Gandhinagar Institute of Technology

Academic Regulation & Curriculum

for

MTech

in

Computer Science and Engineering –
Cyber Security
(CSE-CS)

MTech PROGRAMME

***w.e.f.* 2026-27**

Preamble

We, the members of the Computer Science and Engineering Department, are committed to promoting knowledge, innovation, and technical excellence in the field of Computer Science and Engineering. We aim to create a positive learning environment where students are encouraged to think creatively, work collaboratively, and develop practical skills for real-world challenges.

The curriculum for the M.Tech-CS . in Computer Science and Engineering program has been revised according to the guidelines of UGC, AICTE and NCrF along with the New Education Policy (NEP) under Academic Regulation 2022 and blended with IEEE effective from the academic session 2026–2027. The program follows an Outcome-Based Curriculum (OBC) with a Choice-Based Credit System (CBCS), helping students build strong professional and technical skills through a multidisciplinary approach that meets the needs of industry, higher studies, and accreditation bodies such as NBA and NAAC.

To match current trends and technological advancements, several modern subjects have been included in the syllabus, such as Malware Analysis and Intrusion Detection, Cryptography & Network Security Forensics, Blockchain Infrastructure and Decentralized Systems, Research Methodology and IPR, Cyber Crime, Cyber Laws and IPR, Risk Assessment and Security Audit, Secure Distributed Cloud Systems, Biometric Systems & Biometric Image Processing, Machine Learning for Threat Detection and Prevention, Embedded System and Hardware Security, Advanced Digital Forensic and Investigation, Cybersecurity Governance, Risk & Legal Compliance, IT Act Under Cyber Law, Technical Writing, Advanced Firewalls & Intrusion Detection Systems, Advanced Cyber Threat Intelligence & Cyber Warfare, Network, Mobile & Cloud Security, Cyber Disaster Management and Recovery, Advanced Cyber-Physical Systems & Security, and Enterprise Security Architecture. These subjects are designed to provide students with in-depth knowledge of modern cybersecurity practices, digital forensics, intelligent threat detection, cloud and network security, cyber laws, and emerging technologies to address current and future challenges in the field of Cyber Security and Digital Forensics.

Students are encouraged to take MOOC courses of their choice to earn honors and gain additional knowledge in advanced technologies.

The course coding system has been updated from the respective academic sessions, as suggested by the Office of the Controller of Examinations. This change helps clearly distinguish the revised curriculum from previous versions.

The curriculum and syllabi are continuously updated through a structured feedback mechanism involving stakeholders

such as faculty members, experts, industry experts, alumni and parents. This ensures that the program remains relevant, practical, and future-oriented.

With a focus on continuous learning, innovation, research, and adaptability, the department aims to develop skilled cybersecurity professionals, researchers, and future leaders who can contribute effectively to society and the rapidly evolving world of Cyber Security, Digital Forensics, Network and Cloud Security, Ethical Hacking, Cyber Threat Intelligence, Blockchain Technology, Information Security Governance, and advanced cyber defense technologies.

Table of Contents

1. Institutional Vision & Mission ……..……...05

2. Program Objectives(POs) ……..……...06

3. Program Educational Objectives(PEOs) ……..…....07

4. Program Details…….……....08

5. Curriculum Structure…….……..…...10

6. Teaching Learning and Evaluation……..……...14

7. Rules and Regulation……..……...16

8. Student Support……...……...21

9. Program Credibility……..…...……...24

10. Collaborative Field Work / Experimental Work……...……...……...27

11. Market Survey……..……...……...30

12. Review and Revision of Regulation ……..……...35

APPENDIX – I Detailed Syllabus……...……..……..36

APPENDIX – II Industry and Employer Survey Analysis……...……86

1.Institutional Vision & Mission

VISION:

To create a flexible and learner-focused engineering ecosystem that builds strong technical skills, practical knowledge, and innovative thinking, preparing graduates to adapt, perform, and lead in a rapidly evolving technological and societal environment.

MISSION:

To provide a holistic learning environment that develops technical skilled, innovative, and socially responsible engineers capable of addressing industrial, technological, and societal needs.

2.Program Objectives

PEO 1 – Technical Competence

Graduates will demonstrate advanced knowledge and technical expertise in Cyber Security Engineering, including network security, cryptography, ethical hacking, digital forensics, secure software development, cloud security, and cyber defense mechanisms to address complex security challenges.

PEO 2 – Research & Innovation

Graduates will engage in research and innovation in emerging areas of cyber security, develop secure and resilient solutions, and contribute to advancements in cyber defense technologies through analytical and problem-solving skills.

PEO 3 – Industry Readiness & Leadership

Graduates will effectively apply cyber security principles, professional practices, and managerial abilities to lead security projects, manage cyber risk, and work efficiently in industry, government organizations, research institutions, and entrepreneurial ventures.

PEO 4 – Ethical, Legal & Societal Responsibility

Graduates will design and implement secure systems with awareness of ethical hacking practices, cyber laws, privacy protection, data governance, and societal responsibilities, ensuring secure and responsible use of technology.

PEO 5 – Lifelong Learning & Professional Development

Graduates will continuously enhance their professional knowledge and adapt to evolving cyber threats, security standards, and emerging technologies through lifelong learning, certifications, research, and collaborative practices.

3.Program Outcomes (POs)

PO	Title	Description
PO1	**Advanced Knowledge**	Apply advanced knowledge of cyber security principles, computing foundations, cryptography, network security, and secure system design to solve complex security challenges.
PO2	**Problem Analysis**	Identify, analyze, and investigate sophisticated cyber threats, vulnerabilities, and security incidents using analytical, mathematical, and engineering approaches.
PO3	**Design & Development**	Design, develop, and implement secure computing systems, applications, networks, and cyber defense solutions considering security, privacy, legal, and organizational requirements.
PO4	**Research Aptitude**	Conduct independent and collaborative research in cyber security through literature review, experimentation, penetration testing, threat analysis, and validation of innovative solutions.
PO5	**Modern Security Tools & Techniques**	Select and apply modern cyber security tools, technologies, and frameworks such as SIEM tools, IDS/IPS, vulnerability assessment tools, digital forensic platforms, and cloud security solutions.
PO6	**Threat Intelligence & Risk Management**	Analyze cyber threats, assess risks, and implement preventive, detective, and corrective security measures for protecting digital infrastructure and organizational assets.
PO7	**Ethics, Privacy & Cyber Laws**	Understand and apply professional ethics, cyber laws, data privacy regulations, responsible disclosure practices, and ethical hacking principles in cyber security operations.
PO8	**Societal & National Security Impact**	Evaluate the impact of cyber security on society, business, governance, and national security, and contribute to building secure and resilient digital ecosystems.
PO9	**Communication & Collaboration**	Communicate technical findings, security policies, audit reports, and research outcomes effectively through professional documentation, presentations, and teamwork.
PO10	**Project Management & Leadership**	Demonstrate leadership, project management, and decision-making skills in managing cyber security projects, incident response teams, and enterprise security operations.
PO11	**Interdisciplinary Application**	Apply cyber security concepts across interdisciplinary domains such as banking, healthcare, cloud computing, IoT, smart cities, defense, and critical infrastructure systems.
PO12	**Lifelong Learning**	Engage in continuous learning and professional development to adapt to emerging cyber threats, evolving technologies, security standards, and global best practices.

4. **Program Details**

4.1. Program Structure & Duration

- Duration & Intake:2 Years & 60 Seats
- Semesters: 4
- Mode: Full Time
- Credit Structure: As per NEP / University norms
- Medium of Instruction: English
- Intake: 18
- Fees: The fee structure prescribed by the University from time to time shall be applicable.

4.2 Eligibility Criteria for Admission

Candidates seeking admission to M.Tech must have completed a B.E./B.Tech degree or an equivalent qualification in the relevant branch from a recognized university. Generally, candidates belonging to the General category must secure at least 50% marks in the qualifying examination, while candidates from reserved categories such as SC, ST, SEBC, and EWS of Gujarat require a minimum of 45% marks. Admission is primarily based on a valid GATE score, and candidates without GATE qualification can apply through the Gujarat PGCET examination or on the basis of merit as per ACPC rules.

4.3 Admission Procedure

Admission to the M.Tech program shall be granted on the basis of merit obtained in the qualifying examination and/or valid GATE score and/or Gujarat PGCET score, as prescribed by the Admission Committee for Professional Courses (ACPC) and the University from time to time. Candidates must possess a Bachelor's degree in Engineering/Technology or an equivalent qualification in the relevant discipline from a recognized university. The admission process may also include document verification, centralized counseling, choice filling, and seat allotment as per ACPC norms. The University reserves the right to revise the eligibility criteria, admission procedure, and selection process from time to time.

4.4 Credit Framework

Sl. No.	**Course Type**	**MTech-AI Credit**
1.	Dissertation / Project Work (Ph I + II)	28
2.	Professional Core Courses	24
3.	Professional Elective Courses	16
4.	Internal Review (I + II)	04

5.	Mandatory Learning (RM & IPR)	03
6.	Technical Writing	00
	Total	**75**

Definition of Credit (as per UGC / AICTE):

- 1 Hour Lecture (L)per Week=1Credit
- 1 Hour Tutorial (T) per Week=1Credit
- 1 Hour Practical (P) per Week=0.5Credits
- 2 Hours Practical (Lab) per Week=1Credit

Range of Credits (as per UGC / AICTE):

✔ A total of 75 credits will be necessary for a student to be eligible to get MTech degree.

✔ These could be acquired through MOOCs.

✔ Any student completing any course through MOOC will have to submit an appropriate certificate to earn the corresponding credit.

✔ For any additional information , the student may contact the concerned HODs.

5. Curriculum Structure

Gandhinagar Institute of Technology (01)

Mtech CS (Sem - 1)

Program Name: Master of Technology (02) | **Program Code: CS(138)**

Semester / Year : Semester I / First Year | **Effective From Academic Year: 2026-27**

NCrf Level	Subject Code	Course Type	Subject Name	Credit	Hours per week				Theory (Marks)		Practical (Marks)		Total (Marks)
					L	T	P	Total	University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
6.5	11380101	Professional Core	Malware Analysis and Intrusion Detection	4	3	0	2	5	60	40	30	20	150
	11380102	Professional Core	Cryptography & Network Security Forensics	4	3	0	2	5	60	40	30	20	150
	11380110	Professional Core	Blockchain Infrastructure and Decentralized Systems	4	3	0	2	5	60	40	30	20	150
	10000151	Mandatory Learning Course	Research Methodology and IPR	3	1	1	2	4	0	0	80	20	100
	-	Professional Elective	Professional Elective - I	4	3	0	2	5	60	40	30	20	150
	-	Professional Elective	Professional Elective - II	4	3	1	0	4	60	40	0	0	100
			Total	**23**	**16**	**2**	**10**	**28**	**300**	**200**	**200**	**100**	**800**

	11380104	Professional Elective - I	Cyber Crime, Cyber Laws and IPR
	11380105	Professional Elective - I	Risk Assessment and Security Audit
	11380111	Professional Elective - I	Secure Distributed Cloud Systems
	11380107	Professional Elective - II	Biometric Systems & Biometric Image Processing
	11380112	Professional Elective - II	Machine Learning for Threat Detection and Prevention
	11380109	Professional Elective - II	Embedded System and Hardware Security

Gandhinagar Institute of Technology (01)

Mtech AI (Sem - 2)

Program Name: Master of Technology (02) | **Program Code: AI(139)**

Semester / Year : Semester II / First Year | **Effective From Academic Year: 2026-27**

NCrf Level	Subject Code	Course Type	Subject Name	Credit	Hours per week				Theory (Marks)		Practical (Marks)		Total (Marks)
					L	T	P	Total	University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
6.5	11390201	Professional Core	Advanced Natural Language Processing & LLM Architectures	4	3	0	2	5	60	40	30	20	150
	11390202	Professional Core	Neural Networks & Optimization Techniques	4	3	0	2	5	60	40	30	20	150
	11390203	Professional Core	Advance Generative Models (GANs, Diffusion Models)	4	3	0	2	5	60	40	30	20	150
	10000251	Mandatory Learning Course	Technical Writing	0	2	0	0	2	0	50	0	0	50
	-	Professional Elective	Professional Elective - III	4	3	0	2	5	60	40	30	20	150
	-	Professional Elective	Professional Elective - IV	4	3	1	0	4	60	40	0	0	100
			Total	**20**	**17**	**1**	**8**	**26**	**300**	**250**	**120**	**80**	**750**

11390204	Professional Elective - III	Advanced Signal Processing for AI
11390205	Professional Elective - III	Time Series Analysis & Forecasting
11390206	Professional Elective - III	AI-Driven Remote Sensing & GIS

11390207	Professional Elective - IV	AI for Smart Healthcare & Medical Imaging
11390208	Professional Elective - IV	Data Engineering & Data Pipeline Systems
11390209	Professional Elective - IV	Advanced Data Mining &

			Knowledge Discovery										

Gandhinagar Institute of Technology (01)

Mtech CS (Sem - 2)

Program Name: Master of Technology (02) | **Program Code: CS(138)**

Semester / Year : Semester II / First Year | **Effective From Academic Year: 2026-27**

NCrf Level	Subject Code	Course Type	Subject Name	Credit	Hours per week				Theory (Marks)		Practical (Marks)		Total (Marks)
					L	T	P	Total	University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
6.5	11380210	Professional Core	Advanced Digital Forensic and Investigation	4	3	0	2	5	60	40	30	20	150
	11380211	Professional Core	Cybersecurity Governance, Risk & Legal Compliance	4	3	0	2	5	60	40	30	20	150
	11380212	Professional Core	IT Act Under Cyber Law	4	3	0	2	5	60	40	30	20	150
	10000251	Mandatory Learning Course	Technical Writing	0	2	0	0	2	0	50	0	0	50
	-	Professional Elective	Professional Elective - III	4	3	0	2	5	60	40	30	20	150
	-	Professional Elective	Professional Elective - IV	4	3	1	0	4	60	40	0	0	100
			Total	**20**	**17**	**1**	**8**	**26**	**300**	**250**	**120**	**80**	**750**

	11380213	Professional Elective - III	Advanced Firewalls & Intrusion Detection Systems
	11380214	Professional Elective - III	Advanced Cyber Threat Intelligence & Cyber Warfare
	11380215	Professional Elective - III	Network, Mobile & Cloud Security
	11380216	Professional Elective - IV	Cyber Disaster Management and Recovery
	11380217	Professional Elective - IV	Advanced Cyber-Physical Systems & Security
	11380218	Professional Elective - IV	Enterprise Security Architecture

Gandhinagar Institute of Technology (01)

Mtech CS (Sem - 3)

Program Name: Master of Technology (02)	**Program Code: CS(138)**
Semester / Year : Semester III / Second Year	**Effective From Academic Year:2026-27**

NCrf Level	Subject Code	Course Type	Subject Name	Credit	Hours per week				Theory (Marks)		Practical (Marks)		Total (Marks)
					L	T	P	Total	University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
7	11380301	Internal Review	Internal Review I	2	0	0	4	4	0	0	0	100	100
	11380302	Dissertation	Dissertation Phase I	14	0	0	28	28	0	0	100	0	100
			Total	**16**	**0**	**0**	**32**	**32**	**0**	**0**	**100**	**100**	**200**

Gandhinagar Institute of Technology (01)

Mtech CS (Sem - 4)

Program Name: Master of Technology (02)	**Program Code: CS(138)**
Semester / Year : Semester IV / Second Year	**Effective From Academic Year: 2026-27**

NCrf Level	Subject Code	Course Type	Subject Name	Credit	Hours per week				Theory (Marks)		Practical (Marks)		Total (Marks)
					L	T	P	Total	University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
7	11380401	Internal Review	Internal Review II	2	0	0	4	4	0	0	0	100	100
	11380402	Dissertation	Dissertation Phase II	14	0	0	28	28	0	0	100	0	100
			Total	**16**	**0**	**0**	**32**	**32**	**0**	**0**	**100**	**100**	**200**

1stSem	800	**3rdSem**	200				

2ndSem	750	**4th Sem**	200	**Total Credit:**	**75**
				Total Marks:	**1950**

6. Teaching Learning and Evaluation

6.1 Teaching Methodology

The program shall adopt the following teaching methodologies:

- Classroom Teaching
- Case Studies
- Industry Interaction
- Site Visits
- Workshops
- Field Surveys
- Research Projects
- Research work
- Paper Publication
- AI-based Learning Tools
- Blended and Digital Learning

6.2 Attendance Rules

- Minimum 75% attendance shall be mandatory in each course.
- Students below the prescribed attendance may not be permitted to appear in examinations.
- Additional attendance requirements may apply for practical and research work and paper publication.

