Minor Degree Courses offered

by

Department of Information Technology & Computer Application

The department of Information Technology & Computer Application offers the following minor degree course for the students of undergraduate B. Tech. program of other departments.

Minor Degree 1: Cyber Security and Forensics

Category	Subject Code	Name of Subject	Credit			Total Credit
			L	T	P	
PE-1	EIT-103	Cryptography	3	0	2	4
PE-3	EIT-303	Network Security	3	0	2	4
PE-5	EIT-503	Cybersecurity Policies and Management	3	1	0	4
PE-7	EIT-703	Ethical Hacking	3	0	2	4
PE-9	EIT-903	Digital Forensics	3	0	2	4

Minor Degree 2: AI & Data Science

Category	Subject Code	Name of Subject	Credit			Total Credit
			L	T	P	
PE-1	EIT-104	Artificial Intelligence	3	0	2	4
PE-3	EIT-304	Data Science and Analytics	3	0	2	4
PE-5	EIT-504	Machine Learning	3	0	2	4
PE-7	EIT-704	Deep Learning	3	0	2	4
PE-9	EIT-904	Python Programming	3	0	2	4

1. Minor degree courses are optional, but it will be helpful to align the need of industries.
2. Students can only opt for one minor degree course during his/her studies of the B. Tech. program
3. If students complete all 5 PE (professional elective) category courses offered for the minor degree (total 20 credit) from the other department for minor degree, he/shell get a B. Tech. degree in his/her own branch.
4. No extra fee for a minor degree course will be charged by the students
5. In case if a student is unable to complete all 5 PE courses as offered by the other department for minor degree at the time of completion of B. Tech. program in his/her own branch then student will get B. Tech. degree in his/her own branch without completing the minor degree course from other Department.
6. The minor degree course may be offered by the department through MOOC, as per the guidelines in B. Tech. ordinance 3.0 for the MOOC course.

EIT-103	:	**Cryptography**	3-0-2
Course category	:	Program Elective (PE)	
Pre-requisite Subject	:	NIL	
Contact hours/week	:	Lecture: 3, Tutorial: 0, Practical: 2	
Number of Credits	:	4	
Course Assessment methods	:	Continuous assessment through tutorials, attendance, home assignments, quizzes and One Minor tests and One Major Theory Examination	
Course Objectives	:	A cryptography course aims to equip students with a solid understanding of cryptographic techniques and their application in securing information and communications. The course typically covers fundamental concepts like encryption, decryption, and key management, as well as various cryptographic algorithms and protocols.	
Course Outcomes	:	The students are expected to be able to demonstrate the following knowledge, skills and attitudes after completing this course:	

1. Classify the symmetric encryption techniques and illustrate various public key cryptographic techniques
2. Understand security protocols for protecting data on networks and be able to digitally sign emails and files
3. Understand vulnerability assessments and the weakness of using passwords for authentication
4. To be able to perform simple vulnerability assessments and password audits
5. Summarize the intrusion detection and its solutions to overcome the attacks.

UNIT-I 9

Introduction to security attacks, services and mechanism, Classical encryption techniques substitution ciphers and transposition ciphers, cryptanalysis, Modern Block Ciphers: Block ciphers principles, Shannon's theory of confusion and diffusion, fiestal structure, Data encryption standard (DES), Strength of DES, Idea of differential cryptanalysis.

UNIT-II 9

Extended Euclidean Algorithm, Advanced Encryption Standard (AES) encryption and decryption Fermat's and Euler's theorem, Principals of public key crypto systems, RSA algorithm, security of RSA, Message Authentication Codes: Authentication requirements, authentication functions, message authentication code, hash functions, security of hash functions, Secure hash algorithm (SHA).

UNIT-III 9

Digital Signatures: Digital Signatures, Elgamal Digital Signature Techniques, Digital signature standards (DSS), proof of digital signature algorithm, Key Management and distribution: Symmetric key distribution, Diffie-Hellman Key Exchange, Public key distribution.

UNIT-IV 9

IP Security: Architecture, Authentication header, Encapsulating security payloads, combining security associations, key management. Introduction to Secure Socket Layer, Electronic mail security: pretty good privacy (PGP), S/MIME, System Security: Introductory idea of Intrusion, Intrusion detection, Viruses and related threats, firewalls.

