

Himachal Pradesh University

(NAAC Accredited “A” Grade University)

Summerhill, Shimla-171005,

Himachal Pradesh, India

Plan, Scheme, and Course Work Syllabus of

Doctor of Philosophy (Ph.D.)

in the

AI on Cyber Physical Systems

Under the

Faculty of Engineering and Technology

(Effective for the Batch 2026 and onwards)



Center for AI on Cyber Physical Systems

Himachal Pradesh University

(NAAC Accredited A" Grade University)

Summerhill, Shimla-171005

Himachal Pradesh University, Shimla

Vision of University:

The vision of the University is to disseminate and advance knowledge, wisdom and understanding by teaching and research, and by the example and influence of its corporate life.

Mission of University:

To work towards its vision, the University is committed to its mission to:

1. Advance learning and knowledge by teaching and research and by extension programs so as to enable a student to obtain advantages of university education.
2. Provide the right kind of leadership in all walks of life
3. Promote in the students and teachers an awareness and understanding of the social needs of the country and prepare them for fulfilling such needs
4. Take appropriate measures for promoting inter-disciplinary studies in the University
5. Foster the composite culture of India and establish such departments or institutions as may be required for the study and development of the languages, arts and culture of India
6. Make such provision for integrated courses in Humanities, Sciences and Technology in the educational programs of the University.

Vision of Centre:

To seamlessly integrate interdisciplinary technologies and design AI based Cyber Physical Components and systems.

Mission of Centre:

1. Training of the student for various AI & Cyber Physical Systems (CPS) technologies and principles.
2. To address the various technological issue of the Himachal Pradesh with the CPS set up such as smart health care, smart merchandise, smart agriculture, smart cities, intelligent traffic management system, power grid management and development of sector-specific solutions.
3. Secure communication system and Cyber security challenges using AI & CPS

Program's Vision:

To achieve excellence in research & technology and human resource development in the area of AI based CPS.

Program's Mission:

1. To provide multidisciplinary education, research & development solutions with focus on CPS using the AI.
2. The AI & CPS aims to unlock transformative possibilities in automation, data-driven decision-making, and human-machine collaboration.

3. To establish and strengthen the international collaborative research for cross-fertilization of ideas.
4. To provide high-quality trained professionals for the Institutions/ Industry in the country and worldwide.

Program Outcomes (POs) for Ph.D. in the Faculty of Engineering & Technology (Center for AI on Cyber Physical Systems)

PO1: Demonstrate the ability to conduct original research addressing advanced challenges in cyber-physical systems.

PO2: Exhibit proficiency in producing and presenting high-quality scholarly and technical communication in the domain of cyber-physical systems.

PO3: Demonstrate comprehensive doctoral-level knowledge of theories, methods, and emerging technologies in cyber-physical systems and related fields.

PO4: Demonstrate the ability to design, develop, and operate complex and integrated cyber-physical system architectures.

PO5: Critically evaluate the societal, ethical, and sustainability impacts of cyber-physical system technologies.

General Instructions/Guidelines for Execution of Curriculum

1. All candidates admitted to the Ph.D. program in the faculty of engineering & Technology (Center for AI on Cyber Physical Systems) must complete a minimum of **12 credits**.
2. There will be three courses in Ph.D. Program. The students must take 2 compulsory courses [**RPE-PhD and PhD-101**] and at least one additional course out of elective courses [**PhDCPS-102(i-x)**].
3. The detailed syllabi for the courses offered by the Department are appended with a list of suggested readings.

Academic Regulations:

These regulations are framed under the Ordinances of Himachal Pradesh University and are fully aligned with the University Grants Commission (Minimum Standards and Procedures for Award of Ph.D. Degree) Regulations, 2022. They apply to all candidates admitted to the Ph.D. program in the Faculty of Engineering & Technology (Center for AI on Cyber Physical Systems) programme offered by the Centre for AI on Cyber Physical Systems (CAICPS), HPU.

1. Eligibility and Admission

- 1.1 The Centre will admit the Ph.D. candidate from interdisciplinary field of Science and Engineering. A candidate must hold a Master's degree M.Sc. / M.Tech. / Int. M.Sc. (5 years integrated) in Physics / Instrumentation / Electronics/Computer Science. M.Sc./M.Tech. / Int. M.Sc. (5 years integrated) in Mathematics / Applied Mathematics / Industrial Mathematics / Statistics / Operations Research/Applied Operations Research / Mathematics and Computing /Master of Computer Application. M.E. / M.Tech./M.Tech (5 year integrated) in Information Technology/ Computer Science & Engg. / Software Engg. / Artificial Intelligence/Data Science/Electrical Engineering/ Instrumentation and Control Engineering/ Electronics & Communication/ Solid State Electronics Material/Photonics/Nanotechnology/Applied Optics/Optoelectronics and Optical

Centre for AI on Cyber Physical Systems

Communication/Microelectronics / VLSI /Microwaves/Communication Systems / Control Systems / Instrumentation / Circuits & Systems/Power Systems or equivalent. From a recognized university, with minimum marks/grades as prescribed by HPU & UGC time to time.

- 1.2 Admission shall be based on the University's notified process involving an entrance test (where applicable), research proposal/statement of purpose, and interview.
- 1.3 Reservation policy, fee structure, and documentation requirements shall follow HPU rules.

2. Registration and Allocation of Supervisor

- 2.1 After admission, candidates shall be registered as per university ordinances.
- 2.2 Supervisors shall be allotted as per HPU norms, considering eligibility, research specialization, and permissible limits of Ph. D scholars to the research supervisor.

- 2.3 Co-supervisors (internal or external) may be appointed as per university guidelines.

3. Duration of the Programme

- 3.1 Minimum period: Three years, including coursework.
3.2 Maximum period: As prescribed by HPU/UGC, with extensions allowed only under approved conditions.
3.3 Any break, leave, or extension must comply with university rules.

4. Ph.D. Coursework Requirements

- 4.1 All candidates must complete **a minimum of 12 credits**.
4.2 The coursework shall consist of:
 - **Research and Publication Ethics (RPE-PhD): 2 Credit**
 - **Research Methodology (PhDCPS-101): 5 Credits**
 - **At least one elective** from the approved list Coursework must normally be completed within the **first semester** of registration [**PhDCPS-102(i-xi)**] : **5 Credits**
4.3 Evaluation in each course shall comprise internal assessment and end-semester examination, with minimum passing marks/grade as per HPU norms.
4.4 A candidate who fails to complete coursework satisfactorily is liable for cancellation of registration.

5. Attendance and Academic Performance

- 5.1 Candidates must meet the attendance requirements stipulated by the Department/University for all coursework, seminars, and research meetings.
5.2 Poor performance or non-participation may result in probation or cancellation of registration based on evaluation by the Supervisory Committee.

6. Research Progress Monitoring

- 6.1 Progress shall be reviewed periodically through **Research Progress Seminars (RPS)** and written reports submitted to the Supervisory Committee.
6.2 A **pre-synopsis seminar** must be conducted before submission of the synopsis.
6.3 Continuation of registration each year depends on satisfactory progress.

7. Research Publication Requirement

The candidate should publish the research work in the journals and conference as per HPU guidelines.

8. Ethics, Plagiarism and Research Integrity

- 8.1 All research must comply with ethical standards applicable to AI and CPS research, field studies, and data handling.
8.2 The thesis, synopsis, and related submissions must undergo plagiarism checking as per HPU/UGC/INFLIBNET similarity thresholds.
8.3 Submissions exceeding the permissible similarity limit shall be returned for revision.

9. Synopsis Submission

- 9.1 Synopsis may be submitted only after completion of coursework and fulfilment of all progress requirements.
- 9.2 Supervisor recommendation and Departmental Research Committee approval are mandatory before submission to the University.

