

Mahatma Education Society's  
**Pillai College of Arts, Commerce & Science (Autonomous)**  
Affiliated to University of Mumbai

'NAAC Accredited 'A' grade (3 cycles)  
'Best College Award' by University of Mumbai  
ISO 9001:2015 Certified



## **SYLLABUS**

**Program: Master of Science (M. Sc.) in  
Information Technology**

# **M.Sc.- Part I Information Technology**

PCACS/PMSIT/SYL/2024-25/PI


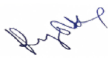




**As per National Education Policy  
Choice Based Credit & Grading System**

**Academic Year 2024-25**



**Attendance for BOS Meeting**  
**Board of Studies in the Department of Computer Science**

Sr. No.	Name of the	Details	Sign
1	Prof. Deepika Sharma	Chairperson (Head of Department of Information Technology & Computer Science), Vice Principal	
2	Dr. Gajanan Wader	Principal	
3.	Mrs.Munawira Kotyad Pillai, Director Pillai Center for Innovation & Research	Management Representative	Absent
4	Dr. Amiya Kumar Tripathy Director Center for GeoAI & ML, Professor, Computer Engineering, Don Bosco Institute of Technology, Mumbai	Subject Expert From Outside Parent University	
5	Dr.Mrs. Anjali Kulkarni CKT College, New Panvel	Vice Chancellor Nominee, University of Mumbai	
6	Mr. Tito Idicula, Director, Programming Hub	Alumni representative	
7	Mr. Anant Baddi, Security Solution Architect, cloud Google Google	Industry Representative (Industry/Corporate/Allied Sector)	Absent
8	Mr. Bhupendra Kesariya Professor,N. M. .College, Vile Parle	Subject Expert in Mathematics From Outside Parent University	
9	Mrs. Anju Somani	Faculty Specialization	
10	Mrs. Shubhangi Pawar	Faculty Specialization	

11	Mrs. Soly Zachariah	Faculty Specialization	
12	Mrs. Ramya S. Kumar	Faculty Specialization	
13	Mrs. Sujata Shahabade	Faculty Specialization	
14	Mrs. Sreevidya T.V.	Faculty Specialization	
15	Mr. Omkar Sherkhane	Faculty Specialization	
16	Mr. Abhijeet Salvi	Faculty Specialization	

# **Introduction to Program**

The Master of Science (M.Sc.) in Information Technology (IT) is a postgraduate degree program designed to provide students with advanced knowledge and skills in various aspects of information technology. This program is suitable for individuals who wish to enhance their expertise in IT and pursue careers in fields such as software development, cybersecurity, data management, systems analysis, and IT management.

The M.Sc. Information Technology program typically offers a comprehensive curriculum that covers both theoretical and practical aspects of IT. Students delve into topics such as computer programming, database management, network security, software engineering, data analytics, artificial intelligence, and human-computer interaction. The program aims to equip students with the necessary skills to tackle complex IT challenges and contribute to the development and implementation of innovative IT solutions.

## Program Outcomes

Sr No	PO Title	POs in brief
PO1	<b>Advanced Knowledge and Expertise</b>	Ability to apply the knowledge of Information Technology with recent trends aligned with research and industry.
PO2	<b>Research and Innovation</b>	Ability to apply IT in the field of Computational Research, Soft Computing, Big Data Analytics, Data Science, Image Processing, Artificial Intelligence, Networking and Cloud Computing.
PO3	<b>Interdisciplinary Perspective</b>	Ability to provide socially acceptable technical solutions in the domains of Information Security, Machine Learning, Internet of Things and Embedded System, Infrastructure Services as specializations.
PO4	<b>Leadership Abilities &amp; Entrepreneurial Mindset</b>	Ability to apply the knowledge of Intellectual Property Rights, Cyber Laws and Cyber Forensics and various standards in interest of National Security and Integrity along with IT Industry.
PO5	<b>Communication Competence</b>	Ability to write effective project reports, research publications and content development and to work in multidisciplinary environment in the context of changing technologies.
PO6	<b>Advanced Tools Usage</b>	The program teaches the students to apply the advances tools to solve real world problems
PO7	<b>Nurturing project Planning and Management Capabilities</b>	The program trains students for designing and conceptualizing the software architecture, planning and managing the product development process of complex and live software projects. It also makes students understand the decision making for selection of an appropriate project management capabilities
PO8	<b>Teamwork and Leadership Development</b>	Trains students to work in a team and also to take leadership of the project management team.

## Program Specific Outcomes

Sr. No	PSOs in brief
<b>PSO1</b>	Competence in employing principles, techniques and tools of data analytics for business analytics.
<b>PSO2</b>	Curiosity and readiness to deal with small and big data and ability to engage in exploratory research.
<b>PSO3</b>	Capability to become a successful trainer in data science, data analytics, productive decision maker and therefore well-respected personality at work and in life.
<b>PSO4</b>	Students completing this programme will become full-stack data scientists, well-equipped for a variety of job roles depending on their choices and temperament including Data Scientists, Data Analysts as well as Industrial and Societal Entrepreneurs.

## M.Sc. Information Technology (PART - I)

Semester I						
Course Code	Course Type	Course Title	Theory/ Practical	Marks	Credits	Lectures/ Week
PMSIT101	<b>Major</b>	Data Science	Theory	100	4	4
PMSIT102	<b>Major</b>	Cloud Computing	Theory	100	4	4
PMSIT103	<b>Major</b>	Soft Computing Techniques	Theory	100	4	4
PMSIT104	<b>Major Elective</b>	a.Image & Video Analytics b.Computer Forensics c.Malware Analysis	Theory	50	2	4
PMSIT105P	<b>Major Practical</b>	Practicals (PMSIT101 + PMSDA102)	Practical	100	2	4
PMSIT106P	<b>Major Practical</b>	Practicals (PMSIT103 +PMSIT104)	Practical	100	2	4
PMSIT107	<b>RM</b>	Research Methodology	Theory	50	2	2
PMSIT108P	<b>RM Practical</b>	Practicals (PMSIT107)	Practical	50	2	2
Total				650	22	28
All Subjects having Field Project as part of Continuous Assessment-2						

**Abbreviations:**

**RM : Research Methodology**

Semester II						
Course Code	Course Type	Course Title	Theory/ Practical	Marks	Credits	Lectures/ Week
PMSIT201	Major	Big Data Analytics	Theory	100	4	4
PMSIT202	Major	Microservice architecture	Theory	100	4	4
PMSIT203	Major	Advanced IOT	Theory	100	4	4
PMSIT204	Major Elective	A. Modern Networking B. Information Security C. Auditing Network Security & Cryptography	Theory	50	2	4
PMSIT205P	Major Practical	Practicals (PMSIT201 + PMSIT202)	Practical	100	2	4
PMSIT206P	Major Practical	Practicals (PMSIT203 + PMSIT204)	Practical	100	2	4
PMSIT207	OJT/FP/RP	Internship / Apprenticeship	-	100	4	(Min. 90 Hrs)
Total				650	22	24
All Subjects having Field Project as part of Continuous Assessment-2						

**Abbreviations:**

**OJT : On Job Training: Internship/ Apprenticeship**

**FP: Field Project**

**RP: Research Project**



## Evaluation Pattern

Marking Code	Marking Scheme
A	60 Marks Final Exam, 20 Marks Internal Exam, 15 Marks Field Project, 5 Marks Attendance
B	50 marks distributed within report /case study/ project/ presentation etc.
C	50 Marks Practical Examination.
D	100 Marks Practical Examination. Subject 1 Practical (50 Marks) + Subject 2 Practical (50 Marks) =100
E	100 Marks distributed within report / internship period / certificate etc.
F	50 Marks Theory Exam.

### SEMESTER - I

Course Code	Course Type	Course Title	Evaluation Pattern	Marks
PMSIT101	<b>Major</b>	Data Science	A	100
PMSIT102	<b>Major</b>	Cloud Computing	A	100
PMSIT103	<b>Major</b>	Soft Computing	A	100
PMSIT104	<b>Major Elective</b>	a. Image & Video Analytics b. Computer Forensics c. Malware Analysis	F	50
PMSIT105P	<b>Major Practical</b>	Practicals (PMSIT101 + PMSDA102)	D	100
PMSIT106P	<b>Major Practical</b>	Practicals (PMSIT103 +PMSIT104)	D	100
PMSIT107	<b>RM</b>	Research Methodology	B	50
PMSIT108P	<b>RM Practical</b>	Practicals (PMSIT107)	C	50
Total				650

**SEMESTER – II**

<b>Course Code</b>	<b>Course Type</b>	<b>Course Title</b>	<b>Evaluation Pattern</b>	<b>Marks</b>
PMSIT201	<b>Major</b>	Big Data Analytics	A	100
PMSIT202	<b>Major</b>	Microservice architecture	A	100
PMSIT203	<b>Major</b>	Advanced IOT	A	100
PMSIT204	<b>Major Elective</b>	a. Modern Networking b. Information Security c. Auditing Network Security & Cryptography	F	50
PMSIT205P	<b>Major Practical</b>	Practicals (PMSIT201 + PMSIT202)	D	100
PMSIT206P	<b>Major Practical</b>	Practicals (PMSIT203 + PMSIT204)	D	100
PMSIT207	<b>OJT/FP/RP</b>	Internship / Apprenticeship	E	100
Total				650

# **SEMESTER - I**

BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	I
Course Name	Data Science
Course Code	PMSIT101
Type of course	Major
Level of the Subject	Advanced
Credit points	4 Theory + 1 Practical

### Course Objectives:

1. Develop in depth understanding of the key technologies in data science and business analytics: data mining, machine learning, visualization techniques, predictive modeling, and statistics.
2. Gain practical, hands-on experience with statistics programming languages and big data tools through coursework and applied research experiences.