6.3 Examination and Evaluation System

6.3.1 Evaluation Components

The evaluation may consist of Continuous Internal Evaluation (CIE) and End Semester Examination (ESE).

Continuous Internal Evaluation (CIE) may include:

- Mid-Semester Examination
- Assignments
- Presentations
- Research work
- Paper Publication
- Class Tests
- AI Quiz & Viva Voce

- Dissertation
- Project Work

6.4 Suggested Weightage

- Continuous Internal Evaluation (CIE): 40%
- End Semester Examination (ESE): 60%

6.5 Passing Standards

- Minimum 50% marks in each component where applicable.
- Minimum 50% aggregate marks for passing the course/program.
- Separate passing may be required in theory and practical examinations.

6.6 Grading System

The program shall follow Gandhinagar University grading norms.

6.6.1 Grade Table

Grade	Grade Points	From Marks	To Marks
AA	10	80	100
AB	9	75	79
BB	8	70	74
BC	7	65	69
CC	6	60	64
CD	0	55	59
DD	-	50	54
DF	-	0	49

6.7 Dissertation / Project Work

Requirements may include:

- Proposal Presentation
- Periodic Review
- Final Report Submission
- Viva Voce Examination

The dissertation shall be evaluated by internal and external examiners.

7. Rules and Regulations

7.1 Rules for Promotion

A student shall be promoted to the next semester as per Gandhinagar University rules, subject to fulfilment of academic requirements, minimum attendance, and completion of required credits.

7.2 Maximum Duration for Completion

The maximum duration for completing the program shall be 2 years from the date of admission (or as prescribed by the University).

7.3 Dissertation Guidelines

7.3.1 Internal Review – I /II

Purpose

Internal Review – I and II is conducted before the formal submission of Dissertation Phase – I and II respectively to evaluate the early-stage research progress.

The review focuses on:

- Research problem identification
- Literature survey quality
- Research gap identification
- Feasibility and relevance of the selected topic
- Research methodology planning
- Implementation progress
- System/model architecture
- Experimental setup
- Preliminary results and analysis
- Performance evaluation
- Challenges faced and solutions adopted
- Future work and completion plan

Student Presentation Requirements

- Proposed research topic
- Problem statement
- Literature review
- Research gap identification
- Objectives of the research
- Proposed methodology/framework
- Expected outcomes
- Implementation status report
- Experimental methodology
- Preliminary results and analysis
- Graphs, tables, or comparative outputs
- Challenges faced and corrective actions
- Updated dissertation draft
- Final work completion plan

Submission Requirements

- Literature survey summary
- Research problem formulation document
- Proposed methodology/framework
- Preliminary research plan
- Timeline for Dissertation Phase – I
- Minimum 10–15 research paper references from reputed journals/conferences
- Implementation status report
- Experimental methodology
- Preliminary results and analysis
- Graphs, tables, or comparative outputs
- Challenges faced and corrective actions
- Updated dissertation draft
- Final work completion plan

7.3.2 Dissertation Phase – I/II

Purpose

Dissertation Phase – I and II focuses on research planning, methodology development, system/model design, and preliminary experimentation.

Students shall work under the guidance of an assigned faculty supervisor.

Activities to be Performed

- Identification of research problem
- Extensive literature review
- Definition of objectives and scope
- Selection of suitable methodology
- Dataset identification and collection
- Initial model/system design
- Tool and technology selection
- Preliminary experimentation and analysis
- Research proposal preparation
- Algorithm/model implementation
- AI model training and testing
- Simulation or deployment
- Experimental analysis
- Comparative performance evaluation
- Result validation
- Optimization and improvements
- Research paper preparation (if applicable)
- Final dissertation report preparation

Seminar and Review

The presentation may include:

- Research significance
- Technical approach
- Proposed framework
- Preliminary results
- Research plan for Phase – II

7.3.3 Final Dissertation Report Structure

The dissertation report shall contain the following chapters:

1. Title Page
2. Certificate
3. Declaration
4. Acknowledgement
5. Abstract
6. Table of Contents
7. List of Figures
8. List of Tables
9. Introduction
10. Literature Review
11. Problem Statement and Research Gap
12. Proposed Methodology / Model
13. System Design and Architecture
14. Implementation and Experimental Setup
15. Results and Analysis
16. Comparison with Existing Methods
17. Conclusion and Future Work
18. References
19. Appendices (if applicable)

7.3.4 Dissertation Submission Requirements

Students must submit:

- Final dissertation report (hard copy and soft copy)
- Plagiarism report as per UGC norms
- Source code/software/project files
- Dataset details (if applicable)
- Research paper/publication details (if any)
- Completion certificate signed by guide
- Presentation slides for viva voce
- Project demonstration (if applicable)

7.4 Discipline Rules

Students shall maintain discipline, professional ethics, and proper conduct within the institution, during industry interactions, examinations, and all academic activities.

Students are expected to:

- Attend classes regularly
- Follow institutional rules and regulations
- Respect faculty members, staff, fellow students, and institutional property
- Maintain academic integrity in assignments, projects, and examinations

Any form of misconduct, ragging, indiscipline, use of unfair means in examinations, damage to institutional property, harassment, or behavior affecting the academic environment shall be treated seriously and may result in disciplinary action including:

- Warning
- Suspension
- Cancellation of Examination
- Withholding of Results
- Expulsion from the Program

Such actions shall be taken as per University rules and UGC regulations.

Students shall also comply with all safety, ethical, and professional standards prescribed by the institution from time to time.

7.5 Anti-Ragging Policy

The program shall strictly follow:

- UGC Anti-Ragging Regulations
- Anti-Ragging Affidavit Requirements
- Institutional Disciplinary Procedures
- Ragging in any form is strictly prohibited.

7.6 Ethical Use of Technology and AI/CS Tools

Students are encouraged to use:

- Various Software and AI Tools
- Data Analytics Tools
- Valuation Software
- Digital Survey Tools
- Network Monitoring and Vulnerability Assessment Tools

- AI and Machine Learning Security Tools
- Digital Forensics and Incident Response Tools
- Cloud Security and Virtualization Platforms
- Secure Coding and DevSecOps Tools
- AI-based Learning and Cyber Range Platforms

Use of AI/CS tools shall be ethical and academic integrity must be maintained.

8. Student Support

8.1 Industry Collaboration

The department shall actively promote collaboration with IT industries, cybersecurity companies, digital forensics organizations, cloud service providers, research institutions, startups, government agencies, defense organizations, banking and financial sectors, and technology firms to enhance practical exposure and industry relevance of the M.Tech (Cyber Security Engineering) program.

Such collaborations may include internships, industrial training, live projects, expert lectures, workshops, cyber drills, hackathons, industrial visits, consultancy assignments, collaborative research activities, certification programs, skill development initiatives, and placement support.

The institution may also establish Memoranda of Understanding (MoUs) with industries, cybersecurity laboratories, research organizations, and professional bodies for academic enrichment, technology support, innovation activities, startup incubation, cyber awareness initiatives, and collaborative research aimed at improving employability, entrepreneurship, technical competency, and industry readiness among students.

8.2 Research and Consultancy

The department shall encourage faculty members and students to actively engage in research, consultancy, innovation, and applied studies related to Cyber Security, Ethical Hacking, Digital Forensics, Network Security, Cloud Security, Cryptography, Malware Analysis, Secure Software Engineering, IoT Security, Blockchain Security, Artificial Intelligence in Cyber Defense, and emerging technologies.

Students may undertake research projects, security audits, penetration testing, cyber threat analysis, forensic investigations, vulnerability assessment studies, secure application development, and industry-oriented projects as part of their academic and professional training.

The institution may also undertake consultancy assignments and collaborative projects for industries, startups, government organizations, healthcare institutions, banking and financial sectors, smart city projects,

defense organizations, and technology firms in areas such as cyber risk assessment, security auditing, incident response, data protection, secure infrastructure development, cyber awareness, and digital security solutions.

Participation in seminars, conferences, workshops, cybersecurity competitions, capture-the-flag (CTF) events, publications, funded projects, patent filing activities, and collaborative research initiatives shall be encouraged to promote academic excellence, innovation, and research-oriented learning.

8.3 Library and Laboratory Facilities

Adequate library, laboratory, computing, and digital learning facilities shall be made available to support effective teaching, practical training, research, and skill development under the M.Tech (Cyber Security Engineering) program.

The department shall facilitate access to relevant books, journals, research publications, e-resources, IEEE papers, digital libraries, cybersecurity repositories, threat intelligence platforms, cloud security resources, and online learning platforms related to Cyber Security and emerging technologies.

Necessary computing facilities, high-performance systems, cybersecurity laboratories, virtual machines, network simulation tools, ethical hacking platforms, digital forensic tools, cloud computing environments, secure coding platforms, internet access, and other technical resources required for practical and project-based learning shall also be provided to enhance industry-oriented education, research capability, innovation, and professional competency among students.

8.4 Student Support and Mentoring

A structured system for student support, academic mentoring, research guidance, and professional counselling shall be implemented for students enrolled in the M.Tech (Cyber Security Engineering) program.

The department shall facilitate academic counselling, dissertation guidance, career mentoring, research support, technical training, certification guidance, and skill development activities to assist students in academic progression and professional growth.

Students may also be provided opportunities for interaction with cybersecurity experts, researchers, alumni, ethical hackers, entrepreneurs, and industry professionals through workshops, seminars, coding competitions, cyber awareness programs, hackathons, technical events, training programs, industrial visits, and extracurricular activities aimed at enhancing employability, leadership qualities, communication skills, teamwork, innovation, and overall personality development.

Necessary support mechanisms for addressing academic and personal concerns shall also be made available as per institutional policies.

8.5 Placement and Career Development

The department shall promote placement assistance and career development activities for students through industry interaction, internships, cybersecurity training, research collaboration, professional networking, technical training programs, and campus engagement initiatives.

Efforts shall be made to establish linkages with cybersecurity companies, software industries, research organizations, cloud computing firms, banking and financial sectors, government cyber cells, startups, digital forensics organizations, and technology-based enterprises to facilitate internships, live projects, industrial exposure, research opportunities, and employment opportunities for students.

Career development activities such as aptitude training, coding practice sessions, cyber security certification training, resume preparation, interview preparation, soft skill development, entrepreneurship guidance, expert sessions, technical workshops, mock interviews, and placement-oriented training programs may also be organized to enhance professional competency, innovation capability, and employability of students.

9. Program Credibility

9.1 Executive Summary

The M.Tech (Cyber Security) program is designed to develop industry-ready professionals, researchers, and innovators with expertise in Cyber Security, Network Security, Digital Forensics, Ethical Hacking, Cloud Security, Information Assurance, Cyber Defense, and emerging security technologies aligned with current industry and national security requirements.

The curriculum integrates strong theoretical foundations with practical implementation, research orientation, industry exposure, and advanced security practices to prepare students for professional careers, higher studies, research, and entrepreneurship in cybersecurity-driven domains.

The program is delivered by experienced faculty members, researchers, industry experts, and professionals actively engaged in Cyber Security, Ethical Hacking, Digital Forensics, Secure Software Development, Cloud Computing, Artificial Intelligence Security, Network Administration, and interdisciplinary security applications, ensuring that students gain practical knowledge along with academic understanding.

Specialized modules related to Network Security, Cryptography, Ethical Hacking, Cyber Threat Intelligence, Digital Forensics, Secure Coding, Cloud Security, Malware Analysis, Incident Response, Cyber Law, and Research Methodology are delivered through laboratory practice, case studies, seminars, workshops, industry interaction, project-based learning, and research activities.

The program emphasizes innovation, analytical thinking, cyber defense strategies, research competency, and ethical practices in cybersecurity through dissertation work, live projects, capture-the-flag activities, security audits, technical training, and collaborative learning activities.

The curriculum is aligned with current technological advancements, cybersecurity industry requirements, emerging cyber threat trends, and national educational guidelines, while integrating advanced computing,

analytical, investigative, and research skills required in academia, industry, government organizations, startups, and research institutions.

Graduates of the program shall be academically and professionally prepared for careers in Cyber Security, Information Security, Ethical Hacking, Security Operations, Digital Forensics, Secure Software Development, Cyber Risk Management, Cloud Security, and emerging cybersecurity-driven industries, as well as for higher studies and doctoral research.

The program also encourages continuous exposure to modern cybersecurity tools, cloud security platforms, open-source technologies, research publications, innovation ecosystems, startup culture, cyber awareness initiatives, and real-world security applications as part of experiential and industry-oriented learning throughout the program duration.

9.2 Scope and Career Opportunities

• Cyber Security Companies
• Information Security Organizations
• Software Development Industries
• Cloud Computing and Data Center Organizations
• Banking, Financial Services, and Insurance (BFSI) Sector
• Government and Defense Organizations
• Digital Forensics and Investigation Agencies
• IT Consulting and Technology Service Firms
• E-Commerce and FinTech Companies
• Healthcare Technology Organizations
• Telecommunications and Networking Industries
• Research and Development Centers
• Smart Systems and IoT Security Industries
• Startups and Innovation Centers
• Academic and Research Institutions

9.3 Potential Job Roles

• Cyber Security Analyst
• Information Security Analyst
• Ethical Hacker
• Penetration Tester

• Security Operations Center (SOC) Analyst
• Digital Forensics Investigator
• Network Security Engineer
• Cloud Security Engineer
• Cyber Threat Intelligence Analyst
• Malware Analyst
• Incident Response Analyst
• Security Consultant
• Cyber Risk Analyst
• Security Auditor
• Application Security Engineer
• Security Architect
• Cyber Defense Specialist
• Research Assistant

9.4 Higher Study and Professional Opportunities

Students may pursue:
• Ph.D. in Cyber Security and related disciplines
• Research Fellowships and Academic Research Programs
• Advanced Certifications in Cyber Security, Ethical Hacking, Cloud Security, and Digital Forensics
• International Professional Certifications
• Industry-based Research and Consultancy Opportunities
• Startup and Entrepreneurship Initiatives
• Patent Filing and Research Publication Activities
• Specialized Training Programs in Emerging Security Technologies

10. Collaborative Field Work / Experimental Work

10.1 Network Security Analysis Exercise

During supervised laboratory sessions, students shall perform network traffic analysis, packet inspection, and vulnerability identification using cybersecurity tools and simulators. Students shall analyze network protocols, identify security loopholes, and prepare a technical report based on network security observations and mitigation strategies.(Recommended Organizations / Platforms: Wireshark, Cisco Networking Academy, NASSCOM, CERT-In)

10.2 Ethical Hacking and Penetration Testing Exercise

Students shall perform ethical hacking and penetration testing activities in controlled laboratory environments using security testing tools and frameworks. The exercise shall include reconnaissance, vulnerability assessment, exploitation techniques, and security reporting based on ethical and legal cybersecurity practices.(Recommended Organizations / Platforms: Kali Linux, Metasploit, EC-Council, Offensive Security)

10.3 Cryptography and Information Security Experimental Work

Students shall implement cryptographic algorithms and information security techniques related to encryption, decryption, hashing, digital signatures, key management, and secure communication systems. Students shall evaluate algorithm performance, security strength, and implementation challenges through experimental analysis.(Recommended Organizations / Platforms: OpenSSL, IBM Security, NIST, Cisco)

10.4 Digital Forensics Laboratory Exercise

Students shall perform digital forensic investigations involving data acquisition, evidence preservation, log analysis, file recovery, and cybercrime investigation techniques. The submission shall include forensic methodology, evidence analysis, reporting procedures, and legal considerations.(Recommended Organizations / Platforms: Autopsy, FTK, Cellebrite, National Cyber Crime Portal)

10.5 Malware Analysis and Threat Detection

Students shall analyze malware behavior, ransomware patterns, phishing attacks, and malicious software using sandbox environments and security analysis tools. Students shall evaluate threat intelligence data and prepare mitigation and incident response reports.(Recommended Organizations / Platforms: VirusTotal, Hybrid Analysis, IBM X-Force, Palo Alto Networks)

10.6 Security Operations Center (SOC) Simulation Exercise

Students shall simulate Security Operations Center activities involving log monitoring, SIEM analysis, intrusion detection, incident response, and security event correlation using enterprise security monitoring platforms. Students shall analyze attack patterns and recommend cybersecurity defense mechanisms.(Recommended Organizations / Platforms: Splunk, IBM QRadar, AlienVault, Microsoft Sentinel)

