

**Vidya Pratishthan's
Kamalnayan Bajaj Institute of
Engineering and Technology
(Autonomous Institute)**



Faculty of Science and Technology

Board of Studies

Information Technology

Syllabus

Honor Courses

(2025 Pattern)
(w.e.f. AY: 2026-27)

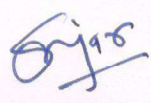
Bucket of HONORS DEGREE

HONORS DEGREE (only for students having CGPA ≥ 7.5)
Honor: Computational Intelligence
Honor: Cloud Computing and Virtualization, Data Science
Honor: Data Science
<u>Honor: Artificial Intelligence</u>
<u>Honor: Cyber security</u>
Honor: VLSI Design Technology
Honor: Advanced Communication Systems
Honor: Advances in Construction Technology
Honor: Advanced Structural Engg.
Honor: Robotics and Automation
Honor: Refrigeration & Air-conditioning
Honor: Renewable Energy and E- mobility

Syllabus: HONORS Information Technology
w. e. f. AY:2026-2027

Honors in Cyber Security

Sr. No.	Course Code	Courses Name	Teaching Scheme			Examination Scheme and Marks							Credits			
			TH	PR	TUT	CAA	ISE	ESE	TW	PR	OR	Total	TH	PR	TUT	Total
1	IT25281TH	Cryptography and Network Security	2	-	-	10	-	60	-	-	-	70	2	-	-	3
	IT25281PR	Cryptography and Network Security	-	2	-	-	-	-	30	-	-	30	-	1	-	
2	IT25291TH	Ethical Hacking	2	-	-	10	-	60	-	-	-	70	2	-	-	3
	IT25291PR	Ethical Hacking	-	2	-	-	-	-	30	-	-	30	-	1	-	
3	IT25381TH	Information Security	3	-	-	10	30	60	-	-	-	100	3	-	-	4
	IT25381PR	Information Security	-	2	-	-	-	-	30	-	-	30	-	1	-	
4	IT25391TH	Cyber Security	3	-	-	10	30	60	-	-	-	100	3	-	-	4
	IT25391PR	Cyber Security	-	2	-	-	-	-	30	-	-	30	-	1	-	
5	IT25491TH	Digital Forensics	3	-	-	10	30	60	-	-	-	100	3	-	-	4
	IT25491PR	Digital Forensics	-	2	-	-	-	-	30	-	-	30	-	1	-	
Total			13	10	0	50	90	300	150	0	0	590	13	5	0	18


Prof.S.A.Takale
HOD-IT

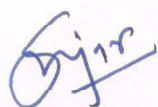

Prof.S.M.Bhosle
Dean Academics


Dr.A.H. Kolekar
CoE

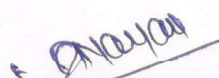

Prof.S.B.Lande
Principal

Honors in Artificial Intelligence

Sr. No.	Course Code	Courses Name	Teaching Scheme			Examination Scheme and Marks							Credits			
			TH	PR	TUT	CAA	ISE	ESE	TW	PR	OR	Total	TH	PR	TUT	Total
1	IT25282TH	Artificial Intelligence: Search Methods and Knowledge Representation	2	-	-	10	-	60	-	-	-	70	2	-	-	3
	IT25282PR	Artificial Intelligence: Search Methods and Knowledge Representation	-	2	-	-	-	-	30	-	-	30	-	1	-	
2	IT25292TH	Deep Learning for Computer Vision	2	-	-	10	-	60	-	-	-	70	2	-	-	3
	IT25292PR	Deep Learning for Computer Vision	-	2	-	-	-	-	30	-	-	30	-	1	-	
3	IT25382TH	Computer Vision	3	-	-	10	30	60	-	-	-	100	3	-	-	4
	IT25382PR	Computer Vision	-	2	-	-	-	-	30	-	-	30	-	1	-	
4	IT25392TH	Deep Learning for Natural Language Processing	3	-	-	10	30	60	-	-	-	100	3	-	-	4
	IT25392PR	Deep Learning for Natural Language Processing	-	2	-	-	-	-	30	-	-	30	-	1	-	
5	IT25492TH	Generative AI and Large Language Models	3	-	-	10	30	60	-	-	-	100	3	-	-	4
	IT25492PR	Generative AI and Large Language Models	-	2	-	-	-	-	30	-	-	30	-	1	-	
Total			13	10	0	50	90	300	150	0	0	590	13	5	0	18



