2nd International Hybrid Workshop on "Start-to-End Beamline Optimization for Synchrotron Radiation and Free-Electron Laser Facilities through Artificial Intelligence Approaches", 17-18 January 2024, DESY-Hamburg-Germany

Contribution ID: **21** Type: **not specified**

Securing Visual Data Processing: Harnessing Deep Learning for Privacy and Security

Thursday 18 January 2024 14:00 (30 minutes)

In recent times, visual surveillance systems have undergone rapid advancements, exhibiting increased capabilities and widespread integration of artificial intelligence. Concurrently, these surveillance systems have raised concerns by exposing the public to emerging privacy and security risks. Instances of overt misuse of surveillance technologies have surged, prompting the implementation of data privacy regulations such as GDPR in Europe to establish guidelines for responsible data collection and processing.

Despite these regulatory measures, there remains a pressing need for a secure and private approach to train sophisticated machine learning and deep learning algorithms. In this paper, we propose a method that prioritizes privacy in visual surveillance. Initially, we curate a dataset consisting of videos with preserved privacy. The content within these videos is obfuscated using a combination of Gaussian Mixture Model (GMM) and selective encryption techniques. Subsequently, we employ this privacy-preserved dataset to train high-performance object detection models.

Primary author: KANWAL, Nadia (Keele University, UK)

Presenter: KANWAL, Nadia (Keele University, UK)