10.7 Cloud Security and Secure Deployment Exercise

Students shall perform cloud security configuration and secure deployment activities involving identity management, access control, cloud vulnerability assessment, data protection, and cloud security monitoring using major cloud platforms.(Recommended Organizations / Platforms: AWS Security, Microsoft Azure Security, Google Cloud Security)

10.8 Cyber Threat Intelligence and Risk Analysis

Students shall perform cyber threat intelligence analysis involving threat indicators, attack vectors, vulnerability assessment, cyber risk analysis, and threat mitigation strategies using cybersecurity intelligence frameworks and tools.(Recommended Organizations / Platforms: MITRE ATT&CK, IBM Security, Cisco Talos, CERT-In)

10.9 IoT and Smart Device Security Experimental Work

Students shall analyze vulnerabilities in IoT devices and smart systems involving sensor security, network protection, firmware analysis, authentication mechanisms, and secure communication protocols. Students shall implement security measures for IoT-enabled applications.(Recommended Organizations / Platforms: Arduino, Raspberry Pi, IoT Security Foundation, Smart India Mission)

10.10 Cybersecurity Data Visualization and Analytics Exercise

Students shall perform cybersecurity data visualization and analytical reporting using tools such as Python, Power BI, Tableau, or SIEM dashboards. Students shall prepare graphical reports, attack trend analysis, and security monitoring dashboards from structured and unstructured security datasets.(Recommended Organizations / Platforms: Tableau, Microsoft Power BI, Splunk, Python Foundation)

10.11 Cybersecurity Research Paper Review and Presentation

Students shall review recent cybersecurity research papers published in reputed journals or conferences and present methodologies, attack analysis, defense mechanisms, findings, and future scope. Students shall prepare technical summaries and presentation reports.(Recommended Organizations / Platforms: IEEE, Springer, Elsevier, ACM)

10.12 Cyber Law, Ethics, and Responsible Security Practices Study

Students shall analyze ethical and legal challenges related to cybersecurity including cyber laws, privacy regulations, digital rights, ethical hacking practices, data protection, and responsible security frameworks. Students shall prepare case studies and recommendation reports based on national and international cybersecurity guidelines.(Recommended Organizations / Platforms: CERT-In, Ministry of Electronics and Information Technology (MeitY), IEEE Standards Association)

10.13 Cybersecurity Hackathon / Mini Project

Students shall participate in cybersecurity hackathons, capture-the-flag competitions, security innovation challenges, or mini-project development activities focused on solving real-world cybersecurity problems using security tools, frameworks, and defensive strategies.(Recommended Organizations / Platforms: Smart India Hackathon, AICTE, EC-Council, TryHackMe, Hack The Box)

10.14 Industry Internship / Industrial Training

Students shall undergo industrial training or internships in cybersecurity organizations, IT industries, research laboratories, government agencies, or security consulting firms to gain practical exposure in information security operations, cyber defense, risk management, and secure system implementation.(Recommended Organizations / Platforms: CERT-In, IBM Security, Cisco, Palo Alto Networks, Cybersecurity Startups)

10.15 Dissertation / Research Project Work

Students shall undertake a research dissertation in Cyber Security or related interdisciplinary domains. The dissertation work shall include problem identification, literature review, research methodology, implementation, experimentation, analysis, and final thesis submission under the supervision of a faculty guide. Students shall present their work through seminars, reviews, dissertation reports, and viva-voce examinations as per University and UGC norms.(Recommended Organizations / Platforms: IEEE, ACM, Springer, Cybersecurity Research Labs)

10.16 Portfolio Presentation and Exit Viva

Students shall prepare a technical portfolio consisting of project work, research outputs, cybersecurity experiments, internship work, penetration testing activities, certifications, and technical achievements

completed during the program. Students shall deliver a final presentation and appear for an exit viva before a faculty and industry panel.

11. Market Survey

Strategic Feasibility for MTech (Cyber Security) in Ahmedabad (Gujarat)

11.1 Executive Summary

India is witnessing rapid growth in the fields of Cyber Security, Information Security, Cloud Computing, Digital Forensics, Ethical Hacking, Artificial Intelligence-based Security Systems, IoT Security, and Secure Digital Infrastructure due to increasing digital transformation across industries, government initiatives, smart technologies, Industry 4.0 adoption, expansion of online services, and rising cyber threats affecting organizations and individuals.

Gujarat, especially Ahmedabad and Gandhinagar, is emerging as a major technology and innovation hub through the development of GIFT City, smart city initiatives, IT parks, startup ecosystems, fintech industries, digital governance projects, and secure digital infrastructure development requiring advanced cybersecurity solutions and skilled professionals.

Considering these emerging opportunities, a market survey and industry interaction were conducted among IT companies, cybersecurity firms, cloud service providers, software industries, digital forensics organizations, research institutions, and technology professionals to assess the need for professionally trained manpower in Cyber Security and Information Security.

The survey confirmed a strong demand for skilled professionals with expertise in Network Security, Ethical Hacking, Penetration Testing, Digital Forensics, Cloud Security, Cyber Threat Intelligence, Incident Response, Malware Analysis, Security Operations, and secure software development.

The industry also highlighted that there is a shortage of technically skilled graduates possessing practical exposure to cybersecurity tools, real-time cyber defense mechanisms, penetration testing frameworks, cloud

security platforms, digital investigation techniques, security monitoring systems, and industry-oriented project development.

Most organizations expressed willingness to support the proposed program through internships, industrial training, live projects, cybersecurity workshops, expert lectures, collaborative research activities, hackathons, capture-the-flag competitions, technical training, and placement opportunities.

The survey findings clearly indicate that introducing an M.Tech program in Cyber Security will be highly beneficial and industry-relevant considering the increasing cyber threats, rapid digital transformation initiatives, demand for secure digital infrastructure, research opportunities, and employment growth in Gujarat and across India.

11.2 Market Demand and Industry Trends

Cyber Security is one of the fastest-growing technology sectors contributing significantly to digital protection, cyber defense, information assurance, secure communication, and national security across industries and government organizations.

The demand for Cyber Security professionals is continuously increasing due to:

- Rapid growth of digital transformation and online services
- Increasing cyber threats, ransomware attacks, and data breaches
- Expansion of cloud computing and remote working environments
- Growth of FinTech, E-Commerce, HealthTech, and Smart Governance systems
- Smart City and Digital India initiatives
- Industry 4.0 and Industrial Control System Security requirements
- Rising adoption of IoT and connected smart devices
- Growth in Cyber Defense and National Security infrastructure
- Expansion of Artificial Intelligence-based threat detection systems
- Increasing compliance requirements related to data privacy and information security

Gujarat is attracting major investments in IT infrastructure, digital governance, fintech services, industrial automation, startup ecosystems, smart technologies, and cybersecurity services, creating substantial employment opportunities for trained Cyber Security professionals.

Upcoming technological developments are expected to generate demand for manpower in areas such as:

- Cyber Security and Information Security
- Ethical Hacking and Penetration Testing

• Network and Cloud Security
• Digital Forensics and Cyber Investigation
• Cyber Threat Intelligence and Incident Response
• Security Operations Center (SOC) Management
• Application and Software Security
• IoT and Smart Device Security
• AI-based Cybersecurity and Threat Analytics
• Secure Software and System Development

11.3 Skill Gap Identified by Industry

The market survey and industry feedback revealed that many graduates lack practical and industry-oriented skills required in the Cyber Security sector.

The major gaps identified by industry professionals include:

• Limited practical exposure to cybersecurity tools and security frameworks
• Lack of hands-on experience in ethical hacking and penetration testing
• Insufficient knowledge of cloud security and secure deployment practices
• Limited understanding of digital forensics and cyber investigation techniques
• Poor exposure to real-time cyber threat analysis and incident response
• Lack of practical implementation skills in network security and malware analysis
• Limited industry interaction and project-based cybersecurity learning
• Insufficient awareness of cyber laws, privacy regulations, and ethical security practices
• Limited exposure to emerging technologies such as AI-driven security, IoT security, and Zero Trust Architecture

The industry emphasized the need for professionally trained graduates who can directly contribute to cybersecurity operations, secure software development, cyber defense, digital investigation, and research activities with minimal additional training.

11.4 Employment Opportunities

Graduates of the M.Tech (Cyber Security) program shall have employment opportunities in IT industries, cybersecurity companies, cloud computing organizations, financial institutions, government agencies, defense organizations, digital forensic laboratories, healthcare technology firms, research laboratories, startups, consulting firms, and academic institutions.

Career opportunities may include roles in:

- Cyber Security Analysis
- Information Security Management
- Ethical Hacking and Penetration Testing
- Network and Cloud Security Engineering
- Security Operations Center (SOC) Analysis
- Digital Forensics and Cyber Investigation
- Cyber Threat Intelligence and Incident Response
- Malware Analysis and Threat Detection
- Security Auditing and Compliance
- Application and Software Security
- Cyber Risk Management and Consulting
- Research and Development in Cyber Security

The program shall also support entrepreneurship and innovation opportunities in cyber security startups, security consulting services, cyber awareness solutions, secure application development, and technology-driven security services.

11.5 Industry Support and Collaboration

The industry has shown strong support for the proposed program through internships, industrial training, live projects, cyber security workshops, capture-the-flag competitions, guest lectures, expert sessions, collaborative research, and placement assistance.

IT companies, cyber security firms, cloud service providers, digital forensics organizations, government agencies, and research institutions have also expressed interest in academic collaboration for providing practical exposure, certification programs, research opportunities, and industry-oriented learning to students.

The institution may establish collaborations and Memoranda of Understanding (MoUs) with industries, cyber security organizations, technology companies, innovation centers, and professional bodies to strengthen research, training, internships, and employability.

11.6 Research and Innovation Opportunities

The proposed program shall encourage research, innovation, patent development, publication activities, and interdisciplinary project work in areas related to Cyber Security, Information Assurance, Ethical Hacking, Digital Forensics, Cloud Security, AI-driven Security Systems, Secure Software Development, and emerging security technologies.

Students and faculty members shall be encouraged to participate in:

- Research publications
- Patent filing activities
- Cyber security innovation projects
- Funded research proposals
- National and international conferences
- Technical competitions, hackathons, and capture-the-flag events
- Startup and incubation initiatives

11.7 Conclusion

The market survey and industry feedback clearly indicate strong demand for professionally trained manpower in the fields of Cyber Security, Information Security, Ethical Hacking, Digital Forensics, Cloud Security, Cyber Defense, and secure software technologies.

Considering the rapid growth of digital transformation, increasing cyber threats, startup expansion, smart governance initiatives, and rising dependence on secure digital infrastructure across industries in Gujarat and India, the proposed M.Tech (Cyber Security) program will provide students with excellent academic, research, and career opportunities while fulfilling the growing manpower requirements of the cybersecurity sector.

The proposed program will therefore be academically relevant, research-oriented, industry-focused, and aligned with present and future technological requirements, national cybersecurity priorities, innovation ecosystems, and UGC guidelines for higher technical education.

12. Review and Revision of Regulations

The University reserves the right to interpret, modify, revise, amend, or update any provision, rule, regulation, curriculum structure, evaluation scheme, academic requirement, course content, or operational guideline related to the M.Tech (Cyber Security) program from time to time in accordance with University regulations, UGC/AICTE guidelines, statutory requirements, technological advancements, industry developments, and academic needs.

In case of any ambiguity or dispute regarding the interpretation of any provision of this Academic Regulations and Curriculum document, the decision of the University and/or Competent Authority shall be final and binding on all stakeholders.

Any amendments, additions, revisions, or modifications approved by the appropriate academic, administrative, or statutory bodies of the University shall automatically become applicable to the program from the date of approval or implementation as notified by the University.

Annexure I: Detail Syllabus

GANDHINAGAR INSTITUTE OF TECHNOLOGY

MTech in Computer Science and Engineering

(Cyber Security)

(CSE-CS)

Semester 1

Subject Code: 11380101	**Subject Title:** Malware Analysis and Intrusion Detection
Pre-requisite: Basic knowledge of Computer Networks and various types of attacks.	

Course Objective:

1. Learn the fundamentals of malware and to set up a protected static and dynamic malware analysis environment.
2. Learn various malware behavior monitoring tools and actionable detection signatures from malware indicators.
3. Learn how to trick malware into exhibiting behaviors that only occur under special conditions.
4. Compare alternative tools and approaches for Intrusion Detection through quantitative analysis to determine the best tool or approach to reduce risk from intrusion.
5. Identify and describe the parts of all intrusion detection systems and characterize new and emerging IDS technologies according to the basic capabilities all intrusion detection systems share.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**

3	0	2	4	60	40	30	20	150

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Introduction Basic Malware Analysis:** Malware classification, types, and platform specific issues with malware, Intrusion into IT and operational network (OT) and their signs. Manual Malware Infection analysis, signature-based malware detection and classification – pros and cons and need for machine learning based techniques.	8	22
2	**Advanced Techniques Malware Analysis:** Static Analysis, Dynamic Analysis and Hybrid Analysis of Windows Malware, Linux Malware and Android Malware	8	16
3	**Case Studies:** Study papers in Malware Analysis from most recent conferences, Presentations and Discussions, and Implementations	6	16
4	**Basic Intrusion Detection:** Intrusion into network – Firewalls, Rule based techniques, signature-based Techniques, Simple Machine Learning Models on Network Data.	8	22
5	**Advanced Intrusion Detection and Case Studies:** Advanced Machine Learning Models for Intrusion Detection in IT Networks, Machine Learning in OT network especially with Cyber Physical Systems. Latest Papers in Intrusion Detection, Their theory and Implementations, and Data Analysis Techniques.	10	22

Course Outcome:

1. understanding of the nature of malware, its capabilities, and how it is combated through detection and classification
2. apply the tools and methodologies used to perform static and dynamic analysis on unknown executables.
3. Understanding of executable formats, Windows internals and API, and analysis techniques.
4. apply techniques and concepts to unpack, extract, decrypt, or bypass new ant analysis techniques in future malware samples.
5. Apply knowledge of the fundamentals and history of Intrusion Detection to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems. Evaluate the security an enterprise and appropriately apply Intrusion Detection tools and techniques to improve their security posture

List of Textbooks:

1. Practical malware analysis The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig ISBN-10: 159327-290-1, ISBN-13: 978-1-59327-290-6, 2012 2
2. Crimeware, Understanding New Attacks and Defenses, Markus Jakobsson and Zulfikar Ramzan, Symantec Press, ISBN: 978-0-321-50195-0 2008**.**

List of Reference Books:

1. The Art of Computer Virus Research and Defense, Peter Szor, Symantec Press ISBN 0-321- 30545-3
2. Android Malware by Xuxian Jiang and Yajin Zhou, Springer ISBN 978-1-4614-7393-0, 2005
3. Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by Michael Davis, Sean Bodmer, Aaron Lemasters, McGraw-Hill, ISBN: 978-0-07-159119-5, 2010
4. Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2015

List of Suggested Experiments:

1. 10-12 experiments based on the syllabus covered as above will be performed and evaluated on a continuous basis.

Subject Code: 11380102	**Subject Title:** Cryptography & Network Security
Pre-requisite: Basic knowledge of computer network and security.	

Course Objective:

1. Explain the importance and application of each of confidentiality, integrity, authentication and availability
2. Understand various cryptographic algorithms.
3. Understand the basic categories of threats to computers and networks
4. Understand Intrusions and intrusion detection
5. Discuss Web security and Firewalls

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	0	2	4	60	40	30	20	150

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Security Concepts** Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms, A model for Network Security Cryptography Concepts and Techniques: Introduction, 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.	8	20
2	**Symmetric key Ciphers** Block Cipher principles, DES, AES, Blowfish, RC5, IDEA, Block cipher operation, Stream ciphers, RC4. Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Elgamal Cryptography, Diffie-Hellman Key Exchange, Knapsack Algorithm.	8	20
3	**Cryptographic Hash Functions** Message Authentication, Secure Hash Algorithm (SHA-512), Message authentication codes: Authentication requirements, HMAC, CMAC, Digital signatures, Elgamal Digital Signature	8	20

	Scheme. Key Management and Distribution: Symmetric Key Distribution Using Symmetric & Asymmetric Encryption, Distribution of Public Keys, Kerberos, X.509 Authentication Service, Public – Key Infrastructure.		
4	**Transport-level Security** Web security considerations, Secure Socket Layer and Transport Layer Security, HTTPS, Secure Shell (SSH) Wireless Network Security: Wireless Security, Mobile Device Security, IEEE 802.11 Wireless LAN, IEEE 802.11i Wireless LAN Security.	8	20
5	**E-Mail Security** Pretty Good Privacy, S/MIME IP Security: IP Security overview, IP Security architecture, Authentication Header, Encapsulating security payload, combining security associations, Internet Key Exchange Case Studies on Cryptography and security: Secure Multiparty Calculation, Virtual Elections, Single sign On, Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability.	8	20

Course Outcome:

1. Classify the various classical encryption techniques.
2. Compare various public key cryptographic techniques.
3. Evaluate authentication and hash algorithms
4. Choose intrusion detection and its solutions to overcome the attacks.
5. Develop strong password methods

List of Textbooks:

1. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.
2. Cryptography and Network Security: Forouzan Mukhopadhyay, Mc Graw Hill, 3rd Edition

List of Reference Books:

1. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.
2. Cryptography and Network Security: Forouzan Mukhopadhyay, Mc Graw Hill, 3rd Edition
3. Introduction to Network Security: Neal Krawetz, Cengage Learning
4. Network Security and Cryptography: Bernard Menezes, Cengage Learning

List of Suggested Experiments:

1. 10-12 experiments based on the syllabus covered above will be performed and evaluated on a continuous basis.