Unit No.	Name of Unit	Content	Hours
1	Introduction to Data Science	<p><b>Data Science Technology Stack:</b> Rapid Information Factory Ecosystem, Data Science Storage Tools, Data Lake, Data Vault, Data Warehouse Bus Matrix, Data Science Processing Tools ,Spark, Mesos, Akka , Cassandra, Kafka, Elastic Search, R ,Scala, Python, MQTT, The Future</p> <p><b>Layered Framework:</b> Definition of Data Science Framework, Cross- Industry Standard Process for Data Mining (CRISP-DM), Homogeneous Ontology for Recursive Uniform Schema, The Top Layers of a Layered Framework, Layered Framework for High-Level Data Science and Engineering</p> <p><b>Business Layer:</b> Business Layer, Engineering a Practical Business Layer</p> <p><b>Utility Layer:</b> Basic Utility Design, Engineering a Practical Utility Layer</p>	15
2	Data Management and Analysis Framework	<p><b>Three Management Layers:</b> Operational Management Layer, Processing-Stream Definition and Management, Audit, Balance, and Control Layer, Balance, Control, Yoke Solution, Cause-and-Effect, Analysis System, Functional Layer, Data Science Process</p> <p><b>Retrieve Superstep :</b> Data Lakes, Data Swamps Training the Trainer Model, Understanding the Business Dynamics of the Data Lake</p> <p>Actionable Business Knowledge from Data Lakes, Engineering a Practical Retrieve Superstep, Connecting to Other Data Sources,</p>	15

3	Optimizing Data Analysis	Assess Superstep: Assess Superstep, Errors, Analysis of Data, Practical Actions, Engineering a Practical Assess Superstep	15
4	Modeling methods	<p><b>Process Superstep:</b> DataVault, Time-Person-Object-Location-Event Data Vault, Data Science Process, Data Science.</p> <p><b>Transform Superstep :</b> Transform Superstep, Building a Data Warehouse, Transforming with Data Science, Hypothesis Testing, Overfitting and Underfitting, Precision-Recall, Cross-Validation Test.</p> <p><b>Transform Superstep:</b> Univariate Analysis, Bivariate Analysis, Multivariate Analysis, Linear Regression, Logistic Regression, Clustering Techniques, ANOVA, Principal Component Analysis (PCA), Decision Trees, Support Vector Machines, Networks, Clusters, and Grids, Data Mining, Pattern Recognition, Machine Learning, Bagging Data, Random Forests, Computer Vision (CV) , Natural Language Processing (NLP), Neural Networks, TensorFlow.</p> <p><b>Organize and Report Supersteps :</b> Organize Superstep, Report Superstep, Graphics, Pictures, Showing the Difference</p>	15
<b>Total No. Of Lectures</b>			<b>60</b>

#### Course Outcomes:

1. Understand the fundamentals concepts of the expert system and its applications..
2. Analyze probability and the concept of fuzzy sets for solving AI based problems.
3. Understand the applications of Machine Learning. The learner can also apply a fuzzy system for solving problems
4. Apply to understand the applications of genetic algorithms in different problems related to artificial intelligence.
5. Create knowledge representation techniques in natural language processing.

#### References:

1. Andreas François Vermeulen (2018). Practical Data Science, APress
2. Sinan Ozdemir (2016), Principles of Data Science, New Delhi: PACKT
3. Joel Grus, T. Devi, (2015). Data Science from Scratch: O'Reilly
4. Joel Grus (2017). Data Science from Scratch first Principle in python, Shroff Publisher s
5. N C Das (2018). Experimental Design in Data science with Least Resources , Shroff Publisher s

<b>CASE STUDY</b>	
1	<p>Scenario: Imagine you are a data scientist at a retail company. Your task is to analyze customer purchase history to improve sales strategies. The company has collected data over the past year, including customer demographics, purchase details, and product information.</p> <p>Task: Your goal is to build a predictive model that can forecast future purchases based on the given data. This model should help the marketing team to target customers more effectively and increase sales.</p>
2	Scenario: A healthcare company wants to optimize its data analysis process to predict

patient readmission rates more accurately. They have collected a vast dataset over several years, including patient demographics, treatment details, and readmission outcomes.  
Task: Your objective is to refine the data analysis process to enhance the predictive accuracy of patient readmissions. This will aid the healthcare company in identifying at-risk patients and improving care management strategies.

## PRACTICALS

Practical No.	Details
1	Create Data Model using Cassandra.
2	Conversion from different formats to HORUS format.
3	Auditing through Logging.
4	Retrieving Data.
5	Assessing Data.
6	Processing Data.
7	Transforming Data.
8	Organizing Data.
9	Generating Reports.
10	Data Visualization with Power BI.

BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	I
Course Name	Cloud Computing
Course Code	PMSIT102
Type of course	Major
Level of the Subject	Advanced
Credit points	4 Theory + 1 Practical

### Course Objectives:

1. To learn how to use Cloud Services. To implement Virtualization.
2. To implement Task Scheduling algorithms. Apply Map-Reduce concept to applications. To build a Private Cloud.

Unit No.	Name of Unit	Content	Hours
1	<b>Introduction to Cloud Computing</b>	<p><b>Introduction to Cloud Computing:</b> Introduction, Historical developments, Building Cloud Computing Environments,</p> <p><b>Principles of Parallel and Distributed Computing:</b> Eras of Computing, Parallel v/s distributed computing, Elements of Parallel Computing, Elements of distributed computing, Technologies for distributed computing.</p> <p><b>Virtualization:</b> Introduction, Characteristics of virtualized environments, Taxonomy of virtualization techniques, Virtualization and cloud computing, Pros and cons of virtualization, Technology examples. Logical Network Perimeter, Virtual Server, Cloud Storage Device, Cloud usage monitor, Resource replication, Ready-made environment.</p>	15
2	<b>Cloud Computing Architecture:</b>	<p><b>Cloud Computing Architecture:</b> Introduction, Fundamental concepts and models, Roles and boundaries, Cloud Characteristics, Cloud Delivery models, Cloud Deployment models, Economics of the cloud, Open challenges</p> <p><b>Fundamental Cloud Security:</b> Basics, Threat agents, Cloud security threats, additional considerations.</p> <p><b>Industrial Platforms and New Developments:</b> Amazon Web Services, Google App Engine, Microsoft Azure.</p>	15
3	<b>Specialized Cloud</b>	<p><b>Specialized Cloud Mechanisms:</b> Automated Scaling listener, Load Balancer, SLA monitor,</p>	

	<b>Mechanisms</b>	<p>Pay-per-use monitor, Audit monitor, fail over system, Hypervisor, Resource Centre, Multidevice broker, State Management Database.</p> <p><b>Cloud Management Mechanisms:</b> Remote administration system, Resource Management System, SLA Management System, Billing Management System,</p> <p><b>Cloud Security Mechanisms:</b> Encryption, Hashing, Digital Signature, Public Key ,Infrastructure (PKI), Identity and Access Management (IAM), Single Sign-On (SSO), Cloud-Based Security Groups, Hardened Virtual Server Images</p>	<b>15</b>
4	<b>AWS Cloud Computing</b>	<p><b>AWS Cloud Computing:</b> Overview of AWS Cloud, AWS Free Tier Account Creation,AWS Management Console,AWS Region,AWS Payment Method,Setting up Billing/Budget Alarm</p> <p><b>Identify and Access Management (IAM):</b>Create IAM users and Group,Copy Permission from existing users,Applying Policies/Permission to Groups,Set Password Policy for IAM Users,Active virtual Multi-Factor Authentication (MFA)</p> <p><b>EC2 :</b>Amazon Machine Image(AIM) ,Launching an EC2 Instance,Create Public/Private Key Pair,Understanding the virtualization concept in AWS (Xen hypervisor)</p> <p>Getting Started with the AWS Elastic Cloud Computing Exploring the databases services on AWS</p>	<b>15</b>
<b>Total No. of Lectures</b>			<b>60</b>

**Course Outcomes :**

1. Analyze the Cloud computing setup with its vulnerabilities and applications using different architectures.
2. Evaluate different workflows according to requirements and apply map reduce programming model.
3. Apply and design suitable Virtualization concepts, Cloud Resource Management and design scheduling algorithms.
4. Create combinatorial auctions for cloud resources and design scheduling algorithms for computing clouds
5. Assess cloud Storage systems and Cloud security, the risks involved, its impact and develop cloud application
6. Apply the impact of engineering on legal and societal issues involved in addressing the security issues of cloud computing.



