Name:

Dipankar Dasgupta, IEEE Fellow

Position and Affiliation:

William Hill Professor of Computer Science
Director, Center for Information Assurance (CfIA)
The University of Memphis
Homepage: www.cs.memphis.edu/~dasgupta
IA center: cfia.memphis.edu

e-mail: dasgupta@memphis.edu

Lecture topic(s):

Topic 1: Computational Intelligence in Cybersecurity.

Topic 2: Adversarial Machine Learning and Defense Strategies.

Topic 3: Adaptive Multi-Factor Authentication & Cyber Identity.

Topic 4: Advances in Immunological Computation.

Topic 5: AI vs AI: Viewpoints.

Lecture topic(s) and Abstract (s):

Topic 1: Computational Intelligence in Cybersecurity.

Computational Intelligence (CI) constitutes an umbrella of techniques, has proven to be flexible in solving dynamic and complex real-world problems. These techniques typically include Machine Learning, Fuzzy Logic, Evolutionary Computation, Intelligent Agent Systems, Neural Networks, Cellular Automata, Artificial Immune Systems, Game Theory and other similar computational models. Cyber defense is a continuously changing attack landscape as the software/hardware components are added and/or updated more frequently at different layers of cyber systems for additional functionalities and/or improved usability while in many cases these are not security-enabled. Attackers exploit these vulnerabilities and find attack paths to compromise the target systems.

In this talk, I will discuss multi-faceted Computational Intelligent (CI) techniques which can provide an efficient security paradigm to deal with influx of new threats in network infrastructures and smart applications. I will cover some CI approaches which are used to augment defense-in-depth and building zero-trust architectures and to add necessary security enhancements to the design, development, testing and operation of cyber-enabled systems.

References:

- IEEE Symposium Series on Computational Intelligence (SSCI)-CICS, organizer: Dr. D. Dasgupta, since 2007.
- Machine learning in cybersecurity: a comprehensive survey. D Dasgupta, Z Akhtar, S Sen. The Journal of Defense Modeling and Simulation, 2020. https://doi.org/10.1177/1548512920951275.

==

Topic 2: Adversarial Machine Learning and Defense Strategies.

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.

References:

- Dual-filtering (DF) schemes for learning systems to prevent adversarial attacks. D Dasgupta, KD Gupta - Complex & Intelligent Systems, pp 1-22, January 2022
- Who is responsible for Adversarial Defense. K Dattagupta and D. Dasgupta. Workshop on Challenges in Deploying and monitoring Machine Learning Systems, ICML 2021.
- Applicability issues of evasion-based adversarial attacks and mitigation techniques. KD Gupta, D Dasgupta, Z Akhtar - 2020 IEEE Symposium Series on Computational …, 2020

==

Topic 3: Adaptive Multi-Factor Authentication & Cyber Identity

Authentication is a critical part to ensure the identity of a legitimate user. During authentication, an individual’s credential is validated with a specific computational technique to determine the association of the user with his/her claimed identity.

In this talk, I will discuss an adaptive multi-factor authentication (A-MFA) framework which uses adaptive selection of multiple modalities at different operating environment so to make authentication strategy unpredictable to hackers. This methodology incorporates a novel approach of calculating trustworthy values of different authentication factors while the computing device being used under different environmental settings. Accordingly, a subset of authentication factors is determined (at triggering events) on the fly thereby leaving no exploitable a priori pattern or clue for adversaries. Such a methodology of adaptive authentication selection can provide legitimacy to user transactions with an added layer of access protection that is not rely on a fixed set of authentication modalities. Robustness of the system is assured by designing the framework in such a way that if any modality data get compromised, the system can still perform flawlessly using other non-compromised modalities. Scalability can also be achieved by adding new and/or improved modalities with existing set of modalities and integrating the operating/configuration parameters for the added modality.

I will highlight what type of evaluation be required for such identity management software to detect possible deep fakes and other forms of faking biometrics. Other attacks on current means of identity validation may become possible. What would be what good figures of merit to be used as response variables? What are good factors over which we would need to test for next-generation identity eco-systems.

References:

- *Advances in User Authentication. Dipankar Dasgupta, Arunava Roy, Abhijit Nag.* Publisher: Springer-Verlag, Inc., August 2017.
- US Patent # 9,912,657: *Adaptive Multi-Factor Authentication*, Dasgupta, et al., March 6, 2018.

==

Topic 4: Advances in Immunological Computation.

