BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(An Autonomous institution affiliated to VTU, Belagavi)
Doddaballapur Main Road, Avalahalli, Yelahanka, Bengaluru 560064

M.Tech - Cyber Security

Scheme and Syllabus

2022 Scheme

Revised Version: 2.0
Revised Year: 2024

Institute Vision

To emerge as one of the finest technical institutions of higher learning, to develop engineering professionals who are technically competent, ethical and environment friendly for betterment of the society.

Institute Mission

Accomplish stimulating learning environment through high quality academic instruction, innovation and industry-institute interface.

Department of Information Science and Engineering

VISION

Emerge as center of learning in the field of Information Science & Engineering with technical competency to serve the society.

MISSION

To provide excellent learning environment through balanced curriculum, best teaching methods, innovation, mentoring and industry institute interaction.

M.Tech in Cyber Security

Program Educational Objectives (PEOs)

PEO1 Apply analytical thinking to solve problems through research and development in the areas of Cyber Security and allied engineering domains.

PEO2 Adapt to changing technological trends through life-long learning by exhibiting professional ethics, integrity and career growth.

PEO3 Develop skills to facilitate in providing sustainable solutions by addressing the ever-growing challenges of the cyberspace in society.

Program Outcomes (POs)

PO1 Independently carry out research and development work to solve practical problems related to Cyber Security and allied engineering domains.

PO2 Write and present a substantial technical report/document.

PO3 Demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program.

PO4 Analyze the acquired domain knowledge for providing feasible security solution(s).

PO5 Relate the learning outcomes to build requisite competency in professional environment.

PO6 Appraise the need for engaging in lifelong learning.

About the Department

The Department of Information Science and Engineering started in the Year 2010 with an approved intake of 60 and enhanced to 120 from the academic year 2018-19 and to 180 from the academic year 2019-20. Currently the Department Intake is 240 from the academic Year 2023-24. The Department has qualified and professionally dedicated faculty member practice OBE in the academic deliverables. The faculties have published research articles in various National, International, IEEE Conferences, and Journals.

The department has modern laboratories to serve the teaching and research needs of the students as well as faculty members. The Department has been organizing conferences, workshops, expert lectures, and student-centric activities to encourage students and faculty to instill lifelong learning. Few of our students are working for consultancy projects along with a few faculty members. The staffs are encouraged to attend the 10 days internship to bridge the gap between the academics and industry. The department has an admirable research ambiance.

About M.Tech in Cyber Security

M.Tech (Cyber Security) commenced in the year 2022 with an intake of 18 students. The Post Graduate Program in Cyber Security is an affiliated program offered by Visvesvaraya Technological University (VTU), Belagavi. The autonomous curriculum is designed by team of experts in the cyber security domain. Highly experienced faculty members with doctoral degrees handle the courses for this program.

Faculty members are proactively involved in high end research activities and have published impetus research publications in domains of Cyber Forensics, Network Security, AI and Data Science in Security (Cognitive). Students undergo six weeks industrial internship in many reputed companies.

PREAMBLE

In keeping abreast with India's recent National Education Policy (NEP 2020), the Indian Institute of Science, Bengaluru, has designed the Master of Technology (Online) degree program, for practicing engineers and scientists. Towards the attainment of such a holistic and multidisciplinary education, the flexible and innovative curriculum has been provided at BMSIT&M with credit-based courses and projects/internships/special courses in the areas of community engagement and public service, environmental education, and value-based education.

The emphasis is more on the core competency in the curriculum of the program to enhance opportunities for placement through industry relevant courses as program core and program electives. This is effectively attained with proper design, operation and improvement in academic components in the system with inclusive focus on Modern teaching methods, advanced curricula, innovative assessment methods, research temperament, industry associated curriculum. Implementation of academic autonomy can is with supportive governance and administrative structure is properly planned and put in place.

Curricular inputs for the framework are from all the stakeholders involved in the academic process and referring curriculum from standard and well-known universities/colleges. Input for the framework is also from professional bodies like IEEE and CSI which recommends the advanced courses for the PG program of 2 years. The expected learning outcomes of autonomous curriculum of BMSIT&M cater to the aspiration of learner in-terms of higher education, research, industry requirements. Develop learner's inquisitiveness and focus on research and development of disruptive technologies. Incorporation of ICT tools imperatively blended in the autonomous curricula reaching all class of learners.

With this preamble, the curriculam for the autonomous BMSIT&M has been

designed to meet the contemporary needs (aspirations) of primary stake holders (students) with the following.

Salient features

1. **Inclusion of NEP 2020:** The aspiration of NEP 2020 and various levels has been incorporated in the M.Tech Computer Science Engineering (Autonomous) with inclusive focus on practical work, industrial internship, emphasis on research to solve the societal issues and latest trends as courses.
2. **Induction Programme:** There will be a week-long induction program for the PG students entering the institution. The incumbents learn about the institutional policies, processes, practices, culture and values.
3. **Post Graduate Program Outcomes (PO) Based Curriculum:** The curricula for the program is designed to meet the post graduate attributes (Program Outcomes) defined by National Board of Accreditation which are based on the knowledge, research, skill, ethics and higher learning.
4. **Emphasis on Research Project Based Learning:** To impart the skills to the prospective researcher, the emphasis on practical sessions is extended in the curricula for all the programs. At each semester, the adequate number of practical/laboratory courses are included. Further, some of the theory courses are blended with practical as integrated course.
5. **Industry exposure through Lab work, Mini projects and Internships:** The curricula include industry internships and mini projects for the students to expose them to the real-world experience at industrial environment. Mini projects expose to better technical articulation and project cycles.
6. **Self-Learning:** The curriculum provides with an opportunity for the students to take the initiative, with or without the assistance of others,

in diagnosing their learning needs, formulating learning goals, identifying human and material resources for learning, and evaluating learning outcomes.

7. **Multiple avenues based on aspirations of the students**: The students will study the program specific courses for two years. There are three major avenues for the aspiring students to pursue:

    - **Industry/Placement:** The students who are aspiring to work as professional engineers in their core industrial domain have the option of studying the courses in the curriculum which are aligned towards the placement opportunities.
    - **Research:** The curriculum provides an opportunity for the students to pursue the courses which are in support of higher learning enabling the learner to do research work in the desired domain of interest.
    - **Presentation and Articulation:** The curriculum provides opportunities to present flexible assessment method for the course which improves communication and expect document this as report.
    - **Industry Certification Program:** The curriculum provides an opportunity to pursue a certification program in cyber security enabling high level industrial practices in the domain.

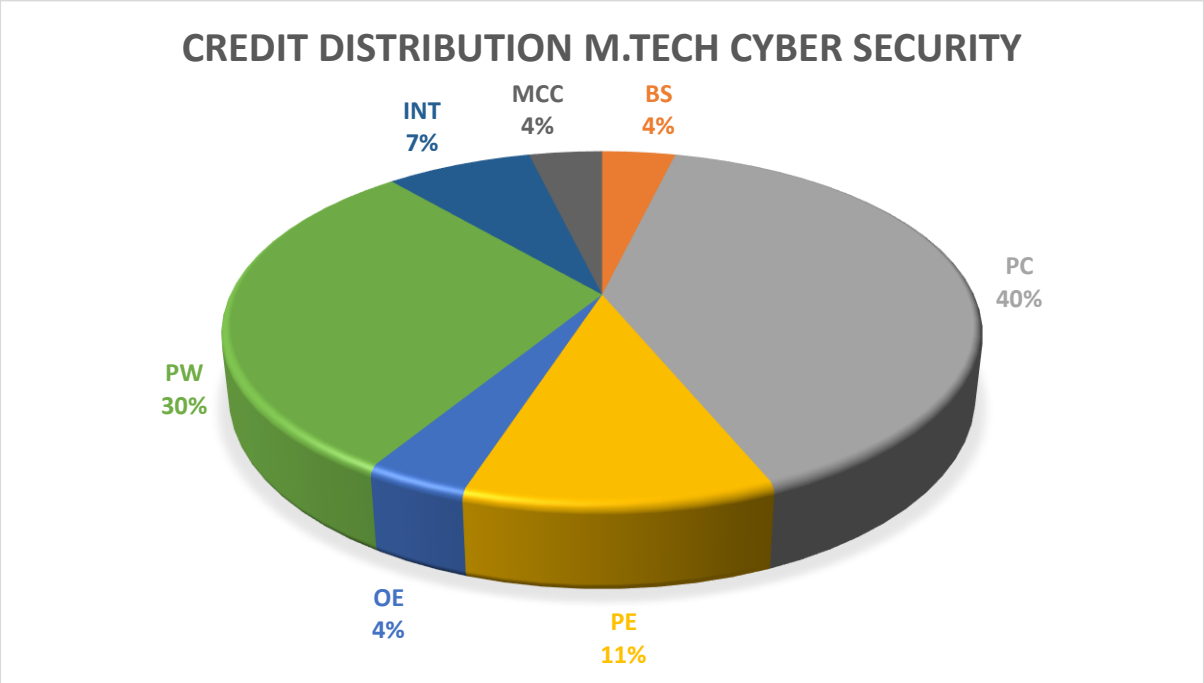
Credit Distribution of M. Tech Cyber Security

(Autonomous-2022)

SEM	AEC	BS	PC	PE	OE	PW	INT	MCC	Total Credits
I	-	3	16					3	22
II			12	6					18
III			4	3	3	6	6		22
IV	-					18			18
Total	-	3	32	9	3	24	6	3	80

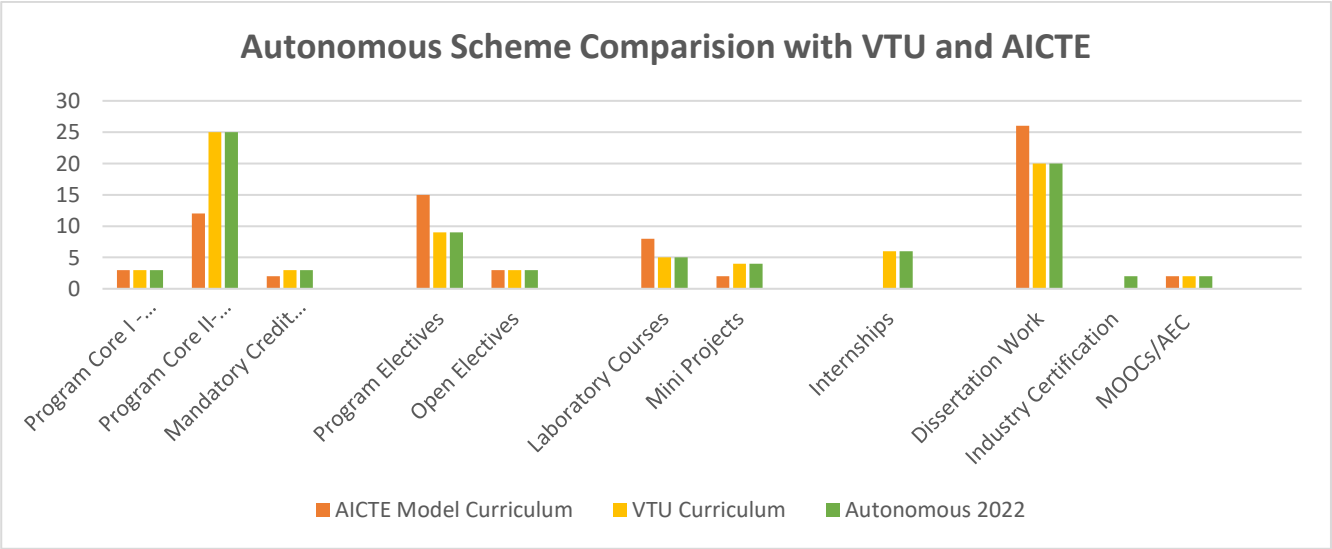
Legend

AEC/AUD	Ability Enhancement Course	**BS**	Basic Science Course
PC	Professional Core	**PE**	Professional Elective
INT	Internship	**PW**	Project Work
MCC	Mandatory Credit Course		