**References:**

1. Rajkumar Buyya, Christian Vecchiola, S. Thamarai Selvi Cloud Computing Foundations and Applications Programming Elsevier
2. Thomas Erl, Zaigham Mahmood, and Ricardo Puttini, "Cloud Computing Concepts, Technology & Architecture", Prentice Hall, 2013.
3. Kai Hwang, Jack Dongarra, Geoffrey Fox, "Distributed and Cloud Computing, From Parallel Processing to the Internet of Things", MK Publishers. 2012.
4. Cloud Computing: Concepts, Technology & Architecture" by Thomas Erl, Ricardo Puttini, and Zaigham Mahmood
5. Cloud Native Infrastructure: Patterns for Scalable Infrastructure and Applications in a Dynamic Environment" by Justin Garrison and Kris Nova

<b>CASE STUDY</b>	
<b>SR. NO</b>	<b>Details</b>
1.	Scenario: JencoMart, a global retailer with over 10,000 stores in 16 countries, is looking to migrate several critical applications to the cloud. Their current infrastructure is at the end of its life and no longer supported. They aim to optimize for capacity during peak periods, guarantee service availability, reduce on-premises footprint, and expand services into Asia. Task: As a Cloud Architect, you are tasked with assessing key applications for cloud suitability, modifying them for the cloud, and leveraging managed services wherever feasible.
2.	A multinational corporation, GlobalTech Inc., is looking to adopt cloud computing to improve its IT infrastructure. The company has a diverse portfolio of products and services and operates in multiple regions across the globe. They aim to enhance their data analytics capabilities, streamline operations, and reduce IT costs. Task: As a Cloud Solutions Architect, you are tasked with designing a cloud computing architecture that meets the company's needs and aligns with its strategic goals.

<b>PRACTICALS</b>	
<b>Practical No.</b>	<b>Details</b>
1	Socket Programming
2	RMI Programming
3	Programming Web Services
4	Implement Xen virtualization and manage with XenCenter
5	Implement virtualization using VMWare ESXi Server and managing with vCenter
6	Implement Windows Hyper V virtualization
7	Develop application for Microsoft Azure
8	Develop application for Google Cloud Platform

BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	I
Course Name	Soft Computing Techniques
Course Code	PMSIT103
Type of course	Major
Level of the Subject	Advanced
Credit points	4 Theory + 1 Practical

**Course Objectives:**

1. Analyze the data and its obstacles along with different learning methods.
2. Apply knowledge of predictive models using statistical and data mining techniques.

Unit No.	Name of Unit	Content	Hours
1	<b>Soft Computing: An Overview of Techniques</b>	<b>Introduction of soft computing</b> , soft computing vs. hard computing, various types of soft computing techniques, Fuzzy Computing, Neural Computing, Genetic Algorithms, Associative Memory, Adaptive Resonance Theory, Classification, Clustering, Bayesian Networks, Probabilistic reasoning, applications of soft computing.	15
2	<b>Unraveling Artificial Neural Networks</b>	<b>Artificial Neural Network:</b> Fundamental concept, Evolution of Neural Networks, Basic Models, McCulloch-Pitts Neuron, Linear Separability, Hebb Network. <b>Supervised Learning Network:</b> Perceptron Networks, Adaptive Linear Neuron, Multiple Adaptive Linear Neurons, Backpropagation Network, Radial Basis Function, Time Delay Network, Functional Link Networks, Tree Neural Network. <b>Associative Memory Networks:</b> Training algorithm for pattern Association, Autoassociative memory network, heteroassociative memory network, bi-directional associative memory, Hopfield networks, iterative autoassociative memory networks, temporal	15

3	<b>Exploring Advanced Neural Networks</b>	<p>UnSupervised Learning Networks: Fixed weight competitive nets, Kohonen self-organizing feature maps, learning vectors quantization, counter propagation networks, adaptive resonance theory networks</p> <p>Special Networks: Simulated annealing, Boltzman machine, Gaussian Machine, Cauchy Machine, Probabilistic neural net, cascade correlation network, cognition network, neo-cognition network, cellular neural network, optical neural network Third Generation Neural Networks</p> <p>Spiking Neural networks, convolutional neural networks, deep learning neural networks, extreme learning machine model.</p>	15
4	<b>Exploring Fuzzy Logic and Soft Computing Techniques</b>	<p><b>Introduction to Fuzzy Logic,</b>  Classical Sets and Fuzzy sets:  Classical sets, Fuzzy sets.  Classical Relations and Fuzzy Relations:  Cartesian Product of relation, classical relation, fuzzy relations, tolerance and equivalence relations, non-iterative fuzzy sets.  Membership Function: features of the membership functions, fuzzification, methods of membership value assignments.  Defuzzification: Lambda-cuts for fuzzy sets, Lambda-cuts for fuzzy relations, Defuzzification methods.  Fuzzy Arithmetic and Fuzzy measures: fuzzy arithmetic, fuzzy measures, measures of fuzziness, fuzzy integrals.</p> <p>Fuzzy Rule base and Approximate reasoning: Fuzzy proportion, formation of rules, decomposition of rules, aggregation of fuzzy rules, fuzzy reasoning, fuzzy inference systems, Fuzzy logic control systems, control system design, architecture and operation of FLC system, FLC system models and applications of FLC System.</p> <p>Genetic Algorithm: Biological Background, Traditional optimization and search techniques, genetic algorithm and search space, genetic algorithm vs. traditional algorithms, basic terminologies, simple genetic algorithm, general genetic algorithm, operators in genetic algorithm, stopping condition for genetic algorithm flow, constraints in genetic algorithm, problem solving using genetic algorithm, the schema theorem, classification of genetic algorithm, Holland classifier systems, genetic programming, advantages and limitations and applications of genetic algorithm.  Differential Evolution Algorithm, Hybrid soft computing</p>	15

		techniques – neuro – fuzzy hybrid, genetic neuro-hybrid systems, genetic fuzzy hybrid and fuzzy genetic hybrid systems.	
<b>Total No. Of Lectures</b>			<b>60</b>

**Course Outcomes:**

1. Apply and describe soft computing techniques and their roles in building intelligent machines
2. Understand the feasibility of applying a soft computing methodology for a particular problem
3. Apply fuzzy logic and reasoning to handle uncertainty and solve engineering problems
4. Apply genetic algorithms to combinatorial optimization problems
5. Apply neural networks for classification and regression problems
6. Analyze the use existing software tools to solve real problems using a soft computing approach

**References:**

1. Artificial Intelligence and Soft Computing by Anandita Das Battacharya SPD publication 3rd. 2018
2. Principles of Soft computing by S.N.Sivananda m S.N.Deepa Wiley publication 3rd 2019
3. Neuro-Fuzzy and Soft Computing by J.S.R.Jang, C.T.Sun and E.Mizutani Prentice Hall of India 2004
4. Neural Networks, Fuzzy Logic and Genetic Algorithms: Synthesis & Applications by S.Rajasekaran, G. A. Vijayalaksham, Prentice Hall of India 2004
5. Fuzzy Logic with Engineering Applications by Timothy J.Ross, McGraw- Hill publisher 1997

<b>CASE STUDY</b>	
<b>1.</b>	<p><b>Prediction of Storm Surge and Inundation Using Soft Computing Techniques</b></p> <p><b>Background</b>  Natural hazards, such as tropical cyclones, have significant socio-economic implications. Operational forecasting of landfall, maximum sustained winds, storm surge height, and associated inland inundation resulting from tropical cyclones is a challenging task. The coast of Odisha, India, which borders the Bay of Bengal, is particularly vulnerable to high-intensity tropical cyclones.</p>
<b>2.</b>	<p><b>Fuzzy Logic in Surveillance Big Video Data Analysis</b></p> <p><b>Background</b>  Continuous surveillance through CCTV cameras generates vast amounts of data daily, leading to the term “Big Video Data” (BVD). BVD encompasses intelligent surveillance, activity recognition, and other challenging tasks. However, existing methods face limitations in terms of computational complexity and practical implementation.</p> <p><b>Objective</b>  The goal of this study is to explore the usage of fuzzy logic for surveillance within the context of BVD. Fuzzy logic, known for its ability to handle real-world uncertainties, can complement large artificial intelligence models and reduce training complexities.</p>

## PRACTICALS

Practical No.	Details
1	a Design a simple linear neural network model. b Calculate the output of a neural net using both binary and bipolar sigmoidal functions.
2	Generate AND/NOT function using McCulloch-Pitts neural net.
3	Generate XOR function using McCulloch-Pitts neural net.
4	Write a program to implement Hebb's rule.
5	Write a program to implement of delta rule.
6	Hebb Network Algorithm
7	Kohonen Self organizing map
8	Hopfield Network Algorithm
9	Membership and Identity Operators   in, not in. Membership and Identity Operators   is, is not.
10	Simple genetic algorithm

BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	I
Course Name	Image & Video Analytics
Course Code	PMSIT104
Type of course	Major Elective
Level of the Subject	Advanced
Credit points	2 Theory + 1 Practical

### Course Objectives:

1. The main objective of this course is making the students know about various fundamental principles of image and video analysis and have an idea of their application.
2. Understand how to apply filters in an image & transformations in images and videos.

