SEMINAR ANNOUNCEMENT

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
FACULTY OF ENGINEERING
Website: https://www.eng.nus.edu.sg/ece/

Area: Communications & Networks

Host: Assoc Prof Bharadwaj Veeravalli

TOPIC	**:**	**Privacy-Preserving Collective Learning With Homomorphic Encryption**
SPEAKER	**:**	**Mr Jestine Paul** **Graduate Student, ECE Dept, NUS**
DATE	**:**	**Friday, 22 October 2021**
TIME	**:**	**10.00AM to 11.00AM**
WEBINAR	**:**	**Join Zoom Meeting** https://nus-sg.zoom.us/j/85882626354?pwd=UEtNUWt2dnM1ZHZVNU9XRC9HTGdMZz09 **Meeting ID: 858 8262 6354** **Password: 749870**

ABSTRACT

Deep learning models such as long short-term memory (LSTM) are valuable classifiers for time series data like hourly clinical statistics. However, access to health data is challenging due to privacy and legal issues. Homomorphic encryption (HE) offers a potential solution by encrypting confidential data. However, the computational complexity of encrypted operations makes it infeasible for training with gradient descent. Prior works only deal with encrypted procedures during the inference phase of the network. To this end, we design Collective Learning protocol, a secure protocol for sharing classified time-series data within entities to train parameters of the binary classifier model partially. The protocol encrypts each data's feature activations using HE and trains the last layers using encrypted logistic regression. We evaluate our protocol on a benchmark LSTM network trained on the Medical Information Mart for Intensive Care (MIMIC-III) dataset. We selected the Cheon-Kim-Kim-Song (CKKS) encryption scheme because of its ability to work with real numbers using approximate arithmetic. Our protocol improved the area under the precision-recall curve (AUPRC) score of the in-hospital mortality prediction model. The same protocol was reimplemented using secure multi-party computation (MPC) and compared.

BIOGRAPHY

Jestine Paul received the B.E. degree in computer engineering from Nanyang Technological University, Singapore, in 2007. He is also currently working as a Senior Research Engineer with the Institute for Infocomm Research, A*STAR, Singapore. His research interests include cryptography, secure computation, and deep learning.

https://www.eng.nus.edu.sg/ece/highlights/events/