Books & References:

1. William Stallings, "Cryptography and Network Security: Principals and Practice", Education.
2. Behrouz A. Frouzan: Cryptography and Network Security, McGraw Hill .
3. C K Shyamala, N Harini, Dr. T.R.Padmnabhan Cryptography and Security ,Wiley
4. Bruce Schiener, "Applied Cryptography". John Wiley & Sons
5. Bernard Menezes," Network Security and Cryptography", Cengage Learning.
6. AtulKahate, "Cryptography and Network Security", McGraw Hill

Experiments:

1. Breaking the Shift Cipher
2. Breaking the Mono-alphabetic Substitution Cipher
3. Message Authentication Codes
4. Cryptographic Hash Functions and Applications
5. Symmetric Key Encryption Standards (DES)
6. Symmetric Key Encryption Standards (AES)
7. Diffie-Hellman Key Establishment
8. Digital Signatures

EIT-303	: **Network Security**	**3-0-2**
Course category	:	Program Elective (PE)
Pre-requisite Subject	:	NIL
Contact hours/week	:	Lecture: 3, Tutorial: 0, Practical: 2
Number of Credits	:	4
Course Assessment methods	:	Continuous assessment through tutorials, attendance, home assignments, quizzes and One Minor tests and One Major Theory Examination
Course Objectives	:	This course focuses on the introduction of network security using various cryptographic algorithms and understanding network security applications and practical applications that have been implemented and are in use to provide email and web security.
Course Outcomes	:	The students are expected to be able to demonstrate the following knowledge, skills and attitudes after completing this course:

1. Understands the basic concepts of cryptography.
2. Apply the symmetric key concepts of DES and AES for securing data.
3. Apply the concepts of number theory of Asymmetric key cryptosystem.
4. Understand the concepts of hash function, MAC and digital signature for data integrity.
5. Explain the symmetric and asymmetric key distribution techniques.
6. Understand the concepts of security mechanism at TCP/IP layer.

UNIT-I 9

Introduction: Introduction to Security Attacks, Services and Mechanism, Classical Encryption Techniques-Substitution Ciphers and Transposition Ciphers, Steganography, Stream and Block Ciphers, Cryptanalysis.

Symmetric Key Cryptosystems: Block Cipher Principles, Shannon's Theory of Confusion and Diffusion, Data Encryption Standard (DES), Strength of DES, Triple DES, Advance Encryption Standard (AES), Linear and Differential Cryptanalysis, Block Ciphers Modes of Operation.

UNIT-II 9

Introduction to Number Theory: Modular Arithmetic, Prime and Relative Prime Numbers, Primitive Roots, Fermat's and Euler's Theorem, Extended Euclidean Algorithm, Chinese Remainder Theorem.

Algebraic Structures: Introduction to Group, Ring & Field of the Form GF(P). Asymmetric Key Cryptosystems: RSA Cryptosystem, Attacks on RSA, Security of RSA, Discrete Logarithm Problem, Elgamal Encryption Algorithm.

UNIT-III 9

Hash Functions and Macs: Authentication Functions, Message Authentication Code, Hash Functions, Birthday Attacks, Security of Hash Functions, Secure Hash Algorithm[SHA-512).
Digital Signature: Digital Signatures, RSA Digital Signature Scheme, Elgamal Digital Signature Techniques, Digital Signature Standards (DSS).
Key Management: Symmetric Key Distribution, Diffie Hellman Key Exchange Algorithm.
Public Key Distribution: X.509 Certificates, Public Key Infrastructure. Authentication Applications and E-Mail Security: Kerberos, Pretty Good Privacy (PGP), S/MIME.

UNIT-IV 9

IP Security and Web Security: IP Sec Architecture, Authentication Header, Encapsulating Security Payloads, Combining Security Associations, Key Management, Introduction to Secure Socket Layer, Transport Layer Security, Secure Electronic Transaction (SET).
System Security: Introductory Idea of Intrusion, Intrusion Detection, Malicious Programs, Firewalls.

Books & References

Textbooks:

1. W. Stallings , "Cryptography and Network Security: Principles and Practices", 8th Edition, Pearson Education, 2023.

Reference Books:

1. B. A. Forouzan, "Cryptography & Network Security", 3rd Edition, Tata McGraw Hill, 2003.
2. Wenbo Mao, "Modern Cryptography: Theory and Practice", Prentice Hall, 2003.
3. Douglas Stinson, "Cryptography Theory and Practice", 2nd Edition, Chapman& Hall/CR

Experiments:

1. Study the working with Sniffers for monitoring network communication using a) Ethereal b) Wireshark c) Snort d) tcpdump.
2. Implementation and Performance evaluation of various cryptographic algorithms in C/C++: a)DES b)RSA.
3. Study of different wireless network components and features of any one of the Mobile Security Apps.
4. Configuring S/MIME for e-mail communication.
5 Using NMAP for port monitoring.

