Cojag Smart Technology Pvt Ltd
Address:- Flat 202, Shyam Palace,
Near Oyster English School,
Manish Nagar, Nagpur 440015.
Telephone:- +91-7410747036
Web:- www.cojag.com
Also visit on www.fb.com/cojag

About Cojag:-

Cojag Smart Technology Pvt.Ltd operating under the trade name COJAG is an Indian technology oriented startup. Cojag was founded as an aim to develop an Internet of things (IoT) devices in IIT Kharagpur, but it's now based in Nagpur. Our aim is to create a unique world by amalgamating technology.

We are a group of young enthusiastic technocrats currently creating our footprints in various domains of IoT sector, agriculture, education and consultancy services. The firm also provides platform to young talent with a vision of acknowledging and materializing their innovative ideas. We have major investments in IoT, Analytics, Machine Learning, Artificial Intelligence, Web & App development and Hardware modelling. We promote the idea of co-working space and provide industrial space on rent to set up new plants.

If you are a startup, small or medium sized enterprise, you can benefit by engaging us in any or all of your areas from product ideation till it become live. The beauty is that we associate ourselves closely with you to ensure the strategies are executed with finesse to deliver results.

Machine learning

Summary

Despite progress during the past decades secure operation of computing systems and components continues to be a fundamental research challenge. Unfortunately, the increasing sophistication of defence mechanisms has resulted in a progressive evolution of increasingly sophisticated attacks.
As a result, the majority of computing systems are still plagued by common vulnerabilities that can readily be exploited by attackers. The concerted efforts of industry to resolve these challenges have resulted in the creation of new hardware security standards.
Machine learning is a core sub-area of artificial intelligence as it enables computers to get into a mode of self-learning without being explicitly programmed. When exposed to new data, computer programs, are enabled to learn, grow, change, and develop by themselves. This workshop provides the opportunity to focus on machine learning while
In corporating the relevance of other related disciplines to foster collaborative efforts in this area.

Abstract

This workshop will bring together various groups concerned with advancing research into improving the trustworthiness in machine learning. The workshop format provides the opportunity to keen focus on machine learning while examining the application of related trust technologies in order to foster collaborative approaches and information exchange in this area. Our aim is to fill the gaps in current re- search. The workshop will result in identification of gaps in current research and recommendations for potential research directions.

Introduction

This workshop, convened to explore the practical application of Machine learning technology to inspire collaborative opportunities and future information exchange among the organization, industry and academic participants. The workshop will target at developing a shared appreciation for the application machine learning the workshop agenda focused on presentations and research papers that help characterize the application of the current machine learning technologies and frame the necessary research to advance the field. The breakout session discussion aimed to identify the difficult challenges in supporting machine learning.

Workshop Goals

While individual technologies already provide enhanced security capabilities, the greatest challenges still lie ahead in combining these technologies in ways that will enable secure,

robust, and manageable trusted systems and components to become the norm for the next-generation of machine learners. The key to addressing these challenges appears to be research in trust-enabling infrastructure and application to machine learnings.

This workshop focused on identifying, supporting, and driving interdisciplinary research activities to address the security challenges relevant to machine learnings. The two-day workshop is intended to foster further collaborative research among academic, industry, and government technologists, linking industry's experience in the development.

Goals for the workshop included:

Students should be able to apply practical knowledge in the field of machine learning.
Build a shared understanding of the following:

- currently available means of instilling machine learning,
- practical limitations bounding that trust within current implementations,
- Promising areas for future research and practice.
- Identify research areas necessary to address the security challenges relevant to embedded systems.
- Produce a summary report on promising research areas, benefits to DOD, and projected timeframes (e.g., for practical application of the proposed research).
- Make contacts for future information exchange and possible collaborative research projects.

Workshop Format and Plenary Sessions

The workshop agenda is a combination of plenary sessions and breakout sessions. The sessions is designed to develop a common perspective on currently available means of instilling machine learning, practical limitations, within current implementations, and promising areas for future research and practice. This workshop will bring together disparate groups to gain a broad perspective of the problem.
Each workshop participant is invited based on their active engagement in research and/or acquisition of either machine learning or artificial intelligence. Our main focus will be on practice with keynote and panel sessions covering challenges and current problems to lay a foundation for shared understanding.

There will be sessions and every group or individual will participate in a problem panel that laid out the problem-set from the view

Introductory Presentations

Introductory presentations is used to set the context of the areas of machine learning and trusted computing in preparation for discussions of the possible overlap and future

opportunities. We will present the challenges that need to be addressed in order to build trustworthy machine learning system.
Problem Panel

Following the introductory presentations, a problem panel session will be held to expose the problem from the perspective of the students and the researcher. The Problem Panel may include any groups (BCA, MCA, BSc. MSc., B. tech, M. tech as well as Ph.D.)

Summary of Plenary Session – Day 1

The initial plenary session is framed as such the challenges and potential gains for necessary research**.**
Also this will include

- Introduction to machine learning,
- Machine Learning Process
- Unsupervised learning techniques
- Detailed study from basics of machine learning
- What is machine learning,
- Why is it becoming so popular?
- Brief explanation about this and everything students need to know about the technology from R-Programing, MATLAB – what it does, how it works
- The way it's affecting how we do business.
- Why is machine learning important?
- What's required to create good machine learning systems?

Summary of Plenary Session – Day 2

We will be focusing on

- Supervised learning techniques and case studies ,
- Ensemble Learning,
- Machine Learning Tools/Framework
- Conclusion with all participants engaging in a brainstorming session to identify current gaps in research in the area.
- Case studies
- Also Participants were invited to inform the workshop attendees of their current research and early results.

Break Out Session – Day 1

Following the problem panel the workshop participants will break into three separate groups with each group challenged to describe a realistic scenario that relied on machine learning and required security.

Each group was free to capitalize on the expertise and interests of their constituents to develop a scenario.
The teams received no guidance or restrictions on what scenario to describe, making them rely on advocacy to emerge from the expertise within each of the teams.

The intention of this exercise was not to derive realistic threats or defense strategies. The goal was to encourage the participants consider the range of the threat environment to on machine learning and the hard challenges of securing faced during this systems.

Summary of Plenary Session - Day 2

Day two of the workshop focused on research. Participants were invited to inform the workshop attendees of their current research and early results.

Current Research Reports

Students will share their current research with the workshop attendees.

Case Study

Students will be explored/ demonstrated with a Case Study relevant to this workshop.

Registrations starting from 1st Sept, 2017

Feel free to contact us on +91 7410747036
And you can reach us cojag@cojag.com, akshita@cojag.com , informcojag@gmail.com , akshitabhonsale93@gmail.com