Unit No.	Unit Name	Content	Hours
1	<b>Digital image representation</b>	<b>Digital image representation</b> - Visual Perception- Sampling and Quantization- Basic Relations between Pixels- Mathematical Tools Used in Digital Image Processing: Fundamental Operations –Vector and Matrix Operations- Image Transforms (DFT, DCT, DWT, Hadamard).	15
2	<b>Fundamentals of spatial filtering:</b>	Fundamentals of spatial filtering: spatial correlation and convolution-smoothing blurring- sharpening edge detection - Basics of filtering in the frequency domain: smoothing-blurring- sharpening – Histograms and basic statistical models of image.	15
3	<b>Color models and Transformations</b>	<b>Color models and Transformations</b> – Image and Video segmentation-Image and video demonizing Image and Video enhancement- Image and Video compression. Object detection and recognition in image and video-Texture models Image and Video classification models- Object tracking in Video.	15
4	<b>Applications and Case studies</b>	<b>Applications and Case studies</b> - Industrial- Retail Transportation & Travel- Remote sensing-Video Analytics in WSN: IoT Video Analytics Architectures.	15
<b>Total No. of Lectures</b>			<b>60</b>

## Course Outcomes:

1. Understand the requirements of image processing.
2. Illustrate the principles and techniques of digital image in applications related to digital imaging systems.
3. Demonstrate image recognition and motion recognition.
4. Understand color models, transformations and the fundamentals of digital video processing.
5. Illustrate the object detection, recognition and tracking of objects.
6. Analysis of the video processing in applications.

## References:

1. Video Analytics for Business Intelligence by Caifeng Shan, FatihPorikli, Tao Xiang, Shaogang Gong Springer
2. Intelligent Transport systems: Technologies and Applications by AsierPerallos, Unai Hernandez-Jayo, Enrique Onieva, Ignacio Julio Garcia Zuazola Wiley\
3. Analysis of Urban Growth and Sprawl from Remote Sensing Data byBasudeb Bhatta Springer
4. Computer Vision: Algorithms and Applications" by Richard Szeliski
5. Digital Image Processing by Rafael C. Gonzalez and Richard E. Woods

CASE STUDY	
1	<p><b>Impact of Spatial Resolution and Filtering Algorithms on DEM Accuracy</b></p> <p><b>Background</b></p> <p>Nowadays, digital elevation models (DEMs) play a crucial role in representing Earth's surface. They are widely used in geospatial analysis, particularly in geomorphometric research. Spaceborne photogrammetry remains an essential technique for obtaining high-resolution elevation data, especially over large or inaccessible areas. However, DEMs acquired directly through remote sensing instruments, such as photogrammetric DEMs, are susceptible to uncertainty.</p> <p><b>Study Area: Sahel-Doukkala, Morocco</b></p> <p>Our case study focuses on the Sahel-Doukkala region, characterized by relatively low relief. We aim to provide a comprehensive understanding of high-resolution Spaceborne photogrammetric DEM generation and enhancement for geomorphometric studies in this area.</p>
2	<p><b>Color Transformation in Digital Art</b></p> <p><b>Background</b></p> <p>In the vibrant world of digital art, color plays a pivotal role. Artists often manipulate colors to evoke emotions, create visual impact, and convey their artistic vision. Our case study revolves around a talented digital artist named Maya, who is working on a series of abstract paintings.</p> <p><b>Scenario</b></p> <p>Maya has just completed her latest artwork, titled "Cosmic Symphony." The painting features swirling galaxies, nebulae, and celestial bodies. However, she feels that the color palette lacks the desired cosmic intensity. She wants to transform the existing colors to achieve a more otherworldly effect.</p>

## PRACTICALS

<b>Practical No</b>	<b>Details</b>
1	Write a python program to perform fundamental operations on Image.
2	Write a python program to filter images by using spatial domain in Digital Image Processing.
3	Write a python program to filter image by using the frequency domain in digital image processing
4	Write a program to perform segmentation on Image and Video.
5	Write a program to apply enhancement on Image and video.
6	Write a program to perform compression Image and Video.
7	Write a program to build a Video classification model.
8	Develop an application to Object detection and recognition in image and video.
9	Develop an application to Object tracking in Video.
10	Develop an application to Video Analytics in WSN.



BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	I
Course Name	Computer Forensics
Course Code	PMSIT104
Type of course	Major Elective
Level of the Subject	Advanced
Credit points	2 Theory + 1 Practical

**Course Objectives:**

1. To correctly define and cite appropriate instances for the application of computer forensics  
Correctly collect and analyze computer forensic evidence.
2. Identify the essential and up-to-date concepts, algorithms, protocols, tools, and methodology of Computer Forensics

Unit No.	Unit Name	Content	Hours
1	<b>Cyber Crime and computer crime</b>	Introduction to Digital Forensics, Definition and types of cybercrimes, electronic evidence and handling, electronic media, collection, searching and storage of electronic media, introduction to internet crimes, hacking and cracking, credit card and ATM frauds, web technology, cryptography, emerging digital crimes and modules.	15
2	<b>Basics of Computer organization, component</b>	Computer organization, components of computer- input and output devices, CPU, Memory hierarchy, types of memory, storage devices, system softwares, application softwares, basics of computer languages.	15
3	<b>Computer Forensics</b>	Definition and Cardinal Rules, Data Acquisition and Authentication Process, Windows Systems-FAT12, FAT16, FAT32 and NTFS, UNIX file Systems, mac file systems, computer artifacts, Internet Artifacts, OS Artifacts and their forensic applications	15
4	<b>Forensic Tools and Processing of Electronic Evidence</b>	Introduction to Forensic Tools, Usage of Slack space, tools for Disk Imaging, Data Recovery, Vulnerability Assessment Tools, Encase and FTK tools, Anti Forensics and probable counters, retrieving information, process of computer forensics and digital investigations, processing of digital evidence, digital images, damaged SIM and data recovery, multimedia evidence, retrieving deleted data: desktops, laptops and mobiles, retrieving data from slack space, renamed file, ghosting, compressed files.	15
<b>Total No. of Lectures</b>			<b>60</b>

**Course Outcomes:**

1. Understand the fundamentals of Computer Forensics
2. Apply, analyze and validate Forensics Data
3. Analyze the tools and tactics associated with Computer Forensics
4. Evaluate and cite appropriate instances for the application of computer forensics Correctly collect and analyze computer forensic evidence
5. Analyze The essential and up-to-date concepts, algorithms, protocols, tools, and methodology of Computer Forensics
6. Understand the threats in networks and security concepts.

**References:**

1. C. Altheide & H. Carvey Digital Forensics with Open Source Tools, Syngress, 2011. ISBN: 9781597495868.
2. Selected readings from various sources as assigned
3. Online Course management System: <https://esu.desire2learn.com/>
4. Computer Forensics: Investigating File and Operating Systems, Wireless Networks, and Storage" by John R. Vacca
5. Guide to Computer Forensics and Investigations" by Bill Nelson, Amelia Phillips, and Christopher Steuart

<b>CASE STUDY</b>	
<b>1</b>	<p><b>The Mysterious Data Breach</b></p> <p><b>Background</b></p> <p>A prominent financial institution, SecureBank, recently experienced a significant data breach. The bank’s internal systems were compromised, leading to unauthorized access to sensitive customer information. The incident was discovered when several customers reported fraudulent transactions and unauthorized account access.</p> <p><b>Incident Timeline</b></p> <ol style="list-style-type: none"><li>1. Initial Discovery (Day 0): SecureBank’s security team noticed unusual network activity. They identified a suspicious IP address attempting to gain access to the bank’s database servers.</li><li>2. Investigation (Days 1-3): The security team isolated the affected servers. They discovered that an employee’s credentials were used to access the system. The employee, Alex Turner, was placed under investigation.</li><li>3. Forensic Analysis (Days 4-7): The digital forensics team examined Alex Turner’s workstation. They found evidence of malware, specifically a keylogger, installed on his computer. The keylogger captured login credentials, including those of other employees.</li><li>4. Recovery and Mitigation (Days 8-10): SecureBank reset all compromised passwords. They patched vulnerabilities in their systems. Alex Turner was terminated from his position.</li></ol>
<b>2</b>	<p><b>The Mysterious Insider Leak</b></p> <p><b>Background</b></p> <p>A prominent financial institution, GlobalBank, has been experiencing a series of data leaks. Confidential client information, transaction records, and internal communications have been exposed. The bank suspects an insider is responsible for these leaks.</p>

**Incident Details**

**Date:** March 15, 2024

**Incident:** A sensitive internal memo containing details about a high-profile merger was leaked to a competitor.

**Suspects:** Three employees with access to the memo:

1. Alice Thompson (Senior Analyst)
2. David Miller (IT Administrator)
3. Sophia Lee (Legal Counsel)

**Evidence Collected****1. Email Logs:**

Suspicious email exchanges between Alice and an external email address.

