Seventh Semester Professional Elective Course 1

Dr. Ambedkar Institute of Technology, Bengaluru-56
Department of Computer Science & Engineering
Scheme and Syllabus - NEP – 2022 -2023

Course Title	**DEEP LEARNING**						
Course Code	**21CST7031**						
Category	Professional Elective Course (PEC)						
Scheme and Credits	No. of Hours/Week					Total teaching hours	Credits
	L	T	P	SS	Total		
	03	00	00	00	03	42	03
CIE Marks: 50	**SEE Marks: 50**		**Total Max. marks=100**		**Duration of SEE: 03 Hours**		

COURSE OBJECTIVES:

1. Understand the foundational concepts of neural networks and the backpropagation algorithm for training them.
2. Learn about various optimization techniques and the architecture and functioning of CNN's.
3. Gain knowledge on advanced topics like convolutional networks and autoencoders for unsupervised learning tasks.
4. Explore the structure and applications of recurrent neural networks, attention mechanisms, and transformer models.
5. Investigate the principles of reinforcement learning and the workings of GAN's for generative modeling.

UNIT I **08 Hours**

NEURAL NETWORKS: Real Neurons, Artificial Neurons, Drawing the Neurons, Feed-Forward Networks, Neural Network Graphs, Initializing the Weights, Deep Networks, Fully Connected Layers, Tensors, Preventing Network Collapse, Activation Functions, SoftMax.

BACKPROPAGATION: A High-Level Overview of Training, Backprop on a Tiny Neural Network, Backprop on a Larger Network, The Learning Rate.

UNIT II **08 Hours**

OPTIMIZERS: Error as a 2D Curve, Adjusting the Learning Rate, Updating Strategies, Gradient Descent Variations, Choosing an Optimizer, Regularization.

CONVOLUTIONAL NEURAL NETWORKS: Introducing Convolution, Multidimensional Convolution, Multiple Filters, Convolution Layers, Changing Output Size, Hierarchies of Filters.

UNIT III **08 Hours**

CONVNETS IN PRACTICE: Categorizing handwritten digits, VGG 16, Visualizing filters, Adversaries.

AUTOENCODERS: Introduction to Encoding, Blending Representations, The Simplest Autoencoder, Exploring the Autoencoder, Convolutional Autoencoder, Denoising, Variational Autoencoders, Exploring the VAE.

UNIT IV	**09 Hours**
RECURRENT NEURAL NETWORKS: Working with Language, Fully connected Prediction, Recurrent Neural Networks, Using Recurrent Neural Networks, Seq2Seq. **ATTENTION AND TRANSFORMERS:** Embedding, Attention, Transformers, BERT and GPT-2.	
UNIT V	**09 Hours**
REINFORCEMENT LEARNING: Basic ideas, Learning a New Game, The Structure of Reinforcement Learning, Flippers, L-Learning, Q-Learning, SARSA. **GENERATIVE ADVERSARIAL NETWORKS:** Forging Money, Implementing GANs, GANs in Action, DCGANs, Challenges.	

TEACHING LEARNING PROCESS: Chalk and Talk, power point presentation, animations, videos

COURSE OUTCOMES: On completion of the course, student should be able to:

CO1: Examine the backpropagation algorithm in neural network training.
CO2: Choose different optimizers and design convolutional neural networks for image processing tasks.
CO3: Applying convolutional networks and autoencoders to various machine learning problems.
CO4: Develop proficiency in writing and deploying of RNNs, attention-based models, and transformers for sequential data.
CO5: Illustrate expertise in formulating reinforcement learning problems and generating synthetic data using GAN's.

TEXT BOOKS

1. Andrew Glassner, **"Deep Learning: A Visual Approach",** 1st Edition, No Starch Press Publications, 2021. (ISBN: 978-1718500723)

REFERENCE BOOKS

1. Ian Good fellow, Yoshua Bengio and Aaron Courville, **"Deep Learning",** 1st Edition, The MIT Press, 2016. (ISBN: 978-0262035613)
2. François Chollet, **"Deep Learning with Python**", 2nd Edition, Manning Publications, 2021. (ISBN: 978-1617296864)
3. Jeremy Howard and Sylvain Gugger, **"Deep Learning for Coders with fastai and PyTorch",** 1st Edition, O'Reilly Publications, 2020. (ISBN: 978-1492045526)
4. Sebastian Raschka, Yuxi (Hayden) Liu, Vahid Mirjalili, **"Machine Learning with PyTorch & Scikit-Learn",** 3rd Edition, Packt Publications, 2022. (ISBN: 978-1801819312)