EIT-503	:	**Cybersecurity Policies and Management** **3-1-0**
Course category	:	Program Elective (PE)
Pre-requisite Subject	:	NIL
Contact hours/week	:	Lecture: 3, Tutorial: 1, Practical: 0
Number of Credits	:	4
Course Assessment methods	:	Continuous assessment through tutorials, attendance, home assignments, quizzes and One Minor tests and One Major Theory Examination
Course Objectives	:	To equip students with the technical knowledge and skills needed to protect and defend against cyber threats. To develop skills in students that can help them plan, implement, and monitor cyber security mechanisms to ensure the protection of information technology assets. To systematically educate the necessity to understand the impact of cyber-crimes and threats with solutions in a global and societal context.
Course Outcomes	:	The students are expected to be able to demonstrate the following knowledge, skills and attitudes after completing this course:

1. Analyze and evaluate the cyber security needs of an organization.
2. Analyze software vulnerability and Security Solutions to reduce the risk of exploitation.
3. Measure the performance and troubleshoot cyber security systems.
4. Explore the ethical hacking features and opportunities.

UNIT-I **9**

Overview of Cyber security:

Cyber security increasing threat landscape, Cyber security terminologies- Cyberspace, Attack, Attack Vector, Attack Surface, Threat, Risk, Vulnerability, Exploit, Exploitation, Hacker, Non-state actors, Cyber Terrorism, Protection of end user machine, Critical IT and National Critical Infrastructure.

UNIT-II **9**

Cyber Law:

Cyber-crime and legal landscape around the world, IT Act - 2000 and its amendments. Limitations of IT Act – 2000, Cyber-crime and punishments, Cyber Laws and Legal and ethical aspects related to new technologies- AI/ML, Darknet and Social media, Cyber Laws of other countries.

UNIT-III **9**

Data Privacy and Data Security:

Defining data, Meta-data, Big data, Non-personal data. Data protection, Data privacy and data security, Personal Data Protection Bill and its compliance, Data protection principles, Big data security issues and challenges, Social media- data privacy and security issues.

UNIT-IV **9**

Cyber security Management:

Cyber security policy, Cyber crises management plan, Business continuity, Risk assessment,

Types of security controls and their goals, Cyber security audit and compliance, National cyber security policy and strategy.

Books & References:

1. Cybersecurity Policy Guidebook" by Jennifer L. Bayuk
2. Information Security Policies, Procedures, and Standards: guidelines for effective information security management" by Thomas R. Peltier.
3. Cyber Forensics - Concepts and Approaches, Ravi Kumar &B Jain, 2006, icfai university press.
4. Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press12 Series: Computer Forensics),2010

EIT-703	:	**Ethical Hacking**	**3-0-2**
Course category	:	Program Elective (PE)	
Pre-requisite Subject	:	NIL	
Contact hours/week	:	Lecture: 3, Tutorial: 0, Practical: 2	
Number of Credits	:	4	
Course Assessment methods	:	Continuous assessment through practical, attendance, home assignments, quizzes and One Minor tests and One Major Theory Examination	
Course Objectives	:	The aim of the course is to introduce the methodologies and framework of ethical hacking for enhancing the security. The course includes-Impacts of Hacking; Types of Hackers; Information Security Models; Information Security Program; Business Perspective; Planning a Controlled Attack; Framework of Steps (Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Deliverable and Integration)	
Course Outcomes	:	The students are expected to be able to demonstrate the following knowledge, skills and attitudes after completing this course:	

1. Gain the knowledge of the use and availability of tools to support an ethical hack.
2. Gain the knowledge of interpreting the results of a controlled attack.
3. Understand the role of politics, inherent and imposed limitations and metrics for planning of a test.
4. Comprehend the dangers associated with penetration testing.

9

UNIT-I

Introduction:

Hacking Impacts, The Hacker Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration Information Security Models: Computer Security, Network Security, Service Security, Application Security, Security Architecture Information Security Program: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking.

UNIT-II 9

The Business Perspective:

Business Objectives, Security Policy, Previous Test Results, Business Challenges Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, Timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement.

UNIT-III 9

Preparing for a Hack:

Technical Preparation, Managing the Engagement Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance.

UNIT-IV 9

Enumeration:

Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase Exploitation, Deliverable: The Deliverable, The Document, Overal Structure, Aligning Findings, Presentation Integration, Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion.

Books & References

1. James S. Tiller, "The Ethical Hack: A Framework for Business Value Penetration Testing", Auerbach Publications, CRC Press.
2. EC-Council, "Ethical Hacking and Countermeasures Attack Phases", Cengage Learning.
3. Michael Simpson, Kent Backman, James Corley, "Hands-On Ethical Hacking and Network Defense", Cengage Learning.

Experiments:

1. To gather preliminary information about a target system or network using passive and active techniques.
2. To identify live hosts, open ports, and services running on a target using scanning tools.
3. To extract user names, machine names, network resources, shares, and services from the target system.
4. To discover known vulnerabilities in the target system using vulnerability scanning tools.
5. To gain unauthorized access to a system and escalate privileges using password cracking and exploit techniques.
6. To create a basic malware sample (e.g., Trojan) and analyze its behavior in a secure environment.
7. To capture and analyze network packets to find sensitive data like credentials using tools like Wireshark.
8. To simulate a phishing or pretexting attack and understand how attackers exploit human psychology.
9. To identify and exploit common vulnerabilities like SQL Injection and Cross-Site Scripting (XSS) in web apps.
10. To capture wireless traffic and crack Wi-Fi security protocols (e.g., WEP, WPA2) using real-time tools.

