COURSE OBJECTIVES

- This workshop is designed to provide a deeper understanding of Cyber Security and Malware.
- The main goal of this workshop is to introduce participants to the fundamental and applications of Machine Learning (ML) in Cyber Security by giving them a shared forum to communicate with experts.
- It aims to deliver a content on Android malware, static and dynamic analysis of malware using appropriate tools and datasets.
- It aims to provide an overview of the DNS ecosystem, DNS abuse and security measures.
- It focuses on applying ML for Document-based malware.
- It aims to extract features of malware executables in virtualized environment.
- It aims to introduce Memory Forensics.
- It aims to teach the participants on Deep Learning (DL) models for malware analysis.

RESOURCE PERSONS

The course content will be delivered from a pool of resource persons on the subject from leading prestigious academic institutions and Industries such as CDAC and CISCO.

INFORMATION FOR PARTICIPANTS

- The proposed workshop is meant to support motivated **PG and Ph.D. level students**, who are having a strong willingness to get excellence in their scientific and engineering research pursuits in the area of ML and Cyber Security.
- **Course Registration is free** for all the participants.
- **Seats are limited (only 25)** and the participants are selected by organizers on **first come first served basis.**
- Shortlisted candidates will be informed through email with the link for google form to submit NOC.
- Shortlisted candidates should submit NOC, then only their participation will be confirmed.
- On completion of the course, an objective/quiz-based assessment of all participants will be done.
- TA will be provided to all the participants by producing the tickets with shortest route as per the norms.
- The workshop will be conducted in face-face mode.
- Food and accommodation will be provided at a free of cost.

REGISTRATION

Participants interested to attend this program should register online in the below mentioned link:

https://forms.gle/GLSdHB9gWP5okFDF9

Last date for Registration: 12th Jan 2023

Selection Intimation by email: 13th Jan 2023

Participants Confirmation: 14th Jan 2023

The selected Ph.D./P.G students should **provide the NOC from the supervisor or HOD** of respective institution.

ORGANIZING COMMITTEE

Patron

Dr. N V S N Sarma, Director

Chair

Dr. R. Dhanalakshmi, Associate Professor, HoD

Coordinators

Dr. N. Renugadevi, Assistant Professor/CSE

Dr. M. Senthil Sivakumar, Assistant Professor/ECE

CONTACT DETAILS

Dr. N. Renugadevi

Department of CSE, IIIT Tiruchirappalli.

Email: *workshopandfdp@gmail.com*

For Further Assistance:

Ms. S. Divya, *Research Scholar*

Phone no: 8610846406

Science & Engineering Research Board (SERB)

(ACCELERATE VIGYAN SCHEME)

High End Workshop (Kaaryashala)

Science & Engineering Research Board (SERB)

ACCELERATE VIGYAN SCHEME

Sponsored

High End Workshop

On

"Machine Learning For Cyber Security"

From 18-01-2023 to 24-01-2023

Department of Computer Science and Engineering,

Indian Institute of Information Technology, Sethurapatti, Trichy-Madurai Highway, Tiruchirappalli, Tamil Nadu - 620012

www.iiitt.ac.in

ABOUT SERB

SERB has a vision to position science and technology as the fulcrum for social and economic change by supporting competitive, relevant and quality scientific research and development. As the premier national research funding agency, the mission is to raise the quality and footprint of Indian science and engineering to the highest global levels in an accelerated mode, through calibrated, competitive support of research and development.

Although a nascent organization, SERB can trace its existence to the erstwhile Science and Engineering Research Council (SERC), a division of DST that provided extramural funding for S&T research in India for more than four decades.

ABOUT ACCELERATE VIGYAN

"Accelerate Vigyan" (AV) strives to provide a big push to high-end scientific research and prepare scientific manpower which can venture into researchcareers and knowledge-based economy. Recognizing that all research has at its base as development of quality, well-trained researchers; AV will initiate and strengthen mechanisms of identifying research potential, mentoring, training and hands-on workshops, on a broad-based national scale.

The aim is to expand the research base in the country, with three broad goals - consolidation / aggregation of all scientific training programs, initiating High end Orientation Workshops and creating opportunities for Training and Skill Internship.

ABOUT INSTITUTE

The Indian Institute of Information Technology Tiruchirappalli (IIITT) was established in the year 2013-14 as the Institute with National Importance under Public Private Partnership Mode by the Ministry of Human Resource Development (MHRD), Govt. of India.

The Stakeholders of IIITT are Central Govt. of India, State Govt. of Tamil Nadu, and Industry partners, viz., TCS, CTS, Infosys, Ramco Systems, ELCOT, and Navitas

A major objective in establishing IIITT is to set up a model of education which can produce best-in-class human resources in IT and harnessing the multidimensional facets of IT in various domains. The focus of IIITT is to address the challenges faced by the Indian IT industry and growth of the domestic IT market. IIIT Tiruchirappalli has started operating from the permanent campus at Sethurappatti, Trichy- Madurai Highway, Tiruchirappalli, Tamil Nadu- 620012.

ABOUT DEPARTMENT

The Department of Computer Science and Engineering aims to deepen the knowledge and skills of the students on the basic concepts and theories that will equip them in their professional work involving analysis, system implementation, programming, networking, and maintenance of the various web applications.

ABOUT THE WORKSHOP

This workshop on ML for cyber security aims to bring together researchers from academia and industries, especially early career researchers and PhD students. In the ever-changing cyber threat landscape, cyber security has become more vital than ever. The capability to detect, analyze, and defend against threats in real-time conditions is not possible without employing ML techniques. ML-based developments in cyber security field promise to be a great solution, helping cyber security experts stay ahead of threats.

The main goal of this workshop is to introduce participants to the fundamentals and latest developments in ML-Based Cyber Security by giving them a shared forum to communicate with experts. This program will serve as a platform for gathering and sharing precise ideas about ML-Based Malware Detection with researchers who are already active in this field. This initiative also inspires research ideas with useful applications by the experts.

Topics to be covered:

- Cyber Security, Malware and Malware Analysis
- Android Security- Architecture, Static and dynamic analysis for android malware.
- Training ML Models, Model Evaluations and Data Processing.
- Introduction to DNS Ecosystem.
- Fundamentals and Feature Extraction of malware executables in virtualized environment.
- Memory Forensics.
- Document Malware Analysis.

Hands-On Sessions:

- Android Security- Tools - API-Monitor, Monkey, strace, DroidBox etc, Datasets - DroidBench, MalGenome, Drebin, CICAndMal2017, Contagio Minidump etc
- Training ML Models, Model Evaluations and Data Processing.
- Setting up DNS servers and DNS abuse and Security Measures.
- Malware: under the hood- ollydbg, ghidra
- Tools and Dataset for Virtualized environment.
- Memory Forensics using tools
- ML for Document-based malware: Extracting right attributes, trends and models
- ML and DL models for malware analysis.

EXPECTED OUTCOME

At the end of the program, the participants shall able to

- Understand the fundamentals of malware analysis on ML Models and set preventative measures against data misuse into action.
- Be aware and concerned about Cyber Security risks and Memory forensics.
- Extract the right attributes from Document-based malware using ML.
- Identify threats, attacks and defenses for Android security.
- To have a clear idea on DNS abuse and security measures.
- Use ML and DL models for malware analysis.