10. Thesis Submission, Evaluation and Viva-Voce

- 10.1 The Ph.D. thesis must be prepared in the prescribed format and submitted both in hard copy and electronic form as required by HPU.
- 10.2 The thesis shall be evaluated by at least two external examiners appointed as per UGC/HPU norms.
- 10.3 A candidate may appear in the open viva-voce only after receiving favorable reports from examiners.
- 10.4 Decisions on acceptance, corrections, or rejection shall follow University procedures.

11. Corrections and Resubmission

- 11.1 Candidates must complete examiner-recommended corrections within the specified time frame.
- 11.2 Resubmission and re-evaluation rules shall follow HPU ordinances.

12. Award of Degree

- 12.1 The Ph.D. degree shall be awarded upon:
 - successful completion of coursework
 - satisfactory progress reviews
 - publication fulfilment
 - acceptance of thesis
 - successful viva-voce defence
 - completion of all University formalities
- 12.2 An e-copy of the thesis must be deposited in INFLIBNET/Shodh ganga as per national requirements.

13. Leave, Suspension and Cancellation

- 13.1 Leave rules (casual, medical, maternity/paternity) follow HPU notifications.
- 13.2 Unauthorized absence or prolonged non-performance may lead to suspension or cancellation of registration.

14. Joint, Collaborative or Sandwich Ph.D. Provisions

- 14.1 Any collaborative, inter departmental, inter-university, or industry-linked component must receive prior approval from the University.
- 14.2 All such arrangements must comply with UGC and HPU norms.

15. Grievance Redressal and Academic Misconduct

- 15.1 Academic grievances, research disputes, and supervision issues shall be addressed through the Departmental Research Committee and University Grievance mechanisms.
- 15.2 Allegations of research misconduct shall be handled as per university disciplinary rules.

These regulations may be updated periodically by the Board of Studies, Faculty, and Academic Council to maintain conformity with UGC and University amendments.

Outline of the Course Work for Ph.D. in Cyber Physical Systems

Code	Title of Paper	Max Marks	Credits
RPE-PhD	Research and Publication Ethics	50	2
PhDCPS-101	Research Methodology	100	5
Elect any one of the following i.e. PhD-CPS-102 (i-X) (Elective)		100	5
PhDCPS-102(i)	Nano-photonics		
PhDCPS-102(ii)	Artificial Intelligence		
PhDCPS-102(iii)	Design of IOT		
PhDCPS-102(iv)	Advanced Network Security		
PhDCPS-102(v)	Sensors and Transducer		
PhDCPS-102(vi)	Electric Vehicles		
PhDCPS-102(vii)	Natural Language Processing		
PhDCPS-102(viii)	Cyber Security and Frauds		
PhDCPS-102(ix)	Health Data Management and Security		
PhDCPS-102(x)	Advanced Cyber Security		
PhDCPS-102(xi)	Advanced Wireless Networks		
Total Marks/Credits		250	12

Name of the Course	Research And Publication Ethics	
Course Code: RPE-PhD	Credits-2, MM-50	L-5, T-0, P-0
Course Objectives • Promote the importance of research integrity. • Discuss the principles of publication ethics. • Educate on identifying research misconduct and predatory publishing. • Discuss indexing and citation databases. • Provide information on open-access publications and research metrics. • Introduce various plagiarism detection tools.		
Evaluation Continuous assessment will be conducted through tutorials, assignments, quizzes, and group discussions. At the end of the course, a final written examination of 50 Marks will be conducted. 1. Students who have at least 75% attendance in classes will be considered eligible for the final written examination. 2. The exam will be conducted for a three-hour duration Note: The passing marks for Ph.D. course work will be 55% aggregate with minimum 50% in each individual course (All three courses).		
Note for Paper Setting <i>There will be 7 questions covering all the units. The first six questions (1, 2, 3, 4, 5 & 6) of 6 marks each will consist of one question from each unit, with internal choice provided, meaning there will be two questions from each unit. The 7th question will consist of 10 short answer type questions using Roman numerals (i, ii, iii,... x) each with 2 marks. There will be at least one question from each unit, and students will be required to attempt any seven questions out of ten.</i>		
Units	Syllabus	
Unit 1	1. Introduction to philosophy: definition, nature and scope, concept, branches 2. Ethics: definition, moral philosophy, nature of moral judgments and reactions	
Unit 2	1. Ethics with respect to science and research 2. Intellectual honesty and research integrity 3. Scientific misconducts: Falsification, Fabrication, and Plagiarism (FFP) 4. Redundant publications: duplicate and overlapping publications, salami slicing 5. Selective reporting and misrepresentation of data	
Unit 3	1. Publication ethics: definition, introduction, and importance 2. Best practices/standards setting initiatives and guidelines: COPE, WAME, etc. 3. Conflicts of interest 4. Publication misconduct: definition, concept, problems that lead to unethical behavior and vice versa, types 5. Violation of publication ethics, authorship and contributor ship 6. Identification of publication misconduct, complaints and appeals 7. Predatory publishers and journals	
Unit 4	1. Open-access publications and initiatives 2. SHERPA/ROMEO online resource to check publisher copyright & self-archiving policies 3. Software tool to identify predatory publications developed by SPPU 4. Journal finder/journal suggestion tools viz. JANE, Elsevier Journal Finder, Springer Journal, etc.	
Unit 5	A. Group Discussions 1. Subject-specific ethical issues, FFP, authorship 2. Conflicts of interest 3. Complaints and appeals: examples and fraud from India and abroad B. Software tools Use of plagiarism software like Turnitin, Urkund, and other open-source software tools	
Unit 6	A. Databases 1. Indexing databases 2. Citation databases: Web of Science, Scopus, etc. B. Research Metrics 1. Impact Factor of journal as per Journal Citation Report, SNIP, SJR, IPP, Cite Score 2. Metrics: h-index, g index, i10 index, altmetrics	
Course Outcomes (COs) At the end of the course students will be able to:		

CO1: Demonstrate conceptual understanding of philosophy of science, ethical reasoning, and research integrity, and relate these principles to responsible scientific practice.

CO2: Evaluate various forms of research and publication misconduct, including FFP, redundant publishing, authorship issues, conflict of interest, and selective reporting.

CO3: Apply ethical guidelines, open-access principles, journal evaluation tools, and plagiarism-detection software to ensure high-quality, ethical, and compliant research publication.

Suggested Readings:

- Beall, J. (2012). Predatory publishers are corrupting open access. *Nature*, Vol. 489(7415), 179. <https://doi.org/10.1038/489179a>.
- Bird, A. (2006). *Philosophy of Science*. Routledge.
- Bretag, Tracey (2016). *The Handbook of Academic Integrity*. Springer.
- Chaddah, P. (2018). *Ethics in Competitive Research: Do not get scooped; do not get Plagiarized*. ISBN:978- 9387480865.
- Grudniewicz, Agnes, D. Moher, Kelly D. Cobey+32 authors (2019). Predatory journals: no definition, no defense. *Nature*, Vol. 576.
- Indian National Science Academy (2019). *Ethics in Science Education, Research and Governance* (2019). ISBN:978-81-939482-1- 7. http://www.insaindia.res.in/pdf/Ethics_Book.pdf
- Israel, Mark, Iain Hay (2006). *Research Ethics for Social Scientists*. London.
- Lang, James M. (2013). *Cheating Lessons: Learning from Academic Dishonesty*. Harvard University Press.
- MacIntyre, Alasdair (1967). *A Short History of Ethics*. London.
- National Academy of Sciences, National Academy of Engineering and Institute of Medicine. (2009). *On Being a Scientist: A Guide to Responsible Conduct in Research*. Third Edition. National Academies Press.
- Resnik, D. B. (2011). What is ethics in research & why is it important. *National Institute of Environmental Health Sciences*, 1-10. <https://www.niehs.nih.gov/research/resources/bioethics/whatis/index.cfm>
- Whitley Jr., Bernard E. & Patricia Keith-Spiegel (2001). *Academic Dishonesty: An Educator's Guide*. Psychology Press.

