SIES COLLEGE OF COMMERCE & ECONOMICS

AUTONOMOUS

DEPARTMENT OF INFORMATION TECHNOLOGY

Date of BOS meeting: 23rd April 2021

Name of BOS Chairperson: Mrs. Bhavini Deepak Shah

Sr. No.	Heading	Particulars
1	Title of the course	M. Sc. (Information Technology)
2	Eligibility for admission	BSc IT, BSc CS, BE, BCA, BSc Physics, BSc Maths, BSc Statistics, BSc Electronics
3	Minimum percentage	40 %
4	Semesters	III & IV
5	Level	PG
6	Pattern	02 years & 04 semesters CBGS
7	To be implemented from	From Academic year 2021-22 in a progressive manner

SIES COLLEGE OF COMMERCE & ECONOMICS
(AUTONOMOUS)
(Affiliated to University of Mumbai)
RE-ACCREDITED GRADE "A" BY NAAC

BOARD OF STUDIES
INFORMATION TECHNOLOGY

(WITH EFFECT FROM THE ACADEMIC YEAR 2020-2021)

Artificial Intelligence Track
Image Processing Track
Cloud Computing Track
Security Track

SEMESTER - III					
	Course Title				
Course Code	Theory	Credits	Course Code	Practical	Credits
MITS301	Technical Writing and Entrepreneurship Development	4	MITS3P1	Project Documentationand Viva	2
Elective 1: Select Any one from the courses listed below along with corresponding practical course					
MITS302a	Applied Artificial Intelligence	4	MITS3P2a	Applied Artificial Intelligence Practical	2
MITS302b	Computer Vision		MITS3P2b	Computer Vision Practical	
MITS302c	Cloud Application Development		MITS3P2c	Cloud Application Development Practical	
MITS302d	Security Breaches and Countermeasures		MITS3P2d	Security Breaches and Countermeasures Practical	
Elective 2: Select Any one from the courses listed below along with corresponding practical course					
MITS303a	Machine Learning	4	MITS3P3a	Machine Learning Practical	2
MITS303b	Biomedical Image Processing		MITS3P3b	Biomedical Image Processing Practical	
MITS303c	Cloud Management		MITS3P3c	Cloud Management Practical	
MITS303d	Malware Analysis		MITS3P3d	Malware Analysis Practical	
Elective 3: Select Any one from the courses listed below along with corresponding practical course					
MITS304a	Robotic Process Automation	4	MITS3P4a	Robotic Process Automation Practical	2
MITS304b	Virtual Reality and Augmented Reality		MITS3P4b	Virtual Reality andAugmented Reality Practical	
MITS304c	Data Center Technologies		MITS3P4c	Data Center Technologies Practical	
MITS304d	Offensive Security		MITS3P4d	Offensive Security Practical	
	Total Theory Credits	**16**		Total Practical Credits	**8**
Total Credits for Semester III: 24					

SEMESTER - IV					
	Course Title				
Course Code	Theory	Credits	Course Code	Practical	Credits
MITS401	Blockchain	4	MITS4P1	Blockchain Practical	2
Elective 1: Select Any one from the courses listed below along with corresponding practical course					
MITS402a	Natural Language Processing	4	MITS4P2a	Natural Language Processing Practical	2
MITS402b	Digital Image Forensics		MITS4P2b	Digital Image Forensics Practical	
MITS402c	Advanced IoT		MITS4P2c	Advanced IoT Practical	
MITS402d	Cyber Forensics		MITS4P2d	Cyber Forensics Practical	
Elective 2: Select Any one from the courses listed below along with corresponding practical course					
MITS403a	Deep Learning	4	MITS4P3a	Deep Learning Practical	2
MITS403b	Remote Sensing		MITS4P3b	Remote Sensing Practical	
MITS403c	Server Virtualization on VMWare Platform		MITS4P3c	Server Virtualization on VMWare Platform Practical	
MITS403d	Security Operations Center		MITS4P3d	Security Operations Center Practical	
Elective 3: Select Any one from the courses listed below. Project Implementation and Viva is compulsory					
MITS404a	Human Computer Interaction	4	MITS4P4	Project Implementation andViva	2
MITS404b	Advanced Applications of Image Processing				
MITS404c	Storage as a Service				
MITS404d	Information Security Auditing				
	Total Theory Credits	**16**		Total Practical Credits	**8**
Total Credits for Semester IV: 24					

SEMESTER III

Technical Writing and Entrepreneurship Development

COURSE CODE: MITS301 **COURSE CREDIT: 04**

Course Objectives:

- This course aims to provide conceptual understanding of developing strong foundation in general writing, including research proposal and reports.
- It covers the technological developing skills for writing Article, Blog, E-Book, Commercial web Page design, Business Listing Press Release, E-Listing and Product Description.
- This course aims to provide conceptual understanding of innovation and entrepreneurship development.

Sr. No	Modules/Units	No of Lectures
1.	**Introduction to Technical Communication:** What Is Technical Communication? The Challenges of Producing Technical Communication, Characteristics of a Technical Document, Measures of Excellence in Technical Documents, Skills and Qualities Shared by Successful Workplace Communicators, How Communication Skills and Qualities Affect Your Career? **Understanding Ethical and Legal Considerations:** A Brief Introduction to Ethics, Your Ethical Obligations, Your Legal Obligations, The Role of Corporate Culture in Ethical and Legal Conduct, Understanding Ethical and Legal Issues Related to Social Media, Communicating Ethically Across Cultures, Principles for Ethical Communication **Writing Technical Documents:** Planning, Drafting, Revising, Editing, Proofreading **Writing Collaboratively:** Advantages and Disadvantages of Collaboration, Managing Projects, Conducting Meetings, Using Social Media and Other Electronic Tools in Collaboration, Importance of Word Press Website, Gender and Collaboration, Culture and Collaboration.	12
2.	**Introduction to Content Writing:** Types of Content (Article, Blog, E-Books, Press Release, Newsletters Etc), Exploring Content Publication Channels. Distribution of your content across various channels. **Blog Creation:** Understand the psychology behind your web traffic, Creating killing landing pages which attract users, Using Landing Page Creators, Setting up Accelerated Mobile Pages, Identifying UI UX Experience of your website or blog. **Organizing Your Information:** Understanding Three Principles for Organizing Technical Information, Understanding Conventional Organizational Patterns, **Emphasizing Important Information:** Writing Clear, Informative Titles, Writing Clear, Informative Headings, Writing Clear Informative Lists, Writing Clear Informative Paragraphs.	12

3.	**Creating Graphics:** The Functions of Graphics, The Characteristics of an Effective Graphic, Understanding the Process of Creating Graphics, Using Color Effectively, Choosing the Appropriate Kind of Graphic, Creating Effective Graphics for Multicultural Readers. **Researching Your Subject:** Understanding the Differences Between Academic and Workplace Research, Understanding the Research Process, Conducting Secondary Research, Conducting Primary Research, **Research and Documentation:** Literature Reviews, Interviewing for Information, Documenting Sources, Copyright, Paraphrasing, Questionnaires. **Report Components:** Abstracts, Introductions, Tables of Contents, Executive Summaries, Feasibility Reports, Investigative Reports, Laboratory Reports, Test Reports, Trip Reports, Trouble Reports	12
4.	**Writing Proposals:** Understanding the Process of Writing Proposals, The Logistics of Proposals, The ―Deliverables‖ of Proposals, Persuasion and Proposals, Writing a Proposal, The Structure of the Proposal. **Writing Informational Reports:** Understanding the Process of Writing Informational Reports, Writing Directives, Writing Field Reports, Writing Progress and Status Reports, Writing Incident Reports, Writing Meeting Minutes. **Writing Recommendation Reports:** Understanding the Role of Recommendation Reports, Using a Problem-Solving Model for Preparing Recommendation Reports, Writing Recommendation Reports. **Reviewing, Evaluating, and Testing Documents and Websites:** Understanding Reviewing, Evaluating, and Testing, Reviewing Documents and Websites, Conducting Usability Evaluations, Conducting Usability Tests, Using Internet tools to check writing Quality, Duplicate Content Detector, What is Plagiarism?, How to avoid writing plagiarism content? **Innovation management: an introduction:** The importance of innovation, Models of innovation, Innovation as a management process. **Market adoption and technology diffusion:** Time lag between innovation and useable product, Innovation and the market Innovation and market vision ,Analysing internet search data to help adoption and forecasting sales ,Innovative new products and consumption patterns, Crowd sourcing for new product ideas, Frugal innovation and ideas from everywhere, Innovation diffusion theories.	12
5.	**Managing innovation within firms:** Organisations and innovation, The dilemma of innovation management, Innovation dilemma in low technology sectors, Dynamic capabilities, Managing uncertainty, Managing innovation projects **Operations and process innovation:** Operations management, The nature of design and innovation in the context of operations, Process design, Process design and innovation **Managing intellectual property:** Intellectual property, Trade	12

	secrets, An introduction to patents, Trademarks, Brand names, Copyright **Management of research and development:** What is research and development?, R&D management and the industrial context, R&D investment and company success, Classifying R&D, R&D management and its link with business strategy, Strategic pressures on R&D, Which business to support and how?, Allocation of funds to R&D, Level of R&D expenditure **Managing R&D projects:** Successful technology management, The changing nature of R&D management, The acquisition of external technology, Effective R&D management, The link with the product innovation process, Evaluating R&D projects.	

REFERENCE BOOKS:

Books and References:					
Sr. No.	**Title**	**Author/s**	**Publisher**	**Edition**	**Year**
1.	Technical Communication	Mike Markel	Bedford/St. Martin's	11	2014
2.	Innovation Management and New Product Development	Paul Trott	Pearson	06	2017
3.	Handbook of Technical Writing	Gerald J. Alred , Charles T. Brusaw , Walter E. Oliu	Bedford/St. Martin's	09	2008
4.	Technical Writing 101: A Real-World Guide to Planning and Writing Technical Content	Alan S. Pringle and Sarah S. O'Keefe	scriptorium	03	2009
5.	Innovation and Entrepreneurship	Peter Drucker	Harper Business	03	2009

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Introduction to Technical Communication, Understanding Ethical and Legal Considerations, Writing Technical Documents, Writing Collaboratively	No Change	NIL
Unit 2 Introduction to Content Writing, Organizing Your Information, Emphasizing Important Information	No Change	NIL
Unit 3 Creating Graphics, Researching Your Subject, Research and Documentation, Report Components	No Change	NIL
Unit 4 Writing Proposals, Writing Informational Reports, Writing Recommendation Reports, Reviewing, Evaluating, and Testing Documents and Websites, Innovation management: an introduction, Market adoption and technology diffusion	No Change	NIL
Unit 5 Managing innovation within firms, Operations and process innovation, Managing intellectual property, Management of research and Development, Managing R&D projects	No Change	NIL

Project Documentation and Viva

COURSE CODE: MITS3P1 **COURSE CREDIT: 02**

The learners are expected to develop a project beyond the undergraduate level. Normal websites, web applications, mobile apps are not expected. Preferably, the project should be from the elective chosen by the learner at the post graduate level. In semester three, the learner is supposed to prepare the synopsis and documentation. The same project has to be implemented in Semester IV.
More details about the project is given is Appendix 1.

Elective 1

Applied Artificial Intelligence

COURSE CODE: MITS302a **COURSE CREDIT: 04**

Course Objectives:

- To explore the applied branches of artificial intelligence
- To enable the learner to understand applications of artificial intelligence
- To enable the student to solve the problem aligned with derived branches of artificial intelligence.

Sr. No	Modules/Units	No of Lectures
1.	**Review of AI:** History, foundation and Applications **Expert System and Applications:** Phases in Building Expert System, Expert System Architecture, Expert System versus Traditional Systems, Rule based Expert Systems, Blackboard Systems, Truth Maintenance System, Application of Expert Systems, Shells and Tools	12
2.	**Probability Theory:** joint probability, conditional probability, Bayes's theorem, probabilities in rules and facts of rule based system, cumulative probabilities, rule based system and Bayesian method **Fuzzy Sets and Fuzzy Logic:** Fuzzy Sets, Fuzzy set operations, Types of Member ship Functions, Multivalued Logic, Fuzzy Logic, Linguistic variables and Hedges, Fuzzy propositions, inference rules for fuzzy propositions, fuzzy systems, possibility theory and other enhancement to Logic	12
3.	**Machine Learning Paradigms:** Machine Learning systems, supervised and un-supervised learning, inductive learning, deductive learning, clustering, support vector machines, cased based reasoning and learning. **Artificial Neural Networks:** Artificial Neural Networks, Single-Layer feedforward networks, multi-layer feed-forward networks, radial basis function networks, design issues of artificial neural networks and recurrent networks	12
4.	**Evolutionary Computation:** Soft computing, genetic algorithms, genetic programming concepts, evolutionary programming, swarm intelligence, ant colony paradigm, particle swarm optimization and applications of evolutionary algorithms. **Intelligent Agents:** Agents vs software programs, classification of agents, working of an agent, single agent and multiagent systems, performance evaluation, architecture, agent communication language, applications	12
5.	**Advanced Knowledge Representation Techniques:** Conceptual dependency theory, script structures, CYC theory, script structure, CYC theory, case grammars, semantic web. **Natural Language Processing:** Sentence Analysis phases, grammars and parsers, types of parsers, semantic analysis, universal networking language, dictionary	12

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Artificial Intelligence	Saroj Kaushik	Cengage	1st	2019
2.	Artificial Intelligence: A Modern Approach	A. Russel, Peter Norvig		1st	
3.	Artificial Intelligence	Elaine Rich,Kevin Knight,Shivashankar B. Nair	Tata Mc-Grawhill	3rd	

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Review of AI, Expert System and Applications	No Change	NIL
Unit 2 Probability Theory, Fuzzy Sets and Fuzzy Logic	No Change	NIL
Unit 3 Machine Learning Paradigms, Artificial Neural Networks	No Change	NIL
Unit 4 Evolutionary Computation, Intelligent Agents	No Change	NIL
Unit 5 Advanced Knowledge Representation Techniques, Natural Language Processing	No Change	NIL

Artificial Intelligence Practical

COURSE CODE: MITS3P2a **COURSE CREDIT: 02**

- To understand the fundamentals concepts of expert system and its applications.
- To use probability and concept of fuzzy sets for solving AI based problems.
- To be able to understand the applications of Machine Learning and also apply fuzzy system for solving problems.
- To understand the applications of genetic algorithms in different problems related to artificial intelligence.
- To use knowledge representation techniques in natural language processing.

List of Practical:	
1.	Design an Expert system using AIML E.g: An expert system for responding the patient query for identifying the flu.
2.	Design a bot using AIML.
3.	Implement Bayes Theorem using Python
4.	Implement Conditional Probability and joint probability using Python
5.	Write a program for to implement Rule based system.
6.	Design a Fuzzy based application using Python / R.
7.	Write an application to simulate supervised and un-supervised learning model.
8.	Write an application to implement clustering algorithm.
9.	Write an application to implement support vector machine algorithm.
10.	Simulate artificial neural network model with both feed forward and back propagation approach. [You can add some functionalities to enhance the model].
11.	Simulate genetic algorithm with suitable example using Python / R or any other platform.
12.	Design an Artificial Intelligence application to implement intelligent agents.
13.	Design an application to simulate language parser.
14.	Design an application to simulate semantic web.

Computer Vision

COURSE CODE: MITS302b **COURSE CREDIT: 04**

Course Objectives:

- To develop the student's understanding of the issues involved in trying to define and simulate perception.
- To familiarize the student with specific, well known computer vision methods, algorithms and results.
- To provide the student additional experience in the analysis and evaluation of complicated systems.
- To provide the student additional software development experience.
- To provide the student with paper and proposal writing experience.

Sr. No	Modules/Units	No of Lectures
1.	**Introduction:** What is computer vision?, A brief history, Image formation, Geometric primitives and transformations, Geometric primitives, D transformations, D transformations, D rotations, D to D projections, Lens distortions, Photometric image formation, Lighting, Reflectance and shading, Optics, The digital camera, Sampling and aliasing, Color, Compression **Feature-based alignment**: D and D feature-based alignment, D alignment using least squares , Application:Panography , Iterative algorithms , Robust least squares and RANSAC , D alignment , Pose estimation , Linear algorithms, Iterative algorithms , Application: Augmented reality , Geometric intrinsic calibration, Calibration patterns, Vanishing points , Application: Single view metrology , Rotational motion ,Radial distortion	12
2.	**Structure from motion :** Triangulation, Two-frame structure from motion , Projective (uncalibrated) reconstruction, Self-calibration , Application: View morphing , Factorization, Perspective and projective factorization , Application: Sparse D model extraction, Bundle adjustment, Exploiting sparsity , Application: Match move and augmented reality , Uncertainty and ambiguities , Application: Reconstruction from Internet photos , Constrained structure and motion , Line-based techniques , Plane-based techniques **Dense motion estimation :** Translational alignment , Hierarchical motion estimation, Fourier-based alignment, Incremental refinement , Parametric motion, Application: Video stabilization, Learned motion models, Spline-based motion, Application: Medical image registration, Optical flow, Multi-frame motion estimation, Application: Video denoising , Application: De- interlacing , Layered motion, Application: Frame interpolation, Transparent layers and reflections	12

3.	**Image stitching :** Motion models, Planar perspective motion, Application: Whiteboard and document scanning, Rotational panoramas , Gap closing , Application: Video summarization and compression, Cylindrical and spherical coordinates, Global alignment, Bundle adjustment, Parallax removal , Recognizing panoramas, Direct vsfeature-based alignment, Compositing , Choosing a compositing surface, Pixel selection and weighting (de-ghosting), Application:Photomontage, Blending **Computational photography :** Photometric calibration, Radiometric response function ,Noise level estimation, Vignetting ,Optical blur (spatial response) estimation, High dynamic range imaging ,Tone mapping, Application: Flash photography, Super-resolution and blur removal, Color image demosaicing, Application: Colorization, Image matting and compositing ,Blue screen matting ,Natural image matting ,Optimization- based matting ,Smoke, shadow, and flash matting ,Video matting ,Texture analysis and synthesis ,Application: Hole filling and inpainting ,Application: Non- photorealistic rendering	12
4.	**Stereo correspondence** Epipolar geometry , Rectification ,Plane sweep , Sparse correspondence , D curves and profiles , Dense correspondence, Similarity measures , Local methods , Sub-pixel estimation and uncertainty , Application: Stereo-based head tracking , Global optimization , Dynamic programming , Segmentation-based techniques, Application: Z-keying and background replacement, Multi-view stereo, Volumetric and D surface reconstruction, Shape from silhouettes **3D reconstruction :** Shape from X , Shape from shading and photometric stereo, Shape from texture, Shape from focus , Active rangefinding , Range datamerging , Application: Digital heritage , Surface representations , Surface interpolation, Surface simplification, Geometry images , Point-based representations, Volumetric representations , Implicit surfaces and level sets , Model-based reconstruction, Architecture, Heads and faces , Application: Facial animation, Whole body modeling and tracking, Recovering texture maps and albedos , Estimating BRDFs Application: D photography	12
5.	**Image-based rendering :** View interpolation, View- dependent texture maps, Application: Photo Tourism , Layered depth images, Impostors, sprites, and layers, Light fields and Lumigraphs , Unstructured Lumigraph, Surface light fields, Application: Concentric mosaics, Environment mattes, Higher-dimensional light fields , The modeling to rendering continuum, Video-based rendering , Video-based animation, Video textures , Application: Animating pictures, D Video, Application: Video-based walkthroughs **Recognition :** Object detection, Face detection, Pedestrian detection, Face recognition, Eigenfaces, Active appearance and D shape models, Application: Personal photo collections, Instance recognition, Geometric alignment, Large databases, Application: Location recognition, Category recognition, Bag of words, Part-based models, Recognition with segmentation,	12

	Application: Intelligent photo editing, Context and scene understanding , Learning and large image collections, Application: Image search, Recognition databases and test sets	

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Computer Vision: Algorithms and Applications	Richard Szeliski	Springer	1st Edition	2010

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Introduction, Feature-based alignment	No Change	NIL
Unit 2 Structure from motion, Dense motion estimation	No Change	NIL
Unit 3 Image stitching, Computational photography	No Change	NIL
Unit 4 Stereo correspondence, 3D reconstruction	No Change	NIL
Unit 5 Image-based rendering, Recognition	No Change	NIL

Computer Vision Practical

COURSE CODE: MITS3P2b **COURSE CREDIT: 02**

Course Objectives:

- To understand the basics of computer vision.
- To understand and analyse various structure form motion and various estimates of Dense Motion.
- To apply various motion models to images and understand computation photography techniques.
- To apply Epipolar geometry, Rectification and various other 3D correspondence and Stereo reconstruction techniques.
- To understand image-based rendering and reconstruction.

List of Practical:

10 practicals covering the entire syllabus must be performed. The detailed list of practical will be circulated later in the official workshop.

Cloud Application Development

COURSE CODE: MITS302c **COURSE CREDIT: 04**

Course Objectives:

- To develop and deploy Microservices for cloud.
- To understand Kubernetes and deploy applications on Azure Kubernetes Service.
- To understand DevOps for Azure.
- To follow the DevOps practices for software development.
- To build APIs for Azure and AWS.

Sr. No	Modules/Units	No of Lectures
1.	**Implementing Microservices:** Client to microservices communication, Interservice communication, data considerations, security, monitoring, microservices hosting platform options. **Azure Service Fabric:** Introduction, core concepts, supported programming models, service fabric clusters, develop and deploy applications of service fabric. **Monitoring Azure Service Fabric Clusters:** Azure application, resource manager template, Adding Application Monitoring to a Stateless Service Using Application Insights, Cluster monitoring, Infrastructure monitoring.	12
2.	**Azure Kubernetes Service (AKS):** Introduction to kubernetes and AKS, AKS development tools, Deploy applications on AKS. **Monitoring AKS:** Monitoring, Azure monitor and analytics, monitoring AKS clusters, native kubernetes dashboard, Prometheus and Grafana. **Securing Microservices:** Authentication in microservices, Implenting security using API gateway pattern, Creating application using Ocrlot and securing APIs with Azure AD. **Database Design for Microservices:** Data stores, monolithic approach, Microservices approach, harnessing cloud computing, dataase options on MS Azure, overcoming application development challenges. **Building Microservices on Azure Stack:** Azure stack, Offering IaaS, PaaS on-premises simplified, SaaS on Azure stack.	12
3.	.**NET DevOps for Azure:** DevOps introduction, Problem and solution. **Professional Grade DevOps Environment:** The state of DevOps, professional grade DevOps vision, DevOps architecture, tools for professional DevOps environment, DevOps centered application. **Tracking work:** Process template, Types of work items, Customizing the process, Working with the process. **Tracking code:** Number of repositories, Git repository, structure, branching pattern, Azure repos configuration, Git and Azure.	12

4.	**Building the code:** Structure of build, using builds with .NET core and Azure pipelines, **Validating the code:** Strategy for defect detection, Implementing defect detection. **Release candidate creation:** Designing release candidate architecture, Azure artifacts workflow for release candidates, **Deploying the release:** Designing deployment pipeline, Implementing deployment in Azure pipelines. **Operating and monitoring release:** Principles, Architectures for observability, Jumpstarting observability.	12
5.	**Introduction to APIs:** Introduction, API economy, APIs in public sector. **API Strategy and Architecture:** API Strategy, API value chain, API architecture, **API** management. **API Development:** Considerations, Standards, kick-startAPI development, team orientation. **API Gateways:** API Gateways in public cloud, Azure API management, AWS API gateway. **API Security:** Request-based security, Authentication and authorization.	12

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Building Microservices Applications on Microsoft Azure- Designing, Developing, Deploying, and Monitoring	Harsh Chawla Hemant Kathuria	Apress	--	2019
2.	.NET DevOps for Azure A Developer's Guide to DevOps Architecture the Right Way	Jeffrey Palermo	Apress	--	2019
3.	Practical API Architecture and Development with Azure and AWS - Design and Implementation of APIs for the Cloud	Thurupathan Vijayakumar	Apress	--	2018

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Implementing Microservices, Azure Service Fabric, Monitoring Azure Service Fabric Clusters	No Change	NIL
Unit 2 Azure Kubernetes Service (AKS), Monitoring AKS, Securing Microservices, Database Design for Microservices, Building Microservices on Azure Stack	No Change	NIL
Unit 3 .NET DevOps for Azure, Professional Grade DevOps Environment, Tracking work, Tracking code	No Change	NIL
Unit 4 Building the code, Validating the code, Release candidate creation, Deploying the release, Operating and monitoring release	No Change	NIL
Unit 5 Introduction to APIs, API Strategy and Architecture, API Development, API Gateways, API Security	No Change	NIL

Cloud Application Development Practical

COURSE CODE: MITS3P2c **COURSE CREDIT: 02**

- To develop the Microservices for cloud and deploy them on Microsoft Azure.
- To build and deploy services to Azure Kubernetes service.
- To understand and build the DevOps way.
- To thoroughly build the applications in the DevOps way.
- To build the APIs for Microsoft Azure and AWS.

