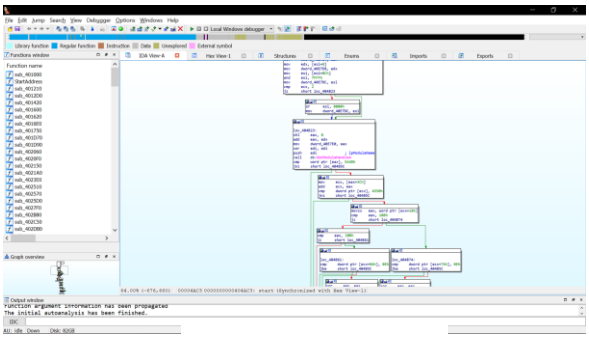
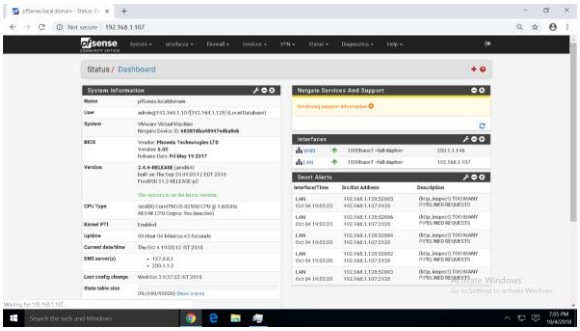
Curriculum & Contents

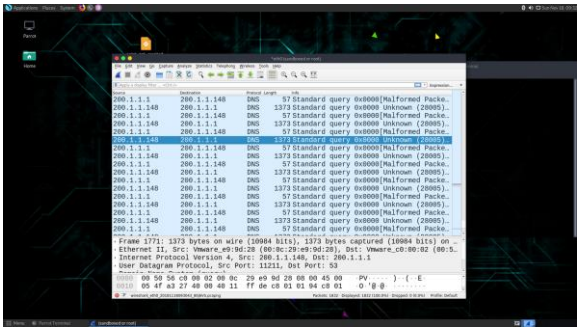
M Tech (Information Security)



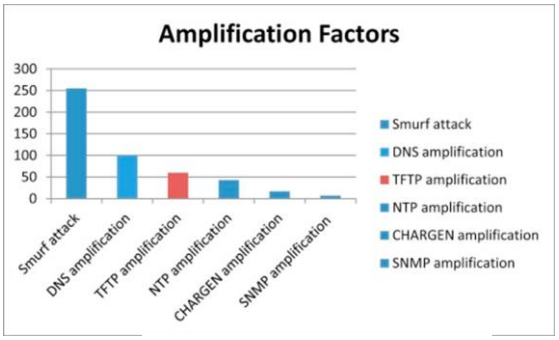
IDA Disassemble



pfSence firewall



pfSence firewall



Binary ninja disassemble

विश्वजीवनामृतं ज्ञानम्

ABV-Indian Institute of Information Technology & Management, Gwalior

June 2019

Semester - I

S. No.	Subject Code	Course Title	L	T	P	Credits
1.	MTAS-6101	Modelling and Simulation	3	0	0	3
2.	MTIS-6101	Modern Cryptography	3	1	0	4
3.	MTIS-6102	Introduction to Computer and Network Security	3	0	0	3
4.		Elective – I	3	0	0	3
5.		Elective II	3	0	0	3
6.	MTIS-6103	Computer and Network Security laboratory	0	0	2	1
7.	MTAS-6102	Modeling and Simulation laboratory	0	0	2	1
8.	MTHS-6101	Professional Ethics	2	0	0	1
		Total				**19**

Semester - II

S. No.	Subject Code	Course Title	L	T	P	Credits
1.	MTIS-6201	Information Security Risk Management	3	0	0	3
2.	MTIS-6202	Data Mining and Machine Learning	3	0	0	3
3.	MTIS-6203	Formal Techniques for Software reliability	3	1	0	4
4.	MTHS-6201	Research Methodology	2	0	2	3
5.		Elective III	3	0	0	3
6.		Elective IV	3	0	0	3
7.	MTIS-6204	Data Mining and Machine Learning Laboratory	0	0	2	1
		Total				**20**

Semester – III

S. No.	Subject Code	Course Title	L	T	P	Credits
1.	MTIS-7101	Technical Report Writing	0	0	2	1
2.	MTIS-7101	Seminar	0	0	2	1
3.		Elective V	2	0	0	2
4	MTIS-7199	Major Project Part I				6
		Total				**10**

Semester – IV

S. No.	Subject Code	Course Title	L	T	P	Credits
1.	MTIS-7299	Major Project Part II				12
		Total				**12**

Total credits to be earned over 4 semesters are 60.

List of Elective subjects

S. No.	Subject Code	Course Title	L	T	P	Credits
Application Security						
1.	MTIS-9101	Secure Software Systems	3	0	0	3
2.	MTIS-9102	Database Security	3	0	0	3
3.	MTIS-9103	Web Architecture Security	3	0	0	3
4.	MTIS-9104	Computer Security Audit and Assurance #	3	0	0	3
5.	MTIS-9105	Secure Enterprise Computing	3	0	0	3
6.	MTIS-9106	Digital Watermarking and Steganalysis	3	0	0	3
7.	MTIS-9107	Advanced Distributed System Security	3	0	0	3
8.	MTIS-9108	Analysis and Verification of Cryptographic Protocols	3	0	0	3
9.	MTIS-9109	Game Theory and Applications #	3	0	0	3

10.	MTIS-9110	Computational Number Theory	3	0	0	3
Security Analysis						
11.	MTIS-9201	Design and Analysis of Secured Networked Systems	3	0	0	3
12.	MTIS-9202	Cyber Security and IoT	3	0	0	3
13.	MTIS-9203	Cloud Security: Architecture and Technologies	3	0	0	3
14.	MTIS-9204	Public Key Infrastructure and managing E-Security	3	0	0	3
15.	MTIS-9205	Applied Cryptography	3	0	0	3
16.	MTIS-9206	Information Systems Security Risk Analysis	3	0	0	3
17.	MTIS-9207	Malware Analysis	3	0	0	3
18.	MTIS-9208	Privacy and Security for online Social Networks	3	0	0	3
Cyber-Threat Intelligence						
19.	MTIS-9301	Cyber Threat Intelligence	3	0	0	3
20.	MTIS-9302	Cyber Forensics Technologies and Requirements	3	0	0	3
21.	MTIS-9303	Cyber-Physical System Security	3	0	0	3
22.	MTIS-9304	Intrusion Detection and Prevention	3	0	0	3
23.	MTIS-9305	Information Assurance and Analysis	3	0	0	3
24.	MTIS-9306	Fundamentals of Intrusion Analysis	3	0	0	3

*The list can vary based on the requirement of Industry and Academia

Compulsory specialization electives

Please note:

a) The course contents are indicative in nature. Actual contents followed may deviate based on students/faculty interests.

b) Typically the evaluation is based on various components such as Minors (In-semester tests), Major examination (End-semester test), assignments, term papers, quizzes, presentations and class participation. The weightages for these components will be decided by the respective course instructors.

Semester – I

1	**Code of the subject**	MTAS-6101
2	**Title of the subject**	Modeling and Simulation
3	**Any prerequisite**	Engineering Mathematics and Probability & Statistics
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr Ajay Kumar
6	**Will this course require visiting faculty**	NO
7	**Learning Objectives of the subject (in about 50 words)**	To teach the application of mathematics and statistics in real life problems.
8	**Brief Contents**	**Introduction:** Concept of a system, System Environment, Modeling and Simulation of Real world problems, Classification of Models and examples, Static and Dynamic models, Principles used in modeling; **System Studies:** Subsystems, A Corporate models, Block diagram of modeling and simulation, System Analysis, System Design; **Mathematical Models:** Mathematical models in population dynamics, Epidemic Models, some mathematical modeling in Biology and Medicine Innovation diffusion models in marketing; **System Simulation:** The technique of simulation, the Monte Carlo Method, Types of system simulation, Continuous and Discrete time Simulation; **Probability Concepts in Simulation:** Stochastic variables, Discrete and continuous probability distributions, Measures of probability functions, Random numbers generation, Stochastic Processes: Poisson Process, Markov Process, Queuing Theory, Reliability; **Linear programming in Simulation:** Introduction, Transportation problem, Assignment problem and other simulation techniques in Operation research; **Software in System Simulation:** Numerical computation technique for continuous and discrete models (MATLAB).
9	**Contents for lab (If applicable)**	Given separately.
10	**List of text books/references**	1. Banks, J., Carson, I. I., Nelson, B. L., & Nicol, D. M., Discrete-event system simulation. Pearson, 2005 2. Kishor S Trivedi, Probability & Statistics With Reliability, Queuing And Computer Science Applications, Wiley, 2016. 3. Geoffrey Gordon, System Simulation, Prentice-Hall, 1979.