Subject Code: 11380110	**Subject Title:** Blockchain Infrastructure and Decentralized Systems
Pre-requisite: Computer Networks and Security, Information Security and Applied Cryptography	

Course Objective:

1. Introduce the concept and the basics of blockchain technologies
2. Enable awareness on the different generations of blockchains.
3. Provide knowledge on various applications of blockchain technologies

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	0	2	4	60	40	30	20	150

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Introduction** – Blockchain history, basics, architectures, Types of blockchain, Base technologies – Dockers, Hash function, Digital Signature - ECDSA, Zero Knowledge Proof.	8	25
2	**Bitcoins** – Fundamentals, aspects of bitcoins, properties of bitcoins, bitcoin transactions, bitcoin P2P networks, block generation at bitcoins, consensus algorithms- Proof of Work, Proof of Stake, Proof of Burn.	8	25
3	**Ethereum**- Introduction to Ethereum, Consensus Mechanisms, Smart Contracts.	8	25
4	**Applications** – Blockchain applications, e-governance, smart cities, smart industries, Finance, Medical Record Management System, use cases, trends on Blockchains.	8	25

Course Outcome:

1. Understand the basics of blockchain Technologies and its various applications.

2. Implement blockchain ledgers.
3. Capable of identifying problems on which blockchains could be applied.

List of Textbooks:

1. Baxv Kevin Werbach, The Blockchain and the new architecture of Trust, MIT Press, 2018
2. Joseph J. Bambara and Paul R. Allen, Blockchain – A practical guide to developing business, law, and technology solutions, McGraw Hill, 2018.

List of Reference Books:

1. Joseph J. Bambara and Paul R. Allen, Blockchain, IoT, and AI: Using the power of three to develop business, technical, and legal solutions, Barnes & Noble publishers, 2018.
2. Melanie Swan, Blockchain – Blueprint for a new economy, OReilly publishers, 2018.
3. Jai Singh Arun, Jerry Cuomo, Nitin Gaur, Blockchain for Business, Pearson publishers, 2019.
4. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.

List of Suggested Experiments:

1. 10-12 experiments based on the syllabus covered as above will be performed and evaluated on continuous basis.

SubjectCode:10000151	Subject Title: Research Methodology and IPR
Pre-requisite: Nil	

Course Objective:

1. To provide fundamental and advanced knowledge of the subject domain.
2. To develop analytical, problem-solving, and research-oriented skills among students.
3. To enable students to understand modern tools, techniques, and emerging technologies relevant to the course.
4. To enhance practical implementation abilities for solving real-world industrial and research problems.
5. To encourage innovation, critical thinking, and continuous learning in the respective field of study.

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
				Theory		Practical		
Lecture	Tutorial	Practical	Credit	University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	Total
1	1	2	3	0	0	80	20	100

	Subject Content		
Sr. No.	Topic	Total Hours	Weight (%)
1	Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations	05	17
2	Effective literature studies approaches, analysis Plagiarism, Research ethics,	04	15
3	Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.	05	17
4	MoNature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.	05	17

	Subject Content		
Sr. No.	**Topic**	**Total Hours**	**Weight (%)**
5	New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.	05	17
6	New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.	05	17

Course Outcomes

1. Understand research problem formulation.
2. Analyze research related information
3. Follow research ethics
4. Understand that today's world is controlled by Computer, Information Technology, but tomorrow world will be ruled by ideas, concept, and creativity.
5. Understanding that when IPR would take such important place in growth of individuals & nation, it is needless to emphasis the need of information about Intellectual Property Right to be promoted among students in general & engineering in particular.
6. Understand that IPR protection provides an incentive to inventors for further research work and investment in R & D, which leads to creation of new and better products, and in turn brings about, economic growth and social benefits.

List of Text Books

1. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students'"
2. Wayne Goddard and Stuart Melville, "Research Methodology: An Introduction"
3. Ranjit Kumar, 2nd Edition, "Research Methodology: A Step by Step Guide for beginners"
4. Halbert, "Resisting Intellectual Property", Taylor & Francis Ltd, 2007.
5. Mayall, "Industrial Design", McGraw Hill, 1992.
6. Niebel, "Product Design", McGraw Hill, 1974
7. Asimov, "Introduction to Design", Prentice Hall, 1962.
8. Robert P. Merges, Peter S. Menell, Mark A. Lemley, "Intellectual Property in New Technological Age", 2016.

List of Reference Books

1. Probability and Statistics for Engineers and Scientists — Ronald E. Walpole**.**
2. Probability and Statistical Inference — Robert V. Hogg and Elliot Tanis.
3. Machine Learning: A Probabilistic Perspective — Kevin P. Murphy, MIT Press**.**
4. Statistical Methods — N. G. Das, McGraw Hill Education.
5. Fundamentals of Statistics — S. C. Gupta, Himalaya Publishing House.

Open e-Resources

1. NPTEL: https://onlinecourses.nptel.ac.in/noc19_ge21/preview
2. NPTEL: https://onlinecourses.nptel.ac.in/noc22_ge08/preview

Subject Code: 11380104	**Subject Title:** Cyber Crime, Cyber Law and IPR
Pre-requisite: Cyber security fundamentals	

Course Objective:

1. Understand the core fundamentals of cyber space
2. Understand the IT act 2000.
3. To understand the patent, copy right and trademark polices.
4. To know the evolution of ecommerce.
5. Learn the crime investigation methods.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	0	2	4	60	40	30	20	150

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Introduction:** Emergence of Cyber space. Cyber Jurisprudence, Jurisprudence and law, Doctrinal approach, Consensual approach, Real Approach, Cyber Ethics, Cyber Jurisdiction, Hierarchy of courts, Civil and criminal jurisdictions, Cyberspace-Web space, Web hosting and web Development agreement, Legal and Technological Significance of domain Names, Internet as a tool for global access.	11	25
2	**Overview of IT Act 2000:** Amendments and Limitations of IT Act, Digital Signatures, Cryptographic Algorithm, Public Cryptography, Private Cryptography, Electronic Governance, Legal Recognition of Electronic Records, Legal Recognition of Digital Signature Certifying Authorities, Cyber Crime and Offences, Network Service Providers Liability, Cyber Regulations Appellate Tribunal, Penalties and Adjudication.	11	25
3	**Patent Law, Trademark Law, Copyright, Software** Copyright or Patented, Domain Names and Copyright disputes, Electronic Data Base and its Protection, IT Act and Civil Procedure Code, IT Act and Criminal Procedural Code, Relevant Sections of Indian Evidence Act, Relevant Sections of Bankers Book	10	20

	Evidence Act, Relevant Sections of Indian Penal Code, Relevant Sections of Reserve Bank of India Act, Law Relating to Employees and Internet, Alternative Dispute Resolution, Online Dispute Resolution.		
4	**Evolution and development in E-commerce:** paper vs. paperless contracts E-Commerce models- B2B, B2C, E security. **Application area**: Business, taxation, electronic payments, supply chain, EDI, E-markets, Emerging Trends.	5	15
5	**Case Study on Cyber Crimes:** Harassment Via E-Mails, Email Spoofing (Online A Method of Sending E-Mail Using a False Name or E-Mail Address to Make It Appear That the E-Mail Comes from Somebody Other Than the True Sender, Cyber Pornography (Exam. MMS), Cyber-Stalking, etc.	5	15

Course Outcome:

1. Analyze and evaluate the social and Intellectual Property issues emerging from Cyberspace.
2. Apply the legal and Policy developments in various countries to regulate Cyberspace
3. Implement in-depth knowledge of Information Technology Act and legal framework of Right to Privacy, Data Security and Data Protection
4. Understanding of relationship between commerce and cyberspace
5. Analyze cybercrime and investigation of cases.

List of Textbooks:

1. K.Kumar," Cyber Laws: Intellectual property & E Commerce, Security", 1st Edition, Dominant Publisher, 2011.
2. Rodney D. Ryder, "Guide to Cyber Laws", Second Edition, Wadhwa and Company, New Delhi, 2007.

List of Reference Books:

1. Vakul Sharma, "Handbook of Cyber Laws" Macmillan India Ltd, 2nd Edition, PHI, 2003.
2. Justice Yatindra Singh, "Cyber Laws", Universal Law Publishing, 1st Edition, New Delhi, 2003.
3. Sharma, S.R., "Dimensions of Cyber Crime", Annual Publications Pvt. Ltd., 1st Edition, 2004.
4. Augastine, Paul T.," Cyber Crimes and Legal Issues", Crecent Publishing Corporation, 2007**.**

List of Suggested Experiments:

1. 10-12 experiments based on the syllabus covered as above will be performed and evaluated on continuous basis.

Subject Code:11380105	**Subject Title:** Risk Assessment and Security Audit

Pre-requisite: Basic knowledge of cyber security.

Course Objective:

1. To gain knowledge about Information Risk.
2. To discover knowledge in collecting data about organization.
3. To do various analyses on Information Risk Assessment.
4. To understand IT audit and its activities.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	0	2	4	60	40	30	20	150

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Introduction:** what is risk and risk management, risk assessment, monitoring and review, cyberspace, cyber system. What is cyber security, how does cyber security relate to information security, how does cyber security relate to critical infrastructure protection, how does cyber security relate to safety, what is cyber risk, communication and consultation of cyber risk, cyber risk assessment, monitoring and review of cyber risk	8	20
2	**Risk identification techniques**: malicious risks, non-malicious risks, risk analysis, threat analysis, vulnerability analysis, likelihood of incidents, consequences of incidents 4 10%, Risk evaluation, consolidation of risk analysis results, evaluation of risk level, risk aggregation, risk grouping, risk treatment identification, risk acceptance	8	20
3	**Risk Factor:** Two-factor measure, three-factor measure, many-factor measure, which measure to use for cyber risk? classification of scales, qualitative versus quantitative risk assessment, scale for likelihood, scale for consequence, what scale to use for cyber risk, defining information security metrics, Risk analysis techniques, Automating metric calculations and tools.	14	35
4	**Security Audit:** What is an IT security assessment, what is an IT security audit, what is compliance, how does an audit differ from assessment, case study:	10	25

	Enron, WorldCom, TJX Credit Card Breach 2 5% 11. Organization does to comply, Auditing within IT infrastructure, managing IT compliance 3 5% 12. Auditing standards and frameworks, COSO, COBIT, ISO/IEC 27001 standard, ISO/IEC 27002 standard, NIST 800-53.		

Course Outcome:

1. Design information security risk management framework and methodologies
2. Identify and modeling information security risks
3. Judge the difference between qualitative and quantitative risk assessment methods
4. Articulate information security risks as business consequences

List of Textbooks:

1. Mark Talabis, "Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis", Kindle Edition. ISBN:978-1-59749-735-0.
2. David L. Cannon, "CISA Certified Information Systems Auditor Study Guide",SYBEX Publication. ISBN: 978-0-470-23152-4.

List of Reference Books:

1. Cyber-Risk Management by AtleRefsdal, Bj¢rnarSolhaug and KetilSt¢len - Springer
2. Quantitative Risk Assessment: The Scientific Platform by TerjeAven – Cambridge University Press
3. IT Security Risk Control Management – An Audit Preparation Plan by Raymond Pompon – Apress
4. Auditing IT Infrastructures for Compliance by Marty M. Weiss and Michael G. Solomon – Jones & Bartlett Learning

List of Suggested Experiments:

1. 10-12 experiments based on the syllabus covered as above will be performed and evaluated on continuous basis.

Subject Code: 11380111	**Subject Title:** Secure Distributed Cloud Systems

Pre-requisite: Basic knowledge of computer fundamentals

Course Objective:

1. Compare modern security concepts as they are applied to cloud computing
2. Assess the security of virtual systems
3. Evaluate the security issues related to multi-tenancy
4. Appraise compliance issues that arise from cloud computing

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	0	2	4	60	40	30	20	150

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Cloud Security Concepts:** Confidentiality, privacy, integrity, authentication, non-repudiation, availability, access control, defense in depth, least privilege, how these concepts apply in the cloud, what these concepts mean and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud; Cryptographic Systems- Symmetric cryptography, stream ciphers, block ciphers, modes of operation, public-key cryptography, hashing, digital signatures, public-key infrastructures, key management, X.509 certificates, OpenSSL.	10	25
2	**Multi-Tenancy Issues**: Isolation of users/VMs from each other. How the cloud provider can provide this; Virtualization System Security Issues- e.g. ESX and ESXi Security, ESX file system security, storage considerations, backup and recovery; Virtualization System Vulnerabilities- Management console vulnerabilities, management server vulnerabilities, administrative VM vulnerabilities, guest VM vulnerabilities, hypervisor vulnerabilities, hypervisor escape vulnerabilities, configuration issues, malware (botnets etc).	9	18
3	**Virtualization System-Specific Attacks:** Guest hopping, attacks on the VM (delete the VM, attack on the control of the VM, code or file injection into the virtualized file structure), VM migration attack, hyper jacking.	7	14

4	**Technologies For Virtualization-Based Security Enhancement:** IBM security virtual server protection, virtualization-based sandboxing; Storage Security-HIDPS, log management, Data Loss Prevention. Location of the Perimeter.	9	18
5	**Legal And Compliance Issues:** Responsibility, ownership of data, right to penetration test, local law where data is held, examination of modern Security Standards (eg PCIDSS), how standards deal with cloud services and virtualization, compliance for the cloud provider vs. compliance for the customer.	10	25

Course Outcome:

1. Analyze and evaluate the cloud security needs of an organization.
2. Analyze the security Multi-Tenancy Issues.
3. Apply the security principles to virtualization system-specific attacks.
4. Implement and manage the security essentials in IT Sector
5. Analyze architecture and implementation of modern security systems.

List of Textbooks:

1. Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" O'Reilly Media; 1 edition [ISBN: 0596802765], 2009.
2. Ronald L. Krutz, Russell Dean Vines, "Cloud Security" [ISBN: 0470589876], 2010.

List of Reference Books:

1. Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing" 2009.
2. VMware "VMware Security Hardening Guide" White Paper, June 2011.
3. Cloud Security Alliance 2010, "Top Threats to Cloud Computing" Microsoft 2013.
4. Timothy Grance; Wayne Jansen; NIST "Guidelines on Security and Privacy in Public Cloud Computing", 2011.

List of Suggested Experiments:

1. 10-12 experiments based on the syllabus covered above will be performed and evaluated on a continuous basis.

Subject Code:11380107	**Subject Title:** Biometric Systems & Biometric Image Processing
Pre-requisite: Basic knowledge of cyber security.	