David accessed the memo file on the server multiple times.

Sophia had a heated argument with her supervisor about the merger.

**2. Network Traffic Analysis:**

Unusual data transfers from Alice's workstation to an external IP address.

David's workstation communicated with a known hacking forum.

Sophia's laptop showed signs of encrypted communication.

**3. Physical Evidence:**

Alice's desk contained handwritten notes related to the merger.

David's office had a hidden USB drive with confidential files.

Sophia's trash bin contained shredded documents.

**PRACTICALS**

<b>Practical No</b>	<b>Details</b>
1	Live Case Studies
2	Linux commands
3	Open Source Forensic Tools
4	Disk Forensics and Data Recovery
5	Steganography
6	Keyloggers
7	Network monitors
8	Flowchart management
9	UML diagrams
10	eCommerce on websites

BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	I
Course Name	Malware Analysis
Course Code	PMSIT104
Type of course	Major Elective
Level of the Subject	Advanced
Credit points	2 Theory + 1 Practical

### Course Objectives:

1. Understanding the fundamentals of malware forensics and binary analysis.
2. Performing basic and advanced static analyses of malware and unknown binary files.

Unit No.	Unit Name	Content	Hours
1	<b>Introduction to Malware Analysis &amp; its techniques</b>	<b>Malware Analysis:</b> Introduction, Techniques, Types of malware, General rules for Malware Analysis. <b>Basic Static Techniques:</b> 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. <b>Malware Analysis in Virtual Machines:</b> Structure of VM, Creating and using Malware Analysis machine, Risks of using VMware for malware analysis, Record/Replay. <b>Basic Dynamic Analysis:</b> 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 <b>IDA PRO:</b> Loading an executable, IDA Pro Interface, Using cross references, Analysing functions, Using graphing options, Enhancing disassembly, Extending IDA with plug-ins.	15
2	<b>Malware Analyzing &amp; Advanced Dynamic Analysis.</b>	<b>Recognising C Code constructs in assembly:</b> 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. <b>Analysing Malicious Windows Programs:</b> The windows API, The Windows Registry, Networking APIs Understanding running malware. Kernel v/s user mode, Native API. <b>Advanced Dynamic Analysis – Debugging:</b> Sourcelevel v/s Assembly-level debugging, kernel v/s user mode debugging, Using a debugger, Exceptions, Modifying	15

		execution with a debugger, modifying program execution <b>Advanced Dynamic Analysis – OLLYDBG:</b> 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.	
3	<b>Working with malware activity.</b>	<b>Kernel Debugging with WINDBG:</b> Drivers and kernel code, Using WinDbg, Microsoft Symbols, kernel debugging and using it, Rootkits, Loading drivers, kernel issues with windows. <b>Malware Functionality – Malware Behavior:</b> Downloaders and launchers, Backdoors, Credential stealers, Persistence mechanisms, Privilege escalation, covering the tracks. <b>Covert Malware Launching:</b> Launchers, Process injection, Process replacement, Hook injection, detours, APC injection. <b>Data Encoding:</b> Goal of Analysing algorithms, Simple ciphers, Common cryptographic algorithms, Custom encoding, decoding. <b>Malware – focused network signatures:</b> Network countermeasures, Safely investigating attackers online, Content-Based Network Countermeasures, Combining Dynamic and Static Analysis Techniques, Understanding the Attacker’s Perspective.	15
4	<b>Working with Anti-disassembly &amp; Anti-Virtual machine techniques</b>	<b>Anti-disassembly:</b> Concepts, Defeating disassembly algorithms, anti-disassembly techniques, Obscuring flow control, Thwarting stack-frame analysis. <b>Anti-debugging:</b> Windows debugger detection, debugger behavior, Interfering with debugger functionality, Debugger vulnerabilities <b>Anti-virtual machine techniques:</b> VMWare artifacts, Vulnerable functions, Tweaking settings, Escaping the virtual machine. <b>Packers and unpacking:</b> Packer anatomy, Identifying Packed Programs, Unpacking options, Automated Unpacking, Manual Unpacking, Common packers, Analysing without unpacking, Packed DLLs, <b>Shellcode Analysis:</b> Loading shellcode for analysis, Position-independent Code, Identifying Execution Location, Manual Symbol Resolution, Shellcode encoding, NOP Sleds, Finding Shellcode. <b>64-bit Malware:</b> Why 64-bit malware? Differences in x64 architecture, Windows 32-bit on Windows 64-bit, 64-bit hints at malware functionality	15
<b>Total No. of Lectures</b>			<b>60</b>

#### Course Outcomes:

1. Understand various introductory techniques of malware analysis and creating the testing environment.
2. Create advanced dynamic analysis and recognize constructs in assembly code.
3. Create Reverse Engineering using OLLYDBG and WINDBG and study the behaviors and functions of malware
4. Understand data encoding, various techniques for anti-disassembly and anti-debugging.
5. Understand various anti virtual machine techniques and
6. Apply shellcode analysis of various languages along with x64 architecture.

**References:**

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
4. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig
5. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory" by Michael Hale Ligh, Andrew Case, Jamie Levy, and Aaron Walter

<b>CASE STUDY</b>	
<b>1</b>	<p><b>The Mysterious Malware</b></p> <p><b>Background</b> A cybersecurity analyst named Alex received an anonymous email containing an attachment named "Invoice.docx." The email claimed to be from a legitimate vendor, but Alex's instincts told them something was amiss. They decided to investigate further.</p> <p><b>Analysis Steps</b></p> <p><b>1. Static Analysis:</b></p> <ul style="list-style-type: none"><li>● Alex extracted the "Invoice.docx" file and examined its properties.</li><li>● Key findings:<ul style="list-style-type: none"><li>○ The document contained macros.</li><li>○ The macros were obfuscated and triggered when the document was opened.</li><li>○ The macros attempted to download a suspicious executable file from a remote server.</li></ul></li></ul> <p><b>Dynamic Analysis:</b></p> <ul style="list-style-type: none"><li>● Alex ran the suspicious executable in a controlled environment (sandbox).</li><li>● Behavior observed:<ul style="list-style-type: none"><li>○ The executable created a hidden folder in the user's profile directory.</li><li>○ It attempted to connect to a command-and-control (C2) server.</li><li>○ It started encrypting files on the local machine.</li></ul></li></ul> <p><b>Hybrid Analysis:</b></p> <ul style="list-style-type: none"><li>● Combining static and dynamic findings, Alex concluded:<ul style="list-style-type: none"><li>○ The malware was ransomware.</li><li>○ It encrypted files using AES-256.</li><li>○ The C2 server was located in a foreign country.</li></ul></li></ul>
<b>2</b>	<p><b>Handling Anti-Virtual Machine Techniques in Malicious Software</b></p> <p>In this study, researchers explored methods to detect and mitigate VM-aware malware. The objective was to identify and address evasion techniques used by malicious software to evade detection within virtualized environments.</p> <p><b>Key Findings:</b></p> <p><b>Dynamic Analysis:</b> Researchers employed dynamic analysis techniques to monitor the behavior of suspicious executables. By observing runtime characteristics, they could differentiate between VMs and physical machines. For instance, VMs often exhibit specific timing patterns, memory access behaviors, and CPU instructions that differ from physical hosts.</p> <p><b>Hardware-Based Checks:</b> The study investigated hardware-based checks. Some malware attempts to query specific hardware features (such as CPU vendor IDs or virtualization extensions) to determine if it is running in a VM. Researchers proposed countermeasures,</p>

such as modifying the reported values or introducing delays, to confuse the malware.

**Memory Inspection:** Malware often inspects memory to identify VM-specific artifacts (e.g., hypervisor strings or memory structures). Researchers developed techniques to obfuscate or hide these artifacts, making it harder for malware to detect virtualization.

**Timing Attacks:** VMs exhibit consistent timing behavior due to virtualized hardware. Malware can exploit this by measuring execution time for specific operations. Researchers explored ways to introduce random delays or jitter to disrupt this consistency.

**Environmental Checks:** Malware may query environment variables or registry keys associated with virtualization software. Researchers proposed altering these values or providing fake information to mislead the malware.