1	**Code of the subject**	MTIS-6101
2	**Title of the subject**	Modern Cryptography
3	**Any prerequisite**	NIL
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr Anuraj Singh
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	• To develop a framework to understand and implement cryptographic aspects. • To enhance an ability to analyze a problem, and identify and define the computing requirements for data security • To prepare abstract and critical thinking background for computer science students
8	**Brief Contents**	**Introduction:** Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Steganography, Security Attacks, Stream Cipher and Block Cipher**; Finite Fields and Number Theory:** Groups, Rings, Fields, Modular Arithmetic, Euclid's Algorithm, Finite Fields of Form GF (p) And GF (2n), Polynomial Arithmetic, Prime Numbers, Fermat's And Euler's Theorem, Testing For Primality, The Chinese Remainder Theorem, Discrete Logarithms**; Symmetric Cipher:** Block Cipher Principles, Data Encryption Standard, Multiple Encryption, Triple Des, Advanced Encryption Standard (AES), Block Cipher Modes of Operation, Blowfish, RC5 Algorithm**; Public Key Encryption:** Principles Of Public Key Cryptosystems, The RSA Algorithm, Key Management, Diffie Hellman Key Exchange, Elgamal Encryption, Elliptic Curve Arithmetic, Elliptic Curve Cryptography**; Cryptographic Protocols:** Authentication Requirement, Authentication Function, MAC, Hash Functions, Security of Hash Function , Digital Signatures, Authentication Protocols, SHA, MD5, SHA-1.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. William Stallings, Cryptography and Network security, 4e, Prentice Hall of India, New Jersey, 2008. 2. Christof Paar, Jan Pelzl, Understanding Cryptography, Springer-Verlag, Berlin, 2010 3. Behrouz A Forouzan, Cryptography and Network security, Tata Mc-Graw Hill, New York, 2007.

1	**Code of the subject**	MTIS-6102
2	**Title of the subject**	Introduction to Computer and Network Security
3	**Any prerequisite**	No
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Saumya Bhadauria
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	To be able to explain security principles, evaluate risks faced by computer systems, and explain how various attack scenarios work
8	Brief Contents	CIA Triad, User authentication, access Controls: security model, security policy, security mechanisms, DAC, MAC, RBAC; Denial of service attacks, Distributed Denial of Service attacks; Session hijacking, Spoofing: IP spoofing, ARP spoofing, DNS Spoofing, DNS hijacking, N-X Domain attack, DNS tunneling, Phantom Domain Attack, Random Subdomain Attack, DNS firewall, DNS Sec; Internet Security: Honeypots, Domain Key Identified Mail, Pretty Good Privacy, S/MIME.
9	**Contents for lab (If applicable)**	Mentioned in the lab course
10	**List of text books/references**	• William Stallings and Lawrie Brown. 2014. Computer Security: Principles and Practice (3rd ed.). Prentice Hall Press, Upper Saddle River, NJ, USA. • Wenliang Du. Computer Security: A Hands-on Approach. • Introduction to Computer Security Michael Goodrich and Roberto Tamassia Addison-Wesley, 2010

1	**Code of the subject**	MTIS-6103
2	**Title of the subject**	Computer and Network Security laboratory
3	**Any prerequisite**	Introduction to Computer and Network Security
4	**L-T-P**	0-0-2
5	**Name of the proposer**	Dr. Saumya Bhadauria
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	To have a hands on experience of the security tools and various attacks and their detection methods
8	**Brief Contents**	Wireshark, Implementation of DoS attacks, detection and analysis; Implementation of IP spoofing attack; DoS attack with spoofed IP address, detection and analysis.
9	**List of text books/references**	1. William Stallings and Lawrie Brown. Computer Security: Principles and Practice. Prentice Hall Press, Upper Saddle River, NJ, USA, 2014 2. Wenliang Du. Computer Security: A Hands-on Approach, 2017. 3. Introduction to Computer Security Michael Goodrich and Roberto Tamassia Addison-Wesley, 2010.

1	**Code of the subject**	MTAS-6102
2	**Title of the subject**	Modeling and Simulation Lab
3	**Any prerequisite**	Basic knowledge of Mathematics, statistics, excel
4	**L-T-P**	0-0-2
5	**Name of the proposer**	Dr Ajay Kumar
6	**Will this course require visiting faculty**	NO
7	**Learning Objectives of the subject (in about 50 words)**	To teach the applications of mathematics and statistics
8	**Brief Contents**	Monte Carlo simulation: Finding value of pi, Area under the curve, Double , integration, Multiple integration, Area of irregular shaped body, Discrete Event simulation, Tossing a coin/dice simulation, Singer server queue, Multiple server queues, Inventory problems; Other Tools: Computer Generation of Random Numbers, Testing Random Number Generators, Fitting a statistical distribution, Chi-square goodness-of-fit test, One-sample Kolmogorov-Smirnov test, Test for Standard Normal Distribution.
9	**List of text books/references**	1. Banks, J., Carson, I. I., Nelson, B. L., & Nicol, D. M. (2005). Discrete-event system simulation. Pearson. 2. Kishor S Trivedi, Probability & Statistics With Reliability, Queuing And Computer Science Applications, 2nd Ed, Wiley. 3. Geoffrey Gordon, System Simulation, Prentice-Hall, 1977

1	**Code of the subject**	MTHS-6101
2	**Title of the subject**	Professional Ethics
3	**Any prerequisite**	No
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Prof. V.S.R. Krishnaiah
6	**Will this course require visiting faculty**	Yes
7	**Learning Objectives of the subject (in about 50 words)**	The primary objective of this course is to sensitize students on the concept of Ethics and Human Values and make them understand the relevance of these ideas in their day to day personal and professional lives. The Course aims to instill moral and social values as well as professional code of conduct in the students to make them good quality professionals so as to perform their professional responsibilities better in their future career.
8	**Brief Contents**	Definitions of Ethics, Engineering Ethics, and Morality. Categorization of Ethics, Differentiation of Morality and Ethics, Ten personal ethical behaviors which are globally acceptable, Definition of virtues, Elaboration of cardinal virtues, Definition of human values, Shalome H Shwartz value classification with examples; Definition of Profession and Professional, Responsibilities of professionals, the objectives of any one professional association, ACM Code of Ethics and Professional Conduct, IEEE Code of Ethics; Significance of ethics in ICT sector, Global Ethical Issues in ICT Sector with examples, Definitions of CSR, The stakeholders and their expectations from an organization, The Company Act 2013, Benefits of CSR in organization, Examples of CSR in ICT sector; Definition of Emotional intelligence, Importance of Emotional intelligence for Professionals, Five elements of Emotional intelligence, Significance of EI for professional success with examples, Ethical Dilemmas, Main features of Whistle Blowing, Preparation for Professionals and CEOs for avoiding unethical issues in their organizations
9	**Contents for lab**	Not Applicable
10	**List of text books/references**	1.Professional Ethics by R.Subramanian, Oxford University Press, 2013 2. Working with Emotional Intelligence by Daniel Goleman, Bloomsbury, 2004

Semester – II

1	**Code of the subject**	MTIS-6201
2	**Title of the subject**	Information Security Risk Management
3	**Any prerequisite**	Basic knowledge of internet technologies
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Debanjan Sadhya
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	• Manage risks associated with the use of information technology. • Identify and assess risks to the confidentiality, integrity, and availability of an organization's assets. • Treat risks in accordance with an organization's overall risk tolerance.
8	**Brief Contents**	Development of concepts required for risk-based planning and risk management of computer and information systems (Risk analysis, risk perception, Communicating risk, risk mitigation); Objectives and methods for vulnerability assessment for natural disaster, technological hazards, and terrorist threats; implications for emergency response, vulnerability of critical infrastructures. Overview of the course, history of information security, terminology, goals of information security, critical characteristics of information, the CIA model, controls; Cryptography basics- One Time Pad (OTP), perfect secrecy, public key cryptography, block ciphers, stream ciphers, private key cryptography, RSA, El-Gamal, Diffie-Hellman key exchange protocol, Hash functions; Threat analysis- Objectives of threat analysis, aspects of threats, threat vectors, threat source and targets, Trojan programs (including RATs), viruses, worms, Advanced Persistent Threats (APT), manual attack (packet sniffing), Man-in-the-middle attacks (ARP poisoning, MAC flooding, DHCP poisoning); Risk analysis- What is risk analysis, objectives, formal definition of risk, quantitative approach, qualitative approach, Risk Management Plan; Web Application Security: OWASP, Common Issues in Web Apps, What is XSS,SQL injection, CSRF, Password Vulnerabilities, SSL, CAPTCHA, Session Hijacking, Local and Remote File Inclusion, Audit Trails, Web Server Issues; Windows and Linux security, Types of Audits in Windows Environment: Server Security, Active Directory (Group Policy), Anti-Virus, Mails, Malware, End point protection, Shadow Passwords, SUDO users.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. "Information Security", Mark Rhodes-Ousley, *McGraw Hill Education (Indian) Private Limited*, 2013. 2. "Information Security: Principles and Practices", Mark S. Merkow, Jim Breithaupt, *Pearson*, 2006 3. "Introduction to Information Security I" (NPTEL Course), V. Kamakoti. (https://nptel.ac.in/courses/106106129/2)

