

National Workshop on Deep Learning for Cyber Security – 6,7 March 2020

Speakers' Profile



Dr R Chidambaram

Inaugural Address

Dr R Chidambaram,
(Homi Bhabha Professor, BARC and Former Principal Scientific Adviser to the Government of India)



Dr. Ravindran B
IIT-Madras

Keynote Address

Dr Ravindran is a Professor at the Department of Computer Science and Engineering at the Indian Institute of Technology Madras and a Mindtree Faculty Fellow. He heads the Robert Bosch Centre for Data Science and AI at the Indian Institute of Technology, Madras. He completed his Ph.D. at the Department of Computer Science, University of Massachusetts, Amherst. He has worked with Prof. Andrew G. Barto, a pioneer in the field of Reinforcement Learning on an algebraic framework for abstraction in Reinforcement Learning. His academic work spans across over two decades and has produced 170 research papers. As part of his Ph.D. work on RL, Ravindran introduced the notion called SMDP (Semi-Markov Decision Process) homomorphisms. He has around 400 citations across the different papers he has written on symmetry.

Ravindran's research work also revolves around making useful tweaks on existing deep RL algorithms. The survey paper on Reinforcement Learning that he made along with his master's thesis advisor grew so popular that Oxford University Press invited them to write a chapter in their handbook on neural computation. His current research interests span the broader area of Machine learning, ranging from Spatio-Temporal Abstractions in Reinforcement Learning to Social Network Analysis and Data/Text Mining.



Dr. P V Ananda Mohan
C-DAC, Bangalore

Keynote Address - Deep Learning / AI for Hardware Security

Dr P V Ananda Mohan obtained his Ph D degree from IISc, Bangalore in 1975. Since 1973, he has worked at the R & D, ITI Limited, Bangalore at various levels for more than three decades and was heading the R & D division of ITI Limited, Bangalore. Then he moved to ECIL, Bangalore as Executive Director and Later to C-DAC, Bangalore as Technology Advisor. He has published five books on Analog Filters and Residue Number Systems and several papers in IEEE transactions and IETE Journals. He is Life Fellow of IEEE, fellow of National Academy of Engineering and FIETE.



Dr. Arun Balaji Buduru,
IIIT-Delhi

TOPIC: Cybersecurity and Deep Learning – Intelligence through Data Integration

Abstract: Cyber systems, including Internet of Things (IoT), are increasingly being used ubiquitously to vastly improve operational efficiencies and reduce costs in critical areas, such as finance, transportation, defence, healthcare. Over the past two decades, dramatic improvement in computing efficiencies and hardware costs have made most of our today's economy increasingly ever more digitized. It is important to note that such wide spread use of devices for providing various services has resulted in generation of large amounts of rich user data which needs to be protected. Emerging trends in successful targeted cyber system breaches have shown increasing sophistication, with most of them using intelligence generated through collection and integration of publicly available data. Such sophisticated attacks can only be thwarted by defence mechanisms which rely on specific actionable intelligence. Although it is true that more data from diverse sources are available, such data may not automatically translate to actionable intelligence. In fact, translating large quantities of such diverse datasets into actionable intelligence is a non-trivial process. It involves identifying and integrating useful pieces of information from large quantities of noisy and biased datasets. In this talk we will discuss some useful deep learning techniques and various challenges in generating actionable pieces of intelligence utilized for thwarting such sophisticated targeted attacks.

Profile: Dr Arun Balaji Buduru is an Assistant Professor at Indraprastha Institute of Information Technology, Delhi. He received his Ph.D. in Computer Science, specializing in Information Assurance from Arizona State University in 2016. His research interests include cyber security and reinforcement learning. He received his B.E. in Computer Science in 2011 from Anna University, Chennai. He has worked as a research intern as part of Cisco IoT Architecture Group. His current research focuses on Adaptive User Re-authentication on touch-based devices, Differential Privacy, Adversarial Learning, and User Behaviour based Adaptive IoT device reconfiguration.