EIT-903	:	**Digital Forensics** **3-0-2**
Course category	:	Program Elective (PE)
Pre-requisite Subject	:	NIL
Contact hours/week	:	Lecture: 3, Tutorial: 0, Practical: 2
Number of Credits	:	4
Course Assessment methods	:	Continuous assessment through practical, attendance, home assignments, quizzes and One Minor tests and One Major Theory Examination
Course Objectives	:	To understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices. To understand how to examine digital evidences such as the data acquisition, identification analysis.
Course Outcomes	:	The students are expected to be able to demonstrate the following knowledge, skills and attitudes after completing this course:

1. Know how to apply forensic analysis tools to recover important evidence for identifying computer crime.
2. To be well-trained as next-generation computer crime investigators.
3. Gain hands-on experience with digital forensic tools.
4. Simulate real-world cybercrime investigation scenarios.

UNIT-I 9

Fundamentals of Digital Forensics: Computer forensics fundamentals, Benefits of forensics, computer crimes, computer forensics evidence and courts, legal concerns and private issues.

UNIT-II 9

Investigation Procedures and Environments: Understanding Computing Investigations – Procedure for corporate High-Tech investigations, understanding data recovery workstation and software, conducting and investigations.

UNIT-III 9

Data Acquisition and Evidence Handling: Understanding storage formats and digital evidence, determining the best acquisition method, acquisition tools, validating data acquisitions, performing RAID data acquisitions, remote network acquisition tools, and other forensics acquisitions tools. Processing crimes and incident scenes, securing a computer incident or crime, seizing digital evidence at scene, storing digital evidence, obtaining digital hash, reviewing case.

UNIT-IV 9

Tools and Techniques in Digital Forensics: Current computer forensics tools- software, hardware tools, validating and testing forensic software, addressing data-hiding techniques, performing remote acquisitions, E-Mail investigations- investigating email crime and violations, understanding E-Mail servers, specialized E-Mail forensics tools.

Books & References:

1. Warren G. Kruse II and Jay G. Heiser, “Computer Forensics: Incident Response Essentials”, Addison Wesley, 2002.
2. Nelson, B, Phillips, A, Enfinger, F, Stuart, C., “Guide to Computer Forensics and Investigations, 2nd ed., Thomson Course Technology, 2006, ISBN: 0-619-21706-5.
3. Vacca, J, Computer Forensics, Computer Crime Scene Investigation, 2nd Ed, Charles River Media, 2005, ISBN: 1-58450-389.

Experiments:

1. Introduction to Digital Forensics Tools (Autopsy, FTK Imager, CAINE, etc.).
2. Creating a Forensic Disk Image using FTK Imager or dd command.
3. File Carving and Deleted File Recovery using Autopsy.
4. Verifying Data Integrity with Hash Functions (MD5, SHA1, SHA256).
5. Analysis of Windows Event Logs and Registry using Registry Viewer tools.
6. Email Header Analysis and Tracing IP using online tools and forensic software.
7. Network Packet Capture and Analysis using Wireshark.
8. Steganography Detection and Recovery using tools like Steghide or OpenStego.
9. RAM Acquisition and Volatile Memory Analysis using Volatility Framework.
10. Mobile Device Forensics (Android) using MOBILedit or open-source tools.

EIT- 104	:	**Artificial Intelligence**	**3-0-2**
Course category	:	Program Elective (PE)	
Pre-requisite Subject	:	NIL	
Contact hours/week	:	Lecture: 3, Tutorial: 0, Practical: 2	
Number of Credits	:	4	
Course Assessment methods	:	Continuous assessment through tutorials, attendance, home assignments, quizzes and One Minor tests and One Major Theory Examination.	
Course Objectives	:	Introduce the fundamentals of Artificial Intelligence. Develop problem-solving skills using AI techniques. Understand knowledge representation and reasoning mechanisms. Introduce machine learning principles and expert systems. Explore advanced AI topics and ethical considerations.	
Course Outcomes	:	The students are expected to be able to demonstrate the following knowledge, skills and attitudes after completing this course:	

1. Understand the fundamentals of Artificial Intelligence.
2. Apply search strategies to solve problems.
3. Represent knowledge and perform logical reasoning.
4. Design and develop machine learning and expert systems.
5. Explore advanced AI techniques and applications.

UNIT-I 9

Introduction to Artificial Intelligence: Definition and history of AI, Foundations and goals of AI, Intelligent agents and their types, Environment types (fully/partially observable, deterministic/stochastic), Problem-solving agents, **Search strategies:** Uninformed Search (BFS, DFS, Depth-limited, Iterative deepening), Informed Search (Greedy, A*, heuristics).