1	**Code of the subject**	MTIS-6202
2	**Title of the subject**	Data Mining and Machine Learning
3	**Any prerequisite**	Data Structures, Algorithms, Linear Algebra, and Probability and Statistics
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Prof. Pramod Kumar Singh
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	• Learning information hidden in the heap of data and convert it into useful knowledge to develop applications. • Make computer to learn from data and take appropriate decision accordingly without any human intervention.
8	**Brief Contents**	**Introduction to Data, Data Mining, and Data Preprocessing:** Basics, Kinds of Data for Mining, Kinds of Pattern Mining; Data: Data Objects and Attributes Types, Basic Statistical Descriptions, Visualization, Similarity and Dissimilarity Measures. Preprocessing: Overview, Data Cleaning, Data Integration, Data Reduction, and Data Transformation and Data Discretization; **Mining Frequent Patterns, Associations, and Correlation:** Basic Concepts, Frequent Itemset Mining Methods, Interestingness of patterns, Pattern Mining in Multilevel, Multidimensional Space, Constraint-Based Frequent Patten Mining, Mining High-Dimensional Data; **Classification:** Basic Concepts, Decision Tree Induction, Bayes Classification Methods, Rule-Based Classification, Model Evaluation and Selection, Improvement in Classification Accuracy, Classification Using Frequent Patterns, Lazy Learners, Classification Methods based on Genetic Algorithm, Rough Set, Fuzzy Set, and Support Vector machine, Classification by Backpropagation; **Clustering:** Basic Concepts, Partitioning Methods, Hierarchical Methods, Density-Based Methods, Grid-Based Methods, Evaluation of Clustering, Probabilistic Model-Based Clustering, Clustering High-Dimensional Data, Clustering Graph and Network Data; **Machine Learning:** Basic Concepts, Unsupervised Learning, Supervised learning, Combining Multiple Learners, Reinforcement Learning; **Design and Analysis of Machine Learning Experiments:** Introduction and Basic concepts, Cross-validation and Resampling Methods, Hypothesis Testing, Assessing Classification Algorithm's Performance, Comparing Two Classification Algorithms, Comparing Multiple Algorithms, Comparison over Multiple Datasets, Multivariate Tests.
9	**Contents for lab (If applicable)**	Lab course is separate.
10	**List of text books/references**	1. Data Mining: Concepts and Techniques, Jiawei Han, Micheline Kambar, and Jian Pei, Morgan Kaufmann, 2011 2. Introduction to Data Mining, Pang-Ning Tan, Michael Steinbach, and Vipin Kumar, Pearson, 2016 3. Introduction to Machine Learning, Ethem Alpaydin, PHI, 2014 4. Machine Learning, Tom M Mitchell, McGraw Hill, 1997.

1	**Code of the subject**	MTIS-6203
2	**Title of the subject**	Formal Techniques for Software Reliability
3	**Any prerequisite**	Engineering Mathematics and Probability & Statistics
4	**L-T-P**	3-1-0
5	**Name of the proposer**	Dr Ajay Kumar
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	To teach the application of mathematics and statistics in software reliability and quality.
8	**Brief Contents**	**Introduction:** The need for system software reliability, software-related problems, software reliability engineering, future problems in the twenty-first century; **System Reliability Concepts:** Reliability measures, common distribution functions (Binominal, Poisson, Exponential, memorylessness, Normal, log-normal, Weibull, Gama, Beta, Parato, and Rayleigh), Poisson process and NHPP; **Theory of Estimation:** Maximum likelihood estimation, goodness of fit, least square estimation and linear regression, **Software Development Lifecycle:** Software vs hardware reliability, software reliability and testing concepts, software lifecycle, software development process and its applications, software verification and validation, data analysis, failure data sets; **Software Reliability Modeling:** Halstead's software metric, McCabe's cyclomatic complexity metric, error seeding models, failure rate models, curve fitting models, reliability growth models, Non-homogeneous Poisson process models; **NHPP Perfect-debugging Models:** NHPP Exponential Models, NHPP Exponential Models, NHPP Imperfect Debugging Models, NHPP Imperfect Debugging S-shaped Models, Software release time determination.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. Pham, Hoang. System software reliability. Springer Science & Business Media, 2007. 2. R. Subburaj, Software Reliability Engineering, McGraw Hill Education. 3. Kan, Stephen H. Metrics and models in software quality engineering. Addison-Wesley Longman Publishing Co., Inc., 2002.

1	**Code of the subject**	MTHS-6201
2	**Title of the subject**	Research Methodology
3	**Any prerequisite**	No
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Prof. Pankaj Srivastava
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	To enable researchers (Ph.D., MTech students), irrespective of their discipline, in developing the most appropriate methodology for their research studies. To make them familiar with the art of using different research methods and techniques
8	**Brief Contents**	**Research fundamentals:** Research, types of research, Research vs research methods, Research process, Relevant and quality research. Problem-solving in engineering, Identification of research topic, Problem definition, Literature survey, literature survey, Literature review, Research Design; **Mathematical modelling and simulation:** Models in general, Mathematical models, Model classifications, Modeling of engineering systems Theoretical models, Empirical models, Model evaluation, Limitations of mathematical models. Simulation models, Steps in a simulation study, Simulation software, Validation and data collection, Applications; **Hypothesis testing, analysis and scaling techniques:** Formulation of Hypothesis, Testing of hypothesis, Analysis of variance, Design of experiments, Multivariate analysis, Simple regression and correlation, measurement & scaling techniques; **Analysis and interpretation of data:** Data checking, Data analysis, Statistical, Graphical and Numerical data analysis, Interpretation of results in research , need for Interpretation, Accuracy, Precision, Uncertainty and variability, Repeatability and reproducibility, Error definition and classification, Analysis of errors, Statistical analysis of errors; **Skills and ethics in research:** Basic communication model, Preparing papers for journals, synopsis of research work, Reference citation, Listing of References. Thesis writing, Steps in writing the report, presentation of graphs, figures, tables, Structure of thesis report, main body of thesis, summary, references, Evaluation of a thesis, Ethics in research, Intellectual property rights, copyright laws, Patent rights.
9	**Contents for lab (If applicable)**	Introduction to LaTex document prepration Practical applications of SPSS, ANOVA Applications and case studies of parametric and non-parametric tests
10	**List of text books/references**	1. Research Methodology- C R Kothari, New Age International, 2019 2. Research Methodology: A step by step guide for beginners- Ranjit Kumar, Sage Publications, 2005. 3. Guide to Research & Documentation- Kirk G. Rasmussen, Prentice Hall, 2003 4. Research Methods- R. Panneerselvan, Prentice Hall, 2010 5. Research Methodology for Engineers- R Ganeshan, MJP Publishers, 2011

1	**Code of the subject**	MTIS-6204
2	**Title of the subject**	Data Mining and Machine Learning Laboratory
3	**Any prerequisite**	Data Structures, Algorithms, Linear Algebra, and Probability and Statistics
4	**L-T-P**	0-0-2
5	**Name of the proposer**	Prof. Pramod Kumar Singh
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	• Practical implementation of Data Mining and Machine Learning algorithms in a language of choice, e.g., Python, R. • Learning software tools and packages to implement Data Mining and Machine Learning algorithms.
8	**Brief Contents**	Assimilation with software tools and packages to implement Data Mining and Machine Learning algorithms along with direct implementation using a language of choice, e.g., Python, R.
9	**List of text books/references**	1. Data Mining: Concepts and Techniques, Jiawei Han, Micheline Kambar, and Jian Pei, Morgan Kaufmann, 2011 2. Introduction to Data Mining, Pang-Ning Tan, Michael Steinbach, and Vipin Kumar, Pearson, 2005 3. Introduction to Machine Learning, Ethem Alpaydin, PHI, 2015 4. Python Crash Course: A Hands-On, Project-Based Introduction to Programming, Eric Matthes, No Starch Press, 2019 5. R for Data Science: Import, Tidy, Transform, Visualize, and Model Data, Hadley Wickham and Garrett Grolemund, O'reilly, 2017.

Semester – III

1	**Code of the subject**	MTIS-7101
2	**Title of the subject**	Technical Report Writing
3	**Any prerequisite**	-
4	**L-T-P**	0-0-2
5	**Name of the proposer**	Dr. Arun Kumar
6	**Will this course require visiting faculty**	Yes
7	**Learning Objectives of the subject (in about 50 words)**	• To learn written communication skills in the wake of present day professional world • To enhance the understanding of written communication with practice oriented approach • To collect, analyze and report data • To familiarize with grammar and usage • To acquire higher order writing skills through project assignments
8	**Brief Contents**	Fundamentals of communication; Elements of Report writing; Types of reports such as memo, corrigendum; Technical reports; Sources of data; Data analysis; Illustrating data; Mechanics of writing; Report structure; Oral presentation; Issues related to plagiarism and ways to counter the same.
9	**Contents for lab (If applicable)**	• Data Analysis • Report writing • Report presentation
10	**List of text books/references**	1. Sharma, R.C. and K. Mohan, Business Correspondence and Report Writing, Tata McGraw Hill, 5th edition, 2016. 2. Gerson, Sharon J and Stern M. Gerson, Technical Writing: Process and Product, Pearson, 3rd edition, 2000

1	**Code of the subject**	MTIS-7101
2	**Title of the subject**	Seminar
3	**Any prerequisite**	N/A
4	**L-T-P**	0-0-2
5	**Name of the proposer**	Dr. Debanjan Sadhya
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	This course is intended for students pursuing post-graduation in the specialized area of information security. Students will have to choose a recent topic in security related areas (or industry practices) and prepare a write up along with suitable presentation and demonstration.
8	**Brief Contents**	Emerging /recent research topics of significance is taken as a study and written report along with presentation.
9	**Contents for lab (If applicable)**	N/A
10	**List of text books/references**	

1	**Code of the subject**	MTIS-7199
2	**Title of the subject**	Major Project Part-I
3	**Any prerequisite**	Academic honesty, ethics and a deeper understanding of the topic under research
4	**L-T-P**	0-0-12
5	**Name of the proposer**	Dr. K. K. Pattanaik
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	The course will help understand the system level details of the Internetworking technology, issues, and approaches.
8	**Brief Contents**	The purpose of this course is to enable the student to develop deeper knowledge, understanding, capabilities and attitudes in the context of the programme of study. Specific learning outcomes for a Master's thesis are for the student to demonstrate: • Considerably more in-depth knowledge of the major subject/field of study, including deeper insight into current research and development work. • Deeper knowledge of methods in the major subject/field of study. • A capability to contribute to research and development work. • The capability to create, analyse and critically evaluate different technical/architectural solutions. • The capability to clearly present and discuss the conclusions as well as the knowledge and arguments that form the basis for these findings in written and spoken English. • A consciousness of the ethical aspects of research and development work. Overall a Master's thesis for a 12 credit course must be considerably more ambitious with respect to the scientific level or technical/architectural realisation.
9	**Contents for lab (If applicable)**	Not applicable.

