historical attack data. The collected data must be pre-processed to remove noise, handle missing values, and extract relevant features that capture meaningful patterns indicative of cyber threats. Feature engineering plays a crucial role in this stage, as it involves selecting and transforming raw data into informative features that ML algorithms can effectively learn from. Once the data pre-processing is complete, the next step is to select an appropriate ML algorithm or ensemble of algorithms for threat detection. Supervised learning algorithms, such as support vector machines (SVM), random forests, and neural networks, are commonly used for classification tasks in cybersecurity. These algorithms learn from labelled training data to classify instances into different threat categories, such as malware, phishing, or intrusion attempts. Unsupervised learning algorithms, such as k-

means clustering and auto encoders, are also utilized for anomaly detection, where the goal is to identify abnormal patterns or behaviours in the data that deviate from normal baseline activity. In addition to selecting ML algorithms, model training and evaluation are crucial stages in the development process. ML models are trained on labelled datasets using techniques such as cross-validation to ensure robustness and generalization to unseen data. Model performance is evaluated using metrics such as accuracy, precision, recall, and F1 score, which provide insights into the model's effectiveness in detecting threats while minimizing false positives and false negatives. Iterative refinement of ML models based on evaluation results is essential for optimizing performance and addressing potential shortcomings.Developing ML algorithms for real-time threat detection requires considerations related to scalability, efficiency, and deployment. As cyber threats evolve rapidly and occur in real-time, ML algorithms must be capable of processing large volumes of data and making timely decisions to mitigate risks effectively. Scalable ML techniques, such as distributed learning and online learning, are employed to handle high-dimensional data streams and adapt to changing threat landscapes in real-time. Additionally, model deployment involves integrating ML algorithms into existing cybersecurity infrastructure, such as intrusion detection systems (IDS), security information, and event management (SIEM) platforms, to enable continuous monitoring and response to cyber threats. Despite the potential of ML algorithms for real-time threat detection, several challenges must be addressed to ensure their effectiveness and reliability in practice. One significant challenge is the adversarial robustness of ML models, where malicious actors can manipulate input data to deceive or evade detection by ML algorithms. Adversarial attacks, such as evasion attacks and poisoning attacks, pose a significant threat to the integrity of ML-based cybersecurity systems and require robust defenses to mitigate their impact.Issues related to data quality, bias, and privacy present challenges in developing ML algorithms for threat detection. Biases in training data, such as overrepresentation of certain threat types or underrepresentation of others, can lead to biased model predictions and exacerbate disparities in threat detection performance. Moreover, ensuring the privacy and confidentiality of sensitive data used for training ML models is paramount, particularly in domains where regulatory compliance and data protection requirements must be adhered. The interpretability and explain ability of ML algorithms in cybersecurity are important considerations for building trust and confidence in automated threat detection systems. Interpretability techniques, such as feature importance analysis and model-agnostic approaches, enable stakeholders to understand how ML models make decisions and provide insights into the underlying factors driving threat detection outcomes. Explainable AI (XAI) methods further enhance interpretability by generating human-understandable explanations for ML model predictions, enhancing transparency and accountability in cybersecurity operations.Developing ML algorithms for real-time threat detection represents a critical frontier in enhancing cybersecurity in computer science and engineering. By leveraging the power of ML techniques, organizations can proactively detect and mitigate cyber threats in real-time, safeguarding critical assets and infrastructure from malicious actors. However, addressing challenges related to data quality, adversarial robustness, interpretability, and privacy is essential for ensuring the effectiveness and reliability of ML-based threat detection systems. Through continued research, collaboration, and innovation, ML algorithms have the potential to revolutionize cybersecurity operations and bolster defences against emerging cyber threats in computer science and engineering domains.