The biological immune system is a robust, complex, adaptive system that defends the body from foreign pathogens. It is able to categorize all cells (or molecules) within the body as self or non-self substances. It does this with the help of a distributed task force (immune cells) that has the intelligence to take action from a local and also a global perspective using its network of chemical messengers for communication. Immunological Computation (or Artificial Immune Systems) works are spanning from theoretical modeling and simulation to wide variety of applications. Some of the studies are of synthetic approaches to understand and simulate the biological immune system, and others that develop computational methodologies inspired by the immune system to solve real-world problems.

In this talk, I will discuss different Immunological Computation (IC) models including immune network model, negative selection algorithm (NSA), clonal selection, and danger theory, etc. Also summarize progresses made in IC to solve problems in different domain. I will then highlight variations of NSA, provide comparative analysis, their scope and limitations in different application domains. Studies show that NSA performs better for nonlinear representation than most of the other computation methods, and it can outperform neural-based models in computation time. I will summarize NSAs development over the years and highlight challenges in solving real-world problems.

References:

- *Negative Selection Algorithm Research and Applications in the last decade: A Review.* K Dattagupta and D. Dasgupta. In.IEEE transaction of Artificial Intelligence, September 2021.
- *Immunological Computation: Theory and Applications*. Dipankar Dasgupta and Fernando Nino, (authors), CRC press, September 2008.

===

Topic 5: AI vs AI: Viewpoints

(AI is a double-edged technology, need to use it for greater good!)

Artificial Intelligence (AI) has become a buzzword in every industry that claims to provide an excellent product/service features to promote its sales and marketing. In many cases, justifications for using AI/ML are not very clear or their technical benefits are poorly understood. It may not be necessary to use AI/ML techniques for well-defined problems where exhaustive searches, look-up tables or some statistical measures may produce similar outcomes. There exists more than fifty so-called AI/ML algorithms and heuristics. It is very important to understand the complexity of data features, associated constraints, and proper data representation (encoding); also, there are other determining factors while choosing a specific AI/ML technique. As reported *"AI is not magic, it is computational logic"* indicated that mathematics and statistics are underlying building blocks of all AI/ML algorithms and require in-depth knowledge of techniques to efficiently solve different real-world problems. Moreover, if the environment is unpredictably dynamic, uncertain, misleading, and have man-made obfuscation where behavior profiling or knowledge patterns are difficult to harness, most AI/ML techniques in practice today may miserably fail.

In this talk, I will discuss some important use of AI in search, optimization, prediction and discovery; how algorithmic bias can impact decisions; how AI can play dual-role and can be applied in many ways with varying intent. I will also exhibit use cases on "Defensive AI and Offensive AI", and in designing "Digital Twin". Finally, I will ague that with the significant business benefits of using AI/ML techniques, there exist possibilities of misuse/abuse or inappropriate use of such techniques. So, regulations such as Algorithmic Accountability Act. become essential for AI-based developers to take responsibilities of their products and services.

References:

- *An Empirical Study on Algorithmic Bias*. S. Sen, D. Dasgupta and K. D. Gupta, 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1189-1194, Madrid, Spain, 2020.
- *AI vs. AI: Viewpoints*, D. Dasgupta, Technical Report, no. CS-19-001, The University of Memphis, May 2019.

==

SPEAKER BIOSKETCH:

Dr. Dipankar Dasgupta is a professor of Computer Science at the University of Memphis since 1997, an IEEE Fellow, an ACM Distinguished Speaker (2015-2020) and an IEEE Distinguished Lecturer (2022-2024). Dr. Dasgupta is known for his pioneering work on the design and development of intelligent solutions inspired by natural and biological processes. During 1990-2000, he extensively studied different AI/ML techniques and research in the development of an efficient search and optimization method (called structured genetic algorithm) has been applied in engineering design, neural-networks, and control systems. He is one of the founding fathers of the field of artificial immune systems (a.k.a Immunological Computation) and is at the forefront of applying bio-inspired approaches to cyber defense. His notable works in digital immunity, negative authentication, cloud insurance modeling, dual-filtering and adaptive multi-factor authentication demonstrated the effective use of various AI/ML algorithms. His research accomplishments and achievements have appeared in Computer World Magazine, NASA's website, and in local TV Channels and Newspapers.

Dr. Dasgupta has authored four books, 5 patents (including 2 under submissions) and have more than 300 research publications (20,000 citations as per google scholar) in book chapters, journals, and international conference proceedings. Among many awards, he was honored with the 2014 ACM-SIGEVO Impact Award for his seminal work on negative authentication, an AI-based approach. He also received five best paper awards in different international conferences and has been organizing IEEE Symposium on Computational Intelligence in Cyber Security at SSCI since 2007. Dr. Dasgupta is an ACM Distinguished Speaker, regularly serves as panelist and keynote speaker and offer tutorials in leading computer science conferences and have given more than 350 invited talks in different universities and industries.