Name of the Course		Research Methodology	
Course Code: PhD-CPS-101		Credits-5, MM-100	L-5, T-0, P-0
Course Objectives - To equip researchers with fundamental concepts of research design, problem formulation, hypothesis development, and literature review. - To develop competence in experimental design, analytical tools, research instrumentation, scientific writing, and proposal development.			
Evaluation Continuous assessment will be conducted through tutorials, assignments, quizzes, and group discussions. At the end of the course, a final written examination of 100 Marks will be conducted. 1. Students who have at least 75% attendance in classes will be considered eligible for the final written examination. 2. The exam will be conducted for a three-hour duration Note: The students can opt for MOOCs/SWAYAM and other accredited online platforms, with prior approval of relevant bodies. The passing marks for Ph.D. course work will be 55% aggregate with minimum 50% in each individual course (All three courses).			
Note for Paper Setting <i>There will be 11 questions covering all units. The first 10 questions of explanatory answers of 12 marks each will consist of one question from each unit with internal choice provided, meaning there will be two questions from each unit (5X2=10). The students will be required to attempt one question from each unit. The 11th question will consist of 10 short answer type questions using Roman numerals (i, ii,iii.....x) each with 5 marks covering with all the units. The students will be required to attempt any 8 questions out of 10.</i>			
Units	Syllabus		
Unit 1	Foundations of Research: Meaning, objectives of research; criteria of good research; basic steps of research; types of research. Problem Identification & Formulation: selection of research problem. Hypothesis: Qualities of a good Hypothesis, Null & Alternative Hypothesis, Hypothesis Testing, Logic & Importance Review of related literature: Meaning, necessity and sources.		
Unit 2	Research Process and Experiment Design: Concept and Importance in Research, features of a good research design. Exploratory Research Design concept, types and uses, Descriptive Research Designs concept, types and uses, Concept of Independent & Dependent variables. Research Report: Writing preliminaries, main body of research, references and bibliography.		
Unit 3	Research and Development of Projects: Project formulation, National and international funding agencies for R & D projects, proposal submission. Analytical Tools and Techniques in Research: Working principles, types, basic operation and application of Microscopy, Scanning Electron Microscopy (SEM), Transmission Electron Microscopy (TEM), Electrophoresis, Spectrophotometry, Chromatography and Mass spectrometry.		
Unit 4	Search engines: NCBI, PubMed, Google Scholar, Thomson Reuters, SCI etc, Reference Management Software like Zotero/Mendeley, Software for paper formatting like LaTeX/MS Office. Bioinformatics tools and applications.		
Unit 5	Writing Innovation: Introduction to Intellectual Property Rights (IPR), Basic forms of IPRs: – Patent, Copyright, Trademark, Designs, Process patent versus product patent, Art of writing a patent/innovation and claims, Preliminary patent. Intellectual Property, Patent Database Search and Patent.		
Course Outcomes (COs) At the end of the course students will be able to: CO1: Identify appropriate research designs, sampling methods, data collection approaches, and analytical techniques for scientific investigations. CO2: Apply core principles of research methodology to design, conduct, document, and communicate high-quality research work. CO3: At the end of the course students are able to understand how to set up the Research and development projects, paper writing methods.			
Suggested Readings: Council of Biology Editors–CRE Style Manual, American Institute of Biological Sciences,			

Washington. D.C.

- Effective Writing for Engineers, Managers, Scientists: Tichy AJIO.
- Scientific and Technical papers: Tribcase SF.
- How to write and publish a scientific paper: Day RA.
- Kothari, C. R. (2004). Research Methodology- Methods and Technique (New Age International, New Delhi)

Name of the Course	Nano-photonics	
Course Code: PhDCPS-102(i)	Credits-5, MM-100	L-5, T-0, P-0
Course Objectives - The course is aimed to: Expose them to the emerging area of nano photonic and the phenomena involved in such devices. - Provide deep understandings of light – matter interaction at Nano scale. - Study different types of nano photonic crystal-based devices and systems		
Course Evaluation Continuous assessment will be conducted through tutorials, assignments, quizzes, and group discussions. At the end of the course, a final written examination of 100 Marks will be conducted. 1. Students who have at least 75% attendance in classes will be considered eligible for the final written examination. 2. The exam will be conducted for a three-hour duration Note: The students can opt for MOOCs/SWAYAM and other accredited online platforms, with prior approval of relevant bodies. The passing marks for Ph.D. course work will be 55% aggregate with minimum 50% in each individual course (All three courses).		
Note for Paper Setting There will be 11 questions covering all units. The first 10 questions of explanatory answers of 12 marks each will consist of one question from each unit with internal choice provided, meaning there will be two questions from each unit (5X2=10). The students will be required to attempt one question from each unit. The 11th question will consist of 10 short answer type questions using Roman numerals (i, ii,iii.....x) each with 5 marks covering with all the units. The students will be required to attempt any 8 questions out of 10.		
Units	Syllabus	
Unit 1	Review Of Electro Magnetics: Maxwell equations Wave optics Electromagnetic radiations and evanescent waves Quantum mechanics and band theory of solids Particle wave duality Schrodinger equation and electron states Energy bands in solids Optical properties of bulk materials linear optical properties Nonlinear optical effects.	
Unit 2	Conventional Photonics: Fresnel Coefficients, Total internal reflection, Evanescent waves, Dielectric waveguides and cavities, Group velocity and density of states. Surface Plasmon Polaritons. Optical properties of noble metals, Nonlocal effects, Surface plasmon polaritons waveguides, Light focusing. Localized Surface Plasmons. Near-field enhancement and cross section. Simple geometries in the quasi-static limit. Quantum emitters. Purcell effect.	
Unit 3	Current Topics on Nano Photonics: Photonic Crystals, Meta materials, Super resolution imaging, Plasmonics in 2D materials, Super-Planckian radiative heat transfer.	
Unit 4	Silicon Photonics: Optical properties of silicon, Silicon-based photonic components and devices, Photonic crystals, 1D, 2D, and 3D photonic crystals Photonic crystal fibers Photonic Meta materials Electric, magnetic, negative index, and chiral Meta materials Applications of optical meta materials.	
Unit 5	Neuromorphic Photonics: Neuromorphic Computing Beyond von Neumann and Moore, Technology Platforms, Neuromorphic Microelectronics, Photonic Spike Processing, Photonic Reservoir Computing , Challenges for Integrated Neuromorphic Photonics, Photonic Neuron.	
Course Outcomes (COs) <i>At the end of the course students will be able to:</i> CO1: Gain the foundations of nano photonics. CO2: Understand the mathematical synthesis of Maxwell equations for Photonic systems. CO3: Acquire the understanding and importance of confinement and propagation. CO4: Obtain the knowledge of 1-D, 2-D and 3-D Photonic Crystals. CO5: Gain the design and scope of nano-photonics applications. CO6: Learn the foundation of plasmonics.		

Suggested Readings:

- L. Novotny and B. Hecht, Principles of Nano-Optics. Cambridge University Press, 2nd edition, 2012.
- J. D. Jackson, Classical Electrodynamics. Wiley, 3rd edition, 1999.
- S. A. Maier, Plasmonics: Fundamentals and Applications. Springer, 1st edition, 2007.

