

**SRI VENKATESWARA COLLEGE OF ENGINEERING (SVCE)
PENNALUR, SRIPERUMBUDUR-602117
(An Autonomous Institution)**

DEPARTMENT OF INFORMATION TECHNOLOGY

**REPORT ON AICTE SPONSORED ATAL FDP ON DEEP LEARNING FOR CYBER
SECURITY**

SPEAKERS: Mr.Maithili Sharan Gupta. Retired DGP, Madhya Pradesh, Mr.Krishnan Balaji, Principal, Maharishi Patanjali College of Yoga, Mangadu, Chennai, Dr.G.Sumathi, Professor, Department of IT, SVCE, Chennai, Ms.D.Jayanthi, Assistant Professor, Department of IT, SVCE, Chennai, Mr.Thiruppathi, Scientists, SETS, Chennai, Mr.Nithiyanandam Ramesh, Technical Consultant, Corporate, Chennai, Dr.N.Bhalaji, Associate Professor, Department of IT, SSN College of Engineering, Chennai, Dr.K.B.Sundharakumar, Assistant Professor, Department of IT, SSN College of Engineering, Chennai, Mr.Vijayan Muralidaran, Manager, Information Security, Corporate, Chennai, Mr.Ravikumar Jothiramalingam, Service Delivery Manager, Senior Consultant, Corporate, Chennai, Mr.Balaji V Teshma, Chief Technology Officer, USRSystems, Chennai, Mr.N.Harikumar, Senior Researcher, Ericsson, Chennai.

Dates: 30/11/2020 to 04/12/2020 (Online mode)

Time: 9.30 AM to 3.45 PM

Objectives

The main objective of the AICTE sponsored ATAL FDP on deep learning for cyber security is to understand importance of deep learning models for security analytics. Also, the objective is to gain knowledge on mitigating cyber attacks through deep learning and to understand the transfer learning for cyber security.

About the programme

About 167 participants attended the AICTE ATAL FDP programme from various institutions. Day 1 (30.11.2020) – The first session was the Inaugural address. Mr. Maithili Sharan Gupta, Retired DGP, Madhya Pradesh, delivered an insightful talk and shared his experience with the participants on Awareness about cyber crimes and need for Cyber Security. The second session was the Art of living session. All the participants got inspired and learnt about different yogas and other mantras delivered by Mr.P.KrishnanBalaji, Principal, Maharishi Patanjali College of Yoga. The speaker for the session 3 was Dr.G.Sumathi, Professor, Dept of IT, SVCE. She delivered a talk on Cyber security Concepts. She presented an insightful talk on cyber security domains, secure system development life cycle, Business continuity and disaster recovery, operation security and network security.

Day 2 (01.12.2020) – The speaker for the session 1 is Ms.D.Jayanthi, Assistant Professor, Dept. of IT, SVCE. She delivered a talk on Artificial Neural Networks to Convolutional Neural Networks, and an introduction of Deep Learning for Security Analytics. She gave an overview of cyber security problems, RNN, LSTM, deep learning frameworks and implementation. Session 2 was about Dataset preparation methods for Intrusion Detection System. Mr.Thiruppathi, Scientist, SETS, Chennai, delivered a talk on IDS, types of IDS, datasets, Building a reliable benchmark dataset, feature extraction and selection, demo on Feature extraction from sample pcaps. The last session was about Cyber security Standards, Regulation

and Compliance. Mr.Nithiyanandam Ramesh, Technical Consultant gave an Insight on challenges of standardization, Drivers, compliance and consequences, Accreditation of certification bodies ISO21001:2018.

Day 3 (02.12.2020) - The speaker for the session 1 is Dr. N.Bhalaji, Associate Professor, Dept. of IT, SSN College of Engineering, Chennai. He delivered a talk on fundamentals of cyber security, hands-on with basic cyber security tools, exposure to threats actors, attacks and mitigation, role of AI techniques and algorithms in cyber security space. Session 2 was about Adversarial examples in Deep Learning. Dr.K.B.Sundharakumar, Assistant Professor, Dept. of IT, SSN College of Engineering, delivered a talk on Targeted attack, 1-pixel attack, PDG attack, non targeted attack, black box attack, defenses against adversarial attacks and working of GAN. Also, in the last session he gave hands-on session on Deep Learning and Adversarial examples.

Day 4 (03.12.2020) - The speaker for the session 1 is Mr.Vijayan Muralidaran, Manager, Information Security. He delivered a talk on Cyber Security and its Significance. Threats, Attacks & Defenses with tools and technologies. He covered about myths of cyber security, roles and response, GRC- governance, risk management and compliance. Session 2 was about hands-on session on Cyber Security tools. Mr.Ravikumar Jothiramalingam, Service Delivery Manager, Senior Consultant, delivered a talk on Risk management program – how to identify risk, assess and respond to risk and how to monitor the risk. The last session was about Real-time attack and exploits, defence technologies overview, and Mr.Vijayan Muralidaran explained about what is there beyond technology.

Day 5 (04.12.2020) - The speaker for the session 1 is Mr.N.Harikumar, Senior Researcher, Ericsson. He delivered a talk on Data and Image Security using Deep Learning. He covered about Image steganography and role of ML & DL in image data security. Session 2 was about Mitigating Cyber Attacks through Deep Learning and Transfer Learning for cyber security delivered by Mr. Balaji V Thesma, Chief Technology Officer. The last session was online test and Valedictory function. Dr. Santha, Vice Principal, SVCE delivered the valedictory address.

Benefits

Participants were benefited and gained knowledge on,

1. Deep learning for security analytics.
2. Dataset preparation methods, cyber security standards and compliance.
2. Cyber security and Artificial Intelligence, Deep adversarial networks with hands-on.
3. Data and image security using deep learning.
4. Mitigating Cyber Attacks through Deep Learning and Transfer Learning for Cybersecurity.

COORDINATORS

Dr.G.Sumathi, Prof., Dept. of Information Technology, SVCE.

Ms.D.Jayanthi, Assistant Prof. , Dept. of Information Technology, SVCE.

Mr.AR.Guru Gokul, Assistant Prof. , Dept. of Information Technology, SVCE.

PHOTOS

