Eligibility

The workshop is open to Faculty, research scholars, students from Computer Science and Forensics Science, Industry and Law enforcement officers.

Registration

Participants can register using the following link

https://forms.gle/vaogsggWHRMqbbVh6

Registration Fee: Rs. 500 + 18% GST

The payment should be done through:

A/C Name : Head , Department of Computer Applications

A/C No : 67216724749

IFSC : SBIN0070235

Last date for registration 12 Dec 2020

Workshop Coordinator

Dr. Vinod P
Professor
Dept. of Comp. Applications, CUSAT

Workshop Joint Coordinators

Dr. Sabu M K
Professor & Head, DCA, CUSAT

Dr. A Sreekumar
Professor, DCA, CUSAT

Dr. Judy M.V
Professor, DCA, CUSAT

Rafidha Rehiman KA
Assistant Professor, DCA, CUSAT

Contact Us

Vinod P
94971 79735
vinod.p@cusat.ac.in

Rafidha Rehiman K A
99471 42132
rafidharehimanka@cusat.ac.in

International Workshop on

INFORMATION AND NETWORK SECURITY CHALLENGES AND SOLUTIONS USING ARTIFICIAL INTELLIGENCE APPROACHES

14 -18 Dec 2020

COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY

Organized by

Cyber Intelligence Research Lab
Department of Computer Applications
Cochin University of Science and Technology
Cochin - 682022
Kerala

CUSAT

Cochin University of Science and Technology (CUSAT) was established in 1971 for Higher Education with particular emphasis on Post Graduate studies in applied sciences, technology, industry, and commerce. The University's basic philosophy and goals find eloquent expression in its Coat of Arms emblazoning the motto "Tejaswinavadhitamastu" and to focus on knowledge integration , generation and dissemination.

Dept. of Comp. Applications

Computer Application is one of the thrust areas in Science and Technology. In appreciation of its growing importance in business and the industrial scenario, the University established a Department of Computer Applications to facilitate research and human resources development in the subject.

About the Workshop

Information and Network Security Challenges and Solutions using Artificial Intelligence Approaches.

The massive number and volume of heterogenous connected devices in an open space, as well as the advancements in Human Computer Interaction (HCI), Artificial Intelligence (AI), computing and communication technologies have led to an increasing number of personal and ubiquitous intelligent systems. Such a wide deployment of connected smart technologies introduces new challenges to system security and privacy computing systems. Therefore, innovative security methods and privacy protection solutions are needed to provide more secure and robust privacy-preserving intelligent systems. To achieve this, security systems need to adapt to the changing cyber security threats with minimal user intervention to provide maximum protection against cyber-attacks, intrusions, malware and various types of data breaches. AI has the potential to be leveraged in different aspects of cybersecurity and cyber threat detection. It has received significant interest lately, where a plethora of AI and other intelligent learning solutions are now being integrated into cybersecurity systems to provide more secure and robust privacy-preserving solutions for personal and ubiquitous systems. Such integration will play a vital role in providing enhanced security for intelligent autonomous systems and enables organizations to make crucial changes to their security landscape. This aims at providing recent advances in security network and system management solutions using AI. Topics of interest include

- Security, privacy, and trust issues in cyber space.
- Utilizing AI technologies for cyber investigation and threat intelligence.
- AI and ML for intrusion detection/prevention in sensitive environments.
- Trust management in cyber-physical networks and systems.
- Cybersecurity management to protect organizations' sensitive data using intelligent learning techniques.
- Malware Reverse Engineering.
- Machine learning and Deep-learning-based detection of mobile malware.
- Adversarial machine learning techniques.
- Computer Forensics, Network Forensics and Live Memory Forensics.

Resource Persons

1. Prof. MS Gaur, IIT Jammu
2. Prof. Vijay Laxmi, Malaviya NIT, Jaipur
3. Prof. Akka Zemmari, LaBRI Research Lab, University of Bordeaux, France
4. Prof. Suleiman Yerima, De Mont Fort, UK
5. Dr. Parag H. Rughani, Associate Professor, (Digital Forensics), National Forensic Sciences University, Gandhinagar, Gujarat – India
6. Dr. Corrado Aaron Visaggio, Associate Professor Dept. of Engineering, University of Sannio, Italy
7. Dr. Nicola Laurenti, Associate Professor, University of Padua, Italy
8. Dr. Jyoti Gajrani, Govt. Engg College, Ajmer, Rajasthan
9. Dr. Riccardo Spolar, School of Computer Science and Technology, Shandong University, Qingdao Campus, R.P.China
10. Sri. Shyam Sundar Ramaswami, Head of Threat research group for Asia Pacific, Cisco, Bangalore, India
11. Sri. Bhavik Shah, CISCO Security TAC, Bangalore, India
12. Sri. Swapneel Patnekar, MD of Shreshta IT Bangalore, India
13. Prof. Sreekumar A, DCA, CUSAT
14. Prof. Vinod P ,DCA, CUSAT