Name of the Course	Artificial Intelligence & Machine Learning	
Course Code: PhDCPS-102(ii)	Credits-5, MM-100	L-5, T-0, P-0
Course Objectives The objective of this subject is to be familiar with the applicability, strengths, and weaknesses of the basic knowledge representation, problem analyzing, and learning methods in solving particular engineering problems		
Course Evaluation Evaluation Continuous assessment will be conducted through tutorials, assignments, quizzes, and group discussions. At the end of the course, a final written examination of 100 Marks will be conducted. 1. Students who have at least 75% attendance in classes will be considered eligible for the final written examination. 2. The exam will be conducted for a three-hour duration Note: The students can opt for MOOCs/SWAYAM and other accredited online platforms, with prior approval of relevant bodies. The passing marks for Ph.D. course work will be 55% aggregate with minimum 50% in each individual course (All three courses).		
Note for Paper Setting There will be 11 questions covering all units. The first 10 questions of explanatory answers of 12 marks each will consist of one question from each unit with internal choice provided, meaning there will be two questions from each unit (5X2=10). The students will be required to attempt one question from each unit. The 11th question will consist of 10 short answer type questions using Roman numerals (i, ii,iii.....x) each with 5 marks covering with all the units. The students will be required to attempt any 8 questions out of 10.		
Units	Syllabus	
Unit 1	Fundamental Issues: Overview of AI problems, Examples of successful recent AI applications, Intelligent behavior, The Turing test, Rational versus nonrational reasoning, Problem characteristics: Fully versus partially observable, Single versus multi-agent, Deterministic versus stochastic, Static versus dynamic, Discrete versus continuous, Nature of agents: Autonomous versus semi-autonomous, Reflexive, Goal-based, and Utility- based, Importance of perception and environmental interactions, Philosophical and ethical issues.	
Unit 2	Basic Search Strategies: Problem spaces (states, goals and operators), Problem solving by search, Factored representation (factoring state into variables), Uninformed search (breadth-first, depth-first, depth-first with iterative deepening), Heuristics and informed search (hill-climbing, generic best-first, A*), Space and time efficiency of search, Constraint satisfaction (backtracking and local search methods). Advanced Search: Constructing search trees, Dynamic search space, Combinatorial explosion of search space, Stochastic search: Simulated annealing, Genetic algorithms, Monte-Carlo tree search, Implementation of A* search, Beam search, Minimax Search, Alpha-beta pruning, Expectimax search (MDP-solving) and chance nodes.	
Unit 3	Knowledge Representation: Propositional and predicate logic, Resolution in predicate logic, Question answering, Theorem proving, Semantic networks, Frames and scripts, conceptual graphs, conceptual dependencies. Reasoning under Uncertainty: Review of basic probability, Random variables and probability distributions: Axioms of probability, Probabilistic inference, Bayes' Rule, Conditional Independence, Knowledge representations using Bayesian Networks, Exact inference and its complexity, Randomized sampling (Monte Carlo) methods (e.g. Gibbs sampling), Markov Networks, Relational probability models, Hidden Markov Models, Decision Theory Preferences and utility functions, Maximizing expected utility	
Unit 4	Agents: Definitions of agents, Agent architectures (e.g., reactive, layered, cognitive), Agent theory, Rationality, Game Theory Decision-theoretic agents, Markov decision processes (MDP), Software agents, Personal assistants, and Information access Collaborative agents, Information- gathering agents, Believable agents (synthetic characters, modeling emotions in agents), Learning agents, Multi-agent systems Collaborating agents, Agent teams, Competitive agents (e.g., auctions, voting), Swarm systems and Biologically inspired models Expert Systems: Architecture of an expert system, existing expert systems: MYCIN, RI. Expert system shells.	
Unit 5	Introduction: Defining learning systems, Goals and applications of machine learning.	

	Aspects of developing a learning system: training data, concept representation, function approximation, supervised learning, unsupervised learning, Reinforcement learning, learning algorithms. Decision Tree Learning: Representing concepts as decision trees. Recursive induction of decision trees. Picking the best splitting attribute: entropy and information gain. Searching for simple trees and computational complexity, Overfitting, noisy data, and pruning.
Course Outcomes (COs) <i>At the end of the course students will be able to:</i> CO1: The students will be able to. Analyze the applications of artificial intelligence and categorize various problem domains, uninformed and informed search methods. CO2: Identify advanced search techniques and algorithms like mini max for game playing. Recognize the importance of probability in knowledge representation for reasoning under uncertainty. CO3: Describe Bayesian networks and drawing Hidden Markov Models. CO4: Interpret the architecture for intelligent agents and implement an intelligent agent.	
Suggested Readings: • Rich E., Artificial Intelligence, Tata McGraw Hills (2009)3rded. • George F. Luger, Artificial Intelligence: Structures and Strategies for Complex Problem Solving, Pearson Education Asia (2009)6thed. • Patterson D.W, Introduction to AI and Expert Systems, McGraw Hill (1998), 1sted. • Shivani Goel, Express Learning- Artificial Intelligence, Pearson Education Asia (2013),1sted.	

Name of the Course	Design For IOT	
Course Code: PhDCPS-102(iii)	Credits-5, MM-100	L-5, T-0, P-0
Course Objectives - Students will be able to understand the concepts of Internet of Things (IoT) and can able to build IoT based applications. - The students able to develop network and communication protocol, using IOT based systems. - The students will able to develop Experiments with Arduino Hardware and sensor interfacing procedures.		
Course Evaluation Evaluation Continuous assessment will be conducted through tutorials, assignments, quizzes, and group discussions. At the end of the course, a final written examination of 100 Marks will be conducted. 1. Students who have at least 75% attendance in classes will be considered eligible for the final written examination. 2. The exam will be conducted for a three-hour duration Note: The students can opt for MOOCs/SWAYAM and other accredited online platforms, with prior approval of relevant bodies. The passing marks for Ph.D. course work will be 55% aggregate with minimum 50% in each individual course (All three courses).		
Note for Paper Setting There will be 11 questions covering all units. The first 10 questions of explanatory answers of 12 marks each will consist of one question from each unit with internal choice provided, meaning there will be two questions from each unit (5X2=10). The students will be required to attempt one question from each unit. The 11th question will consist of 10 short answer type questions using Roman numerals (i, ii,iii.....x) each with 5 marks covering with all the units. The students will be required to attempt any 8 questions out of 10.		
Units	Syllabus	
Unit 1	Introduction to IoT: Defining IoT, Characteristics of IoT, Physical design of IoT, Logical design of IoT, Functional blocks of IoT, Communication models & APIs IoT& M2M: Machine to Machine, Difference between IoT and M2M, Software define Network Sensors and Actuators modules: Concept, layout, working and applications of different sensors and actuators: temperature sensor, motion sensor LDR sensors, IR sensor, Ultrasonic sensor, Relay etc.	
Unit 2	Embedded Systems for IoT: Introduction to Arduino Programming, Arduino interfacing with sensors and actuators, IoT based actuator operation using Arduino, Introduction to R-pi and its Programming, R-pi hardware interfacing and applications, Smartphone interfacing with R-pi, Wi-Fi module interfacing with R-pi and associated applications.	
Unit 3	Network and Communication Protocol: Wireless medium access issues, MAC protocol survey, Constrained Application Protocol (CoAP), Message Queue Telemetry Transport Protocol (MQTT), Sensor deployment & Node discovery, Data handling and analytics, Cloud platform for IoTs.	
Unit 4	Developing IoT based Systems: Experiments with Arduino Hardware and sensor interfacing procedures. Automatic lighting control using IoT, home automation, connected health, smart farming, industry applications, connected vehicles, smart city, developing sensor-based application through embedded system platform. Introduction to Python, Implementing IoT concepts with python Challenges in IoT: Design challenges, Development challenges, Security challenges, other challenges.	
Unit 5	Description Logic (DL), Structure Matching, Classification Extensions of DL, The ALC Language, Inheritance in Taxonomies Default Reasoning, Circumscription, The Event Calculus Revisited Default Logic, auto epistemic Logic, Epistemic Logic, Multi Agent Scenarios.	
Course Outcomes (COs) <i>At the end of the course students will be able to:</i> CO1: On successful completion of the course, the student will be able to: Recognize the concepts of Internet of Things. CO2: Demonstrate the interfacing of different sensors and actuators modules with embedded systems. CO3: Analyze basic protocols in wireless sensor network.		

