IEEE Computational Intelligence Society

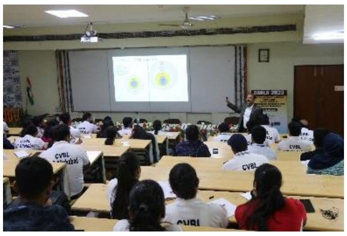
Technically Co-Sponsored by IEEE UP SECTION (INDIA)

IEEE Advancing Technology for Humanity

IEEE Computational Intelligence Society (CIS) Distinguished Lecture by Prof. Dipankar Dasgupta, University of Memphis, USA

CVBL IIIT Allahabad

July 20, 2023, IIIT Allahabad, India



About: Prof. Dipankar Dasgupta from University of Memphis visited Indian Institute of Information Technology Allahabad, Prayagraj on 20th July 2023. He delivered an IEEE CIS distinguished lecture in physical mode. Prof. Dipankar also participated in discussion with the faculty members along with the participants and students. His talk was also part of IEEE CIS CADLA 2023 Summer School.

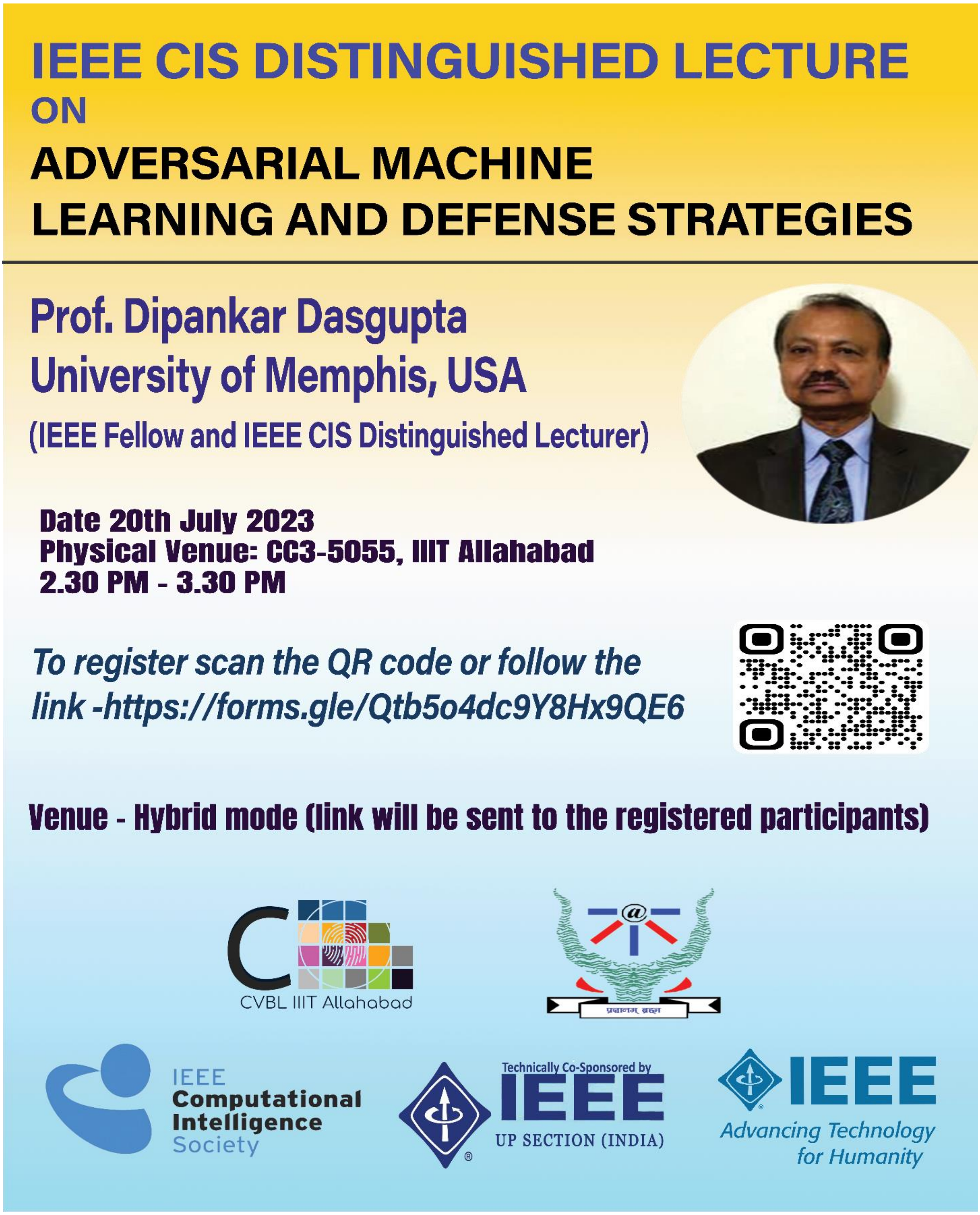
Lecture Title: Adversarial Machine Learning and Defense Strategies