<b>PRACTICALS</b>	
<b>Practical No</b>	<b>Details</b>
1	Antivirus Scanning: <ul style="list-style-type: none"> <li>○ Assignment: Set up an antivirus scanner (such as ClamAV) and analyze a suspicious file using it.</li> <li>○ Tools: ClamAV, VirusTotal.</li> </ul>
2	Hashing and Finding Strings: <ul style="list-style-type: none"> <li>○ Assignment: Calculate hash values (MD5, SHA-256) for a set of files. Extract strings from a binary.</li> <li>○ Tools: md5sum, sha256sum, strings.</li> </ul>
3	Recognizing C Code Constructs in Assembly: <ul style="list-style-type: none"> <li>○ Assignment: Disassemble x86 code snippets. Identify global vs. local variables, loops, if statements, and function call conventions.</li> <li>○ Tools: IDA Pro, objdump.</li> </ul>
4	Analyzing Malicious Windows Programs: <ul style="list-style-type: none"> <li>○ Assignment: Investigate Windows API calls, registry interactions, and network-related activities in a malware sample.</li> <li>○ Tools: Process Monitor, Process Explorer, Wireshark.</li> </ul>
5	Dynamic Analysis in Virtual Machines: <ul style="list-style-type: none"> <li>○ Assignment: Set up a virtual machine for malware analysis. Understand risks and record/replay techniques.</li> <li>○ Tools: VMware, VirtualBox.</li> </ul>
6	Kernel Debugging with WinDbg: <ul style="list-style-type: none"> <li>○ Assignment: Debug a kernel-mode driver. Analyze memory maps, threads, and exceptions.</li> <li>○ Tools: WinDbg, Driver Verifier.</li> </ul>
7	Advanced Dynamic Analysis with OllyDbg: <ul style="list-style-type: none"> <li>○ Assignment: Load malware in OllyDbg. Explore memory, breakpoints, loading DLLs, and analyzing shellcode.</li> <li>○ Tools: OllyDbg.</li> </ul>
8	Malware Behavior Analysis: <ul style="list-style-type: none"> <li>○ Assignment: Run malware samples and observe their behavior. Understand user vs. kernel mode execution.</li> <li>○ Tools: Procmon, API Monitor.</li> </ul>

9	<p>Anti-Disassembly Techniques:</p> <ul style="list-style-type: none"><li>○ Assignment: Create a simple piece of code (in C/C++ or assembly) that employs anti-disassembly techniques. Use manual crafting to confuse disassembly tools (such as IDA Pro or radare2). For instance, you can insert junk instructions, reorder code, or use obfuscation.</li><li>○ Tools: IDA Pro, radare2.</li></ul>
10	<p>Anti-Virtual Machine Techniques:</p> <ul style="list-style-type: none"><li>○ Assignment: Develop a shellcode that detects if it's running inside a virtual machine (e.g., VMware). Investigate VMWare artifacts (e.g., registry keys, device names) that can be used for detection. Experiment with tweaking VM settings (e.g., CPUID masking) to evade detection.</li><li>○ Tools: VMware, VirtualBox, OllyDbg.</li></ul>



BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	I
Course Name	Research Methodology
Course Code	PMSIT107+PMSIT108P
Type of course	Research Methodology
Level of the Subject	Advanced
Credit points	2 Theory + 2 Practical

**Course Objectives:**

1. To be able to conduct research with an understanding of all the latest theories.
2. To develop the ability to explore research techniques used for solving any real world or innovative problem.

Unit No.	Name of Unit	Content	Hours
1	Introduction to Research	Meaning, Characteristics of Research, Objectives of research	15
		Types of research: Basic Research, Applied Research, Descriptive Research, Analytical Research, Empirical research	
		Ethical issues and Problems in research, Meaning of research methodology, Stages in Scientific Research Process	
		Measurement concepts: Scales of measurement - nominal, ordinal, ratio and interval, Types of measurement scales: comparative scales- Paired Comparison Scale, Rank Order Scale, Q-Sort Scale and non comparative scales- Continuous Rating Scale, Itemized Rating Scale, Likert Scale, Stapel Scale, Semantic Differential Scale.	
2	Sampling Design and Questionnaire Design	Sampling design- meaning and significance, Essentials of good sampling, Stages in sampling design, Sampling errors	15
		Types of Probability sampling- simple random sampling, stratified random sampling, systematic random sampling, and cluster random sampling. Types of non-probability sampling- Convenience sampling, Quota sampling,	

		Self-selection (volunteer) sampling, Snowball sampling, Purposive (judgmental) sampling.	
		Types of data- Primary data and secondary data meaning, significance and limitations, Collection of primary and secondary data	
		Designing of a questionnaire- meaning, stages in questionnaire designing, Essentials of a good questionnaire.	
3	Data Analysis and Presentation:	Determination of sample size, Editing and Coding	15
		Basic Data Analysis Arithmetic Mean, Median, mode, Standard deviation, Correlation, Regression analysis	
		Hypothesis testing for significance, Types of errors in Hypothesis testing	
		Hypothesis testing for significance for mean/s and proportion for large samples, t test for single mean, paired and unpaired means, Chi-Square test. ANOVA-One way and Two way.	
	<b>Total No. of Lectures</b>		<b>45</b>

### Course Outcomes :

1. Create skills to apply appropriate methods to the research in hand
2. Understand aptitude for establishing rapport in the field
3. Analyze knowledge about sampling methods
4. Analyze the ability to scan secondary sources for research
5. Create skills to analyze the quantitative and qualitative data
6. Create knowledge in using statistical tools and techniques

### Reference:

1. Business Research Methods William G.Zikmund, B.J Babin, J.C. Carr, Cengage 8e 2016 Atanu Adhikari, M.Griffin
2. Business Analytics Albright Winston Cengage 5e 2015
3. Research Methodology-Method and Techniques 3e 2014
4. Research Methodology: A Step-by-Step Guide for Beginners" by Ranjit Kumar
5. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches" by John W. Creswell and J. David Creswell

## PRACTICALS

Practical No.	Details
1	Using R execute the basic commands
2	Import the data from Excel / .CSV find mean median mode,standard deviation variance
3	Perform R program for making Diagrams(Bar Diagram,Multiple Bar Diagram,Pie Chart)
4	Perform R program for making Graphs(Histogram,Frequency Polygon,Ogive)
5	Import the data from Excel / .CSV and perform the Chi-square Test,goodness of fit ,Independence of attributes
6	Perform an R program on z-test- one population mean, Two population means.One population proportion,two population proportion.
7	Perform an R program on t test- one sample, paired and unpaired
8	Perform an R program on Non ParametricTest -Sign test, wilcoxon signed rank test
9	Perform an R program on One way ANOVAand Two way ANOVA
10	Perform an R program on Friedman Test and Kruskal Wallis test

# **Semester – II**

BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	II
Course Name	Big Data Analytics
Course Code	PMSIT201
Type of course	Major
Level of the Subject	Advanced
Credit points	4 Theory + 1 Practical

### Course Objectives:

1. To provide an overview of an exciting growing field of big data analytics,
2. To introduce the tools required to manage and analyze big data like Hadoop, NoSql MapReduce.

Unit No.	Name of Unit	Content	Hours
1	<b>Introduction</b>	<p>Introduction to Big Data, Characteristics of Data, and Big Data Evolution of Big Data, Definition of Big Data, Challenges with big data, Why Big data?</p> <p>Big Data, Definition of Big Data, Challenges with big data, Why Big data? Data Warehouse environment, Traditional Business Intelligence versus Big Data. State of Practice in Analytics, Key roles for New Big Data Ecosystems, Examples of big Data Analytics.</p> <p>Big Data Analytics, Introduction to big data analytics, Classification of Analytics, Challenges of Big Data</p> <p>Importance of Big Data, Big Data Technologies, Data Science, Responsibilities, Soft state eventual consistency. Data Analytics Life Cycle</p>	<b>15</b>
2	<b>Analytical Theory and Methods</b>	<p>Analytical Theory and Methods: Clustering and Associated Algorithms, Association Rules, Apriori Algorithm, Candidate Rules</p> <p>Applications of Association Rules, Validation and Testing, Diagnostics, Regression, Linear Regression, Logistic Regression, Additional Regression Models.</p>	<b>15</b>

3	<b>Classification</b>	<p>Analytical Theory and Methods: Classification, Decision Trees, Naïve Bayes, Diagnostics of Classifiers, Additional Classification Methods, Time Series Analysis,</p> <p>Box Jenkins methodology, ARIMA Model, Additional methods. Text Analysis, Steps, Text Analysis Example, Collecting Raw Text, Representing Text, Term Frequency-Inverse</p> <p>Document Frequency (TFIDF), Categorizing Documents by Topics, Determining Sentiments</p>	15
4	<b>Data Product, Building Data:</b>	<p>Data Product, Building Data Products at Scale with Hadoop, Data Science Pipeline and Hadoop Ecosystem,</p> <p>Operating System for Big Data, Concepts, Hadoop Architecture, Working with Distributed file system, Working with Distributed Computation, Framework for Python and Hadoop Streaming, Hadoop Streaming, MapReduce with Python,</p>	15
<b>Total No. of Lectures</b>			<b>60</b>

### Course Outcomes

1. Understand the key issues in big data management and its associated applications in intelligent business and scientific computing.
2. Create fundamental enabling techniques and scalable algorithms like Hadoop, Map Reduce and NO SQL in big data analytics
3. Understand business models and scientific computing paradigms, and apply software tools for big data analytics
4. Analyze Adequate perspectives of big data analytics in various applications like recommender systems, social media applications etc
5. Understand the principles and techniques of time series analysis, including the Box-Jenkins methodology and the ARIMA model
6. Analyze an understanding of the importance of data validation and testing in analytics, particularly in association rules and regression analysis

### References:

1. Big Data and Analytics: Subhashini Chellappan Seema Acharya, First Edition , Wiley
2. Data Analytics with Hadoop An Introduction for Data Scientists by Benjamin Bengfort and Jenny Kim O'Reilly Publisher 2016
3. Big Data Analytics: Turning Big Data into Big Money" by Frank J. Ohlhorst
4. Big Data Analytics: A Practical Guide for Managers" by Kim H. Pries and Robert Dunnigan
5. Big Data Analytics Methods: Concepts, Algorithms, and Applications" edited by Saumyadipta Pyne

## CASE STUDY

SR. NO

### 1 **Big Data Analytics for AMI Data in London**

#### **Background:**

The low carbon London project ran from 2011 to 2014, involving approximately 5,567 households in London. Around 1,100 customers experienced a dynamic time-of-use (dToU) energy price scheme in 2013.