CO4: Design IoT applications in different domain and be able to analyze their performance.

CO5: Develop and implement IoT applications using Python.

Suggested Readings:

- Vijay Madisetti, Arshdeep Bahga, “Internet of Things: A Hands-On Approach”.
- Adrian McEwen, Hakim Cassimally, "Designing the Internet of Things" John Wiley (2014)1sted.
- Hanes David ,Salgueiro Gonzalo, Grossetete Patrick, Barton Rob, Henry Jerome,” IoT Fundamentals: Networking Technologies, Protocols and Use Cases for the Internet of Things”, Pearson(2016).

Name of the Course	Advanced Network Security	
Course Code: PhDCPS-102(iv)	Credits-5, MM-100	L-5, T-0, P-0
Course Objectives - To describe the following electronic payment systems: NetBill, PayWords, MicroMint, fair exchange protocols. - To explain the two types of group management techniques: group key agreement and group key distribution. - To explain at least on secure MANET routing protocol.		
Course Evaluation Evaluation Continuous assessment will be conducted through tutorials, assignments, quizzes, and group discussions. At the end of the course, a final written examination of 100 Marks will be conducted. 1. Students who have at least 75% attendance in classes will be considered eligible for the final written examination. 2. The exam will be conducted for a three-hour duration Note: The students can opt for MOOCs/SWAYAM and other accredited online platforms, with prior approval of relevant bodies. The passing marks for Ph.D. course work will be 55% aggregate with minimum 50% in each individual course (All three courses).		
Note for Paper Setting There will be 11 questions covering all units. The first 10 questions of explanatory answers of 12 marks each will consist of one question from each unit with internal choice provided, meaning there will be two questions from each unit (5X2=10). The students will be required to attempt one question from each unit. The 11th question will consist of 10 short answer type questions using Roman numerals (i, ii,iii.....x) each with 5 marks covering with all the units. The students will be required to attempt any 8 questions out of 10.		
Units	Syllabus	
Unit 1	Introduction to the Concepts of Security: The need for security, Security Approaches, Principles of Security, Types of Attacks. Cryptographic Techniques: Plain Text and Cipher Text, Substitution Techniques, Transposition Techniques, Encryption and Decryption, Symmetric and Asymmetric Key Cryptography, Steganography, Key Range and Key Size, Possible Types of Attacks.	
Unit 2	Modular arithmetic, prime numbers, relative prime numbers, Euler’s function, GCD. Computer based Symmetric Key Cryptographic Algorithms: Algorithm Types and Modes, International Data Encryption Algorithm (IDEA), RC5, Blowfish, AES, Differential and Linear Cryptanalysis.	
Unit 3	Computer-based Asymmetric Key Cryptography: Brief History of Asymmetric Key Cryptography, An overview of Asymmetric Key Cryptography, Rabin Algorithm, Elgamal Algorithm, Knapsack Algorithm, ID-based cryptography.	
Unit 4	Public Key Infrastructure: Digital Certificates, Private Key Management, The PKI Model, Internet Security Protocols: Secure Socket Layer, Secure Electronic Transaction, SHTTP, Time Stamping Protocol, 3-D Secure Protocol, Electronic payment systems: Electronic billing systems, Micropayments, Fair exchange protocols, E-mail Security.	
Unit 5	Understanding Session Hijacking, Spoofing, TCP Concepts Sequence numbers. Sniffing, RDDoS, XSS Attack, WLAN Scanners, Securing Wireless Networks, Anonymous Wireless Communication, Jamming and anti-jamming techniques for wireless networks.	
Course Outcomes (COs) At the end of the course students will be able to: CO1: Have a knowledge of the threats faced by computer operating systems, applications and networks that originate from network-based attacks, intrusion and misuse CO2: Have a knowledge of the types of countermeasures that can be put in place in computer systems, networks, and network infrastructures to identify, reduce or prevent problems caused by network attacks or misuse. CO3: Be capable of making informed choices of the appropriate countermeasures that should be put in place to protect systems from network attacks or misuse and to maintain network security.		

Suggested Readings:

- Cryptography and Network Security by Behrouz A. Forouzan, 2nd Edition TMH.
- Cryptography and Network Security, W. Stallings, Prentice Hall, 5th Edition, 2010.
- Network Security Essentials, William Stallings, Prentice Hall, 5th Edition, 2013.
- Firewalls and Internet Security, William R. Cheswick and Steven M. Bellovin, Addison-Wesley Professional, 2nd Edition, 2003.
- Hackers Beware, Eric Core, EC-Council Press, 2003

Name of the Course		Sensors and Transducer	
Course Code: PhDCPS-101(v)		Credits-5, MM-100	Duration-3 Hrs.
Course Objectives • Introduce the students to sensors, as transducers from physical parameters to signals. • Explain the sensor range, sensitivity, accuracy, repeatability, and noise. • To provide a strong foundation in subject fundamentals required to solve industry-based problems. • To acquire the basic knowledge of transducers and signal conditioning for research applications.			
Evaluation Continuous assessment will be conducted through tutorials, assignments, quizzes, and group discussions. At the end of the course, a final written examination of 100 Marks will be conducted. 1. Students who have at least 75% attendance in classes will be considered eligible for the final written examination. 2. The exam will be conducted for a three-hour duration Note: The students can opt for MOOCs/SWAYAM and other accredited online platforms, with prior approval of relevant bodies. The passing marks for Ph.D. course work will be 55% aggregate with minimum 50% in each individual course (All three courses).			
Note for Paper Setting <i>There will be 11 questions covering all units. The first 10 questions of explanatory answers of 12 marks each will consist of one question from each unit with internal choice provided, meaning there will be two questions from each unit (5X2=10). The students will be required to attempt one question from each unit. The 11th question will consist of 10 short answer type questions using Roman numerals (i, ii,iii.....x) each with 5 marks covering with all the units. The students will be required to attempt any 8 questions out of 10.</i>			
Units	Syllabus		
Unit 1	Introduction to transducer and sensor: Definitions, terminology, classification, Static vs dynamic properties of transducers, Transfer functions, Ideal and realistic transducer models, Resolution, linearization, dynamic range, detection threshold, Selectivity & sensitivity, Difference between sensor and transducer.		
Unit 2	Type of Transducer: Strain, vibration, pressure, Flow, temperature, force, torque, liquid level, Humidity, P. H. value, velocity (angular and linear) etc. Basic principles of resistive transducers, Inductive transducers, capacitive transducers, Thermoelectric transducers, Piezoelectric transducers, Hall effect transducers, Electromechanical transducers, Photoelectric transducers, Digital transducers.		
Unit 3	Signal Processing Circuits: Introduction, ideal op-amp, Operational amplifier specifications, zero crossing detector, zero crossing detector with Hysteresis, inverting and non-inverting amplifiers, Voltage-follower, adder, subtractor, integrator, Differentiator, voltage to current converter, current to voltage converter, Phase shifter circuit, Absolute-Value circuit, Peak detector, AC to DC converter, Instrumentation amplifier.		
Unit 4	Data Display and Recording Systems: Introduction to Analog and digital display methods, Analog Recorders, C.R.O., digital input output Devices, Digital frequency meter, Digital Voltmeter.		
Unit 5	Data Transmission and Telemetry: Introduction, Methods of data transmission, General telemetering system, Electrical telemetering systems, Transmission channels and media, Multiplexing in telemetering systems, Characteristics of Frequency division multiplexing, Time-division multiplexing.		
Course Outcomes (COs) At the end of the course students will be able to: CO1: Describe working principles of sensors and transducers. CO2: Understand working principle of transducers used for measurement and comparative study of various transducers. CO3: The Understanding of different transducers and sensors for applications in industry. CO4: Develop understanding of real-world needs by studying the different case studies.			
Suggested Readings:			