Dr. A. Shahina,
SSN College of
Engineering, Chennai

TOPIC: An Introduction: Artificial Neural Networks to Convolutional Neural Networks

Abstract: To be updated

Profile: Dr.A.Shahina is a professor in the department of Information Technology at SSN. She has 20 years of teaching and research experience. She obtained her PhD and M.Tech in Department of Computer Science Engineering from IIT-Madras and B.E from Govt. College of Engineering, Salem. She has worked as a project officer for a DRDO-sponsored project at IIT-Madras. Her research interests include Artificial Intelligence, Machine learning, Deep Learning and Speech Processing (using alternate anatomical speech sensors). Her other areas of expertise are Speech

Applications, Man-Machine Interface, Pattern Recognition (especially of physiological signals) etc. She was a co-coordinator in a DIT sponsored project on the Development of Text to Speech (TTS) System in Tamil. She has also worked on several other projects sponsored by SSN trust. Currently, her teaching areas include Artificial Intelligence, Machine Learning and Deep Learning. She has more than 35 research publications, including refereed international journals and international conferences.



Mr. Ramesh Naidu
Laveti,
C-DAC, Bangalore

TOPIC: Towards Trustworthy Deep Learning – Attacks, Defences and Evaluation

Abstract: While back, we are very familiar that hackers modify code. Now, hackers shifted their focus to DATA. With the rapid progress and successes in a broad spectrum of applications, Deep Learning is being applied in many safety-critical applications. However, Deep Neural Networks have been found vulnerable to well-designed perturbed samples, called adversarial examples. Such an adversary can cause Deep Learning to make mistakes in predictions. The vulnerability to adversarial examples becomes one of the major risks for applying deep neural networks in safety-critical applications. In this talk, the details of recent findings of adversarial attacks on deep learning, counter measures and defence methods will be discussed. Further, the evaluation methods of robustness of defences to adversarial examples will be discussed.


Profile: Mr Ramesh Naidu Laveti is currently working as a Joint Director, Big Data Analytics and Machine Learning Group at C-DAC. He has more than 13-years of experience in Deep Learning, Machine Learning, Big Data Analytics and Scientific Computing. He is actively involved in design and development of Parallel Spherical Harmonic Transform Libraries and Math Kernels for Weather and Climate modelling, Prediction of Indian summer monsoon using coupled models and Hybrid Recommender Systems. Lately, his focus has been on the study of neurodevelopmental disorders and epileptic seizures using AI. His areas of interest include: Deep Learning, Multi-Stage Ensemble Methods, Probabilistic Graphical Models and Reinforcement Learning. He has published and presented over 15+ research papers in various Journals and Conferences.





Mr. Amarnath
Chatterjee,
Paladion Networks

TOPIC: Next-Gen Malware Detection and Response using AI and ML

Abstract: In recent times, two issues have posed a tough challenge for cybersecurity experts. Ransomwares and Data Wipers. Data Wipers rose during US and Iran tensions recently. That been said, a discussion on trends in malware detection and response would cater best to the audience expectation. This talk would cover Malware detection and response, Traditional approaches and their short falls, Data Mining based approach, Machine Learning based approach (including deep learning), Destructive malwares (Ransomwares, Data Wipers, and System Hijackers), Next generation malwares, Next Generation of detection and response and Future of cybersecurity.

