2026 ASEE ANNUAL CONFERENCE June 21–24, 2026 | Charlotte Convention Center, NC
Host Sponsor UNC Charlotte
Paper ID #50451

# NSF-DGE: An Embedded Case Study Approach for Broadening Students' Mindset for Ethical and Responsible Cybersecurity

**Dr. Aditya Johri, George Mason University**

Aditya Johri is Professor in the department of Information Sciences & Technology. Dr. Johri studies the use of information and communication technologies (ICT) for learning and knowledge sharing, with a focus on cognition in informal environments. He also

**Arka Ghosh, George Mason University**
**Sai Sharanya Garika, George Mason University**

# NSF-DGE: An Embedded Case Study Approach for Broadening Students' Mindset for Ethical and Responsible Cybersecurity

The increasing use of AI-enabled technologies in social domains poses safety and security risks that future cybersecurity professionals will need to address. Importantly, many of these risks go beyond narrow notions of robustness against attack to include concerns about misuse, unintended consequences, fairness across users, and other possible harms that happen when technologies are broadly used in society. This raises the need for future cybersecurity professionals to be aware of these harms and to consider ethics and responsibility of the systems they secure. This goal of this project is to help students develop an ethical and responsible mindset towards cybersecurity topics, focusing on technologies that use artificial intelligence (AI) in security and privacy.

To achieve this goal, the project team is developing a series of case studies of AI-based technologies designed for social problems, helping students reason about aspects of the design that can raise or mitigate security and privacy risks. Case studies have shown to be effective in teaching students about sociotechnical dimensions of engineering [1].

The cases are being implemented in a series of undergraduate and graduate cybersecurity-related courses, with the idea that repeated exposure to these topics will make ethical considerations an integral part of the security curriculum, and that seeing them in different contexts will reinforce student learning and prepare students to transfer these mindsets and skills across contexts as they enter the workforce.

*Case Study Design*: Using prior research on situated learning and perspectival thinking, the project team has created a series of four role-play-based case studies that highlight different social and ethical risks that often arise around AI technologies designed for security-related problems [2]. Role-play based methods are an effective pedagogical technique for learning and perspective-taking; the team plans to combine them with a concept map-based assessment approach that is well-suited for the kind of longitudinal assessment that will be needed for a multi-course curriculum effort. The concept map elicitation is grounded in common security standards and rubrics, tightening the connection between the role-playing exercises and the security workforce development goals of the project.

*Case Study Example*: Topics have been chosen to highlight different areas of cybersecurity, different social contexts, and different risks; the current cases address automated video monitoring for surveillance, privacy of smart home devices, and algorithmic evaluation of candidates for jobs in the curriculum. The face recognition case study, for instance, asks students to act as a member of a taskforce that has been assembled at a large university to ascertain if video-based monitoring should be used on campus for enhanced safety [3]. Students take on a role and research it and then discuss the merits and disadvantages of using video-based monitoring on campus.

*Case Study Implementation*: The case study was implemented as part of multiple courses, both at the undergraduate and graduate levels. At the undergraduate level, the cases were implemented in a course on technology and ethics. Data collected from 38 students shows that during the case discussion students focused on both the pros and cons of using the technology and reflected on

the foreseeable problems and improvements that can be achieved in the future. Interestingly, we found that although the groups discussed the same case, the discussion varied, and the groups reached different final recommendations. Overall, assessment of student learning shows that students learned both technical knowledge related to security and sociotechnical implications of using technology. We will present detailed findings in the poster.

*GENCAS – A GenAI-based System for Case Study Assessment and Feedback*: In the most recent semester, and another study we will discuss in the poster session, focused on use of generative AI (GenAI) for teaching and learning. As the use of GenAI among students has increased, it has become imperative that instructional approaches also examine how it can be incorporated into pedagogy. With this goal in mind, we designed GENCAS or GenAI-Based Case Study Assessment and Feedback System. This is an interactive, AI-enabled educational platform designed to evaluate and enhance student understanding of real-world case studies. Leveraging our prior work on using the case study approach, we used anonymized transcripts from prior group discussions to train the AI system to assess and provide feedback to students. Our system combines a lightweight user interface with a Retrieval-Augmented Generation (RAG) workflow to deliver context-aware, personalized feedback on student responses. A student goes through a structured question flow and submits open ended answers. For each answer, the application retrieves the most relevant prior discussion fragments and constructs a composite prompt consisting of the current question, the student's answer, and contextual snippet. This prompt is sent to an OpenAI model (gpt-4o-mini) to generate formative feedback that references authentic peer reasoning rather than generic rubric language. GENCAS demonstrates a practical, privacy-conscious pattern for augmenting assessment with retrieval-grounded generative AI to produce timely, context-rich feedback that scales beyond traditional manual evaluation. We will present detailed findings from user evaluation where most users rate the system positively.

**Acknowledgement**
This work is partly supported by U.S. NSF Award# DGE-2335636. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agencies.

**References**
1. Martin, Diana Adela, Eddie Conlon, and Brian Bowe. "The role of role-play in student awareness of the social dimension of the engineering profession." European Journal of Engineering Education 44, no. 6 (2019): 882-905.

2. Hingle, Ashish, and Aditya Johri. "Role-Play Case Studies to Teach Computing Ethics: Theoretical Foundations and Practical Guidelines." Proceedings of HICSS (2024).

3. Johri, Aditya. "Facial Recognition Case Description and Details". (2024) Available: https://onlineethics.org/cases/george-mason-tech-ethics/utilizing-facial-recognition-university-campus