Course Objective:

1. To understand the technologies of fingerprint, iris, face and speech recognition
2. To understand the general principles of design of biometric systems and the underlying trade-offs.
3. To recognize personal privacy and security implications of biometrics-based identification technology.
4. To identify issues in the realistic evaluation of biometrics-based systems.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	1	0	4	60	40	0	0	100

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Introduction**- benefits of biometrics over traditional authentication systems -benefits of biometrics in identification systems-selecting a biometric for a system –Applications - Key biometric terms and processes - biometric matching methods -Accuracy in biometric systems	6	15
2	**Fingerprint Identification Technology**: Fingerprint Patterns, Fingerprint Features, Fingerprint Image, width between two ridges - Fingerprint Image Processing – Minutiae Determination – Fingerprint Matching: Fingerprint Classification, Matching policies.	8	20
3	**Face Recognition**: Introduction, components, Facial Scan Technologies, Face Detection, Face Recognition, Representation and Classification, Kernel- based Methods and 3D Models, Learning the Face Spare, Facial Scan Strengths and Weaknesses, Methods for assessing progress in Face Recognition.	8	20
4	**Fusion in Biometrics:** Introduction to Multibiometric – Information Fusion in Biometrics – Issues in Designing a Multibiometric System – Sources of Multiple	12	30

	Evidence – Levels of Fusion in Biometrics – Sensor level, Feature level, Rank level, Decision level fusion – Score level Fusion. Examples – Biopotential and gait based biometric systems. **Case Study Presentations:** Biometrics in Banking Industry, Biometrics in Computerized, Patient Records, Biometrics in Credit Cards, Biometrics in Mass Disaster Victim, Identification Forensic Odontology		
5	**Image Processing:** Digital image representation, fundamental steps in image processing. Image enhancement: The spatial domain methods. The frequency domain methods image segmentation: Pixel classification by thresholding, histogram technique, smoothing and thresholding, gradient based segmentation: gradient image, boundary tracking Laplacian edge detection.	6	15

Course Outcome:

1. Demonstrate knowledge of the basic physical and biological science and engineering principles underlying biometric systems.
2. Understand and analyze biometric systems at the component level and be able to analyze and design basic biometric system applications.
3. Demonstrate knowledge engineering principles underlying biometric systems.
4. Analyze design basic biometric system applications.
5. Understand various Biometric security issues.

List of Textbooks:

1. James Wayman, Anil Jain, Davide Maltoni, Dario Maio, Biometric Systems, Technology Design and Performance Evaluation, Springer, 2005.
2. David D. Zhang, Automated Biometrics: Technologies and Systems, Kluwer Academic Publishers, New Delhi, 2000.

List of Reference Books:

1. Arun A. Ross, Karthik Nandakumar, A.K.Jain, Handbook of Multibiometrics, Springer, New Delhi, 2006.
2. Samir Nanavathi, Michel Thieme, and Raj Nanavathi : “Biometrics -Identity verification in a network”, 1st Edition, Wiley Eastern, 2002.
3. John Chirillo and Scott Blaul: “Implementing Biometric Security”, 1st Edition, Wiley Eastern Publication, 2005.
4. John Berger: “Biometrics for Network Security”, 1st Edition, Prentice Hall, 2004.

Subject Code: 11380112	**Subject Title:** Machine Learning for Threat Detection and Prevention
Pre-requisite: Basic knowledge of machine learning.	

Course Objective:

1. To describe the fundamental concepts of machine learning for devising security mechanisms.
2. To enumerate the techniques for intrusion detection and malware detection and analysis using machine learning.
3. To learn the machine learning techniques for network traffic analysis
4. To analyses the machine learning approaches for security for probable abuse by the adversary.
5. To design secure machine learning based schemes for malware detection and intrusion detection

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	1	0	4	60	40	0	0	100

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Introduction:** Introduction to Information Assurance. Review of Cybersecurity Solutions: Proactive Security Solutions, Reactive Security Solutions: Misuse/Signature Detection, Anomaly Detection, Hybrid Detection, Scan Detection. Profiling Modules. Understanding the Fundamental Problems of Machine-Learning Methods in Cybersecurity. Incremental Learning in Cyber infrastructures. Feature Selection/Extraction for Data with Evolving Characteristics. Privacy-Preserving Data Mining. Motivation for ML in security with real-world case studies. Topics of interest in applications of machine learning for security.	4	10
2	**Machine learning techniques for intrusion detection:** Emerging Challenges in Cyber Security for Intrusion Detection: Unifying the Current Anomaly Detection Systems, Network Traffic Anomaly Detection. Imbalanced Learning Problem and Advanced Evaluation Metrics for IDS. Reliable Evaluation Data Sets or Data Generation Tools. Privacy Issues in Network Anomaly Detection. Machine	8	20

	Learning Techniques: for Anomaly Detection, for Misuse/Signature detection, for Hybrid detection, for Scan detection. Cost-Sensitive Modeling for Intrusion Detection. Data Cleaning and Enriched Representations for Anomaly Detection in System Calls.		
3	**Machine learning techniques for malware analysis:** Emerging Cyber Threats in malwares: Threats from Malware, Botnets, Cyber Warfare, Mobile Communication. Cyber Crimes. Malware Analysis: Feature generation, Features to Classification. Taxonomy of malware analysis approaches based on machine learning. Malware Detection, Similarity Analysis, Category Detection. Feature Extraction. PE Features. Supervised, Unsupervised and Semi-supervised learning algorithms for Malware Detection. Using Deep Learning Approaches: Generative Adversarial Networks.	8	20
4	**Network traffic analysis & web abuse detection:** Machine Learning for Profiling Network Traffic: Theory of Network defense (access control, authentication, detecting in-network attackers, data-centric security, honeypots), Predictive model for classifying network attacks.	8	20
5	**Machine learning in privacy preservation & adversarial machine learning:** k-anonymity; l-diversity; deferentially private data storage/release; verifiable differential privacy; privacy-preserving inference of social networking data; privacy-preserving recommender system; privacy versus utility. Machine learning techniques for Privacy Preserving Data Mining. Adversarial Machine Learning: Motivation and Background. Practical Scenarios and Examples. Modelling the Adversary: Attack Surface Adversary Goals Adversary capabilities. Taxonomy of Adversarial Attacks on Machine Learning: Influence Specificity Security Violation. Data poisoning; Perturbation; Defense mechanism; Generative Adversarial Networks. A peep into Industry Perspectives: Theme of inference Secure Software Development Life Cycle or Secure Development Cycle. Key Inferences in terms of Security gaps, Suggested panacea	12	30

Course Outcome:

1. Have a knowledge of the limitations of the conventional security software in the wake of machine learning based attacks on the security software
2. Be able to apply the concepts of machine learning based intrusion detection to analyze the ids.
3. Be able to analyze the malware analysis and mitigation-based solutions for the probable threats therein.
4. Be able to design threat models based on machine learning approaches for network analysis.
5. Be able to use the concepts of machine learning to prevent security design faults

List of Textbooks:

1. Clarence Chio, David Freeman. Machine Learning and Security. Protecting Systems with Data and Algorithms, O'Reilly Media Publications. 2018

2. Marcus A. Maloof (Ed.), Machine Learning and Data Mining for Computer Security: Methods and Applications, Springer-Verlag London Limited, 2006

List of Reference Books:

1. Sumeet Dua and Xian Du. Data Mining and Machine Learning in Cybersecurity. CRC Press, Taylor and Francis Group, LLC. 2011
2. Tom Mitchell. Machine Learning. McGraw Hill, 1997.
3. Gupta, Brij B., and Quan Z. Sheng, eds. Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press, 2019.
4. Artificial Intelligence and Data Mining Approaches in Security Frameworks Editor(s): Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, Rashmi Agrawal, 2021

Subject Code:11380109	**Subject Title:** Embedded System and Hardware Security
Pre-requisite: Basic electronic fundamentals	

Course Objective:

1. Understand the core fundamentals of embedded systems security
2. Understand common hardware security
3. To understand the embedded hardware and hacking discovery
4. To know the embedded software detection and prevention policies
5. Learn the security principles of embedded system design.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	1	0	4	60	40	0	0	100

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Introduction to Embedded Systems:** Embedded hardware units, Embedded system software, Device drivers and interrupt services, Inter-process communication and synchronization of processes.	5	10
2	**Embedded System Security and Trust:** Physical attacks, Side channel analysis, Trusted integrated circuit, Trusted platform module (TPM), Hardware Trojans, Cryptographic hashing, Stack-based attacks against embedded systems (Code injection and return-oriented programming), Physically unclonable functions, Fault injection attacks, Reverse engineering, Supply chain security and trust.	10	20
3	**Embedded Hardware Security and Hacking:** Securing external memory, JTAG/Debug port considerations, Physical attack vectors, Temper detection and logging, Soldering techniques, Board analysis methodology, Component Identification, Device instrumentation, Bus monitoring and decoding, Access via JTAG.	15	30

4	**Embedded Software Security:** Fundamentals of embedded software security, Common firmware vulnerabilities, Software vulnerabilities in ARM/MIPS/etc., Embedded code vulnerabilities, Assembly code analysis.	7	20
5	**Embedded Exploitation:** Exploitation techniques on ARM/MIPS/x86, Defenses against ARM exploits, Security practices for embedded software, Defensive software architectures, Defensive hardware interfaces.	8	20

Course Outcome:

1. Analyze and evaluate the embedded systems security needs of an organization.
2. Apply the security principles to embedded systems trust.
3. Implement and manage the hardware security essentials in embedded systems.
4. Understand fundamental concepts of embedded software security.
5. Analyze Exploitation and implementation of embedded software.

List of Textbooks:

1. Tehranipoor, Mohammad, Wang, Cliff (Eds.), Introduction to Hardware Security and Trust, Springer
2. David Kleidermacher and Mike Kleidermacher, Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development, Elsevier Science, Newnes Publication

List of Reference Books:

1. Louis Goubin and Mitsuru Matsui, Cryptographic Hardware and Embedded Systems, Springer¬Verlag Berlin and Heidelberg GmbH & Co. KG
2. Tammy Noergaard "Embedded Systems Architecture: A Comprehensive Guide for Engineers and Programmers", Elsevier (Singapore) Pvt. Ltd. Publications, 2005.
3. John H. Davies "MSP430 Microcontroller Basics ",Elsevier Ltd Publications, Copyright 2008.
4. Manuel Jiménez Rogelio, PalomeraIsidoro Couvertier "Introduction to Embedded Systems Using Microcontrollers and the MSP430" Springer Publications, 2014.

Semester 2

Subject Code: 11380210	Advanced Digital Forensic and Investigation
Pre-requisite: Computer Networks, Operating Systems, Information Security, Basics of Cyber Laws.	

Course Objective:

1. To provide in-depth knowledge of digital forensic principles and investigation processes.
2. To enable students to acquire, preserve, analyze, and present digital evidence.
3. To develop expertise in computer, network, mobile, and cloud forensic techniques.
4. To understand legal, ethical, and procedural aspects of digital investigations.
5. To prepare students for advanced research and professional forensic practice.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	0	2	4	60	40	30	20	150

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Foundations of Digital Forensics:** Introduction to digital forensics science, history, scope, and importance, Digital evidence definition and types (volatile/non-volatile), Principles of digital forensics, admissibility & integrity, Forensic readiness and planning, Cybercrime overview and role of forensics in investigation.	04	12
2	**Digital Investigation Process & Legal Aspects:** Digital forensic investigation lifecycle and models. Incident response and first responder guidelines. Search and seizure procedures. Chain of custody and evidence handling. Indian IT Act, Evidence Act (relevant sections), international cyber laws. Ethics and professional conduct in forensic investigations	06	15
3	**Computer & File System Forensics:** File system structures – FAT, NTFS, ext4. Disk imaging and acquisition techniques. Hashing and verification methods. Deleted file recovery and data carving. Windows registry analysis. Memory and live system forensics.	08	20

4	**Network, Email & Cloud Forensics:** Network traffic capture and analysis. Log analysis – firewall, IDS/IPS, server logs. Email forensics – header analysis, spoofing detection, tracing techniques. Cloud forensic challenges and models. Investigation of attacks in cloud environments.	08	20
5	**Mobile Forensics, Anti-Forensics & Case Studies:** Mobile device forensics – Android & iOS architecture, acquisition techniques, SIM and SD card analysis. Anti-forensic techniques and countermeasures. Forensic report writing and expert testimony. Real-world cybercrime case studies and analysis.	08	33

Course Outcome:

1. CO1: Understand digital forensic concepts, principles, and investigation methodologies.
2. CO2: Acquire and preserve digital evidence while maintaining integrity and legal compliance.
3. CO3: Perform computer, network, mobile, and cloud forensic analysis using standard techniques.
4. CO4: Detect and counter anti-forensic techniques used by cybercriminals.
5. CO5: Prepare forensic reports and present digital evidence in legal and professional settings.

List of Textbooks:

1. Eoghan Casey, Handbook of Digital Forensics and Investigation, Academic Press.
2. John Sammons, The Basics of Digital Forensics, Syngress.

List of Reference Books:

1. Bill Nelson, Amelia Phillips, Christopher Steuart, Guide to Computer Forensics and Investigations, Cengage Learning.
2. Warren G. Kruse & Jay G. Heiser, Computer Forensics: Incident Response Essentials, Addison-Wesley.
3. Brian Carrier, File System Forensic Analysis, Addison-Wesley.

List of Suggested Experiments:

1. 10-12 experiments based on the syllabus covered as above will be performed and evaluated on a continuous basis

Subject Code: 11380211	Cybersecurity Governance, Risk & Legal Compliance
Pre-requisite: Information Security Fundamentals, Computer Networks, Basics of Cyber Laws, Management Principles	

Course Objective:

1. To understand cybersecurity governance frameworks and organizational security structures.
2. To develop risk assessment, analysis, and mitigation strategies for cyber threats.
3. To gain knowledge of national and international cybersecurity laws, regulations, and compliance standards.
4. To understand privacy, data protection, and regulatory requirements across industries.
5. To enable students to align cybersecurity strategy with business and legal objectives.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	0	2	4	60	40	30	20	150

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Cybersecurity Governance:** Concept and importance of cybersecurity governance. Roles and responsibilities of board, management, and CISO. Security policies, standards, procedures, and guidelines. Enterprise security architecture. Governance frameworks – COBIT, ISO/IEC 27001, NIST CSF.	08	20
2	**Cyber Risk Management:** Cyber risk concepts and threat landscape. Risk assessment methodologies – qualitative and quantitative risk analysis. Risk identification, evaluation, treatment, and acceptance. Business impact analysis (BIA). Third-party and supply chain risk management.	08	20
3	**Compliance & Security Standards:** Information, security standards and best practices. ISO 27001/27002 controls. PCI-DSS, HIPAA, SOX, GDPR overview. Auditing, monitoring, and compliance management. Security metrics and KPIs.	08	20
4	**Cyber Laws & Legal Frameworks:** Indian IT Act 2000 (amended), Digital Personal Data Protection Act (DPDP). Indian Evidence Act (relevant sections).	08	20

	Cybercrime laws and investigation procedures. International cyber laws and conventions. Jurisdiction and cross-border legal challenges.		
5	**Privacy, Ethics & Emerging Issues:** Data privacy principles and privacy-by-design. Ethical issues in cybersecurity governance. Incident response from legal perspective. Breach notification requirements. Emerging legal challenges in cloud, AI, IoT, and digital forensics. Case studies on compliance failures.	08	20

Course Outcome:

1. CO1: Understand cybersecurity governance models and organizational security structures.
2. CO2: Perform cyber risk assessment and develop risk mitigation strategies.
3. CO3: Apply cybersecurity standards and compliance frameworks in organizations.
4. CO4: Interpret and apply national and international cyber laws and regulations.
5. CO5: Address privacy, ethical, and legal challenges in modern cybersecurity environments.

List of Textbooks:

1. Joseph Migga Kizza, Guide to Computer Network Security, Springer.
2. Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley.

List of Reference Books:

1. William Stallings & Lawrie Brown, Computer Security: Principles and Practice, Pearson.
2. Mark S. Merkow & Lakshmikanth Raghavan, Information Security and Risk Management, Pearson.
3. Deborah Russell, Privacy and Data Protection, CRC Press.