Statistical Comparison Curriculum Components with AICTE and VTU

Sl. No	Curriculum Components	AICTE Model Curriculum	VTU Curriculum	Autonomous 2022
1	Program Core I - Mathematics	3	3	3
2	Program Core II- Domain Specific	12	25	25
3	Mandatory Credit Courses	2	3	3
4	Program Electives	15	12	12
5	Open Electives	3	-	-
6	Laboratory Courses	8	5	5
7	Mini Projects	2	4	4
8	Internships	-	6	6
9	Dissertation Work	26	20	18
10	Industry Certification	-	-	2
11	MOOCs/AEC	2	2	2



Inclusion the autonomous curriculum is at par and above the standard prescribed

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(An Autonomous Institute affiliated to VTU)
Scheme of Teaching and Examination: Effective from AY 2022-23
Choice Based Credit System (CBCS)

PG PROGRAM: CYBER SECURITY (MCR) | **Semester: I**

Sl. No.	Course Category	Course Code	Course Title	Teaching Dept.	Teaching Hours /Week			Credits	Examination			
					L	T	P/S		Duration	CIE Marks	SEE Marks	Total Marks
1	BS	22MCR11	Foundation of Mathematics for Cyber Security	Maths	2	2	0	3	3	50	50	100
2	MCC	22MCC12	Research Methodology and IPR	CY	3	0	0	3	3	50	50	100
3	PCC	22MCR13	Social and Ethical Issues of the Internet	CY	3	2	0	4	3	50	50	100
4	IPCC	22MCR14	Cyber Security Essentials	CY	3	0	2	4	3	50	50	100
5	PCC	22MCR15	Information Security and Privacy-Policies and Standards	CY	3	2	0	4	3	50	50	100
6	PCC	22MCR16	Cloud Security	CY	3	0	0	3	3	50	50	100
7	PCL	22MCRL17	Cloud Security Laboratory	CY	0	0	2	1	3	50	50	100
8	AUD/AEC	22AUD18	MOOCs - Online	CY	Classes and evaluation procedures are as per the policy of the online course providers.							PP
				TOTAL	**17**	**6**	**4**	**22**	-	**350**	**350**	**700**

- **Audit Courses /Ability Enhancement Courses Suggested by BOS (ONLINE courses):** Audit Courses: These are prerequisite courses suggested by the Interim Board of Studies – M.Tech Cyber Security. Ability Enhancement Courses will be suggested by the BoS if prerequisite courses are not required for the programs. Ability Enhancement Courses:
  - These courses are prescribed to help students to enhance their skills in in fields connected to the field of specialisation as well allied fields that leads to employable skills. Involving in learning such courses are impetus to lifelong learning.
  - The courses under this category are online courses published in advance and approved by the concerned Board of Studies.
  - Registration to Audit /Ability Enhancement Course shall be done in consultation with the mentor and is compulsory during the concerned semester.
  - In case a candidate fails to appear for the proctored examination or fails to pass the selected online course, he/she can register and appear for the same course if offered during the next session or register for a new course offered during that session, in consultation with the mentor.
  - The Audit Ability Enhancement Course carries no credit and is not counted for vertical progression. However, a pass in such a course is mandatory for the award of the degree.

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(An Autonomous Institute affiliated to VTU)

Scheme of Teaching and Examination: Effective from AY 2022– 23

Choice Based Credit System (CBCS)

PG PROGRAM: CYBER SECURITY (MCR) | **Semester: II**

Sl. No.	Course Category	Course Code	Course Title	Teaching Dept.	Teaching Hours /Week			Credits	Examination			
					L	T	P/S		Duration	CIE Marks	SEE Marks	Total Marks
1	IPCC	22MCR21	Applied Cryptography	CY	3	0	2	4	3	50	50	100
2	PCC	22MCR22	Cyber Forensics and Cyber Laws	CY	3	2	0	4	3	50	50	100
3	PEC	22MCREXX	Professional Elective	CY	3	0	0	3	3	50	50	100
4	PEC	22MCREXX	Professional Elective	CY	3	0	0	3	3	50	50	100
5	PCL	22MCRL25	Offensive Security Laboratory	CY	0	2	2	2	3	50	50	100
6	PW	22MCR26	Mini Project with Seminar	CY	0	0	4	2	3	50	50	100
7	AUD/AEC	22AUD27	MOOCs - Online	CY	Classes and evaluation procedures are as per the policy of the online course providers.							PP
				TOTAL	**12**	**2**	**10**	**18**	**-**	**300**	**300**	**600**

- **MOOCs:** Students can choose any course related to the domain / program which is for 2 credits (26 hours to 30 hours and 12-14 weeks course). The course can be from NPTEL, Coursera, Udemy or any other leading platform with examination and assessments. The web link for few courses listed in the various platforms is given below
  - NOC | Computer Science and Engineering (nptel.ac.in) - https://nptel.ac.in/noc/courses/106/
  - Top Online Courses and Specializations | Coursera - https://www.coursera.org/courses
- **Mini Project with Seminar:** This may be hands-on practice, survey report, data collection and analysis, coding, mobile app development, field visit and report preparation, modelling of system, simulation, analysing and authenticating, case studies, etc. CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide, if any, and a senior faculty of the department. Students can present the seminar based on the completed mini-project. Participation in the seminar by all postgraduate students of the program shall be **mandatory**. The CIE marks awarded for Mini-Project work and Seminar shall be based on the evaluation of Mini Project work and Report, Presentation skill and performance in Question and Answer session in the ratio 50:25:25. Mini-Project with Seminar shall be considered as a head of passing and shall be considered for vertical progression as well as for the award of degree. Those, who do not take-up/complete the Mini Project and Seminar shall be declared as fail in that course and have to complete the same during the subsequent semester.

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(An Autonomous Institute affiliated to VTU)
Scheme of Teaching and Examination: Effective from AY 2022-23
Choice Based Credit System (CBCS)

PG PROGRAM: CYBER SECURITY (MCR) | **Semester: III**

Sl. No.	Course Category	Course Code	Course Title	Teaching Dept.	Teaching Hours /Week				Credits	Examination			
					L	T	P	PW		Duration	CIE Marks	SEE Marks	Total Marks
1	PCC	22MCR31	Digital Infrastructure Security	CY	4	0	0	0	4	3	50	50	100
2	PEC	22MCREXX	Professional Elective	CY	3	0	0	0	3	3	50	50	100
3	PEC	22MCREXX	Professional Elective	CY	3	0	0	0	3	3	50	50	100
4	PW	22MCR34	Project Phase - 1	CY	0	0	0	6	3	3	100	-	100
5	PW	22MCR35	Societal Project	CY	0	0	0	6	3	3	100	-	100
6	IN	22MCRI36	Internship	CY	0	0	0	12	6	3	50	50	100
				TOTAL	**9**	**2**	**0**	**24**	**22**	-	**400**	**200**	**600**

- **Project Work Phase-1:** Students in consultation with the guide/co-guide if any, shall pursue literature survey and complete the preliminary requirements of selected Project work. Each student shall prepare relevant introductory project document and present a seminar. CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide if any, and a senior faculty of the department. The CIE marks awarded for project work phase -1, shall be based on the evaluation of Project Report, Project Presentation skill and Question and Answer session in the ratio 50:25:25.
- **Societal Project:** Students in consultation with the internal guide as well as with external guide (much preferable) shall involve in applying technology to workout/proposing viable solutions for societal problems. CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide if any, and a senior faculty of the department. The CIE marks awarded shall be based on the evaluation of Project Report, Project Presentation skill, and performance in the Question-and-Answer session in the ratio of 50:25:25. Those, who have not pursued /completed the Societal Project, shall be declared as fail in the course and have to complete the same during subsequent semester/s after satisfying the Societal Project requirements. There is no SEE (University examination) for this course
- **Internship:** All the students shall have to undergo mandatory internship of 6-8 weeks during the vacation of II and III semesters and /or II and III semesters. Those, who have not pursued /completed the internship, shall be declared as fail in internship course and have to complete the same during subsequent semester end examinations after satisfying the internship requirements.

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(An Autonomous Institute affiliated to VTU)
Scheme of Teaching and Examination: Effective from AY 2022-23
Choice Based Credit System (CBCS)

PG PROGRAM: CYBER SECURITY (MCR) | **Semester: IV**

Sl. No.	Course Category	Course Code	Course Title	Teaching Dept.	Teaching Hours /Week				Self-Study	Credits	Examination			
					L	T	P	PW			Duration	CIE Marks	SEE Marks	Total Marks
1	PW	22MCR41	Project Phase – 2	CY	0	0	0	16	0	16	3	50	50	100
2	PW	22MCR42	Industry Certification Program	CY	0	0	0	0	2	2	-	50	-	50
				TOTAL	**0**	**0**	**0**	**16**	**2**	**18**	-	**100**	**50**	**150**

- **Industry Certification Program**: Students can choose the certification programs from leading certification vendors like EC Council, SANS Institute, CISCO and others. They may present the final certificate for internal assessment. This may be taken up during any semester in the 2-year program.

- **Project Work Phase-2:** CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide, if any, and a Senior faculty of the department. The CIE marks awarded for project work phase -2, shall be based on the evaluation of Project Report subjected to plagiarism check, Project Presentation skill and Question and Answer session in the ratio 50:25:25. SEE shall be at the end of IV semester. Project work evaluation and Viva-Voce examination (SEE), after satisfying the plagiarism check (below 20%).

Electives Pool for M.Tech Cyber Security

Course Code	Course Title
22MCRE01	Secured Software Architecture and Design
22MCRE02	Cyber Security Incident Response Management
22MCRE03	Mobile Application Security
22MCRE04	Security Assessment and Verification
22MCRE05	Database Security
22MCRE06	Software Metrics and Quality Assurance
22MCRE07	Operating System Security
22MCRE08	Cognitive Security
22MCRE09	Cyber Threat Intelligence
22MCRE10	Machine Learning Techniques in Cyber Secuirty
22MCRE11	Data Security and Risk Management
22MCRE12	IoT Security
22MCRE13	Software Security Engineering
22MCRE14	Cyber Risk and Disaster Management
22MCRE15	Biometric Security
22MCRE16	Data Haunting

Assessment Pattern for Theory Course

Component		Conducted for Marks	Final	Total	Total Marks
CIE	Internals-I	40	40 (Reduced to 30)	30	50
	Internals-II	40			
	Internals-III	40			
	Assignment I	20	20	20	
	Assignment II	20			
	OR				
	Skill Development Activity/ Flexible Assessment tool	40	20		
SEE	Semester End Exam	100			50
				Total Marks	**100**

Assessment Pattern for Integrated Course

Component		Conducted for Marks	Final	Total	Total Marks
CIE	Internals-I	40	20	20	50
	Internals-II	40			
	Internals-III	40			
				10	
	Assignment I	10	20		
	Assignment II	10			
	OR				
	Skill Development Activity/ Flexible Assessment tool	20	20		
	Lab Experiments	10	10	20	
	Record Evaluation	10			
	Lab Test	10	10		
SEE	Semester End Exam	100			50
				Total Marks	**100**

Assessment Pattern for Practical Course

Component		Conducted for Marks	Final Average	Total Marks
CIE	Internals-I	40	20	50
	Internals-II	40		
	Cumulative Continuous Evaluation (CCE) where every experiment is evaluated for 10 marks (6 marks for execution +4 marks for Viva Voce) **and / or** **Mini Project or Open-ended experiments**	30	30	
SEE	Semester End Exam **20% for Write-up** **60% for Conduction** **20% for Viva-voce** ***Change of the experiments*** is allowed only once and 10% of marks allotted to the procedure part to be made zero.	100		50
			Total Marks	**100**

Minimum passing standards shall be 40% of marks CIE and 40% of marks in SEE. 50% of marks with CIE and SEE combined.