Abstract: Adversarial attacks can disrupt any AI/ML based system functionalities; while handling such attacks are challenging, but also provide significant research opportunities. This talk will cover emerging adversarial machine learning (AML) attacks on systems and the state-of-the-art defense techniques. First, I will discuss how and where adversarial attacks can happen in an AI/ML model and framework. I will then present classification of adversarial attacks and their severity and applicability in real-world problems and what steps can be taken to mitigate their effects. The role of GAN in in adversarial attacks and as a defense strategy. I will discuss a dual-filtering strategy could mitigate adaptive or advanced adversarial manipulations for wide-range of ML attacks with higher accuracy. The developed dual-filter software can be used as a wrapper to any existing ML-based decision support system to prevent a wide variety of adversarial evasion attacks. The DF framework utilizes two set of filters based on positive (input filters) and negative (output filters) verification strategies that can communicate with each other for higher robustness.

Bio of Speaker: Prof. DIPANKAR DASGUPTA joined The University of Memphis as an Assistant Professor, in 1997, and became a Full Professor, in 2004. He is IEEE Fellow, NAI Fellow and IEEE Computational Intelligence Society Distinguished Lecturer. He has been an Advisory Board Member with the Geospatial Data Center (GDC), Massachusetts Institute of Technology, since 2010. He has published a number of books and edited volumes, including Advances in User Authentication (2017), Immunological Computation: Theory and Applications (2008), Artificial Immune Systems (1999), and another book on genetic algorithms (1996). He has published more than 300 research papers with 20000 citations of his work. His research interests include the computational intelligence (including AI and machine learning) for the design and development of intelligent solutions. He is one of the founding father of the field of artificial immune systems, making major contributions in developing tools for digital immunity and survivable systems. He was a recipient of the 2011–2012 Willard R. Sparks Eminent Faculty Award, the highest distinction and most prestigious honor given to a Faculty Member by The University of Memphis. He was also a recipient of the 2014 ACM SIGEVO Impact Award and an ACM Distinguished Speaker, from 2015 to 2020. He currently holds the William Hill Professorship at The University of Memphis.

Registration Statistics:

Total Number of Registration (All from India)	100
Number of Registration from Other Institutes	82
Number of Registration from Host Institution	18
Number of Student Participants	74
Number of Faculty Participants	22
Number of R&D Professional Participants	4
Number of Different Institutions of Participants	40
Number of Different States of Participants	17
Number of IEEE Member Participants	15
Number of Participants Interested to take IEEE CIS membership	28



IEEE CIS DISTINGUISHED LECTURE
ON
ADVERSARIAL MACHINE LEARNING AND DEFENSE STRATEGIES

Prof. Dipankar Dasgupta
University of Memphis, USA
(IEEE Fellow and IEEE CIS Distinguished Lecturer)

Date 20th July 2023
Physical Venue: CC3-5055, IIIT Allahabad
2.30 PM - 3.30 PM

To register scan the QR code or follow the link -https://forms.gle/Qtb5o4dc9Y8Hx9QE6

Venue - Hybrid mode (link will be sent to the registered participants)

CVBL IIIT Allahabad
प्रज्ञानम् ब्रह्म
IEEE Computational Intelligence Society
Technically Co-Sponsored by
IEEE UP SECTION (INDIA)
IEEE Advancing Technology for Humanity