Prof.S.A.Takale
HOD-IT



Prof.S.M.Bhosle
Dean Academics



Dr.A.H. Kolekar
CoE



Prof.S.B.Lande
Principal

Cryptography and Network Security								
Course Code : IT25281			Course Credits: 03			Course Type: HONOR		
Teaching Scheme			Evaluation Scheme					
TH	PR	TUT	CAA	ISE	ESE	TW	PR	OR
2	2	-	10	-	60	30	-	-
Prerequisite Course Mapping: 1.Basics of Computer Networks								
Future Course Mapping: Cyber Security								
Importance of Course: This Subject will help to get acquainted with skills and knowledge required network administrator.								
Course Objectives: 1.To learn network security concepts 2. To differentiate private and public key cryptography.								
Course Outcomes: 1.Understand Network security concepts 2.Identify software Vulnerabilities 3.Understand Private Key Cryptography 4.Understand and Analyse Public key cryptography								
Syllabus								
UNIT No.	Syllabus							Hrs.
I	Introduction to Security: Vulnerabilities, Threats, Threat Modeling, Risk, attack and attack types, Avoiding attacks, Security services. key security properties - Confidentiality, Integrity, Availability. Protocol Vulnerabilities: DoS and DDoS, session hijacking, ARP spoofing, Pharming attack, Dictionary Attacks.							6
II	Software vulnerabilities: Phishing, buffer overflow, Cross-site scripting attack, Virus and Worm Features, Trojan horse, Social engineering attacks, ransomware, SYN-Flooding, SQL- injection, DNS poisoning, Sniffing							6
III	Private Key Cryptography: Mathematical background for cryptography: modulo arithmetic, GCD (Euclid's algorithm), Role of random numbers in security, Importance of prime number, DES, AES. Chinese remainder theorem.							6

IV	Public key cryptography: RSA: RSA algorithm, Key generation in RSA, attacks on RSA. Diffie-Hellman key exchange	6
Text Books: 1. “Cryptography and Network Security-Principles and Practices” by William Stallings, Pearson Education, 2006, ISBN 81-7758-774-9, 4th Edition. 2. “Network Security and Cryptography”, by Bernard Menezes, Cengage Learning, 2010, ISBN 81 315-1349-1, 1st Edition.		
Reference Books: 1. “Computer Security: Art and Science”, by Matt Bishop, Pearson Education, 2002, ISBN 0201440997, 1st Edition. 2. “Network security, private communication in a public world”, by Charlie Kaufman, Radia Perlman and Mike Spencer, Prentice Hall, 2002, ISBN 9780130460196, 2nd Edition.		
Online Resources: https://archive.nptel.ac.in/courses/106/105/106105162/		
Cryptography and Network Security Lab		
Guidelines for Instructor's Manual: The faculty member should prepare the laboratory manual for all the assignments and it should be made available to students and laboratory instructor/Assistant.		
Guidelines for Student's Lab Journal: 1. Students should submit term work in the form of a handwritten journal based on a specified list of assignments. 2. Practical Examination will be based on the term work. 3. Students are expected to know the theory involved in the experiment. 4. The practical examination should be conducted if and only if the journal of the candidate is complete in all respects		
Guidelines for Lab /TW Assessment: 1.Examiners will assess the term work based on performance of students considering the parameters such as timely conduction of practical assignment, methodology adopted for implementation of practical assignment, timely submission of assignment in the form of handwritten write-up along with results of implemented assignment, attendance etc. 2.Examiners will judge the understanding of the practical performed in the examination by asking some questions related to theory & implementation of experiments he/she has carried out. Appropriate knowledge of usage of software and hardware related to respective laboratories should be as a conscious effort and little contribution towards Green IT and environment awareness, attaching printed papers of the program in a journal may be avoided. There must be hand-written write-ups for every assignment in the journal. 3.The HDD/SSD/USB drive containing student programs should be attached to the journal by every student and the same to be maintained by the department/lab In-charge is highly encouraged. For reference one or two journals may be maintained with program prints at Laboratory. Term work shall consist of 5 assignments and Practical's on each Unit-1 to Unit-4 and is based on performance and continuous internal assessment		

Guidelines for Laboratory Conduction:

- 1.All the assignments should be implemented.
- 2.All assignments are compulsory.
- 3.The instructor is expected to frame the assignments by understanding the prerequisites, technological aspects, utility and recent trends related to the topic.
- 4.All the assignments should be conducted on latest version of Windows OS and MS office.
- 5.The following practical should be conducted batch wise using Computer System, with Webcam and headphone facility.

Practical for the subject shall be engaged in minimum four batches (batch size of 20 students)

Guidelines for Practical Examination:

1. Both internal and external examiners should jointly set problem statements for practical examination. During practical assessment, the expert evaluator should give the maximum weightage to **the satisfactory** implementation of the problem statement.
2. The supplementary and relevant questions may be asked at the time of evaluation to judge the student's understanding of the fundamentals, effective and efficient implementation. The evaluation should be done by both external and internal examiners.

