Department of Computer Science

East Carolina University

Seminar

Data Privacy in Cyber-Physical Systems

Abstract. The talk will focus on the concept of pairing confidential-relevant variables (connected variables) using ridge regression and bootstrap sampling for developing perturbation models to data privacy in cyber-physical systems. A single set of perturbation parameters for all the pairs of connected variables has been used a recent approach to achieve trade-off between confidentiality and classification as data utility. It has led to weaker confidentiality protection for some pairs of connected variables than the others. The observation was that the varying correlation characteristics between the variables contribute to this discrepancy. The correlation between a connected variable and other confidential variables influences the correctness of the perturbation parameters of the ridge regression model studied for data privacy. In this talk, I will discuss a recently proposed method, which divides the feature space into correlated subspaces, and examine the performance of ridge regression-based perturbation model with bootstrap sampling in individual subspaces separately. The experimental analysis with IRIS and NSL-KDD datasets has provided an interesting finding with the absolute Pearson correlation coefficient which I will be presenting in this talk.

Biography. Dr. Shan Suthaharan is a Professor of Computer Science at the University of North Carolina at Greensboro (UNCG), North Carolina, USA. He has authored a well received textbook entitled "Machine learning models and algorithms for big data classification: Thinking with examples for effective learning", published Springer US. His research is focused on the characterization and detection of environmental events for security, the exploration of machine learning techniques, and the development of advanced statistical and computational techniques to discover relevant signatures and detect emerging events from structured and unstructured big data and the environment. He is particularly interested in big data privacy and security, machine learning models and algorithms, cognitive computing, and pattern recognition in big data. Dr. Suthaharan has authored or co-authored more than seventy-five research papers in the areas of computer science. He also invented a key management and encryption technology, which has been patented in Australia, Japan, and Singapore. He also received visiting scholar awards from and served as a visiting researcher at University of Sydney, Australia; University of Melbourne, Australia; and University of California, Berkeley, USA.

Dr. Shan Suthaharan

Professor
Department of
Computer Science
University of North Carolina
at Greensboro (UNCG)
s_suthah@uncg.edu

Friday October 28, 2016
1:00pm – 1:50pm
Bate Building
Room 1001
Refreshment will be served