UNIT-II 9

Knowledge Representation and Reasoning: Knowledge representation techniques, Propositional and First-Order Logic, Inference in FOL, Resolution, unification, Semantic networks, frames, Ontologies, Rule-based systems and production systems.

UNIT-III 9

Machine Learning and Expert Systems: Overview of Machine Learning, Supervised, Unsupervised, and Reinforcement learning, Basic ML algorithms (Linear Regression, Decision Trees, Naïve Bayes, k-NN, etc.), **Expert systems:** Architecture, Inference engine, Knowledge base, Applications.

UNIT-IV 9

Advanced Topics and Applications: Natural Language Processing (NLP), Robotics and Perception, Planning and Scheduling, Computer Vision basics, **AI in real-world applications:** Healthcare, Finance, Autonomous systems, Ethics in AI and societal impact.

Books & References:

1. S. Russel and P. Norvig, “Artificial Intelligence – A Modern Approach”, Second Edition, Pearson Education, 2012.
2. David Poole, Alan Mackworth, Randy Goebel, “Computational Intelligence: a logical approach”, Oxford University Press, 2012.
3. G. Luger, “Artificial Intelligence: Structures and Strategies for complex problem solving”, Fourth Edition, Pearson Education, 2012
4. J. Nilsson, “Artificial Intelligence: A new Synthesis”, Elsevier Publishers, 1998

Experiments:

1. Implement Breadth-First Search (BFS) and Depth-First Search (DFS) for a Puzzle Problem.
2. Implement A* Search Algorithm Using Heuristics.
3. Create a Simple Reflex Agent and a Goal-Based Agent Simulation.
4. Represent Knowledge Using Propositional Logic and Evaluate Inference Rules.
5. Implement Unification and Resolution Algorithm in First-Order Logic.
6. Build a Semantic Network and Perform Reasoning.
7. Implement Basic Machine Learning Algorithms (e.g., Linear Regression, Decision Tree).
8. Design a Simple Expert System Using Rule-Based Reasoning.
9. Perform Named Entity Recognition and Tokenization Using NLP Toolkit (spaCy/NLTK).
10. Explore Real-World AI Applications in Healthcare or Finance Using a Public Dataset.

EIT- 304	:	**Data Science and Analytics**	**3-0-2**
Course category	:	Program Elective (PE)	
Pre-requisite Subject	:	NIL	
Contact hours/week	:	Lecture: 3, Tutorial: 0, Practical: 2	
Number of Credits	:	4	
Course Assessment methods	:	Continuous assessment through tutorials, attendance, home assignments, quizzes and One Minor tests and One Major Theory Examination	
Course Objectives	:	The objective of this course is to Conceptualize data and machine learning, including the distinction between trivial data and big data, big data computing technologies, machine learning techniques, and scaling up machine learning approaches.	
Course Outcomes	:	The students are expected to be able to demonstrate the following knowledge, skills and attitudes after completing this course:	

1. Understand the overview of an exciting growing field of Data analytics.
2. Analyze the Data using traditional data mining algorithms.
3. Apply the tools required to manage and analyze big data.
4. Understand the fundamental techniques and principles in achieving data analytics with scalability and streaming capability.
5. Understand the many types of data like data streams.
6. Solve complex real-world problems in for decision support.

UNIT-I 9

Introduction to Data Analytics and Big Data: An Overview Session for the Data Analyst, Data Scientist, Getting Started with Jupyter Notebook, Introduction to the Open Data Science Learning and, Competitive Platforms, IoT and Big Data, IoT Analytics Platform, Use Cases.

UNIT-II 9

Scientific Computing with Python – Numpy: - Introduction to List and Dictionary: Basic operations in List and Dictionary, Importance of Numpy, Array Creation, Data Types, Unary Operations, Shape Manipulation, Reshape, Transpose, Ravel, Universal Functions, Matrix Operations (Addition, Multiplication, Transpose and Inverse), Statistical Methods, Stacking (vstack and hstack), Splitting, Shallow copy and Deep copy/Cloning.

UNIT-III 9

Data Analysis Workflow in Python using Pandas: Introduction to Pandas, Pandas Data Structures, importing files/exporting files (*introduction to OS library), Series & Data Frame, Basic Functions on Data Frame, Indexing & Selecting Data, Selection by Level, Selection by Position, Boolean Selection, Sorting, Group by: Split-Apply- Combine, Handling Missing Data (Missing imputation), Data Analysis Scenarios. Advanced Data Analysis using Pandas: Merging of Data Frame, (Concat and Merge), Reshaping: Stack, Unstack, Pivot, Dummy/Indicator Variables, Working with Databases.