List of Practical:	
1.	Develop an ASP.NET Core MVC based Stateless Web App.
2.	Develop a Spring Boot API.
3.	Create an ASP.NET Core Web API and configure monitoring.
4.	a. Create an Azure Kubernetes Service Cluster
	b. Enable Azure Dev Spaces on an AKS Cluster
	c. Configure Visual Studio to Work with an Azure Kubernetes Service Cluster
	d. Configure Visual Studio Code to Work with an Azure Kubernetes Service Cluster
	e. Deploy Application on AKS i. Core Web API ii. Node.js API
5.	Create an AKS cluster a. from the portal b. with Azure CLI
6.	Create an Application Gateway Using Ocelot and Securing APIs with Azure AD.
7.	Create a database design for Microservices an application using the database.
8.	a. Create an API management service b. Create an API gateway service
9.	Demonstrate a. Securing APIs with Azure Active Directory. b. Issuing a custom JWT token using a symmetric signing key c. Pre-Authentication in Azure API Management d. AWS API Gateway Authorizer
10.	Create a serverless API using Azure functions
11.	Create an AWS Lambda function
12.	Build AWS Lambda with AWS API gateway

Security Breaches and Countermeasures

COURSE CODE: MITS302d **COURSE CREDIT: 04**

Course Objectives:

- To get the insight of the security loopholes in every aspect of computing.
- To understand the threats and different types of attacks that can be launched on computing systems.
- To know the countermeasures that can be taken to prevent attacks on computing systems.
- To test the software against the attacks.

Sr. No	Modules/Units	No of Lectures
1.	**Introduction to Security Breaching**: Overview of Information Security, Threats and Attack vectors, Concepts of Hacking – Ethical and Unethical, Information Security Controls, Concepts of penetration Testing, Information Security Laws and Standards. **Evaluation Security of IT Organisation:** Concepts,Methodology, Tools, Countermeasures, Penetration Testing. **Network Scanning:** Concepts, Scanning beyond IDSand firewalls, Tools, Banner Grabbing, Scanning Techniques, Network Diagrams, penetration testing. **Enumeration:** Concepts, Different types of enumeration: Netbios, SNMP, LDAP, NTP, SMTP, DNS, other enumeration techniques, Countermeasures, Penetration Testing	12
2.	**Analysis of Vulnerability:** Concepts, Assessment Solutions, Scoring Systems, Assessment Tools, Assessment Reports. **Breaching System Security:** Concepts, Cracking passwords, Escalating privileges, Executing Applications, Hiding files, covering tracks, penetration testing. **Threats due to malware:** Concepts, Malware Analysis, Trojan concepts, countermeasures, Virus and worm concepts, anti-malware software, penetration testing. **Network Sniffing:** Concepts, countermeasures, sniffing techniques, detection techniques, tools,penetration testing.	12
3.	**Social Engineering:** Concepts, Impersonation on networking sites, Techniques, Identity theft, Insider threats, countermeasures, Pen testing. **Denial of Service and Distributed Denial of service:** Concepts, techniques, botnets, attack tools, countermeasures, protection tools, penetration testing. **Hijacking an active session:** Concepts, tools, application level session hijacking, countermeasures, network level session hijacking, penetration testing. **Evasion of IDS, Firewalls and Honeypots:** Introduction and concepts, detecting honeypots, evading IDS, IDS and Firewall evasion countermeasures, evading firewalls, penetration testing.	12

4.	**Compromising Web Servers:** Concepts, attacks, attack methodology, attack tools, countermeasures, patch management, web server security tools, penetration testing. **Compromising Web Applications:** Concepts**,** threats, methods, tools, countermeasures, testing tools,penetration testing. **Performing SQL Injection:** Concepts, types, methodology, tools, techniques, countermeasures. **Compromising Wireless Networks:** Concepts, wireless encryption, threats, methodology, tools, compromising Bluetooth, countermeasures, wireless security tools, penetration testing.	12
5.	**Compromising Mobile Platforms:** Attack vectors, Compromising Android OS, Compromising iOS, Mobile spyware, Mobile Device Management, Mobilesecurity, penetration testing. **Compromising IoT:** Concepts, attacks, compromising methodology, tools, countermeasures,penetration testing. **Cloud Security:** Concepts, Security, threats, attacks, tools, penetration testing. **Cryptography:** Concepts, email encryption, algorithms, disk encryption, tools, cryptanalysis, Public key infrastructure, countermeasures.	12

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	CEHv10, Certified Ethical Hacker Study Guide	Ric Messier	Sybex - Wiley	-	2019
2.	All in One, Certified Ethical Hacker	Matt Walker	Tata McGraw Hill	-	2012
3.	CEH V10: EC-Council Certified Ethical Hacker Complete Training Guide	I.P. Specialist	IPSPECIALIST	-	2018

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Introduction to Security Breaching, Evaluation Security of IT Organisation, Network Scanning, Enumeration	No Change	NIL
Unit 2 Analysis of Vulnerability, Breaching System Security, Threats due to malware, Network Sniffing	No Change	NIL
Unit 3 Social Engineering, Denial of Service and Distributed Denial of service, Hijacking an active session, Evasion of IDS, Firewalls and Honeypots	No Change	NIL
Unit 4 Compromising Web Servers, Compromising Web Applications, Performing SQL Injection, Compromising Wireless Networks	No Change	NIL
Unit 5 Compromising Mobile Platforms, Compromising IoT, Cloud Security, Cryptography	No Change	NIL

Security Breaches and Countermeasures Practical

COURSE CODE: MITS3P2d **COURSE CREDIT: 02**

Course Objectives:

- To be able to identify the different security breaches that can occur.
- To be able to identify the vulnerability in the systems, breach the security of the system, identify the threats due to malware and sniff the network.
- To be able to perform social engineering and educate people to be careful from attacks due to social engineering, understand and launch DoS and DDoS attacks, hijack and active session and evade IDS and Firewalls.
- To be able to identify the vulnerabilities in the Web Servers, Web Applications, perform SQL injection and get into the wireless networks.
- To be able to identify the vulnerabilities in the newer technologies like mobiles, IoT and cloud computing.

List of Practical:	
1.	a. Use the following tools to perform footprinting and reconnaissance
	i. Recon-ng (Using Kali Linux)
	ii. FOCA Tool
	iii. Windows Command Line Utilities
	• Ping
	• Tracert using Ping
	• Tracert
	• NSLookup
	iv. Website Copier Tool – HTTrack
	v. Metasploit (for information gathering)
	vi. Whois Lookup Tools for Mobile – DNS Tools, Whois, Ultra Tools Mobile
	vii. Smart Whois
	viii. eMailTracker Pro
	ix. Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool
	b. Scan the network using the following tools:
	i. Hping2 / Hping3
	ii. Advanced IP Scanner
	iii. Angry IP Scanner
	iv. Masscan
	v. NEET
	vi. CurrPorts
	vii. Colasoft Packet Builder
	viii. The Dude
	ix.
2.	c. Use Proxy Workbench to see the data passing through it and save the data to file.
	d. Perform Network Discovery using the following tools:
	i. Solar Wind Network Topology Mapper
	ii. OpManager
	iii. Network View
	iv. LANState Pro
	e. Use the following censorship circumvention tools:
	i. Alkasir

	ii. Tails OS
	f. Use Scanning Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool
3.	a. Perform Enumeration using the following tools:
	i. Nmap
	ii. NetBIOS Enumeration Tool
	iii. SuperScan Software
	iv. Hyena
	v. SoftPerfect Network Scanner Tool
	vi. OpUtils
	vii. SolarWinds Engineer's Toolset
	viii. Wireshark
	b. Perform the vulnerability analysis using the following tools:
	i. Nessus
	ii. OpenVas
4.	a. Perform mobile network scanning using NESSUS.
	b. Perform the System Hacking using the following tools:
	i. Winrtgen
	ii. PWDump
	iii. Ophcrack
	iv. Flexispy
	v. NTFS Stream Manipulation
	vi. ADS Spy
	vii. Snow
	viii. Quickstego
	ix. Clearing Audit Policies
	x. Clearing Logs
5.	a. Use wireshark to sniff the network.
	b. Use SMAC for MAC Spoofing.
	c. Use Caspa Network Analyser.
	d. Use Omnipeek Network Analyzer.
6.	a. Use Social Engineering Toolkit on Kali Linux to perform Social Engineering using Kali Linux.
	b. Perform the DDOS attack using the following tools:
	i. HOIC
	ii. LOIC
	iii. HULK
	iv. Metasploit
	c. Using Burp Suite to inspect and modify traffic between the browser and target application.
7.	a. Perform Web App Scanning using OWASP Zed Proxy.
	b. Use droidsheep on mobile for session hijacking
	c. Demonstrate the use of the following firewalls:
	i. Zonealarm and analyse using Firewall Analyzer.
	ii. Comodo Firewall
	d. Use HoneyBOT to capture malicious network traffic.
	e. Use the following tools to protect attacks on the web servers:
	i. ID Server
	ii. Microsoft Baseline Security Analyzer
	iii. Syhunt Hybrid

8.	a. Protect the Web Application using dotDefender.
	b. Demonstrate the following tools to perform SQL Injection:
	i. Tyrant SQL
	ii. Havij
	iii. BBQSQL
9.	Use Aircrack-ng suite for wireless hacking and countermeasures.
10.	Use the following tools for cryptography
	i. HashCalc
	ii. Advanced Encryption Package
	iii. MD5 Calculator
	iv. TrueCrypt
	v. CrypTool

Elective 2

Machine Learning

COURSE CODE: MITS303a **COURSE CREDIT: 04**

Course Objectives:

- Understanding Human learning aspects.
- Understanding primitives in learning process by computer.
- Understanding nature of problems solved with Machine Learning

Sr. No	Modules/Units	No of Lectures
1.	**Introduction:** Machine learning, Examples of Machine Learning Problems, Structure of Learning, learning versus Designing, Training versus Testing, Characteristics of Machine learning tasks, Predictive and descriptive tasks, Machine learning Models: Geometric Models, Logical Models, Probabilistic Models. Features: Feature types, Feature Construction and Transformation, Feature Selection.	12
2.	**Classification and Regression: Classification:** Binary Classification- Assessing Classification performance, Class probability Estimation Assessing class probability Estimates, Multiclass Classification. **Regression**: Assessing performance of Regression- Error measures, Overfitting- Catalysts for Overfitting, Case study of Polynomial Regression. **Theory of Generalization:** Effective number of hypothesis, Bounding the Growth function, VC Dimensions, Regularization theory.	12
3.	**Linear Models:** Least Squares method, Multivariate Linear Regression, Regularized Regression, Using Least Square regression for Classification. Perceptron, Support Vector Machines, Soft Margin SVM, Obtaining probabilities from Linear classifiers, Kernel methods for non-Linearity.	12
4.	**Logic Based and Algebraic Model: Distance Based Models:** Neighbours and Examples, Nearest Neighbours Classification, Distance based clustering-K means Algorithm, Hierarchical clustering, **Rule Based Models:** Rule learning for subgroup discovery, Association rule mining. **Tree Based Models:** Decision Trees, Ranking and Probability estimation Trees, Regression trees, Clustering Trees.	12
5.	**Probabilistic Model:** Normal Distribution and Its Geometric Interpretations, Naïve Bayes Classifier, Discriminative learning with Maximum likelihood, Probabilistic Models with Hidden variables: Estimation-Maximization Methods, Gaussian Mixtures, and Compression based Models. **Trends In Machine Learning :** Model and Symbols- Bagging and Boosting, Multitask learning, Online learning and Sequence Prediction, Data Streams and Active Learning, Deep Learning, Reinforcement Learning.	12

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Machine Learning: The Art and Science of Algorithms that Make Sense of Data	Peter Flach	Cambridge University Press		2012
2.	Introduction to Statistical Machine Learning with Applications in R	Hastie, Tibshirani, Friedman	Springer	2nd	2012
3.	Introduction to Machine Learning	Ethem Alpaydin	PHI	2nd	2013

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Introduction	No Change	NIL
Unit 2 Classification and Regression, Regression, Theory of Generalization	No Change	NIL
Unit 3 Linear Models	No Change	NIL
Unit 4 Logic Based and Algebraic Model: Distance Based Models, Rule Based Models, Tree Based Models	No Change	NIL
Unit 5 Probabilistic Model, Trends In Machine Learning	No Change	NIL

Machine Learning Practical

COURSE CODE: MITS3P3a **COURSE CREDIT: 02**

Course Objectives:

- To understand the key issues in Machine Learning and its associated applications in intelligent business and scientific computing.
- To acquire the knowledge about classification and regression techniques.
- To understand and implement the techniques for extracting the knowledge using machine learning methods.
- To achieve adequate perspectives of big data analytics in various applications like recommender systems, social media applications etc.
- To understand the statistical approach related to machine learning and apply the algorithms to a real-world problem, optimize the models learned and report on the expected accuracy that can be achieved by applying the models.

List of Practical:	
1.	a. Design a simple machine learning model to train the training instances and test the same.
	b. Implement and demonstrate the FIND-S algorithm for finding the most specific hypothesis based on a given set of training data samples. Read the training data from a .CSV file
2.	a. Perform Data Loading, Feature selection (Principal Component analysis) and Feature Scoring and Ranking.
	b. For a given set of training data examples stored in a .CSV file, implement and demonstrate the Candidate-Elimination algorithm to output a description of the set of all hypotheses consistent with the training examples.
3.	a. Write a program to implement the naïve Bayesian classifier for a sample training data set stored as a .CSV file. Compute the accuracy of the classifier, considering few test data sets.
	b. Write a program to implement Decision Tree and Random forest with Prediction, Test Score and Confusion Matrix.
4.	a. For a given set of training data examples stored in a .CSV file implement Least Square Regression algorithm.
	b. For a given set of training data examples stored in a .CSV file implement Logistic Regression algorithm.
5.	a. Write a program to demonstrate the working of the decision tree based ID3 algorithm. Use an appropriate data set for building the decision tree and apply this knowledge to classify a new sample.
	b. Write a program to implement k-Nearest Neighbour algorithm to classify the iris data set.
6.	a. Implement the different Distance methods (Euclidean) with Prediction, Test Score and Confusion Matrix.
	b. Implement the classification model using clustering for the following techniques with K means clustering with Prediction, Test Score and Confusion Matrix.
7.	a. Implement the classification model using clustering for the following techniques with hierarchical clustering with Prediction, Test Score and Confusion Matrix
	b. Implement the Rule based method and test the same.

8.	a. Write a program to construct a Bayesian network considering medical data. Use this model to demonstrate the diagnosis of heart patients using standard Heart Disease Data Set.
	b. Implement the non-parametric Locally Weighted Regression algorithm in order to fit data points. Select appropriate data set for your experiment and draw graphs.
9.	a. Build an Artificial Neural Network by implementing the Backpropagation algorithm and test the same using appropriate data sets.
	b. Assuming a set of documents that need to be classified, use the naïve Bayesian Classifier model to perform this task.
10.	a. Write a program to demonstrate the working of the decision tree based ID3 algorithm. Use an appropriate data set for building the decision tree and apply this knowledge to classify a new sample.
	b. Build an Artificial Neural Network by implementing the Backpropagation algorithm and test the same using appropriate data sets.
11.	Perform Text pre-processing, Text clustering, classification with Prediction, Test Score and Confusion Matrix

Biomedical Image Processing

COURSE CODE: MITS303b **COURSE CREDIT: 04**

Course Objectives:

- To design intelligent systems that can analyze biomedical images.
- To understand different scientific approaches in biomedical image processing.
- To understand the structure of biomedical images and how to correlate it with different biological data.
- To design systems to identify different physical conditions on the basis of biomedical data.

Sr. No	Modules/Units	No of Lectures
1.	**Introduction:** Biosignals, Biosignal Measurement Systems, Transducers, Amplifier/Detector, Analog Signal Processing and Filters, ADC Conversion, Data Banks **Bio signal Measurements, Noise, and Analysis:** Biosignals, Noise, Signal Analysis: Data Functions and Transforms **Spectral Analysis: Classical Methods :** Fourier Series Analysis, Power Spectrum, Spectral Averaging: Welch's Method **Noise Reduction and Digital Filters :** Noise Reduction, Noise Reduction through Ensemble Averaging, Z-Transform, Finite Impulse Response Filters, Infinite Impulse Response Filters	12
2.	**Modern Spectral Analysis: The Search for Narrowband Signals:** Parametric Methods, Nonparametric Analysis: Eigen analysis Frequency Estimation **Time Frequency Analysis:** Basic Approaches, The Short-Term Fourier Transform: The Spectrogram, The Wigner Ville Distribution: A Special Case of Cohen's Class, Cohen's Class Distributions **Wavelet Analysis:** Continuous Wavelet Transform, Discrete Wavelet Transform, Feature Detection:Wavelet Packets **Optimal and Adaptive Filters:** Optimal Signal Processing: Wiener Filters, Adaptive Signal Processing, Phase-Sensitive Detection	12
3.	**Multivariate Analyses:** Principal Component Analysis and Independent Component Analysis : Linear Transformations, Principal Component Analysis, Independent Component Analysis **Chaos and Nonlinear Dynamics :** Nonlinear Systems, Phase Space, Estimating the Embedding Parameters, Quantifying Trajectories in Phase Space: The Lyapunov Exponent, Nonlinear Analysis: The Correlation Dimension, Tests for Nonlinearity: Surrogate Data Analysis **Nonlinearity Detection: Information-Based Methods:** Information and Regularity, Mutual InformationFunction, Spectral Entropy, Phase-Space-Based Entropy Methods, Detrended Fluctuation Analysis	12

4.	**Image Processing: Filters, Transformations, and Registration :** Two-Dimensional Fourier Transform, Linear Filtering, Spatial Transformations, ImageRegistration **Image Segmentation :** Pixel-Based Methods, Continuity-Based Methods, Multi thresholding Morphological Operations, Edge-Based Segmentation **Image Acquisition and Reconstruction :** Imaging Modalities, CT, PET, and SPECT, Magnetic Resonance Imaging, Functional MRI	12
5.	**Classification I: Linear Discriminant Analysis and Support Vector Machines :** Linear Discriminators, Evaluating Classifier Performance, Higher Dimensions:Kernel Machines Support Vector Machines, Machine Capacity: Overfitting or –Less Is More", Extending the Number of Variables and Classes, Cluster Analysis **Classification II: Adaptive Neural Nets :** Training the McCullough Pitts Neuron, The Gradient Decent Method or Delta Rule, Two-Layer Nets: Back Projection, Three-Layer Nets, Training Strategies, Multiple Classifications, Multiple Input Variables	12

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Biosignal and Medical Image Processing	John L. Semmlow, Benjamin Griffel	CRC Press	3rd	2014
2.	Biomedical Signal and Image Processing	Kayvan Najarian Robert Splinter	CRC Press	2nd	2012
3.	Introduction to Biomedical Imaging	Andrew Webb	Wiley-Interscience		2003

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Introduction, Bio signal Measurements, Noise, and Analysis, Spectral Analysis: Classical Methods, Noise Reduction and Digital Filters	No Change	NIL
Unit 2 Modern Spectral Analysis: The Search for Narrowband Signals, Time Frequency Analysis, Wavelet Analysis, Optimal and Adaptive Filters,	No Change	NIL
Unit 3 Chaos and Nonlinear Dynamics, Nonlinearity Detection: Information-Based Methods	No Change	NIL
Unit 4 Image Processing: Filters, Transformations, and Registration, Image Segmentation, Image Acquisition and Reconstruction	No Change	NIL
Unit 5 Classification I: Linear Discriminant Analysis and Support Vector Machines, Classification II: Adaptive Neural Nets	No Change	NIL

Biomedical Image Processing Practical

COURSE CODE: MITS3P3b **COURSE CREDIT: 02**

Course Objectives:

- Understand basics of Bio signals and various classical techniques of bio signal processing.
- Understand various modern spectral analysis techniques.
- Understand and apply various multivariate analysis techniques on bio signals.
- Understand and apply various transformations filters to images, and different techniques for image acquisition and construction.
- Understand the AI perspective in biological image processing using SVM and NeuralNetworks.

List of Practical:

10 practicals covering the entire syllabus must be performed. The detailed list ofpractical will be circulated later in the official workshop.

Cloud Management

COURSE CODE: MITS303c **COURSE CREDIT: 04**

Course Objectives:

- To Understand the Fundamental Ideas Behind Cloud Computing, The Evolution Of The Paradigm, Its Applicability; Benefits, As Well As Current And Future Challenges;
- The Basic ideas And Principles In Data Center Design; Cloud Management Techniques And Cloud Software Deployment Considerations;
- Different CPU, Memory And I/O Virtualization Techniques That Serve In Offering Software, Computation
- And Storage Services On The Cloud; Software Defined Networks (SDN) And Software Defined Storage (SDS);
- Cloud Storage Technologies And Relevant Distributed File Systems, Nosql Databases And Object Storage;
- The Variety Of Programming Models And Develop Working Experience In Several Of Them.