SEMESTER – I

M.TECH Cyber Security

Choice Based Credit System (CBCS)

SEMESTER - I

Foundation of Mathematics for Cyber Security (2:1:0) 3

(Effective from the academic year 2022-23)

Course Code	22MCR11	CIE Marks	50
Teaching Hours/Week (L:T:P)	2:2:0	SEE Marks	50
Total Number of Contact Hours	50	Exam Hours	3

Course Objectives:

This course will enable students to:

1. Provide the mathematical background required for cyber security.
2. Familiarize the basic building blocks of important cyber security applications
3. Discuss the theoretical aspects of number theory
4. Study the security model and analyze them before being used in many commercial, industrial as well as web applications.

Module – 1

Preamble: Significance and Scope of the course, Importance of the course in the societal, political, and economic growth of the nation, Impact of the course on societal and ethical issues, and career perspective

Algebraic Structures

Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots - Discrete logarithms. Rings – Sub rings, ideals, and quotient rings, Integral domains. Fields – Finite fields – GF (pn), GF(2n) - Classification - Structure of finite fields. Lattice, Lattice as Algebraic system, sub lattices, some special lattices

(10 hours)

(RBT Levels: L1, L2 and L3)

Module – 2

Introduction: Understanding of Vector spaces, graph theory, Statistical models & their applications in Engineering, Economics and Statistics.

Linear Algebra-I

Vector Spaces: Vector spaces; subspaces Linearly independent and dependent vectors, Basis and dimension, coordinate vectors-Illustrative examples. Linear transformations, Representation of transformations by matrices

(10 hours)

(RBT Levels: L1, L2 and L3)

Module – 3

Linear Algebra-II

Computation of Eigen values and Eigen vectors of real symmetric matrices-Jacobi and Given's method. Orthogonal vectors and orthogonal basis. Gram-Schmidt orthogonalization process. QR decomposition, singular value decomposition**.**

(10 hours)

(RBT Levels: L1, L2 and L3)

Module – 4

Number Theory and Algebraic Geometry

Elliptic curves, basic facts, elliptic curve cryptosystems, elliptic curve primality test – elliptic curve factorization.

(10 hours)

(RBT Levels: L1, L2 and L3)

Module – 5

Coding Theory:

Introduction - Basic concepts: codes, minimum distance, the equivalence of codes, Linear codes - Linear codes - Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes – Hadamard codes - Goppa codes**.**

(10 hours)

(RBT Levels: L1, L2 and L3)

Course outcomes:

The students will be able to

CO1: Understand basic concepts of various algebraic structures and theorems which are used for designing security algorithms.

CO2: Linearly transform the system from one dimension to another and represent the pertinent linear transformation in matrix form.

CO3: Apply techniques of constrained optimization and singular value decomposition to problems arising in power/control system analysis, signals, and systems.

CO4: Identify the approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.

CO5: Understand coding theory which will be useful for data compression and maintaining confidentiality.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1. David C.Lay, Steven R.Lay and J.J.McDonald, "Linear Algebra and its Applications", 5th Edition, Pearson Education Ltd., 2015.
2. Neal Coblitz, "A Course in Number Theory and Cryptography", Springer Verlag, Second edition.

References:

1. C.L. Liu, 'Elements of Discrete Mathematics', McGraw Hill, 2008.
2. Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006.
3. Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa, 1998.
4. D. S. Malik, J. Mordeson, M. K. Sen, "Fundamentals of Abstract Algebra, Tata McGraw Hill.
5. P. K. Saikia, "Linear Algebra", Pearson Education.
6. Niven, H.S. Zuckerman and H. L. Montgomery, "An Introduction to the Theory of Numbers", John Wiley and Sons,.
7. Leigh Metcalf, William Casey, "Cybersecurity and Applied Mathematics", Syngress Publisher.

M.TECH CYBER SECURITY

Choice Based Credit System (CBCS)

SEMESTER – I

Research Methodology and Intellectual Property Rights (3:0:0) 3

(Effective from the academic year 2022 -2023)

Course Code	22MCC12	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:

This course will enable students to:

1. Give an overview of the research methodology and explain the technique of defining a research problem.
2. Explain the functions of the literature review in research and carry out a literature search, its review and develop theoretical and conceptual frameworks.
3. Explain various research designs, sampling designs, and also different methods of data collections.
4. Understand hypothesis and chi- square test.
5. Develop the art of interpretation and the art of writing different research reports.
6. Explain various forms of the intellectual property, its relevance and business impact in the changing global business environment.

Module – 1

Introduction: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective.

Research Methodology: Introduction, Meaning of Research, Objectives of Research, Motivation in Research, Types of Research, Research Approaches, Significance of Research, Research Methods versus Methodology, Research and Scientific Method, Importance of Knowing How Research is Done, Research Process, Criteria of Good Research, and Problems Encountered by Researchers in India.

Defining the Research Problem: Research Problem, Selecting the Problem, Necessity of Defining the Problem, Technique Involved in Defining a Problem, An Illustration.

(8 Hours)

Module – 2

Reviewing the literature: Place of the literature review in research, bringing clarity and focus to your research problem, Improving research methodology, Broadening knowledge base in research area, Enabling contextual findings, How to review the literature, searching the existing literature, reviewing the selected literature, Developing a theoretical framework, Developing a conceptual framework, Writing about the literature reviewed.

Research Design: Meaning of Research Design, Need for Research Design, Features of a Good Design, Important Concepts Relating to Research Design, Different Research Designs, Basic Principles of Experimental Designs, Important Experimental Designs.

(8 Hours)

Module – 3
Design of Sampling: Introduction, Sample Design, Sampling and Non-sampling Errors, Sample Survey versus Census Survey, Types of Sampling Designs. **Measurement and Scaling:** Qualitative and Quantitative Data, Classifications of Measurement Scales, Goodness of Measurement Scales, Sources of Error in Measurement Tools, Scaling, Scale Classification Bases, Scaling Technics, Multidimensional Scaling, Deciding the Scale. **Data Collection:** Experimental and Surveys, Collection of Primary Data, Collection of Secondary Data, Selection of Appropriate Method for Data Collection, Case Study Method. (8 Hours)
Module – 4
Testing of Hypotheses: Hypothesis, Basic Concepts Concerning Testing of Hypotheses, Testing of Hypothesis, Test Statistics and Critical Region, Critical Value and Decision Rule, Procedure for Hypothesis Testing, Hypothesis Testing for Mean, Proportion, Variance, for Difference of Two Mean, for Difference of Two Proportions, for Difference of Two Variances, P-Value approach, Power of Test, Limitations of the Tests of Hypothesis. **Chi-square Test:** Test of Difference of more than Two Proportions, Test of Independence of Attributes, Test of Goodness of Fit, and Cautions in Using Chi Square Tests. (8 Hours)
Module – 5
Interpretation and Report Writing: Meaning of Interpretation, Technique of Interpretation, Precaution in Interpretation, Significance of Report Writing, Different Steps in Writing Report, Layout of the Research Report, Types of Reports, Oral Presentation, Mechanics of Writing a Research Report, Precautions for Writing Research Reports. **Intellectual Property:** The Concept, Intellectual Property System in India, Development of TRIPS Complied Regime in India, Patents Act, 1970, Trade Mark Act, 1999,The Designs Act, 2000, The Geographical Indications of Goods (Registration and Protection) Act1999, Copyright Act,1957,The Protection of Plant Varieties and Farmers' Rights Act, 2001,The Semi-Conductor Integrated Circuits Layout Design Act, 2000, Trade Secrets, Utility Models, IPR and Biodiversity, The Convention on Biological Diversity (CBD) 1992, Competing Rationales for Protection of IPRs, Leading International Instruments Concerning IPR, World Intellectual Property Organisation (WIPO),WIPO and WTO, Paris Convention for the Protection of Industrial Property, National Treatment, Right of Priority, Common Rules, Patents, Marks, Industrial Designs, Trade Names, Indications of Source, Unfair Competition, Patent Cooperation Treaty (PCT), Advantages of PCT Filing, Berne Convention for the Protection of Literary and Artistic Works, Basic Principles, Duration of Protection, Trade Related Aspects of Intellectual Property Rights(TRIPS) Agreement, Covered under TRIPS Agreement, Features of the Agreement, Protection of Intellectual Property under TRIPS, Copyright and Related Rights, Trademarks, Geographical indications, Industrial Designs, Patents, Patentable Subject Matter, Rights Conferred, Exceptions, Term of protection, Conditions on Patent Applicants, Process Patents, Other Use without Authorization of the Right Holder, Layout-Designs of Integrated Circuits, Protection of Undisclosed Information, Enforcement of Intellectual Property. **Recap / Summary of the Course** (8 Hours)

Course Outcomes: The student will be able to:

CO1: Understand the concepts of research methodology, research problem and literature review.
CO2: Understand various forms of the intellectual property rights, its relevance and business impact in the changing global business environment and leading International Instruments concerning IPR.
CO3: Analyze various research designs, sampling designs, measurement and scaling techniques and different methods of data collections.
CO4: Apply several parametric tests of hypotheses.
CO5: Develop the art of interpretation and writing research reports.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks :

1. C.R. Kothari, Gaurav Garg, "Research methodology: Methods and Techniques", New Age International, 4th Edition, 2018.
2. Ranjit Kumar, "Research Methodology a step-by-step guide for beginners", SAGE Publications Ltd., 4th Edition, 2014.
3. The Institute of Company Secretaries of India, Statutory Body Under an Act of Parliament, Study Material (For the topic Intellectual Property under module 5), Professional Programme Intellectual Property Rights, Law and Practice, September 2013.

References:

1. Trochim , Research Methods: the concise knowledge base , Atomic Dog Publishing, 2005.
2. Fink A, Conducting Research Literature Reviews: From the Internet to Paper, Sage Publications, 2009.
3. Panneerselvam R, Research Methodology, Prentice Hall of India, New Delhi, 2004.

M. Tech CYBER SECURITY

Choice Based Credit System (CBCS)

SEMESTER – I

Social and Ethical issues of Internet (3:2:0)4

(Effective from the academic year 2022-23)

Course Code	22MCR13	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:2:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:

This course will enable students to:

1. Identify and describe common ethical concepts and theories.
2. Analyze ethical dilemmas and articulate a clear, descriptive account prior to forming a normative course of action.
3. Demonstrate one or more processes of philosophical analysis.
4. Identify common ethical issues facing professionals in the field of information technology.
5. Apply ethical concepts and an analytical process to common dilemmas found in the information technology field.

Module – 1

Introduction: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective.

Traditional Definition- Ethical Theories, Consequentialism, Deontology, Human Nature, Relativism, Hedonism, Emotivism, Functional Definition of Ethics, Ethical Reasoning and Decision Making, A Framework for Ethical Decision Making, Making and Evaluating Ethical Arguments, Codes of Ethics, Preamble, Objectives of Codes of Ethics, Reflections on Computer Ethics.