Semester - IV

1	**Code of the subject**	MTIS-7299
2	**Title of the subject**	Major Project Part-II
3	**Any prerequisite**	Academic honesty, ethics and a deeper understanding of the topic under research
4	**L-T-P**	0-0-24
5	**Name of the proposer**	Dr. K. K. Pattanaik
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	The course will help understand the system level details of the Internetworking technology, issues, and approaches.
8	**Brief Contents**	This shall be in continuation to the Major Project Part-I. A thesis should be written at the end of the programme and must delve more deeply into and synthesise knowledge acquired in previous studies. A thesis for M.Tech. should place emphasis on the technical/scientific/artistic aspects of the subject matter.
9	**Contents for lab (If applicable)**	Not applicable
10		

Electives (Application Security) for M.Tech IS

1	**Code of the subject**	MTIS-9101
2	**Title of the subject**	Secure Software Systems
3	**Any prerequisite**	Basic course of software engineering
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Santosh Singh Rathore
6	**Will this course require visiting faculty**	Yes
7	**Learning Objectives of the subject (in about 50 words)**	• To explore the foundations of software security. • To apply contemporary formal mathematical modeling techniques to model and analyse the security of a software system. • To understand techniques at each phase of the development cycle that can be used to strengthen the security of software systems.
8	**Brief Contents**	Introduction to secure software system, Buffer overflow; Requirements: abuse & misuse cases, security requirements; Planning: risk assessment, Protection Poker OS command injection & Hardcoded credentials; Design: secure design patterns, test planning, Design: architectural risk & threat modeling; Implementation: defensive coding practices, Web applications, Cross-Site Request Forgery, Code Inspections, File system permissions; Cryptography: authentication, public-key, symmetric key, SSH Activity, Hashing salt; Deployment & Distribution: patching, security managers, Java security manager Java reflection, Black box testing; Low level security: Memory layout, code injection, other memory exploits, format string vulnerabilities.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. Gary McGraw, “Software Security: Building Security”, Addison-Wesley, ISBN 978-321-35670-3, 2006. 2. Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, and Nancy Mead. Addison-Wesley, “Software Security Engineering: A Guide for Project Managers”, ISBN 978-0-32-150917-8, 2008. 3. Charles P. Pfleeger and Shari Lawrence Pfleeger, “Analyzing Computer Security”, Prentice Hall, Upper Saddle River, NJ, 2011. ISBN 978-0-13-278946-2.

1	**Code of the subject**	MTIS-9102
2	**Title of the subject**	Database Security
3	**Any prerequisite**	Database management system
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Debanjan Sadhya
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	• Learn techniques to protect databases against compromises of their confidentiality, integrity and availability. • Explain the place of database security in the context of security analysis and management. • Apply the security concepts relevant to database systems.
8	**Brief Contents (module wise)**	Database design and use of DBMS, Relational models and Relational algebra and design principles, network models, object-oriented design, transaction processing, Datalog, temporal databases, advanced topics from data warehousing, knowledge discovery, data mining, middleware etc. Introduction: Overview of the course, what is database security, database privacy, the CIA model, and security threats (accidental and deliberate); Fundamentals of access control: Physical security, information system access control, authorization, identification, authentication, accountability; Database access control: Access control matrix, use of views, security logs and audit trails, SQL data control language (authorization graphs); Security mechanisms: Symmetric key encryption, public key encryption, Statistical database security, SQL injection; Database security and the internet: Proxy servers, firewalls, digital signatures, certification authorities (SSL, Kerberos); Privacy preservation: What is database privacy, micro-databases, need for privacy, linking attacks, k-anonymity, l-diversity, t-closeness.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. “Database Design and Development: An Essential Guide for IT Professionals”, Paulraj Ponniah, *John Wiley and Sons*, 2012 2. "Introduction to Database Security (chapter 8)”, Catherine M. Ricardo, Susan D. Urban, Databases Illuminated (Book), *Jones & Bartlett Learning*, 2015 3. "Handbook of Database Security - Applications and Trends”, Michael Gertz, Sushil Jajodia, *Springer*, 2008

1	**Code of the subject**	MTIS-9103
2	**Title of the subject**	Web Architecture Security
3	**Any prerequisite**	Information Security
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Debanjan Sadhya
6	**Will this course require visiting faculty**	Yes
7	**Learning Objectives of the subject (in about 50 words)**	• Get an overview of web applications and its history, benefits, drawbacks, future. • Look at the emerging Web services architecture and take a first pass at identifying some of the major soft spots. • Be aware of the vulnerabilities of web applications. • Get a clear understanding of the flaws, myths and best practices for WAS.
8	**Brief Contents**	Web security model - Browser security model including same-origin policy, Client-server trust boundaries, e.g., cannot rely on secure execution in the client Session management, Application vulnerabilities and defenses- SQL injection, XSS, CSRF Client-side security - Cookies security policy, HTTP security extensions, e.g. HSTS, Plugins, extensions, and web apps, Web user tracking Server-side security tools, e.g. Web Application Firewalls (WAFs) and fuzzers Major Browser Attacks. Introduction to Web services architecture, Service oriented architecture and distributed systems; The architectural models: policy model, service oriented model, resource oriented model, message oriented model; Web Applications and IT Infrastructure essentials: explain how a web application works (http, cookies, session affinity etc.), middleware components part of the application chain, TCP/IP transport protocol and the BGP protocol, the HTTP protocol and session management; Security controls offered by SSL/TLS and identify the steps for a successful SSL/TLS handshake, symmetric and asymmetric encryption, understand why certificate management is vital; High Availability, Operational Management and Application Chains: Understand the different levels of high availability, latency; Recovery Time Objective (RTO) and Recovery Point Objective (RPO), horizontal and vertical scaling.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. "Designing Security Architecture Solutions", Jay Ramachandran, *Wiley*, 2007 2. " Web Application Security, A Beginner's Guide" Bryan Sullivan, Vincent Liu, *McGraw Hill*, 2011 3. Web Services Architecture and Security (https://www.owasp.org/index.php/Web_Services_Architecture_and_Security).

1	**Code of the subject**	MTIS-9104
2	**Title of the subject**	Computer Security Audit and Assurance
3	**Any prerequisite**	Introduction to Computer and Network Security
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Saumya Bhadauria
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	It is designed to introduce the terminology, technology and its applications, which enable a clear understanding of the difference between Security Metrics and Audits. and to introduce the tools, technologies used in day to day security analysis.
8	Brief Contents (module wise)	Security Policy frameworks: practices, and procedures, business practice disclosures, Policy authority and practices, information security practices, personal and physical security practices, operation management practices, PKIs and key management schemes, key generation, key storage, backup, recovery and distribution, XML frameworks for security policy specification, certificate management life cycle. Information Security Performance Metrics and Audit: Introduction to Security Audit, Information Security Methodologies (Black-box, White-box, Greybox), Phases of Information Security Audit and Strategies; Vulnerability Management: Information Security Vulnerabilities – Threats and Vulnerabilities, Human-based Social Engineering, Computer-based Social Engineering, Social Media Countermeasures; Information Security Assessments: Vulnerability Assessment, Classification, Types of Vulnerability Assessment, Vulnerability; Assessment Phases.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. Assessing Information Security: Strategies, Tactics, Logic and Framework. by Andrew Vladimirov, Konstantin Gavrilenko , Andrei Michajlowski , IT Governance Publishing, 2011 2. Information Security Management Handbook, Volume 6, 16 Nov 2016 by Harold F. Tipton , Micki Krause Nozaki 3. Michael E. Whitman, Herbert J. Mattord, Management of Information Security, 5th Edition, Course Technology, 2016.

