Unit 4 (8 Hours)
Recurrent neural networks (RNNs): Sequence modeling using RNNs, Backpropagation through time, LongShort Term Memory (LSTM), Bidirectional RNN, Bidirectional LSTM
Unit 5 (8 Hours)
Unsupervised deep learning: Autoencoders, Generative Adversarial Networks.

Unit 6 (5 Hours)
Applications: Computer vision, Speech recognition and NLP.

Essential/recommended readings

1. Ian Goodfellow, Yodhua Bengio and Aaron Courville, *Deep Learning,* MIT Press Book**,** 2016.
2. Francois Chollet, *Deep Learning with python***,** *2nd edition*, Meaning Publications Co, 2021.

Additional References

1. Bunduma, N., *Fundamentals of Deep Learning*, 1st edition, O'reilly Books, 2017.
2. Heaton, J., *Deep Learning and Neural Networks*, 1st edition, Heaton Research Inc., 2015.

Suggested Practical List :

Practical exercises such as

The following practicals are to be conducted using Python.

1. Implement a feed-forward neural networks for classifying movie reviews as positive or negative(using IMDB dataset)
2. Implement a deep-neural feed-forward network for estimating the price of house, given real-estate data(Boston Housing Price)
3. Implement a deep-neural network for classifying news wires by topic (Reuters dataset).
4. Implement CNN for classifying MNIST dataset
5. Create a model for time-series forecasting using RNN/LSTM
6. Implement an auto-encoder

DISCIPLINE SPECIFIC ELECTIVE COURSE: Ethical Hacking

Credit distribution, Eligibility and Pre-requisites of the Course

Course title & Code	Credits	Credit distribution of the course			Eligibility criteria	Pre-requisite of the course
		Lecture	Tutorial	Practical/ Practice		
Ethical Hacking	**4**	**3**	**0**	**1**	Pass in Class XII	Any Programming Language at plus 2 level or above

Learning Objectives

The objective of this course is to enable students to be part of such a team that can conduct the security assessment of an organization through the process of ethical hacking. This course will introduce the students, the idea of security assessment of systems and networks under investigation and how to perform them under the legal and ethical framework. Further, this course will outline the importance of various stages of ethical hacking, including but not limited to tasks such as penetration testing, and usage of various tools at each stage.

Learning outcomes

On successful completion of this course, the student will be able to:

- Understand and acknowledge the relevance of legal, ethical, and professional challenges faced by an ethical hacker.
- Apply fundamental principles of system, application, and network security to ethically attack / penetrate the system to uncover the security flaws.
- Perform evaluation of security systems through a systematic ethical hacking process and recommend countermeasures to improve security.
- Understand and use various tools and techniques used in various stages of the ethical hacking process.

SYLLABUS OF DSE

Unit 1 (4 Hours)

Introduction: Overview of information security threats and attack vectors, vulnerability assessment and penetration testing concepts, information security controls, security laws and standards. OWASP.

Unit 2 (6 hours)

Footprinting and Reconnaissance: Introduction to network reconnaissance tools such ipconfig, ifconfig, domain tools, nmap, Wireshark, etc.

Unit 3 (6 hours)

Scanning and Enumeration: Network penetration testing, Password cracking techniques and countermeasures, NetBIOS tools

Unit 4 (6 hours)

Gaining and Maintaining Access: Network level attacks and countermeasures, Metasploit framework, Burp Suite

Unit 5 (6 hours)

Exploitation and Covering Tracks: Privilege escalation, social Engineering**,** identity theft, countermeasures, Covering tracks using attrib command and creating Alternate Data Stream (ADS) in Windows, Erasing evidence from Windows logs, Strategies for maintaining access.

Unit 6 (6 hours)

Advanced stages: Denial of service, Session hijacking, hacking web servers, hacking web applications, sql injection etc.

Unit 7 (6 hours)

NIST Cybersecurity framework and ISO standards: NIST cybersecurity framework, Cyber Kill chain, ISO/IEC 27001 and related standards.

Unit 8 (5 Hours)

Cyber Defense and Reporting: Preparing vulnerability assessment reports, presenting post testing findings, preparing recommendations

Essential/recommended readings

1. Patrick Engbretson, The Basics of Hacking and Penetration Testing, 2nd Edition, Syngress, 2013.
2. Georgia Weidman, Penetration TEsting: A Hands-On Introduction to Hacking, 1st Edition, No Starch Press, 2014.

Additional References

1. Peter Kim, The Hacker Playbook 3: Practical Guide to Penetration Testing, Zaccheus Entertainment, 2018.
2. Jon Erickson, Hacking: The Art of Exploitation, No Starch Press, 2008.
3. Online Resources:
    a. https://www.sans.org/cyberaces/
    b. https://skillsforall.com/
    c. https://www.hackingloops.com/ethical-hacking/

Suggested Practical List

Practical exercises such as

Perform the following activities.

(NOTE: Exercise extra caution while performing these exercises and codes)

1. Perform various Virtual Machine based exercises on https://vulnhub.com/
2. Perform exercises from https://www.hacker101.com/
3. Follow the lessons and activities from https://www.hackingloops.com/ethical-hacking/
4. Activities on Google site for hacking https://google-gruyere.appspot.com/
5. ACtivities on OWASP WebGoat https://github.com/WebGoat/WebGoat

DISCIPLINE SPECIFIC ELECTIVE COURSE: Cloud Computing

Credit distribution, Eligibility and Pre-requisites of the Course

Course title & Code	Credits	Credit distribution of the course			Eligibility criteria	Pre-requisite of the course
		Lecture	Tutorial	Practical/ Practice		
Cloud Computing	**4**	**3**	**0**	**1**	Pass in Class XII	NIL

Learning Objectives

The objective of an undergraduate cloud computing course is to provide students with a comprehensive understanding of cloud computing technologies, services, and applications.

Learning outcomes

On successful completion of this course, the student will be able to:

- Knowledge of the fundamental concepts and principles of cloud computing, including virtualization, scalability, reliability, and security.
- Ability to design, develop, and deploy cloud-based applications using popular cloud platforms and services.
- Familiarity with cloud computing architectures, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
- Understanding of the economic, legal, and ethical implications of cloud computing, including issues related to data privacy, ownership, and security.
- Ability to evaluate and select cloud-based solutions based on their technical, economic, and business requirements.
- Understanding of the broader societal and environmental impacts of cloud-based services and applications.

SYLLABUS OF DSE

Unit 1

Overview of Computing Paradigm: Recent trends in Computing : Grid Computing, Cluster Computing, Distributed Computing, Utility Computing, Cloud Computing,

Unit 2