UNIT-IV 9

Data Analysis Scenarios: Converting Series to Time Series, Handling Invalid Data, Date-Time Index, Indexing, Time/Date Components, Period & Period Index, Parsing & Manipulating Dates. Data Visualization: -Introduction, Creating Different Types of Plots Scatter Plots, Line Graphs, Bar Plots, X and Y Ticks and Rotations ,Histograms, Box Plot, Stacked Plots.

Books & References

Textbooks:

1. "Python for Data Analysis", Wes McKinney O'Reilly Media.
2. "Data Science from Scratch: First Principles with Python", Joel Grus O'Reilly Media.
3. "Data Analytics Made Accessible", Anil Maheshwari.

Reference Books:

1. "Python Data Science Handbook," Jake VanderPlas, O'Reilly Media
2. "Hands-On Data Analysis with Pandas," Stefanie Molin Packt Publishing
3. "Big Data: Principles and Best Practices of Scalable Real-Time Data Systems", Nathan Marz and James Warren, Manning Publications

Experiments:

1. Getting Started with Jupyter Notebook and Python for Data Science.
2. Exploring IoT Datasets and Describing Use Cases Using Big Data Concepts.
3. Perform Array Operations Using NumPy: Creation, Reshaping, and Mathematical Operations.
4. Implement Matrix Operations: Addition, Multiplication, Transpose, and Inverse with NumPy.
5. Explore Lists and Dictionaries and Perform Shallow vs Deep Copy in Python.
6. Read, Clean, and Explore a Dataset Using Pandas (e.g., CSV file import, NaN handling, sorting).
7. Perform GroupBy Operations and Generate Summary Statistics Using Pandas.
8. Merge Multiple DataFrames and Use Stack/Unstack and Pivot Operations.
9. Convert Series to Time Series, Parse Dates, and Extract Date-Time Features.
10. Visualize Data Using Matplotlib and Seaborn: Scatter, Line, Bar, Histogram, Box, and Stacked Plot

EIT- 504	**:**	**Machine Learning** **3-0-2**
Course category	:	Program Elective (PE)
Pre-requisite Subject	:	NIL
Contact hours/week	:	Lecture: 3, Tutorial: 0, Practical: 2
Number of Credits	:	4
Course Assessment methods	:	Continuous assessment through tutorials, attendance, home assignments, quizzes and One Minor tests and One Major Theory Examination
Course Objectives	:	The objective of this course is to introduce the foundational principles and techniques of machine learning, including both supervised and unsupervised learning methods. It aims to equip students with the ability to understand and implement various machine learning algorithms. By the end of the course, learners will be able to analyze and apply suitable machine-learning approaches to real-world problems.
Course Outcomes	:	The students are expected to be able to demonstrate the following knowledge, skills and attitudes after completing this course:

1. Understand the fundamental concepts, types, and challenges of machine learning and apply foundational learning algorithms.
2. Implement and evaluate supervised learning models addressing model performance and inductive biases.
3. Apply probabilistic models for learning.
4. Analyze ensemble learning techniques to enhance model accuracy and reduce variance in supervised learning systems.
5. Demonstrate competency in unsupervised learning techniques for effective feature selection.

UNIT-I 9

Introduction: Types, Applications and Challenges of Machine Learning, Testing and Validating, Learning problems, Designing a Learning system, Perspectives and Issues.

Concept Learning Task: Concept learning task as search, Find-S algorithm, Version space, Candidate Elimination algorithm, Inductive Bias.

UNIT-II 9

Supervised Machine Learning: Decision Trees: Decision Tree Representation, Problems, Hypothesis Space Search, Inductive Bias and issues. Pruning, Rule extraction from Decision trees.

Instance- Based Learning: Support Vector Machines: Linear and Non-Linear, SVM regression, k- Nearest Neighbor Learning, Locally Weighted Regression.

UNIT-III 9

Bayesian Learning: Concept Learning, Maximum Likelihood, Minimum Description Length Principle, Bayes Optimal Classifier, Naïve Bayes Classifier, Bayesian Belief Network, EM Algorithm.

Ensemble and Probabilistic Learning Model: Voting classifiers, Bagging and pasting, Random patches, Random forests, Boosting, stacking.

UNIT-IV 9

Unsupervised Machine Learning: Clustering: K means, Spectral, Hierarchical; Association rule mining, Anomaly detection.

Dimensionality Reduction: Subset selection, Main Approaches for Dimensionality Reduction, PCA, Kernel PCA, LLE, Linear Discriminant Analysis (LDA).

Books & References

Textbooks:

1. Machine Learning, Tom Mitchell, McGraw Hill, 3rd Edition, 1997.
2. Introduction to Machine Learning, Ethem Alpaydın, 3rd Edition, MIT press, 2014.