1	**Code of the subject**	MTIS-9105
2	**Title of the subject**	Secure Enterprise Computing
3	**Any prerequisite**	
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Pinku Ranjan
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	• This course covers the computing background for large-scale enterprise computing, including the out-sourcing of computing to the cloud. • Web applications in the cloud: ASP.NET and Windows Azure. • Enterprise Web services: Windows Communication Foundation (WCF) and the Web Services stack.
8	**Brief Contents (module wise)**	Introduction to enterprise and cloud computing: SaaS, PaaS, IaaS. Introduction to Windows Azure and Amazon EC2; Server-side processing: ASP.NET MVC ASP; Application architectures and database storage. Entity Framework and Language in Query (LINQ); Web server security. Authentication and authorization. Threats and defenses: SQL injection, XSS, CSRF; Cloud storage: Blobs, NoSQL (Tables) and Relational (SQL Database). CDNs; Services and Contracts. Web services for B2B E-commerce: SOAP, WSDL, WS-Policy. Example: Google Adwords. WCF contract languages; Web Services: WCF sessioning and design patterns. WCF concurrency control; Queues and Service Bus. WCF and Azure Service Bus security. Azure cloud services; NoSQL: MongoDB. MongoDB views MapReduce; Virtualization; Secure virtualization. KVM and SELinux. Type enforcement. SVirt; SELinux: Roles and MLS; Input-output virtualization. Data center design: virtualization and interconnection networks; Map-Reduce queries in MongoDB. Hadoop in Windows Azure. Web API.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. J. Galloway, P. Haack, B. Wilson, K.S. Allen, and D. Matson , [ASP] Professional ASP.NET MVC 5 , Wiley, 2014 2.K. Hwang, G. Fox, and J. Dongarra , [HFD] Distributed and Cloud Computing , Morgan Kaufmann, 2011 3.K. Chodorow , [M] MongoDB: The Definitive Guide , O'Reilly, 2013 4. S. Krishnan , [WA] Programming Windows Azure: Programming the Microsoft Cloud , O'Reilly, 2010 5. J. Lowry , [WCF] Programming WCF Services: Mastering WCF Services and the Azure AppFabric Bus , O'Reilly, 2011

1	**Code of the subject**	MTIS-9106
2	**Title of the subject**	Digital Watermarking & Steganalysis
3	**Any prerequisite**	No
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Prof. Mahua Bhattacharya
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	The objective of the course makes students familiar about Digital watermarking and steganography.
8	**Brief Contents**	**Introduction:** Information Hiding, Steganography, and Watermarking, Importance of Digital Watermarking, Steganography; **Applications and Properties:** Applications of Watermarking, Applications of Steganography, Properties of Watermarking Systems, Evaluating Watermarking Systems, Properties of Steganographic and Steganalysis Systems, Evaluating and Testing Steganographic Systems; **Models of Watermarking:** Communication-Based Models of Watermarking, Geometric Models of Watermarking, Modeling Watermark Detection by Correlation; **Basic Message Coding:** Mapping Messages into Message Vectors, Error Correction Coding, Detecting Multi-symbol Watermarks; **Watermarking with Side Information:** Informed Embedding, Watermarking Using Side Information, Dirty-Paper Codes; **Robust Watermarking:** Approaches, Robustness to Volumetric Distortions, Robustness to Temporal and Geometric Distortions; **Watermark Security:** Security Requirements, Watermark Security and Cryptography, Some Significant Known Attacks; **Content Authentication:** Exact Authentication, Selective Authentication, Localization, Restoration; **Steganography:** Notation and Terminology, Information-Theoretic Foundations of Steganography, Practical Steganographic Methods, Minimizing the Embedding Impact; **Steganalysis:** Steganalysis Scenarios, Some Significant Steganalysis Algorithms.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. Digital Watermarking and Steganography, Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, Morgan Kauffman, 2007 2. Digital Watermarking principles, Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Morgan Kauffman, 2007

1	**Code of the subject**	MTIS-9107
2	**Title of the subject**	Advanced Distributed System Security
3	**Any prerequisite**	Introduction to Computer and Network Security, Operating Systems, DataBase Systems
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Saumya Bhadauria
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	To learn the state of the art and open problems in networks and distributed systems security and privacy
8	**Brief Contents**	Access control systems, Hardware and software capability systems; Security of the Internet infrastructure; Distributed systems: introduction to distributed systems, client/server and peer2peer model, standard protocol, methods for large systems, scaling and load-balancing; Cloud computing security/privacy.
9	**Contents for lab (If applicable)**	NIL
10	**List of text books/references**	1. William Stallings and Lawrie Brown. 2014. Computer Security: Principles and Practice (3rd ed.). Prentice Hall Press, Upper Saddle River, NJ, USA. 2. Trent Jaeger. 2008. Operating System Security (1st ed.). Morgan and Claypool Publishers. 3. Dollimore J, Kindberg T, Coulouris G (2005), Distributed Systems: Concepts and Design. 4 edition. Addison Wesley (944 p).

1	**Code of the subject**	MTIS-9108
2	**Title of the subject**	Analysis and Verification of Cryptographic Protocols
3	**Any prerequisite**	Introduction to Computer and Network Security, Cryptography
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Saumya Bhadauria
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	To study the building blocks used in cryptographic protocols, and the operations of mainstream cryptographic protocols used in computer networks
8	**Brief Contents**	Formal Notions of Attacks, Public key ciphers; Digital signatures, Key exchange protocols, and password based key derivation, Random number generation and public key infrastructure; Crypto protocols for resource constrained networks, Cryptographic obfuscation , Crypto protocols for enhancing privacy.
9	**Contents for lab (If applicable)**	NIL
10	**List of text books/references**	1. Hans Delfs, Helmut Knebl, "Introduction to Cryptography, Principles and Applications", Springer Verlag, 2007 2. Wenbo Mao, "Modern Cryptography, Theory and Practice", Pearson Education, 2016 3. N. Ferguson, B. Schneier, and T. Kohno, Cryptography Engineering, Wiley, 2010. 4. A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

1	**Code of the subject**	MTIS-9109
2	**Title of the subject**	Game Theory and its Application
3	**Any prerequisite**	Basic knowledge of Engineering Mathematics and Statistics
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr Ajay Kumar
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	To teach the applications of game theory, auction and equilibrium.
8	**Brief Contents**	Introduction to Game Theory, Dominant Strategies and Nash Equilibrium, Alternate Strategies: Maximin, Maximax, and Minimax Regret Solvability, N-Player Games, Mixed Strategy Nash Equilibria, Subgame Perfection in Discrete Choice Games, Continuous Games and Imperfect Competition, Infinitely Repeated Games, Tacit Collusion: An application of Infinites Repeated Games, imperfect Information: Simultaneous-play, ayesian Games, Applications of Bayesian Games: Auctions and Voting, Cournot's Duopoly with Imperfect Information 3.Radio Spectrum, With Arbitrary Distribution of Valuations, Extensive Form Game with Perfect Information, Stackelberg Model of Duopoly, Buying Votes, Committee Decision-Making, Repeated games, The Prisoner's Dilemma, General Result, Supermodular Game and Potential Game, Supermodular Game and Potential Game, Wireless Networks: Resource Allocations, Admission Control, Routing in Sensor and Ad-Hoc Networks, Modeling Network Traffic and Strategic Network Formation, Rubinstein Bargaining Model with Alternating Offers, Nash Bargaining Solution, Relation of Axiomatic and Strategic Model, Auction and Mechanism Design with Applications, Revenue Equivalence, Risk Averse Bidders, Asymmetries among Bidders, Mechanism, Optimal Mechanism.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. Martin Osborne, An Introduction to Game Theory, Oxford University Press, 2003 2. Prajit Dutta, Strategies and Games, MIT Press, 1999 3. K H Ericson, Game Theory, Createspace Independent Publishing Platform, 2013

1	**Code of the subject**	MTIS-9110
2	**Title of the subject**	Computational Number Theory
3	**Any prerequisite**	NIL
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr Anuraj Singh
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	• To develop a framework to understand and implement cryptographic algorithm. • To enhance an ability to analyze a problem, and identify and define the computing requirements appropriate to its solution. • To impart Number Theory concepts to understand Computational Complexity.
8	**Brief Contents**	Primes, Divisibility, Greatest common divisor, Euclidean algorithm, Fundamental theorem of arithmetic, Perfect numbers, Mersenne primes and Fermat numbers; Farey sequences. Congruence and modular arithmetic, Residue and reduced residue classes, Chinese remainder theorem, Fermat's little theorem; Wilson's theorem, Euler's theorem and its application to cryptography, Arithmetic functions; Möbius inversion formula, Greatest integer function. Primitive roots and indices, quadratic residues, Legendre symbol, Euler's criterion, Gauss's lemma, Quadratic reciprocity law, Jacobi symbol; Representation of an integer as a sum of two and four squares, Diophantine equations ax+by = c, $x^2 + y^2 = z^2, x^4 + y^4 = z^4$. Binary quadratic forms and Equivalence of quadratic forms.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. David M. Burton, Elementary Number Theory, Wm. C. Brown Publishers, Dubuque, 1994. 2. G.A. Jones and J.M. Jones, Elementary Number Theory, Springer-Verlag, 1998. 3. W. Sierpinski, Elementary Theory of Numbers, North-Holland, Ireland, 1988.