Sr. No	Modules/Units	No of Lectures
1.	What is VMM? What's new in VMM Get Started Release notes - VMM Turn telemetry data on/off Deploy a VMM cloud Create a VMM cloud Manage a VMM cloud Deploy a guarded host fabric Deploy guarded hosts Configure fallback HGS settings Deploy a shielded VHDX and VM template Deploy a shielded VM Deploy a shielded Linux VM Deploy and manage a software defined network (SDN) infrastructure Deployan SDN network controller Deploy an SDN SLB Deploy an SDN RAS gateway Deploy SDN using PowerShell Set up a VM network in SDN Encrypt VM networks in SDN Allow and block VMtraffic with SDN port ACLs Control SDN virtualnetwork bandwidth with QoS Load balance network traffic Set up NAT for traffic forwarding in an SDNRoute traffic across networks in the SDN infrastructure Configure SDN guest clusters Update the NC servercertificate Set up SDN SLB VIPs Back up and restore the SDN infrastructure Remove an SDN from VMM Manage SDN resources in the VMM fabric Deploy and manage Storage Spaces Direct Set up a hyper-converged Storage Spaces Direct cluster Set up a disaggregated Storage Spaces Direct cluster Manage Storage Spaces Direct clusters Assign storage QoS policies for Clusters How To Plan System requirements – VMM Plan VMM installation Plan a VMM high availability deployment Identify VMM ports and protocols Plan the VMM compute fabric Plan the VMM networking fabric Identify supported storage arrays Upgrade and install Upgrade VMM Install VMM Install the VMM console Enable	12

	enhanced console session Deploy VMM for high availability Deploy a highly available VMM management server Deploy a highly available SQL Server database for VMM Deploy a highly available VMM library Set up TLS 1.2 Deploy update rollups Back up and restore VMM Manage the VMM library Library overview Add file-based resources to the VMM library Add profiles to the VMM library Add VM templates to the VMM library Add service templates to the VMM library Manage VMM library resources Manage virtualization servers Manage VMM host groups Addexisting Hyper-V hosts and clusters to the fabric Add a Nano server as a Hyper-V host or cluster Run a script on host Create a cluster from standalone Hyper-V hosts Provision a Hyper-V host or cluster from bare-metal Create a guest Hyper-V cluster from a service template Set up networking for Hyper-V hosts and clusters Set up storage for Hyper-V hosts and clusters Manage MPIO for Hyper-V hosts and clusters Manage Hyper-V extended port ACLs Manage Hyper-V clusters Update Hyper-V hosts and clusters Run a rolling upgrade of Hyper-V clusters Service Hyper-V hosts for maintenance Manage VMware servers Manage management servers Manage infrastructure servers Manage update servers Manage networking Network fabric overview Set up logical networks Set up logical networks in UR1 Set up VM networks Set up IP address pools Add a network gateway Set up port profiles Set up logical switches Set up MAC address pools Integrate NLB with service templates Set up an IPAM server Manage storage Set up storage fabric Set up storage classifications Add storage devices Allocate storage to host groups Set up a Microsoft iSCSI Target Server Set up a Virtual Fibre Channel Set up file storage Set up Storage Replica in VMM	
2.	Service Manager What's new in Service Manager Get started Evaluation and activation of Service Manager Service Manager components Supported configurations System requirements - Service Manager Release notes - Service Manager Enable service log on Manage telemetrysettings How to Plan Planning for Service Manager Plan for deployment Service Manager editions Recommended deployment topologies Operations Manager considerations ServiceManager databases Port assignments Prepare for deployment Service Manager performance Plan for performance and scalability Plan for hardware performance Deploy Deploy Service Manager Deployment scenarios Install on a single computer Install on two computers Install on four computers Set up remote SQL Server Reporting Services Use SQL Server AlwaysOn availability groups for failover Create and deploy server images Install on VMs Configure PowerShell Register with the data warehouseto enable reporting Deploy additional management servers Deployment considerations with a disjointednamespace Learn about the new	12

	Self Service portal Deploy the Self-Service portal Set up load balancing Back up the encryption key Index non-Englishknowledge articles Troubleshoot deployment issues Deploy fromacommand line Move databases Upgrade Upgrade Service Manager Upgrade the self-service portal to Service Manager 2016 Upgrade SQL Server Reporting Services Set up a lab environment for upgrade Prepare the productionenvironment Prepare the lab environment Run an upgrade Complete tasks after upgrade Troubleshoot upgrade issues Administer Use management packs to add functionality Use connectors to import data Import data from Active Directory Domain Services Import data and alerts from Operations Manager Import data from Configuration Manager Import runbooks from Orchestrator Import data from VMM Use a CSV file to import data Optionally disable ECL logging for faster connector synchronization Configuration items Configure incident management Configure service level management Configure workflows Configure change and activity management Configure release management Configure Desired Configuration Management to generate incidents Configure notifications Use the service catalog to offer services Use groups, queues, and lists in Service Manager Use runbooks to automate procedures User interface customization Manage user roles Manage Run As accounts Manageknowledge articles Configure and use Service Manager cmdlets Manage the data warehouse Register source systems to the data warehouse Troubleshoot computer problems with tasks Configure your preference for sharing diagnostic and usage data Operate Search for information Manage incidents andproblems Manage changes and activities Manage service requests Manage release records Data warehouse reporting and analytics Use and manage standard reports	
3.	What is Configuration Manager? Microsoft Endpoint Configuration Manager FAQ What happened to SCCM? Introduction Find help for Configuration Manager How to use the docs How to use the console Accessibility features Software Center user guide Fundamentals Configuration Manager fundamentals Sites and hierarchies About upgrade, update, and install Manage devices Client management Security Role-based administration Configuration Manager and Windows as aService Plan and design Get ready for Configuration Manager Product changes Features and capabilities Security and privacy for Configuration Manager Security and privacyoverview Plan for security Security best practices and privacyinformation Privacy statement - Configuration Manager Cmdlet Library Additional privacy information Configuresecurity Cryptographic	12

	controls technical reference Enable TLS About enabling TLS Enable TLS on clients Enable TLS on site servers and remote site systems Common issues when enabling TLS 1Migrate data between hierarchies Migration overview Plan for migration Planning for migration Prerequisites for migration Checklists for migration Determine whether to migrate data Planning the source hierarchy Planning migration jobs Planning client migration Planning for content deployment Planning to migrate objects Planning to monitor migration Planning to complete migration Configure source hierarchies and source sites Operations for migrating Security and privacy for migration Deploy servers and roles Deploy servers and roles Install infrastructure Get installation media Before you run setup Setup reference Setup downloader Prerequisite checker Prerequisite checks Installing sites Prepare to install sites overview Prepare to install sites Prerequisites for installing sites Use the setup wizard Use a command-line Command- line overview Command-line options Install consoles Upgrade an evaluation install Upgrade to Configuration Manager Scenarios to streamline your installation Configure sites and hierarchies Configure sites and hierarchies overview Add site system roles Add site system roles overview Install site system roles Install cloud-based distribution points About the service connection point Configuration options for site system roles Database replicas for management points Site components Publish site data Manage content and content infrastructure Content infrastructure overview Install and configure distribution points Deployand manage content Monitor content Microsoft Connected Cache Troubleshoot Microsoft Connected Cache Run discovery Discovery methods overview About discovery methods Select discovery methods Configure discovery methods Site boundaries and boundary groups Site boundaries and boundary groups overview Boundaries Boundary groups Procedures for boundary groups High availability High availability options Site server high availability Flowchart - Passive site server setup Flowchart - Promotesite server (planned) Flowchart - Promote site server (unplanned) Prepare to use SQL Server Always On Configure SQL Server Always On Use a SQL Server cluster Custom locations for database files Configure role-based administration	
4.	What's new in Orchestrator Automate with runbooks Get started Install Orchestrator Work with runbooks in the Orchestrator console Example runbook: Creating a runbook to monitor a folder Release notes – Orchestrator Turn on/off telemetryHow To Plan Database sizing and performance Feature performance considerations System requirements – Orchestrator Design a runbook Deploy Upgrade Orchestrator Deploy runbooks	12

	Configure Orchestrator database connections Migrate Orchestrator between environments Change the Orchestrator database Manage Runbooks Design and build runbooks Create and test a sample runbook Control runbook activities Monitor activities Runbook properties Track runbooks Install TLS Install and enable TLS 1.2 Manage Orchestrator Servers Runbook permissions Backup Orchestrator Bench mark Optimize performance of .Net activities Configure runbook throttling Recover a database Recover web components Add an integration pack View Orchestrator data with PowerPivot Change Orchestrator user groups Common activity properties Computer groups Standard Activities Orchestrator standard activities Alphabetical list of Standard Activities Ports and protocols of Standard Activities System Run Program Run .NET Script End Process Start/Stop Service Restart System Save Event Log Query WMI Run SSH Command Get SNMP Variable Monitor SNMP Trap Send SNMP Trap Set SNMP Variable Scheduling Monitor Date/Time Check Schedule Monitoring Monitor Event Log Monitor Service Get Service Status Monitor Process Get Process Status Monitor Computer/IP Get Computer/IP Status Monitor Disk Space Get Disk Space Status Monitor Internet Application Get Internet Application Status Monitor WMI File Management Compress File Copy File Create Folder Decompress File Delete File Delete Folder Get File Status Monitor File Monitor Folder Move File Move Folder PGP Decrypt File PGP Encrypt File Print File Rename File Email Send Email Notification Send Event Log Message Send Syslog Message Send Platform Event Utilities Apply XSLT Query XML Map Published Data Compare Values Write Web Pages Read Text Log Write to Database Query Database Monitor Counter Get Counter Value Modify Counter Invoke Web Services Format Date/Time Generate Random Text Map Network Path Disconnect Network Path Get Dial-up Status Connect/Disconnect Dial-up Text File Management Append Line Delete Line Find Text Get Lines Insert Line Read Line Search and Replace Text Runbook Control Invoke Runbook Initialize Data Junction Return Data Orchestrator Integration Toolkit Overview of Orchestrator Integration Toolkit Installation Command Line Activity Wizard Integration Pack Wizard Integration Packs Active Directory Active Directory activities Add Computer To Group Add Group To Group Add User To Group Create Computer Create Group Create User Delete Computer Delete Group Delete User Disable Computer Disable User Enable Computer Enable User Get Computer Get Group Get Organizational Unit Get User Move Computer Move Group Move User Remove Computer From Group Remove Group From Group Remove User From Group Rename	

	Group Rename User Reset User Password Unlock User Update Computer Update Group Update User	
5.	Data Protection Manager How does DPM work? What can DPM back up? DPM-compatible tape libraries Get Started DPM build versions DPM release notes What's new in DPM What DPM supports How To Plan Your DPM Environment Get ready to deploy DPMservers Prepare your environment for DPM Prepare data storage Identify compatible tape libraries Identify data sources you want to protect Install or Upgrade DPM Install DPM Upgrade your DPM installation Add Modern Backupstorage Deduplicate DPM storage Deploy DPM Deploy the DPM protection agent Deploy protection groups Configure firewall settings Offline backup Using own disk ProtectWorkloads Back up Hyper-V virtual machines Back up Exchange with DPM Back up SharePoint with DPM Back up SQL Server with DPM Back up client computers with DPM Back up file data with DPM Backup system state and bare metal Back up and restore VMware servers Back up and restore VMM servers Prepare to back up a generic data source Prepare machines in workgroups and untrusted domains for backup Back up the DPM server Monitor and Manage Monitor DPM Set up DPM logging Generate DPM reports Use SCOM to manage and monitor DPM servers Improve replication performance Use central console to manage DPM servers	12

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Microsoft SCVMM 2019	Whitepaper	Microsoft		2019
2.	Microsoft Endpoint Manager 2019	Whitepaper	Microsoft		2019
3.	Microsoft SCO 2019	Whitepaper	Microsoft		2019
4.	Microsoft SCOM 2019	Whitepaper	Microsoft		2019
5.	Microsoft SCSM 2019	Whitepaper	Microsoft		2019
6.	Microsoft DPM 2019	Whitepaper	Microsoft		2019
7.	Introducing Microsoft	Mitch Tulloch with	Microsoft		2012
	System Center 2012	Symon Perriman and the System Center Team	Press		

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 What is VMM? What's new in VMM	No Change	NIL
Unit 2 Service Manager What's new in Service Manager Get started	No Change	NIL
Unit 3 What is Configuration Manager?, Introduction	No Change	NIL
Unit 4 What's new in Orchestrator Automate with runbooks Get started	No Change	NIL
Unit 5 Data Protection Manager How does DPM work?	No Change	NIL

Cloud Management Practical

COURSE CODE: MITS3P3c **COURSE CREDIT: 02**

Course Objectives:

- To understand the concepts of VMM, SDN, NAS, HyperV etc.
- To understand and demonstrate the use of Service manager with various deployments that can be performed using it.
- To understand SCCM and demonstrate the use of Configuration Manager.
- To understand automation with runbooks and demonstrate the use of Windows Orchestrator.
- To understand and demonstrate the use of Data Protection Manager.

List of Practical:	
1.	a. Create and Manage Cloud using SCVMM 2019
	b. Deploy a guarded host fabric using Microsoft SCVMM 2019
2.	a. Deploy and manage SDN Infra structure using SCVMM 2019
	b. Deploy and Manage Storage Space Direct (S2D) using SCVMM 2019
3.	a. Deploy Service Manager 2019 and install on 4 Computer Scenario
	b. Setup SQL Server reporting Service using Service Manager 2019
4.	a. User Connectors to import data: i. Import data from Active Directory Domain Services ii. Import data and alerts from Operations Manager iii. Import data from Configuration Manager iv. Import runbooks from Orchestrator v. Import data from VMM vi. Use a CSV file to import data
	b. Automate IT processes with workflows vii. Add or remove workflow activities viii. Configure the way activities manage and pass information ix. Deploy a workflow to Service Manager using the Authoring Tool x. Configure the Activities Toolbox in the Authoring Tool
5.	a. Managing devices with Configuration Manager
	b. Design a hierarchy of sites using Microsoft End Point Configuration manager.
6.	a. Data transfers between sites i. Types of data transfer ii. File-based replication iii. Database replication
	b. Configure sites and hierarchies i. Add site system roles ii. Install site system roles iii. Install cloud-based distribution points iv. Configuration options for site system roles v. Database replicas for management points
7.	a. Install Orchestrator.
	b. Create and test a monitor runbook

8.	a. Manage Orchestrator Servers - 1 i. Runbook permissions
	ii. Back up Orchestrator iii. Bench mark iv. Optimize performance of .Net activities v. Configure runbook throttling vi. Recover a database
	b. Manage Orchestrator Servers - 2 i. Recover web components ii. Add an integration pack iii. View Orchestrator data with PowerPivot iv. Change Orchestrator user groups v. Common activity properties vi. Computer groups
9.	Install and Deploy DPM i. Install DPM ii. Deploy the DPM protection agent iii. Deploy protection groups iv. Configure firewall settings
10.	Protect Workloads i. Back up Hyper-V virtual machines ii. Back up SQL Server with DPM iii. Back up file data with DPM iv. Backup system state and bare metal v. Backup and restore VMware servers vi. Backup and restore VMM servers

Malware Analysis

COURSE CODE: MITS303d **COURSE CREDIT: 04**

Course Objectives:

- Possess the skills necessary to carry out independent analysis of modern malware samples using both static and dynamic analysis techniques.
- Have an intimate understanding of executable formats, Windows internals and API, and analysis techniques.
- Extract investigative leads from host and network-based indicators associated with a malicious program.
- Apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples.
- Achieve proficiency with industry standard tools including IDA Pro, OllyDbg, WinDBG, PE Explorer, ProcMon etc.

Sr. No	Modules/Units	No of Lectures
1.	**Malware Analysis:** Introduction, Techniques, Types of malware, General rules for Malware Analysis. **Basic Static Techniques:** Antivirus Scanning, Hashing, Finding Strings, Packed and Obfuscated Malware, Portable Executable Malware, Portable executable File Format, Linked Libraries and Functions, Static Analysis, The PE file headers and sections. **Malware Analysis in Virtual Machines:** Structure of VM, Creating and using Malware Analysis machine, Risks of using VMware for malware analysis, Record/Replay. **Basic Dynamic Analysis:** Sandboxes, Running Malware, Monitoring with process monitor, Viewing processes with process explorer, Comparing registry snapshots with regshot, Faking a network, Packet sniffing with Wireshark, Using INetSim, Basic Dynamic Tools. x86 Disassembly	12
2.	**IDA PRO:** Loading an executable, IDA Pro Interface, Using cross references, Analysing functions, Using graphing options, Enhancing disassembly, Extending IDA with plug-ins. **Recognising C Code constructs in assembly:** Global v/s local variables, Disassembling arithmetic operations, recognizing if statements, recognizing loops, function call conventions, Analysing switch statements, Disassembling arrays, Identifying structs, Analysing linked list traversal. **Analysing Malicious Windows Programs:** The windows API, The Windows Registry, Networking APIs, Understanding running malware. Kernel v/s user mode, Native API. **Advanced Dynamic Analysis – Debugging:** Source- level v/s Assembly-level debugging, kernel v/s user mode debugging, Using a debugger, Exceptions, Modifying execution with a debugger, modifying program execution.	12

3.	**Advanced Dynamic Analysis – OLLYDBG:** Loading Malware, The Ollydbg Interface, Memory Map, Viewing threads and Stacks, Executing code, Breakpoints, Loading DLLs, Tracing, Exception handling, Patching, Analysing shell code, Assistance features, Plug-ins, Scriptable debugging. **Kernel Debugging with WINDBG:** Drivers and kernel code, Using WinDbg, Microsoft Symbols, kernel debugging and using it, Rootkits, Loading drivers, kernel issues with windows. **Malware Functionality – Malware Behavior:** Downloaders and launchers, Backdoors, Credential stealers, Persistence mechanisms, Privilege escalation, covering the tracks. **Covert Malware Launching:** Launchers, Process injection, Process replacement, Hook injection, detours, APC injection.	12
4.	**Data Encoding:** Goal of Analysing algorithms, Simple ciphers, Common cryptographic algorithms, Custom encoding, decoding. **Malware – focused network signatures:** Network countermeasures**,** Safely investigating attacker online, Content-Based Network Countermeasures, Combining Dynamic and Static Analysis Techniques, Understanding the Attacker's Perspective**.** **Anti-disassembly:** Concepts, Defeating disassembly algorithms, anti-disassembly techniques, Obscuring flow control, Thwarting stack-frame analysis. **Anti-debugging:** Windows debugger detection, debugger behavior, Interfering with debugger functionality, Debugger vulnerabilities.	12
5.	**Anti-virtual machine techniques:** VMWare artifacts, Vulnerable functions, Tweaking settings, Escaping the virtual machine. **Packers and unpacking:** Packer anatomy, Identifying Packed Programs, Unpacking options, Automated Unpacking, Manual Unpacking, Common packers, Analysing without unpacking, Packed DLLs, **Shellcode Analysis:** Loading shellcode for analysis, Position-independent Code, Identifying Execution Location, Manual Symbol Resolution, Shellcode encoding, NOP Sleds, Finding Shellcode. **C++ Analysis:** OOP, Virtual and Non-virtual functions, Creating and destroying objects. **64-bit Malware:** Why 64-bit malware? Differences in x64 architecture, Windows 32-bit on Windows 64-bit,64-bit hints at malware functionality.	12

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Practical Malware Analysis – The Hands-On Guide to Dissecting Malicious Software	Michael Sikorski, Andrew Honig	No Scratch Press	-	2013
2.	Mastering Malware Analysis	Alexey Kleymenov, Amr Thabet	Packt Publishing	-	2019
3.	Windows Malware Analysis Essentials	Victor Marak	Packt Publishing		2015

Note:

Particulars (University syllabus)	**Proposed Syllabus**	**Remarks**
Unit 1 Malware Analysis, Basic Static Techniques, Malware Analysis in Virtual Machines, Basic Dynamic Analysis	No Change	NIL
Unit 2 IDA PRO, Recognising C Code constructs in assembly, Analysing Malicious Windows Programs, Advanced Dynamic Analysis – Debugging	No Change	NIL
Unit 3 Advanced Dynamic Analysis – OLLYDBG, Kernel Debugging with WINDBG, Malware Functionality – Malware Behavior, Covert Malware Launching	No Change	NIL
Unit 4 Data Encoding, Malware – focused network signatures, Anti-disassembly, Anti-debugging	No Change	NIL
Unit 5 Anti-virtual machine techniques, Packers and unpacking, Shellcode Analysis, C++ Analysis, 64-bit Malware	No Change	NIL

Malware Analysis Practical

COURSE CODE: MITS3P3d **COURSE CREDIT: 02**

Course Objectives:

- To understand various introductory techniques of malware analysis and creating thetesting environment.
- To perform advanced dynamic analysis and recognize constructs in assembly code.
- To perform Reverse Engineering using OLLYDBG and WINDBG and study the behaviours and functions of malware.
- To understand data encoding, various techniques for anti-disassembly and anti-debugging.
- To understand various anti virtual machine techniques and perform shellcode analysis of various languages along with x64 architecture.

List of Practical:	
1.	a. Files: *Lab01-01.exe* and *Lab01-01.dll*.
	i. Upload the files to *http://www.VirusTotal.com/* and view the reports. Does either file match any existing antivirus signatures?
	ii. When were these files compiled?
	iii. Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators?
	iv. Do any imports hint at what this malware does? If so, which imports are they?
	v. Are there any other files or host-based indicators that you could look for on infected systems?
	vi. What network-based indicators could be used to find this malware on infected machines?
	vii. What would you guess is the purpose of these files?
	b. Analyze the file *Lab01-02.exe*.
	i. Upload the *Lab01-02.exe* file to *http://www.VirusTotal.com/*. Does it match any existing antivirus definitions?
	ii. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.
	iii. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
	iv. What host- or network-based indicators could be used to identify this malware on infected machines?
	c. Analyze the file Lab01-03.exe.
	i. Upload the *Lab01-03.exe* file to *http://www.VirusTotal.com/*. Does it match any existing antivirus definitions?
	ii. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.
	iii. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
	iv. What host- or network-based indicators could be used to identify this malware on infected machines?
	d. Analyze the file Lab01-04.exe.
	i. Upload the *Lab01-04.exe* file to *http://www.VirusTotal.com/*. Does it match any existing antivirus definitions?
	ii. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

	iii. When was this program compiled?
	iv. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
	v. What host- or network-based indicators could be used to identify this malware on infected machines?
	vi. This file has one resource in the resource section. Use Resource Hacker to examine that resource, and then use it to extract the resource. What can you learn from the resource?
	e. Analyze the malware found in the file Lab03-01.exe using basic dynamic analysis tools.
	i. What are this malware's imports and strings?
	ii. What are the malware's host-based indicators?
	iii. Are there any useful network-based signatures for this malware? If so, what are they?
	f. Analyze the malware found in the file Lab03-02.dll using basic dynamic analysis tools.
	i. How can you get this malware to install itself?
	ii. How would you get this malware to run after installation?
	iii. How can you find the process under which this malware is running?
	iv. Which filters could you set in order to use procmon to glean information?
	v. What are the malware's host-based indicators?
	vi. Are there any useful network-based signatures for this malware?
	g. Execute the malware found in the file Lab03-03.exe while monitoring it using basic dynamic analysis tools in a safe environment
	i. What do you notice when monitoring this malware with Process Explorer?
	ii. Can you identify any live memory modifications?
	iii. What are the malware's host-based indicators?
	iv. What is the purpose of this program?
	h. Analyze the malware found in the file Lab03-04.exe using basic dynamic analysis tools.
	i. What happens when you run this file?
	ii. What is causing the roadblock in dynamic analysis?
	iii. Are there other ways to run this program?
2.	a. Analyze the malware found in the file Lab05-01.dll using only IDA Pro. The goal of this lab is to give you hands-on experience with IDA Pro. If you've already worked with IDA Pro, you may choose to ignore these questions and focus on reverse- engineering the malware.
	i. What is the address of DllMain?
	ii. Use the Imports window to browse to gethostbyname. Where is the import located?
	iii. How many functions call gethostbyname?
	iv. Focusing on the call to gethostbynamelocated at 0x10001757, can you fig-ure out which DNS request will be made?
	v. How many local variables has IDA Pro recognized for the subroutine at 0x10001656?
	vi. How many parameters has IDA Pro recognized for the subroutine at 0x10001656?
	vii. Use the Strings window to locate the string \cmd.exe /cin the disassembly. Where is it located?
	viii. What is happening in the area of code that references \cmd.exe/c?
	ix. In the same area, at 0x100101C8, it looks like dword_1008E5C4 is a global

	variable that helps decide which path to take. How does the malware set dword_1008E5C4? (Hint: Use dword_1008E5C4's cross-references.)
	x. A few hundred lines into the subroutine at 0x1000FF58, a series of com- parisons use memcmpto compare strings. What happens if the string compar- ison to robotwork is successful (when memcmpreturns 0)?
	xi. What does the export PSLISTdo?
	xii. Use the graph mode to graph the cross-references from sub_10004E79. Which API functions could be called by entering this function? Based on the API functions alone, what could you rename this function?
	xiii. How many Windows API functions does DllMaincall directly? How many at a depth of 2?
	xiv. At 0x10001358, there is a call to Sleep (an API function that takes one parameter containing the number of milliseconds to sleep). Looking backward through the code, how long will the program sleep if this code executes?
	xv. At 0x10001701 is a call to socket. What are the three parameters?
	xvi. Using the MSDN page for socketand the named symbolic constants func- tionality in IDA Pro, can you make the parameters more meaningful? What are the parameters after you apply changes?
	xvii. Search for usage of the in instruction (opcode 0xED). This instruction is used with a magic string VMXh to perform VMware detection. Is that in use in this malware? Using the cross-references to the function that executes the in instruction, is there further evidence of VMware detection?
	xviii. Jump your cursor to 0x1001D988. What do you find?
	xix. If you have the IDA Python plug-in installed (included with the com- mercial version of IDA Pro), run Lab05-01.py, an IDA Pro Python script provided with the malware for this book. (Make sure the cursor is at 0x1001D988.) What happens after you run the script?
	xx. With the cursor in the same location, how do you turn this data into a single ASCII string?
	xxi. Open the script with a text editor. How does it work?
	b. analyze the malware found in the file Lab06-01.exe.
	i. What is the major code construct found in the only subroutine called by main?
	ii. What is the subroutine located at 0x40105F?
	iii. What is the purpose of this program?
	c. Analyze the malware found in the file Lab06-02.exe.
	i. What operation does the first subroutine called by mainperform?
	ii. What is the subroutine located at 0x40117F?
	iii. What does the second subroutine called by maindo?
	iv. What type of code construct is used in this subroutine?
	v. Are there any network-based indicators for this program?
	vi. What is the purpose of this malware?
	d. analyze the malware found in the file Lab06-03.exe.
	i. Compare the calls in main to Lab 6-2's main method. What is the new function called from main?
	ii. What parameters does this new function take?
	iii. What major code construct does this function contain?
	iv. What can this function do?
	v. Are there any host-based indicators for this malware?
	vi. What is the purpose of this malware?
	e. analyze the malware found in the file Lab06-04.exe.
	i. What is the difference between the calls made from the main method in Labs 6-3 and 6-4?