Reference Books:

1. MACHINE LEARNING - An Algorithmic Perspective, Stephen Marsland, 2nd Edition, 2015.
2. Introduction to Machine Learning with Python, A Guide for Data Scientists, Andreas C.Miller and Sarah Guido, O'Reilly Media, 2017.
3. Hands-on Machine Learning with Scikit-Learn and Tensor Flow: concepts, tools, and techniques to build intelligent systems, Aurelien Geron, O'Reilly Media, 2019.

Experiments:

1. Implement the Find-S Algorithm and Candidate Elimination Algorithm.
2. Design a Simple Machine Learning System for Classification with Data Preprocessing.
3. Build and Visualize a Decision Tree Classifier on a Dataset (e.g., Iris, Titanic).
4. Implement K-Nearest Neighbors (k-NN) Algorithm from Scratch and Evaluate Performance.
5. Train a Support Vector Machine (SVM) Classifier with Linear and Non-Linear Kernels.
6. Apply Naïve Bayes Classifier on a Text Classification Problem (e.g., spam detection).
7. Compare Bagging, Random Forests, and Boosting (AdaBoost/XGBoost) on any Dataset.
8. Perform K-Means and Hierarchical Clustering with Visualization (e.g., on Mall Customers data).
9. Apply Association Rule Mining (Apriori/FP-Growth) on Market Basket Data.
10. Implement Dimensionality Reduction using PCA and LDA and Visualize in 2D.

EIT- 704	:	**Deep Learning** **3-0-2**
Course category	:	Program Elective (PE)
Pre-requisite Subject	:	NIL
Contact hours/week	:	Lecture: 3, Tutorial: 0, Practical: 2
Number of Credits	:	4
Course Assessment methods	:	Continuous assessment through practical, attendance, home assignments, quizzes and One Minor tests and One Major Theory Examination
Course Objectives	:	The objective of the Deep Learning is to provide students with foundational knowledge of deep learning, enable them to build and train neural networks using modern tools, and apply these models to solve real-world problems effectively.
Course Outcomes	:	The students are expected to be able to demonstrate the following knowledge, skills and attitudes after completing this course:

1. Understand and explain foundational concepts of Deep Learning
2. Design and implement basic neural network architectures
3. Apply advanced training strategies and optimization techniques,
4. Analyze and implement deep learning models
5. Apply concepts of model interpretability using tools like SHAP and LIME to explain model decisions in applied contexts.

UNIT-I 9

Foundations of Deep Learning:

Introduction to Deep Learning: What is Deep Learning? History and Real-World Successes, Basics of Machine Learning: Gradient Descent, Logistic Regression, Probability Theory: Discrete and Continuous Distributions, Maximum Likelihood Estimation and its Application in Learning, Introduction to Neural Networks: Hypotheses, Tasks, Training Data, Cost Functions: MSE, Cross-Entropy, Likelihood-based Cost Functions.

UNIT-II 9

Neural Network Architecture and Learning:

Feedforward Neural Networks: Architecture and Components, Multilayer Perceptron (MLP), Sigmoid and Tanh Units, Neuroscience Inspiration Behind Neural Networks, Learning in Neural Networks: Output vs. Hidden Layers, Linear vs. Nonlinear Networks, Backpropagation: Gradient Descent, Chain Rule, Recursive Learning, Overfitting, Underfitting: Bias-Variance Trade-off, Regularization Techniques: L1, L2 Regularization, Dropout.

UNIT-III 9

Advanced Deep Learning Techniques:

Output Units: Linear, Softmax, Hidden Units: RELU, Leaky RELU, ELU, Deep Learning Training Strategies: GPU Acceleration, Batch Normalization, Early Stopping, Transfer Learning: Concept and Applications, Optimization Algorithms: Adam, RMSprop, SGD, Model Evaluation: Accuracy, Precision, Recall, Confusion Matrix, ROC and AUC Curve.

UNIT-IV 9

Deep Learning Models and Applications:
Convolutional Neural Networks (CNNs): Architecture, Use Cases, Recurrent Neural Networks (RNNs) and Variants: LSTM, GRU, Deep Belief Networks and Restricted Boltzmann Machines, Autoencoders: Variants, Applications in Unsupervised Learning, Generative Models: GANs, VAEs (Basic Intro), Explainability in Deep Learning: SHAP, LIME (Introduction), Hands-on Projects using TensorFlow/PyTorch, Applications in Image, Text, Audio, and Time-Series Data.

Books & References:

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
2. Nielsen, M. A. (2015). Neural networks and deep learning. Determination Press.
3. Chollet, F. (2018). Deep learning with Python. Manning Publications.
4. Géron, A. (2019). Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow (2nd ed.). O'Reilly Media.
5. Buduma, N., & Locascio, N. (2017). Fundamentals of deep learning: Designing next-generation machine intelligence algorithms. O'Reilly Media.