(8 Hours)

Module – 2

Ethics and the Professions - Introduction, Evolution of Professions, Origins of Professions, Requirements of a Professional, Pillars of Professionalism, The Making of an Ethical Professional: Education, and Licensing , Formal Education, Licensing Authorities, Professional Codes of Conduct, Professional Decision Making and Ethics, Professional Dilemma in Decision Making, Guilt and Making Ethical Decisions, Professionalism and Ethical Responsibilities, Whistle-Blowing, Harassment and Discrimination, Ethical and Moral Implications

(8 Hours)

Module – 3

New Frontiers for Computer Ethics: Cyberspace - Introduction, Cyberspace and the Concepts of Telepresence and Immersion, Securing Cyberspace, Detecting Attacks in Cyberspace, Cyberspace Systems Survivability, Personal Identity, Regulating and Censoring Cyberspace, The Social Value of Cyberspace, Privacy in Cyberspace, Privacy Protection, Global Cybernetics, Cyberspace Lingua Franca, Global Cyber Culture

(8 Hours)

Module – 4

Social Context of Computing -Introduction, The Digital Divide, Access, Technology, Humanware (Human Capacity), Infrastructure, Enabling Environments, Obstacles to Overcoming the Digital Divide, ICT in the Workplace, The Electronic Office, Office on Wheels and Wings, The Virtual Workplace, The Quiet Revolution: The Growth of Telecommuting, Employee Social and Ethical Issues, Employee Monitoring
Workplace Privacy and Surveillance, Electronic Monitoring, Workplace, Employee, Health, and Productivity, Ergonomics

(8 Hours)

Module – 5

Ethical, Privacy, and Security Issues in the Online -Social Network Ecosystems, Introduction, Introduction to Computer Networks, Computer Network Models, Computer Network Types, Social Networks, Online Social Networks(OSNs), Types of Online Social Networks , Online Social Networking Services, The Growth of Online Social Networks , Ethical and Privacy Issues in Online Social Networks, Privacy Issues in OSNs, Strengthening Privacy in OSNs, Ethical Issues in Online Social Networks, Security and Crimes in Online Social Networks, Beware of Ways to Perpetuate Crimes in Online, Social Networks, Defense Against Crimes in Online Social Networks , Proven Security Protocols and Best Practices in Online, Social Networks, Authentication, Access Control, Legislation, Self-Regulation Detection, Recovery.

Recap/Summary of the course.

(8 Hours)

Course Outcomes: At the end of this course, the student will be able to

CO1: Identify common ethical issues facing professionals in the field of information technology.
CO2: Apply ethical concepts and an analytical process to common dilemmas found in the information technology field.
CO3: Analyze ethical dilemmas and articulate a clear, descriptive account prior to forming a normative course of action.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks

1. Joseph Migga Kizza, Ethical and Social Issues in the Information Age, Fifth Edition, Springer London, 2013.

References:

1. Quinn, M. J. (2012). Ethics for the information age. Upper Saddle River, NJ: Addison-Wesley. 5th Ed. ISBN 978-0-13-285553-2
2. Adelson, H., Ledeen, K., & Lewis, H. (2008). Blown to bits: Your life, liberty, and happiness after the digital explosion. (1st ed.). Addison-Wesley. ISBN 978-0-13-285553-2. Download PDF Format through Creative Commons Licensing: http://www.bitsbook.com/excerpts/ .

M. Tech CYBER SECURITY

Choice Based Credit System (CBCS)

SEMESTER – I

Cyber Security Essentials (3:0:2)4

(Effective from the academic year 2022-23)

Course Code	22MCR14	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:2	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:

This course will enable students to:

1. Gain knowledge of the various aspects of network architecture and protocols, Network performance
2. Understand effective communication mechanisms
3. Students will learn about the issues in 802.11 LANs
4. Learn various congestion control algorithms.

Module – 1

Introduction: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective.

Foundation: Building a Network, Requirements, Perspectives, Scalable Connectivity, Cost-Effective Resource sharing, Support for Common Services, Manageability, Protocol layering, Performance, Bandwidth and Latency, Delay X Bandwidth Product, Perspectives on Connecting, Classes of Links, Reliable Transmission, Stop-and-Wait ,Sliding Window, Concurrent Logical Channels.

(8 Hours)

Module – 2

Internetworking I: Basic Internetworking (IP), What is an Internetwork?, Service Model, Global Addresses, Datagram Forwarding in IP, subnetting and classless addressing, Address Translation (ARP), Host Configuration (DHCP), Error Reporting (ICMP), Virtual Networks and Tunnels. Internetworking- II: Network as a Graph, Distance Vector (RIP), Link State (OSPF), Metrics, The Global Internet, Routing Areas, Routing among Autonomous systems (BGP), IP Version 6 (IPv6), Mobility and Mobile IP.

(8 Hours)

Module – 3

Security Essentials:

Network Security: Internet Architecture, Network Protocols and Vulnerability, Application-Layer Security- Public Key Infrastructure, DNS Security Extensions, Hyper Text Transfer Protocol Secure (HTTPS), Network Time Protocol (NTP) Security, Transport-Layer Security- Handshake, Key-Derivation, Data-Transfer, Quick UDP Internet Connections (QUIC), Network Layer Security - IP Masquerading, IPv6 Security- Routing Protocol Security, Border Gateway Protocol (BGP) Security

(8 Hours)

Module – 4

Cryptographic Building Blocks, Principles of Ciphers, Symmetric-Key Ciphers, Public-Key Ciphers, Authenticators, key Pre-distribution, Pre-distribution of Public Keys, Pre-distribution of Symmetric Keys, Authentication Protocols, Originality and Timeliness Techniques,

(8 Hours)

Module – 5

Authentication and others: Public-Key Authentication Protocols, Symmetric-Key Authentication Protocols, Diffie-Hellman Key Agreement, Example Systems, Pretty Good Privacy (PGP),Secure Shell (SSH), Transport Layer Security (TLS, SSL, HTTPS),IP Security (IPsec), Wireless Security (802.11i),Firewalls, Strengths and Weaknesses of Firewalls

Recap/Summary of the course.

(8 Hours)

Course Outcomes:

The student will be able to

CO1: Apply various protocols to develop applications using the sockets API.
CO2: Demonstrate effective communication mechanisms in computer networks
CO3: Analyze the concepts and issues in Mobile and Wireless Networks.
CO4: Examine possible research opportunities and challenges within the network application and security.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

List of Experiments-PART A

1. Apply the RSA algorithm on a text file to produce cipher text file.
2. Develop a mechanism to setup a security channel using Diffie-Hellman Key Exchange between client and server.
3. Implement secure hash algorithm for Data Integrity. Implement MD5 and SHA-1 algorithm, which accepts a string input, and produce a fixed size number - 128 bits for MD5; 160 bits for SHA-1, this number is a hash of the input. Show that a small change in the input results in a substantial change in the output
4. Write a TCP client/server program in which client sends three numbers to the server in a singlemessage. Server returns sum, difference and product as a result single message. Client programshould print the results appropriately.

Textbooks

1. Larry Peterson and Bruce S Davis "Computer Networks: A System Approach", 5 Edition, Elsevier 2014.
2. CyBoK, The Cyber Security Book of Knowledge, Oct 2019.

References:

1. Uyless Black, "Computer Networks, Protocols , Standards and Interfaces" 2 nd Edition PHI.
2. Douglas E Comer, "Internetworking with TCP/IP, Principles, Protocols and Architecture", 6th Edition, PHI – 2014.
3. Behrouz A Forouzan, "TCP /IP Protocol Suite" 4th Edition – Tata McGraw-Hill.
4. James F. Kurose and Keith W. Ross, Computer Networking: A Top-Down Approach, 6/e, Pearson Education, 2012.

M.TECH CYBER SECURITY

Choice Based Credit System (CBCS)

SEMESTER – I

Information Security and Privacy - Policies and Standards (3:2:0) 4

(Effective from the academic year 2022-23)

Course Code	22MCR15	CIE Marks	50
Teaching Hours/Week (L: T:P)	3:2:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:

This course will enable students to:

1. Understand the polices established IT governance.
2. Audit vulnerabilities based on the IT security standards
3. Analyse business case studies for IT security.
4. Explain managing of security models using information security standards.

Module – 1

Preamble: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective.

Introduction to Information Security Policies: About Policies, why Policies are Important, When policies should be developed, How Policy should be developed, Policy needs, Identify what and from whom it is being protected, Data security consideration, Backups, Archival storage and disposal of data, Intellectual Property rights and Policies, Incident Response and Forensics, Management Responsibilities, Role of Information Security Department, Security Management and Law Enforcement, Security awareness training and support.

(8 Hours)

Module – 2

Policy Definitions, Standards, Guidelines, Procedures with examples, Policy Key elements, Policy format and Basic Policy Components, Policy content considerations, Program Policy Examples, Business Goal Vs Security Goals, Computer Security Objectives, Mission statement Format, Examples, Key roles in Organization, Business Objectives, Standards: International Standards.

(8 Hours)

Module – 3

Writing The Security Policies: Computer location and Facility construction, Contingency Planning, Periodic System and Network Configuration Audits, Authentication and Network Security, Addressing and Architecture, Access Control, Login Security, Passwords, User Interface, Telecommuting and Remote Access, Internet Security Policies, Administrative and User Responsibilities, WWW Policies, Application Responsibilities, E-mail Security Policies.

(8 Hours)

Module – 4

Privacy & Online Rights - Privacy as Confidentiality, Data Confidentiality Cryptography-based access control, Obfuscation-based inference control , Metadata Confidentiality , Privacy as Control , Support for privacy settings configuration , Support for privacy policy negotiation , Support for privacy policy interpretability , Privacy as Transparency , Feedback-based transparency , Audit-based transparency, Privacy Technologies and Democratic Values, Privacy technologies as support for democratic political systems , Censorship resistance and freedom of speech ,Privacy Engineering

(8 hours)

Module – 5

The Information Security Blueprint: The ISO 27000 Series, NIST Security Models, IETF Security Architecture Baselining and Best Business Practices, Design of Security Architecture

Recap/ Summary of the Course

(8 hours)

Course Outcomes: The students will be able to:

CO1: Write policy document for securing network connection and interfaces.
CO2: Explain the standards, guidelines, Procedures, and key roles of the organization.
CO3: Write, monitor, and review policy document.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1. Scott Barman, Writing Information Security Policies, Sams Publishing 2002.
2. CyBoK, The Cyber Security Book of Knowledge, Oct 2019.
3. Michael E. Whitman, Principles of Information Security, Fourth Edition, Cengage Learning,2012.

References:

1. Thomas R Peltier, Justin Peltier, Information Security Fundamentals, John Backley CRC Press, 2005.
2. Harold F. Tipton and Micki Krause, Information Security Management Handbook Auerbach publications, 5th Edition, 2005.

M.Tech CYBER SECURTIY

Choice Based Credit System (CBCS)

SEMESTER – I

Cloud Security (3:0:0) 3

(Effective from the academic year 2022-23)

Course Code	22MCR16	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:

This course will enable students to:

1. To summarize the concepts of secure architecture design patterns.
2. To investigate software vulnerabilities and its impacts on attacks.
3. To illustrate tools used in secured designing
4. To apply the policies, security standards on software architectures.

Module – 1

Preamble: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective.

Cloud Computing Architectural Framework: Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Cloud Service Models, Multi- Tenancy, Approaches to create a barrier between the Tenants, cloud computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing, How Security Gets Integrated.

(8 Hours)

Module – 2

Compliance and Audit: Cloud customer responsibilities, Compliance and Audit Security Recommendations. Portability and Interoperability: Changing providers reasons, Changing providers expectations, Recommendations all cloud solutions, IaaS Cloud Solutions, PaaS Cloud Solutions, SaaS Cloud Solutions.