	ii. What new code construct has been added to main?
	iii. What is the difference between this lab's parse HTML function and those of the previous labs?
	iv. How long will this program run? (Assume that it is connected to the Internet.)
	v. Are there any new network-based indicators for this malware?
	vi. What is the purpose of this malware?
3.	a. Analyze the malware found in the file Lab07-01.exe.
	i. How does this program ensure that it continues running (achieves per-sistence) when the computer is restarted?
	ii. Why does this program use a mutex?
	iii. What is a good host-based signature to use for detecting this program?
	iv. What is a good network-based signature for detecting this malware?
	v. What is the purpose of this program?
	vi. When will this program finish executing?
	b. Analyze the malware found in the file Lab07-02.exe.
	i. How does this program achieve persistence?
	ii. What is the purpose of this program?
	iii. When will this program finish executing?
	c. For this lab, we obtained the malicious executable, Lab07-03.exe, and DLL, Lab07- 03.dll, prior to executing. This is important to note because the mal- ware might change once it runs. Both files were found in the same directory on the victim machine. If you run the program, you should ensure that both files are in the same directory on the analysis machine. A visible IP string beginning with 127 (a loopback address) connects to the local machine. (In the real version of this malware, this address connects to a remote machine, but we've set it to connect to localhost to protect you.)
	i. How does this program achieve persistence to ensure that it continues running when the computer is restarted?
	ii. What are two good host-based signatures for this malware?
	iii. What is the purpose of this program?
	iv. How could you remove this malware once it is installed?
	d. Analyze the malware found in the file Lab09-01.exe using OllyDbg and IDA Pro to answer the following questions. This malware was initially analyzed in the Chapter 3 labs using basic static and dynamic analysis techniques.
	i. How can you get this malware to install itself?
	ii. What are the command-line options for this program? What is the pass- word requirement?
	iii. How can you use OllyDbg to permanently patch this malware, so that it doesn't require the special command-line password?
	iv. What are the host-based indicators of thismalware?
	v. What are the different actions this malware can be instructed to take via the network?
	vi. Are there any useful network-based signatures for this malware?
	e. Analyze the malware found in the file Lab09-02.exe using OllyDbg to answer the following questions.
	i. What strings do you see statically in the binary?
	ii. What happens when you run this binary?
	iii. How can you get this sample to run its malicious payload?
	iv. What is happening at 0x00401133?
	v. What arguments are being passed to subroutine 0x00401089?
	vi. What domain name does this malware use?

	vii. What encoding routine is being used to obfuscate the domainname?
	viii. What is the significance of the CreateProcessAcall at 0x0040106E?
	f. Analyze the malware found in the file Lab09-03.exe using OllyDbg and IDA Pro. This malware loads three included DLLs (DLL1.dll, DLL2.dll, and DLL3.dll) that are all built to request the same memory load location. Therefore, when viewing these DLLs in OllyDbg versus IDA Pro, code may appear at different memory locations. The purpose of this lab is to make you comfortable with finding the correct location of code within IDA Pro when you are looking at code in OllyDbg
	i. What DLLs are imported by Lab09-03.exe?
	ii. What is the base address requested by DLL1.dll, DLL2.dll, and DLL3.dll?
	iii. When you use OllyDbg to debug Lab09-03.exe, what is the assigned based address for: DLL1.dll, DLL2.dll, and DLL3.dll?
	iv. When Lab09-03.exe calls an import function from DLL1.dll, what does this import function do?
	v. When Lab09-03.exe calls WriteFile, what is the filename it writes to?
	vi. When Lab09-03.exe creates a job using NetScheduleJobAdd, where does it get the data for the second parameter?
	vii. While running or debugging the program, you will see that it prints out three pieces of mystery data. What are the following: DLL 1 mystery data 1, DLL 2 mystery data 2, and DLL 3 mystery data 3?
	viii. How can you load DLL2.dll into IDA Pro so that it matches the load address used by OllyDbg?
4.	a. This lab includes both a driver and an executable. You can run the executable from anywhere, but in order for the program to work properly, the driver must be placed in the C:\Windows\ System32 directory where it was origi- nally found on the victim computer. The executable is Lab10-01.exe, and the driver is Lab10-01.sys.
	i. Does this program make any direct changes to the registry? (Use procmon to check.)
	ii. The user-space program calls the ControlService function. Can you set a breakpoint with WinDbg to see what is executed in the kernel as a result of the call to ControlService?
	iii. What does this program do?
	b. The file for this lab is Lab10-02.exe.
	i. Does this program create any files? If so, what are they?
	ii. Does this program have a kernel component?
	iii. What does this program do?
	c. This lab includes a driver and an executable. You can run the executable from anywhere, but in order for the program to work properly, the driver must be placed in the C:\Windows\System32 directory where it was originally found on the victim computer. The executable is Lab10-03.exe, and the driver is Lab10-03.sys.
	i. What does this program do?
	ii. Once this program is running, how do you stop it?
	iii. What does the kernel component do?
5.	a. Analyze the malware found in Lab11-01.exe
	i. What does the malware drop to disk?
	ii. How does the malware achieve persistence?
	iii. How does the malware steal user credentials?
	iv. What does the malware do with stolen credentials?
	v. How can you use this malware to get user credentials from your test environment?

	b. Analyze the malware found in Lab11-02.dll. Assume that a suspicious file named Lab11-02.ini was also found with this malware.
	i. What are the exports for this DLL malware?
	ii. What happens after you attempt to install this malware using
	iii. rundll32.exe?
	iv. Where must Lab11-02.ini reside in order for the malware to install properly?
	v. How is this malware installed for persistence?
	vi. What user-space rootkit technique does this malware employ?
	vii. What does the hooking code do?
	viii. Which process(es) does this malware attack and why?
	ix. What is the significance of the .ini file?
	c. Analyze the malware found in Lab11-03.exe and Lab11-03.dll. Make sure that both files are in the same directory during analysis
	i. What interesting analysis leads can you discover using basic static analysis?
	ii. What happens when you run this malware?
	iii. How does Lab11-03.exe persistently install Lab11-03.dll?
	iv. Which Windows system file does the malware infect?
	v. What does Lab11-03.dll do?
	vi. Where does the malware store the data it collects?
6.	a. Analyze the malware found in the file Lab12-01.exe and Lab12-01.dll. Make sure that these files are in the same directory when performing the analysis.
	i. What happens when you run the malware executable?
	ii. What process is being injected?
	iii. How can you make the malware stop the pop-ups?
	iv. How does this malware operate?
	b. Analyze the malware found in the file Lab12-02.exe.
	i. What is the purpose of this program?
	ii. How does the launcher program hide execution?
	iii. Where is the malicious payload stored?
	iv. How is the malicious payload protected?
	v. How are strings protected?
	c. Analyze the malware extracted during the analysis of Lab 12-2, or use the file Lab12-03.exe.
	i. What is the purpose of this malicious payload?
	ii. How does the malicious payload inject itself?
	iii. What filesystem residue does this program create?
	d. Analyze the malware found in the file Lab12-04.exe.
	i. What does the code at 0x401000 accomplish?
	ii. Which process has code injected?
	iii. What DLL is loaded using LoadLibraryA?
	iv. What is the fourth argument passed to the CreateRemoteThread call?
	v. What malware is dropped by the main executable?
7.	a. Analyze the malware found in the file Lab13-01.exe.
	i. Compare the strings in the malware (from the output of the strings command) with the information available via dynamic analysis. Based on this comparison, which elements might be encoded?
	ii. Use IDA Pro to look for potential encoding by searching for the string xor. What type of encoding do you find?
	iii. What is the key used for encoding and what content does it encode?
	iv. Usethestatictools FindCrypt2, Krypto ANALyzer(KANAL), and the IDA Entropy Plugin to identify any other encoding mechanisms. What do you

	find?
	v. What type of encoding is used for a portion of the network traffic sent by the malware?
	vi. Where is the Base64 function in the disassembly?
	vii. What is the maximum length of the Base64-encoded data that is sent? What is encoded?
	viii. In this malware, would you ever see the padding characters (=or ==) in the Base64-encoded data?
	ix. What does this malware do?
	b. Analyze the malware found in the file Lab13-02.exe.
	i. Using dynamic analysis, determine what this malware creates.
	ii. Use static techniques such as an xor search, FindCrypt2, KANAL, and the IDA Entropy Plugin to look for potential encoding. What do you find?
	iii. Based on your answer to question 1, which imported function would be a good prospect for finding the encoding functions?
	iv. Where is the encoding function in the disassembly?
	v. Trace from the encoding function to the source of the encoded content. What is the content?
	vi. Can you find the algorithm used for encoding? If not, how can you decode the content?
	vii. Using instrumentation, can you recover the original source of one of the encoded files?
	c. Analyze the malware found in the file Lab13-03.exe.
	i. Compare the output of strings with the information available via dynamic analysis. Based on this comparison, which elements might be encoded?
	ii. Use static analysis to look for potential encoding by searching for the string xor. What type of encoding do you find?
	iii. Use static tools like FindCrypt2, KANAL, and the IDA Entropy Plugin to identify any other encoding mechanisms. How do these findings com- pare with the XOR findings?
	iv. Which two encoding techniques are used in thismalware?
	v. For each encoding technique, what is the key?
	vi. For the cryptographic encryption algorithm, is the key sufficient? What else must be known?
	vii. What does this malware do?
	viii. Create code to decrypt some of the content produced during dynamic analysis. What is this content?
8.	a. Analyze the malware found in file Lab14-01.exe. This program is not harmful to your system.
	i. Which networking libraries does the malware use, and what are their advantages?
	ii. What source elements are used to construct the networking beacon, and what conditions would cause the beacon to change?
	iii. Why might the information embedded in the networking beacon be of interest to the attacker?
	iv. Does the malware use standard Base64 encoding? If not, how is the encoding unusual?
	v. What is the overall purpose of this malware?
	vi. What elements of the malware's communication may be effectively detected using a network signature?
	vii. What mistakes might analysts make in trying to develop a signature for this malware?
	viii. What set of signatures would detect this malware (and future variants)?
	b. Analyze the malware found in file Lab14-02.exe. This malware has been

	configured to beacon to a hard-coded loopback address in order to prevent it from harming your system, but imagine that it is a hard-coded external address.
	i. What are the advantages or disadvantages of coding malware to use direct IP addresses?
	ii. Which networking libraries does this malware use? What are the advantages or disadvantages of using these libraries?
	iii. What is the source of the URL that the malware uses for beaconing? What advantages does this source offer?
	iv. Which aspect of the HTTP protocol does the malware leverage to achieve its objectives?
	v. What kind of information is communicated in the malware's initial beacon?
	vi. What are some disadvantages in the design of this malware's communication channels?
	vii. Is the malware's encoding scheme standard?
	viii. How is communication terminated?
	ix. What is the purpose of this malware, and what role might it play in the attacker's arsenal?
	c. This lab builds on Practical 8 a. Imagine that this malware is an attempt by the attacker to improve his techniques. Analyze the malware found in file Lab14-03.exe.
	i. What hard-coded elements are used in the initial beacon? What elements, if any, would make a good signature?
	ii. What elements of the initial beacon may not be conducive to a longlasting signature?
	iii. How does the malware obtain commands? What example from the chapter used a similar methodology? What are the advantages of this technique?
	iv. When the malware receives input, what checks are performed on the input to determine whether it is a valid command? How does the attacker hide the list of commands the malware is searching for?
	v. What type of encoding is used for command arguments? How is it different from Base64, and what advantages or disadvantages does it offer?
	vi. What commands are available to this malware?
	vii. What is the purpose of this malware?
	viii. This chapter introduced the idea of targeting different areas of code with independent signatures (where possible) in order to add resiliency to network indicators. What are some distinct areas of code or configuration data that can be targeted by network signatures?
	ix. What set of signatures should be used for this malware?
	d. Analyze the sample found in the file Lab15-01.exe. This is a command-line program that takes an argument and prints "Good Job!" if the argument matches a secret code.
	i. What anti-disassembly technique is used in this binary?
	ii. What rogue opcode is the disassembly tricked into disassembling?
	iii. How many times is this technique used?
	iv. What command-line argument will cause the program to print "Good Job!"?
	e. Analyze the malware found in the file Lab15-02.exe. Correct all anti-disassembly countermeasures before analyzing the binary in order to answer the questions.
	i. What URL is initially requested by the program?
	ii. How is the User-Agent generated?
	iii. What does the program look for in the page it initially requests?
	iv. What does the program do with the information it extracts from the page?
	f. Analyze the malware found in the file Lab15-03.exe. At first glance, this binary appears to be a legitimate tool, but it actually contains more functionality than

	advertised.
	i. How is the malicious code initially called?
	ii. What does the malicious code do?
	iii. What URL does the malware use?
	iv. What filename does the malware use?
9.	a. Analyze the malware found in Lab16-01.exe using a debugger. This is the same malware as Lab09-01.exe, with added anti-debugging techniques.
	i. Which anti-debugging techniques does this malware employ?
	ii. What happens when each anti-debugging technique succeeds?
	iii. How can you get around these anti-debugging techniques?
	iv. How do you manually change the structures checked during runtime?
	v. Which OllyDbg plug-in will protect you from the anti-debugging techniques used by this malware?
	b. Analyze the malware found in Lab16-02.exe using a debugger. The goal of this lab is to figure out the correct password. The malware does not drop a mali- cious payload.
	i. What happens when you run Lab16-02.exe from the command line?
	ii. What happens when you run Lab16-02.exe and guess the command-line parameter?
	iii. What is the command-line password?
	iv. Load Lab16-02.exe into IDA Pro. Where in the mainfunction is strncmp
	v. found?
	vi. What happens when you load this malware into OllyDbg using the default settings?
	vii. What is unique about the PE structure of Lab16-02.exe?
	viii. Where is the callback located? (Hint: Use CTRL-E in IDA Pro.)
	ix. Which anti-debugging technique is the program using to terminate immediately in the debugger and how can you avoid this check?
	x. What is the command-line password you see in the debugger after you disable the anti-debugging technique?
	xi. Does the password found in the debugger work on the command line?
	c. Analyze the malware in Lab16-03.exe using a debugger. This malware is similar to Lab09-02.exe, with certain modifications, including the introduction of anti-debugging techniques.
	i. Which strings do you see when using static analysis on the binary?
	ii. What happens when you run this binary?
	iii. How must you rename the sample in order for it to run properly?
	iv. Which anti-debugging techniques does this malware employ?
	v. For each technique, what does the malware do if it determines it is running in a debugger?
	vi. Why are the anti-debugging techniques successful in this malware?
	vii. What domain name does this malware use?
	d. Analyze the malware found in Lab17-01.exe inside VMware. This is the same malware as Lab07-01.exe, with added anti-VMware techniques.
	i. What anti-VM techniques does this malware use?
	ii. If you have the commercial version of IDA Pro, run the IDA Python script from Listing 17-4 in Chapter 17 (provided here as findAntiVM.py). What does it find?
	iii. What happens when each anti-VM technique succeeds?
	iv. Which of these anti-VM techniques work against your virtual machine?
	v. Why does each anti-VM technique work or fail?
	vi. How could you disable these anti-VM techniques and get the malware to run?

	e. Analyze the malware found in the file Lab17-02.dll inside VMware. After answering the first question in this lab, try to run the installation exports using rundll32.exe and monitor them with a tool like procmon. The following is an example command line for executing the DLL: rundll32.exe Lab17-02.dll,InstallRT (or InstallSA/InstallSB)
	i. What are the exports for this DLL?
	ii. What happens after the attempted installation using rundll32.exe?
	iii. Which files are created and what do they contain?
	iv. What method of anti-VM is in use?
	v. How could you force the malware to install during runtime?
	vi. How could you permanently disable the anti-VM technique?
	vii. How does each installation export function work?
	f. Analyze the malware Lab17-03.exe inside VMware.
	i. What happens when you run this malware in a virtual machine?
	ii. How could you get this malware to run and drop its keylogger?
	iii. Which anti-VM techniques does this malware use?
	iv. What system changes could you make to permanently avoid the anti-VM techniques used by this malware?
	v. How could you patch the binary in OllyDbg to force the anti-VM techniques to permanently fail?
10.	a. Analyze the file Lab19-01.bin using shellcode_launcher.exe
	i. How is the shellcode encoded?
	ii. Which functions does the shellcode manually import?
	iii. What network host does the shellcode communicate with?
	iv. What filesystem residue does the shellcode leave?
	v. What does the shellcode do?
	b. The file Lab19-02.exe contains a piece of shellcode that will be injected into another process and run. Analyze this file.
	i. What process is injected with the shellcode?
	ii. Where is the shellcode located?
	iii. How is the shellcode encoded?
	iv. Which functions does the shellcode manually import?
	v. What network hosts does the shellcode communicate with?
	vi. What does the shellcode do?
	c. Analyze the file Lab19-03.pdf. If you get stuck and can't find the shellcode, just skip that part of the lab and analyze file Lab19-03_sc.bin using shellcode_launcher.exe.
	i. What exploit is used in this PDF?
	ii. How is the shellcode encoded?
	iii. Which functions does the shellcode manually import?
	iv. What filesystem residue does the shellcode leave?
	v. What does the shellcode do?
	d. The purpose of this first lab is to demonstrate the usage of the thispointer. Analyze the malware in Lab20-01.exe.
	i. Does the function at 0x401040 take any parameters?
	ii. Which URL is used in the call to URLDownloadToFile?
	iii. What does this program do?
	e. Analyze the malware In Lab20-02.exe.
	i. What can you learn from the interesting strings in this program?
	ii. What do the imports tell you about this program?
	iii. What is the purpose of the object created at 0x4011D9? Does it have any

	virtual functions?
	iv. Which functions could possibly be called by the call [edx] instruction at 0x401349?
	v. How could you easily set up the server that this malware expects in order to fully analyze the malware without connecting it to the Internet?
	vi. What is the purpose of this program?
	vii. What is the purpose of implementing a virtual function call in this program?
	f. Analyze the malware in Lab20-03.exe.
	i. What can you learn from the interesting strings in this program?
	ii. What do the imports tell you about this program?
	iii. At 0x4036F0, there is a function call that takes the string Config error, followed a few instructions later by a call to CxxThrowException. Does the function take any parameters other than the string? Does the function return anything? What can you tell about this function from the context in which it's used?
	iv. What do the six entries in the switch table at 0x4025C8 do?
	v. What is the purpose of this program?
	g. Analyze the code in Lab21-01.exe
	i. What happens when you run this program without any parameters?
	ii. Depending on your version of IDA Pro, main may not be recognized automatically. How can you identify the call to the main function?
	iii. What is being stored on the stack in the instructions from 0x0000000140001150 to 0x0000000140001161?
	iv. How can you get this program to run its payload without changing the filename of the executable?
	v. Which two strings are being compared by the call to strncmp at 0x0000000140001205?
	vi. Does the function at 0x00000001400013C8 take any parameters?
	vii. How many arguments are passed to the call to CreateProcess at 0x0000000140001093? How do you know?
	h. Analyze the malware found in Lab21-02.exe on both x86 and x64 virtual machines.
	i. What is interesting about the malware's resource sections?
	ii. Is this malware compiled for x64 or x86?
	iii. How does the malware determine the type of environment in which it is running?
	iv. What does this malware do differently in an x64 environment versus an x86 environment?
	v. Which files does the malware drop when running on an x86 machine? Where would you find the file orfiles?
	vi. Which files does the malware drop when running on an x64 machine? Where would you find the file or files?
	vii. What type of process does the malware launch when run on an x64 system?
	viii. What does the malware do?

Elective 3

Robotic Process Automation

COURSE CODE: MITS304a **COURSE CREDIT: 04**

Course Objectives:

- To make the students aware about the automation today in the industry.
- To make the students aware about the tools used for automation.
- To help the students automate a complete process.

Sr. No	Modules/Units	No of Lectures
1.	**Robotic Process Automation:** Scope and techniques of automation, About UiPath **Record and Play:** UiPath stack, Downloading and installing UiPath Studio, Learning UiPath Studio, Task recorder, Step-by-step examples using the recorder.	12
2.	**Sequence, Flowchart, and Control Flow:** Sequencing the workflow, Activities, Control flow, various types of loops, and decision making, Step-by-step example using Sequence and Flowchart, Step-by-step example using Sequence and Control flow **Data Manipulation:** Variables and scope, Collections, Arguments – Purpose and use, Data table usage with examples, Clipboard management, File operation with step-by-step example, CSV/Excel to data table and vice versa (with a step-by-step example)	12
3.	**Taking Control of the Controls :** Finding and attaching windows, Finding the control, Techniques for waiting for a control, Act on controls – mouse and keyboard activities, Working with UiExplorer, Handling events, Revisit recorder, Screen Scraping, When to use OCR, Types of OCR available, How to use OCR, Avoiding typical failure points **Tame that Application with Plugins and Extensions:** Terminal plugin, SAP automation, Java plugin, Citrix automation, Mail plugin, PDF plugin, Web integration, Excel and Word plugins, Credential management, Extensions – Java, Chrome, Firefox, and Silverlight	12
4.	**Handling User Events and Assistant Bots:** What are assistant bots?, Monitoring system event triggers, Hotkey trigger, Mouse trigger, System trigger, Monitoring image and element triggers, An example of monitoring email, Example of monitoring a copying event and blocking it, Launching an assistant bot on a keyboard event **Exception Handling, Debugging, and Logging:** Exception handling, Common exceptions and ways to handle them, Logging and taking screenshots, Debugging techniques, Collecting crash dumps, Error reporting	12
5.	**Managing and Maintaining the Code:** Project organization, Nesting workflows, Reusability of workflows, Commenting techniques, State Machine, When to use Flowcharts, State	12

	Machines, or Sequences, Using config files and examples of a config file, Integrating a TFS server **Deploying and Maintaining the Bot:** Publishing using publish utility, Overview of Orchestration Server, Using Orchestration Server to control bots, Using Orchestration Server to deploy bots, License management, Publishing and managing updates	

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Learning Robotic Process Automation	Alok Mani Tripathi	Packt	1st	2018
2.	Robotic Process Automation Tools, Process Automation and their benefits: Understanding RPA and Intelligent Automation	Srikanth Merianda	Createspace Independent Publishing	1st	2018
3.	The Simple Implementation Guide to Robotic Process Automation (Rpa): How to Best Implement Rpa in an Organization	Kelly Wibbenmeyer	iUniverse	1st	2018

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Robotic Process Automation, Record and Play	No Change	NIL
Unit 2 Sequence, Flowchart, and Control Flow, Data Manipulation	No Change	NIL
Unit 3 Taking Control of the Controls, Tame that Application with Plugins and Extensions	No Change	NIL
Unit 4 Handling User Events and Assistant Bots, Exception Handling, Debugging, and Logging	No Change	NIL
Unit 5 Managing and Maintaining the Code, Deploying and Maintaining the Bot	No Change	NIL

Robotic Process Automation Practical

COURSE CODE: MITS3P4a **COURSE CREDIT: 02**

Course Objectives:

- To understand the mechanism of business process and can provide the solution in an optimize way.
- To understand the features use for interacting with database plugins.
- To use the plug-ins and other controls used for process automation.
- To use and handle the different events, debugging and managing the errors.
- To test and deploy the automated process.