Electives (Security Analysis) for M.Tech IS

1	**Code of the subject**	MTIS-9201
2	**Title of the subject**	Design and Analysis of Secured Networked Systems
3	**Any prerequisite**	No
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Sunil Kumar
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	After successful completion of this course, students will able to understand basic concepts of cyber security and how it can be applied to identify vulnerabilities/threat in a network system. The course will also discuss about risk management framework for analyzing the risks in a network system, and how it can data in computer systems using basic cyber security principles.
8	**Brief Contents**	Course overview: Cyber-security Concepts and Security Principles; Factors of cyber attack, Principle for protecting data and secure the computer systems, Risk management framework and Authenticity; Protect Data Access and Verify Source of Trust - Principle of Least Privileges for Access Control; Unix file access mechanism, Adequate data protection; Enforcement Access Control; Sign and/or Verify Software - GPG software tool for generating public key private key pair, Public key vs Private key, Encryption algorithms, GnuPG software tool-apache and putty, Software-sign/listing/signature on website; Setup Secure Server and Client Certificate - Public Key Infrastructure (PKI, Operation of CA, Sign certificate request, Server certificate requests, Set up a client certificate for signing and encrypting emails.
9	**Contents for lab (If applicable)**	NA
10	**List of text books/references**	1. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010 2. Michael T. Goodrich and Roberto Tamassia,Introduction to Computer Security, Addison Wesley, 2011 3. Secure Session Management With Cookies for Web Applications. Chris Palmer 4. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress (Congressional Research Services report)

1	**Code of the subject**	MTIS-9202
2	**Title of the subject**	Cyber Security and IoT
3	**Any prerequisite**	NA
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Prasenjit Chanak
6	**Will this course require visiting faculty**	NA
7	**Learning Objectives of the subject (in about 50 words)**	The objective of this course is to acquaint participants with some of the fundamental concepts and state-of-the-art research in the areas of Cyber Security and IoT. This is a research oriented course. This course has no official prerequisites. However, it is implicitly expected that the registrants have already gone through the basic courses on mathematics. The outline of the course is given below
8	**Brief Contents**	**The course will be broad in nature and will include the following topics:** Stuxnet worm and its after effects in the Critical Infrastructure security; Consequent Presidential Executive Order for Securing Critical Infrastructure in 2013 and its impact: Policy Issues in Security of Critical Infrastructure; Security and Vulnerability of Cyber-Physical Infrastructures; Game Theory and other analytical modeling of the security problems of critical infrastructures; Security of the Networked Infrastructure; IoT definitions: overview, applications, potential & challenges; Competitive Landscape; IoT examples: Case studies. Sensor body-area- network, Control of a smart home, Smart Vehicles, Smart Manufacturing & Smart Factory; Architecture; Protocols; Performance Modeling & Analysis; Industrial IoT (IIoT) and the Industrial Internet Consortium (IIC); Introduction to IoT Security; Emerging IoT Standards; Open Problems & Research challenges.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. Handbook on Securing Cyber-Physical Critical Infrastructure, Sajal K. Das, Krishna Kant, Nan Zhang, Morgan Kaufmann (Elsevier), ISBN 978-0-12-415815-3, Publication: 2012. 2. Journal articles, conference papers, reports, advanced texts, and/or personal notes will be provided.

1	**Code of the subject**	MTIS-9203
2	**Title of the subject**	Cloud Security: Architecture and Technologies
3	**Any prerequisite**	No
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Debanjan Sadhya
6	**Will this course require visiting faculty**	Yes
7	**Learning Objectives of the subject (in about 50 words)**	• Learn techniques which provide on-demand computing service for shared pool of resources (servers, storage, networking, software, database, applications etc.) over the Internet. • Introduce various aspects of cloud computing, including fundamentals, management issues, security challenges and future research trends.
8	**Brief Contents**	Introduction: Basics of the cloud, On-premise vs Hosted solutions, Cloud service models, Types of clouds, Augmenting security with cloud services; Virtualization: The Deployment Model, How does storage work in Azure? Virtual Machine Types, Virtual Network capabilities; Redundancy: Backups, High Availability, Disaster Recovery, Virtual Machine Backups; Security: IaaS Security, Virtual Private Network (VPN), Azure Security Center (ASC) Dashboard, Data Security Considerations, Security Threats; Active directory: Active Directory in Azure, Role Based Access Control, Azure Active Directory Business to Business (B2B) and B2C, How to Sync on premises and cloud identity; Research trends.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. “Cloud Computing: Principles and Paradigms", Editors: Rajkumar Buyya, James Broberg, Andrzej M. Goscinski, *Wiley*, 2011 2. "Enterprise Cloud Computing - Technology, Architecture, Applications", Gautam Shroff, *Cambridge University Press*, 2010 3. "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Ronald L. Krutz, Russell Dean Vines, *Wiley- India*, 2010. 4. "Cloud computing" (NPTEL Course), Soumya Kanti Ghosh. (https://nptel.ac.in/syllabus/106105167/)

1	**Code of the subject**	MTIS-9204
2	**Title of the subject**	Public Key Infrastructure and managing E-Security
3	**Any prerequisite**	Computer Networks, Introduction to Computer and Network Security, Information Systems Security
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Saumya Bhadauria
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	• To enable the student to understand the foundational elements and complexity of a public key infrastructure • To explain the need for a rigorous identity management process and its role in a public key infrastructure
8	**Brief Contents**	Client side and server side authentication, E-Security Challenges, Symmetric/Asymmetric Cryptology Basics, Infrastructure Concepts; Public key infrastructure basics, kerberoes, X.509 authentication service, types of certificates, Federated Identity Management; IPSec, IKE, ISAKMP, PKI architectures, CRL, CRT, Online Certificate Status Protocol(OCSP); Nginx, OCSP Stapling, HTTP Pinning, Management Protocols required in PKIES.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. William Stallings and Lawrie Brown. 2014. Computer Security: Principles and Practice (3rd ed.). Prentice Hall Press, Upper Saddle River, NJ, USA. 2. PKI: Implementing & Managing E-Security. Andrew Nash, Derek Brink, William Duane, Celia A. Joseph McGraw Hill Professional, 17-Apr-2001. 3. Suranjan Choudhury, Kartik Bhatnagar, and Wasim Haque. 2002. Public Key Infrastructure Implementation and Design (1st ed.). John Wiley & Sons 4. Jan Camenisch and Costas Lambrinoudakis. 2011. Public Key Infrastructures, Services and Applications

1	**Code of the subject**	MTIS-9205
2	**Title of the subject**	Applied Cryptography
3	**Any prerequisite**	No
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Jeevaraj S
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	• To make the students understand the process of deciphering coded messages without being told the key. • To study of codes and the art of writing and solving them. • To give motivation towards recent research development in the field of cryptography, cryptanalysis, and steganography. • Overall this course explores modern cryptographic (code making) and cryptanalytic (code breaking) techniques in detail.
8	**Brief Contents**	Number Theory Basics: Modular arithmetic, Fields, Binary Fields, primes, GCD and Chinese reminder theorems, Extended Euclidean Algorithm, Fermat's Little Theorem, Euler Phi function; Block Ciphers in Mathematical way, DES, AES, ECB, CBC; Public Key Cryptography, RSA, Two fish, Bluefish, Lai-Massey scheme; Enigma Machine, ADFGVX Cipher, Play fair cipher, and other similar ciphers and their working (mathematical) methodologies; Crypt Analysis of various Ciphering Algorithms, Cryptocurrency; Recent Research development in the field of cryptography, cryptanalysis and steganography, , RC algorithms (RC2, RC4, etc.,).
9	**Contents for lab (If applicable)**	NA
10	**List of text books/references**	1. **''Cryptography: Theory and Practice"**, Third Edition, by Douglas R. Stinson, CRC Press, Taylor and Francis Group, 2005 2. **''Handbook of Applied Cryptography''**, Fifth Printing, by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, CRC Press, 2001 3. **''Cryptography and Network Security: Principles and Practices''**, Sixth Edition, by William Stallings, 2014 4. **"The Code Book- The secret history of Codes & Code-breaking"** by Simon Singh, 2010.

1	**Code of the subject**	MTIS-9206
2	**Title of the subject**	Information Systems Security Risk Analysis
3	**Any prerequisite**	Basic knowledge of internet technologies
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Debanjan Sadhya
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	• Manage risks associated with the use of information technology. • Identify and assess risks to the confidentiality, integrity, and availability of an organization's assets. • Treat risks in accordance with an organization's overall risk tolerance.
8	**Brief Contents**	**Introduction:** Overview of the course, history of information security, terminology, goals of information security, critical characteristics of information, the CIA model, controls; **Cryptography basics**- One Time Pad (OTP), perfect secrecy, public key cryptography, block ciphers, stream ciphers, private key cryptography, RSA, El-Gamal, Diffie-Hellman key exchange protocol, Hash functions; **Threat analysis**-Objectives of threat analysis, aspects of threats, threat vectors, threat source and targets, Trojan programs (including RATs), viruses, worms, Advanced Persistent Threats (APT), manual attack (packet sniffing), Man-in-the-middle attacks (ARP poisoning, MAC flooding, DHCP poisoning); **Risk analysis**- What is risk analysis, objectives, formal definition of risk, quantitative approach, qualitative approach, Risk Management Plan; **Web Application Security**: OWASP, Common Issues in Web Apps, What is XSS,SQL injection, CSRF, Password Vulnerabilities, SSL, CAPTCHA, Session Hijacking, Local and Remote File Inclusion, Audit Trails, Web Server Issues; **Windows and Linux security**-Types of Audits in Windows Environment: Server Security, Active Directory (Group Policy), Anti-Virus, Mails, Malware, End point protection, Shadow Passwords, SUDO users.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. "Information Security", Mark Rhodes-Ousley, *McGraw Hill Education (Indian) Private Limited*, 2013 2. "Information Security: Principles and Practices", Mark A. Merkow, Jim Breithaupt, *Pearson*, 2014 3. "Introduction to Information Security I" (NPTEL Course), V. Kamakoti. (https://nptel.ac.in/courses/106106129/2)

