UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Machine Learning for the Internet of Things: Applications, Implementation and Security

by

Vishalini Laguduva Ramnath

For the Ph.D. degree in Computer Science and Engineering

Artificial intelligence and ubiquitous sensor systems have seen tremendous advances in recent times, resulting in groundbreaking impact across domains such as healthcare, entertainment and transportation through a collective ecosystem called the Internet of Things. Such frameworks do not inherently take into account the issues that come with scale such as privacy, security of the data and the ability to provide a completely immersive experience. This is particularly significant since, due to the somewhat limited scope of computing resources, the IoT edge nodes themselves do not process the observed data. Instead, they transmit the collected data to more powerful servers for processing. This information transmission can place strain on the network while introducing security concerns such as eavesdropping and man-in-the-middle attacks. In this dissertation, we address these concerns by using machine learning as a disruptive tool by developing privacy-aware, lightweight algorithms while evaluating the feasibility of hardware security primitives such as physical unclonable functions (PUFs) for IoT node security. We offer a way forward for the development of an IoT framework for continuous activity monitoring that can scale to millions of nodes while ensuring the privacy and security of the observed data.

Examining Committee
Andrew M. Hoff Ph.D., Chairperson
Srinivas Katkoori Ph.D., Major Professor
Sriram Chellapan Ph.D.
Robert Karam Ph.D.
Morris Chang Ph.D.
Ramachandran Kandethody Ph.D.

Thursday, June 18, 2020
1:30 PM
Online (Microsoft Teams)
Please email for more information
vishalini@usf.edu
THE PUBLIC IS INVITED

Publications

1) **Vishalini Laguduva,** et al. "Machine learning based IoT edge node security attack and countermeasures." 2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). IEEE, 2019.
2) **Vishalini Laguduva,** et al. "Latent Space Modeling for Cloning Encrypted PUF-Based Authentication." IFIP International Internet of Things Conference. Springer, Cham, 2019.
3) **Vishalini Laguduva,** et al. " Dissecting Convolutional Neural Networks for Efficient Implementation on Constrained Platforms." 2020 International Conference on VLSI Design (VLSID). 2020.
4) **Vishalini Laguduva,** Srinivas Katkoori, and Robert Karam. "Machine Learning Attacks and Countermeasures for PUF-based IoT Edge Node Security." Springer Nature Computer Science Journal. Under Review
5) **Vishalini Laguduva,** Srinivas Katkoori. "A Smart IoT System for Continuous Sleep State Monitoring." IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), 2020. Under Review
6) **Vishalini Laguduva,** Srinivas Katkoori. "Evaluating Security Concerns in Internet of Medical Things." ACM Transaction on Internet of Things. To be Submitted.
7) **Vishalini Laguduva**, Srinivas Katkoori. "Exploring Design Accuracy Trade off's in Quantized Neural Networks in IoT Edge Nodes." IEEE Internet of Things Journal. To be Submitted.

Robert Bishop, Ph.D.
Dean, College of Engineering

Dwayne Smith, Ph.D.
Dean, Office of Graduate Studies

Disability Accommodations:
If you require a reasonable accommodation to participate, please contact the Office of Diversity & Equal Opportunity at 813-974-4373 at least five (5) working days prior to the event.