7a.013.UVA - Privacy Preserving Multi-Party Analytics

Project - Team

Team Member	Role	Email	Phone Number	Academic Sites/Industry Members
Peter Beling	PI	beling@virginia.edu	(434) 982-2066	University of Virginia
Stephen Adams	Researcher	sca2c@virginia.edu	(757) 870-4954	University of Virginia
Alex Langevin	Student	arl4zk@virginia.edu	Not Available	University of Virginia
Ronald Colmone	Project Mentor	ronald.colmone@broadcom.com	Not Available	**Broadcom**
Steven Greenspan	Project Mentor	sgreenspan@gmail.com	Not Available	**Funded By: CA Technologies**

Project - Summary

Many domains and industries would benefit from sharing data for predictive modeling but for privacy, legal/regulatory, competitive, or other reasons, parties may be unwilling or unable to share information with each other. Differential privacy (DP), whereby carefully selected random noise is added to the development process, presents a way to share (approximate) information while guaranteeing mathematically a level of privacy for each party.

Year 6 of the project developed a DP method for jointly training a deep learning model applied to credit card fraud detection. Year 6 results successfully demonstrated multi-party deep learning under certain conditions and simplifying assumptions. In Year 7, we intend to leverage the results of Year 6 and examine alternate learning solutions, as well as relax some key assumptions, moving towards more realistic settings.

Year 7 will see the introduction of dataset heterogeneity –it will no longer be assumed that each party collects the same data on their customers and/or have the same customer (i.e. Data) distribution. In this scenario, it may no longer make sense to jointly develop a single general model that fails to account for local peculiarities in each party's data. To address this we plan to incorporate generative adversarial networks (GANs), which are models that learn the underlying structure of a dataset, and can generate synthetic data that mimics the distribution of the real data.

The methods developed in Year 6 can be used to train DP GANs, which can then be shared with other parties and used to augment the training of local models. GANs can also be used to address issues with imbalanced data – our dataset has a fraud rate of 0.14%. We also plan to utilize the discriminator model, which is often overlooked in the literature outside of training, to pre-select data from other the GANs with a view of optimizing local model development.

The primary challenge foreseen will be the development of GANs for discrete data, for which there is currently no established method, and integrating this discrete model into a joint discrete/continuous GAN.

Project - Novelty of Approach

Attention Project PIs

PIs are responsible for keeping up the content of their project page and have the ability to EDIT the page.

- To **EDIT**, click the edit "pencil icon" in the top right-hand corner of this page
- To **PUBLISH** your changes, click the blue "Publish" button in the lower right-hand corner of this page
- If you need help or have questions, please contact Site Admin: Sally.Johnson@louisiana.edu

Table of Contents

Spaces

- All Spaces

CVDI 2017 IAB Fall Meeting

CVDI 2018 IAB Fall Meeting

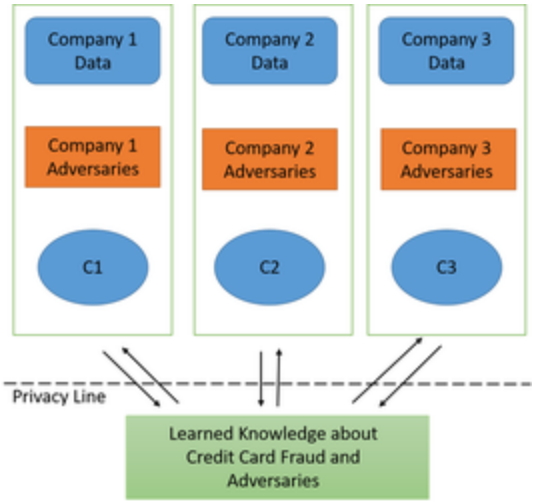
CVDI 2018 IAB Spring Meeting

CVDI 2019 IAB Fall Meeting

CVDI 2019 IAB Spring Meeting

CVDI Calendar

CVDI Leadership



Project - Deliverables

	Deliverable
1.	Literature review
2.	Develop and test GAN for continuous data
3.	Develop and test alternative methods for discrete/categorical data GANs
4.	Develop architecture for joint continuous/categorical GANs
5.	Test GAN performance in public (i.e. no differential privacy) setting
6.	Build differential privacy into the discriminator model and re-evaluate
7.	Introduce multi-party setting with heterogeneous data
8.	Performance benchmarking

Project - Benefits to IAB

- This project will provide the ground work for competitors to be able to collaborate to solve industry wide issue without disclosing private information.
- Companies that are involved in an adversarial environment will benefit from the adversarial models developed in this project

Project - Presentation Video (Spring 2018)

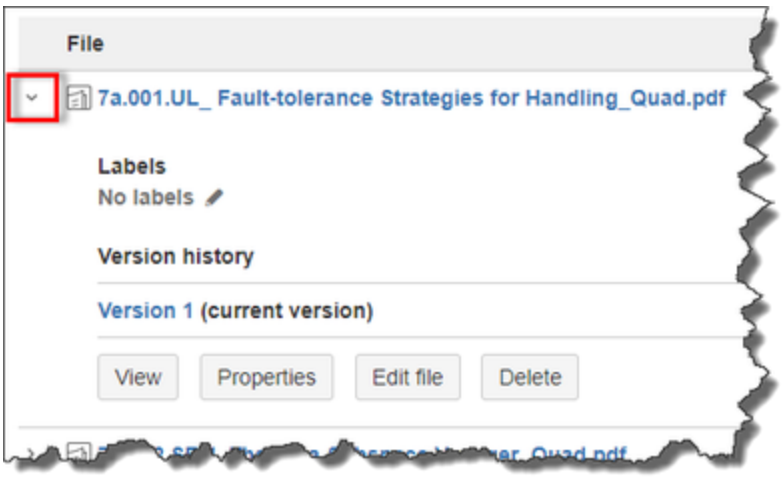
Video Link (9:03 minutes)

Project - Documents

For viewing/editing options, please click left arrow next to document name.

You will see different options depending on your access level.

(All Sites)
CVDI Marketing Materials
CVDI Reports & Document Library
CVDI SITE (Drexel University)
CVDI SITE (Stony Brook University)
CVDI SITE (Tampere University)
CVDI SITE (University of Louisiana at Lafayette)
CVDI SITE (University of North Carolina at Charlotte)
CVDI SITE (University of Virginia)
IAB - Industry Advisory Board
Year 6 - Funded Projects (7/1/17 - 6/30/18)
Year 7 - Funded Projects (7/1/18 - 6/30/19)
Year 8 - Proposed Projects



File	Modified
image2017-11-15_10-48-48.png	Nov 15, 2017 by Sally Johnson
7a.013.UVA_Privacy-Preserving Analytics in Adversarial Environments_Quad_2017 Fall Meeting.pptx	Nov 15, 2017 by Sally Johnson
7a.013.UVA_Executive Summary.docx	Feb 28, 2018 by Sally Johnson
7a.013.UVA_Quad Chart_2018 Spring Meeting.pdf	Mar 15, 2018 by Sally Johnson
7a.013.UVA_Poster_2018 Spring Meeting.pdf	Mar 15, 2018 by Sally Johnson
7a.013.UVA_2018 Fall Meeting Poster.pptx	Nov 13, 2018 by Sally Johnson
7a.013.UVA_Year 7_CVDI Mid-Year Report.docx	Dec 13, 2018 by stephen adams

Drag and drop to upload or browse for files

Download All

Project - Comments