Creating Interpretable Collaborative Patterns to Detect Insider Threats
You Chen, Vanderbilt University

It has been shown that health information system (HIS) can enable healthcare organizations (HCOs) to function in a collaborative manner. This enables the composition of teams of care providers that improve efficiency, while facilitating better quality in patient treatment. However, at the same time, the detail and sensitive nature of the patient information in an HIS make it attractive to numerous adversaries. It is believed that the greatest security threats to HIS stems from insiders. Collaborative relational models can be learned as compact patterns in an unsupervised manner, which can be leveraged to detect and prevent insider threats to HIS. In this talk, I will review how such collaborative patterns can be composed and applied to various types of adversaries. Additionally, I will demonstrate the potential for such patterns using audit data and patient information from multiple real HIS.

Despite the mathematical sophistication of such models and their capability to detect anomalous behavior, approaches based on unsupervised learning are unlikely to be relied upon by HCO administrators unless the resulting patterns reflect the expected operations of the healthcare system. As such, this talk will further illustrate how to evaluate the extent to which inferred organizational relations meet the expectations of HCO employees. Specifically, this section of the talk will review a survey (and results) that captures the degree to which employees agree with inferred organizational behavior. This survey was conducted with employees from four areas in the Vanderbilt Medical Center; two administrative areas: Coding & Charge Entry and Medical Information Services and two clinical areas: Anesthesiology and Psychiatry. The HCO employee expectations were compared to the learned collaborative models using a linear-mixed effects regression models. The findings confirm that employees can distinguish between organization rules of high and low likelihood, which suggests that the learned collaborative patterns through utilization of HIS are believable for detecting insider threats in collaborative environments.