	<p>Profile: Mr Amarnath Chatterjee, Principal Data Scientist is associated with AVP - Products, Paladion Network since 2010 and is currently supervising design and development of Paladion EDR (Endpoint detection and Response) agents. He has 15 years of overall experience in IT sector and 10 years in information security. He is an Endpoint Compromise Assessment and Threat Hunting Practitioner. He also handles Malware Forensics and Investigation services.</p>
 <p>Dr Balamurali A R Acalvio Technologies</p>	<p>TOPIC: Mitigating Cyber Attacks through Deep Learning</p> <p>Abstract: The breakout time of cyber intrusion has been steadily decreasing over the years. The reasons for this are plenty; from better efficacy of hackers in compromising systems to fatigue of security operatives' due to large-scale false positives. In this talk, we look at the security industry perspectives of- securing an enterprise as well as detecting breaches. To do so, we categorize different tactics and techniques attackers might use, and accordingly design a plan to secure the enterprise. We leverage MITRE ATT&CK threat model to accomplish the same. Irrespective of elaborate safeguards, attacks are bound to happen. We look at two tactics: command and control (C&C) detection and exfiltration and see how Deep learning can be employed to mitigate the damages. For C&C detection, we model it as sequence learning problem and leverage LSTM based model to identify spurious url links. For Exfiltration, we study anonymous traffic emanating from the enterprise and how it can be detected using a deep Feed forward estimator.</p> <p>Profile: Balamurali A R obtained his PhD degree from IIT Bombay and Monash University, Australia. He pursued his postdoctoral studies in conversation analysis at LIF labs, CNRS, in Marseille, France. He has worked with Samsung R&D and was a visiting Faculty to IIM V. At present he is working as a Principal Data Scientist at Acalvio Technologies. He holds various patents and has published his research in prestigious international conferences.</p>
<p>Ms. S. Irene, C-DAC, Chennai</p>	<p>TOPIC: Similarity Learning using CNN</p> <p>Abstract: For the past few years, deep learning models are used extensively to solve various machine learning tasks. It has proven itself as a successful set of models for learning useful representations of data. These representations are used to distinguish between available classes. The representations from semantically similar classes will be located nearby, while those of semantically dissimilar classes will be located far apart. This presentation gives an introduction to similarity learning which is the process of training a metric to compute the similarity between two classes.</p> <p>Profile: Ms. S. Irene is a Joint Director at the Centre for Development of Advanced Computing (C-DAC), Chennai. She has been working in C-DAC</p>

	<p>since 2006. Her research interests include machine learning, human activity recognition, context reasoning and inter-operability. She completed her M.E in VLSI Design from Government College of Technology, Coimbatore and is pursuing her Ph.D. at the Anna University. She has 1 patent, 4 research publications in International and 4 research publications at National conferences. Her current research focuses on Deep Learning and Computer Vision.</p>
 <p>Mr. Tapas Saini, CDAC- Hyderabad</p>	<p>TOPIC: Deep learning-based Face Biometrics</p> <p>Abstract: Face biometrics is an area of fetching unique face features from images and utilizing these features of biometrics authentications and identification purposes. Machine learning and Deep learning has proven successful in object identification on images in recent times. This has shown that deep learning models can process images to solve many problems. Face biometrics on images is another area on which deep learning models have state of the art results. We will try to understand the modus operandi of deep learning models on face images. Additionally, we may explore ML/DL techniques in cyber security domain.</p> <p>Profile: Mr. Tapas is working as a Principal Technical Officer at CDAC Hyderabad. He has been associated with CDAC for past 14 years. He has worked on various domains of computing like wireless sensor networks, routing protocol design, smart parking system, Road Traffic demand estimation through mobile phone data, genetic algorithms, machine learning, computer vision and deep learning. He has fetched international awards for project work, papers in reputed IEEE conferences and filed 1 patent. Currently he is working on video analytics domain with applications of DL.</p>
 <p>Dr. N. Sarat Chandra Babu, SETS, Chennai</p>	<p>TOPIC: Transfer Learning for Cyber Security</p> <p>Abstract: Growing concerns of Cyber-attacks and ever-increasing threat canvass, has led the researchers across the globe to look at new ways of addressing challenges posed by the cyber-attacks. Artificial Intelligence and ANNs encompassing ML/ DL algorithms have been considered widely by the researchers in different domains. In this context Cyber security is no exception. There are number of AI tools/ products to address use cases such as Network threat analysis, malware detection, security analyst augmentation, AI based threat mitigation etc.</p> <p>Transfer Learning – a concept where knowledge of the already trained machine learning model is applied to a different task/ domain but to a related task/ domain. Transfer learning will be beneficial, especially when the related task/ domain is not having enough labelled data. This would also help in improving the efficiency of training in terms of reducing computational requirements and also the training time. This talk covers basics of transfer learning, different approaches, its benefits and also</p>

considers how it could be used in network security problems.