- A course in Electrical, Electronic Measurements and Instrumentation by A.K. Sawhney, Dhanpat Rai & Sons.
- Transducers and Instrumentation by D.V.S. Murty, Prentice Hall of India Private Limited.
- Measurement Systems (Application & Design) by Ernest O. Doebelin, McGraw Hill Higher Education, New Delhi.
- Instrumentation Devices and Systems by C.S. Rangan, G.R. Sharma, and V.S.V. Mani, TMH New Delhi.
- Operational Amplifiers and Linear Integrated Circuits by Robert F. Coughlin and Frederick F. Driscoll, Prentice-Hall of India.

Name of the Course	Electric Vehicles	
Course Code: PhDCPS-101(vi)	Credits-5, MM-100	Duration-3 Hrs
Course Objectives - Comprehend the basics concepts of electric vehicles, their architecture, and technologies. - Able to understand the operation of battery driven and designing of Battery Pack. - Able to interpret the working of different electrical machines in electric vehicles and their control technique. - Ability to understand the control and configurations of EV chargers and charging stations.		
Evaluation Continuous assessment will be conducted through tutorials, assignments, quizzes, and group discussions. At the end of the course, a final written examination of 100 Marks will be conducted. 1. Students who have at least 75% attendance in classes will be considered eligible for the final written examination. 2. The exam will be conducted for a three-hour duration Note: The students can opt for MOOCs/SWAYAM and other accredited online platforms, with prior approval of relevant bodies. The passing marks for Ph.D. course work will be 55% aggregate with minimum 50% in each individual course (All three courses).		
Note for Paper Setting <i>There will be 11 questions covering all units. The first 10 questions of explanatory answers of 12 marks each will consist of one question from each unit with internal choice provided, meaning there will be two questions from each unit (5X2=10). The students will be required to attempt one question from each unit. The 11th question will consist of 10 short answer type questions using Roman numerals (i, ii,iii.....x) each with 5 marks covering with all the units. The students will be required to attempt any 8 questions out of 10.</i>		
Units	Syllabus	
Unit 1	Vehicle Dynamics: Forces and aerodynamic drag, rolling resistance and uphill resistance, power and torque to accelerate, concept of drive cycles and energy, design of EV drive train.	
Unit 2	EV Battery Pack: Introduction to battery parameters, Li-Ion battery cells, SoH and SoC estimation and self-discharge, battery pack development, computation of effective cost of battery and batteries charging.	
Unit 3	Battery Pack Design: Mechanical Design and Thermal Design, Electrical Design, BMS Design of Electric Vehicle, Cell Testing & Characterization.	
Unit 4	EV Motors and Controllers: Vehicle Dynamics, Power and Efficiency, Torque Production, Speed and Back EMF, Field oriented control of induction machines, BLDC motor, Modelling of PMSM Drives, Vector Control of PMSM Drives.	
Unit 5	EV Chargers: Introduction, Slow or Fast chargers, Battery Swapping, Standardization and on-board Chargers, Public Chargers, Bulk Chargers/Swap Stations	
Course Outcomes (COs) <i>At the end of the course students will be able to:</i> CO1: Analyze vehicle dynamic forces and evaluate the effect of aerodynamic drag, rolling resistance, and road gradients on electric vehicle performance. CO2: Design EV battery packs considering mechanical, thermal, electrical aspects along with BMS architecture, and perform cell testing and characterization. CO3: Evaluate different types of EV motors and controllers, including torque production, efficiency, back-EMF CO4: Compare EV charger types, standards, on-board/off-board chargers, and assess suitability of slow/fast charging and battery swapping systems for various EV applications.		
Suggested Readings: - Husain, Iqbal. Electric and hybrid vehicles: design fundamentals. CRC press, 2021. - Denton, Tom. <i>Electric and hybrid vehicles</i>. Routledge, 2020. - Ehsani, Mehrdad, Yimin Gao, Stefano Longo, and Kambiz Ebrahimi. <i>Modern electric, hybrid electric, and fuel cell vehicles</i>. CRC press, 2018.		

Name of the Course		Natural Language Processing	
Course Code: PhDCPS-101(vii)		Credits-5, MM-100	Duration-3 Hrs
Course Objectives - To understand natural language processing and to learn how to apply basic algorithms in this field. - To get acquainted with the algorithmic description of the main language levels: morphology, syntax, semantics, and pragmatics, as well as the resources of natural language data - corpora. - To conceive basics of knowledge representation, inference, and relations to the artificial intelligence			
Evaluation Continuous assessment will be conducted through tutorials, assignments, quizzes, and group discussions. At the end of the course, a final written examination of 100 Marks will be conducted. 1. Students who have at least 75% attendance in classes will be considered eligible for the final written examination. 2. The exam will be conducted for a three-hour duration Note: The students can opt for MOOCs/SWAYAM and other accredited online platforms, with prior approval of relevant bodies. The passing marks for Ph.D. course work will be 55% aggregate with minimum 50% in each individual course (All three courses).			
Note for Paper Setting <i>There will be 11 questions covering all units. The first 10 questions of explanatory answers of 12 marks each will consist of one question from each unit with internal choice provided, meaning there will be two questions from each unit (5X2=10). The students will be required to attempt one question from each unit. The 11th question will consist of 10 short answer type questions using Roman numerals (i, ii,iii.....x) each with 5 marks covering with all the units. The students will be required to attempt any 8 questions out of 10.</i>			
Units	Syllabus		
Unit 1	Introduction: Introduction to the Morphology, Syntax, Semantics by linking the “linguistics view” (computational linguistics) with the “artificial intelligence view” (natural language processing).		
Unit 2	Morphology: Analysis and generation of language on word level: e.g. problems with compounding and idiomatic phrases, homophonous strings as well as loan words and their processing using e.g. finite state automata as well as semantic networks. Ambiguities in words like “pen” and “pipe”, but will also discuss some complex strings.		
Unit 3	Syntax: Analysis and generation of language on phrasal and sentence level: e.g. applications such as machine translation and grammar checking and the processing using phase structure PhDCSPET008 NATURAL LANGUAGE PROCESSING L T P C Version 1.0 Date of Approval: 3 1 0 4 grammars as well as unification-based formalisms and relating those formalisms to recursive transition networks (RTNs) as well as augmented transition networks (ATNs).		
Unit 4	Semantics: Language ambiguities on the level of “meaning”: represented by case structures and conceptual dependency structures. We will look at famous utterances such as: Colorless green ideas sleep furiously. And will discuss why the machine runs into problems during analysis, and how these problems can be overcome.		
Unit 5	Applications of NLP: Machine Translation, Grammar Checkers Dictation, Automatic Document Generation, NL Interfaces.		
Course Outcomes (COs) <i>At the end of the course students will be able to:</i> CO1: The students will get acquainted with natural language processing and learn how to apply basic algorithms in this field. CO2: They will understand the algorithmic description of the main language levels: morphology, syntax, semantics, and pragmatics, as well as the resources of natural language data - corpora. CO3: They will also grasp basics of knowledge representation, inference, and relations to the artificial intelligence.			
Suggested Readings: Daniel Jurafsky, James H. Martin “Speech and Language Processing” Second Edition, Prentice Hall, 2008.			