(8 Hours)

Module – 3

Traditional Security, Business Continuity, Disaster Recovery, Risk of insider abuse, Security baseline, Customers actions, Contract, Documentation, Recovery Time Objectives (RTOs), Customers responsibility, Vendor Security Process (VSP).

(8 Hours)

Module – 4

Data Center Operations: Data Center Operations, Security challenge, Implement Five Principal Characteristics of Cloud Computing, Data center Security Recommendations. Encryption and Key Management: Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards, Recommendations.

(8 Hours)

Module – 5

Identity and Access Management: Identity and Access Management in the cloud, Identity and Access Management functions, Identity and Access Management (IAM) Model, Identity Federation, Identity Provisioning Recommendations, Authentication for SaaS and Paas customers, Authentication for IaaS customers, Introducing Identity Services, Enterprise Architecture with IDaaS ,IDaaS Security Recommendations. Virtualization: Hardware Virtualization, Software Virtualization, Memory Virtualization, Storage Virtualization, Data Virtualization, Network Virtualization, Virtualization Security Recommendations.

Recap/Summary of the course

(8 Hours)

Course Outcomes: The students will be able to:

CO1: Generalize the Data Centre operations, encryption methods and deployment details

CO2: Demonstrate the growth of Cloud computing, architecture and different modules of implementation.

CO3: Provide recommendations for using and managing the customer's identity and choose the type of virtualization to be used.

CO4: Evaluate the different types of cloud solutions among IaaS, PaaS, SaaS.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance, Oreilly Media,2009.

References:

1. Vic (J.R.) Winkler, Securing the Cloud, Cloud Computer Security Techniques and Tactics, Syngress, 2011.

M.TECH CYBER SECURITY
Choice Based Credit System (CBCS)
SEMESTER – I

Cloud Security Laboratory (0:0:2) 1

(Effective from the academic year 2022-23)

Course Code	22MCRL17	CIE Marks	50
Teaching Hours/Week (L: T:P)	0:0:2	SEE Marks	50
Total Number of Contact Hours	26	Exam Hours	3

Course Objectives:

This course will enable students to:

1. To provide skills for designing and analyzing cloud Concepts.
2. To enable students to work on various cloud platforms.
3. To provide skills to work towards solution of real-life problems

List of Experiments

1. AWS Security, Identity & Compliance
2. Managing User Identities with Long Term Credentials in AWS IAM
3. Managing Access using IAM User Groups & Roles
4. Using IAM Policies to Define and Manage Permissions
5. Knowledge Check: Overview of AWS Identity and Access Management (IAM)
6. Implementing Cross-Account Access Using IAM
7. Securing AWS Organizations with Service Control Policies (SCPs)

Course Outcomes: The students will be able to:

CO1: Demonstrate how secure communication between various cloud platforms/applications .

CO2: Implement various security techniques.

Web References:

1. Cloud Academy Security Labs Details: https://cloudacademy.com/learning-paths/aws-security-services-42/
2. Udemy Certification on AWS security fundamentals: https://www.udemy.com/course/aws-hands-on-labs-2020-step-by-step-for-beginners-new/?utm_source=adwords&utm_medium=udemyads&utm_campaign=LongTail_la.EN_cc.INDIA&utm_content=deal4584&utm_term=_.ag_77882236223_.ad_533093955804_.kw_.de_c_.dm_.pl_.ti_dsa-1007766171032_.li_9062044_.pd_.&matchtype=&gclid=Cj0KCQiA1sucBhDgARIsAFoytUtbiwTaUqvVRLrS0glkHq0HrOBbBayvYat0B6_p35i5MeOUdfA9ZuMaAiPPEALw_wcB

M.TECH CYBER SECURITY

Choice Based Credit System (CBCS)

SEMESTER – I

MOOCs

(Effective from the academic year 2022-23)

Course Code	22AUD18	CIE Marks	-
Teaching Hours/Week (L: T:P: SS)	-	SEE Marks	-
Total Number of Contact Hours	-	Exam Hours	-

Preamble:

Students can choose any course related to the domain / program which is for 2 credits (26 hours to 30 hours and 12-14 weeks course). The course can be from NPTEL, Coursera, Udemy or any other leading platform with examination and assessments. The web link for few courses listed in the various platforms is given below

- Computer Science and Engineering (nptel.ac.in) - https://nptel.ac.in/noc/courses/106/
- Top Online Courses and Specializations | Coursera - https://www.coursera.org/courses

Course Outcome: The students will be able to:

CO1: Acquire the knowledge beyond the curriculum

CO2: Facilitate practical learning by leading practitioners around the world in the field of study.

CO3: Exposure to various assessment methods for all round application of the chosen topic

CO4: Earn industry badges /certification in the leading topics in the field of study.

SEMESTER – II

M.TECH CYBER SECURITY

Choice Based Credit System (CBCS)

SEMESTER – II

Applied Cryptography (3:0:2) 4

(Effective from the academic year 2022 -23)

Course Code	22MCR21	CIE Marks	50
Teaching Hours/Week (L: T:P)	3:0:2	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:

This course will enable students to:

1. Explain standard algorithms used to provide confidentiality, integrity and authenticity.
2. Distinguish key distribution and management schemes.
3. Deploy encryption techniques to secure data in transit across data networks.
4. Implement security applications in the field of Information technology.

Module – 1

Introduction: Significance and Scope of the course, Importance of the course in societal, political, and economic growth of the nation. Impact of the course on societal and ethical issues and career perspective.

Overview of Cryptography: Introduction, Information security and cryptography, Basic terminology and concepts, Symmetric key encryption, Digital signatures, Public-key cryptography, Hash functions, Protocols and mechanisms, Key establishment, management, and certification, Pseudorandom numbers and sequences, Classes of attacks and security models.

(8 Hours)

Module – 2

Symmetric & Asymmetric Cryptography: Classical encryption techniques, Block cipher design principles and modes of operation, Data encryption standard, Evaluation criteria for AES, AES cipher, Principles of public key cryptosystems, The RSA algorithm, Key management – Diffie Hellman Key exchange, Elliptic curve arithmetic-Elliptic curve cryptography.

(8 Hours)

Module – 3

Mathematical Background: Probability theory, Information theory, Complexity theory, Number theory, Abstract algebra, Finite fields, The integer factorization problem, The RSA problem, The Diffie-Hellman problem, Composite moduli.

Number Theory: Introduction to number theory, Overview of modular arithmetic, discrete logarithms, and primality/factoring, Euclid's algorithm, Finite fields, Prime numbers, Fermat's and Euler's theorem- Testing for primality, A quick introduction to groups, rings, integral domain and fields.

(8 Hours)

Module – 4

Geometric Extensions: Fields, Characteristic of a field, prime fields, Arithmetic of polynomials over fields. Field extensions, Galois group of a field extensions, Fixed field and Galois extensions. Minimum polynomial, Construction of fields with the help of an irreducible polynomial. Splitting field of a polynomial, Separable polynomial and Separable extensions. Construction of finite fields and their structure. Enumeration of irreducible polynomials over finite fields. Fundamental theorem of Galois Theory. Cyclotomic extensions, Geometric constructions and Galois theory of Equations (Statement only of Abel Ruffini), Solving Cubic and Bi-quadratic polynomials using radicals.

(8 Hours)

Module – 5

Quantum Cryptography and Quantum Teleportation: Heisenberg uncertainty principle, polarization states of photons, quantum cryptography using polarized photons, local vs. nonlocal interactions, entanglements, EPR paradox, Bell's theorem, Bell basis, teleportation of a single qubit theory and experiments.

Recap/Summary of the course.

(8 Hours)

Course Outcomes: The students will be able to:

CO1: Apply the OSI security architecture and classical encryption techniques for simple Applications

CO2: Compare various cryptographic techniques.

CO3: Analyze the vulnerabilities in any computing system.

CO4: Evaluate security mechanisms using rigorous approaches, including theoretical.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1. Alfred J. Menezes, Paul C. vanorschot and Scott A. Vanstone, "Handbook of Applied Cryptography" CRC Press.
2. Neal Koblitz, A Course in Number Theory and Cryptology, Springer 1987.
3. William Stallings, Cryptography and Network Security Principles And Practice, 6th edition, 2019.

References:

1. Damien Vergnaud and Michel Abdalla, Applied Cryptography and Network Security, 7th International Conference, ACNS 2009, Paris-Rocquencourt, France, June 2-5, 2009, Proceedings.
2. B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd Edition, John Wiley & Sons, 1995.
3. Mihir Bellare and Phillip Rogaway, "Introduction to Modern Cryptography", 2005.

List of Experiments:

1. Raju wants to build encrypted and decryption algorithms of Playfair cipher. Help him to build a key matrix using the key "mrecwautonomous"
2. By using key **"CBDE"** sender would like send message (plain text) **"HELLOWORLD"**. Build encryption process and find out what is the encrypted message (cipher text) by using **Hill Cipher**. Implement decryption process and find out what is the decrypted message (plain text) of cipher text "SLHZYATGZT" by using Hill Cipher.
3. Implementation of Encryption and Decryption of **Vigenère Cipher** keyword deceptive
   Key: deceptivedeceptivedeceptive
   Plaintext: wearediscoveredsaveyourself
   Cipher text: ZICVTWQNGRZGVTWAVZHCQYGLMG
4. Implement the Euclidean Algorithm for integers and polynomials.
5. Implement AES Key Expansion.
6. Implementation of AES encryption and decryption
7. Implementation of Simplified DES Encryption and decryption
8. Implementation of RC4
9. Implementation of Diffie-Helman key exchanges.

M. Tech CYBER SECURITY

Choice Based Credit System (CBCS)

SEMESTER – II

Cyber Forensics and Cyber Laws (3:2:0)4

(Effective from the academic year 2022-23)

Course Code	22MCR22	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:2:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:

This course will enable students to:

1. Gain knowledge of the various aspects of cyber security and law aspects.
2. Understand effective mechanisms for forensics applications
3. Identify issues in detection and investigation of Cyber Crime.
4. Learn various acts related to cyber security world.

Module – 1

Introduction: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective.

Introduction to Cybercrime: Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals? , Classifications of Cybercrimes, Cybercrime: The Legal Perspectives, Cybercrimes: An Indian Perspective, Cybercrime and the Indian ITA 2000, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens. Cyberoffenses: How Criminals Plan Them: How Criminals Plan the Attacks, Social Engineering, Cyberstalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing.

(8 Hours)

Module – 2

Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops

Module – 3

Tools and Methods Used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks. Phishing and Identity Theft: Introduction, Phishing, Identity Theft (ID Theft).

(8 Hours)

Module – 4

Understanding Digital Forensics: Introduction, Historical Background of Cyber-forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber-forensics and Electrical Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation, Setting up a Computer Forensics Laboratory: Understanding the Requirements, Computer Forensics and Steganography, Relevance of the OSI 7 Layer Model to Computer Forensics, Forensics and Social Networking Sites: The Security/Privacy Threats, Computer Forensics from Compliance Perspective, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing, Anti-forensics.

(8 Hours)

Module – 5

Legal aspects of Digital Forensics: Introduction to Security Policies and Cyber Laws: Need for An Information Security Policy, Information Security Standards – Iso, Introducing Various Security Policies and Their Review Process, Introduction to Indian Cyber Law, Objective and Scope of the it Act, 2000, Intellectual Property Issues, Overview of Intellectual - Property - Related Legislation in India, Patent, Copyright,Law Related to Semiconductor Layout and Design, Software License.

Recap/Summary of the course.