Profile: Dr. Sarat is presently working as the Executive Director of Society for Electronic Transactions & security (SETS), Chennai. He obtained his Ph.D. from IIT, Delhi. He has considerable experience of Four decades in R&D, Project implementation and Co-ordination, Education & training. At SETS he is leading the cyber security teams working in Hardware Security, Cryptography (Post quantum & QKD), and Network Security. Prior to joining SETS, he worked as Executive Director, C-DAC Bangalore and he was Founder Director of C-DAC Hyderabad. He worked at Department of Electronics, Govt. of India (Presently MeitY) at various levels. He has earlier worked at Indian Telephone Industries Ltd., Bangalore and as faculty at REC, Warangal (presently NIT, Warangal). He took lead in arriving at the Feasibility study report of India Microprocessor. He designed a six months diploma in Embedded Systems Design, now popular as DESD at C-DAC. Responsible for conducting many National conferences, Workshops such as Think parallel; ParCompTech; ElelTech; WORTICS etc. He has published around 70 papers in various National and International Journals & Conferences.



Shri. R. Pitchiah
SETS, Chennai

TOPIC: National Strategy on Artificial Intelligence and Cyber Security (AI-CS)

Abstract: Artificial Intelligence (AI) and Machine Learning (ML) are rapidly advancing technologies and many applications ranging from machine translation to medical image analysis are being built and demonstrated. In addition, AI and ML technologies can contribute to improving cyber security defence capability to protect from ever- growing sophisticated cyber -threats. While AI is enabling more automated defence systems, it is simultaneously enabling more sophisticated attacks.

Many advanced countries have come out with discussion papers and plan to address the impact of AI/ML in their national economies. There have been efforts to introduce AI within their departments in an effort to develop effective strategies against cyber-attacks. It is imperative for us to build self-reliance in Technology development in "Cyber Security Tools using AI/ML and building secured AI/ML systems and applications" for protecting our ICT systems including critical infrastructure. In this presentation, a brief survey of initiatives on AI-CS by international institutions, and by SETS on AI-CS Project Management Unit (PMU) will be presented.

Profile: Shri.R.Pitchiah is currently functioning as Technology Adviser at Society for Electronic Transactions and Security (SETS), Chennai and coordinating the AI-CS Project Management Unit. He served in the Ministry Electronics and Information Technology, MeitY (formerly Department of Electronics), Government of India, for more than 37 years, in various capacities and as Senior Director / Scientist- "G" from 2014-2018. He was responsible for initiating R&D projects in areas Convergence, Communications and Broadband Technology including next-generation communication systems, 5G, Internet of Things, Cyber Physical

Systems, strategic and critical communication systems such as Software Defined Radio, MANET. As Senior Director, MeitY, he served many technical committees as a member including, Steering Committee, “5G India 2020 Forum”; Steering Committee, Centre for Development of Telematics (C-DoT); Research Advisory Committee (RAC), Society for Applied Microwave Research in Engineering (SAMEER) and Governing Council, Centre of Excellence in Wireless Technology, CeWiT, IIT Madras.

He functioned as Group Coordinator, Real-time Systems Development Group at Centre for Development of Advanced Computing (C-DAC), Bangalore, on deputation, and was leading the development of real-time fault-tolerant systems and development and engineering of RTUs. He was responsible for initiating National Ubiquitous Computing Research Programme from the Ministry, and leading the development of smart home artefacts such as Interactive Mirror, Smart Kitchen cabinet and Smart Bed for predicting sleep disorders. He was leading the development of Zigbee based Home-area Network, Occupancy based LED Lighting, HVAC and Indoor Air Quality as part of “Development Smart building technologies with low carbon emissions” project at C-DAC.