- Chris Manning and Hinrich Schütze, “Foundations of Statistical Natural Language Processing”, MIT Press. Cambridge, MA: May 1999.
- Allen, James, Natural Language Understanding, Second Edition, Benjamin/Cumming, 1995. 4. Charniack, Eugene, Statistical Language Learning, MIT Press, 1993.

Name of the Course	Cyber Security and Frauds	
Course Code: PhDCPS-102(viii)	Credits-5, MM-100	L-5, T-0, P-0
Course Objectives - Understand fundamental cybersecurity concepts, cryptographic methods, and common attack types. - Apply AI and machine learning techniques to enhance security and mitigate related risks. - Recognize and counter threats in datasets, networks, and IoT environments using ML-enabled anomaly-detection approaches. - Analyze and mitigate emerging AI-driven threats such as deepfakes, Gen-AI risks, and cloud-based security challenges.		
Course Evaluation Evaluation Continuous assessment will be conducted through tutorials, assignments, quizzes, and group discussions. At the end of the course, a final written examination of 100 Marks will be conducted. 1. Students who have at least 75% attendance in classes will be considered eligible for the final written examination. 2. The exam will be conducted for a three-hour duration Note: The students can opt for MOOCs/SWAYAM and other accredited online platforms, with prior approval of relevant bodies. The passing marks for Ph.D. course work will be 55% aggregate with minimum 50% in each individual course (All three courses).		
Note for Paper Setting There will be 11 questions covering all units. The first 10 questions of explanatory answers of 12 marks each will consist of one question from each unit with internal choice provided, meaning there will be two questions from each unit (5X2=10). The students will be required to attempt one question from each unit. The 11th question will consist of 10 short answer type questions using Roman numerals (i, ii,iii.....x) each with 5 marks covering with all the units. The students will be required to attempt any 8 questions out of 10.		
Units	Syllabus	
Unit 1	Fundamentals of Cyber Security, Privacy, Confidentiality, Integrity and Authentication, Anonymity, Cryptographic Algorithm, Types of attacks and Security assessment.	
Unit 2	AI for Security, Using AI models to ensure security, Algorithms, Benefits and Threats to AI models, Securing a machine learning system, Types of attacks on a machine learning system, Mitigation of risks.	
Unit 3	Dataset related threats, Data corruption cases, Feature Manipulation threat cases, Risks of Dataset modification, Strategies for detecting and Analyzing anomalies, Network level threats and mitigation using machine learning, IOT threats and mitigation using machine learning.	
Unit 4	Ramifications and Deep fakes, Implications of explainable AI, Threats and mitigation for Gen AI, Fraud prevention with Cloud AI solutions.	
Unit 5	Advanced AI-driven threats and attacks (adversarial ML, AI-powered malware), Security implications of IoT and cloud integration in AI systems, Case studies of AI-based cybersecurity incidents, Best practices and strategies for future-proofing AI-enabled systems	
Course Outcomes (COs): At the end of the course students will be able to: CO1 : To understand types of Cyber security threats CO2 : To appreciate the AI considerations as applied to system components CO3 : To understand application of AI to mitigate cyber threats CO4 : To understand mitigation of risks using machine learning.		
Reference Books/Learning Resources: - Hands-on Artificial Intelligence for Cybersecurity, Alessandro Parisi, O'Reilly, 2019. - Artificial Intelligence - AI Governance and Cyber-Security: A beginner's handbook on securing and governing AI systems, Taimur Ijlal, 2022, Kindle edition.		

Name of the Course	Health Data Management and Security	
Course Code: PhDCPS-102(ix)	Credits-5, MM-100	L-5, T-0, P-0
Course Objectives - Understand basic concepts of health data management, healthcare information systems, and medical terminology. - Apply methods for collecting, storing, processing, and transforming health data. - Analyze and visualize health data and explain the role of HIE and EHR systems. - Implement health data standards, interoperability, privacy, and security techniques.		
Course Evaluation Evaluation Continuous assessment will be conducted through tutorials, assignments, quizzes, and group discussions. At the end of the course, a final written examination of 100 Marks will be conducted. 1. Students who have at least 75% attendance in classes will be considered eligible for the final written examination. 2. The exam will be conducted for a three-hour duration Note: The students can opt for MOOCs/SWAYAM and other accredited online platforms, with prior approval of relevant bodies. The passing marks for Ph.D. course work will be 55% aggregate with minimum 50% in each individual course (All three courses).		
Note for Paper Setting There will be 11 questions covering all units. The first 10 questions of explanatory answers of 12 marks each will consist of one question from each unit with internal choice provided, meaning there will be two questions from each unit (5X2=10). The students will be required to attempt one question from each unit. The 11th question will consist of 10 short answer type questions using Roman numerals (i, ii,iii.....x) each with 5 marks covering with all the units. The students will be required to attempt any 8 questions out of 10.		
Units	Syllabus	
Unit 1	Introduction: Introduction to Health Data Management and Security, Healthcare Information Systems, Basics of Medical Terminology.	
Unit 2	Data Storage & Processing: Health Data Collection Methods, Data Storage Technologies in Healthcare, Data Processing and Transformation Techniques	
Unit 3	Management: Health Data Analysis and Visualization, Introduction to Health Information Exchange (HIE) and Management, Electronic Health Records (EHR) Systems	
Unit 4	Security: Health Data Standards and Interoperability, Introduction to Health Data Privacy and Security, Techniques for Health Data Privacy and Security.	
Unit 5	Advanced Applications and Emerging Trends: Health Data Analytics using AI and Machine Learning, Predictive Healthcare and Personalized Medicine, Blockchain-based Health Data Security, Cloud Integration and Telemedicine Data Security, Case Studies of Healthcare Data Breaches and Mitigation Strategies, Best Practices for Protecting Health Information.	
Course Outcomes (COs) At the end of the course students will be able to: CO1: To understand the importance of health data management and security in modern healthcare systems. CO2: To analyze different types of health data and apply appropriate techniques for data processing and analysis. CO3: To implement security measures to protect health information against unauthorized access, breaches, and cyber threats. CO4: To evaluate the ethical and legal issues related to health data privacy, confidentiality, and compliance with regulatory standards.		
Reference Books/Learning Resources: - Robert E. Hoyt and Ann K. Yoshihashi. Health Informatics: Practical Guide for Healthcare and Information Technology Professionals. Chicago: AHIMA Press, 2014. - Kathleen A. McCormick. Healthcare Information Technology Exam Guide for CompTIA Healthcare IT		

Technician and HIT Pro Certifications. New York: McGraw-Hill Education, 2017.

- Tim Benson. Principles of Health Interoperability HL7 and SNOMED. New York: Springer, 2012.
- Chandan K. Reddy, Charu C. Aggarwal, and Haixun Wang. Healthcare Data Analytics. Boca Raton: CRC Press, 2015.
- Harold F. Tipton and Micki Krause. Information Security Management Handbook. Boca Raton: CRC Press, 2017.