List of Practical:	
1.	a. Create a simple sequence based project.
	b. Create a flowchart-based project.
	c. Create an UiPath Robot which can empty a folder in Gmail solely on basis of recording.
2.	a. Automate UiPath Number Calculation (Subtraction, Multiplication, Division of numbers).
	b. Create an automation UiPath project using different types of variables (number, datetime, Boolean, generic, array, data table)
3.	a. Create an automation UiPath Project using decision statements.
	b. Create an automation UiPath Project using looping statements.
4.	a. Automate any process using basic recording.
	b. Automate any process using desktop recording.
	c. Automate any process using web recording.
5.	a. Consider an array of names. We have to find out how many of them start with the letter "a". Create an automation where the number of names starting with "a" is counted and the result is displayed.
6.	a. Create an application automating the read, write and append operation on excel file.
	b. Automate the process to extract data from an excel file into a data table and vice versa
7.	a. Implement the attach window activity.
	b. Find different controls using UiPath.
	c. Demonstrate the following activities in UiPath: i. Mouse (click, double click and hover) ii. Type into iii. Type Secure text
8.	a. Demonstrate the following events in UiPath: i. Element triggering event ii. Image triggering event iii. System Triggering Event
	b. Automate the following screen scraping methods using UiPath i. Full Test ii. Native iii. OCR
	c. Install and automate any process using UiPath with the following plug-ins: i. Java Plugin ii. Mail Plugin iii. PDF Plugin iv. Web Integration

	v. Excel Plugin vi. Word Plugin vii. Credential Management
9.	a. Automate the process of send mail event (on any email).
	b. Automate the process of launching an assistant bot on a keyboard event.
	c. Demonstrate the Exception handing in UiPath.
	d. Demonstrate the use of config files in UiPath.
10.	a. Automate the process of logging and taking screenshots in UiPath.
	b. Automate any process using State Machine in UiPath.
	c. Demonstrate the use of publish utility.
	d. Create and provision Robot using Orchestrator.

Virtual Reality and Augmented Reality

COURSE CODE: MITS304b **COURSE CREDIT: 04**

Course Objectives:

- To learn background of VR including a brief history of VR, different forms of VR and related technologies, and broad overview of some of the most important concepts.
- To provide background in perception to educate VR creators on concepts and theories of how we perceive and interact with the world around us.
- To make learner aware of high-level concepts for designing/building assets and how subtle design choices can influence user behavior.
- To learn about art for VR and AR should be optimized for spatial displays with spatially aware input devices to interact with digital objects in true 3D.
- Walkthrough of VRTK, an open source project meant to spur on cross-platform development.

Sr. No	Modules/Units	No of Lectures
1.	Introduction: What Is Virtual Reality, A History of VR, An Overview of Various Realities, Immersion, Presence, and Reality Trade-Offs, The Basics: Design Guidelines, Objective and Subjective Reality, Perceptual Models and Processes, Perceptual Modalities	12
2.	Perception of Space and Time, Perceptual Stability, Attention, and Action, Perception: Design Guidelines, Adverse Health Effects, Motion Sickness, Eye Strain, Seizures, and Aftereffects, Hardware Challenges, Latency, Measuring Sickness, Reducing Adverse Effects, Adverse Health Effects: Design Guidelines	12
3.	Content Creation, Concepts of Content Creation, Environmental Design, Affecting Behavior, Transitioning to VR Content Creation, Content Creation: Design Guidelines, Interaction, Human- Centered Interaction, VR Interaction Concepts, Input Devices, Interaction Patterns and Techniques, Interaction: Design Guidelines	12
4.	Design and Art Across Digital Realities, Designing for Our Senses, Virtual Reality for Art, 3D Art Optimization, Computer Vision That Makes Augmented Reality Possible Works, Virtual Reality and Augmented Reality: Cross-Platform Theory	12
5.	Virtual Reality Toolkit: Open Source Framework for the Community, Data and Machine Learning Visualization Design and Development in Spatial Computing, Character AI and Behaviors, The Virtual and Augmented Reality Health Technology Ecosystem	12

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	The VR Book, Human Centered Design for Virtual Reality	Jason Jerald	ACM Books	1st	2016
2.	Creating Augmented and Virtual Realities	Erin Pangilinan, Steve Lukas, Vasanth Mohan	O'Reilly	1st	2019
3.	Virtual reality with VRTK4	Rakesh Baruah	APress	1st	2020

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Introduction	No Change	NIL
Unit 2 Perception	No Change	NIL
Unit 3 Content Creation, Interaction	No Change	NIL
Unit 4 Design and Art Across Digital Realities, Virtual Reality and Augmented Reality: Cross-Platform Theory	No Change	NIL
Unit 5 Virtual Reality Toolkit	No Change	NIL

Virtual Reality and Augmented Reality Practical

COURSE CODE: MITS3P4b **COURSE CREDIT: 02**

Course Objectives:

- To apply the concepts of VR and AR in real life.
- To reduce the greatest risk to VR.
- To design the way users interact within the scenes they find themselves in.
- To be exposed to VR, AR and today's resources.
- To effectively use open source VR software.

List of Practical:

10 practicals covering the entire syllabus must be performed. The detailed list ofpractical will be circulated later in the official workshop.

Data Centre Technologies

COURSE CODE: MITS304c **COURSE CREDIT: 04**

Course Objectives:

- Identify important requirements to design and support a data center.
- Determine a data center environment's requirement including systems and network architecture as well as services.
- Evaluate options for server farms, network designs, high availability, load balancing, data center services, and trends that might affect data center designs.
- Assess threats, vulnerabilities and common attacks, and network security devices available to protect data centers.
- Design a data center infrastructure integrating features that address security, performance, and availability.
- Measure data center traffic patterns and performance metrics.

Sr. No	Modules/Units	No of Lectures
1.	Virtualization History and Definitions Data Center Essential Definitions Data Center Evolution Operational Areas and Data Center Architecture The Origins of Data Center Virtualization Virtual Memory Mainframe Virtualization Hot Standby Router Protocol Defining Virtualization Data Center Virtualization Timeline Classifying Virtualization Technologies A Virtualization Taxonomy Virtualization Scalability Technology Areas Classification Examples Summary Data Center Network Evolution Ethernet Protocol: Then and NowEthernet media Coaxial Cable Twisted-Pair optical Fiber Direct-Attach Twin axial cables Ethernet Data Rate Timeline Data Center Network Topologies Data Center Network Layers Design Factors for Data Center Networks Physical Network Layout Considerations The ANSI/TIA-942 Standard Network Virtualization Benefits Network Logical Partitioning Network Simplification and Traffic Load Balancing Management Consolidation and Cabling Optimization Network Extension The Humble Beginnings of Network Virtualization Network Partitioning Concepts from the Bridging World Defining VLANs VLAN Trunks Two Common Misconceptions About VLANs Misconception Number 1: A VLAN Must Be Associated to an IP Subnet Misconception Number 2: Layer 3 VLANs Spanning Tree Protocol and VLANs Spanning Tree Protocol at Work Port States Spanning Tree Protocol Enhancements Spanning Tree Instances Private VLANs VLAN Specifics Native VLAN Reserved VLANs IDs Resource SharingControl and Management Plane Concepts from the Routing World Overlapping Addresses in a Data Center Defining and Configuring VRFs VRFs and Routing Protocols VRFs and the Management Plane VRF-Awareness VRF Resource Allocation Control	12

2.	An Army of One: ACE Virtual Contexts Application Networking Services The Use of Load Balancers Load-Balancing Concepts Layer 4 Switching Versus Layer 7 Switching Connection Management Address Translation and Load Balancing Server NAT Dual NAT Port Redirection Transparent Mode Other Load-Balancing Applications Firewall Load Balancing Reverse Proxy Load Balancing Offloading Servers SSL Offload TCP Offload HTTP Compression Load Balancer Proliferation in the Data Center Load Balancer Performance Security Policies Suboptimal Traffic Application Environment Independency ACE Virtual Contexts Application Control Engine Physical Connections Connecting an ACE Appliance Connecting an ACE Module Creating and Allocating Resources to VirtualContexts Integrating ACE Virtual Contexts to the Data Center Network Routed Design Bridged Design One-Armed Design Managing and Configuring ACE Virtual Contexts Allowing Management Traffic to a Virtual Context Allowing Load Balancing Traffic Through a Virtual Context Controlling Management Access to Virtual Contexts ACE Virtual Context Additional Characteristics Sharing VLANs Among Contexts Virtual Context Fault Tolerance Instant Switches: Virtual Device Contexts Extending Device Virtualization Why Use VDCs? VDCs in Detail Creating and Configuring VDCs VDC Names and CLI Prompts Virtualization Nesting Allocating Resources to VDCs Using Resource Templates Managing VDCs VDC Operations Processes Failures and VDCs VDC Out-of-Band Management Role-Based Access Control and VDCs Global Resources Fooling Spanning Tree Spanning Tree Protocol and Link Utilization Link Aggregation Server Connectivity and NIC Teaming Cross-Switch PortChannels Virtual PortChannels Virtual PortChannel Definitions Configuring Virtual PortChannels Step 1: Defining the Domain Step 2: Establishing Peer Keepalive Connectivity Step 3: Creating the Peer Link Step 4: Creating the Virtual PortChannel Spanning Tree Protocol and Virtual Port Channels Peer Link Failure and Orphan Ports First-Hop Routing Protocols and Virtual Port Channels Layer 2 Multipathing and vPC+ FabricPath Data Plane FabricPath Control Plane FabricPath and Spanning Tree Protocol Virtual PortChannel Plus Virtualized Chassis with Fabric Extenders Server Access Models Understanding Fabric ExtendersFabric Extender Options Connecting a Fabric Extender to a Parent Switch Fabric Extended Interfaces and Spanning Tree Protocol Fabric Interfaces Redundancy Fabric Extender Topologies Straight-Through Topologies Dual-Homed Topologies	12
3.	Virtualized Chassis with Fabric Extenders Server Access Models Understanding Fabric Extenders Fabric Extender Options Connecting a Fabric Extender to a Parent Switch Fabric Extended Interfaces and Spanning Tree Protocol	

	Fabric Interfaces Redundancy Fabric Extender Topologies Straight-Through Topologies Dual-Homed TopologiesUse Case: Mixed Access Data Center A Tale of Two Data Centers A Brief History of Distributed Data Centers The Cold Age (Mid-1970s to 1980s) The Hot Age (1990s to Mid-2000s) The Active-Active Age (Mid-2000s to Today) The Case for Layer 2 Extensions Challenges of Layer 2 Extensions Ethernet Extensions over Optical Connections Virtual PortChannels FabricPath Ethernet Extensions over MPLS MPLS Basic Concepts Ethernet over MPLS Virtual Private LAN Service Ethernet Extensions over IP MPLS over GRE Overlay Transport Virtualization OTV Terminology OTV Basic Configuration OTV Loop Avoidance and Multihoming Migration to OTV OTV Site Designs VLAN Identifiers and Layer 2 Extensions Internal Routing in Connected Data Centers Use Case: Active-Active Greenfield Data Centers Summary Storage Evolution Data Center Storage Devices Hard Disk Drives Disk Arrays Tape Drives and Libraries Accessing Data in Rest Block- Based Access *Small Computer Systems Interface Mainframe Storage Access* Advanced Technology Attachment File Access Network File System Common Internet File System Record Access Storage Virtualization Virtualizing Storage Devices Virtualizing LUNs Virtualizing File Systems VirtualizingSANs	12
4.	Server Evolution Server Architectures Mainframes RISC Servers x86Servers x86 Hardware Evolution CPU Evolution Memory Evolution Expansion BusEvolution Physical Format Evolution Introducing x86 Server Virtualization Virtualization unleashed Unified Computing Changing Personalities Server Provisioning Challenges Server Domain Operations Infrastructure Domain Operations Unified Computing and Service Profiles Building Service Profiles Identifying a Service Profile Storage Definitions Network Definitions Virtual Interface Placement Server Boot Order Maintenance Policy Server Assignment Operational Policies Configuration External IPMI Management Configuration Management IP Address *Additional Policies* Associating a Service Profile to a Server Installing an Operating System Verifying Stateless Computing Using Policies BIOS Setting Policies Firmware Policies Industrializing Server Provisioning Cloning Pools Service Profile Templates Server Pools Use Case: Seasonal Workloads	12
5.	Moving Targets Virtual Network Services Definitions Virtual Network Services Data Path vPath-Enabled Virtual Network Services Cisco Virtual Security Gateway: Compute Virtual Firewall Installing Virtual Security Gateway Creating Security Policies, Sending Data Traffic to VSG Virtual Machine Attributes and Virtual Zones Application Acceleration, WAN Acceleration and OnlineMigration Routing in the Virtual World Site Selection and Server Virtualization Route Health Injection Global Server Load Balancing Location/ID Separation Protocol Use Case: Virtual Data Center The Virtual Data Center and Cloud Computing	12

	The Virtual Data Center Automation and StandardizationWhat Is Cloud Computing? Cloud Implementation Example Journey to the Cloud Networking in the Clouds Software-Defined Networks Open Stack Network Overlays	

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Data Center Virtualization Fundamentals	Gustavo Alessandro Andrade Santana	Cisco Press	1st	2014

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Virtualization History and Definitions, Ethernet Protocol	No Change	NIL
Unit 2 An Army of One: ACE Virtual Contexts	No Change	NIL
Unit 3 Virtualized Chassis with Fabric Extenders	No Change	NIL
Unit 4 Server Evolution	No Change	NIL
Unit 5 Moving Targets	No Change	NIL

Data Centre Technologies Practical

COURSE CODE: MITS3P4c **COURSE CREDIT: 02**

Course Objectives:

- To understand basic concepts in Virtualization.
- To understand concepts of Load Balancing and Aggregation /virtual switching.
- To understand Data center Migration and Fabric Building.
- To understand various Changes in Server Architecture.
- To understand the concepts of Cloud computing and how to move towards a cloudcomputing technology.

List of Practical:	
1.	**Configuring ESXi Hosts**
	a. Install ESXi on a VM using your student desktop
	b. Install ESXi
2.	**Configuring ESXi Hosts**
	a. Examine the Options in the DCUI
	b. Configure the Management Network
	c. Enable SSH
3.	**Deploying and Configuring a Virtual Machine**
	a. Create a Virtual Machine
	b. Install a Guest Operating System and Disable Windows Updates
	c. Install VMware Tools/Install Files
4.	**Working with vCenter Server**
5.	**Navigating the vSphere Clients**
6.	**Creating Folders in vCenter Server Appliance**
7.	**Using Standard Switches**
8.	**Accessing iSCSI Storage**
a.	Managing VMFS Datastores
b.	Accessing NFS Storage
9.	**Using Templates and Clones**
10.	**Modifying Virtual Machines**
11.	a. Migrating Virtual Machines
	b. Managing Virtual Machines

Offensive Security

COURSE CODE: MITS304d **COURSE CREDIT: 04**

Course Objectives:

- Understanding of security requirements within an organization
- How to inspect, protect assets from technical and managerial perspectives
- To learn various offensive strategies to penetrate the organizations security.
- To learn various tools that aid in offensive security testing.

Sr. No	Modules/Units	No of Lectures
1.	Fault Tolerance and Resilience in Cloud Computing Environments, Securing Web Applications, Services,and Servers, Wireless Network Security, Wireless Sensor Network Security: The Internet of Things, Security for the Internet of Things, Cellular Network Security	12
2.	Social Engineering Deceptions and Defenses, What Is Vulnerability Assessment, Risk Management, Insider Threat, Disaster Recovery, Security Policies and PlansDevelopment	12
3.	Introduction to Metasploit and Supporting Tools The importance of penetration testing Vulnerability assessment versus penetration testing The need for a penetration testing framework Introduction to Metasploit When to use Metasploit? Making Metasploit effective and powerful using supplementary tools Nessus NMAP w3af Armitage Setting up Your Environment Using the Kali Linux virtual machine - the easiest way Installing Metasploit on Windows Installing Metasploit on Linux Setting up exploitable targets in a virtual environment Metasploit Components and Environment Configuration Anatomy and structure of Metasploit Metasploit components Auxiliaries Exploits Encoders Payloads Post, Playing around with msfconsole Variables in Metasploit Updating the Metasploit Framework 55	12
4.	Information Gathering with Metasploit Information gathering and enumeration Transmission Control Protocol User Datagram Protocol File Transfer Protocol Server Message Block Hypertext Transfer ProtocolSimple Mail Transfer Protocol Secure Shell Domain Name System Remote Desktop Protocol Password sniffing Advanced search with shodan Vulnerability Hunting with Metasploit Managing the database Work spaces Importing scans Backing up the database **NMAP** NMAP scanning approach **Nessus** Scanning using Nessus from msfconsole Vulnerability detection with Metasploit auxiliaries Auto exploitation with db_autopwn **Post exploitation** What is meterpreter? Searching for content Screen capture Keystroke logging Dumping the hashes and cracking with JTR Shell command Privilege escalation Client-side Attacks with Metasploit Need of client-side attacks What are	12

	client-side attacks? What is a Shellcode? What is a reverse shell? What is a bind shell? What is an encoder? **The msfvenom utility** Generating a payload with msfvenom Social Engineering with Metasploit Generating malicious PDF Creating infectious media drives	
5.	Approaching a Penetration Test Using Metasploit Organizing a penetration test Preinteractions Intelligence gathering/ reconnaissance phase Predicting the test grounds Modeling threats Vulnerability analysis Exploitation and post-exploitation Reporting Mounting the environment Setting up Kali Linux in virtual environment The fundamentals of Metasploit Conducting a penetration test with Metasploit Recalling the basics of Metasploit Benefits of penetration testing using Metasploit Open source Support for testing large networks and easy naming conventions Smart payload generation and switching mechanism Cleaner exits The GUI environment Penetration testing an unknown network Assumptions Gathering intelligence Using databases in Metasploit Modeling threats Vulnerability analysis of VSFTPD backdoor The attack procedure The procedure of exploiting the vulnerability Exploitation and post exploitation Vulnerability analysis of PHP-CGI query string parameter vulnerability Exploitation and post exploitation Vulnerability analysis of HFS Exploitation and post exploitation Maintaining access Clearing tracks Revising the approach Reinventing Metasploit Ruby – the heart of Metasploit Creating your first Ruby program Interacting with the Ruby shell Defining methods in the shell Variables and data types in Ruby Working with strings Concatenating strings The substring function The split function Numbers and conversions in Ruby Conversions in Ruby Ranges in Ruby Arrays in Ruby Methods in Ruby Decision-making operators Loops in Ruby Regular expressions Wrapping up with Ruby basics **Developing custom modules** Building a module in a nutshell The architecture of the Metasploit framework Understanding the file structure The libraries layout Understanding the existing modules The format of a Metasploit module Disassembling existing HTTP server scanner moduleLibraries and the function Writing out a custom FTP scanner module Libraries and the function Using msftidy Writing out a custom SSH authentication brute forcerRephrasing the equation Writing a drive disabler post exploitation module Writing a credential harvester post exploitation module **Breakthrough meterpreter scripting** Essentials of meterpreter scripting Pivoting the target network Setting up persistent access API calls and mixins Fabricating custom meterpreter scripts Working with RailGun Interactive Ruby shell basics Understanding RailGun and its scripting Manipulating Windows API calls Fabricating sophisticated RailGun scripts The Exploit Formulation Process The absolute basics of exploitation The basics The architecture System organization basicsRegisters Exploiting stack-based buffer overflows with Metasploit Crashing the vulnerable application Building the exploit base Calculating the offset Using the	12

	pattern_create tool Using the pattern_offset tool Finding the JMP ESP address Using Immunity Debugger to find executable modules Using msfbinscan Stuffing the space Relevance of NOPs Determining bad characters Determining space limitations Writing the Metasploit exploit module Exploiting SEH-based buffer overflows with Metasploit Building the exploit base Calculating the offset Using pattern_create tool Using pattern_offset tool *Table of Contents* Finding the POP/POP/RET addressThe Mona script Using msfbinscan Writing the Metasploit SEH exploit module Using NASM shell for writing assembly instructions **Bypassing DEP in Metasploit modules** Using msfrop to find ROP gadgets Using Mona to create ROP chains Writing the Metasploit exploit module for DEP bypass	

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Computer and Information Security Handbook	John R. Vacca	Morgan Kaufmann Publisher	3rd	2017
2.	Metasploit Revealed: Secrets of the Expert Pentester	Sagar Rahalkar	Packt Publishing		2017

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Fault Tolerance and Resilience in Cloud ComputingEnvironments, Sensor Network Security	No Change	NIL
Unit 2 Social Engineering Deceptions and Defenses	No Change	NIL
Unit 3 Introduction to Metasploit and Supporting Tools	No Change	NIL
Unit 4 Information Gathering with Metasploit, The msfvenom utility	No Change	NIL
Unit 5 Approaching a Penetration Test Using Metasploit, Developing custom modules, Breakthrough meterpreter scripting, Bypassing DEP in Metasploit modules	No Change	NIL

Offensive Security Practical

COURSE CODE: MITS3P4d **COURSE CREDIT: 02**

Course Objectives:

- To understand basic security issues in cloud, IoT etc.
- To understand different security techniques and policies.
- To use Vulnerability assessment and exploitation tool.
- To analyze the network perform reconnaissance and enumerate the target to detect vulnerabilities.
- To perform offensive tests using Metasploit on various application, generating payloadsetc.

List of Practical: to be performed with Kali Linux and Meta-Sploit Framework)	
0.	Installation and preparing the lab ready Virtual or physical machine with Kali Linux. Exploring and getting acquainted with he other operating distributions used for offensive security testing mainly • Lion Sec • BackBox • Parrot • BlackArch
2.	Exploring the command line arguments
a.	Environment Variables , Tab Completion , Bash History Tricks
b.	Piping and Redirection, Text Searching and Manipulation
c.	Editing Files from the Command Line, Comparing Files, Managing Processes
3.	
a.	Using NETCAT Socat
b.	PowerShell and Powercat
c.	Wireshark and Tcpdump
4.	Passive Information Gathering
a.	Whois Enumeration/ Google Hacking
b.	Netcraft, Recon-ng, Shodan
c.	SSL Server Test
5.	User Information Gathering
a.	Email Harvesting, Password Dumps
b.	Information Gathering Frameworks- OSINT Framework, Maltego
6.	Active Information Gathering
a.	DNS Enumeration
b.	Port Scanning
	SMB Enumeration
	NFS Enumeration
7.	Vulnerability Scanning
a.	Vulnerability Scanning with Nessus
b.	Vulnerability Scanning with Nmap

8.	Web Application Assessment Tools
a.	DIRB
b.	Burp Suite
c.	Nikto
d.	SQL Injection
9.	Client-Side Attacks
c.	HTA Attack
d.	Exploiting Microsoft Office
10.	Privilege Escalation
a.	Windows Privilege Escalation
b.	Linux Privilege Escalation
11.	Password Attacks
a.	Wordlists, Brute Force Wordlists
b.	Common Network Service Attack Methods
12.	Port Redirection and Tunneling
a.	Port Forwarding- RINETD
b.	SSH Tunneling
c.	PLINK., NETSH , HTTPTunnel-ing Through Deep Packet Inspection

SEMESTER IV

Blockchain
COURSE CODE: MITS401 **COURSE CREDIT: 04**

Course Objectives:

- To provide conceptual understanding of the function of Blockchain as a method of securing distributed ledgers, how consensus on their contents is achieved, and the new applications that they enable.
- To cover the technological underpinnings of blockchain operations as distributed data structures and decision-making systems, their functionality and different architecture types.
- To provide a critical evaluation of existing smart contract capabilities and platforms, and examine their future directions, opportunities, risks and challenges.