List of Assignments

- 1.Implement symmetric key algorithm.
- 2 Implement asymmetric key algorithm and key exchange Algorithm.
- 3.Demonstrate intrusion detection system using any tool.
- 4.Explore network monitoring tools as wire shark , snort etc.
- 5.Study to configure Firewall.
6. Study and analyse the Honey Pots.
7. Configuration of Virtual Private Network .
8. Study and Analyse Digital Signature standards.

Ethical Hacking								
Course Code : IT25291			Course Credits: 03			Course type: HONOR		
Teaching Scheme			Evaluation Scheme					
TH	PR	TUT	CAA	ISE	ESE	TW	PR	OR
2	2	–	10	-	60	30	-	-
Prerequisite Course Mapping: 1. Computer Network, Cyber security basics, operating system								
Future Course Mapping: 1. Certified Ethical Hacking, Ethical Hacking NPTEL								
Importance of Course: Ethical Hacking concepts will be understood and those are important to become cyber security analyst								
Course Objectives: 1. Understand Importance of Ethical Hacking and legalities of penetration Testing 2. Create awareness about web application security and Hacking 3. Analyze Meta sploit tool with Kali Linux for penetration testing 4. Apply WiFi Hacking and security Techniques								
Course Outcomes: 1. Identify Ethical hacking processes and become acquainted with Penetration testing. 2. Construct Secure Web Applications to understand Hacking Techniques. 3. Build knowledge about Meta sploit tool with Kali Linux 4. Recognize Wifi Hacking and Security techniques.								
Unit No.	Syllabus							Hrs.
1	Introduction to Basics of Ethical Hacking and Penetration Testing Introduction to basic Terminologies of Ethical Hacking, CIA(confidentiality, Integrity Availability , Types of Hackers , Ethical Hacking Process, Different tools for Ethical Hacking, Introduction to Kali Linux, What Is a Penetration Test, Vulnerability Assessments versus Penetration Test,Types of Penetration Testing:Network Penetration Test, Web Application Penetration Test,Mobile Application Penetration Test, Social Engineering Penetration Test, Physical Penetration Test							6
2	Web Application Hacking and Security Introduction to Hacking Web Applications, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), XML External Entity (XXE), Injections: SQL Injection& Code Injection, Denial of Service (DoS), Exploiting Third-Party Dependencies Web Application Security: Securing Modern Web Applications,							6

	Secure Application Architecture, OWASP Top 10 Web Application Security Risks and tools	
3	System Security and Hacking Introduction to Metasploit ,Reconnaissance with Metasploit , Port Scanning with Metasploit , Compromising a Windows Host with Metasploit ,Client Side Exploitation Methods , E– Mails with Malicious Attachments ,Creating a Custom Executable , Creating a Backdoor with SET – PDF Hacking – Social Engineering Toolkit – Browser Exploitation – Post– Exploitation Introduction :Cracking Passwords – Password Cracking Websites – Password Guessing – Password Cracking Tools – Password Cracking Countermeasures – Escalating Privileges – Executing Applications – Keyloggers and Spyware	6
4	Wi-Fi Hacking and Security Wi-Fi Security: Introduction to Wireless Security, Working, Types of Security, Protocols- WEP, WPA, WPA2 cracking, Threats to Wi-Fi Security, Secure Home and Business Wi-Fi Network, Stronger Wi-Fi Security, Updating WiFi Security Settings for Home WiFi Networks. Wi-Fi Hacking: Essential Tools for Hacking Wireless Networks, Evil Twin attack, Network Sniffing and social engineering	6
Practical Assignments		
Assign No	Title	
1	Study installation of Kali Linux	
2	Learn various tools related to security	
3	To perform reconnaissance on a website using google dorking technique on a tryhackme room. Perform Google Dorking: https://tryhackme.com/room/googledorking	
4	To perform reconnaissance on a website using web OSINT technique on a tryhackme room. Perform Web OSINT: https://tryhackme.com/room/webosint .	
5	Scanning, enumeration, and analysis: To perform scanning using nmap(a powerful network scanning tool) in a tryhackme room. Perform scanning using Nmap tools: https://tryhackme.com/room/furthernmap	
6	To perform scanning using nessus	
7	Perform vulnerability analysis using Nessus tool: https://tryhackme.com/room/rpnessusredux	
8	POST-EXPLOITATION: Perform Windows Privilege Escalation: https://tryhackme.com/room/windowsprivescarena	
9	Perform Post-Exploitation: https://tryhackme.com/room/postexploit Perform Linux	