Name of the Course	Advanced Cyber Security	
Course Code: PhDCPS-102(x)	Credits-5, MM-100	L-5, T-0, P-0
Course Objectives - Understand foundational concepts of cybersecurity, threats, and the CIA model. - Apply network security, cryptography, and secure software development practices. - Identify and mitigate security risks in web applications, cloud, and IoT systems. - Implement identity and access management, incident response, and analyze emerging cybersecurity trends.		
Course Evaluation Evaluation Continuous assessment will be conducted through tutorials, assignments, quizzes, and group discussions. At the end of the course, a final written examination of 100 Marks will be conducted. 1. Students who have at least 75% attendance in classes will be considered eligible for the final written examination. 2. The exam will be conducted for a three-hour duration Note: The students can opt for MOOCs/SWAYAM and other accredited online platforms, with prior approval of relevant bodies. The passing marks for Ph.D. course work will be 55% aggregate with minimum 50% in each individual course (All three courses).		
Note for Paper Setting There will be 11 questions covering all units. The first 10 questions of explanatory answers of 12 marks each will consist of one question from each unit with internal choice provided, meaning there will be two questions from each unit (5X2=10). The students will be required to attempt one question from each unit. The 11th question will consist of 10 short answer type questions using Roman numerals (i, ii,iii.....x) each with 5 marks covering with all the units. The students will be required to attempt any 8 questions out of 10.		
Units	Syllabus	
Unit 1	Advanced Cybersecurity Concepts and Threats: Introduction to advanced cybersecurity concepts, Evolution of cyber threats and the cybersecurity landscape, Types of advanced threats: APTs, zero-day attacks, and insider threats, Case studies of significant cybersecurity incidents, Advanced techniques for risk assessment and management, Cyber risk quantification and mitigation strategies, Cybersecurity policies and frameworks, Regulatory compliance, and standards.	
Unit 2	Advanced Network Security and Cryptography: Modern cryptographic algorithms and their applications, Cryptanalysis, Secure communication protocols (SSL/TLS, IPsec), Advanced firewall configurations and VPNs, Advanced intrusion detection and prevention systems (IDPS), Anomaly detection and response strategies.	
Unit 3	Securing Emerging Technologies: Cloud Security: Advanced cloud security concepts and architecture, IoT Security: Techniques for securing IoT devices and networks, and AI and Cybersecurity.	
Unit 4	Identity and Access Management (IAM) and Cybersecurity Operations: Managing user identities, authentication, authorization, and access control, Role-Based and Attribute-Based Access Control (RBAC & ABAC), Privileged Access Management (PAM), Identity governance, Business Continuity Planning (BCP) and Disaster Recovery (DR), Advanced cybersecurity operations and threat intelligence, AI applications in monitoring and responding to cyber threats.	
Unit 5	Incident Response, Forensics, and Future Trends: Incident Response Strategies, Case studies of incident response, Techniques for digital forensics and investigation, Tools and methodologies for forensic analysis, Cybersecurity in Emerging Technologies: Blockchain Security, Future Trends and Research Directions.	
Course Outcomes (COs) At the end of the course students will be able to: CO1: Understand and apply advanced concepts in cybersecurity to identify and mitigate evolving cyber threats. CO2: Implement advanced network security measures and cryptographic techniques to secure communication channels.		

CO3: Secure emerging technologies, including cloud, IoT, and AI systems, while addressing specific security challenges. **CO4:** Develop and execute advanced incident response strategies to investigate cybersecurity incidents. **CO4:** Exploring emerging cybersecurity technologies, trends, and best practices.

Reference Books/Learning Resources:

- M. E. Whitman and H. J. Mattord, Principles of Information Security. 6th ed. Cengage Learning, 2018.
- C. P. Pfleeger, S. L. Pfleeger, and J. Margulies, Security in Computing. 5th ed. Prentice Hall, 2015.
- R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed., Wiley, 2020.

Name of the Course	Advanced Wireless Networks	
Course Code: PhDCPS-102(xi)	Credits-5, MM-100	L-5, T-0, P-0
Course Objectives • Understand the fundamentals of wireless networks, including protocols, standards, and service integration. • Identify vulnerabilities and analyze security challenges in wireless networks. • Apply security mechanisms and evaluate performance and implementation strategies for robust network operation.		
Course Evaluation Evaluation Continuous assessment will be conducted through tutorials, assignments, quizzes, and group discussions. At the end of the course, a final written examination of 100 Marks will be conducted. 1. Students who have at least 75% attendance in classes will be considered eligible for the final written examination. 2. The exam will be conducted for a three-hour duration Note: The students can opt for MOOCs/SWAYAM and other accredited online platforms, with prior approval of relevant bodies. The passing marks for Ph.D. course work will be 55% aggregate with minimum 50% in each individual course (All three courses).		
Note for Paper Setting There will be 11 questions covering all units. The first 10 questions of explanatory answers of 12 marks each will consist of one question from each unit with internal choice provided, meaning there will be two questions from each unit (5X2=10). The students will be required to attempt one question from each unit. The 11th question will consist of 10 short answer type questions using Roman numerals (i, ii,iii.....x) each with 5 marks covering with all the units. The students will be required to attempt any 8 questions out of 10.		
Units	Syllabus	
Unit 1	Fundamentals: 4G Networks and Composite Radio Environment, Protocol Boosters, Hybrid 4G Wireless Network Protocols, Green Wireless Networks, Physical Layer and Multiple Access, Multicarrier CDMA, Ultra-wide Band Signal, MIMO Channels and Space Time Coding.	
Unit 2	Introduction to Wireless Networking: Introduction, Difference between wireless and fixed telephone networks, WLAN, Development of wireless networks, 3G and 4G Networks, Traffic routing in wireless networks. Wireless Networking, Packet Processing, Network Speed, Packet Buffering. Bluetooth: Overview, Radio specification, Base band specification, Links manager specification, Logical link control and adaptation protocol. Introduction to WLL Technology.	
Unit 3	Mobile Network: IP packet delivery – Agent advertisement and solicitation – Registration – Tunneling and Encapsulation – Optimizations – Reverse Tunneling – Ipv6., Dynamic Host Configuration protocol, Traditional TCP - Congestion control – Slow start – Fast retransmit/fast recovery – Classical TCP improvements: Indirect TCP – Snooping TCP – Mobile TCP. Registration – Tunneling and Encapsulation – Optimizations – Reverse Tunneling – Ipv6., Dynamic Host Configuration protocol, Traditional TCP - Congestion control – Slow start – Fast retransmit/fast recovery – Classical TCP improvements: Indirect TCP – Snooping TCP – Mobile TCP.	
Unit 4	Mobility and Resource Management: Prioritized Handoff, Cell Residing Time Distribution, Mobility Prediction in Pico- and Micro-Cellular Networks, Channel Assignment Schemes, Resource Management in 4G. Mobile Agent-based Resource Management, Joint Data Rate and Power Management, Dynamic Spectra Sharing in Wireless Networks.	
Unit 5	Ad Hoc and Sensor Networks: Routing Protocols, Hybrid Routing Protocol, Scalable Routing Strategies, Multipath Routing, Clustering Protocols. Distributed Quos Routing, Sensor Networks Parameters, Sensor Networks Architecture. Wireless Network Security: IEEE 802.11i Wireless LAN Security, Wireless Application Protocol Overview, Wireless Transport Layer Security, WAP End to-End Security.	

Course Outcomes (COs)

At the end of the course students will be able to:

CO1: Understand wireless network fundamentals, standards, and key protocols.

CO2: Acquire knowledge about Routing and Application Layer Protocols.

CO3: Recognize the various Network Standards and their utility in real world.

Reference Books/Learning Resources:

- Rappaport, T.S., Wireless Communications, Pearson Education (2007) 2nd ed.
- Zheng, Jun and Jamalipour, Abbas, Wireless Sensor Networks: A Networking Perspective, Wiley-IEEE Press (2009).
- Tanenbaum, A.S., Computer Networks, 4th Edition, Prentice Hall (2007).
- Stallings, W., Network Security Essentials, Prentice Hall (2017) 6th Edition.