(8 Hours)

Course Outcomes:

The student will be able to

CO1: Illustrate evidence collection and legal challenges
CO2: Demonstrate cyber security cybercrime and forensics.
CO3: Apply the cybercrime with the support tools and methods.
CO4: Examine possible research opportunities and challenges within the cyber laws and security.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks

1. Sunit Belapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India Pvt Ltd 2013.
2. Surya Prakash Tripathi, Ritendra Goyal, Praveen Kumar Shukla, Introduction to information security and cyber laws, Dream tech Press 2015.

References:

1. Thomas J. Mowbray, Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions, John Wiley & Sons.

M.TECH CYBER SECURITY
Choice Based Credit System (CBCS)
SEMESTER – II

Offensive Security Laboratory (0:2:2) 2

(Effective from the academic year 2022-23)

Course Code	22MCRL25	CIE Marks	50
Teaching Hours/Week (L: T:P)	0:2:2	SEE Marks	50
Total Number of Contact Hours	26	Exam Hours	3

Course Objectives:

This course will enable students to:

1. To provide skills for designing and analyzing Cyber Security Tools.
2. To enable students to work on various Vulnerability scanners.
3. To provide skills to work towards solution of real-life problems

List of Experiments-PART A

1. Cyber-kill chain: Reconnaissance and Information Gathering : OSINT, Breached credentials, Subdomain brute forcing, Directory scanning.
2. Scanning and Enumeration : Scanning and exploiting open ports and services, Scanning for potential exploits in public vulnerability databases.
3. Exploitation Basics : Metasploit, Gaining access to machines using vulnerabilities, Custom exploitation scripts, Password brute forcing, Password spraying.
4. Active Directory : LLMNR poisoning, SMB relays, IPv6 DNS takeovers, pass-the-hash/pass-the- password, token impersonation, kerberoasting, GPP attacks, golden ticket attacks.
5. Maintaining access : Reverse shell, file transfer. Web Application Penetration Testing. Automated Vulnerability scanners: Nessus, NMap, Metasploit, Acunetix.
6. Report Writing : Statements of Work, Rules of Engagement, Non-Disclosure Agreements,

Course Outcomes: The students will be able to:

CO1: Familiarization with cyber kill-chain (Reconnaissance, Scanning and Enumeration, Exploitation, Privilege escalation, Maintaining access etc)

CO2: Understanding the usage of industry standard tools used as a part of the VAPT process such as Metasploit, nmap, Nessus.

CO3: Ability to perform pentest a target and generate a report based on the test.

Textbooks:

1. Bugcrowd, “The Ultimate Guide to Penetration Testing”, 2020 edition
2. HackerOne, “Web hacking 101”

M.TECH CYBER SECURITY

Choice Based Credit System (CBCS)

SEMESTER – II

Mini Project with Seminar (0:0:4) 2

(Effective from the academic year 2022-23)

Course Code	22MCR26	CIE Marks	50
Teaching Hours/Week (L: T:P:PW)	0:0:4	SEE Marks	50
Total Number of Contact Hours	48	Exam Hours	3 hrs

Preamble: Mini Project for PG students gives an opportunity to build upon learning gained in the earlier years, and to broaden the scope of understanding. Students are required to take complete ownership of their project, and this necessitates a considerable time and effort beyond the exercise of knowledge and skills. They must be self-regulating and self-directed in their time management. It is expected that the students use the wide range of knowledge and skills that they have gathered over the course of their post graduate program.

M.Tech Students are motivated to focus on projects related to the following area (Specialization):

- Cyber Security.
- Cyber Forensics
- Application of Cyber Security

Synopsis Phase (Review 1)

All project proposals (Synopsis) submitted must be approved by the Project Evaluation Committee (**PEC**). The role of PEC is to verify, approve and evaluate the projects submitted by students.

Project Evaluation Committee (PEC)

The projects are evaluated by Project Evaluation Committee (PEC). The committee consists of HOD, guide and senior faculty members as shown in table below-

Name	Role
Head of Department, Dept. of Cyber Security	Chairman
Senior Faculty-1	Member
Senior Faculty -2	Member
Senior Faculty -3	Member
Guide	Member

Mini Project + Seminar (Review 2)

Students shall submit detailed presentation and report with chosen topic in 2nd semester. The presentation shall cover the design methodology, requirement analysis covering detailed functional and non-functional requirements. The design shall cover both high level and low-level design aspects of the system. The presentation shall be with PEC committee identified for the students in the previous semester. This shall be considered for 50% of the CIE marks allocated for the Mini project. The seminar will be on topic related to the project chosen by the student and guide. Students shall present a paper in reputed international conference / journals relevant to the area of the project work for the literature work carried out in the last semester along with proposed method.

All students shall submit the detailed presentation with demonstration of the project work. The student shall prepare to submit his/her experimental results in peer review

high impact indexed journals or submit a patent application on the work carried out. A draft mini project report will be submitted to PEC members prior to the presentation date. This review will be for 50% of the marks allocated to CIE. Corrections shall be suggested by guide, PEC member, PG Coordinator and HoD. After all corrections are made, the student shall prepare to submit the final report copy.

Course Outcome: The students will be able to:

CO1: Identify the requirements for the real-life problems.

CO2: Conduct a survey of several available literatures in the preferred field of study.

CO3: Develop project successfully by coding, emulating and testing.

CO4: Prepare quality report and present the findings of the project conducted in the preferred domain.

SEMESTER – III

M. Tech CYBER SECURITY

Choice Based Credit System (CBCS)

Semester III

Digital Infrastructure Security (4:0:0)4

(Effective from the academic year 2022-23)

Course Curriculum jointly Curated with SISA Institute

Course Code	22MCR31	CIE Marks	50
Teaching Hours/Week (L:T:P)	4:0:0	SEE Marks	50
Total Number of Contact Hours	50	Exam Hours	3

Course Objectives:

This course will enable students to:

1. Identify and differentiate between different digital infrastructures.
2. Explain the relationship between digital infrastructures, digital practice, the concept of institutional facts.
3. Anticipate and provide examples of different levels of interoperability problems and solutions.
4. Anticipate, explain and provide examples of relationships between material and digital resources in digital infrastructures.

Module – 1

Introduction: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective.

Introduction to Digital Infrastructure: Social Engineering, Types of Social Engineering, Defining Social Engineering Attacks, Templates for Social Engineering Attacks, Application of the Social Engineering Attack Templates Cyber Security Threat Landscape and Techniques, Cyber Security Threat Landscape Emerging Cyber Security Threats, Cyber Security Techniques, Firewall

(10 Hours)

Module – 2

Information Security Standards: ISO/IEC 27000 family, ISO/IEC 15408, ISO/IEC 18043, CIS, ISO 22301, NIST, SANS Security Policy Resource, ISO 28000, OWASP Foundation, ISO/IEC 27037, PCI DSS, CSA,ISO/SAE 21434,ISO/IEC 27400, ISO/IEC 27017

(10 Hours)

Module – 3

Financial IT Infrastructure and Framework: PCI DSS Requirements, PCI Mandate, Driving Compliance, compliance program requirements, The most important slide, PCI DSS Certification Journey, PCI DSS Success Plan, PCI Steering Committee, Payment Data Security Awareness, Trainings, Mandatory Documentation.

(10 Hours)

Module – 4

Introduction to Critical Information Infrastructure: Online Banking, Credit Card and UPI Security, Online Banking Security, Mobile Banking Security, Security of Debit and Credit Card, UPI Security 2. Micro ATM, e-wallet and POS Security, Security of Micro ATMs, e-wallet Security Guidelines, Security Guidelines for Point of Sales(POS).

(10 Hours)

Module – 5

Introduction to Zero Trust, Cyber Space. History of Internet , Cyber Crime , Information Security , Computer Ethics and Security Policies, Choosing the Best Browser according to the requirement and email security: Guidelines to choose web browsers , Securing web browser, Antivirus, Email security, Guidelines for secure password and wi-fi security, Guidelines for setting up a Secure password, Two-steps authentication, Password Manager, Wi-Fi Security

Recap/Summary of the course.

(10 Hours)

Course Outcomes:

The student will be able to

CO1:	Identify suitable information security standards for each digital infrastructure. (K3)
CO2:	Examine the payment security standards and its eco-system. (K4).
CO3:	Analyse the cyber security needs of every infrastructure. (K4).
CO4:	Infer better policies and guidelines to secure the cyber space and infrastructure. (K4)

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks or Web References:

1. Introduction to Cyber Security available at http://uou.ac.in/foundation-course
2. Cyber Security Techniques http://uou.ac.in/progdetail?pid=CEGCS-17
3. Cyber Threat Landscape https://www.upguard.com/blog/cyber-threat-landscape
4. Cyber Attacks and Counter Measures: User Perspective http://uou.ac.in/progdetail?pid=CEGCS-17
5. Information System http://uou.ac.in/progdetail?pid=CEGCS-17
6. Information Security Standards - https://www.bsigroup.com/en-IN/Cyber-Security/standards-for-it-and-cyber-security/

Electives Pool for M.Tech Cyber Security

Course Code	Course Title
22MCRE01	Secured Software Architecture and Design
22MCRE02	Cyber Security Incident Response Management
22MCRE03	Mobile Application Security
22MCRE04	Security Assessment and Verification
22MCRE05	Database Security
22MCRE06	Software Metrics and Quality Assurance

22MCRE07	Operating System Security
22MCRE08	Cognitive Security
22MCRE09	Cyber Threat Intelligence
22MCRE10	Machine Learning Techniques
22MCRE11	Data Security and Risk Management
22MCRE12	IoT Security
22MCRE13	Software Security Engineering
22MCRE14	Risk and Disaster Management
22MCRE15	Biometric Security

M.Tech. CYBER SECURTIY
Choice Based Credit System (CBCS)
SEMESTER – II/III

Secured Software Architecture and Design (3:0:0) 3
(Effective from the academic year 2022-23)

Course Code	22MCRE01	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:

This course will enable students to:

1. To summarize the concepts of secure architecture design patterns.
2. To investigate software vulnerabilities and its impacts on attacks.
3. To illustrate tools used in secured designing
4. To apply the policies, security standards on software architectures.

Module – 1

Preamble: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective.

Architecture and Security: Architecture Reviews, Software Process, Reviews and the Software Development Cycle, Software Process and Architecture Models, Software Process and Security, Architecture Review of System, Security Assessments, Security Architecture Basics, Architecture Patterns in Security

(8 Hours)

Module – 2

Low-Level Architecture: Code Review, importance of code review, Buffer Overflow Exploits, Countermeasures Against Buffer Overflow Attacks, patterns applicable, Security and Perl, Bytecode Verification in Java-Good Coding Practices Lead to Secure Code, Cryptography, Trusted Code, Secure Communications.

(8 Hours)

Module – 3

Mid-Level Architecture: Middleware Security, Middleware and Security, The Assumption of Infallibility, The Common Object Request Broker Architecture, The OMG CORBA Security Standard, Vendor Implementations of CORBA Security, CORBA Security Levels, Secure Interoperability, Application, Unaware Security, Application, Aware Security, Application Implications, Web Security, Application and OS Security, Database Security.

(8 Hours)

Module – 4

High-Level Architecture: Security Components, Secure Single Sign-On- Public-Key Infrastructures, Firewalls, Intrusion Detection Systems, LDAP and X.500 Directories, Kerberos, Distributed Computing Environment,The Secure Shell, or SSH, The Distributed Sandbox, Security and Other Architectural Goals, Metrics for Non-Functional Goals, Force Diagrams around Security, High Availability, Robustness, Reconstruction of Events, Ease of Use, Maintainability, Adaptability, and Evolution, Scalability, Interoperability, Performance, Portability.

