CAE Forum

Wednesday, December 1, 2021

Kubernetes Security Attacks (1:00 - 1:50 pm EST)

Securing Big Data in the Age of Artificial Intelligence (2:00 – 2:50 pm EST)

Mark your calendar and come join us for CAE Forum! CAE Forum is a live, real-time, online, academic forum where members of the CAE community give non-technical presentations on topics of value to the CAE community. CAE Forum is about sharing your ideas, knowledge, and expertise to empower and strengthen our community. It's that simple. CAE Forum presentations are normally held on the third Wednesday of each month during the Fall and Spring semesters.

PRESENTATION #1

Title/Topic: Kubernetes Security Attacks

Time: 1:00 - 1:50 pm EST

Location: https://caecommunity.zoom.us/my/caeforum

Just log in as "Guest" and enter your name. No password required.

Audience: Students, Professors, Govt.

Presenter(s): Md Shazibul Islam Shamim, Tennessee Tech University

Description: With the rapid adoption of Kubernetes among the organizations such as IBM, Capital One, Netflix, and government organizations like the US department of defense, Kubernetes has become one of the fastest-growing open-source software in the history of open-source with 77% of market share in container orchestration. However, in recent Kubernetes security incidents in Capital One, Tesla revealed that the Kubernetes cluster could be susceptible to attack. According to the Redhat 2021 survey, 94% of IT practitioners reported having experienced at least one security incident in the last 12 months. In this CAE forum presentation, the presenter will discuss Kubernetes security attacks for violating security best practices and possible mitigation strategies.

PRESENTATION #2

Title/Topic: Securing Big Data in the Age of Artificial Intelligence

Time: 2:00 - 2:50 pm EST

Location: https://caecommunity.zoom.us/my/caeforum

Just log in as "Guest" and enter your name. No password required.

Audience: Students, Professors, Govt.

Presenter(s): Dr. Murat Kantarcioglu, University of Texas at Dallas

Description: Recent cyberattacks have shown that the leakage/stealing of big data may result in enormous monetary loss and damage to organizational reputation, and increased identity theft risks for individuals. Furthermore, in the age of big data and Artificial Intelligence (AI), protecting the security and privacy of stored data is paramount for maintaining public trust, accountability and getting the full value from the collected data. Therefore, we need to address security and privacy challenges ranging from allowing access to big data to building novel AI models using the privacy sensitive data. In this talk, the presenter will provide an overview of our end-to-end solution framework that addresses these security and privacy challenges arise in the age of AI. In addition, we will discuss our federated learning framework that is designed to be robust against poisoning attacks.

A recording of the live presentation will be available following the pre of the presentation at: https://www.caecommunity.org/resources/cae-forum-resources

Contact us at: caeforum@caecommunity.org