ONLINE RESOURCES

1. https://onlinecourses.nptel.ac.in/noc20_cs62/preview
2. https://www.udemy.com/course/practical-transfer-learning-in-python/

SCHEME FOR EXAMINATIONS

Theory Question Paper Pattern:

1. **Answer ANY ONE from Question No. 1 and 2**
2. **Answer ANY ONE from Question No. 3 and 4**
3. **Answer ANY ONE from Question No. 5 and 6**
4. **Answer ANY ONE from Question No. 7 and 8**
5. **Answer ANY ONE from Question No. 9 and 10**

MAPPING of COs with POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	2	2	2	-	-	-	-	-	-	-
CO2	3	3	3	2	3	-	-	-	-	-	-	-
CO3	3	3	3	3	3	-	-	-	-	-	-	-
CO4	3	3	2	3	2	-	-	-	-	-	-	-
Strength of correlation: Low - 1, Medium - 2, High - 3												

Dr. Ambedkar Institute of Technology,

Bengaluru-56

Department of Computer Science & Engineering

Scheme and Syllabus - NEP – 2023 -2024

Course Title	**Cyber Forensics**						
Course Code	**21CST7032**						
Category	**Professional Elective Course (PEC)**						
Scheme and Credits	No. of Hours/Week					Total teaching hours	Credits
	L	T	P	SS	Total		
	03	00	**00**	00	**03**	**42**	**03**
CIE Marks: 50	**SEE Marks: 50**		**Total Max. marks=100**		**Duration of SEE: 02 Hours**		

COURSE OBJECTIVES

This course will enable students to:

1. Define and classify cybercrimes
2. Explore various Cyber forensic concepts and Forensic examination processes.
3. Learn the acquisition, analysis, and validation of forensics data.
4. Get familiarized with existing forensics tools.
5. Identify the best practices followed in the organization with respect to cyber security

Unit No	Syllabus Content	No of Hrs
1	**Introduction to Cybercrime** Cybercrime: Introduction, Role of Electronic Communication devices and Information and Communication Technologies in Cybercrime, Types of Cybercrime, Classification of Cyber criminals, Cybercrime, The Present and the Future: Cryptocurrency characteristics and types, Deep web, and Dark web	8
2	**Introduction to Cyber forensics** Interrelation among Cybercrime, Cyber Forensics and Cyber Security, Cyber Forensics: Definition, Need, Objectives, Computer Forensics Investigations, Steps in Forensic Investigation, Forensic Examination Process, Methods employed in Forensic Analysis, Classification of Cyber Forensics: Disk, Network, Wireless, Database, Malware, Mobile, GPS, Email and Memory Forensics	8
3	**Digital Evidence Analysis using Forensic Tools and Techniques** **Digital evidence:** Collection procedure, Sources, Digital evidence from stand alone computers/Electronic Communication Device, Evidence from mobile devices, Digital evidence on the internet. **Acquisition and handling of digital evidence:** Preliminaries of	9

	Electronic or digital evidence, Acquisition and seizure of evidence, Chain of Custody, Acquisition of evidence from Mobile phone and PDA, Optical and removable media. **Analysis of Digital Evidence:** Introduction to Analysis of digital evidence, Capturing Forensic copy of memory and hard drive with Toolkit Forensic imager, RAM analysis with Volitility, Analysing hard drive with Win Hex, Working with Autopsy, email tracing and tracking. **Admissibility of Digital Evidence**: Introduction, Digital evidence electronic record.	
4	**Cyber security: Organizational Implications** Introduction, Cost of Cybercrimes and IPR issues, Web threats for organizations, Security, and privacy implications from Cloud computing social media marketing: security risks, Protecting people's privacy in organization, Organizational guidelines for internet usage, safe computing and computer usage policy, Incident Handling: essential component of cyber security. Forensics best practices for organizations, Media and asset protection.	9
5	**Cyber Forensics case studies and Cyber Laws** Importance of end-point security. Cyber breaches examples and case studies discussion: New Zealand's Waikato District Health Board cyber attack, Colonial pipeline cyber attack (ransomware case study) etc.; Introduction to Cyber laws: need, legal issues; Cyber laws in India and case studies: Cyber laws in India, Information Technology Act 2000; Cyber Laws associated to Cyber crime against Individual, Property and Nation, Cyber laws for Cyber security,	8