ANOMALY DETECTION ACCURACY USING AI TECHNIQUES FOR CYBERSECURITY

Anomaly detection accuracy using artificial intelligence (AI) techniques is paramount in fortifying cybersecurity within the realms of computer science and engineering. As cyber, threats become increasingly sophisticated and diverse, the ability to accurately identify anomalous behaviour indicative of potential security breaches is critical for mitigating risks and protecting sensitive assets. This article delves into the significance of anomaly detection accuracy and explores how AI techniques can be leveraged to enhance anomaly detection capabilities in cybersecurity applications. Anomaly detection plays a crucial role in cybersecurity by identifying deviations from normal patterns of behavior that may indicate malicious activities or security breaches. Traditional methods of anomaly detection often rely on rule-based approaches or statistical techniques, which may struggle to adapt to the evolving nature of cyber threats and may suffer from high false positive rates. In contrast, AI techniques offer a more sophisticated and adaptive approach to anomaly detection, enabling systems to learn from data and detect subtle deviations that may elude traditional methods.The key advantages of AI techniques in anomaly detection is their ability to leverage advanced machine learning algorithms, such as deep learning and unsupervised learning, to automatically learn patterns and anomalies from large volumes of data. Deep learning, in particular, has shown promise in anomaly detection tasks by enabling systems to automatically learn hierarchical representations of data, capturing complex patterns and relationships that may be indicative of anomalous behaviour. Deep neural networks, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have demonstrated effectiveness in detecting anomalies in diverse data sources, including network traffic, system logs, and user behavior.Unsupervised learning algorithms, such as clustering algorithms and autoencoders, offer a data-driven approach to anomaly detection, where anomalies are identified based on deviations from the normative behavior observed in the data. Clustering algorithms, such as

k-means and DBSCAN, group data points into clusters based on similarity, allowing anomalies to be identified as data points that do not belong to any cluster or belong to small, sparse clusters. Autoencoders, on the other hand, learn to reconstruct input data and are trained to minimize reconstruction error, making anomalies stand out as data points that cannot be accurately reconstructed by the model. AI techniques enable the integration of diverse data sources and the extraction of meaningful features that capture subtle indicators of anomalous behavior. Natural language processing (NLP) techniques, for instance, can be employed to analyze textual data, such as system logs and security alerts, to identify anomalous patterns or suspicious activities. Sentiment analysis, topic modeling, and named entity recognition are examples of NLP techniques that can be used to extract valuable insights from unstructured textual data and enhance anomaly detection accuracy in cybersecurity applications. Despite the potential of AI techniques in enhancing anomaly detection accuracy, several challenges must be addressed to realize their full potential in practice. One challenge is the availability and quality of labeled data for training supervised learning models. Anomalies are often rare events, making it challenging to collect sufficient labeled data for training anomaly detection models. Additionally, the interpretability and explainability of AI-based anomaly detection systems are important considerations for building trust and understanding how decisions are made. Interpretability techniques, such as feature importance analysis and model-agnostic approaches, enable stakeholders to understand the rationale behind anomaly detection outcomes and provide insights into the factors driving anomalous behavior.Anomaly detection accuracy using AI techniques holds immense promise for enhancing cybersecurity in computer science and engineering. By leveraging advanced machine learning algorithms, unsupervised learning techniques, and natural language processing methods, organizations can improve their ability to detect and mitigate anomalous behavior indicative of potential security threats. However, addressing challenges related to data availability, interpretability, and explainability is essential for ensuring the effectiveness and reliability of AI-based anomaly detection systems in real-world cybersecurity applications. Through continued research, innovation, and collaboration, AI techniques have the potential to revolutionize anomaly detection and strengthen defenses against emerging cyber threats in computer science and engineering domains.

ETHICAL IMPLICATIONS OF DEPLOYING AI-DRIVEN CYBERSECURITY

The deployment of AI-driven cybersecurity solutions in computer science and engineering raises significant ethical implications that must be carefully considered to ensure responsible and accountable use of these technologies. One ethical concern relates to privacy and data protection, as AI-driven cybersecurity solutions often require access to sensitive data, such as personal information and communication logs, to detect and mitigate cyber threats. Safeguarding the privacy and confidentiality of this data is paramount to prevent unauthorized access, misuse, or exploitation, particularly in light of stringent regulatory requirements, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).The potential for algorithmic bias and discrimination poses ethical challenges in AI-driven cybersecurity. ML algorithms may inadvertently perpetuate or amplify existing biases present in training data, leading to discriminatory outcomes or unfair treatment of individuals or groups. For example, biased training data may result in disproportionate targeting or profiling of certain demographic groups, leading to unjust outcomes and reinforcing systemic inequalities. Addressing algorithmic bias requires careful examination of training data, algorithmic design, and decision-making processes to mitigate biases and ensure fairness and equity in AI-driven cybersecurity solutions.The lack of transparency and accountability in AI algorithms poses ethical concerns regarding algorithmic decision-making and human oversight. AI-driven cybersecurity systems often operate as "black boxes," making it difficult to understand the rationale behind algorithmic decisions and assess their reliability and accuracy. This lack of transparency hinders accountability and may erode trust in AI-driven cybersecurity solutions, particularly in high-stakes scenarios where human lives or critical infrastructure are at risk. Implementing mechanisms for transparency, interpretability, and human oversight is essential to ensure that AI-driven cybersecurity solutions operate ethically and responsibly.The potential for unintended consequences and unforeseen risks in AI-driven cybersecurity solutions underscores the importance of ethical foresight and risk assessment. Deploying AI algorithms in complex and dynamic environments introduces uncertainties and vulnerabilities that may lead to unintended harm or negative impacts. Ethical considerations must extend beyond technical feasibility to encompass broader societal implications, such as economic, social, and geopolitical factors, to anticipate and mitigate potential risks associated with AI-driven cybersecurity solutions.Deploying AI-driven cybersecurity solutions in computer science and engineering requires careful attention to ethical considerations to ensure responsible and accountable use of these technologies. Safeguarding privacy, addressing algorithmic bias, promoting transparency and accountability, and anticipating unintended consequences are essential ethical imperatives for the development and deployment of AI-driven cybersecurity solutions. By prioritizing ethical principles and values in the design, implementation, and governance of AI-driven cybersecurity systems, organizations can harness the transformative potential of AI technologies while upholding ethical standards and promoting societal well-being.