(8 Hours)

Module – 5

Enterprise Security Architecture: Security as a Process, Security Data, Enterprise Security as a Data Management Problem, Tools for Data Management, David Isenberg and the “Stupid Network”, Extensible Markup Language, The XML Security Services Signaling Layer, XML

and Security Standards, The Security Pattern Catalog Revisited, XML-Enabled Security Data-HGP: A Case Study in Data Management, Business Cases and Security, Building Business Cases for Security G Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux.

Recap/Summary of the course

(8 Hours)

Course Outcomes:

The students will be able to:

CO1: Identify the components targeted for each zone.

CO2: Map site zones with level of security

CO3: Design the secured sites based on tools & techniques

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1. Jay Ramachandran, Designing Security Architecture Solutions, Wiley Computer Publishing, 2010.

References:

1. Markus Schumacher, Security Patterns: Integrating Security and Systems Engineering, Wiley Software Pattern Series, 2010.

M.Tech. CYBER SECURTIY
Choice Based Credit System (CBCS)
SEMESTER – II/III

Cyber Security Incident Response Management (3:0:0) 3
(Effective from the academic year 2022-23)

Course Code	22MCRE02	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:
This course will enable students to:
1. To understands cyber incident response and its components.
2. To plan for incident response readiness and managing the operational aspects of the incident response team.
3. To organize an incident response team in a manner that ensures good handling of incidents while also making sure staff burnout is avoided.

Module – 1

Preamble: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective.
Introduction: Definitions of incident response and forensic analysis, relation of incident response to the rest of cybersecurity operations, incident response phases - preparation, identification, containment, eradication, recovery, follow-up, indicators of compromise (IOC), forensic analysis as an incident response tool and as support for cybercrime investigations, cybersecurity forensics principles.

(8 Hours)

Module – 2

Preparation: Policies and procedures, incident workflows, guidelines, incident handling forms, principles of malware analysis, log analysis, threat intelligence, vulnerability management, penetration testing, digital forensics, incident ticketing systems, incident documentation templates. **Identification:** Detection, incident triage, information gathering and reporting, incident classification, indicators of compromise (IOC).

(8 Hours)

Module – 3

Containment: Damage limitation, network segment isolation, system isolation, forensic backup and imaging, use of write blockers, temporary fixes, malware spread limitation. **Eradication:** Actual removal and restoration of affected systems, removal of attack artifacts, scanning of other systems to ensure complete eradication, use of IOCs on other systems and local networks, cooperation with forensic analysis to understand the attack fully.

(8 Hours)

Module – 4

Recovery: Test and validate systems before putting back into production, monitoring of system behavior, ensuring that another incident will not be created by the recovery process. **Follow-up:** Documenting lessons learned, preparatory activities for similar future incidents, technical training, process improvement.

(8 Hours)

Module – 5

Advanced computer network defense: vulnerability and threat management, threat intelligence and situational awareness, tools and processes, frameworks (ATT&CK, Cyber Kill Chain, etc.), threat hunting, information sharing
Planning and running incident response team exercises.

Recap/Summary of the course.

(8 Hours)

Course Outcomes:

The students will be able to:

CO1: Describe the main phases of incident response.

CO2: Identify different kinds of attacks methods to counter their effects

CO3: Describe the application of such techniques to real situations and the connection with incident response.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1. Ten Strategies of a World-Class Cybersecurity Operations Center, Carson Zimmermann, The MITRE Corporation, 2014. Free e-book available from https://www.mitre.org/publications/all/ten-strategies-of-a-world-class-cybersecurity-operations-center
2. Jason T. Luttgens and Matthew Pepe, "Incident Response & Computer Forensics, Third Edition" .

References:

1. Don Murdoch, "Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder".
2. Leighton Johnson, "Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response".

M.Tech CYBER SECURTIY

Choice Based Credit System (CBCS)

SEMESTER – II /III

Mobile Application Security (3:0:0) 3

(Effective from the academic year 2022-23)

Course Code	22MCRE03	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:

This course will enable students to:

1. To learn about securing wireless networks
2. To Identify and analyze various the security issues in wireless mobile communication
3. To learn various issues of application-level security in wireless environment and its related solution.

Module – 1

Preamble: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective.

Security Issues in Mobile Communication: Mobile Communication History, Security Wired Vs Wireless, Security Issues in Wireless and Mobile Communications

(8 Hours)

Module – 2

Security of Device, Network, and Server Levels: Mobile Devices Security Requirements, Mobile Wireless network level Security, Server Level Security. Application Level Security in Wireless Networks - Application of WLANs, Wireless Threats, Security for 2G Wi-Fi Applications,Recent Security Schemes for Wi-Fi Applications.

(8 Hours)

Module – 3

Application-Level Security in Cellular Networks: Generations of Cellular Networks, Security Issues and attacks in cellular networks, GSM,GPRS and UMTS security for applications, 3G security for applications

(8 Hours)

Module – 4

Application-Level Security in Ubiquitous Networks: Ubiquitous Computing, Need for Novel Security Schemes for UC, Security Challenges for UC.

(8 Hours)

Module – 5

Application Level Security in Heterogeneous Wireless Networks: Heterogeneous Wireless network architecture, Heterogeneous network application in disaster management, Security problems and solutions in heterogeneous wireless networks.

Recap/Summary of this course

(8 Hours)

Course Outcomes:

The students will be able to:

CO1: Identify the requirement of security and various issues at wireless and mobile network.

CO2: Analyze the threats in wireless environment including device, networks and servers.

CO3: Distinguish the attacks at various protocols in wireless network and differentiate the solution required for them.

CO4: Assess the security requirement for mobile adhoc environment, ubiquitous environment.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1. Pallapa Venkataram, Satish Babu, Wireless and Mobile Network Security, First Edition, Tata McGraw Hill, 2010.
2. Hakima Chaouchi, Maryline Laurent-Maknavicius, Wireless and Mobile Network Security Security Basics, Security in On-the-shelf and Emerging Technologies, Wiley, 2009.

References:

1. Tara M. Swaminathan and Charles R. Eldon, Wireless Security and Privacy- Best Practices and Design Techniques, Addison Wesley, 2002.

M.Tech CYBER SECURTIY

Choice Based Credit System (CBCS)

SEMESTER – II /III

Security Assessment and Verification (3:0:0) 3

(Effective from the academic year 2022-23)

Course Code	22MCRE04	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Module-1

Evolution of information security: information assets, security standards, organizational impacts, security certifications, elements of information security program, need for security assessment, security assessment process.

Module 2

Security assessment planning: Business drivers, scope definition, consultant's perspective, Client's perspective, Development of project plan. Initial information gathering, Initial preparation, analysis of gathered information.

Module 3

Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation.

Module 4

Security Risk assessment project management, Security risk assessment approaches and methods.

Module 5

Information security standards, Information security Legislation, Formal security verification, Security verification with SSL.

Course outcomes: At the end of the course the student will be able to:

CO1: Illustrate the roles information security and its management

CO2: Select appropriate techniques to tackle and solve problems in the discipline of information security assessment

CO3: Design an information security and validation system

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbook/ Textbooks

1. Sudhanshu Kairab , A practical assessment guide to security, CRC press, 2005.
2. Douglas J. Landoll, A Security Handbook risk assessment, Auerbach publications, 2006.

M.Tech CYBER SECURTIY

Choice Based Credit System (CBCS)

SEMESTER – II /III

Database Security (3:0:0) 3

(Effective from the academic year 2022-23)

Course Code	22MCRE05	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Module-1

Introduction: Introduction to Databases, Security Problems in Databases Security Controls Conclusions. Security Models 1: Introduction, Access Matrix Model, Take-Grant Model, Acten Model, PN Model, Hartson and Hsiao's Model, Fernandez's Model, Bussolati and Martella's Model for Distributed databases.

Module 2

Security Models 2: Bell and LaPadula's Model, Biba's Model, Dion's Model, Sea View Model, Jajodia and Sandhu's Model, The Lattice Model for the Flow Control conclusion. Security Mechanisms: Introduction, User Identification/Authentication, Memory Protection, Resource Protection, Control Flow Mechanisms, Isolation, Security Functionalities in Some Operating Systems, Trusted Computer System, Evaluation Criteria.

Module 3

Security Software Design: Introduction, A Methodological Approach to Security, Software Design, Secure Operating System Design, Secure DBMS Design, Security Packages, Database Security Design.

Module 4

Statistical Database Protection & Intrusion Detection Systems: Introduction, Statistics, Concepts and Definitions, Types of Attacks, Inference Controls, evaluation Criteria for Control Comparison, Introduction IDES System, RETISS System, ASES System Discovery.

Module 5

Models For The Protection Of New Generation Database Systems 1: Introduction, A Model for the Protection of Frame Based Systems, A Model for the Protection of Object-Oriented Systems, SORION Model for the Protection of Object-Oriented Databases. Models For The Protection Of New Generation Database Systems 2: A Model for the Protection of New Generation Database Systems, the Orion Model, Jajodia and Kogan's Model, A Model for the Protection of Active Databases Conclusions.

Course outcomes: At the end of the course the student will be able to:

- CO1: Carry out a risk analysis for a large database
- CO2: Implement identification and authentication procedures, fine-grained access control and data encryption techniques.
- CO3: Set up accounts with privileges and roles.
- CO4: Audit accounts and the database system

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbook/ Textbooks

1. Hassan A. Afyoun, Database Security and Auditing, CENGAGE Learning, 2009.
2. Castano, Database Security, Pearson Education

References:

1. Alfred Basta, Melissa Zgola, Database security,CENGAGE learning

M.Tech CYBER SECURTIY

Choice Based Credit System (CBCS)

SEMESTER – II /III

Software Metrics & Quality Assurance(3:0:0) 3

(Effective from the academic year 2022-23)

Course Code	22MCRE06	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Module-1

What Is Software Quality: Quality: Popular Views, Quality Professional Views, Software Quality, Total Quality Management and Summary. **Fundamentals Of Measurement Theory:** Definition, Operational Definition, And Measurement, Level Of Measurement, Some Basic Measures, Reliability And Validity, Measurement Errors, Be Careful With Correlation, Criteria For Causality, Summary. **Software Quality Metrics Overview:** Product Quality Metrics, In Process Quality Metrics, Metrics for Software Maintenance, Examples For Metrics Programs, Collecting Software Engineering Data.

Module -2

Applying The Seven Basic Quality Tools In Software Development: Ishikawa's Seven BasicTools, Checklist, Pareo Diagram, Histogram, Run Charts, Scatter Diagram, Control Chart, Cause And Effect Diagram. **The Rayleigh Model:** Reliability Models, The Rayleigh Model Basic Assumptions, Implementation, Reliability And Predictive Validity.

Module – 3

Complexity Metrics And Models: Lines Of Code, Halstead's Software Science , Cyclomatic Complexity Syntactic Metrics, An Example Of Module Design Metrics In Practice .**Metric And Lessons Learned For Object Oriented Projects:** Object Oriented Concepts And Constructs, Design And Complexity Metrics, Productivity Metrics, Quality And Quality Management Metrics, Lessons Learned For object oriented Projects.

Module-4

Availability Metrics: Definition And Measurement Of System Availability, Reliability Availability And Defect Rate, Collecting Customer Outage Data For Quality Improvement, In Process Metrics For Outage And Availability .**Conducting Software Project Assessment :**Audit Ad Assessment , Software Process Maturity Assessment And Software Project Assessment , Software Process Assessment A Preponed Software Project Assessment Method.