List of Suggested Experiments/ Case Studies:

1. Cyber risk assessment of an enterprise
2. Compliance gap analysis using ISO 27001
3. Study of major data breach incidents and legal implications
4. Analysis of GDPR / DPDP Act compliance scenarios

Subject Code: 11380212	**IT Act Under Cyber Law**
Pre-requisite: Basic understanding of computer networks, internet technologies, and fundamental cybersecurity concepts	

Course Objective:

1. This course introduces students to the legal aspects of cyberspace, digital technologies, and online behavior. It aims to:
2. Build awareness of digital rights and responsibilities.
3. Explain laws governing internet use and cyber activities.
4. Develop safe and ethical online practices.
5. Provide basic understanding of cybercrimes and remedies.
6. Encourage responsible digital citizenship.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	0	2	4	60	40	30	20	150

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	Unit I. Introduction to Cyber Space and Cyber Law ● Cyber space, regulation, scope, current legal challenges ● Cyber law - the Information technology law and its application ● Meaning of computer, computer network, computer system, communication device, addressee, originator Statute The Information Technology Act, 2000 - Section 1(2), Definitions -Section 2, subsections (b), (ha), (i), (j), (k), (l), (o), (v), (w), (za)	6	15
2	Unit II. Jurisdiction in Cyber Space ● No geographical boundaries, applicability of traditional rules of jurisdiction on internet, rules of private international law ● Personal jurisdiction on defendant Cause of action carries on business Hague convention on Choice of court agreements, 2005; adjudicating officer and cyber appellate tribunal under the Information Technology Act, 2000 (power of	7	15

	adjudging compensation and penalties under the Information Technology Act, 2000; no criminal jurisdiction)		
3	Unit III. Electronic Contracts ● Types of Electronic Contracts-email contracts, clickwrap contracts, shrinkwrap contracts;Issues of Security /Issues of Privacy/ Technical Issues Legal issues in Cyber Contracts ● International efforts to resolve the issues - UNCITRAL Models: E-commerce, 1996, Electronic signatures, 2001, Convention on Electronic Communications in International Contracts, 2005 ; ● Indian Position - Legal issues in cyber contracts - Formation of cyber contract; Standard form contracts requirement of notice[(Specht v. Netscape Communications, 306 F. 3d 17 (October 1, 2002) Caspi v. The Microsoft Network, LLC., 1999 N.J. Super, Lexis 254 (July 2,1999) Writing and Signature Requirement; Legislative efforts under the Information Technology Act, 2000 ● Legal recognition of electronic record and electronic signatures; digital signature -its functions, asymmetric cryptosystem, key pair, public key, private key, Secure electronic record and secure electronic signature, Public key Infrastructure	8	20
4	**Unit IV Cyber Warfare** • National Security and Cyberspace – threats to cyber domain; Cases on Cyber Attacks • Estonia Case, Georgia Case and Stun text & Iranian Nuclear Programme, Whisper gate destructive malware; Cyber Terrorism • legal framework in U.K. and Indian criminal law; • Cyber-attack war or a conflict or espionage? • Application of international principles of jus ad bellum and jus in bello.	6	15
	Unit V Freedom of Speech & Human Rights Issues in Internet. • Freedom of Expression in Internet • Issues of Censorship -Blocking of content- hate speech, national security • (blocking of yahoo groups, Facebook contents etc.) liability of intermediary; Privacy Issues • Information Privacy; interception, monitoring [Apple iPhone v. IFB (privacy v national security), Ratan Tata v. Union of India, Writ Petition (Civil)No. 98 of 2010] • Computer emergency response team (CERT)	4	15
	UNIT-6 Cyber Crimes • Introduction to Cyber crimes and cyber forensics • Kinds of cyber crimes -Fraud and identity theft, cyber stalking; cyber pornography • Cyber terrorism • Cyber defamation, Phishing, Hacking etc. • Issues relating to Investigation, Jurisdiction, Evidence	6	20

Course Outcome:

1. CO1: Understand basic concepts of cyber law and digital governance
2. CO2: Identify common cyber-crimes and methods of prevention
3. CO3: Explain key provisions of Indian cyber laws and regulation
4. CO4: Demonstrate awareness of digital rights, privacy, and ethical issues
5. CO5: Apply cyber safety practices in personal and professional life

List of Textbooks:

1. Kamath Nandan, Law Relating to Computers Internet & E-commerce - A Guide to Cyberlaws & The Information Technology Act, Rules, Regulations and Notifications along with Latest Case Laws 2016
2. Kamlesh K Bajaj, Debjani Nag, E-commerce: the cutting edge of business, 2nd Ed. 2017
3. Vakul Sharma, Information Technology Law & Practice, 8th ed. 2023
4. Karnika Seth, Computers Internet and New Technology Laws, 2nd ed. 2016
5. Apar Gupta Commentary on Information Technology Act, 3rd ed. 2015
6. Aparna Viswanathan, Cyber Law (Indian & International Perspectives on key topics including Data Security, E-commerce, Cloud Computing and Cyber Crimes) 2012.
7. Derek S. Reverson, "An Introduction to National Security and Cyberspace" in Dereck S. Reverson(ed.), Cyberspace and National Security; Threats, opportunities and power in a virtual world pp.4 -19 (2013)
8. Clair Finkelstein and Kevin Govern, "Introduction; Cyber and Changing face of War" in Jens David.
9. Kamlesh K Bajaj, "Apple v. National Security"
10. Derek S. Reverson (ed.), Cyberspace and National Security;Threats, Oppurtunities, and Power in the Virtual World, Satyam Law International, First Indian Reprint (2013)

List of Suggested Experiments:

1. Study of cyber-crime case reports
2. Analysis of phishing and online fraud scenarios
3. Review of IT Act provisions through case examples
4. Digital privacy and footprint assessment exercise
5. Cyber safety awareness presentation
6. Preparation of cyber incident reporting format
7. Case study discussion on landmark cyber law judgments

Subject Code: 10000251	Technical Writing
Pre-requisite: Basic Language Skills	

Course Objective:

1. Technical Writing focuses on planning and preparation of word choices and sentences and focuses on vocabulary building and helps them to be an effective communicator.
2. Students will be able to produce a set of documents related to writing in the workplace and will be able to improve their ability to write clearly and accurately.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
2	0	0	0	-	50	-	-	50

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	Planning and Preparation, Word Order, Breaking up long sentences, Structuring	4	10
2	Paragraphs and Sentences, Being Concise and Removing Redundancy, Avoiding Ambiguity and Vagueness	4	10
3	Sections of a paper – Title, abstract, introduction, etc. review of the literature, writing - methods, results, discussion, conclusions and final check	6	20
4	Organization of technical report: Title, Authors, Affiliation, Abstract,	4	20
5	Three pass reading. Effective communication– Teacher/Student perspective. Listening – Hearing Vs. Listening. Notes Taking. Elevator Pitch. Technical writing.	4	20
6	Useful phrases and punctuation, in-text citation and bibliography– MLA/APA styles.	4	20

Course Outcome:

1. Understand that how to improve your writing skills and level of readability.
2. Learn about what to write in each section.

3. Learn various skills necessary that are necessary for doing research.
4. Ensure the good quality of paper at very first-time submission..

List of Reference Book:

1. Adrian Wallwork, English for Writing Research Papers, Springer New York Dordrecht Heidelberg London, 2011
2. Day R, How to Write and Publish a Scientific Paper, Cambridge University Press, 2006
3. Raman, Meenakshi and Sangeeta Sharma, "Technical Communication: Principle and Practice", Oxford University Press.
4. Goldbort R. Writing for Science, Yale University Press, 2006

Open e-Resource:

1. https://onlinecourses.nptel.ac.in/
2. https://nptel.ac.in/courses

Subject Code: 11380213	**Subject Title:** Advanced Firewalls & Intrusion Detection Systems
Pre-requisite: Computer Networks, Operating System, Cloud Computing	

Course Objective:

- To provide in-depth knowledge of firewall technologies and network security architectures.
- To understand the design, configuration, and deployment of advanced firewall systems.
- To study intrusion detection and prevention techniques for network and host systems.
- To analyze modern cyber attacks and detection mechanisms using IDS/IPS tools.
- To develop practical skills in configuring and evaluating security monitoring systems.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	0	2	4	60	40	30	20	150

	Subject Contents		
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Fundamentals of Network Security and Firewalls**: Network security architecture, role of firewalls in enterprise security, types of firewalls (packet filtering, stateful inspection, application gateway, proxy firewall), firewall policies and rule management, network segmentation, demilitarized zones (DMZ), next-generation firewall (NGFW) concepts.	8	18%
2	**Advanced Firewall Technologies and Configuration**: Firewall architectures and deployment models, unified threat management (UTM), deep packet inspection, application-layer filtering, VPN integration with firewalls, firewall high availability and load balancing, firewall logging and monitoring, configuration of enterprise firewalls.	10	22%
3	**Intrusion Detection Systems (IDS):** Concepts of intrusion detection, host-based IDS (HIDS) and network-based IDS (NIDS), signature-based and anomaly-based detection, IDS architecture and components, detection algorithms, alert management and event correlation.	8	18%
4	**Intrusion Prevention Systems (IPS) and Security Monitoring**: IPS architecture and operation, inline intrusion prevention techniques, threat intelligence integration, security information and event management (SIEM), log management and analysis, behavioral analysis for attack detection.	8	18%
5	**Advanced Threat Detection and Case Studies**: Detection of modern cyber attacks (DDoS, malware, phishing, botnets, advanced persistent threats), machine learning approaches for intrusion detection, cloud and virtualized firewall environments, real-world case studies, security incident response and mitigation strategies.	8	24%

Course Outcome:

CO1: Understand advanced firewall architectures and security policies.
CO2**:** Configure and deploy firewall solutions for enterprise networks.
CO3**:** Analyze network traffic and detect malicious activities using IDS tools.
CO4**:** Implement intrusion prevention and security monitoring mechanisms.
CO5**:** Evaluate modern cyber threats and design appropriate defense strategies.

List of Textbooks:

1. William Stallings, Network Security Essentials: Applications and Standards, Pearson.
2. Chris Sanders & Jason Smith, Applied Network Security Monitoring, Syngress.

List of References:

1. Eric Cole, Ronald Krutz, James W. Conley, Network Security Bible, Wiley.
2. Stephen Northcutt & Judy Novak, Network Intrusion Detection, New Riders.
3. Richard Bejtlich, The Practice of Network Security Monitoring, No Starch Press.

List of Suggested Experiments:

1. 10 experiments/case studies based on the syllabus covered as above will be performed and evaluated on a continuous basis.

Subject Code: 11380214	**Subject Title:** Advanced Cyber Threat Intelligence & Cyber Warfare
Pre-requisite: Computer Networks, Network Security, Cryptography, Information Security Fundamentals.	

Course Objective:

- To provide advanced understanding of cyber threat intelligence (CTI) frameworks and methodologies.
- To study cyber warfare concepts, strategies, and national cyber defense mechanisms.
- To analyze threat actors, attack patterns, and advanced persistent threats (APT).
- To understand threat intelligence collection, analysis, and sharing mechanisms.
- To develop expertise in cyber threat hunting and incident response strategies.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	0	2	4	60	40	30	20	150

	Subject Contents		
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Introduction to Cyber Threat Intelligence**: Fundamentals of cyber threat intelligence, CTI lifecycle, strategic, tactical, operational, and technical intelligence, threat intelligence sources (open-source intelligence, dark web intelligence, malware analysis), cyber threat landscape and evolving attack vectors.	8	18%
2	**Threat Intelligence Collection and Analysis**: Intelligence gathering techniques, data collection and processing, indicators of compromise (IoCs), indicators of attack (IoAs), threat modeling techniques, MITRE ATT&CK framework, cyber kill chain model, threat attribution methods.	10	22%
3	**Cyber Warfare Concepts and Strategies**: Introduction to cyber warfare, cyber weapons and cyber espionage, cyber warfare strategies and doctrines, nation-state cyber operations, cyber terrorism and cyber espionage, international cyber conflict case studies.	8	18%
4	**Threat Hunting and Incident Response**: Proactive threat hunting methodologies, security operations centers (SOC), threat intelligence platforms (TIP), incident detection and response processes, digital evidence analysis, threat containment and mitigation strategies.	8	18%
5	**Advanced Topics in Cyber Warfare and Threat Intelligence**: Advanced persistent threats (APT), malware campaigns and botnet infrastructures, cyber deception techniques, information warfare and psychological operations, AI and machine learning in threat intelligence, real-world cyber warfare case studies and future trends.	8	24%

Course Outcome:

CO1: Understand the concepts and lifecycle of cyber threat intelligence.

CO2**:** Analyze threat intelligence data and identify indicators of compromise.

CO3**:** Understand cyber warfare strategies and nation-state cyber operations.

CO4**:** Perform proactive threat hunting and incident response activities.

CO5**:** Evaluate emerging cyber threats and develop intelligence-based defense strategies.

List of Textbooks:

1. Kyle Wilhoit & Joseph Muniz, Cyber Threat Intelligence, Packt Publishing.
2. Ben Buchanan, The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics, Harvard University Press.

List of References:

1. Allan Liska & Geoffrey Stowe, Cyber Threat Intelligence, O'Reilly Media.
2. Eric Cole, Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization, Syngress.
3. Jason Andress & Steve Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Syngress.

List of Suggested Experiments:

1. 10 experiments/case studies based on the syllabus covered as above will be performed and evaluated on a continuous basis.

Subject Code: 11380215	**Subject Title:** Network, Mobile & Cloud Security
Pre-requisite: Computer Networks, Operating System, Cloud Computing	

Course Objective:

- To understand security threats and defences in modern networks
- To analyse mobile and wireless security mechanisms
- To study cloud computing security challenges and solutions
- To apply cryptographic techniques in networked environments
- To evaluate real-world security breaches and countermeasures

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	0	2	4	60	40	30	20	150

	Subject Contents		
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Fundamentals of Network Security:** Security goals: CIA triad, AAA model, Types of attacks: passive vs active, DoS, spoofing, MITM Network vulnerabilities and threat modelling, Secure network architecture and defence-in-depth, Firewalls: packet filtering, stateful inspection, application firewalls, Intrusion Detection and Prevention Systems (IDS/IPS).	6	15%
2	**Cryptography & Secure Network Protocols:** Symmetric key cryptography (AES, DES – overview). Asymmetric cryptography (RSA, ECC – overview), Hash functions and message authentication codes Digital signatures and Public Key Infrastructure (PKI), Secure protocols: SSL/TLS, HTTPS, IPsec architecture and VPN concepts.	5	20%
3	**Mobile & Wireless Network Security:** Security issues in wireless networks IEEE 802.11 security: WEP, WPA, WPA2, WPA3, Bluetooth and ZigBee security, Mobile network security: GSM, UMTS, LTE vulnerabilities, Ad-hoc and sensor network security challenges, Secure routing and key management in wireless networks.	8	25%
4	**Mobile Platform & Application Security**: Mobile device threats and attack surfaces, Android security architecture, iOS security model, Mobile malware and spyware, Application-level vulnerabilities Secure mobile app development principles, Privacy, location tracking, and data leakage issues.	4	15%
5	**Cloud Computing Security:** Cloud computing overview and service models (IaaS, PaaS, SaaS), Cloud deployment models and shared responsibility model, Virtualization and hypervisor security Identity and Access Management (IAM), Data security: encryption at rest and in transit, Key management and secure storage, Cloud security threats and mitigation strategies, Compliance, governance, and auditing in cloud.	5	25%

Course Outcome:

CO1: Analyze network security threats and protection mechanisms
CO2: Design secure mobile and wireless communication systems
CO3: Explain cloud security models, risks, and controls
CO4: Apply cryptographic protocols for secure communication
CO5: Evaluate emerging security challenges in networks and cloud

List of Textbooks:

1. William Stallings, *Network Security Essentials*, Pearson
2. Kaufman, Perlman, Speciner, *Network Security*, Prentice Hall
3. Mather et al., *Cloud Security and Privacy*, O'Reilly

List of References:

1. Security and Privacy in Mobile and Wireless Networking – Gritzalis
2. Cloud Computing Security – John Rittinghouse
3. Android Security Internals – Nikolay Elenkov

List of Suggested Experiments:

1. 10 experiments/case studies based on the syllabus covered as above will be performed and evaluated on a continuous basis.

Subject Code: 11380216	**Subject Title:** Cyber Disaster Management & Recovery
Pre-requisite: Computer Networks, Operating System, Information Security Management.	