Shri.R.Pitchiah obtained his M.E. degree in Electronics and Communication from Delhi College of Engineering, Delhi University. He was a research scholar at Indian Institute of Science, Bangalore and completed the course work requirements, under the External Research Programme. He was an UNIDO Fellow in the area of “Microprocessor based control of Process Plants,” at Liverpool Polytechnic, UK and University of Bremen, Germany. He also visited University of Ghent, Belgium and University of Bremen as part of EEC’s Expert training on “Transputers and Parallel Processing”. He has 25 research publications in International and National conferences, workshops and journals.



Dr. Prem Laxman
Das,
SETS, Chennai

TOPIC: Privacy Techniques in Machine Learning

Abstract: ML techniques are increasingly being used for providing better services like medical, financial and judicial. The usage of highly private and sensitive personal data has led to increased interest in privacy/Anonymity techniques. It may be noted that machine learning algorithms leak some personal information during their execution, which can cause financial or personal loss to the said individual. We will describe how differential privacy techniques can be applied to machine learning.

Profile: Dr M. Prem Laxman Das has completed his Ph.D. in Mathematics from Indian Statistical Institute. He works broadly in the domain of algorithmic aspects of algebra and number theory. In cryptology, his interests include cryptanalysis of public key systems, pairing-based crypto with applications to cloud computing security and aspects of post-quantum cryptography. He has executed a project on cryptography for MANETs funded by BEL. Currently he is working on Artificial Intelligence.



Ms. A.Suganya,
SETS, Chennai

TOPIC: Machine Learning based DDoS Detection and Mitigation

Abstract: Denial of Service attacks are a major threat to the modern electronic society. Carefully crafted attacks of large magnitude, better referred to as Distributed Denial of Service attacks (DDoS) have the ability to cause havoc at the highest level, national information infrastructure. There are multiple perspectives of dealing with the DoS attack problem, in order to mitigate, detect and cope with detected attack. Techniques dealing with each of these aspects can be integrated to make a fool-proof system. An important such perspective in terms of detecting DoS attacks is to view the problem as that of a classification problem on network state (and not on individual packets or other units) by modelling normal and attack traffic and classifying the current state of the network as good or bad, thereby detecting attacks when they happen. Classical machine learning algorithms are used to solve the problem. In this talk, the approach to a carefully engineered, practically realisable system to detect DoS attacks based on a Naive Bayesian classifier is covered. The system is designed to be near the target.

Profile: Ms Suganya Annadurai obtained her M.Tech in VLSI Design from SASTRA University, Thanjavur. In her 15 years of experience at SETS she has developed core competency in side channel analysis and secure and efficient realisation of cryptography modules. Her research interests include Side Channel Analysis attacks and countermeasures, analysis and design of efficient and secure crypto modules for communication systems, ubiquitous devices, and embedded devices. She played a major role in the establishment of Side channel analysis evaluation laboratory at SETS for the evaluation of crypto modules. She has good number of publications in reputed International conferences to her credit.





Mr. Dillibabu S,
SETS, Chennai

TOPIC: Evaluation of Side Channel Analysis using Deep Learning

Abstract: Evaluating the resilience of cryptographic algorithms to side-channel analysis (SCA) is required by several national and private certification schemes, like Common Criteria (CC) and FIPS-140-2/3 standards. A typical SCA evaluation requires a complex end-to-end procedure: an initial Test Vector Leakage Assessment (TVLA), then explore one or several attack methods(non-profiled) to retrieve secret information and finally analyze the strength of countermeasures over cryptographic algorithms. In a state-of-art evaluation process, the framework may not be enough to evaluate the resilience of these primitives. Deep learning has been introduced to evaluate the resilience of crypto primitives hardware realization against side-channel attacks.