	Privilege Escalation: https://tryhackme.com/room/linuxprivesc
10	Study Web application security tools
Text Books: 1. Rafay Baloch, “Ethical Hacking and Penetration Testing Guide”, CRC Press, 2014. 2. Andrew Hoffman, Web Application Security-Exploitation and Countermeasures for Modern Web Applications, O’Reilly publication 3. Marcus Pinto, Dafydd Stuttard, The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws, Wiley Publication 4. Alexis Ahmed, “Privilege Escalation Techniques, O'Reilly Media Company. Packt publishing. 2021	
Reference Books: 1. Hacking: The Art of Exploitation by Jon Erickson 2. Basics of Hacking and Penetration testing: Made Easy by Patrick Engebreston 3. Penetration Testing: A Hands-on Introduction to Hacking by Georgia Weidman	
Online Resources: 1. https://resources.infosecinstitute.com/topic/process-scanning-and-enumeration/ 2. https://owasp.org/Top10 3. https://medium.com/techloop/reconnaissance-the-key-to-ethical-hacking-3b853510d977	

Information Security								
Course Code : IT25381			Course Credits: 04			Course type: Honors		
Teaching Scheme			Evaluation Scheme					
TH	PR	TUT	CAA	ISE	ESE	TW	PR	OR
3	2	-	10	30	60	30	-	-
Prerequisite Course Mapping: 1.Basics of Computer Networks 2.Discrete Mathematics								
Future Course Mapping: 1.Cyber Security								
Course Objectives: 1.To understand the basic approaches in cyber security and Information Security 2. To analyze the cryptography and networking terms. 3. To Understand Cryptography and network basics. 4. To Use different authentication techniques 5. To study digital Signature.								
Course Outcomes: 1. Understand and explain the risks faced by computer systems and networks. 2. Identify and analyze security problems in computer systems and networks. 3. Explain how standard security mechanisms work. 4. Develop security mechanisms to protect computer systems and networks. 5. Design more secure information system. 6. Use cryptography algorithms and protocols to achieve computer security.								
UNIT No.	Syllabus							Hrs.
I	Introduction to Information Security : Attacks -Definition, Types Vulnerability, Security Goals, Security Services and Security mechanisms.							6
II	Conventional Cryptographic Techniques : Conventional substitution and transposition ciphers, One-time Pad, Block cipher and Stream Cipher, steganography.							6
III	Symmetric and Asymmetric Cryptographic Techniques : Data Encryption Algorithm (DES), Advanced Encryption Standard (AES), (Rivest–Shamir–Adelman)RSA, (Secure Hash Algorithm) SHA, (Message-Digest Algorithm 5) MD5 algorithms.							7
IV	Authentication and Digital Signatures : Use of Cryptography for authentication, Secure Hash function, Key management – Kerberos.							6
V	Program Security : Non malicious Program errors – Buffer overflow, Incomplete mediation, Time-of-check to Time-of use Errors, Viruses, Trapdoors, Salami attack, Man-in-the middle attacks, Covert channels.							7
VI	Security in Networks : Threats in networks, Network Security Controls – Architecture, Encryption, Content Integrity, Strong Authentication, Access Controls, Wireless Security, Honeypots, Traffic flow security, Firewalls –IDS, Email Security.							7

List of Practical Assignments:

Implement symmetric key algorithm.

2 Implement asymmetric key algorithm and key exchange Algorithm.

3. Demonstrate intrusion detection system using any tool.

4. Explore network monitoring tools as wire shark, snort etc.

5. Study to configure Firewall.

6. Study and analyze the Honey Pots.

7. Configuration of Virtual Private Network .

8. Study and Analyze Digital Signature standards.

Text Books :

1. Network Security Essentials: Applications and Standards, by William Stallings, Prentice Hall.

2. Security in Computing, Fourth Edition, by Charles P. Pfleeger, Pearson Education.

Reference Books:

1. Cryptography And Network Security Principles And Practice, Fourth or Fifth Edition, William Stallings, Pearson.

2. Modern Cryptography: Theory and Practice, by Wenbo Mao, Prentice Hall.

Online Resources:

1. https://onlinecourses.swayam2.ac.in/cec22_cs15/

2 <https://archive.nptel.ac.in/courses/106/106/106106129/>

Cyber Security								
Course Code : IT25391			Course Credits: 04		Course type: Honor			
Teaching Scheme			Evaluation Scheme					
TH	PR	TUT	CAA	ISE	ESE	TW	PR	OR
3	2	-	10	30	60	30	-	-
Prerequisite Course Mapping: Basics of computer network and computer programming								
Future Course Mapping: Quantum cryptography								
Course Objectives: 1. To understand the basic approaches in cyber security and Information Security. 2. To analyze the cryptography and networking terms. 3. To understand about different types of hacking and cyber-crimes. 4. To apply and analyze the issues related to cyber forensics. 5. To learn cyber security implications. 6. To understand privacy issues.								
Course Outcomes: 1. Understand various basic approaches in cyber security and Information Security. 2. Understand Cryptography and network basics. 3. To analyze the types of hacking and cyber crimes. 4. Understand cyber forensics. 5. Learn security implications. 6. Analyze privacy issues.								
UNIT No.	Syllabus							Hrs.
I	Introduction to Cyber Security, Information Security Basics Confidentiality, Integrity & Availability (CIA), The challenges of Security, Threats, Attacks, Operational Model of Security, Cryptography, Symmetric and Asymmetric Cryptography, Brute-Force Attack. Cyber Security Basics: Introduction to Cyber Security, Need, Importance and challenges in Cyber Security, Cyberspace, Cyber threats, Cyber-warfare, Cyber Terrorism.							8
II	Network Fundamentals, Cryptography Basics LAN, MAN, WAN, Wi-Fi, Network Protocols (TCP/IP, DNS, HTTP), Network Devices (Routers, Switches, Firewalls), Cryptography Basics: Encryption, Decryption, Types of Encryption (Symmetric Cipher-DES, Asymmetric Cipher-RSA, Diffie Hellman, Cryptographic Hash functions and Message Authentication codes).							6
III	Cyber Crimes and Hacking Cyber stalking, forgery, software piracy, cyber terrorism, phishing, computer hacking, creating and distributing viruses over the internet, spamming, cross site scripting, cybersquatting, logic bombs, web jacking, internet time thefts, DoS attack, Man in the middle attack, salami attack, data diddling, email spoofing, Types of Hacking.							7
IV	Cyber Forensics Cyber forensics, cyber forensics investigation process, digital evidence, challenges in cyber forensics, Web Attack Forensics: Intrusion forensics, database forensics, preventive forensics, Anti forensics practices, Anti-forensics detection techniques, Network forensics analysis tools, Email Forensics: e-mail Protocols, email crimes, email forensics, Bitcoin Forensics: crypto currency, crimes related to bitcoin.							6

V	Cyber Security- Organizational Implications: Introduction, cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for organizations.	6
VI	Privacy Issues: Basic Data Privacy Concepts: Fundamental Concepts, Data Privacy Attacks, Data linking and profiling, privacy policies and their specifications, privacy policy languages, privacy in different domains- medical, financial, etc Cybercrime: Examples and Mini-Cases Examples: Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions of Rupees, Parliament Attack, Pune City Police Bust Nigerian Racket, e-mail spoofing instances. MiniCases: The Indian Case of Online Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.	6
List of Practical Assignments: 1. Perform port scanning with nmap. 2. Install Wireshark and monitor network communication with sniffers. 3. Install Jscript/Cryptool tool (or any other equivalent) and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital/PKI signatures. 4. Study and execute OpenSSL commands to generate minimum 10 passwords of length 12 characters. 5. Perform email analysis using the Autopsy tool.		
Text Books : 1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley 2. B.B. Gupta, D.P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018. 3. Real Digital Forensics for Handheld Devices, E. P. Dorothy, Auerback Publications, 2013. 4. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.		
Reference Books: 1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press. 2. Introduction to Cyber Security, Chwan-Hwa(john) Wu, J. David Irwin, CRC Press T&F Group. 3. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010. 4. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C. H. Malin, E. Casey and J. M. Aquilina, Syngress, 2012. 5. The Best Damn Cybercrime and Digital Forensics Book Period, J. Wiles and A. Reyes, Syngress, 2007.		
Online Resources: 1. https://onlinecourses.nptel.ac.in/noc23_cs127/preview 2. https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=en-US		

Digital Forensics								
Course Code: IT25491			Course Credits: 04		Course type: Honors			
Teaching Scheme			Evaluation Scheme					
TH	PR	TUT	CAA	ISE	ESE	TW	PR	OR
3	2	-	10	30	60	30	-	-
Prerequisite Course Mapping: 1. Computer Network and Security 2. Cyber Security								
Future Course Mapping: Cyber Crime Investigation								
Course Objective: 1. To discuss the need and process of digital forensics and Incident Response Methodology. 2. To explore the procedures for identification, preservation, and acquisition of digital evidence. 3. To explore techniques and tools used in digital forensics for Operating system and malware investigation. 4. To explore techniques and tools used for Mobile forensics and browser, email forensics.								
Course Outcomes: On completion of the course, learner will be able to 1. Understand the phases of Digital Forensics and methodology to handle the computer security incident. 2. Analyze the process of collection, analysis and recovery of the digital evidence. 3. Explore various tools to analyze malwares and acquired images of RAM/hard drive. 4. Acquire adequate perspectives of digital forensic investigation in mobile devices 5. Analyze the source and content authentication of emails and browsers. 6. Produce unambiguous investigation reports which offer valid conclusions.								
UNIT No.	Syllabus							Hrs
I	Introduction to Digital Forensics Digital Forensics Definition, Digital Forensics Goals, Digital Forensics Categories - Computer Forensics, Mobile Forensics, Network Forensics, Database Forensics, Introduction to Incident - Computer Security Incident, Goals of Incident Response, CSIRT, Incident Response Methodology, Phase after detection of an incident							7
II	Digital Evidence, Forensics Duplication and Digital Evidence Acquisition Digital evidence, Types of Digital Evidence, Challenges in acquiring Digital evidence, Admissibility of evidence, Challenges in evidence handling, Chain of Custody, Digital Forensics Examination Process - Seizure, Acquisition, Analysis, Reporting. Necessity of forensic duplication, Forensic image formats, Forensic duplication techniques.							7
III	Forensics Investigation Analyzing Hard Drive Forensic Images, Analyzing RAM Forensic Image, Investigating Routers, Malware Analysis - Malware, Viruses, Worms, Essential skills and tools for Malware Analysis, List of Malware Analysis Tools and Techniques							6
IV	Windows and Unix Forensics Investigation Investigating Windows Systems - File Recovery, Windows Recycle Bin Forensics, Data Carving, Windows Registry Analysis, USB Device Forensics, File Format Identification, Windows Features Forensics Analysis, Windows 10 Forensics, Cortana Forensics, Investigating Unix Systems - Reviewing Pertinent Logs, Performing Keyword Searches,							6