#### **Objectives:**

The primary goal was to understand user consumption patterns in relation to seasonal variables.

#### **Approach:**

##### **1. Data Collection:**

- The study collected smart metering data from participating households.
- These data included energy consumption information.

#### **Big Data Framework:**

- Researchers implemented a big data framework for efficient handling of large-scale data.
- The framework allowed for scalability and real-time processing.

#### **Data Analytics Techniques:**

- Various data analytics techniques were applied to the collected data.
- These techniques aimed to uncover patterns, trends, and correlations.
- Insights and Recommendations:

#### **Analysis of the data revealed:**

- Peak consumption hours during different seasons.
- Energy usage patterns based on weather conditions.
- Behavioral insights related to energy consumption.

#### **Outcomes:**

- The case study demonstrated how big data analytics could:
- Optimize energy pricing based on consumption patterns.
- Inform energy-saving strategies for households.
- Enhance overall energy efficiency in the city.

### 2 **Building Data-Driven Insights for an E-Commerce Platform**

#### **Background**

Our client, an established e-commerce platform, faced challenges in understanding customer behavior, optimizing inventory management, and enhancing personalized recommendations. They wanted to leverage big data analytics to gain deeper insights into their operations and drive business growth.

#### **Objectives**

1. Customer Segmentation: Identify distinct customer segments based on purchasing behavior, demographics, and preferences.
2. Inventory Optimization: Optimize inventory levels to reduce stockouts and

overstock situations.

3. Recommendation Engine Enhancement: Improve product recommendations for users based on their browsing history and purchase patterns.

#### **Approach**

##### **Data Collection and Integration:**

- Gather data from various sources, including transaction records, website logs, and customer profiles.
- Integrated data into a centralized data lake for further analysis.

##### **Exploratory Data Analysis (EDA):**

- Explored data to understand patterns, missing values, and outliers.
- Conducted statistical analyses to identify correlations and trends.

##### **Customer Segmentation:**

- Utilized clustering algorithms (e.g., k-means) to group customers based on their behavior.
- Segmented customers into categories such as “loyal,” “occasional,” and “new.”

##### **Inventory Optimization:**

- Developed predictive models to forecast demand for different products.
- Used inventory turnover ratios to determine optimal stock levels.

##### **Recommendation Engine Enhancement:**

- Implemented collaborative filtering techniques to personalize product recommendations.
- Considered user-item interactions and similarity scores.

#### **Results**

##### **Customer Segmentation:**

- Identified five customer segments: “Tech Enthusiasts,” “Budget Shoppers,” “Fashionistas,” “Occasional Buyers,” and “Gift Seekers.”
- Tailored marketing campaigns and promotions for each segment.

##### **Inventory Optimization:**

- Reduced excess inventory by 20% and stockouts by 15%.
- Improved overall supply chain efficiency.

##### **Recommendation Engine Enhancement:**

- Increased click-through rates by 10%.
- Enhanced user satisfaction and engagement.

## **PRACTICALS**

<b>Practical No.</b>	<b>Details</b>
1	Install, configure and run Hadoop and HDFS and explore HDFS
2	Implement word count / frequency programs using MapReduce
3	Implement an MapReduce program that processes a weather dataset.
4	Implement an application that stores big data in Hbase / MongoDB and manipulate it using R / Python



5	Implement the program in practical 4 using Pig.
6	Configure the Hive and implement the application in Hive.
7	Write a program to illustrate the working of Jaql.
8	Implement the following: a. Implement Decision tree classification techniques b. Implement SVM classification techniques
9	Solve the following: a. REGRESSION MODEL Import a data from web storage. Name the dataset and now do Logistic Regression to find out relation between variables that are affecting the admission of a student in an institute based on his or her GRE score, GPA obtained and rank of the student. Also check the model is fit or not. require (foreign), require(MASS). MULTIPLE REGRESSION MODEL Apply multiple regressions, if data have a continuous independent variable. Apply on above dataset.
10	Solve the Following: CLASSIFICATION MODEL a. Install relevant package for classification. b. Choose classifier for classification problem. c. Evaluate the performance of classifier. CLUSTERING MODEL a. Clustering algorithms for unsupervised classification. b. Plot the cluster data using R visualizations

BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	II
Course Name	Microservices Architecture
Course Code	PMSIT202
Type of course	Major
Level of the Subject	Advanced
Credit points	4 Theory + 1 Practical

**Course Objectives:**

1. Gain a thorough understanding of the philosophy and architecture of Web applications using ASP.NET Core MVC;
2. Gain a practical understanding of .NET Core

Unit No.	Name of Unit	Content	Hours
1	<b>Microservices</b>	Microservices: Understanding Microservices, Adopting Microservices, The Microservices Way. Microservices Value Proposition: Deriving Business Value, defining a Goal-Oriented, Layered Approach, Applying the Goal-Oriented, Layered Approach. Designing Microservice Systems: The Systems Approach to Microservices, A Microservices Design Process, Establishing a Foundation: Goals and Principles, Platforms, Culture.	15
2	<b>Service Design</b>	Service Design: Microservice Boundaries, API design for Microservices, Data and Microservices, Distributed Transactions and Sagas, Asynchronous Message-Passing and Microservices, dealing with Dependencies, System Design and Operations: Independent Deployability, More Servers, Docker and Microservices, Role of Service Discovery, Need for an API Gateway, Monitoring and Alerting.  Adopting Microservices in Practice: Solution Architecture Guidance, Organizational Guidance, Culture Guidance, Tools and Process Guidance, Services Guidance.	15

3	<b>Building Microservices with ASP.NET Core</b>	<p>Building Microservices with ASP.NET Core: Introduction, Installing .NET Core, Building a Console App, Building ASP.NET Core App.</p> <p>Delivering Continuously: Introduction to Docker, Continuous integration with Wercker, Continuous Integration with Circle CI, Deploying to Dicker Hub.</p> <p>Building Microservice with ASP.NET Core: Microservice, Team Service, API First Development, Test First Controller, Creating a CI pipeline, Integration Testing, Running the team service Docker Image. Backing Services:</p> <p>Microservices Ecosystems, Building the location Service, Enhancing Team Service.</p>	15
4	<b>Creating Data Service</b>	<p>Creating Data Service: Choosing a Data Store, Building a Postgres Repository, Databases are Backing Services, Integration Testing Real Repositories, Exercise the Data Service.Event Sourcing and CQRS: Event Sourcing, CQRS pattern, Event Sourcing and CQRS, Running the samples.</p> <p>Building an Microservices Application with Spring Boot: Spring Boot Core Basics, Building Cloud-Native Web Applications. Service Discovery: Cloud Native Factors, Netflix Eureka, Discovering and Advertising Web Services. DNS and Platform Supported Discovery.</p> <p>Configuring Microservice Ecosystems: Using Environment Variables with Docker, Using Spring Cloud Config Server, Configuring Microservices with etcd, Securing Applications and Microservices: Security in the Cloud, Securing ASP.NET Core Web Apps, Securing ASP.NET Core Microservices. Building Real-Time Apps and Services: Real-Time Applications Defined, Websockets in the Cloud, Using a Cloud Messaging Provider, Building the Proximity Monitor.</p>	15
<b>Total No. of Lectures</b>			<b>60</b>

### Course Outcomes

1. Remember web applications using Model View Control.
2. Create MVC Models and write code that implements business logic within Model methods, properties, and events.
3. Create Views in an MVC application that display and edit data and interact with Models and Controllers.
4. Analyze your hire ability through innovative and independent learning.
5. Evaluate a thorough understanding of the philosophy and architecture of .NET Core.
6. Understanding packages, metapackages and frameworks Acquiring a working knowledge of the .NET programming model Implementing multi-threading effectively in .NET applications

**References:**

1. Building Microservices" by Sam Newman:
2. Microservices Patterns: With examples in Java" by Chris Richardson
3. Monolith to Microservices: Evolutionary Patterns to Transform Your Monolith" by Sam Newman
4. Production-Ready Microservices: Building Standardized Systems Across an Engineering Organization" by Susan
5. Implementing Microservices: The Migration from Monolithic Architectures and Monolithic Culture to Microservices" by Boris Scholl, Gang Chen, and Gary Brown