1	**Code of the subject**	MTIS-9207
2	**Title of the subject**	Malware Analysis
3	**Any prerequisite**	Computer Organization, Computer Architecture, Networks, and Operating Systems, and memory layout of programs; be able to understand x86 and other assembly; a general understanding of computer security.
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Prof. Shashikala Tapaswi
6	**Will this course require visiting faculty**	As expert lectures
7	**Learning Objectives of the subject (in about 50 words)**	The increasingly networked nature of the modern world has also enabled th e spread of malicious software, or "malware", ranging from annoying adware to advanced nation-state sponsored cyber-weaponry. As a result, the ability to detect, analyze, understand, control, and eradicate malware is an increasin gly important issue of economic and national security. This course will intr oduce students to modern malware analysis techniques through readings a nd hands-on interactive analysis of real-world samples. After successful completion of this course students will be equipped with the skills to analyze advanced contemporary malware using both static and dynamic anal ysis. Focus on executable binaries, object file formats, and the use of tools such as debuggers, virtual machines, and disassemblers. Obfuscation and packing schemes will be discussed, along with various issues related to Windows internals.
8	**Brief Contents**	Introduction to malware, Basic Static and Dynamic Analysis, Overview of Windows file format, PEView.exe, Patching Binaries , Disassembly(objdump, IDA Pro), Introduction to IDA, Introduction to Reverse Engineering, Extended Reverse Engineering using GDB and IDA, Advanced Dynamic Analysis - debugging tools and concepts, Malware Behavior - malicious activities and techniques, Knowledge of relevant system internals, and experience in using various malware analysis tools Analyzing Windows programs – WinAPI, Handles ,Networking , COM, Data Encoding, Malware Countermeasures , Covert Launching and Execution, Anti Analysis - Anti Disassembly, VM, Debugging -, Packers – packing and upacking, Intro to Kernel – Kernel basics, Windows Kernel API, Windows Drivers, Kernel Debugging, Rootkit Techniques- Hooking, Patching, Kernel Object Manipulation , Rootkit Anti-forensics , Covert analysis.
9	**Contents for lab (If applicable)**	"Hands on" students may bring their laptops to class session.
10	**List of text books/references**	1. "Practical Malware Analysis" by Michael Sikorski and Andrew Honig, ISBN: 1593272901, No Starch Press,2012 2. "The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the Sys tem" , Second Edition by Reverend Bill Blunden, 2009 3. "Rootkits: Subverting the Windows Kernel" by Jamie Butler and Greg H oglund, 2005 4. "Practical Reverse Engineering" by Dang, Gazet, Bachaalany, Wiley, 2014 5. "The IDA PRO Book: The Unofficial Guide to the World's Most Popular Disassembler, 2nd Edition" by Chris Eagle (published by No Starch Press, 2011)

1	**Code of the subject**	MTIS-9208
2	**Title of the subject**	Privacy and Security for online Social Networks
3	**Any prerequisite**	No
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Prasenjit Chanak
6	**Will this course require visiting faculty**	NA
7	**Learning Objectives of the subject (in about 50 words)**	With increase in the usage of the Internet, there has been an exponential increase in the use of online social media and networks on the Internet. Websites like Facebook, YouTube, LinkedIn, Twitter, Flickr, Instagram, Google+, FourSquare, Pinterest, Tinder, and the likes have changed the way the Internet is being used. However, widely used, there is a lack of understanding of privacy and security issues on online social media. Privacy and security of online social media need to be investigated, studied and characterized from various perspectives (computational, cultural, psychological, etc.). Student completing the course will be able to appreciate various privacy and security concerns (spam, phishing, fraud nodes, identity theft) on Online Social Media and Student will be able to clearly articulate one or two concerns comprehensively on one Online Social Media, this will be achieved by homework.
8	**Brief Contents**	What is Online Social Networks, data collection from social networks, challenges, opportunities, and pitfalls in online social networks, APIs; Collecting data from Online Social Media; Trust, credibility, and reputations in social systems; Trust, credibility, and reputations in social systems; Online social Media and Policing; Information privacy disclosure, revelation and its effects in OSM and online social networks; Phishing in OSM & Identifying fraudulent entities in online social networks.
9	**Contents for lab (If applicable)**	**NA**
10	**List of text books/references**	1. Research articles from the ACM and IEEE digital libraries.

Electives (Cyber Threat Intelligence) for M.Tech IS

1	**Code of the subject**	MTIS-9301
2	**Title of the subject**	Cyber Threat Intelligence
3	**Any prerequisite**	Basics of Network Security and Internet
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Sunil Kumar
6	**Will this course require visiting faculty**	Yes
7	**Learning Objectives of the subject (in about 50 words)**	The course objective is to designed and developed a cybersecurity and threat intelligence system to help organizations to identify and mitigate business risks by converting unknown (internal and external) threats into known threats. It is a high-level program that teaches a hierarchical approach for building effective threat intelligence system
8	**Brief Contents**	Introduction of the course - What is cybercrime? What is not cybercrime? What is cyber threat intelligence? TTPs, and Hacktivism; Computer Network Exploitation (CNE) - its purpose. Insiders - Types of insiders pose cyber threats; Cyber-security - How can physical security affect cyber security; physical security vs cyber security; Critical Infrastructure and Key Resources (CIKR), Effect of cyber activity on CIKR; Disruptive and emerging technologies; Effect of biases, mindsets, assumptions, and uncertainty on our assumption. Cyber Ethics; Is back-tracking/back-hacking ethical? What are the ethics of victim notification?
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010 2. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress (Congressional Research Services report) 3. http://www.dni.gov/files/documents. 4. https://www.albany.edu/rockefeller/syllabi/fall2015/2015 5. https://www.udemy.com/level-1-intelligence-analyst-certification/ 6. https://www.first.org/global/sigs/cti/curriculum/training

1	**Code of the subject**	MTIS-9302
2	**Title of the subject**	Cyber Forensics Technologies and Requirements
3	**Any prerequisite**	No
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Prasenjit Chanak
6	**Will this course require visiting faculty**	NA
7	**Learning Objectives of the subject (in about 50 words)**	The objective of this course is to acquaint participants with some of the fundamental concepts and state-of-the-art research in the areas of Cyber Forensics Technologies and Requirements. This course has no official prerequisites. However, it is implicitly expected that the registrants have already gone through the basic courses on mathematics. The outline of the course is given below
8	**Brief Contents**	**Computer Forensics Fundamentals:** What is Computer Forensics?, Use of Computer Forensics in Law Enforcement, Computer Forensics Assistance to Human Resources/Employment Proceedings, Computer Forensics Services, Benefits of Professional Forensics Methodology, Steps taken by Computer Forensics Specialists Types of Computer Forensics Technology: Types of Military Computer Forensic Technology, Types of Law Enforcement — Computer Forensic Technology — Types of Business Computer Forensic Technology Computer Forensics Evidence and Capture: Data Recovery Defined — Data Back-up and Recovery — The Role of Back-up in Data Recovery — The Data-Recovery Solution.; **Evidence Collection and Data Seizure:** Why Collect Evidence? Collection Options — Obstacles — Types of Evidence — The Rules of Evidence — Volatile Evidence — General Procedure — Collection and Archiving — Methods of Collection — Artifacts — Collection Steps — Controlling Contamination: The Chain of Custody Duplication and Preservation of Digital Evidence: Preserving the Digital Crime Scene — Computer Evidence Processing Steps — Legal Aspects of Collecting and Preserving Computer Forensic Evidence Computer Image Verification and Authentication: Special Needs of Evidential Authentication — Practical Consideration —Practical Implementation; **Computer Forensics analysis and validation:** Determining what data to collect and analyze, validating forensic data, addressing data-hiding techniques, performing remote acquisitions Network Forensics: Network forensics overview, performing live acquisitions, developing standard procedures for network forensics, using network tools, examining the honeynet project. Processing Crime and Incident Scenes: Identifying digital evidence, collecting evidence in private-sector incident scenes, processing law enforcement crime scenes, preparing for a search, securing a computer incident or crime scene, seizing digital evidence at the scene, storing digital evidence, obtaining a digital hash, reviewing a case; **Current Computer Forensic tools:** evaluating computer forensic tool needs, computer forensics software tools, computer forensics hardware tools, validating and testing forensics software E-Mail Investigations: Exploring the role of e-mail in investigation, exploring the roles of the client and server in e-mail, investigating e-mail crimes and violations, understanding e-mail servers, using specialized e-mail forensic tools. Cell phone and mobile device forensics: Understanding mobile device forensics, understanding acquisition procedures for cell phones and mobile devices; **Working with Windows and DOS Systems:** understanding file systems, exploring Microsoft File Structures, Examining NTFS disks, Understanding whole disk encryption, windows registry, Microsoft startup tasks, MS-DOS startup tasks, virtual machines.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. Computer Forensics, Computer Crime Investigation by John R. Vacca, Firewall Media, New Delhi, 2015 2. Computer Forensics and Investigations by Nelson, Phillips Enfinger, Steuart, CENGAGE Learning, 2004