Sr. No	Modules/Units	No of Lectures
1.	**Blockchain:** Introduction, History, Centralised versus Decentralised systems, Layers of blockchain, Importance of blockchain, Blockchain uses and use cases. **Working of Blockchain:** Blockchain foundation, Cryptography, Game Theory, Computer Science Engineering, Properties of blockchain solutions, blockchain transactions, distributed consensus mechanisms, Blockchain mechanisms, Scaling blockchain **Working of Bitcoin:** Money, Bitcoin, Bitcoin blockchain, bitcoin network, bitcoin scripts, Full Nodesand SVPs, Bitcoin wallets.	12
2.	**Ethereum:** three parts of blockchain, Ether as currency and commodity, Building trustless systems, Smart contracts, Ethereum Virtual Machine, The Mist browser, Wallets as a Computing Metaphor, The Bank Teller Metaphor, Breaking with Banking History, How Encryption Leads to Trust, System Requirements, Using Parity with Geth, Anonymity in Cryptocurrency, Central Bank Network, Virtual Machines, EVM Applications, State Machines, Guts of the EVM, Blocks, Mining's Place in the State Transition Function, Renting Time on the EVM, Gas, Working with Gas, Accounts, Transactions, and Messages, Transactions and Messages, Estimating Gas Fees for Operations, Opcodes in the EVM. **Solidity Programming:** Introduction, Global Banking Made Real, Complementary Currency, Programming the EVM, Design Rationale, Importance of Formal Proofs, Automated Proofs, Testing, Formatting Solidity Files, Reading Code, Statements and Expressions in Solidity,	12

	Value Types, Global Special Variables, Units, and Functions,	
3.	**Hyperledger:** Overview, Fabric, composer, installing hyperledger fabric and composer, deploying, running the network, error troubleshooting. **Smart Contracts and Tokens:** EVM as Back End, Assets Backed by Anything, Cryptocurrency Is a Measure of Time, Function of Collectibles in Human Systems, Platforms for High-Value Digital Collectibles, Tokens as Category of Smart Contract, Creating a Token, Deploying the Contract, Playing with Contracts	12
4.	**Mining Ether:** Why? Ether's Source, Defining Mining, Difficulty, Self-Regulation, and the Race for Profit, How Proof of Work Helps Regulate Block Time, DAG and Nonce, Faster Blocks, Stale Blocks, Difficulties, Ancestry of Blocks and Transactions, Ethereum and Bitcoin, Forking, Mining, Geth on Windows, Executing Commands in the EVM via the Geth Console, Launching Geth with Flags, Mining on the Testnet, GPU Mining Rigs, Mining on a Pool with Multiple GPUs. **Cryptoecnomics:** Introduction, Usefulness of cryptoeconomics, Speed of blocks, Ether Issuance scheme, Common Attack Scenarios.	12
5.	**Blockchain Application Development:** Decentralized Applications, Blockchain Application Development, Interacting with the Bitcoin Blockchain, Interacting Programmatically with Ethereum—Sending Transactions, Creating a Smart Contract, Executing Smart Contract Functions, Public vs. Private Blockchains, Decentralized Application Architecture, **Building an Ethereum DApp:** The DApp, Setting Up a Private Ethereum Network, Creating the Smart Contract, Deploying the Smart Contract, Client Application, **DApp deployment:** Seven Ways to Think About Smart Contracts, Dapp Contract Data Models, EVM back-end and front-end communication, JSONRPC, Web 3, JavaScript API, Using Meteor with the EVM, Executing Contracts in the Console,Recommendations for Prototyping, Third-Party Deployment Libraries, **Creating Private Chains.**	12

REFERENCE BOOKS:

Books and References:					
Sr. No.	**Title**	**Author/s**	**Publisher**	**Edition**	**Year**
1.	Beginning Blockchain A Beginner's Guide to Building Blockchain Solutions	Bikramaditya Singhal, Gautam Dhameja, Priyansu Sekhar Panda	Apress		2018
2.	Introducing Ethereum and Solidity	Chris Dannen	Apress		2017
3.	The Blockchain Developer	Elad Elrom	Apress		2019
4.	Mastering Ethereum	Andreas M. Antonopoulos Dr. Gavin Wood	O'Reilly	First	2018
5.	Blockchain Enabled Applications	Vikram Dhillon David Metcalf Max Hooper	Apress		2017

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Blockchain Working of Blockchain Working of Bitcoin	No Change	NIL
Unit 2 Ethereum Solidity Programming	No Change	NIL
Unit 3 Hyperledger Smart Contracts and Tokens	No Change	NIL
Unit 4 Mining Ether: Cryptoecnomics	No Change	NIL
Unit 5 Blockchain Application Development Building an Ethereum DApp DApp deployment Creating Private Chains	No Change	NIL

Blockchain Practical

COURSE CODE: MITS4P1 **COURSE CREDIT: 02**

List of Practical:

10 practicals covering the entire syllabus must be performed. The detailed list of practical will be circulated later in the official workshop.

Elective 1

Natural Language Processing
COURSE CODE: MITS402a **COURSE CREDIT: 04**

Course Objectives:

- The prime objective of this course is to introduce the students to the field of Language Computing and its applications ranging from classical era to modern context.
- To provide understanding of various NLP tasks and NLP abstractions such as Morphological analysis, POS tagging, concept of syntactic parsing, semantic analysis etc.
- To provide knowledge of different approaches/algorithms for carrying out NLP tasks.
- To highlight the concepts of Language grammar and grammar representation in Computational Linguistics.

Sr. No	Modules/Units	No of Lectures
1.	Introduction to NLP, Brief history, Working of NLP NLP applications: Speech to Text(STT), Text to Speech(TTS), Text Summarization, Text classification, Sentiment Analysis, Grammar/Spell Checkers, NL tasks: Segmentation, Chunking, tagging, NER, Parsing, Word Sense Disambiguation, NL Generation, Sentiment Analysis, Text Entailment, Cross Lingual Information Retrieval (CLIR)	12
2.	Text Processing Challenges, Segmentation: word level(Tokenization), Sentence level. Regular Expression and Automata Morphology, Types, Survey of English and Indian Languages Morphology, Morphological parsing FSA and FST, Porter stemmer, Rule based and Paradigm based Morphology, Human Morphological Processing, Machine Learning approaches	12
3.	Word Classes ad Part-of-Speech tagging(POS), survey of POS tagsets, Rule based approaches (ENGTOWL), Stochastic approaches(Probabilistic, N-gram and HMM), Evaluation metrics: Precision/Recall/F-measure, error analysis.	12
4.	NL parsing basics, approaches: TopDown, BottomUp, Overview of Grammar Formalisms: constituency and dependency school, Grammar notations CFG, LFG, PCFG, LTAG, Feature-Unification, overview of English CFG, Indian Language Parsing in Paninian Karaka Theory, Probabilistic parsing, Dependency	12

	Parsing: Covington algorithm, MALT parser, MST parser.	
5.	Concepts and issues in NL, Theories and approaches for Semantic Analysis, Meaning Representation, word similarity, Lexical Semantics, word senses and relationships, WordNet (English and IndoWordnet), Word Sense Disambiguation: Lesk Algorithm Walker's algorithm, Coreferences Resolution: Anaphora, Cataphora	12

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Handbook of Natural Language Processing	Indurkhya, N., & Damerau, F. J.	CRC Press Taylor and Francis Group	2nd	2010
2.	Speech and Language Processing	Martin, J. H., & Jurafsky, D.	Pearson Education India	2nd	2013
3.	Foundations of Statistical Natural Language Processing	Manning, Christopher and Heinrich, Schutze	MIT Press	1st	1997
4.	Natural Language Processing With Python	Steven Bird, Edward Loper	O'Reilly Media	2nd	2016
5.	Video Links				

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Introduction to NLP NL tasks Web 2.0 Applications	Topic added : Working of NLP Topics removed : Story Understanding, NL Generation, QA system, Machine Translation challenges/Open Problems, NLP abstraction levels, Natural Language (NL) Characteristics and NL computing approaches/techniques and steps	Working of NLP consists of architecture that helps us to understand the working of NLP from NLU to NLG These topics are repeated in the syllabus.
Unit 2 Text Processing Challenges Segmentation	Topics removed : Overview of Language Scripts and their representation on Machines using Character Sets, Language, Corpus and Application Dependence issues	These topics are repeated in the syllabus.
Unit 3 Word Classes ad Part-of-Speech tagging evaluation metrics	Topics removed : TBL morphology, unknown word handling	These topics are repeated in the syllabus.
Unit 4 NL parsing basics, approaches Overview of Grammar Formalisms	Topics removed : CFG parsing using Earley's and CYK algorithms	These topics are repeated in the syllabus.
Unit 5 Concepts and issues in NL Theories and approaches for Semantic Analysis Word Sense Disambiguation Resolution	No Change	NIL

Natural Language Processing Practical

COURSE CODE: MITS4P2a **COURSE CREDIT: 02**

List of Practical:

10 practicals covering the entire syllabus must be performed. The detailed list of practical will be circulated later in the official workshop.

Digital Image Forensics
COURSE CODE: MITS402b **COURSE CREDIT: 04**

Course Objectives:

- To understand describe the origin of computer forensics and the relationship between law enforcement and industry.
- Describe electronic evidence and the computing investigation process.
- Extracting Digital Evidence from Images and establishing them in court of Law.
- Enhancing images for investigation and various techniques to enhance images.
- Interpret and present Evidences in Court of Law.

Sr. No	Modules/Units	No of Lectures
1.	History of Forensic Digital Enhancement, Establishing Integrity of Digital Images for Court,	12
2.	Digital Still and Video Cameras, Color Modes and Channel Blending to Extract Detail	12
3.	Multiple Image Techniques, Fast Fourier Transform (FFT) – Background Pattern Removal	12
4.	Contrast Adjustment Techniques, Advanced Processing Techniques, Comparison and Measurement	12
5.	The Approach – Developing Enhancement Strategies for Images Intended for Analysis, Digital Imaging in the Courts, Interpreting and Presenting Evidence.	12

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Forensic Digital Image Processing: Optimization of Impression Evidence	Brian Dalrymple, Jill Smith	CRC Press		2018
2.	Forensic Uses of Digital Imaging	John C. Russ, Jens Rindel, P. Lord	Taylor & Francis Group	2nd	2016

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 History of Forensic Digital Enhancement, Establishing Integrity of Digital Images for Court,	No Change	NIL
Unit 2 Digital Still and Video Cameras, Color Modes and Channel Blending to Extract Detail	No Change	NIL
Unit 3 Multiple Image Techniques, Fast Fourier Transform (FFT) – Background Pattern Removal	No Change	NIL
Unit 4 Contrast Adjustment Techniques, Advanced Processing Techniques, Comparison and Measurement	No Change	NIL
Unit 5 The Approach – Developing Enhancement Strategies for Images Intended for Analysis, Digital Imaging in the Courts, Interpreting and Presenting Evidence	No Change	NIL

Digital Image Forensics Practical

COURSE CODE: MITS4P2b **COURSE CREDIT: 02**

List of Practical:

10 practicals covering the entire syllabus must be performed. The detailed list of practical will be circulated later in the official workshop.

Advanced IoT

COURSE CODE: MITS402c **COURSE CREDIT: 04**

Course Objectives:

- To understand the latest developments in IoT
- To build smart IoT applications
- To leverage the applications of IoT in different technologies
- To build own IoT platform

Sr. No	Modules/Units	No of Lectures
1.	The Artificial Intelligence 2.0, IoT and Azure IoT Suite, Creating Smart IoT Application	12
2.	Cognitive APIs, Consuming Microsoft Cognitive APIs, Building Smarter Application using Cognitive APIs.	12
3.	Implementing Blockchain as a service, Capturing, Analysing and Visualizing real-time data, Making prediction with machine learning.	12
4.	IoT and Microservices, Service Fabric, Build your own IoT platform: Introduction, Building blocks for IoT solution, Essentials for building your own platform, Platform requirements, building the platform by initializing cloud instance, installing basic software stacks, securing instance and software, installing node.js and Node-RED, Message broker.	12
5.	Building Critical components, configuring message broker, creating REST interface, Rule engine and authentication, documentation and testing, Introspection on what we build and deliverables.	12

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	IoT, AI, and Blockchain for .NET- Building a Next-Generation Application from the Ground Up	Nishith Pathak Anurag Bhandari	Apress	--	2018
2.	Microservices, IoT and Azure	Bob Familiar	Apress	--	2015
3.	Build your own IoT Platform	Anand Tamboli	Apress	--	2019
4.	Internet of Things Architectures, Protocols and Standards	Simone Cirani Gianluigi Ferrari Marco Picone Luca Veltri	Wiley	1	2019

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 The Artificial Intelligence 2.0, IoT and Azure IoT Suite, Creating Smart IoT Application	No Change	NIL
Unit 2 Cognitive APIs	No Change	NIL
Unit 3 Implementing Blockchain as a service, Capturing, Analysing and Visualizing real-time data, Making prediction with machine learning	No Change	NIL
Unit 4 IoT and Microservices, Service Fabric, Build your own IoT platform	No Change	NIL
Unit 5 Building Critical components, configuring message broker, creating REST interface, Rule engine and authentication, documentation and testing, Introspection on what we build and deliverables.	No Change	NIL

Advanced IoT Practical

COURSE CODE: MITS4P2c **COURSE CREDIT: 02**

List of Practical:

10 practicals covering the entire syllabus must be performed. The detailed list of practical will be circulated later in the official workshop.

Cyber Forensics

COURSE CODE: MITS402d **COURSE CREDIT: 04**

Course Objectives:

- Explain laws relevant to computer forensics
- Seize digital evidence from pc systems
- Recover data to be used as evidence
- Analyse data and reconstruct events
- Explain how data may be concealed or hidden

Sr. No	Modules/Units	No of Lectures
1.	Computer Forensics: The present Scenario, The Investigation Process, Computers – Searching and Seizing, Electronic Evidence, Procedures to be followed by the first responder.	**12**
2.	Setting up a lab for Computer Forensics, Hard Disksand File Systems, Forensics on Windows Machine, Acquire and Duplicate Data	**12**
3.	Recovery of deleted files and partitions, Using Access Data FTK and Encase for forensics Investigation, Forensic analysis of Steganography and Image files, Cracking Application passwords.	**12**
4.	Capturing logs and correlating to the events, NetworkForensics – Investigating logs and Network traffic, Investigating Wireless and Web Attacks.	**12**
5.	Email Tracking and Email Crime investigation. Mobile Forensics, Reports of Investigation, Become an expert witness.	**12**

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	EC-Council CHFIv10 Study Guide	--	EC-Council	--	2018
2.	The official CHFI Exam 312-49 study Guide	Dave Kleiman	SYNGRESS	--	2007
3.	Digital Forensics and Incident Response	Gerard Johansen	Packt Publishing	--	2020
4.	Practical Cyber Forensics	Niranjan Reddy	Apress	--	2019

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Computer Forensics	No Change	NIL
Unit 2 Setting up a lab for Computer Forensics	No Change	NIL
Unit 3 Recovery of deleted files and partitions, Forensic analysis of Steganography and Image files, Cracking Application passwords	No Change	NIL
Unit 4 Capturing logs and correlating to the events, Network Forensics	No Change	NIL
Unit 5 Email Tracking and Email Crime investigation. Mobile Forensics, Reports of Investigation, Become an expert witness.	No Change	NIL

Cyber Forensics Practical

COURSE CODE: MITS4P2d **COURSE CREDIT: 02**

List of Practical:

10 practicals covering the entire syllabus must be performed. The detailed list of practical will be circulated later in the official workshop.

Elective 2

Deep Learning

COURSE CODE: MITS403a **COURSE CREDIT: 04**

Course Objectives:

- To present the mathematical, statistical and computational challenges of building neural networks
- To study the concepts of deep learning
- To enable the students to know deep learning techniques to support real-time applications.

Sr. No	Modules/Units	No of Lectures
1.	**Applied Math and Machine Learning Basics:** Linear Algebra: Scalars, Vectors, Matrices and Tensors, Multiplying Matrices and Vectors , Identity and Inverse Matrices, Linear Dependence and Span ,norms, special matrices and vectors, eigen decompositions. **Numerical Computation:** Overflow and under flow, poor conditioning, Gradient Based Optimization, Constraint optimization.	12
2.	**Deep Networks:** Deep feedforward network, regularization for deep learning, Optimization for Training deep models	12
3.	Convolutional Networks, Sequence Modelling, Applications	12
4.	**Deep Learning Research**: Linear Factor Models, Autoencoders, representation learning	12
5.	Approximate Inference, Deep Generative Models	12

REFERENCE BOOKS:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Deep Learning	Ian Goodfellow, Yoshua Bengio, Aaron Courvile	An MIT Press book	1st	2016
2.	Fundamentals of Deep Learning	Nikhil Buduma	O'Reilly	1st	2017
3.	Deep Learning: Methods and Applications	Deng & Yu	Now Publishers	1st	2013
4.	Deep Learning CookBook	Douwe Osinga	O'Reilly	1st	2017

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Applied Math and Machine Learning Basics Numerical Computation	No Change	NIL
Unit 2 Deep Networks	No Change	NIL
Unit 3 Convolutional Networks, Sequence Modelling, Applications	No Change	NIL
Unit 4 Deep Learning Research	No Change	NIL
Unit 5 Approximate Inference, Deep Generative Models	No Change	NIL

Deep Learning Practical

COURSE CODE: MITS4P3a **COURSE CREDIT: 02**

List of Practical:

10 practicals covering the entire syllabus must be performed. The detailed list of practical will be circulated later in the official workshop.

Remote Sensing

COURSE CODE: MITS403b **COURSE CREDIT: 04**

Course Objectives:

- Attain a foundational knowledge and comprehension of the physical, computational, and perceptual basis for remote sensing.
- Gain familiarity with a variety of physical, biological, and human geographic applications of remote sensing.
- Gain basic experience in the hands-on application of remote sensing data through visual interpretation and digital image processing exercises.
- Analyze and synthesize understanding by identifying and developing a research and application proposal using remote sensing.

Sr. No	Modules/Units	No of Lectures
1.	Remote Sensing: Basic Principles Introduction, Electromagnetic Radiation and Its Properties, Terminology, Nature of Electromagnetic Radiation, The Electromagnetic Spectrum, Sources of Electromagnetic Radiation, Interactions with the Earth's Atmosphere, Interaction with Earth-Surface Materials, Spectral Reflectance of Earth Surface Materials Remote Sensing Platforms and Sensors Introduction, Characteristics of Imaging Remote Sensing Instruments, Spatial Resolution, Spectral Resolution, Radiometric Resolution, Optical, Near- infrared and Thermal Imaging Sensors, Along-Track Scanning Radiometer (ATSR), Advanced Very High Resolution Radiometer (AVHRR) and NPOESS VIIRS, MODIS, Ocean Observing Instruments, IRS LISS, Landsat Instruments, SPOT Sensors, Advanced Spaceborne Thermal Emission and Reflection Radiometer (ASTER), High-Resolution Commercial and Small Satellite Systems, Microwave Imaging Sensors, European Space Agency Synthetic Aperture Spaceborne Radars, Radarsat, TerraSAR-X and COSMO/Skymed, ALOS PALSAR	**12**
2.	Hardware and Software Aspects of Digital Image Processing Introduction, Properties of Digital Remote Sensing Data, Digital Data, Data Formats, System Processing, Numerical Analysis and Software Accuracy, Some Remarks on Statistics, Preprocessing of Remotely-Sensed Data Introduction, Cosmetic Operations, Missing Scan Lines, Destriping Methods, Geometric Correction and Registration, Orbital Geometry Model, Transformation Based on Ground Control Points, Resampling Procedures, Image Registration, Other Geometric Correction Methods, Atmospheric Correction, Background, Image-Based Methods, Radiative Transfer Models, Empirical Line Method, Illumination and View Angle Effects, Sensor Calibration, Terrain Effects	12

3.	Image Enhancement Techniques Introduction, Human Visual System, Contrast Enhancement, Linear Contrast Stretch, Histogram Equalization, Gaussian Stretch, Pseudocolour Enhancement, Density Slicing, Pseudocolour Transform, Image Transforms Introduction, Arithmetic Operations, Image Addition, Image Subtraction, Image Multiplication, Image Division and Vegetation Indices, Empirically Based Image Transforms, Perpendicular Vegetation Index, Tasselled Cap (Kauth–Thomas) Transformation, Principal Components Analysis, Standard Principal Components Analysis, Noise-Adjusted PCA, Decorrelation Stretch, Hue-Saturation-Intensity (HSI) Transform, The Discrete Fourier Transform, Two- Dimensional Fourier Transform, Applications of the Fourier Transform, The Discrete Wavelet Transform, The One-Dimensional Discrete Wavelet Transform, The Two-Dimensional Discrete Wavelet Transform, Change Detection, Introduction, NDVI Difference Image, PCA, Canonical Correlation Change Analysis, Image Fusion, HSI Algorithm, PCA, Gram-Schmidt Orthogonalization, Wavelet-Based Methods, Evaluation – Subjective Methods, Evaluation – Objective Methods	12
4.	Filtering Techniques, Spatial Domain Low-Pass (Smoothing) Filters, Moving Average Filter, Median Filter, Adaptive Filters, Spatial Domain High-Pass (Sharpening) Filters, Image Subtraction Method, Derivative-Based Methods, Spatial Domain Edge Detectors, Frequency Domain Filters **Classification :** Geometrical Basis of Classification, Unsupervised Classification, The *k*-Means Algorithm, ISODATA, A Modified *k*-Means Algorithm, Supervised Classification, Training Samples, Statistical Classifiers, Neural Classifiers, Subpixel Classification Techniques, The Linear Mixture Model, Spectral Angle Mapping, ICA, Fuzzy Classifiers, More Advanced Approaches to Image Classification, Support Vector Machines , Decision Trees , Other Methods of Classification, Incorporation of Non-spectral Features, Texture, Use of External Data, Contextual Information, Feature Selection, Classification Accuracy Advanced Topics Introduction, SAR Interferometry, Basic Principles, Interferometric Processing, Problems in SAR Interferometry, Applications of SAR Interferometry, Imaging Spectroscopy, Processing Imaging Spectroscopy Data, Lidar, Lidar Details, Lidar Applications	12
5.	**Environmental Geographical Information Systems**: A Remote Sensing Perspective, Definitions, The Synergy between Remote Sensing and GIS, Data Models, Data Structures and File Formats, Spatial Data Models, Data Structures, File Formats, Raster to Vector and Vector to Raster Conversion, Geodata Processing, Buffering, Overlay, Locational Analysis, Slope and Aspect, Proximity Analysis, Contiguity and Connectivity, Spatial Analysis, Point Patterns and Interpolation. **Relating Field and Remotely-Sensed Measurements**: Statistical Analysis, Exploratory Data Analysis and Data Mining, Environmental Modelling, Visualization, Multicriteria Decision Analysis of Groundwater Recharge Zones, Data Characteristics, Multicriteria Decision Analysis, Evaluation, Assessing Flash Flood Hazards by Classifying Wadi Deposits in Arid Environments, Water Resources in Arid Lands, Case Study from the Sinai Peninsula, Egypt, Optical and Microwave Data Fusion, Classification of Wadi Deposits, Correlation of Classification Results with Geology and Terrain Data, Remote Sensing and GIS in Archaeological Studies, Introduction, Homul (Guatemala)	12

	Case Study, Aksum (Ethiopia) Case Study	

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Computer Processing of Remotely-Sensed Images: An Introduction	Paul M. Mather, Magaly Koch	Wiley-Blackwell	4th	2011
2.	Remote Sensing for Geoscientists Image Analysis and Integration	Gary L. Prost	CRC Press	3rd	2014
3.	Remote Sensing: Models and Methods for Image Processing	Robert A. Schowengerdt	Elsevier	3rd	2007
4.	Introductory Digital Image Processing: A Remote Sensing Perspective	John R. Jensen	Pearson		2015

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Remote Sensing: Basic Principles Remote Sensing Platforms and Sensors	No Change	NIL
Unit 2 Hardware and Software Aspects of Digital Image Processing Preprocessing of Remotely-Sensed Data	No Change	NIL
Unit 3 Image Enhancement Techniques Image Transforms	No Change	NIL
Unit 4 Filtering Techniques Classification Advanced Topics	No Change	NIL
Unit 5 Environmental Geographical Information Systems Relating Field and Remotely-Sensed Measurements	No Change	NIL

Remote Sensing Practical

COURSE CODE: MITS4P3b **COURSE CREDIT: 02**

List of Practical:

10 practicals covering the entire syllabus must be performed. The detailed list of practical will be circulated later in the official workshop.