Course Objective:

- To understand cyber disasters and their impact on organizations and society
- To study principles of cyber disaster preparedness, response, and recovery
- To design effective incident response and disaster recovery plans
- To analyse real-world cyber incidents and resilience strategies
- To ensure business continuity and compliance in cyber environments

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	1	0	4	60	40	0	0	100

	Subject Contents		
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Introduction to Cyber Disasters:** Definition and classification of disasters, Cyber disasters vs physical disasters, Types of cyber disasters: ransomware, DDoS, data breaches, insider threats, Cyber warfare and cyber terrorism, Impact of cyber disasters on critical infrastructure, Cyber risk landscape and emerging threats.	5	15%
2	**Cyber Risk Assessment & Preparedness:** Cyber risk assessment methodologies, Threat modelling and vulnerability analysis, Cyber security policies and preparedness planning, Asset identification and criticality analysis, Cyber hygiene and preventive controls, Role of awareness and training in preparedness.	4	15%
3	**Incident Response & Crisis Management:** Cyber incident lifecycle Incident detection and reporting mechanisms, Incident response team (CSIRT / CERT) roles, Containment, eradication, and mitigation strategies, Digital forensics basics in incident response, Communication and coordination during cyber crises.	6	20%
4	**Disaster Recovery & Business Continuity:** Disaster Recovery (DR) concepts and strategies, Business Continuity Planning (BCP) Backup strategies and recovery techniques, RTO (Recovery Time Objective) and RPO (Recovery Point Objective), High availability and fault tolerance, Testing and maintenance of DR and BCP plans.	6	10%
5	**Governance, Legal & Emerging Trends:** Cyber laws and regulations related to disasters, Role of government agencies and CERTs, Compliance standards (ISO 22301, ISO 27001 – overview), Cyber insurance and risk transfer, Case studies of major cyber disasters, Emerging trends: AI in cyber resilience, Zero Trust, cloud DR	6	10%

Course Outcome:

CO1: Identify and classify various types of cyber disasters

CO2: Analyse cyber risk, impact, and vulnerability scenarios

CO3: Design cyber disaster recovery and incident response plans

CO4: Implement business continuity and resilience strategies

CO5: Evaluate legal, regulatory, and governance aspects of cyber disasters

List of Textbooks:

1. Harold F. Tipton, Information Security Management Handbook
2. Gregory White et al., Cybersecurity and Cyberwar
3. Snedaker, Business Continuity and Disaster Recovery Planning for IT Professionals

List of References:

1. NIST Special Publications (SP 800-34, SP 800-61)
2. ISO 22301: Business Continuity Management Systems
3. ENISA Cyber Crisis Management Guidelines

Subject Code: 11380217	Advanced Cyber-Physical Systems & Security
Pre-requisite: Computer Networks, Operating Systems, Information Security, Basics of Cyber Laws.	

Course Objective:

1. To provide advanced knowledge of Cyber-Physical Systems (CPS) architecture and design principles.
2. To understand the integration of computation, networking, and physical processes in CPS.
3. To study security threats, vulnerabilities, and protection mechanisms in CPS environments.
4. To analyze secure communication and control mechanisms for IoT-based CPS.
5. To explore real-world applications of CPS in smart grids, healthcare, transportation, and industrial systems.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	1	0	4	60	40	0	0	100

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Introduction to Cyber-Physical Systems**: Concept and characteristics of CPS, evolution of embedded and cyber-physical systems, architecture and components of CPS, interaction between cyber and physical components, sensors and actuators, CPS design principles, CPS vs IoT systems, applications of CPS in modern infrastructure.	04	12
2	**Modeling and Design of CPS**: System modeling techniques, hybrid systems modeling, discrete and continuous dynamics, real-time systems in CPS, control theory fundamentals, feedback systems, CPS design methodologies, middleware and system integration techniques.	06	15
3	**Communication and Networking in CPS**: Wireless sensor networks, IoT communication protocols (MQTT, CoAP, Zigbee), real-time communication constraints, time synchronization, data acquisition and processing, distributed control systems, edge and fog computing in CPS environments.	08	20

4	**Communication and Networking in CPS**: Wireless sensor networks, IoT communication protocols (MQTT, CoAP, Zigbee), real-time communication constraints, time synchronization, data acquisition and processing, distributed control systems, edge and fog computing in CPS environments.	08	20
5	**Applications and Case Studies of CPS Security**: Smart grid security, industrial control systems (ICS) and SCADA security, autonomous vehicles and transportation systems, healthcare CPS and medical devices, smart cities and IoT infrastructure, resilience and fault tolerance in CPS, emerging research challenges in CPS security.	08	33

Course Outcome:

1. CO1: Understand the architecture and design principles of Cyber-Physical Systems.
2. CO2: Model and analyze CPS integrating computational and physical components.
3. CO3: Design communication and networking mechanisms for CPS environments.
4. CO4: Identify security threats and implement protection mechanisms in CPS.
5. CO5: Analyze real-world CPS applications such as smart grids, healthcare, and industrial systems

List of Textbooks:

1. Rajeev Alur, Principles of Cyber-Physical Systems, MIT Press.
2. Edward A. Lee & Sanjit A. Seshia, Introduction to Embedded Systems: A Cyber-Physical Systems Approach, MIT Press.

List of Reference Books:

1. Houbing Song, Danda Rawat, Sabina Jeschke, Christian Brecher, Cyber-Physical Systems: Foundations, Principles and Applications, Academic Press.
2. Al-Sakib Khan Pathan, Security of Cyber-Physical Systems, CRC Press.
3. Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Crown Publishing.

Subject Code: 11380218	Enterprise Security Architecture
Pre-requisite: Basic knowledge of Computer Networks, Operating Systems, and Fundamentals of Information Security.	

Course Objective:

1. To understand security challenges in modern enterprise environments
2. To learn enterprise-wide security architecture principles and frameworks
3. To design secure infrastructure, application, and data architectures
4. To gain exposure to governance, risk, compliance, and incident response
5. To prepare students for security architect and GRC-related roles

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
3	1	0	4	60	40	0	0	100

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Introduction to Enterprise Security Architecture:** Enterprise Environment Overview. Security Challenges in Large Organizations. CIA Triad and Extended Security Principles. Threats, Vulnerabilities, and Risk Concepts. Role of Enterprise Security Architect. Business Alignment with Security Architecture.	06	12
2	**Security Architecture Frameworks & Standards** Security Architecture Concepts. TOGAF Security Architecture (High-level). SABSA Framework (Conceptual). NIST Cybersecurity Framework. ISO/IEC 27001 Overview. Layered Security Architecture (Business, Application, Data, Technology)	08	16
3	**Enterprise Infrastructure & Network Security Architecture:** Network Security Design. Firewalls, IDS/IPS, VPNs. Secure Network Segmentation and DMZ. Endpoint Security and Patch Management. Identity and Access Management (IAM). Authentication, Authorization, MFA. Zero Trust Model (Introductory).	10	24

4	**Application, Data & Cloud Security Architecture:** Secure Application Architecture. Secure SDLC Overview. Common Enterprise Application Threats. Data Security Architecture: Encryption, Data Classification, Access Control. Cloud Security Architecture. Shared Responsibility Model. Basics of Virtualization and Container Security.	10	24
5	**Governance, Risk, Compliance & Incident Management: Risk Assessment** and Risk Treatment. Security Policies, Standards, and Procedures. Governance, Risk and Compliance (GRC). Regulatory Compliance Overview (GDPR, HIPAA, PCI-DSS). Security Audits and Assessments. Incident Response Lifecycle. Business Continuity and Disaster Recovery (BCP/DR)	08	24

Course Outcome:

1. CO1: Explain enterprise security concepts, threats, and architectural needs
2. CO2: Understand and apply standard security architecture frameworks
3. CO3: Design basic enterprise infrastructure and network security architectures
4. CO4: Analyze application, data, and cloud security requirements
5. CO5: Apply risk management, governance, and incident response principles

List of Textbooks

1. Sherwood, Clark & Lynas – Enterprise Security Architecture
2. Ross Anderson – Security Engineering
3. *NIST Special Publications (800 Series – Selected)

List of Reference Books

1. ISO/IEC 27001 Standard Documentation
2. TOGAF Documentation (Security Architecture Section)
3. William Stallings – Network Security Essentials

Semester 3

Subject Code: 11380301	Internal Review I

Course Objective:

1. To guide students in finalizing the research problem and scope.
2. To assess the quality of literature review and research gap identification.
3. To ensure the research methodology is clearly defined.
4. To provide constructive feedback before proceeding to Dissertation Phase–I implementation.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
0	0	4	2	0	0	0	100	100

Internal Review – I ,is conducted before the formal submission of Dissertation Phase–I. The review is carried out by the faculty guide/supervisor to monitor the early-stage research progress.

Students are required to present:

- Proposed research topic in Cyber Security
- Problem statement
- Literature review
- Research gap identification
- Objectives of the research
- Proposed methodology or framework
- Expected outcomes

The guide evaluates the **research feasibility, technical depth, and relevance** of the selected topic.

Review Components

Students must submit and present:

- Topic approval document
- Literature survey summary
- Research problem formulation
- Proposed methodology
- Preliminary research plan
- Timeline for Dissertation Phase–I

Subject Code: 11380302	Dissertation Phase I
Pre-requisite: Network Security, Cryptography, Ethical Hacking, Secure Programming, Cyber Law, Research Methodology, or related Cyber Security courses.	

Course Objective:

1. To enable students to identify a research problem in Cyber Security and Information Security domains.
2. To develop skills in literature survey, vulnerability analysis, and security research methodologies.
3. To analyze existing cyber security frameworks, tools, and defense mechanisms.
4. To design novel security solutions, threat detection systems, or protection mechanisms.
5. To prepare students for independent research in cyber security technologies and applications.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
0	0	28	14	0	0	100	0	100

Course Description

In this phase of dissertation work, students must select a research topic in Cyber Security or related interdisciplinary areas.

Possible research domains include:

- Network Security and Intrusion Detection Systems (IDS/IPS)
- Cryptography and Secure Communication
- Malware Analysis and Detection
- Ethical Hacking and Penetration Testing
- Blockchain Security
- Cloud Security
- Internet of Things (IoT) Security
- Digital Forensics
- Cyber Threat Intelligence
- AI/ML for Cyber Security
- Web Application Security
- Mobile Security
- Privacy Preservation and Data Protection

Students will work under the supervision of a faculty guide and conduct a detailed literature review to identify research gaps and define the problem statement.

The work in Phase-I should include:

- Selection of research topic
- Literature review and related work analysis
- Identification of security vulnerabilities or research gaps
- Problem formulation
- Design of proposed methodology or security model
- Initial experimental setup or simulation (if applicable)

Students are required to present their research proposal through seminars and review meetings conducted by the department.

Progress Report (Submission Requirements)

Students must submit a progress report (3–5 pages) including:

- Research problem statement
- Literature review and related work
- Identified security challenges or vulnerabilities
- Research objectives
- Proposed methodology or framework
- Expected outcomes

Students must present their work before the departmental review committee.

Assessment Components

Evaluation will be based on:

- Research problem relevance to cyber security
- Quality of literature survey
- Identification of security gaps
- Proposed methodology
- Seminar presentation
- Progress report documentation

Semester 4

Subject Code: 11380401	Internal Review II

Course Objective:

1. To evaluate the implementation progress of the dissertation work.
2. To assess experimental setup, security analysis, and preliminary results.
3. To guide improvements in methodology and experimentation.
4. To ensure readiness for final Dissertation Phase–II submission.
5. To improve research documentation and presentation quality.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
0	0	4	2	0	0	0	100	100

Course Description

Internal Review – II is conducted after completion of Dissertation Phase–I and before Dissertation Phase–II submission.

This review evaluates the progress of implementation, experiments, and initial results.

The review is conducted by the research guide/supervisor to ensure that the student is progressing toward the successful completion of the dissertation.

Students must present:

- Implementation progress
- System architecture or model design
- Experimental setup
- Preliminary results
- Security evaluation or performance analysis
- Planned improvements and future work

Review Components

- Implementation status report
- Experimental setup and methodology
- Preliminary results and analysis
- Challenges faced and solutions
- Plan for final dissertation completion

Subject Code: 11380402	Dissertation Phase II
Pre-requisite: Successful completion of Dissertation Phase-I	

Course Objective:

1. To implement the cyber security solution or model proposed in Phase-I.
2. To perform experiments, vulnerability testing, and security validation.
3. To analyze the effectiveness of the proposed solution against existing cyber threats.
4. To prepare a technical dissertation report.
5. To develop skills for research presentation and defense.

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
0	0	28	14	0	0	100	0	100

Course Description

In Phase-II, students will implement and validate the cyber security solution proposed in Phase-I. This phase focuses on experimentation, evaluation, and documentation.

The dissertation work may include:

- Development of cyber security algorithms or tools
- Implementation of intrusion detection or prevention systems
- Malware analysis frameworks
- Cryptographic system design
- Secure communication protocols
- Penetration testing tools
- Security monitoring systems
- Digital forensic analysis frameworks

Students must evaluate their solution using security metrics such as detection accuracy, attack resistance, latency, encryption strength, or system performance.

Finally, students must prepare a complete dissertation thesis and present their research work through a seminar and viva-voce examination.

Dissertation Report Structure

The final thesis should include:

- Introduction
- Literature Review

- Problem Statement and Research Gap
- Proposed Methodology / Model
- Implementation and Experimental Setup
- Results and Analysis
- Comparison with Existing Methods
- Conclusion and Future Work
- References

Assessment Components

Evaluation will be based on:

- Technical implementation
- Experimental validation and security analysis
- Quality of dissertation report
- Research contribution to cyber security
- Seminar presentation and viva-voce

ANNEXURE III
Industry & Employer Survey Analysis

Sample Size	Survey Period	Region	Framework
25 Organizations	**February – April 2026**	**Gujarat / Pan-India**	**NEP 2020 / UGC 2024**

1. Executive Summary

A structured industry validation survey was conducted among 25 senior technology leaders, HR professionals, and security managers across IT, BFSI, manufacturing, healthcare, and public-sector organizations in Gujarat and pan-India to assess the demand for formally trained M.Tech. graduates in Cyber Security Engineering and to validate the need for the proposed programme at the University.[1]

The findings are unambiguous and strongly positive. India faces a structural cyber security talent deficit of exceptional severity. The industry projects 3.5 million unfilled cybersecurity positions globally by 2025, with India's demand alone expected to reach one million professionals — yet the country currently musters only approximately 80,000 fully qualified experts, creating a more than 90% supply gap.[2] The India cybersecurity market, valued at USD 11.3 billion in 2025, is projected to reach USD 44.0 billion by 2034, growing at a CAGR of 15.46% — one of the fastest rates in the entire technology sector.[3]

Simultaneously, India's Digital Personal Data Protection (DPDP) Act, 2023 — with DPDP Rules notified on 13 November 2025 — has elevated cybersecurity from an IT obligation to a statutory, board-level enterprise responsibility carrying penalties of up to ₹250 crore for non-compliance.[4] This regulatory inflection is generating urgent demand for compliance-literate cybersecurity engineers across BFSI, healthtech, fintech, and public-sector organizations, precisely the domain competency the University's proposed M.Tech. Cyber Security Engineering programme will deliver.

Every survey respondent confirmed a significant talent gap in the current market. Twenty-two out of twenty-five organizations expressed willingness to recruit graduates from a formally structured university M.Tech. programme aligned with UGC's Curriculum and Credit Framework for PG Programmes (June 2024) and NEP 2020. Twenty organizations expressed interest in participating as industry partners. The survey validates the University's decision to launch this programme and provides strong industry backing for an immediate start.[5]

Confirm critical cyber security talent gap in current market	**100%**
Would actively recruit M.Tech. graduates	**88%**

Open to formal industry partnership with the University	**80%**
Average rating — recommend programme launch	**4.5 / 5**
Overall recommendation score (launch now / with adjustments)	**96%**

2. Regulatory and Policy Framework

The proposed M.Tech. in Cyber Security Engineering is designed in full conformity with applicable national regulatory instruments. The University Grants Commission (UGC), as the statutory body set up by the Ministry of Education, Government of India, is responsible for maintaining the standards of Higher Education in India, and UGC approval is mandatory for degree validity.[6] AICTE approval is additionally mandatory for all technical engineering programmes and is responsible for the planning and development of technical as well as management education in India.[7]

In June 2024, the UGC released its Curriculum and Credit Framework for Post-graduate Programmes under NEP 2020, which provides for flexible one-year and two-year PG programme structures, exit provisions at the end of Year 1, multi-disciplinary elective baskets, and creditization of work experience under the National Credit Framework (NCrF).[8]

NEP 2020 explicitly mandates that universities should focus on postgraduate programmes in cybersecurity as a critical component of India's digital security infrastructure. The DPDP Act 2023 and the DPDP Rules 2025 have further transformed this regulatory environment, requiring organizations across sectors to appoint Data Protection Officers, conduct Data Protection Impact Assessments, implement 72-hour breach-notification SOCs, and maintain ISO 27001-aligned security controls — creating a massive, immediate demand for formally trained, compliance-literate cybersecurity engineers.[4][9]

For M.Tech. eligibility, candidates who have completed a 4-year undergraduate programme or a 3-year undergraduate programme and a 2-year PG programme in STEM subjects are eligible for admission to M.E./M.Tech. in allied areas.[10] The University's proposed programme mirrors IIT Roorkee's best-practice basket-based PG curriculum structure — including Programme Core Courses (PCC), Programme Elective Courses (PEC), Social Sciences Courses (SSC), and mandatory Industrial Internship/Social Activity (ISA) — to ensure national comparability.[11]

3. Respondent Profile

The 25 respondents were drawn from technology-intensive organizations across five sectors — Information Technology & Software, Banking, Financial Services & Insurance (BFSI), Manufacturing

& Industry 4.0, Healthcare & Life Sciences, and Public Sector & Smart City initiatives — spanning Ahmedabad, Gandhinagar, Surat, and national tech hubs (Bengaluru, Pune, Hyderabad). Respondent designations included Chief Technology Officers, Heads of AI/ML, Senior Engineering Managers, HR & Talent Acquisition Heads, and R&D Directors, ensuring responses reflect both technical requirements and strategic hiring decisions.