Module-5

Dos And Don'ts Of Software Process Improvement : Measuring Process Maturity, Measuring Process Capability, Staged Versus Continuous Debating Religion, Measuring Levels Is Not Enough, Establishing The Alignment Principle , Take Time Getting Faster, Keep it Simple Or Face Decomplexification, Measuring The Value Of Process Improvement , Measuring Process Compliance , Celebrate The Journey Not Just The Destination. **Using Function Point Metrics to Measure Software Process Improvement: Software** Process Improvement Sequences, Process Improvement Economies, Measuring Process Improvement at Activity Levels

Course outcomes: At the end of the course the student will be able to:

- CO1: Identify and apply various software metrics, which determines the quality level of software.
- CO2: Identify and evaluate the quality level of internal and external attributes of the software product.
- CO3: Compare and Pick out the right reliability model for evaluating the software.
- CO4: Evaluate the reliability of any given software product.
- CO5: Design new metrics and reliability models for evaluating the quality level of the software based on the requirement.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1. Stephen H Khan, Metrics and Models in Software Quality Engineering, Pearson 2nd edition, 2013.

References:

1. Norman E-Fentor and Share Lawrence Pflieger, Software Metrics, International Thomson Computer Press 1997.
2. S.A.Kelkar, Software quality and Testing Market,. PHI Learning, Pvt, Ltd 2012
3. Watts S Humphrey, Managing the Software Inc,. Process Pearson Education, 2008.
4. Mike Konrad and Sandy, CMMIPearson Education(Singapore), 2003.

M.Tech CYBER SECURTIY

Choice Based Credit System (CBCS)

SEMESTER – II /III

Operating System Security (3:0:0) 3

(Effective from the academic year 2022-23)

Course Code	22MCRE07	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Module-1

Introduction: Secure Os, Security Goals, Trust Model, Threat Model, Access Control. Fundamentals: Protection system, Lampson's Access Matrix, Mandatory protection system.

Module 2

Multics: Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis.

Module 3

Security in ordinary operating system: UNIX security, windows security Verifiable security goals: Information flow, information flow secrecy, models, information flow integrity model, the challenges of trusted, process, covert channels.

Module 4

Security Kernels: The Security Kernels, secure communications, processor Scomp, Gemini secure OS, Securing commercial OS, Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX era- IX, domain and type enforcement.

Module 5

Case study: Solaris Extensions Trusted extensions, access control, Solaris compatibility, trusted extensions, mediations process rights management, role based access control, trusted extensions, networking trusted extensions, multilevel services, trusted extensions administration.

Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux.

Course outcomes: At the end of the course the student will be able to:

- CO1: Gain the knowledge of fundamental concepts and mechanisms for enforcing security in OS.
- CO2: Analyze how to build a secure OS by exploring the early work in OS.
- CO3: Identify and compare different formal security goals and variety of security models proposed for development of secure operating systems.
- CO4: Interpret architectures of various secure OS and retrofitting security feature on existing commercial OS's.
- CO5: Shows variety of approaches applied to the development & extension services for securing operating systems.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1. Trent Jaeger, Operating system security, Morgan & Claypool Publishers, 2008.
2. Michael Palmer, Guide to Operating system Security, Thomson, 2009.

M.Tech CYBER SECURTIY

Choice Based Credit System (CBCS)

SEMESTER – II /III

Cognitive Security(3:0:0) 3

(Effective from the academic year 2022-23)

Course Code	22MCRE08	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Module-1

Linguistic aspects of natural language processing, A.I. And Quantum Computing, Applications of Artificial Intelligence (AI) in business.

Module-2

Emotion Recognition using human face and body language, AI based system to predict the diseases early, Smart Investment analysis, AI in Sales and Customer Support.

Module-3

Robotic Processes Automation for supply chain management.

Module-4

AI-Optimized Hardware, Digital Twin i.e. AI Modelling, Information Technology &Security using AI.

Module-5

Recent Topics in AI/ML: AI/ML in Smart solutions, AI/ML in Social Problems handling, Block chain and AI.

Course Outcomes: At the end of this course, students are able to:

CO1: Correlate the AI and solutions to modern problem.

CO2: Decide when to use which type of AI technique.

Question Paper Pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1. Sameer Dhanrajani, AI and Analytics, Accelerating Business Decisions, John Wiley &Sons.
2. Artificial Intelligence in Practice: How 50 Successful Companies Used AI andMachine Learning to Solve Problems, Bernard Marr, Matt Ward, Wiley.
3. Life 3.0: Being Human in the Age of Artificial Intelligence by Max Tegmark, 2018.
4. Homo Deus: A Brief History of Tomorrow by Yuval Noah Harari, 2017

M. Tech CYBER SECURITY
Choice Based Credit System (CBCS)
SEMESTER – II /III

Machine Learning Techniques (3:0:0)3
(Effective from the academic year 2022-23)

Course Code	22MCRE10	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:
This course will enable students to:

1. Gain knowledge about basic concepts of Machine Learning
2. Study about different learning algorithms
3. Learn about of evaluation of learning algorithms
4. Learn about Dimensionality reduction

Module – 1

Introduction: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective.

Introduction: Definition of learning systems, Goals and applications of machine learning, Aspects of developing a learning system: training data, concept representation, function approximation. Inductive Classification: The concept learning task, Concept learning as search through a hypothesis space, Generalto-specific ordering of hypotheses, Finding maximally specific hypotheses, Version spaces and the candidate elimination algorithm, Learning conjunctive concepts, The importance of inductive bias

(8 Hours)

Module – 2

Decision Tree Learning: Representing concepts as decision trees, Recursive induction of decision trees, Picking the best splitting attribute: entropy and information gain, Searching for simple trees and computational complexity, Occam's razor, Overfitting, noisy data, and pruning. Experimental Evaluation of Learning Algorithms: Measuring the accuracy of learned hypotheses. Comparing learning algorithms: cross-validation, learning curves, and statistical hypothesis testing.

(8 Hours)

Module – 3

Computational Learning Theory: Models of learnability: learning in the limit; probably approximately correct (PAC) learning. Sample complexity for infinite hypothesis spaces, Vapnik-Chervonenkis dimension. Rule Learning: Propositional and First-Order, Translating decision trees into rules, Heuristic rule induction using separate and conquer and information gain, First-order Horn-clause induction (Inductive Logic Programming) and Foil, Learning recursive rules, Inverse resolution, Golem, and Progol.

(8 Hours)

Module – 4

Artificial Neural Networks: Neurons and biological motivation, Linear threshold units. Perceptrons: representational limitation and gradient descent training, Multilayer networks and backpropagation, Hidden layers and constructing intermediate, distributed representations. Overfitting, learning network structure, recurrent networks. Support Vector Machines: Maximum margin linear separators. Quadractic programming solution to finding maximum margin separators. Kernels for learning non-linear functions.

(8 Hours)

Module – 5

Bayesian Learning: Probability theory and Bayes rule. Naive Bayes learning algorithm. Parameter smoothing. Generative vs. discriminative training. Logisitic regression. Bayes nets and Markov nets for representing dependencies. Instance-Based Learning: Constructing explicit generalizations versus comparing to past specific examples. K-Nearest-neighbor algorithm. Case-based learning.

Recap/Summary of the course.

(8 Hours)

Course Outcomes:

The student will be able to

CO1: Identify machine learning techniques suitable for a given problem
CO2 Solve the problems using various machine learning techniques
CO3: Apply Dimensionality reduction techniques.
CO4: Design application using machine learning techniques

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks

1. Tom M. Mitchell , "Machine learning", McGraw Hill 1997
2. M. Bishop, Pattern Recognition and Machine Learning, Springer, 2006.
3. Rajjan Shinghal, "Pattern Recognition", Oxford Press, 2006.

References:

1. Ethem Alpaydin, "Introduction to machine learning", PHI learning, 2008.
2. Hastie, Tibshirani, Friedman, "The Elements of Statistical Learning", Springer 2001.
3. R.O. Duda, P.E. Hart and D.G. Stork, Pattern Classification, Wiley-Interscience, 2nd Edition, 2000.
4. T. Hastie, R. Tibshirani and J. Friedman, The Elements of Statistical Learning: Data Mining, Inference and Prediction, Springer, 2nd Edition, 2009.

M. Tech CYBER SECURITY

Choice Based Credit System (CBCS)

Semester III

Digital Infrastructure Security (4:0:0)4

(Effective from the academic year 2022-23)

Course Curriculum jointly Curated with SISA Institute

Course Code	22MCR31	CIE Marks	50
Teaching Hours/Week (L:T:P)	4:0:0	SEE Marks	50
Total Number of Contact Hours	50	Exam Hours	3

Course Objectives:

This course will enable students to:

1. Identify and differentiate between different digital infrastructures.
2. Explain how digital infrastructures affect behavior, norms, and attitudes of individuals, groups, and organizations.
3. Explain the relationship between digital infrastructures, digital practice, and institutions, and explain the concept of institutional facts.
4. Anticipate, explain and provide examples of different levels of interoperability problems and solutions.
5. Anticipate, explain and provide examples of relationships between material and digital resources in digital infrastructures.

Module – 1

Introduction: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective.

Cyber Security Threat Landscape, Emerging Cyber Security Threats, Social Engineering, Types of Social Engineering, How Cyber Criminal Works, How to prevent for being a victim of Cyber Crime, Cyber Security Threat Landscape and Techniques, Cyber Security Threat Landscape Emerging Cyber Security Threats, Cyber Security Techniques, Firewall.

(10 Hours)

Module – 2

Information Security Standards: ISO/IEC 27000 family, ISO/IEC 15408, ISO/IEC 18043, CIS, ISO 22301, NIST, SANS Security Policy Resource, ISO 28000, OWASP Foundation, ISO/IEC 27037, PCI DSS, CSA,ISO/SAE 21434,ISO/IEC 27400, ISO/IEC 27017

(10 Hours)

Module – 3

PCI DSS Requirements: PCI Mandate, Driving Compliance, compliance program requirements, The most important slide, PCI DSS Certification Journey, PCI DSS Success Plan, PCI Steering Committee, Payment Data Security Awareness, Trainings, Mandatory Documentation.

(10 Hours)

Module – 4

Online Banking, Credit Card and UPI Security, Online Banking Security, Mobile Banking Security, Security of Debit and Credit Card, UPI Security 2. Micro ATM, e-wallet and POS Security, Security of Micro ATMs, e-wallet Security Guidelines, Security Guidelines for Point of Sales(POS).

(10 Hours)

Module – 5

Introduction to Cyber Space. History of Internet , Cyber Crime , Information Security , Computer Ethics and Security Policies, Choosing the Best Browser according to the requirement and email security: Guidelines to choose web browsers , Securing web browser, Antivirus, Email security, Guidelines for secure password and wi-fi security, Guidelines for setting up a Secure password, Two-steps authentication, Password Manager, Wi-Fi Security

Recap/Summary of the course.

(10 Hours)

Course Outcomes:

The student will be able to

CO1: Analyse the cyber security needs of an organization.
CO2: Conduct a cyber security risk assessment.
CO3: Implement cyber security solutions.
CO4: Use cyber security, information assurance, and cyber/computer forensics software/tools

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks

1. Introduction to Cyber Security available at http://uou.ac.in/foundation-course
2. Fundamentals of Information Security http://uou.ac.in/progdetail?pid=CEGCS-17
3. Cyber Security Techniques http://uou.ac.in/progdetail?pid=CEGCS-17
4. Cyber Attacks and Counter Measures: User Perspective http://uou.ac.in/progdetail?pid=CEGCS-17
5. Information System http://uou.ac.in/progdetail?pid=CEGCS-17