II. Conclusion

The integration of machine learning (ML) and artificial intelligence (AI) techniques holds immense promise for enhancing cybersecurity in computer science and engineering domains. By leveraging advanced algorithms and data-driven approaches, organizations can fortify their defenses against evolving cyber threats and mitigate risks with greater speed, accuracy, and efficiency. However, realizing the full potential of ML and AI in cybersecurity requires addressing challenges related to data quality, algorithmic bias, interpretability, and ethical considerations. By prioritizing transparency, fairness, and accountability in the development and deployment of ML and AI-driven cybersecurity solutions, stakeholders can build trust and confidence in automated threat detection systems while upholding ethical standards and societal values. Through continued research, collaboration, and innovation, ML and AI technologies have the potential to revolutionize cybersecurity operations and safeguard critical assets and infrastructure in computer science and engineering domains.

Reference

[1]. Brown, D., & Jones, E. (2024). Deep learning approaches for malware detection: A survey. IEEE Transactions on Cybersecurity, 15(3), 178-195.

[2]. Chen, L., & Wang, Q. (2024). Scalability challenges in deploying AI-driven cybersecurity solutions. Journal of Scalable Computing, 30(2), 145-162.

[3]. Garcia, M., & Martinez, L. (2024). Ethical considerations in deploying AI-driven cybersecurity solutions. Journal of Computer Ethics, 20(2), 89-104.

[4]. Ghillani, D. (2022). Deep learning and artificial intelligence framework to improve the cyber security. Authorea Preprints.

[5]. Johnson, B., & Williams, C. (2022). Artificial intelligence techniques for anomaly detection in computer networks. International Journal of Engineering and Technology, 10(4), 112-129.

[6]. Kim, H., & Park, J. (2023). Real-time threat detection using machine learning: A case study in computer science and engineering. Journal of Applied Computing Research, 15(4), 210-225.

[7]. Lee, J., & Kim, S. (2023). Enhancing cybersecurity through machine learning-based intrusion detection systems. Computers & Security, 32(1), 56-78.

[8]. Patel, R., & Gupta, S. (2023). Privacy-preserving machine learning for cybersecurity: A survey. Journal of Privacy and Confidentiality, 12(1), 34-51.

[9]. Prasad, R., Rohokale, V., Prasad, R., & Rohokale, V. (2020). Artificial intelligence and machine learning in cyber security. Cyber security: the lifeline of information and communication technology, 231-247.

[10]. Satheesh Kumar, M., Ben-Othman, J., Srinivasagan, K. G., & Umarani, P. (2022). Machine Learning Methods for Enhanced Cyber Security Intrusion Detection System. Advances in Computing, Informatics, Networking and Cybersecurity: A Book Honoring Professor Mohammad S. Obaidat's Significant Scientific Contributions, 733-754.

[11]. Smith, A. (2023). Machine learning applications in cybersecurity: A comprehensive review. Journal of Computer Science and Engineering, 8(2), 45-67.

[12]. Wang, Y., & Zhang, L. (2023). Explainable AI techniques for improving transparency in cybersecurity. IEEE Security & Privacy, 25(4), 67-82.