	Reviewing Relevant Files, Identifying Unauthorized User Accounts or Groups, Identifying Rogue Processes, Checking for Unauthorized Access Points, Analyzing Trust Relationships.	
V	Mobile Forensics Android Forensics, Mobile Device Forensic Investigation - Storage location, Acquisition methods, Data Analysis, GPS forensics - GPS Evidentiary data, GPS Exchange Format (GPX), GPX Files, Extraction of Waypoints and Track Points, Display the Tracks on a Map. SIM Cards Forensics - The Subscriber Identification Module (SIM), SIM Architecture, Security, Evidence Extraction.	7
VI	Browser, Email Forensic & Forensic Investigation Reporting Web Browser Forensics, Google chrome, Other web browser investigation Email forensics - Sender Policy Framework (SPF), Domain Key Identified Mail (DKIM), Domain based Message Authentication Reporting and Confirmation (DMARC), Investigative Report Template, Layout of an Investigative Report, Guidelines for Writing a Report.	6
Total Teaching Hours		39
List of Practical Assignments: 1: To identify & study different types of Digital forensics. 2. To understand incident response process. 3. To study incident response process. 4. To create a forensic image of a USB drive. 5. To study Hard Drive Forensic Analysis. 6. To Investigate memory artifacts. 7. To analyze router logs. 8. To understand malware behavior. 9. To study Malware Analysis Tools. 10. To study Windows Registry Analysis & Linux Log Analysis.		
Text Books: 1. Kevin Mandia, Chris Prosise, —Incident Response and computer forensicsll, Tata McGrawHill, 2006. 2. Digital Forensics Basics A Practical Guide Using Windows OS — Nihad A. Hassan, APress Publication, 2019. 3. Xiaodong Lin, —Introductory Computer Forensics: A Hands-on Practical Approachll, Springer Nature, 2018 4. Computer Forensics: Computer Crime Scene Investigation, Author: John R. Vacca 5. Guide to Computer Forensics and Investigations, by Bill Nelson, Amelia Phillips, Christopher Steuart, Publisher: Cengage Learning 6. Digital Forensics, Author: Andre Arnes, Wiley Publication 7. Digital Forensics Basics: A Practical Guide Using Windows OS, Author: Nihad A. Hassan Publisher: Apress		
Reference Books: 1. Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, Christopher Steuart, Cengage Learning. 2. Digital Forensics and Incident Response, Gerard Johansen, Packt Publishing. 3. Practical Mobile Forensics, Rohit Tamma, Oleg Skulkin, Heather Mahalik, Satish Bommisetty, Packt Publishing.		

Online Resources:

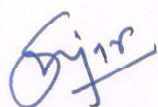
https://onlinecourses.nptel.ac.in/noc26_lw01/preview?