Sector	No. of Respondents	% of Sample
Information Technology & Software	10	40%
Banking, Financial Services & Insurance (BFSI)	5	20%
Manufacturing & Industry 4.0	4	16%
Healthcare & Life Sciences	3	12%
Public Sector / Smart City / E-Governance / Research	3	12%

4. Findings — Q1: AI/ML Talent Gap in Fresh Graduates

Respondents were asked to identify the biggest knowledge gaps they observe when hiring fresh engineering graduates for cyber security roles. Multiple selections were permitted. The responses reveal a consistent and severe pattern. India currently has a demand of approximately one million cybersecurity professionals but has only around 80,000 fully qualified experts — a supply gap exceeding 90%.[2] A 30–50% shortfall of qualified cybersecurity professionals exists even in specialized areas such as cloud security, zero-trust architecture, and AI-driven threat detection.[12]

The demand for cybersecurity professionals in India is projected to grow by 30–35% through 2025–26, with the BFSI sector experiencing the most acute pressure as RBI and SEBI tighten cybersecurity compliance frameworks and the DPDP Act mandates enterprise-wide breach management capabilities.[13] Furthermore, 93% of Indian organizations are increasing their cybersecurity budgets, with 17% planning increases of 15% or more — directly translating into accelerating demand for trained security engineers.[2]

Knowledge Gap Identified	Respondents	Percentage
No hands-on SOC / SIEM / incident response experience	25/25	100%
No cloud security skills (AWS / GCP / Azure Security)	24/25	96%
No network security / penetration testing capability	23/25	92%

Knowledge Gap Identified	Respondents	Percentage
Cannot work with real-world threat intelligence data	22/25	88%
No DPDP / GDPR / compliance & governance literacy	21/25	84%
No applied cryptography / PKI / zero-trust skills	20/25	80%
No malware analysis / digital forensics skills	19/25	76%
Weak understanding of secure SDLC / DevSecOps	18/25	72%
Poor research / documentation / report-writing ability	14/25	56%
No domain knowledge (BFSI / Healthcare / ICS-SCADA)	12/25	48%

Selected Employer Comments — Talent Gap

> "We spend 10–14 weeks onboarding every fresh hire into our SOC before they can handle a live alert independently. An M.Tech. that delivers SIEM-proficient, incident-response-ready graduates from Day 1 would eliminate that cost entirely."
>
> **— Industry Survey Respondent, Ahmedabad IT Sector**

> "The DPDP Act and CERT-In directives now require us to report breaches within 6–72 hours. We cannot find graduates who understand both the technical pipeline and the legal compliance framework simultaneously. That dual literacy is exactly what the market needs."
>
> **— Industry Survey Respondent, BFSI Sector**

> "Cloud-native attacks and AI-assisted threats are now our daily production reality, not theoretical risks. We need engineers who can architect zero-trust environments, run VAPT cycles, and manage security compliance. None of the graduates we interview are equipped without months of additional training."
>
> **— Industry Survey Respondent, Technology Sector**

5. Findings — Q2: MLOps & Production AI Readiness

Respondents were asked how their need for SOC-literate and cloud-security-ready professionals has changed since 2022 and whether they are finding enough qualified professionals in the Gujarat and national market. The responses confirm a structural shortage that has worsened significantly as enterprise cloud migration, the proliferation of UPI-scale digital payment systems, and the DPDP regulatory framework have collectively elevated cybersecurity to a board-level strategic priority.[4][13]

How has demand for MLOps-literate staff changed since 2022?	Count	%
Significantly increased	19	76%
Moderately increased	4	16%
No change	2	8%
Decreased	0	0%

Are you finding enough qualified AI/ML professionals?	Count	%
No — serious shortage at production-ready level	20	80%
Partially — some available but require extensive upskilling	4	16%
Yes — enough supply	1	4%

6. Findings — Q3: Most Valued Curriculum Subject Areas

Respondents were asked which subject areas they feel would most benefit their cyber security engineering teams and which they would most value in M.Tech. graduates. This question was structured to directly inform curriculum design under the UGC PG Credit Framework 2024. The results directly support the University's proposed four-semester curriculum structure distributing core and elective credits across foundational cyber security, applied domains, research methodology, and thesis work.[8][14]

Subject Area / Curriculum Module	Respondents	Percentage
Network Security, Firewalls & Intrusion Detection/Prevention	25/25	100%
SOC Operations, SIEM & Incident Response	24/25	96%
Cloud Security (AWS / GCP / Azure Security Speciality)	23/25	92%
Penetration Testing, Ethical Hacking & Vulnerability Assessment	22/25	88%
Data Privacy, DPDP / GDPR & Regulatory Compliance	21/25	84%

Subject Area / Curriculum Module	Respondents	Percentage
Cryptography, PKI & Zero-Trust Architecture	20/25	80%
Malware Analysis, Reverse Engineering & Digital Forensics	19/25	76%
AI/ML for Threat Detection & Security Analytics	18/25	72%
DevSecOps, Secure SDLC & Application Security	16/25	64%
Domain-specific Security (BFSI / Healthcare / ICS-SCADA / IoT)	15/25	60%
Research Methods & Technical Report / Policy Writing	12/25	48%

7. Findings — Q4: Recruitment Intent

This is the most strategically important finding of the survey. Respondents were asked to rate their likelihood of actively recruiting from a University M.Tech. programme producing graduates trained in production AI/ML engineering, LLM development, MLOps, responsible AI, and applied domain AI. This reflects the market reality described by industry data: average salaries for AI engineers have nearly doubled due to strong demand and a persistent talent shortage, with demand rising 40% year-on-year while supply lags significantly.[16][17]

Rating	Developers	Percentage	Interpretation
5 — Definitely would recruit	14	56%	High intent
4 — Likely to recruit	8	32%	Positive intent
3 — Possibly would recruit	3	12%	Neutral
2 — Unlikely	0	0%	—
1 — Definitely would not	0	0%	—
Average Rating	4.4 / 5.0		Strong positive

Specific roles for which organizations would most actively hire M.Tech. CS graduates:

Target Role	Respondents	Percentage
Security Operations Centre (SOC) Engineer / Analyst	24/25	96%
Cloud Security Engineer / Architect	23/25	92%
Penetration Tester / Vulnerability Assessment Engineer	22/25	88%
Cyber Security Research & Development Engineer	21/25	84%
Data Privacy & DPDP Compliance Analyst	20/25	80%

Target Role	Respondents	Percentage
Digital Forensics & Incident Response (DFIR) Specialist	18/25	72%
DevSecOps / Application Security Engineer	16/25	64%
AI Security / Threat Intelligence Analyst	14/25	56%

8. Findings — Q5: Industry Partnership Interest

Respondents were asked whether they would engage formally with the University as industry partners covering guest faculty, lab sessions, internships, capstone project panels, recruitment letters of intent, and curriculum advisory input. The enthusiasm for partnership reflects the sector's recognition that academia-industry collaboration is essential to closing the AI talent gap identified by NASSCOM and the World Economic Forum.[18]

Partnership Engagement Mode	Respondents	Percentage
Guest faculty / expert lecture sessions	23/25	92%
Industry project / capstone problem host	22/25	88%
Internship provider (6-month structured internship)	21/25	84%
Capstone pitch panelist & industry evaluator	20/25	80%
Letter of Intent for recruitment	18/25	72%
Curriculum advisory board membership	16/25	64%
Cyber security lab / hardware / cloud resource sharing	12/25	48%
Co-branding / sponsorship of student security competitions (CTF)	10/25	40%

Selected Partner Quotes — Industry Partnership

> "We are happy to provide live VAPT engagements and SOC case studies as capstone problem statements. Real-world adversarial scenarios and real compliance constraints are exactly what thesis projects should be built on."
>
> **— Industry Survey Respondent, BFSI Sector**

> "If M.Tech. students work on live cloud security configurations and incident response playbooks during internship, they understand what mean-time-to-detect, DPDP breach

> timelines, and CERT-In reporting actually mean in practice. We can absorb 3–4 interns per year from a structured programme."
>
> **— Industry Survey Respondent, Ahmedabad IT Sector**

> "A formal Letter of Intent from our organization is the minimum we can commit. If the programme delivers research-intensive graduates with real SOC and cloud security exposure, we want to be associated from Batch 1."
>
> **— Industry Survey Respondent, Technology Sector**

9. Overall Programme Recommendation Rating

Respondents were asked to rate overall whether they would recommend that the University proceed with launching the M.Tech. in Cyber Security Engineering programme.

Overall Rating	Count	%	Meaning
5 — Strongly recommend launching now	15	60%	Launch immediately
4 — Recommend with minor conditions	9	36%	Launch with adjustments
3 — Neutral / more information needed	1	4%	Cautious
2 — Do not recommend	0	0%	—
1 — Strongly against	0	0%	—
Average Rating	4.6 / 5.0		

10. Conclusions & Recommendations

The industry validation survey of 25 organizations produces five clear and actionable conclusions:

01 The talent gap is real, acute, and universally confirmed.

Every organization surveyed identified one or more critical knowledge gaps in fresh graduates. SOC/incident-response readiness, cloud security engineering, and DPDP/compliance literacy are the top three deficiencies. India's cybersecurity workforce gap exceeds 90% of stated demand — the second-largest national gap in the world after China. The University's proposed curriculum directly addresses all three primary deficiencies.[2][12]

02 The market is ready to recruit from the programme immediately.

An average recruitment intent score of 4.4 out of 5.0 with 88% of organizations rating 4 or 5 means the placement pipeline for the first batch is already being built before the programme launches. Cybersecurity demand is growing at 30–35% per annum and average salaries are rising 10–15% year-on-year — creating an exceptional graduate outcome environment.[13][15]

03 SOC operations and cloud security are the two most valued subject areas.

100% and 96% of respondents respectively identified network/SOC operations and cloud security as the most critical curriculum areas. This validates the University's decision to embed production security operations, cloud architecture, and regulatory compliance across Semesters I through III rather than treating them as standalone electives.[8][14]

04 The industry partnership interest is exceptional.

84% of organizations are open to internship provision, 72% are ready to issue Letters of Intent for recruitment, and 64% are willing to serve on the curriculum advisory board. This is the credibility infrastructure the programme needs to launch with authority and to ensure the 6-month industry internship embedded in Semester III is operationalized from Day 1.[17]

05 The overall recommendation is to proceed without delay.

96% of respondents gave a rating of 4 or 5, recommending that the University launch the programme. A 4.6 out of 5.0 average recommendation score represents one of the strongest industry validation signals a new academic programme can receive. NEP 2020 and the UGC PG Framework 2024 provide complete regulatory authorization. The DPDP Act, CERT-In directives, India's USD 11.3 billion cybersecurity market, and confirmed employer commitment all point to an immediate launch.[3][4][8]

11. References & Citations

All citations embedded in the body of this Annexure correspond to the following authoritative sources. These references were verified as of April 2026 and are provided to substantiate the market demand analysis, regulatory compliance positioning, and curriculum validation findings presented herein.

[1] Structured Industry Validation Survey — M.Tech. Cyber Security Engineering, University (Internal Document), February–April 2026. Survey administered to 25 senior technology leaders across Gujarat and pan-India.

[2] Taggd. "Cybersecurity Jobs in India: Top Roles, Skills, Salaries, Hiring Challenges." March 2026. India's demand for 1 million professionals vs. 80,000 qualified experts; 93% of Indian companies increasing cybersecurity budgets. Available at: https://taggd.in/blogs/cybersecurity-jobs-in-india/

[3] IMARC Group / GlobalRiskCommunity. "India Cybersecurity Industry Outlook 2026–2034." Market valued at USD 11.3 billion in 2025; projected USD 44.0 billion by 2034 at CAGR 15.46%.

Available at: https://globalriskcommunity.com/profiles/blogs/india-cybersecurity-industry-outlook-2026-2034-market-size-growth

[4] SISA InfoSec / EY India. “Data Protection and Privacy Acts in India: A 2026 Compliance Guide.” DPDP Act 2023 operational; DPDP Rules notified 13 November 2025; penalties up to ₹250 crore for non-compliance. Available at: https://www.sisainfosec.com/blogs/data-protection-and-privacy-laws-in-india-2025/

[5] Structured Industry Validation Survey — M.Tech. Cyber Security Engineering (Internal Document), February–April 2026. Recruitment intent and partnership findings.

[6] StudyRiserr. UGC approval for M.Tech. Cyber Security programmes — statutory requirement for degree validity in India (2025). Available at: https://studyriserr.com

[7] AICTE (All India Council for Technical Education). Approval requirements for technical and management education programmes in India. Available at: https://www.aicte-india.org/

[8] UGC. Curriculum and Credit Framework for Post-graduate Programmes (June 2024). University Grants Commission, Ministry of Education, Government of India. Flexible one-year and two-year PG structures, exit provisions, NCrF creditization. Available at: https://www.ugc.gov.in/pdfnews/4682468_Curriculum-and-Credit-Framework-for-Postgraduate-Programmes.pdf

[9] KS&DK Law. “DPDP Rule 6 and India’s New Cybersecurity Compliance Standard.” November 2025. DPDP Act elevates cybersecurity to board-level statutory responsibility; Rule 6 mandates operational security architecture. Available at: https://ksandk.com/data-protection-and-data-privacy/dpdp-rule-6-and-indias-new-cybersecurity-compliance-standard/

[10] UGC. Curriculum and Credit Framework for Post-graduate Programmes (June 2024), p. 8. Eligibility criteria for M.E./M.Tech. programmes under NEP 2020. Available at: https://www.ugc.gov.in/pdfnews/4682468_Curriculum-and-Credit-Framework-for-Postgraduate-Programmes.pdf

[11] Careers360. “IIT Roorkee revises its postgraduate, MTech curriculum, introduces courses on AI and ML.” March 11, 2024. Flexible basket-based PCC, PEC, SSC, STAR, ISA structure aligned with NEP 2020. Available at: https://news.careers360.com/iit-roorkee-revises-its-postgraduate-mtech-curriculum-introduces-courses-on-ai-and-ml

[12] IPSR / KEYS Inc. “Cybersecurity Talent Shortage 2025.” 30–50% shortfall of qualified cybersecurity professionals in specialized domains; global cybersecurity market reaching $300 billion by 2026. Available at: https://keyssinc.com/surge-in-demand-for-cybersecurity-talent-in-india-why-the-skills-gap-is-widening-in-2025/

[13] WhatIsTheSalary.com. “Cyber Security Salary in India 2026.” Demand for cybersecurity professionals projected to grow 30–35% in 2025–26; DPDP Act driving salary and demand growth. Available at: https://whatisthesalary.com/it-salaries/cyber-security-salary-in-india/

[14] Pondicherry University. M.Tech. Data Science & Artificial Intelligence — Regulations, Curriculum & Syllabus in compliance with UGC Curriculum and Credit Framework for PG Programmes, June 2024 (under NEP 2020). Effective 2025–2026. Available at: https://www.pondiuni.edu.in

[15] GeeksforGeeks / Amity Online. "Cyber Security Salary in India 2026." Average salary ₹10 LPA; range ₹4–15 LPA; top earners ₹30–50 LPA; certified professionals earn 30–50% more than non-certified peers. Available at: https://www.geeksforgeeks.org/gfg-academy/cyber-security-salary/ and https://amityonline.com/blog/cybersecurity-salary-in-india

[16] Networkers Home. "Cybersecurity Salary India by Experience Level 2026." Entry-level ₹3.5–7 LPA; mid-level ₹8–18 LPA; senior/specialized ₹25–45 LPA+; 10–15% annual salary growth projected. Available at: https://www.networkershome.com/cybersecurity-salary-india-by-experience-2026/

[17] Programs.com. "Cybersecurity Talent & Workforce Shortage Stats (2026)." Asia-Pacific workforce gap of 3.4 million (up from 2.7 million YoY); India has over 1 million cybersecurity vacancies — second-largest gap globally. Available at: https://programs.com/resources/cybersecurity-talent-shortage-stats/