1	**Code of the subject**	MTIS-9303
2	**Title of the subject**	Cyber-Physical System Security
3	**Any prerequisite**	Intermediate programming concepts, Basic information security concepts
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Debanjan Sadhya
6	**Will this course require visiting faculty**	Yes
7	**Learning Objectives of the subject (in about 50 words)**	• Understand what cyber-physical systems are. • Understand what makes cyber-physical systems hard to secure. • Understand common methods used to secure cyber-physical systems. • Understand the differences between securing traditional enterprise systems and cyber-physical systems.
8	**Brief Contents**	Introduction: Cyber-Physical Systems (CPS) in the real world, Overview of CPS; Background - Networking, Information security, Control systems, Industrial networks, Industrial cyber security history and threats; Introduction to industrial control systems and operations, Industrial network design and architecture; Industrial network protocols, Power delivery systems; Hacking industrial control systems, Securing industrial control systems; Privacy in Cyber-Physical systems, Threats to Cyber-Physical systems in other domains.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. "Industrial Network Security, Second Edition: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems", Eric D. Knapp, Joel Thomas Langill, *Syngress*, 2011 2. "Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure", Eric D. Knapp, Raj Samani, *Syngress*, 2013 3. http://rbeyah.ece.gatech.edu/classes/summer2018/cs6263/#Overview

1	**Code of the subject**	MTIS-9304
2	**Title of the subject**	Intrusion Detection and Prevention
3	**Any prerequisite**	Computer Networks, Operating Systems, Information Systems Security
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Saumya Bhadauria
6	**Will this course require visiting faculty**	No
7	**Learning Objectives of the subject (in about 50 words)**	• To give students practical, working knowledge in intrusion detection and traffic analysis. • To gain an understanding of the workings of TCP/IP, methods of network traffic analysis and popular network intrusion detection systems.
8	**Brief Contents**	**IDS/IPS definition and classification** -Basic elements of attacks and their detection -Misuse detection systems (search algorithms and applications in IDS); **Anomaly detection systems** (machine learning basics: principles, measures, performance evaluation, method combinations, basics of artificial neural networks, clustering (hierarchical and partitioned) and supervised learning in IDS; **Testing IDS** and measuring their performances, Computational complexity; **Theoretic IDS models** and quality criteria, Intrusion detection in virtual networks.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. William Stallings and Lawrie Brown. 2014. Computer Security: Principles and Practice (3rd ed.). Prentice Hall Press, Upper Saddle River, NJ, USA. 2. Rebecca Gurley Bace, Intrusion Detection, Macmillan, 2000. 3. David J. Marchette, Computer Intrusion Detection and Network Monitoring –A Statistical Viewpoint, Springer Verlag, 2001. 4. Richard Bejtlich, Extrusion Detection - Security Monitoring for Internal Intrusions, Addison-Wesley, 2005.

1	**Code of the subject**	MTIS-9305
2	**Title of the subject**	Information Assurance and Analysis
3	**Any prerequisite**	
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Dr. Pinku Ranjan
6	**Will this course require visiting faculty**	NO
7	**Learning Objectives of the subject (in about 50 words)**	• Ability to recognize the propensity of errors and remedies in processes involving Information Technology • consummate knowledge of risks and controls in IT operations in Industry • An ability to provide protective IT security guidelines for various types of Industries • The necessary wherewithal to become an IS Auditor and/or Security specialist eventually • Evaluate asset safeguarding and data integrity, system effectiveness and system efficiency
8	**Brief Contents**	**Introduction:** Overview of Information Systems Auditing. Conducting an Information Systems Audit. Management and the application; **Control Framework:** Top Management Controls, Security Management Controls. Operations Management Controls. Quality Assurance Management Controls. Boundary Controls. Communication Controls. Evidence Collection and Evidence evaluation: Audit Software. Concurrent Auditing Techniques. Interviews, Questionnaires, and Control Flowcharts. Evaluating Asset Safeguarding; Web service security. Enterprise web service security and SAML. REST security and OAuth; Private key security: Stream ciphers. Birthday theorem. Block ciphers. Hash functions; Public key security: Diffie-Helman, El Gamal, RSA. Public key protocols. Advanced cryptosystems; Cryptography APIs: Java Cryptography Extension (JCE). Bouncy Castle. PKI and certificate management. Hook 8 Multilevel security: Bell-Lapadula, noninterference, non-deducibility. Role-based access control; Multilevel integrity: Biba. Multilateral security: Compartmentation, Chinese Wall, Clark-Wilson, BMA. Secondary uses and privacy; Enterprise security patterns. JEE A4: REST security 11 OCTAVE: managing information security risks; Network security: Vulnerabilities. Firewalls. Intrusion detection. Denial of service; Cyber forensics; Security and privacy in the cloud.
9	**Contents for lab (If applicable)**	No
10	**List of text books/references**	1. Ross Anderson, [A] Security Engineering, 2nd ed., Wiley, 2008. 2. Deepak Alur, Dan Malks, and John Crupi, [JEE] Core J2EE Patterns: Best Practices and Design Strategies, Prentice Hall, 2nd ed., 2003. 3. David Hook, [H] Beginning Cryptography, Wiley, 2005. 4. Ron Weber , Information Systems Control and Audit, Pearson Education 5. John B. Kramerk, The CISA Prep Guide, Wiley Publications 6. Information Systems Control and Audit, BOS, Institute of Chartered Accontants of India, New Delhi

1	**Code of the subject**	MTIS-9306
2	**Title of the subject**	Fundamentals of Intrusion Analysis
3	**Any prerequisite**	Knowledge of Computer Networks, Information security, Network management and Security, including technical security issues. privacy, and ethics.
4	**L-T-P**	3-0-0
5	**Name of the proposer**	Prof. Shashikala Tapaswi
6	**Will this course require visiting faculty**	For Expert Sessions
7	**Learning Objectives of the subject (in about 50 words)**	• To understand about the practices adopted by intruders. • To gain knowledge of network security with a focus on intrusion detection and penetration test in context of real-life applications. • To understand, evaluate critically, and assimilating new knowledge and emerging technology in network security. • To understand the physical location, the operational characteristics and the various functions performed by the intrusion detection/prevention system. • To understand the current network security vulnerabilities and effective procedures of penetration test. • To learn new techniques and to align new security technologies to existing network infrastructure
8	**Brief Contents**	**Introduction:** Understanding Intrusion Detection – Intrusion detection and prevention basics – IDS and IPS analysis schemes, Vulnerabilities and Security Threats to Computer Networks. Sources of vulnerabilities, types of attacks, attacks against various security objectives, countermeasures of attacks. Theoretical foundations of detection: Taxonomy of anomaly detection system – fuzzy logic – Bayes theory – Artificial Neural networks – Support vector machine – Evolutionary computation – Association rules – Clustering; **Architecture and Implementation:** IDS and IPS Centralized – Distributed – Cooperative Intrusion Detection – Tiered architectures, single-tiered, multi-tiered, peer-to-peer. Sensor: sensor functions, sensor deployment and security. Agents: agent functions, agent deployment and security. Alert management: alert types, alert manager deployment and security. Information flow in IDS and IPS, defending IDS/IPS; **Intrusion Detection and Prevention:** Host-based intrusion detection system (IDS) / intrusion prevention system (IPS), network-based IDS/IPS. Detection approaches –Misuse detection – anomaly detection – specification based detection – hybrid detection, pattern matching, policy-based and state-based; anomaly detection: statistical based, honeypots-based; hybrid detection; **Applications and Tools:** Penetration Test Methodologies and Procedures, White-box / grey-box testing, security surfaces for evaluation, automated tools for vulnerability scan and penetration Tool Selection and Acquisition Process – Bro Intrusion Detection – Prelude Intrusion Detection – Snorts Intrusion Detection – NFR (Non-functional Requirements) security. Deployment of IDS/IPS Case study on commercial and open-source IDS; Network Security Monitoring, Network traffic collection and storage, detection mechanisms and indicators of compromise, packet analysis, friendly and threat intelligence; **Legal Issues and Organization Standards:** Law Enforcement / Criminal Prosecutions – Standard of Due Care – Evidentiary Issues, Organizations and Standardizations.
9	**Contents for lab (If applicable)**	Possible Hands on and laboratory sessions on : 1.Vulnerability scan and penetration test 2. Protocol and traffic analysis Intrusion detection using Snort.
10	**List of text books/references**	1. Ali A. Ghorbani, Wei Lu, "Network Intrusion Detection and Prevention: Concepts and Techniques", Springer, 2010. 2. Carl Enrolf, Eugene Schultz, Jim Mellander, "Intrusion detection and Prevention", McGraw Hill, 2004 3. Paul E. Proctor, "The Practical Intrusion Detection Handbook", Prentice Hall, 2001. 4. Earl Carter, Jonathan Hogue, "Intrusion Prevention Fundamentals", Pearson Education, 2006. ***Additional Readings***

		1. Ankit Fadia and Mnu Zacharia, “Intrusiion Alert”, Vikas Publishing house Pvt., Ltd, 2007. 2. J. M. Kizza, Computer Network Security, Springer, 2005. 3. Chris Sanders and Jason Smith, Applied Network Security Monitoring: Collection, Detection, and Analysis, Syngress, 2013. 4. Richard Bejtlich, The Practice of Network Security Monitoring: Understanding Incident Detection and Response, No Starch Press, 2013. 5. Peter Kim, The Hacker Playbook 3: Practical Guide To Penetration Testing, May 2011.

****