[13]. Yang, X., & Li, M. (2022). Bias in machine learning algorithms: Implications for cybersecurity. Journal of Artificial Intelligence Research, 18(3), 102-119.

[14]. Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, 23817-23837.

[15]. "Solving Roulette Wheel Selection Method using Swarm Intelligence for Tragjectory Planning of Intellignet System" by (IEEE) International Conference on Recent Trends in Electronics and Communication (ICRTEC), 03 May 2023, ISBN, 979-8-3503-9619-5/23 DOI 10.1109/ICRTEC56977.2023.10111861.Shashi Kant Gupta, Waseem Ahmad, Dimitrios A. Karras, Alex Khang, Chandra Kumar Dixit, Bhadrappa haralayya,

[16]. "Image Segmentation on Gabor Filtered images using Projective Transformation" by (IEEE) International Conference on Recent Trends in Electronics and Communication (ICRTEC), 03 May 2023, ISBN 978-83503-9619-5 DOI: 10.1109/ICRTEC56977.2023.10000885, Shashi Kant Gupta, Ahmed Alemran, Prabhdeep Singh, Alex Khang, Chandra Kumar Dixit, Bhadrappa haralayya.

[17]. "Detection of Number Plate in Vehicles using Deep Learning based Image Labeler Model", (IEEE) International Conference on Recent Trends in Electronics and Communication (ICRTEC), May 2023, ISBN 979-8-3503-9619-5 DoI:10.1109/ICRTEC56977.2023.10111862, Shashi Kant Gupta, Surabhi Saxena, Alex Khang, Bramah Hazela Chandra Kumar Dixit, Bhadrappa haralayya.

[18]. "High Pressure Isothermal Equation of State for Chalcogenides" by Der Pharma Chemica 2023 volume 15 (4) pp 32-41 ISSN 0975-413X DoI 10.4172/0975-413X.15.4.32.41 website http://derpharmachemica.com/archive.html) Shipra Tripathi, Anjani K Pandey, Shivam Srivastava, prachi Singh and Chandra K Dixit.

[19]. "Solving Roulette Wheel Selection Method using Swarm Intelligence for Trajectory Planning of Intelligent Systems" by 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), IEEE Xplore: 03 May 2023 ISBN:979-8-3503-9619-5 ISBN:979-8-3503-9620-1n DOI: 10.1109/ICRTEC56977.2023.10111861

[20]. "Comparative Study of Elastic Properties of Some Inorganic and Organic Molecular Crystals" by Using Isothermal Eos by Social Science Research Network (SSRN) SSRN: https://ssrn.com/abstract=4427891 or http://dx.doi.org/10.2139/ssrn.4427891 ISSN No 1556-5068, pages 522–533, Anjani Panday, Chandra Kumar Dixit, Shivam Srivastava 24 April 2023.

[21]. "Sanitization and restoration of under-utilized healthcare database in single-cloud and multi-cloud environment using optimal key generation for personalized privacy preservation" by AIP Conference Proceedings Doi:https://doi.org/10.1063/5.0126285 (25 April 2023), ISBN 9780735444430 ISSN- 0094-243X VOL 2603 Shahanawaj Ahamad , J. Jeyasudha , S. Gnanavel, Chandra Kumar Dixit , Shvets Yuriy Yurievich , Ronald M. Hernandez

[22]. "Performance comparison of feature selection algorithms in the life expectancy risk prediction of post-operative lung cancer patients" by AIP Conference Proceedings 2603, 020008 (25 April 2023) https://doi.org/10.1063/5.0126447 Anuradha Misra , Fred Torres-Cruz , Ramiro Pedro, Laura-Murillo , Elqui Yeye Pari-Condori , Chandra Kumar Dixit , Julio Cesar Tisnado Puma

[23]. "Cloud computing based renewable energy demand management system" by AIP Conference Proceedings 2603, 020015 (25 April 2023) https://doi.org/10.1063/5.0126132 Shiva Johri , Balaji Ramkumar Rajagopal , Shahanawaj Ahamad , B.Kannadasan , Chandra Kumar Dixit , Prabhdeep Singh

[24]. White matter microstructural integrity in recovering alcoholic population by AIP Conference Proceedings 2603, 020017 (25 April 2023) https://doi.org/10.1063/5.0126180 D. Sugumar) , Chandra Kumar Dixit , Miguel A. Saavedra-Lopez , Ronald M. Hernandez , Abhishek Madduri , Bhasker Pant