<https://nptel.ac.in/courses/106104467>

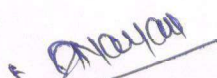
<https://nptel.ac.in/courses/106105217>

Honors in Artificial Intelligence

Sr. No.	Course Code	Courses Name	Teaching Scheme			Examination Scheme and Marks							Credits			
			TH	PR	TUT	CAA	ISE	ESE	TW	PR	OR	Total	TH	PR	TUT	Total
1	IT25282TH	Artificial Intelligence: Search Methods and Knowledge Representation	2	-	-	10	-	60	-	-	-	70	2	-	-	3
	IT25282PR	Artificial Intelligence: Search Methods and Knowledge Representation	-	2	-	-	-	-	30	-	-	30	-	1	-	
2	IT25292TH	Deep Learning for Computer Vision	2	-	-	10	-	60	-	-	-	70	2	-	-	3
	IT25292PR	Deep Learning for Computer Vision	-	2	-	-	-	-	30	-	-	30	-	1	-	
3	IT25382TH	Computer Vision	3	-	-	10	30	60	-	-	-	100	3	-	-	4
	IT25382PR	Computer Vision	-	2	-	-	-	-	30	-	-	30	-	1	-	
4	IT25392TH	Deep Learning for Natural Language Processing	3	-	-	10	30	60	-	-	-	100	3	-	-	4
	IT25392PR	Deep Learning for Natural Language Processing	-	2	-	-	-	-	30	-	-	30	-	1	-	
5	IT25492TH	Generative AI and Large Language Models	3	-	-	10	30	60	-	-	-	100	3	-	-	4
	IT25492PR	Generative AI and Large Language Models	-	2	-	-	-	-	30	-	-	30	-	1	-	
Total			13	10	0	50	90	300	150	0	0	590	13	5	0	18



Prof.S.A.Takale
HOD-IT



Prof.S.M.Bhosle
Dean Academics



Dr.A.H. Kolekar
CoE



Prof.S.B.Lande
Principal

Artificial Intelligence: Search Methods And Knowledge Representation								
Course Code : IT25282			Course Credits: 03			Course type: HONOR		
Teaching Scheme			Evaluation Scheme					
TH	PR	TUT	CAA	ISE	ESE	TW	PR	OR
2	2	-	10	-	60	30	-	-
Prerequisite Course Mapping: 1. Discrete Mathematics 2. Machine Learning 3. Data Structures and Algorithms								
Future Course Mapping: 1. Deep Learning for Computer Vision								
Importance of Course: This course forms the basis for all computer learning and is also the future of all complex decision making.								
Course Objectives: 1. Introduce the fundamental concepts, history, evolution, applications, and ethical implications of Artificial Intelligence. 2. Develop understanding of AI problem-solving, search methodologies, knowledge representation, and expert systems. 3. Explain intelligent agents, adversarial search, constraint satisfaction, optimization, and automated knowledge representation. 4. Develop skills in logical reasoning, logic programming, inference, and resolution for AI-based problem solving.								
Course Outcomes: 1. Understand fundamental concepts, evolution, applications, and ethical implications of Artificial Intelligence. 2. Apply problem-solving, search methodologies, knowledge representation, and expert-system techniques to AI problems. 3. Analyze and formulate problems using intelligent agents, adversarial search, constraint satisfaction, and optimization techniques. 4. Implement logical reasoning, logic programming, inference, and resolution techniques for developing AI-based reasoning systems.								
UNIT No.	Syllabus							Hrs.
I	Introduction to Artificial Intelligence: Overview of AI, History and evolution, Narrow vs. General AI, AI applications, Advances in AI, Impact on society and workforce, Ethical implications, Artificial Life, Learning principles							6
II	Problem Solving, Search Methodologies and Knowledge-Based Systems: Emergent Behavior, Expert Systems, Knowledge Representation, Problem Solving, Search Types, Methodologies, Classical & Beyond.							6
III	Game Theory and CSP: Adversarial Search and Games Adversarial Search, Intelligent Agents, Constraint Satisfaction, Optimization Problems							6
IV	Reasoning Systems and Automated Inference: Automated Knowledge Representation, Logic Reasoning, Reasoning Systems, Logic Programming, Inference and Resolution							6

List of Practical Assignments:

1. Develop a Python-based System using Object-Oriented Programming concepts. The application should demonstrate classes and objects, attributes, inheritance, method overloading and overriding, data hiding, exception handling, debugging, and logging.
2. Develop a Python program for mathematical and scientific computing using NumPy and SciPy. Perform array manipulation, matrix operations, mathematical computations, statistical operations, and numerical analysis on a given dataset.
3. Develop a database-driven web application using Python with Flask or Django. The application should perform database connectivity, CRUD operations, data migration, URL routing, request handling, and interaction with web resources using appropriate Python libraries.
4. Develop a Python-based data analysis and visualization application using Pandas, Matplotlib, Seaborn, Plotly, or ggplot. Perform data loading, cleaning, wrangling, manipulation, aggregation, analysis, and visualization on a real-world dataset using Anaconda or PyCharm.

Text Books :

1. Stuart Russel, Peter Norvig, "AI – A Modern Approach", Third Edition, Pearson Education, 2009 2.
2. Elaine Rich, Kevin Knight and Shivashankar B Nair", Artificial Intelligence ", Tata McGraw Hill Edition 3rd Edition, 2009
3. Patrick Henry Winston, Artificial Intelligence, 3rd Edition, Addison-Wesley.