Server Virtualization on VMWarePlatform

COURSE CODE: MITS403c **COURSE CREDIT: 04**

Course Objectives:

- Identify the need for Server Virtualization
- Describe the components and features of vSphere 6.7 and ESXi
- Describe how VMware's products help solve business and technical challenges withregard to Server Virtualization

Sr. No	Modules/Units	No of Lectures
1.	**Introducing VMware vSphere 6.7:** Exploring VMware vSphere 6.7, Examining the Products in the vSphere Suite, Examining the Features in VMware vSphere, Licensing VMware vSphere, Why Choose vSphere? **Planning and Installing VMware ESXi:** VMware ESXi Architecture, Understanding the ESXi Hypervisor, Examining the ESXi Components, Planning a VMware vSphere Deployment, Choosing a Server Platform, Determining a Storage Architecture, Integrating with the Network Infrastructure, Deploying VMware ESXi, Installing VMware ESXi Interactively, Performing an Unattended Installation of VMware ESXi, Deploying VMware ESXi with vSphere Auto Deploy, Performing Post-installation Configuration, Reconfiguring the Management Network, Using the vSphere Host Client, Configuring Time Synchronization, Configuring Name Resolution, **Installing and Configuring vCenter Server:** Introducing vCenter Server, Centralizing User Authentication Using vCenter Single Sign-On, Understanding the Platform Services Controller, Using the vSphere Web Client for Administration, Providing an Extensible Framework, Choosing the Version of vCenter Server, Planning and Designing a vCenter Server Deployment, Sizing Hardware for vCenter Server, Planning for vCenter Server Availability, Running vCenter Server and Its Components as VMs, Installing vCenter Server and Its Components, Installing vCenter Server in an Enhanced Linked Mode Group, Exploring vCenter Server, The vSphere Web Client Home Screen, Using the Navigator, Creating and Managing a vCenter Server Inventory, Understanding Inventory Views and Objects, Creating and Adding Inventory Objects, Exploring vCenter Server's Management Features, Understanding Basic Host Management, Examining Basic Host Configuration, Using Scheduled Tasks, Using the Events and Events Consoles in vCenter Server, Working with Host Profiles, Tags and Custom Attributes, Managing vCenter Server Settings, General vCenter Server Settings, Licensing, Message of the Day, Advanced Settings, Auto Deploy, vCenter HA, Key Management Servers, Storage Providers, vSphere Web Client Administration, Roles, Licensing, vCenter Solutions Manager, System Configuration,	**12**

	VMware Appliance Management Administration, Summary, Monitor, Access, Networking, Time, Services, Update, Administration, Syslog, Backup.	
2.	vSphere Update Manager and the vCenter Support Tools: vSphere Update Manager, vSphere Update Manager and the vCenter Server Appliance, Installing the Update Manager Download Service, The vSphere Update Manager Plug-in Contents, Reconfiguring the VUM or UMDS, Installation with the Update Manager Utility, Upgrading VUM from a Previous Version, Configuring vSphere Update Manager, Creating Baselines Routine Updates, Attaching and Detaching Baselines or Baseline Groups, Performing a Scan, Staging Patches, Remediating Hosts, Upgrading VMware Tools, Upgrading Host Extensions, Upgrading Hosts with vSphere Update Manager, Importing an ESXi Image and Creating the Host Upgrade Baseline, Upgrading a Host, Upgrading VM Hardware, Performing an Orchestrated Upgrade,Investigating Alternative Update Options, Using vSphere Update Manager PowerCLI, Upgrading and Patching without vSphere Update Manager, vSphere Auto Deploy, Deploying Hosts with Auto Deploy, vCenter Support Tools, ESXi Dump Collector, Other vCenter Support Tools. **Creating and Configuring a vSphere Network:** Putting Together a vSphere Network, Working with vSphere Standard Switches, Comparing Virtual Switches and Physical Switches, Understanding Ports and Port Groups, Understanding Uplinks, Configuring the Management Network, Configuring VMkernel Networking, Enabling Enhanced Multicast Functions, Configuring TCP/IP Stacks, Configuring Virtual Machine Networking, Configuring VLANs, Configuring NIC Teaming, Using and Configuring Traffic Shaping, Bringing It All Together, Working with vSphere Distributed Switches, Creating a vSphere Distributed Switch, Removing an ESXi Host from a Distributed Switch, Removing a Distributed Switch, Managing Distributed Switches, Working with Distributed Port Groups, Managing VMkernel Adapters, Using NetFlow on vSphere Distributed Switches, Enabling Switch Discovery Protocols, Enabling Enhanced Multicast Functions, Setting Up Private VLANs, Configuring LACP, Configuring Virtual Switch Security, Understanding and Using Promiscuous Mode, Allowing MAC Address Changes and Forged Transmits.	**12**

3.	**Creating and Configuring Storage Devices:** Reviewing the Importance of Storage Design, Examining Shared Storage Fundamentals, Comparing Local Storage with Shared Storage, Defining Common Storage Array Architectures, Explaining RAID, Understanding vSAN, Understanding Midrange and External Enterprise Storage Array Design, Choosing a Storage Protocol, Making Basic Storage Choices, Implementing vSphere Storage Fundamentals, Reviewing Core vSphere Storage Concepts, Understanding Virtual Volumes, SCs vs LUNs, Storage Policies, Virtual Volumes, Working with VMFS Datastores, Working with Raw Device Mappings, Working with NFS Datastores, Working with vSAN, Working with Virtual Machine–Level Storage, Configuration, Leveraging SAN and NAS Best Practices **Ensuring High Availability and Business Continuity:** Understanding the Layers of High Availability, Clustering VMs, Introducing Network Load Balancing Clustering, Introducing Windows Server Failover Clustering, Implementing vSphere High Availability, Understanding vSphere High Availability Clusters. Understanding vSphere High Availability's Core Components, Enabling vSphere HA, Configuring vSphere High Availability, Configuring vSphere HA Groups, Rules, Overrides, and Orchestrated VM Restart, Managing vSphere High Availability, Introducing vSphere SMP Fault Tolerance, Using vSphere SMP Fault Tolerance with vSphere High Availability, Examining vSphere Fault Tolerance, Use Cases, Planning for Business Continuity, Providing Data Protection, Recovering from Disasters, Using vSphere Replication. **Securing VMware vSphere:** Overview of vSphere Security, Securing ESXi Hosts, Working with ESXi Authentication, Controlling Access to ESXi Hosts, Keeping ESXi Hosts Patched, Managing ESXi Host Permissions, Configuring ESXi Host Logging, Securing the ESXi Boot Process, Reviewing Other ESXi Security Recommendations, Securing vCenter Server, Managing vSphere Certificates, Working with Certificate Stores, Getting Started with Certificate Management, Authenticating Users with Single Sign-On, Understanding the vpxuser Account, Managing vCenter Server Permissions, Configuring vCenter Server Appliance Logging, Securing Virtual Machines, Configuring a KeyManagement Server for VM and VSAN Encryption, Virtual Trusted Platform Module, Configuring Network Security Policies, Keeping VMs Patched.	

4.	**Creating and Managing Virtual Machines:** Understanding Virtual Machines, Examining Virtual Machines from the Inside, Examining Virtual Machines from the Outside, Creating a Virtual Machine, Choosing Values for Your New Virtual Machine, Sizing Virtual Machines, Naming Virtual Machines, Sizing Virtual Machine Hard Disks, Virtual Machine Graphics, Installing a Guest Operating System, Working with Installation Media, Using the Installation Media, Working in the Virtual Machine Console, Installing VMware Tools, Installing VMware Tools in Windows, Installing VMware Tools in Linux, Managing Virtual Machines, Adding or Registering Existing VMs, Changing VM Power States, Removing VMs, Deleting VMs, Modifying Virtual Machines, Changing Virtual Machine Hardware, Using Virtual Machine Snapshots. **Using Templates and vApps:** Cloning VMs, Creating a Customization Specification, Cloning a Virtual Machine, Introducing vSphere Instant Cloning, Creating Templates and Deploying Virtual Machines, Cloning a Virtual Machine to a Template, Deploying a Virtual Machine from a Template, Using OVF Templates, Deploying a VM from an OVF Template, Exporting a VM as an OVF Template, Examining OVF Templates, Using Content Libraries, Content Library Data and Storage, Content Library Synchronization, Creating and Publishing a Content Library, Subscribing to a Content Library, Operating Content Libraries, Working with vApps, Creating a vApp, Editing a vApp, Changing a vApp's Power State, Cloning a vApp, Importing Machines from Other Environments, **Managing Resource Allocation:** Reviewing Virtual Machine, Resource Allocation, Working with Virtual Machine Memory, Understanding ESXi Advanced Memory Technologies, Controlling Memory Allocation, Managing Virtual Machine CPU Utilization, Default CPU Allocation, Setting CPU Affinity, Using CPU Reservations, Using CPU Limits, Using CPU Shares, Summarizing How Reservations, Limits, and Shares Work with CPUs, Using Resource Pools, Configuring Resource Pools, Understanding Resource Allocation with Resource Pools, Regulating Network I/O Utilization, Controlling Storage I/O Utilization, Enabling Storage I/O Control, Configuring Storage Resource Settings for a Virtual Machine, Using Flash Storage.	**12**

5.	**Balancing Resource Utilization:** Comparing Utilization with Allocation, Exploring vMotion, Examining vMotion Requirements, Performing a vMotion Migration Within a Cluster, Ensuring vMotion Compatibility, Using Per-Virtual-Machine CPU Masking, Using Enhanced vMotion Compatibility, Using Storage vMotion, Combining vMotion with Storage vMotion, Cross-vCenter vMotion, Examining Cross-vCenter vMotion Requirements, Performing a Cross-vCenter Motion, Exploring vSphere Distributed Resource Scheduler, Understanding Manual Automation Behavior, Reviewing Partially Automated Behavior, Examining Fully Automated Behavior, Working with Distributed Resource Scheduler Rules, Working with Storage DRS, Creating and Working with Datastore Clusters , Configuring Storage DRS. **Monitoring VMware vSphere Performance:** Overview of Performance Monitoring, Using Alarms Understanding Alarm Scopes, Creating Alarms, Managing Alarms, Working with Performance Charts, Overview Layout, Advanced Layout, Working with *esxtop*, Monitoring CPU Usage, Monitoring Memory Usage, Monitoring Network Usage, Monitoring Disk Usage. **Automating VMware vSphere:** Why Use Automation? vSphere Automation Automating with PowerCLI, PowerShell and PowerCLI, What's New in PowerCLI, Installing and Configuring PowerCLI on Windows, Installing and Configuring PowerCLI on macOS, Installing and Configuring PowerCLI on Linux, Additional PowerCLI Capabilities Getting Started with PowerCLI, Building PowerCLI Scripts, PowerCLI Advanced Capabilities, Additional Resources.	**12**

REFERENCE BOOKS:

Books and References:					
Sr No	Title	Author/s	Publisher	Edition	Year
1.	Mastering VMware vSphere 67	Nick Marshall, Mike Brown, G Blair Fritz, Ryan Johnson	Sybex, Wiley	--	2019
2.	Mastering VMware vSphere 67	Martin Gavanda, Andrea Mauro, Paolo Valsecchi, Karel Novak	Packt	--	2019

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Introducing VMware vSphere 6.7 Planning and Installing VMware ESXi Installing and Configuring vCenter Server	No Change	NIL
Unit 2 vSphere Update Manager and the vCenter Support Tools Creating and Configuring a vSphere Network	No Change	NIL
Unit 3 Creating and Configuring Storage Devices Ensuring High Availability and BusinessContinuity Securing VMware vSphere	No Change	NIL
Unit 4 Creating and Managing Virtual Machines Using Templates and vApps Managing Resource Allocation	No Change	NIL
Unit 5 Balancing Resource Utilization Monitoring VMware vSphere Performance Automating VMware vSphere	No Change	NIL

Server Virtualization on VMWarePlatform Practical

COURSE CODE: MITS4P3c **COURSE CREDIT: 02**

List of Practical:

10 practicals covering the entire syllabus must be performed. The detailed list of practical will be circulated later in the official workshop.

Security Operations Centre

COURSE CODE: MITS403d **COURSE CREDIT: 04**

Course Objectives:

- The SOC (Security Operations Centre) allows an organization to enforce and test its security policies, processes, procedures and activities through one central platform that monitors and evaluates the effectiveness of the individual elements and the overall security system of the organization.
- This will also allow the learners to configure various use cases and detect various attacks across the network and report them in real time and also take appropriate actions.
- This course will cover the design, deployment and operation of the SOC.
- Once this course is completed, students will have the skills to perform your SOC responsibilities effectively.

Sr. No	Modules/Units	No of Lectures
1.	**Introduction to Security Operations Management** Foundation Topics Introduction to Identity and AccessManagement Phases of the Identity and AccessLifecycle Registration and Identity ValidationPrivileges Provisioning Access Review Access Revocation Password Management Password Creation password Storage and Transmission Password Reset Password SynchronizationDirectory Management Single Sign-On Kerberos Federated SSO Security Assertion MarkupLanguage OAuth OpenID Connect Security Events and Logs Management Logs Collection, Analysis, and Disposal Syslog Security Information and Event Manager Assets Management Assets Inventory Assets Ownership Assets Acceptable Use and Return Policies Assets Classification Assets Labeling Assets and Information Handling Media Management Introduction to Enterprise Mobility Management Mobile Device Management Configuration and Change Management Configuration Management Change Management Vulnerability Management Vulnerability Identification Finding Information about a Vulnerability Vulnerability Scan Penetration Assessment Product Vulnerability Management Vulnerability Analysis and Prioritization Vulnerability Remediation Patch ManagementReferences and Additional Readings **Fundamentals of Cryptography and Public Key Infrastructure** (PKI) Cryptography Ciphers and Keys Ciphers Keys Block and Stream Ciphers Symmetric and Asymmetric Algorithms Symmetric Algorithms Asymmetric Algorithms HashesHashed Message Authentication Code Digital Signatures Digital Signatures in Action Key ManagementNext-Generation Encryption Protocols IPsec and SSL IPsec SSL Fundamentals of PKI Public and Private Key Pairs RSA Algorithm, the Keys, and Digital Certificates Certificate Authorities Root and Identity Certificates Root Certificate Identity Certificate X.500 and X.509v3 Certificates Authenticating and Enrolling with the CA Public	**12**

	Key Cryptography Standards Simple Certificate Enrollment Protocol Revoking Digital Certificates Using Digital Certificates PKI Topologies Single Root CA Hierarchical CA with Subordinate CAs Cross-certifying CAs Exam Preparation Tasks Review All Key Topics Complete Tables and Listsfrom Memory **Introduction to Virtual Private Networks (VPNs)** What Are VPNs? Site-to-site vs. Remote-Access VPNs An Overview of IPsec IKEv1 Phase 1 IKEv1 Phase 2 IKEv2 SSL VPNs SSL VPN Design Considerations User Connectivity VPN Device Feature Set Infrastructure Planning Implementation Scope	
2.	**Windows-Based Analysis** Process and Threads Memory Allocation Windows Registration Windows Management Instrumentation Handles Services Windows Event Logs Exam Preparation Tasks **Linux- and Mac OS X–Based Analysis** Processes Forks Permissions Symlinks Daemons UNIX-Based Syslog Apache Access Logs **Endpoint Security Technologies** Antimalware and Antivirus Software Host-Based Firewalls and Host-Based Intrusion Prevention Application-Level Whitelisting and Blacklisting System-Based Sandboxing	**12**
3.	**Threat Analysis** What Is the CIA Triad: Confidentiality, Integrity, and Availability? Confidentiality Integrity Availability Threat Modeling Defining and Analyzing the Attack Vector Understanding the Attack Complexity Privilegesand User Interaction The Attack Scope Exam Preparation Tasks **Forensics** Introduction to Cybersecurity Forensics The Role of Attribution in a Cybersecurity Investigation The Use of Digital Evidence Defining Digital Forensic Evidence Understanding Best, Corroborating, and Indirect or Circumstantial Evidence Collecting Evidence from Endpoints and Servers Collecting Evidence from Mobile Devices Collecting Evidence from Network Infrastructure Devices Chain of Custody Fundamentals of Microsoft Windows Forensics Processes, Threads, and Services Memory Management Windows Registry The Windows File System Master Boot Record (MBR) The Master File Table (MFT) Data Area and Free Space FAT NTFS MFT Timestamps, MACE, and Alternate Data Streams EFI Fundamentals of Linux Forensics Linux Processes Ext4 Journaling Linux MBR and Swap File System Exam Preparation Tasks **Fundamentals of Intrusion Analysis** Common Artifact Elements and Sources of Security Events False Positives, False Negatives, True Positives,and True Negatives Understanding Regular Expressions Protocols, Protocol Headers, and Intrusion Analysis Using Packet Captures for Intrusion Analysis Mapping Security Event Types to Source	

	Technologies	
4.	**Introduction to Incident Response and the Incident Handling Process** **Introduction to Incident Response** What Are Events and Incidents? The Incident ResponsePlan The Incident Response Process The Preparation Phase The Detection and Analysis Phase Containment, Eradication, and Recovery Post-Incident Activity (Postmortem) Information Sharing and Coordination Incident Response Team Structure The Vocabulary for Event Recording and Incident Sharing (VERIS) **Incident Response Teams** Computer Security Incident Response Teams (CSIRTs)Product Security Incident Response Teams (PSIRTs)Security Vulnerabilities and Their SeverityVulnerability Chaining Role in Fixing Prioritization Fixing Theoretical Vulnerabilities Internally VersusExternally Found Vulnerabilities National CSIRTs andComputer Emergency Response Teams (CERTs)Coordination Centers Incident Response Providers and Managed Security Service Providers (MSSPs) **Compliance Frameworks** Payment Card Industry Data Security Standard (PCIDSS) PCI DSS Data Health Insurance Portability and Accountability Act (HIPAA) HIPAA Security Rule HIPAA Safeguards Administrative Safeguards Physical Safeguards Technical Safeguards Sarbanes-Oxley (SOX) Section302 Section 404 Section 409 SOX Auditing Internal Controls **Network and Host Profiling** Network Profiling Throughput Measuring Throughput Used Ports Session Duration Critical Asset Address Space Host Profiling Listening Ports Logged-in Users/Service AccountsRunning Processes Applications	**12**

5.	**The Art of Data and Event Analysis** Normalizing Data Interpreting Common Data Values into a Universal Format Using the 5-Tuple Correlation to Respond to Security Incidents Retrospective Analysis and Identifying Malicious Files Identifying a Malicious File Mapping Threat Intelligence with DNSand Other Artifacts Deterministic Versus Probabilistic Analysis **Intrusion Event Categories** Diamond Model of Intrusion Cyber Kill Chain Model Reconnaissance Weaponization Delivery Exploitation Installation Command and Control Action and Objectives **Types of Attacks and Vulnerabilities** Types of Attacks Reconnaissance Attacks Social Engineering Privilege Escalation Attacks Backdoors Code Execution Man-in-the Middle Attacks Denial-of-Service Attacks Direct DDoS Botnets Participating in DDoS AttacksReflected DDoS Attacks Attack Methods for Data Exfiltration ARP Cache Poisoning Spoofing Attacks Route Manipulation Attacks Password Attacks Wireless Attacks Types of Vulnerabilities **Security Evasion Techniques** Key Encryption and Tunneling Concepts Resource Exhaustion Traffic Fragmentation Protocol-Level Misinterpretation Traffic Timing,Substitution, and Insertion Pivoting	**12**

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	CCNA Cyber Ops SECOPS 210-255 Official Cert Guide	Omar Santos, Joseph Muniz	CISCO	1st	2017
2.	CCNA Cyber Ops SECFND 210-250 Official Cert Guide	Omar Santos, Joseph Muniz	CISCO	1st	2017
3.	CCNA Cyber security Operations Companion Guide		CISCO	1st	2018

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Introduction to Security Operations Management Fundamentals of Cryptography and Public Key Infrastructure (PKI) Introduction to Virtual Private Networks (VPNs)	No Change	NIL
Unit 2 Windows-Based Analysis Linux- and Mac OS X–Based Analysis Endpoint Security Technologies	No Change	NIL
Unit 3 Threat Analysis Forensics Fundamentals of Intrusion Analysis	No Change	NIL
Unit 4 Introduction to Incident Response and the Incident Handling Process Introduction to Incident Response Incident Response Teams Compliance Frameworks Network and Host Profiling	No Change	NIL
Unit 5 The Art of Data and Event Analysis Intrusion Event Categories Types of Attacks and Vulnerabilities Security Evasion Techniques	No Change	NIL

Security Operations Centre Practical

COURSE CODE: MITS4P3d **COURSE CREDIT: 02**

List of Practical:

10 practicals covering the entire syllabus must be performed. The detailed list of practical will be circulated later in the official workshop.

Elective 3

Human Computer Interaction
COURSE CODE: MITS404a **COURSE CREDIT: 04**
Course Objectives:

- Understand the important aspects of implementation of human-computer interfaces.
- Identify the various tools and techniques for interface analysis, design, and evaluation.
- Identify the impact of usable interfaces in the acceptance and performance utilization of information systems

Sr. No	Modules/Units	No of Lectures
1.	**The Interaction:** Models of interaction, Design Focus, Frameworks and HCI, Ergonomics, Interaction styles, Elements of the WIMP interface, Interactivity **Paradigms:** Introduction, Paradigms for interaction **Interaction design basics:** What is design?, The process of design, User focus, Cultural probes, Navigation design, the big button trap, Modes, Screen design and layout, Alignment and layout matters, Checking screen colors, Iteration and prototyping **HCI in the software process**: The software life cycle, Usability engineering , Iterative design and prototyping, Prototyping in practice, Design rationale	12
2.	**Design**: Principles to support usability, Standards, Guidelines, Golden rules and heuristics, HCI patterns **Implementation support:** Elements of windowing systems, Programming the application, Going with the grain, Using toolkits, User interface management systems **Evaluation techniques:** What is evaluation?, Goals of evaluation, Evaluation through expert analysis, Evaluation through user participation, Choosing an evaluation method	12
3.	**Universal design:** Universal design principles, Multimodal interaction, Designing websites for screen readers, Choosing the right kind of speech, Designing for diversity **User support:** Requirements of user support, Approaches to user support, Adaptive help systems, Designing user support systems **Cognitive models:** Goal and task hierarchies, Linguistic models, The challenge of display-based systems, Physical and device models, Cognitive architectures	12

4.	**Socio-organizational issues and stakeholder** **requirements:** Organizational issues, Capturing requirements **Communication and collaboration models:** Face-to face communication, Conversation, Text-based communication, Group working **Task analysis:** Differences between task analysis and other techniques, Task decomposition, Knowledgebased analysis, Entity–relationship-based techniques, Sources of information and data collection, Uses of task analysis	12
5.	**Dialog notations and design:** What is dialog?, Dialog design notations, Diagrammatic notations, Textual dialog notations, Dialog semantics, Dialog analysis and design **Models of the system:** Standard formalisms, Interaction models, Continuous behavior **Modeling rich interaction:** Status–event analysis, Rich contexts, Low intention and sensor-based interaction	12

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Human Computer Interaction	Alan Dix, Janet Finlay, Gregory Abowd, Russell Beale	Pearson Education	3rd	
2.	Designing the User Interface	Shneiderman B., Plaisant C., Cohen M., Jacobs S.	Pearson	5th	2013

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 The Interaction Paradigms Interaction design basics HCI in the software process	No Change	NIL
Unit 2 Design Implementation support Evaluation techniques	No Change	NIL
Unit 3 Universal design User support Cognitive models	No Change	NIL
Unit 4 Socio-organizational issues and stakeholder requirements Communication and collaboration models Task analysis	No Change	NIL
Unit 5 Dialog notations and design Models of the system Modeling rich interaction	No Change	NIL

Advanced Applications of Image Processing

COURSE CODE: MITS404b **COURSE CREDIT: 04**

Course Objectives:

- To understand the applications on image processing in different disciplines.
- To apply the concepts to new areas of research in Image processing.