Experiments:

1. Install Anaconda or Miniconda and set up Python environments for deep learning projects, or use cloud-based platforms like Google Colab for running experiments without local setup.
2. Implement logistic regression on a simple dataset to understand gradient descent and loss functions.
3. Build a feedforward neural network (MLP) for image classification using datasets like MNIST, experimenting with activation functions like sigmoid, ReLU, and tanh.
4. Manually code the backpropagation algorithm to learn how gradients propagate through a neural network.
5. Design and train a convolutional neural network (CNN) using datasets like CIFAR-10 or Fashion-MNIST to explore feature extraction.
6. Work with recurrent neural networks (RNNs) including vanilla RNN and LSTM on sequence data for tasks such as sentiment analysis or language modeling.
7. Develop autoencoders to perform dimensionality reduction and image reconstruction, visualizing latent space representations.
8. Apply transfer learning by fine-tuning pre-trained CNN models like VGG16 or ResNet on new datasets.
9. Use regularization techniques such as dropout, batch normalization, and L2 regularization to reduce overfitting and improve model generalization.
10. Perform hyperparameter tuning by adjusting learning rates, batch sizes, and optimizers like SGD and Adam, using validation data to optimize performance.

EIT- 904	:	**Python Programming** **3-0-2**
Course category	:	Program Elective (PE)
Pre-requisite Subject	:	NIL
Contact hours/week	:	Lecture: 3, Tutorial: 0, Practical: 2
Number of Credits	:	4
Course Assessment methods	:	Continuous assessment through tutorials, attendance, home assignments, quizzes and One Minor tests and One Major Theory Examination
Course Objectives	:	Upon completion of a Python programming course, students will be able to develop programs using built-in data types, implement functions and data structures, and solve problems using object-oriented programming. They'll also be able to create applications with graphics, handle errors, and use various Python features like loops, conditionals, and file handling.
Course Outcomes	:	The students are expected to be able to demonstrate the following knowledge, skills and attitudes after completing this course:

1. Interpret the fundamental Python syntax and semantics and be fluent in the use of Python control flow statements.
2. Express proficiency in the handling of strings and functions.
3. Determine the methods to create and manipulate Python programs by utilizing the data structures like lists, dictionaries, tuples and sets.
4. Identify the commonly used operations involving file systems and regular expressions.
5. Articulate the Object-Oriented Programming concepts such as encapsulation, inheritance and polymorphism as used in Python.

UNIT-I 9

Introduction to Python: Python variables, Python basic Operators, Understanding python blocks. Python Data Types, Declaring and using Numeric data types: int, float etc. Python Program Flow Control Conditional blocks: if, else and else if, Simple for loops in python, for loop using ranges, string, list and dictionaries. Use of while loops in python, loop manipulation using pass, continue, break and else. Programming using Python conditional and loop blocks.

UNIT-II 9

Python Complex data types: Using string data type and string operations, Defining list and list slicing, Use of Tuple data type. String, List and Dictionary, Manipulations Building blocks of python programs, string manipulation methods, List manipulation. Dictionary manipulation, Programming using string, list and dictionary in-built functions. Python Functions, Organizing python codes using functions.

UNIT-III 9

Python File Operations: Reading files, Writing files in python, Understanding read functions, read(), readline(), readlines(). Understanding write functions, write() and writelines() Manipulating file pointer using seek Programming, using file operations.

UNIT-IV 9

Python packages: Simple programs using the built-in functions of packages matplotlib, numpy, pandas etc. GUI Programming: Tkinter introduction, Tkinter and PythonProgramming, Tk Widgets, Tkinter examples. Python programming with IDE.

Books & References:

1. Wesley J. Chun, "Core Python Applications Programming", 3rd Edition, Pearson Education, 2016.
2. Lambert, Fundamentals of Python: First Programs with MindTap, 2nd 1st edition, Cengage Learning publication.
3. Charles Dierbach, "Introduction to Computer Science using Python", Wiley, 2015.
4. Jeeva Jose &P.SojanLal, "Introduction to Computing and Problem Solving with PYTHON", Khanna Publishers, New Delhi, 2016.
5. Downey, A. et al., "How to think like a Computer Scientist: Learning with Python", John Wiley, 2015.
6. Mark Lutz, "Learning Python", 5th edition, Orelly Publication, 2013, ISBN 978- 1449355739.
7. John Zelle, "Python Programming: An Introduction to Computer Science", Second edition, Course Technology Cengage Learning Publications, 2013, ISBN 978- 1590282410.

Experiments:

1. Learn basic programming constructs –data types, decision structures, control structures in python.
2. Know how to use libraries for string manipulation and user-defined functions.
3. Learn to use in-built data structures in python – Lists, Tuples, Dictionary and File handling.
4. Know how to use functions and modules in Python to solve various problems.
5. Learn about Regular Expressions and work on some examples using Regular Expressions.