Reference Books:

1. Ivan Bratko, Prolog Programming for Artificial Intelligence, 4th Edition, Pearson.
2. Patrick H. Winston, Artificial Intelligence, 3rd Edition, Addison-Wesley.
3. Allen B. Downey, "Think Stats", Second Edition, O'Reilly Media, ISBN: 978-1-491-90733-7
4. K. Boyer, L. Stark, H. Bunke, "Applications of AI, Machine Vision and Robotics, World Scientific PubCo, 1995

Online Resources:

1. <https://nptel.ac.in/courses/106102220>
2. http://onlinestatbook.com/Online_Statistics_Education.pdf
3. <https://london.ac.uk/sites/default/files/study-guides/introduction-to-natural-language-processing.pdf>
4. <https://www.deeplearningbook.org/contents/TOC.html>
5. <https://cvlesalfabegues.com/search/natural-language-understanding-2nd-edition/www.ebookphp.com/data-structures-and-algorithms-professional-edition-beginners-guide-epubpdf/>

Deep Learning For Computer Vision								
Course Code : IT25292			Course Credits: 03			Course type: HONOR		
Teaching Scheme			Evaluation Scheme					
TH	PR	TUT	CAA	ISE	ESE	TW	PR	OR
2	2	–	10	-	60	30	-	-
Prerequisite Course Mapping: 1. Machine Learning 2. Mathematics 1. Image Processing								
Future Course Mapping: Computer Vision								
Course Objectives: 1. Introduce the fundamental concepts of Computer Vision, image processing, and the relationship between Computer Vision and Natural Language Processing. 2. Develop understanding of image features and visual recognition techniques, including edge detection, interest points, corners, image classification, recognition, and Bag of Features. 3. Explain and apply deep learning architectures for Computer Vision, including and Vision Transformers. 4. Develop understanding of object detection and recognition techniques and transfer learning.								
Course Outcomes: 1. Analyze the fundamental concepts of Computer Vision, image processing, visual representations, and different levels of vision. 2. Apply feature extraction and visual recognition techniques for image classification, recognition, and large-scale image analysis. 3. Evaluate deep learning models and Vision Transformers for solving Computer Vision problems. 4. Design and implement deep learning-based object detection and recognition systems and transfer learning.								
Unit No.	Syllabus							Hrs.
1	Introduction and Overview: Introduction to Computer Vision, Computer Vision and Natural Language Processing, The Three R's of Computer Vision, Basics of Image Processing, Low, Mid & High-Level Vision							6
2	Deep Learning Review: Edge Detection, Interest Points and Corners, Image Classification, Recognition, Bag of Features, and Large-scale Instance Recognition, Vision Transformers, Object Detection & Transfer Learning							6

3	Deep Learning Model for Computer Vision: AlexNet, ResNet, Image Net, Introduction to Vision Transformers (ViT), Image Patch Embeddings, Self-Attention in Computer Vision, Gender Prediction, Face / Object Recognition	6
4	Deep Learning Model for object detection Algorithms - RCNN, Fast RCNN, Faster RCNN, Mask RCNN and YOLO.	6
Practical Assignments		
1. Implement basic image processing and feature extraction techniques using Python and OpenCV. Perform image resizing, grayscale conversion, filtering, edge detection, and detection of interest points and corners, and analyze the results. 2. Develop an image classification and recognition system using a Convolutional Neural Network. Train and evaluate the model on a suitable image dataset and analyze its classification performance. 3. Implement a deep learning-based image classification system using a pre-trained AlexNet or ResNet model with transfer learning. Perform image classification and evaluate the model using suitable performance measures. 4. Develop an object detection system using YOLO . 5. Implement a deep learning-based object detection and segmentation system using Faster R-CNN or Mask R-CNN		
Text Books: 1. Gonzalez & Woods, “Digital Image Processing”, Pearson Education 2. Richard Szeliski, Computer Vision: Algorithms and Applications		
Reference Books: 1. Ian Goodfellow, Yoshua Bengio, Aaron Courville, Deep Learning, 2016 2. Michael Nielsen, Neural Networks and Deep Learning, 2016 3. Yoshua Bengio, Learning Deep Architectures for AI, 2009 4. Richard Szeliski, Computer Vision: Algorithms and Applications, 2010. 5. Simon Prince, Computer Vision: Models, Learning, and Inference, 2012. 6. David Forsyth, Jean Ponce, Computer Vision: A Modern Approach, 2002.		
Online Resources: 1. https://onlinecourses.nptel.ac.in/noc21_cs93/preview 2. NPTEL Course on “Deep Learning”, by Prof. Prabir Kumar Bhiswas, IIT Kharagpur, Link of the Course: https://nptel.ac.in/courses/106105215 3. NPTEL Course on “Deep Learning - Part I”, by Prof. Sudarshan Iyengar, Prof Sanatan Sukhija IIT Ropar Link of the Course: https://nptel.ac.in/courses/106106184		