Sr. No	Modules/Units	No of Lectures
1.	Fuzzy Approaches and Analysis in Image Processing, Text information extraction from images, Image and Video steganography based on DCT and wavelet transform.	**12**
2.	Zernike-Moments-Based Shape Descriptors for Pattern Recognition and Classification Applications, An Image De-Noising Method Based on Intensity Histogram Equalization Technique for Image Enhancement, A New Image Encryption Method Based on Improved Cipher Block Chaining with Optimization Technique	**12**
3.	A Technique to Approximate Digital Planar Curve with Polygon, Shape Determination of Aspired Foreign Body on Pediatric Radiography Images Using Rule- Based Approach, Evaluation of Image Detection and Description Algorithms for Application in Monocular SLAM, Diophantine Equations for Enhanced Security in Watermarking Scheme for Image Authentication	**12**
4.	Design, Construction, and Programming of a Mobile Robot Controlled by Artificial Vision, Review and Applications of Multimodal Biometrics for Secured Systems, Background Subtraction and Object Tracking via Key Frame-Based Rotational Symmetry Dynamic Texture, A Novel Approach of Human Tracking Mechanism in Wireless Camera Networks	**12**
5.	Digital Image Steganography: Survey, Analysis, and Application,Vegetation Index: Ideas, Methods, Influences, and Trends, Expert System through GIS- Based Cloud	**12**

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Advanced Image Processing Techniques and Applications	N. Suresh Kumar, Arun Kumar Sangaiah, M. Arun, S. Anand	IGI global	--	2017

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Fuzzy Approaches and Analysis in Image Processing, Text information extraction from images, Image and Video steganography based on DCT and wavelet transform	No Change	NIL
Unit 2 Zernike-Moments-Based Shape Descriptors for Pattern Recognition and Classification Applications An Image De-Noising Method Based on Intensity Histogram Equalization Technique for Image Enhancement A New Image Encryption Method Based on Improved Cipher Block Chaining with Optimization Technique	No Change	NIL
Unit 3 A Technique to Approximate Digital Planar Curve with Polygon Shape Determination of Aspired Foreign Body on Pediatric Radiography Images Using Rule-Based Approach, Evaluation of Image Detection and Description Algorithms for Application in Monocular SLAM, Diophantine Equations for Enhanced Security in Watermarking Scheme for Image Authentication	No Change	NIL
Unit 4 Design, Construction, and Programming of a Mobile Robot Controlled by Artificial Vision, Review and Applications of Multimodal Biometrics for Secured Systems, Background Subtraction and Object Tracking via Key Frame-Based Rotational Symmetry Dynamic Texture, A Novel Approach of Human Tracking Mechanism in Wireless Camera	No Change	NIL
Unit 5 Digital Image Steganography: Survey, Analysis, and Application, Vegetation Index: Ideas, Methods, Influences, and Trends, Expert System through GIS-Based Cloud	No Change	NIL

Storage as a Service

COURSE CODE: MITS404c **COURSE CREDIT: 04**

Course Objectives:

- Understand the need for Storage Area Network and Data protection to satisfy the information explosion requirements.
- Study storage technologies: SAN, NAS, IP storage etc., which will bridge the gap between the emerging trends in industry and academics.
- To get an insight of Storage area network architecture, protocols and its infrastructure.
- To study and discuss the applications of SAN to fulfill the needs of the storage management in the heterogeneous environment.
- Study and understand the management of Storage Networks
- To understand different techniques of managing store.

Sr. No	Modules/Units	No of Lectures
1.	Introduction to Information Storage Information Storage Data Types of Data Big DataInformation Storage Evolution of Storage ArchitectureData Center Infrastructure Core Elements of a DataCenter Key Characteristics of a Data Center Managinga Data Center Virtualization and Cloud Computing Data Center Environment Application Database Management System (DBMS) Host (Compute) Operating System, Memory Virtualization Device Driver 20 Volume Manager File System Compute Virtualization Connectivity Physical Components of Connectivity Interface Protocols IDE/ATA and Serial ATA 28 SCSI and Serial SCSI Fiber Channel Internet Protocol (IP) Storage Disk Drive Components Platter Spindle Read/Write Head Actuator Arm Assembly Drive Controller Board Physical Disk Structure Zoned Bit Recording Logical Block Addressing Disk Drive Performance Disk Service Time Seek Time Rotational Latency Data Transfer Rate Disk I/O Controller Utilization Host Access to Data Direct-Attached Storage DAS Benefit and Limitations Storage Design Based on Application Requirements and Disk Performance Disk NativeCommand Queuing Introduction to Flash Drives Components and Architecture of Flash Drives Features of Enterprise Flash Drives Concept in Practice: VMware ESXi Data Protection: RAID RAID Implementation Methods Software RAID Hardware RAID Array Components RAID Techniques Striping Mirroring Parity RAID Levels RAID 0 RAID 1 Nested RAID RAID 3 RAID 4 RAID 5 RAID 6 RAID Impact on Disk Performance Application IOPS and RAID Configurations RAID Comparison Hot Spares	**12**

2.	**Intelligent Storage Systems** Components of an Intelligent Storage System Front End Cache Structureof Cache Read Operation with Cache Write Operation with Cache Implementation Cache Management Cache Data Protection Back End Physical Disk Storage Provisioning Traditional Storage Provisioning LUNExpansion: MetaLUN Virtual Storage Provisioning 82 Comparison between Virtual and Traditional Storage Provisioning Use Cases for Thin andTraditional LUNs LUN Masking Types of Intelligent Storage Systems High-End Storage Systems Midrange Storage Systems **Fiber Channel Storage Area Networks** Fiber Channel: Overview The SAN and Its Evolution Components of FC SAN Node Ports Cables and Connectors Contents Interconnect Devices SAN Management Software FC Connectivity Point-to-Point Fiber Channel Arbitrated Loop Fiber Channel SwitchedFabric FC-SW Transmission Switched Fabric Ports Fiber Channel Architecture Fiber Channel Protocol Stack, FC-4 Layer FC-2 Layer FC-1 Layer FC-0 Layer Fiber Channel Addressing World Wide Names FC Frame 110. Structure and Organization of FC Data Flow Control BB_Credit EE_Credit Classes of Service Fabric Services Switched Fabric Login Types Zoning Types of Zoning FC SAN Topologies Mesh Topology Core-Edge Fabric Benefits and Limitations of Core- Edge Fabric Virtualization in SAN Block-level Storage Virtualization Virtual SAN (VSAN) **IP SAN and FCoE** iSCSI Components of iSCSI iSCSI Host Connectivity iSCSI Topologies Native iSCSI Connectivity Bridged iSCSI Connectivity Combining FC and Native iSCSI Connectivity iSCSI Protocol Stack iSCSI PDU 6 iSCSI Discovery iSCSI Names iSCSI Session iSCSI Command Sequencing FCIP FCIP Protocol Stack FCIP Topology FCIP Performance and Security FCoE I/O Consolidation Using FCoE Components of an FCoE Network Converged Network Adapter Cables FCoE Switches FCoE Frame Structure FCoE Frame Mapping FCoE Enabling TechnologiesPriority-Based Flow Control (PFC) EnhancedTransmission Selection (ETS Congestion Notification (CN) Data Center Bridging Exchange Protocol (DCBX) 1	**12**
3.	**Network-Attached Storage** General-Purpose Serversversus NAS Devices Benefits of NAS File Systems and Network FileSharing Accessing a File System Network File Sharing Components of NAS NAS I/O Operation NAS Implementations Unifi ed NAS Unifi ed NAS Connectivity 164Gateway NAS Gateway NAS Connectivity Scale-Out NAS Scale-Out NAS Connectivity NAS File-Sharing Protocols NFS CIFS Factors Affecting NAS Performance File-LevelVirtualization	**12**

	Object-Based and Unified Storage Object-Based Storage Devices Object-Based Storage Architecture Components of OSD Object Storage and Retrieval in OSD Benefits of Object-Based Storage Common Use Cases for Object-Based Storage Content- Addressed Storage CAS Use Cases Healthcare Solution: Storing Patient Studies Finance Solution: Storing Financial Records Unified Storage Components of Unifi ed Storage Data Access from Unified Storage Introduction to Business Continuity Information Availability Causes of Information Unavailability Consequences of Downtime Measuring Information Availability BC Terminology BC Planning Life CycleFailure Analysis Single Point of Failure Resolving Single Points of Failure Multipathing Software Business Impact Analysis BC Technology Solutions I/O Operation without PowerPath I/O Operation with PowerPath Automatic Path Failover Path Failure without PowerPath Path Failover with PowerPath: Active-Active ArrayPath Failover with PowerPath: Active-Passive Array Backup and Archive Backup Purpose Disaster Recovery Operational Recovery Archival Backup Considerations Backup Granularity Recovery Considerations Backup Methods 6 Backup Architecture Backup and Restore Operations Backup Topologies Backup in NAS Environments Server-Based and Serverless Backup NDMP-Based Backup Backup Targets Backup to Tape Physical Tape LibraryLimitations of Tape 2 Backup to Disk Backup to Virtual Tape Virtual Tape Library Data Deduplication for Backup Data Deduplication Methods Data Deduplication Implementation Source-Based Data Deduplication Target-Based Data Deduplication Backup in Virtualized Environments Data Archive Archiving Solution Architecture Use Case: E-mail Archiving Use Case: File Archiving	
4.	Local Replication Replication Terminology Uses of Local Replicas Replica Consistency Consistency of a Replicated File System Consistency of a Replicated Database Local Replication Technologies Host-Based Local Replication LVM-Based Replication Advantages of LVM-Based Replication Limitations of LVM-Based Replication FileSystem Snapshot Storage Array-Based Local Replication Full-Volume Mirroring Pointer-Based, Full-Volume Replication Pointer-Based Virtual Replication Network-Based Local Replication Continuous Data Protection CDP Local Replication Operation Tracking Changes to Source and Replica Restore and Restart Considerations Creating Multiple Replicas Local Replication in a Virtualized Environment Remote	**12**

	Replication Modes of Remote Replication RemoteReplication Technologies Host-Based Remote Replication LVM-Based Remote Replication Host-Based Log Shipping Storage Array-Based RemoteReplication Synchronous Replication Mode Asynchronous Replication Mode Disk-BufferedReplication Mode Network-Based Remote ReplicationCDP Remote Replication Three-Site Replication Three-Site Replication — Cascade/Multihop Synchronous + Asynchronous Synchronous + Disk Buffered Three-Site Replication — Triangle/Multitarget Data Migration Solutions Remote Replication and Migration in aVirtualized Environment Cloud Computing Cloud Enabling Technologies Characteristics of Cloud Computing Benefits of Cloud Computing Cloud Service Models Infrastructure-as-a-Service Platform-as-a-Service Software-as-a-Service Cloud Deployment Models Public Cloud Private Cloud Community Cloud Hybrid Cloud Cloud Computing Infrastructure Physical Infrastructure Virtual Infrastructure Applications and Platform Software Cloud Management and Service Creation Tools Cloud Challenges Challenges for Consumers Challenges for Providers Cloud Adoption Considerations	
5.	Securing the Storage Infrastructure Information Security Framework Risk Triad Assets Threats Vulnerability Storage Security Domains Securing the Application Access Domain Controlling User Access to Data Protecting the Storage Infrastructure 341 Data Encryption Securing the Management Access Domain Controlling Administrative Access Protecting the Management Infrastructure Securing Backup, Replication, and Archive Security Implementations in Storage Networking FC SAN FC SAN Security Architecture Basic SAN Security Mechanisms LUN Masking and Zoning Securing Switch Ports Switch-Wide and Fabric-Wide Access Control Logical Partitioning of a Fabric: Virtual SANNAS NAS File Sharing: Windows ACLs NAS File Sharing: UNIX Permissions NAS File Sharing: Authentication and Authorization Kerberos Network-Layer Firewalls IP SAN Securing Storage Infrastructure in Virtualized and Cloud Environments Security Concerns Security Measures Security at the Compute Level Security at the Network Level Security at the Storage Level Concepts in Practice: RSA and VMware SecurityProducts RSA Secure ID RSA Identity and Access Management RSA Data Protection Manager VMware vShieldManaging the Storage Infrastructure Monitoring the Storage Infrastructure Monitoring Parameters Components Monitored HostsStorage Network Storage Monitoring Examples Accessibility Monitoring Capacity	**12**

	Monitoring Performance Monitoring Security Monitoring Alerts Storage Infrastructure Management Activities Availability Management Capacity Management Performance Management Security ManagementReporting Storage Infrastructure Management in aVirtualized Environment Storage ManagementExamples Storage Allocation to a New Server/Host File System Space Management Chargeback Report Storage Infrastructure Management Challenges Developing an Ideal Solution 384Storage Management Initiative Enterprise Management Platform Information Lifecycle Management Storage Tiering Intra-Array Storage Tiering Inter-Array Storage Tiering	

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Information Storage and Management: Storing, Managing, and Protecting Digital Information in Classic, Virtualized, and Cloud Environments	EMC	John Wiley & Sons	2nd	2012

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Introduction to Information Storage Introduction to Flash Drives Concept in Practice: VMware ESXi Data Protection: RAID	No Change	NIL
Unit 2 Intelligent Storage Systems Fiber Channel Storage Area Networks IP SAN and FCoE	No Change	NIL
Unit 3 architecture of NAS and deployment along with Object based and unified storage technologies configure the storage devices to maintain highest level of availability	No Change	NIL
Unit 4 Replication and Migration techniques Local Replication Technologies Host-Based Local Replication LVM-Based Replication Network-Based Local Replication Cloud Enabling Technologies	No Change	NIL
Unit 5 Logical Partitioning of a Fabric NAS File Sharing Managing the Storage Infrastructure Monitoring the Storage Infrastructure Storage Infrastructure Management Activities techniques for managing and securing storage infrastructure.	No Change	NIL

Information Security Auditing

COURSE CODE: MITS404d **COURSE CREDIT: 04**

Course Objectives:

- Understand various information security policies in place.
- Assess an organization based on the needs and suggest the requisite informationsecurity policies to be deployed.
- Audit the organization across relevant policies and assist the organization in implementing such policies along with suggesting improvements.

Sr. No	Modules/Units	No of Lectures
1.	Secrets of a Successful Auditor Understanding the Demand for IS Audits Understanding Policies, Standards, Guidelines, and Procedures Understanding Professional Ethics Understanding the Purpose of an Audit Differentiating between Auditor and Auditee Roles Implementing Audit Standards Auditor Is an Executive Position Understandingthe Corporate Organizational Structure Governance Strategy Planning for Organizational Control Overview of Tactical Management Planning and Performance Overview of Business Process ReengineeringOperations Management Summary Audit Process, Understanding the Audit Program Establishing and Approving an Audit Charter Preplanning Specific Audits Performing an Audit Risk Assessment Determining Whether an Audit Is Possible Performing the Audit Gathering Audit Evidence Conducting Audit Evidence Testing Generating Audit Findings Report Findings Conducting Follow-up (Closing Meeting)	**12**
2.	Information Systems Acquisition and Development Project Governance and Management Business Case and Feasibility Analysis System Development Methodologies Control Identification and Design Testing Methodologies Configuration and Release Management, System Migration, Infrastructure Deployment and Data Conversion, Post-implementation Review	**12**
3.	Information Systems Operations Introduction, Common Technology, Components IT Asset Management, Job Scheduling and Production Process Automation System Interfaces End-user Computing Data Governance Systems Performance Management Problem and Incident Management Change, Configuration, Release and IT Service Level Management Database Management Business Resilience Business Impact Analysis Data Backup, Storage and Restoration Business Continuity Plan Disaster Recovery Plans	**12**

4.	Information Systems Life Cycle Governance in Software DevelopmentManagement of Software Quality Overview of the Executive Steering Committee Change Management Management of the Software Project Overview of the System Development Life CycleOverview of Data Architecture Decision Support Systems Program Architecture Centralization vs. Decentralization Electronic Commerce System Implementation and Operations Understanding the Nature of IT Services Performing IT Operations Management Performing Capacity Management, Using Administrative Protection Performing Problem Management Monitoring the Status of Controls Implementing Physical Protection	**12**
5.	Protecting Information Assets, Understanding the Threat Using Technical Protection Business Continuity and Disaster Recovery Debunking the Myths Understanding the Five Conflicting Disciplines Called Business Continuity Defining DisasterRecovery Defining the Purpose of Business Continuity Uniting Other Plans with Business Continuity Understanding the Five Phases of a Business Continuity Program Understanding the Auditor Interests in BC/DR Plans	**12**

REFERENCE BOOKS:

Books and References:					
Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	CISA®: Certified Information Systems Auditor	David Cannon	SYBEX	Fourth Edition	2016
2.	CISA Review Manual 27th Edition		ISACA		2019
3.	CISA Certified Information Systems Auditor All-in-One Exam Guide, Fourth Edition,		O'Reilly	4th Edition	2019

Note:

Particulars (University syllabus)	Proposed Syllabus	Remarks
Unit 1 Information security policies and process flow, Ethics of an Information security Auditor	No Change	NIL
Unit 2 information systems in an organization, their criticality and various governance and management policies associated with them	No Change	NIL
Unit 3 operational strategies like asset management, data governance etc. and suggest requisite changes as per organizations requirements with improvements	No Change	NIL
Unit 4 the information flow across the organization and identify the weak spots and also suggest improvements to strengthen them.	No Change	NIL
Unit 5 strong strategies to protect information assets and come up with an efficient business continuity plan, disaster recovery strategy	No Change	NIL

Project Implementation and Viva

COURSE CODE: MITS4P4 **COURSE CREDIT: 02**

The project dissertation and Viva Voce details are given in **Appendix 1**.

DEPARTMENT OF INFORMATION TECHNOLOGY
PROPOSED SCHEME OF EXAMINATION

Evaluation Scheme

Internal Evaluation (40 Marks)

The internal assessment marks shall be awarded as follows:

1. **30 marks (Any one of the following):**
   - **a.** Written Test or
   - **b.** SWAYAM (Advanced Course) of minimum 20 hours and certification exam completed or
   - **c.** NPTEL (Advanced Course) of minimum 20 hours and certification exam completed or
   - **d.** Valid International Certifications (Prometric, Pearson, Certiport, Coursera, Udemy and the like)
   - **e.** One certification marks shall be awarded one course only. For four courses, the students will have to complete four certifications.
   - **f.** Research paper publication
2. **10 marks**
   - **a.** Assignments/ Group discussions/ Debates/ Quiz/ Subject specific case study/ Mini Project/ Presentation/ Field work/ Program implementation/ any other

External Examination: (60 marks)

	All questions are compulsory	
Q1	(Based on Unit 1) Attempt ***any two*** of the following:	12
a.		
b.		
c.		
d.		
Q2	(Based on Unit 2) Attempt ***any two*** of the following:	12
Q3	(Based on Unit 3) Attempt ***any two*** of the following:	12
Q4	(Based on Unit 4) Attempt ***any two*** of the following:	12
Q5	(Based on Unit 5) Attempt ***any two*** of the following:	12

Practical Evaluation (50 marks)

A certified copy journal is essential to appear for the practical examination.

1.	Practical Question 1	20
2.	Practical Question 2	20
3.	Journal	5
4.	Viva Voce	5

OR

1.	Practical Question	40
2.	Journal	5
3.	Viva Voce	5

Project Documentation and Viva Voce Evaluation (50 marks)

The documentation should be checked for plagiarism and as per UGC guidelines, should beless than 10%.

1.	Documentation Report (Chapter 1 to 4)	20
2.	Innovation in the topic	10
3.	Documentation/Topic presentation and viva voce	20

Project Implementation and Viva Voce Evaluation (50 marks)

1.	Documentation Report (Chapter 5 to last)	20
2.	Implementation	10
3.	Relevance of the topic	10
4.	Viva Voce	10

Appendix – 1

Project Documentation and Viva-voce (Semester III) and Project Implementation and Viva-Voce (Semester IV)

Goals of the course Project Documentation and Viva-Voce

The student should:

- be able to apply relevant knowledge and abilities, within the main field of study, to a given problem
- within given constraints, even with limited information, independently analyse and discuss complex inquiries/problems and handle larger problems on the advanced level within the main field of study
- reflect on, evaluate and critically review one's own and others' scientific results
- be able to document and present one's own work with strict requirements on structure, format, and language usage
- be able to identify one's need for further knowledge and continuously develop one's own knowledge

To start the project:

- Start thinking early in the programme about suitable projects.
- Read the instructions for the project.
- Attend and listen to other student´s final oral presentations.
- Look at the finished reports.
- Talk to senior master students.
- Attend possible information events (workshops / seminars / conferences etc.) about therelated topics.

Application and approval:

- Read all the detailed information about project.
- Finalise finding a place and supervisor.
- Check with the coordinator about subject/project, place and supervisor.
- Write the project proposal and plan along with the supervisor.
- Fill out the application together with the supervisor.
- Hand over the complete application, proposal and plan to the coordinator.
- Get an acknowledgement and approval from the coordinator to start the project.

During the project:

- Search, gather and read information and literature about the theory.
- Document well the practical work and your results.
- Take part in seminars and the running follow-ups/supervision.
- Think early on about disposition and writing of the final report.
- Discuss your thoughts with the supervisor and others.
- Read the SOP and the rest you need again.

- Plan for and do the mid-term reporting to the coordinator/examiner.
- Do a mid-term report also at the work-place (can be a requirement in some work-places).
- Write the first draft of the final report and rewrite it based on feedback from the supervisor and possibly others.
- Plan for the final presentation of the report.

Finishing the project:

- Finish the report and obtain an OK from the supervisor.
- Ask the supervisor to send the certificate and feedback form to the coordinator.
- Attend the pre-final oral presentation arranged by the Coordinator.
- Rewrite the final report again based on feedback from the opponents and possibly others.
- Prepare a title page and a popular science summary for your report.
- Send the completed final report to the coordinator (via plagiarism software)
- Rewrite the report based on possible feedback from the coordinator.
- Appear for the final exam.

Project Proposal/research plan

- The student should spend the first 1-2 weeks writing a 1-2 pages project plan containing:
- Short background of the project
- Aims of the project
- Short description of methods that will be used
- Estimated time schedule for the project
- The research plan should be handed in to the supervisor and the coordinator.
- Writing the project plan will help you plan your project work and get you started in finding information and understanding of methods needed to perform the project.

Project Documentation

- The documentation should contain:
- Introduction - that should contain a technical and social (when possible) motivation of the project topic.
- Description of the problems/topics.
- Status of the research/knowledge in the field and literature review.
- Description of the methodology/approach. (The actual structure of the chapters here depends on the topic of the documentation.)
- Results - must always contain analyses of results and associated uncertainties.
- Conclusions and proposals for the future work.
- Appendices (when needed).
- Bibliography - references and links.

For the master's documentation, the chapters cannot be dictated, they may vary according to the type of project. However, in Semester III Project Documentation and Viva Voce must contain at least 4 chapters (Introduction, Review of Literature, Methodology / Approach, Proposed Design / UI design, etc. depending on the type of project.) The Semester III report should be spiral bound.

In Semester IV, the remaining Chapters should be included (which should include Experiments performed, Results and discussion, Conclusions and proposals for future work, Appendices) and Bibliography - references and links. Semester IV report should include all the chapters and should be hardbound.