Course Outcomes	**Description**	**RBT Levels**
CO1	Discuss the various types of cyber crimes and Cyber Laws applicable to them	**L1, L2**
CO2	Apply Forensic examination process	**L1, L2, L3, L4**
CO3	Analyze and validate forensics data	**L1, L2, L3, L4**
CO4	Use forensics tools	**L1, L2, L3**
CO5	Analyze and evaluate the Cyber security needs of an organization	**L1, L2**

CO-PO Mapping	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**P06**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CO1	**3**	**2**										
CO2	**3**	**3**	**1**	**3**								**2**
CO3	**3**	**3**	**2**	**3**								**1**
CO4	**3**	**2**	**1**	**2**	**3**							**2**

CO5	**3**	**2**	**2**									**1**

Strong -3 Medium -2 Weak -1

TEXT BOOKS:

1. Dejey, S Murugan, "**Cyber Forensics**", Oxford University Press, 2018.
2. Sunit Belapure and Nina Godbole, **"Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives"**, Wiley India Pvt Ltd, ISBN: 978-81-265-21791, 2011, First Edition (Reprinted 2018)

REFERENCE BOOKS:

1. John R. Vacca, "**Computer Forensics**", Cengage Learning, 2005
2. Marjie T. Britz, "**Computer Forensics and Cyber Crime": An Introduction**", 3rd Edition, Prentice Hall, 2013.

Dr. Ambedkar Institute of Technology,
Bengaluru-56

Department of Computer Science & EngineeringSchemeand
Syllabus-NEP – 2023 -2024

CourseTitle	**CRYPTOGRAPHY AND NETWORK SECURITY**						
CourseCode	**21CST7033**						
Category	**Professional Elective Courses - II (PEC-II)**						
Scheme andCredits	No.of Hours/Week					Total teachinghours	Credits
	L	T	P	SS	Total		
	03	00	**00**	00	**03**	**42**	**03**
CIE Marks: 50	**SEEMarks: 50**		**TotalMax. marks=100**		**DurationofSEE:03Hours**		

1. The students could able to recognize the different terminologies of cryptography
2. Able to understand the working of cryptographic algorithms.
3. Study the concept of Public key cryptosystem.
4. Acquire the knowledge of IP Security concepts.
5. Apply the knowledge in web Security applications

COURSEOBJECTIVES

UNIT I **09 Hours**
Introduction: OSI Security Architecture, Security Attacks, Security Services, Security Mechanism, Model for Network Security. **Classical Encryption Technique:** Symmetric Cipher Model, Substitution Techniques, Transposition Techniques
UNIT II **08 Hours**
Block Ciphers, Data Encryption Standard and Advanced Encryption Standard: Simplified DES, Block Cipher Principles, DES, and Differential and Linear cryptanalysis, Modes of operation. **AES**. Evaluation Criteria for AES, AES Cipher-Encryption and Decryption, Data Structure, Encryption Round, Triple DES, Blowfish
UNIT III **09 Hours**
Public Key Cryptography and Key Management: Principles of Public Key Cryptosystem,

RSA algorithm, Key management, Diffie Hellman Key Exchange, Elliptic curve cryptography..
UNIT IV **08 Hours** **IP Security:** IP Security Overview; IP Security Architecture; Authentication Header; Encapsulating Security Payload; Combining Security Associations; Key Management.
UNIT V **08 Hours** **Web Security:** Web security Considerations; Secure Socket layer (SSL) and Transport layer Security (TLS); Secure Electronic Transaction (SET). **System security** Intruders, Viruses and related threats

TEACHINGLEARNINGPROCESS:ChalkandTalk,powerpointpresentation,animations,videos

COURSEOUTCOMES: Oncompletionofthecourse,studentshouldbeableto,

CO1:Analyze different terminology of cryptography.
CO2: Write algorithm for cryptographic algorithms.

CO3: Describe Public key cryptosystem.

CO4: Understand IP security architecture and key management techniques.

CO5: Summarize Web Security and System security concepts

TEXT BOOK:

1. William Stallings, "Cryptography and Network Security – Principles and Practices", 6th Edition, Pearson Education 2014 ISBN13: 9780133354690

REFERENCE BOOKS/WEBLINKS:

ONLINERESOURCES

1. https://www.youtube.com/playlist?list=PLBlnK6fEyqRgJU3EsOYDTW7m6SUmW6kII
2. **https://archive.nptel.ac.in/courses/106/105/106105162/**

MAPPING of Cos with POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	1	3	3	-	3	-					
CO2	3	3	3	2	1	3	2					
CO3	2	3	2	2	1	3	-					
CO4	3	3	2	3	-	3	-					
CO5	3	3	3	3	3	-	-					
Strengthofcorrelation: Low-1, Medium-2, High-3												