Profile: Mr. Dillibabu Shanmugam, is working as a scientist at SETS. His research interest is on Side-Channel Analysis, Quantum Key Distribution, and Post Quantum Cryptography. In SCA, his focus is on exploring hardware vulnerabilities of crypto primitives, upon

	<p>identification of vulnerabilities, he comes up with suitable countermeasures to protect from threats. Finally, the SCA Evaluation framework will be Security-as-a-Service (SaaS) for strategic sectors. Also, he has published many papers in this domain and he is a SANS, GSec certified professional.</p>
 <p>Mr. Thirupathi, SETS, Chennai</p>	<p>TOPIC: Dataset preparation methods for Intrusion Detection Systems</p> <p>Abstract: Intrusion Detection and Prevention System have become an important security tool in overall security architecture. To simulate an IDS model, huge amount of data are required to train and testing the model. While preparing dataset, feature extraction is the most important pre-processing step. The feature extraction process consists of feature construction and feature selection. The quality of the feature extraction is one of the most important factors that affects the effectiveness of an IDS model accuracy. Real-world scenario availability of dataset is extremely rare, because from one side, many dataset are internal and cannot be shared due to privacy issues, and on the other-hand datasets are heavily anonymized and do not reflect current trends, or they lack of certain statistical characteristics, so a perfect dataset is yet to exist. This talk provides an overview of feature extraction techniques and dataset preparation in network traffic.</p> <p>Profile: Mr Thirupathi K is currently working as Scientist at SETS, Chennai. He did his M.Tech in Cyber Security from Amrita University, Coimbatore. He has more than seven years of experience in developing Network Security products and providing cyber security solutions to the end user. His areas of research include Cyber Security, Internet Traffic Analysis, Machine Learning and the detection of network attacks. He has played a key role in the development of network security products like Unified Threat Management (UTM) devices and Network Security Monitoring (NSM) products at SETS. He is also a Certified Ethical Hacker and a Cisco Certified Network Associate (CCNA).</p>
 <p>Ms. Eswari Devi N, SETS, Chennai</p>	<p>TOPIC: Supervised Learning - Recurrent Neural Network for Cyber Security</p> <p>Abstract: Cyberattacks are widely increasing in day today scenario. Human intervention on cyberattacks for all time becomes impossible. So deep learning methods can be used for examining the presence of attack and to notify / act upon the same to prevent loss of data and to reduce the impact of attack. Recurrent Neural Networks can be used for such an application for ensuring security and safety of the data.</p> <p>Profile: Ms Eswari Devi is working in SETS as a Project Associate in the area of Artificial Intelligence for Cybersecurity. She has completed her M.E</p>

	<p>in VLSI Design as a first rank holder from Kongu Engineering College and awarded as the ‘Best Outgoing Student’ in her UG programme. Her research interests include implementation of Deep Learning algorithms for cybersecurity and implementation of Deep Learning algorithms in creating an efficient floorplan in VLSI Design.</p>
<div data-bbox="217 396 440 651" data-label="Image"> </div> <div data-bbox="217 680 408 750" data-label="Caption"> <p>Ms Samyuktha, SETS, Chennai</p> </div>	<p>TOPIC: Unsupervised Learning in Neural Networks- Auto Encoders and RBMs for Spam Filtering</p> <p>Abstract: Unsupervised learning from Deep neural networks has always been a concept not very familiar to many of the AI novices. This talk would be a detailed focus on Auto-Encoders and Restricted Boltzmann Machines, two of the most widely used Unsupervised Neural Networks. The talk also covers the major differences in both the neural networks on the bases of loss functions, activation functions and implementation.</p> <p>Profile: Ms Samyuktha is currently working as Network Security Analyst at SETS, Chennai. She did her bachelors in Information and Communication Technology from SASTRA University, Thanjavur. She has been rewarded as the ‘Best Outgoing Student’ in her U.G. Programme. She is a SETS Certified Ethical hacker and was the topper of the SETS Certification on Advanced Network Security (SCANS, 2019) course. Her areas of interest include Network Security, Ethical Hacking and Deep Learning.</p>