<b>CASE STUDY</b>	
<b>SR. NO</b>	
<b>1</b>	<p><b>Background</b></p> <p>Uber, the ride-hailing giant, faced significant challenges as it scaled globally. Their initial monolithic architecture struggled to handle the increasing user base, frequent deployments, and fault tolerance. To address these issues, Uber adopted a microservices architecture around 2012-2013.</p> <p><b>Key Decisions and Implementation</b></p> <ol style="list-style-type: none"> <li>1. Decomposition: Uber broke down their monolith into thousands of microservices, each responsible for a specific business domain (e.g., payments, ride requests, driver management).</li> <li>2. Independently Deployable Services: Microservices allowed Uber to deploy individual services independently. This flexibility improved development speed and reduced the risk of system-wide failures.</li> <li>3. Fault Isolation: With microservices, a failure in one service doesn't impact others. This isolation enhances system reliability.</li> <li>4. Communication: Uber's microservices communicate over RPC (Remote Procedure Call). They use tools like Jaeger for tracing transactions between services.</li> <li>5. API Gateway: An entry point for external requests, the API gateway routes them to the appropriate microservices.</li> <li>6. Service Discovery: Mechanisms help locate and connect to microservices dynamically.</li> </ol>
<b>2</b>	<p><b>A Decade of Microservices at a Financial Firm</b></p> <p><b>Background</b></p> <p>Our case study focuses on a financial institution that transitioned from a monolithic architecture to a microservices-based approach. Here are the key highlights:</p> <ol style="list-style-type: none"> <li>1. Initial Challenges: The firm faced challenges with their monolithic system, including inflexibility, slow deployments, and maintenance difficulties.</li> <li>2. Adoption of Microservices: Around a decade ago, they decided to embrace microservices to address these issues and enhance their overall system architecture.</li> </ol> <p><b>Key Decisions and Implementation</b></p>

	<ol style="list-style-type: none"> <li>1. Decomposition: The firm meticulously dissected their monolith into smaller, independent microservices. Each service catered to a specific business domain (e.g., account management, transaction processing, risk assessment).</li> <li>2. Independent Deployability: Microservices allowed them to deploy individual services without affecting the entire system. This agility improved their development speed.</li> <li>3. Scalability: As the firm grew, microservices facilitated seamless scaling. They could add or modify services as needed.</li> <li>4. Fault Isolation: Failures in one microservice didn't cascade to others, ensuring system reliability.</li> <li>5. Communication: They employed RESTful APIs and asynchronous messaging for inter-service communication.</li> </ol>
--	--

<b>PRACTICALS</b>	
Practical No	Details
1	Building APT.NET Core MVC Application
2	Building ASP.NET Core REST API.
3	Working with Docker, Docker Commands, Docker Images and Containers
4	Installing software packages on Docker, Working with Docker Volumes and Networks.
5	Working with Docker Swarm
6	Working with Circle CI for continuous integration.
7	Creating Microservice with ASP.NET Core.
8	Working with Kubernetes
9	Creating Backing Service with ASP.NET Core.
10	Building real-time Microservice with ASP.NET Core

BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	II
Course Name	Advanced IOT
Course Code	PMSIT203
Type of course	Major
Level of the Subject	Advanced
Credit points	4 Theory + 1 Practical

**Course Objectives:**

1. To understand the latest developments in IoT
2. To build smart IoT applications

Unit No.	Name of Unit	Content	Hours
1	<b>The Intersection of Artificial Intelligence and IoT</b>	The Artificial Intelligence IoT and Azure IoT Suite Creating Smart IoT Application	15
2	<b>Building Smart Applications with Cognitive APIs</b>	Cognitive APIs, Consuming Microsoft Cognitive APIs Building Smarter Application using Cognitive APIs	15
3	<b>Next-Generation Solutions</b>	Implementing Blockchain as a service, Capturing, Analysing and Visualizing real-time data, Making prediction with machine learning. IoT and Microservices, Service Fabric, Build your own IoT platform: Introduction, Building blocks for IoT solution, Essentials for building your own platform	15
4	<b>IoT Platform Development</b>	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. Building Critical components, configuring message broker, creating REST interface, Rule engine and authentication, documentation and testing, Introspection on what we build and deliverables.	15
<b>Total No. of Lectures</b>			<b>60</b>

## Course Outcomes:

1. Create smart IoT applications on Azure.
2. Understand Microsoft cognitive APIs to build IoT applications
3. Evaluate Blockchain in IoT.
4. Understand and use microservices in IoT
5. Create your own IoT platform and use it in a customized way
6. Understand, initialize and configure cloud instances, install software stacks, and ensure the security of the platform.

## References:

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. Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry" by Maciej Kranz
5. Hands-On Industrial Internet of Things: Create a powerful Industrial IoT infrastructure using Industry 4.0" by Giacomo Veneri:

CASE STUDY	
SR. NO	
1	<p>Uber's IoT Implementation: A Case Study</p> <p>Background</p> <p>Uber, the global ride-hailing giant, has effectively leveraged IoT technologies to enhance its services, improve efficiency, and provide a seamless experience for both riders and drivers.</p> <p>Key IoT Applications in Uber's Ecosystem</p> <ol style="list-style-type: none"><li>1. Real-Time Location Tracking:<ul style="list-style-type: none"><li>○ Uber relies heavily on GPS-enabled devices to track the real-time location of drivers and riders.</li><li>○ IoT-enabled smartphones and in-car devices communicate with Uber's central servers, allowing precise location updates.</li><li>○ This tracking ensures efficient matching of riders with nearby drivers.</li></ul></li><li>2. Fleet Management:<ul style="list-style-type: none"><li>○ Uber manages a vast fleet of vehicles worldwide. IoT plays a crucial role in fleet management.</li><li>○ Sensors in vehicles monitor fuel levels, engine health, tire pressure, and other critical parameters.</li><li>○ Predictive maintenance alerts help prevent breakdowns and optimize vehicle availability.</li></ul></li><li>3. Driver Behavior Monitoring:<ul style="list-style-type: none"><li>○ IoT devices collect data on driver behavior, such as acceleration, braking,</li></ul></li></ol>

	<p>and speed.</p> <ul style="list-style-type: none"> <li>○ Uber uses this information to encourage safe driving practices and improve overall safety.</li> </ul> <p>4. Dynamic Pricing and Demand Prediction:</p> <ul style="list-style-type: none"> <li>○ IoT data, combined with historical ride patterns, helps Uber predict demand in specific areas.</li> <li>○ Surge pricing adjusts fares based on real-time demand, optimizing revenue and rider allocation.</li> </ul> <p>5. Smart Traffic Management:</p> <ul style="list-style-type: none"> <li>○ Uber collaborates with city authorities to improve traffic flow using IoT data.</li> <li>○ Real-time traffic updates guide drivers to avoid congested routes, reducing travel time.</li> </ul>
2	<p>IoT in Smart Cities: A Case Study</p> <p>Background</p> <p>Smart cities leverage IoT technologies to enhance urban living, improve sustainability, and optimize resource utilization. One notable example is the city of Barcelona, Spain.</p> <p><b>Barcelona’s Smart City Initiatives</b></p> <ol style="list-style-type: none"> <li><b>1. Smart Traffic Management:</b> <ul style="list-style-type: none"> <li>○ Barcelona implemented an intelligent traffic management system using IoT sensors.</li> <li>○ Real-time data from traffic lights, cameras, and road sensors help optimize traffic flow.</li> <li>○ Adaptive traffic signals adjust timings based on congestion, reducing travel time and emissions.</li> </ul> </li> <li><b>2. Waste Management:</b> <ul style="list-style-type: none"> <li>○ IoT-enabled waste bins detect their fill levels.</li> <li>○ Garbage trucks receive real-time alerts, optimizing collection routes.</li> <li>○ This reduces unnecessary trips, saves fuel, and keeps the city cleaner.</li> </ul> </li> <li><b>3. Smart Lighting:</b> <ul style="list-style-type: none"> <li>○ Barcelona uses connected streetlights with motion sensors.</li> <li>○ Lights brighten when pedestrians or vehicles approach and dim when not needed.</li> <li>○ Energy savings and improved safety result from this smart lighting system.</li> </ul> </li> <li><b>4. Environmental Monitoring:</b> <ul style="list-style-type: none"> <li>○ IoT sensors measure air quality, noise levels, and temperature.</li> <li>○ Citizens access real-time environmental data through mobile apps.</li> <li>○ This promotes awareness and informs policy decisions.</li> </ul> </li> </ol>

<b>Practicals</b>	
<b>Practical No</b>	<b>Details</b>
1	Loading Raspbian and Windows IoT Core on Raspberry Pi and executing



2	applications on it using Python and node.js.
3	Create a home automation system and control the devices remotely.
4	Create the programs using the Microsoft Cognitive APIs for IoT.
5	Create blockchain on Raspberry Pi and implement and test it. Authenticate IoT with blockchain.
6	Implement Microservices on IoT device.
7	Build your own IoT platform.
8	Use IoT device with AWS.
9	Send telemetry from a device to an IoT hub and read it with a service application.
10.	Use the Azure CLI and Azure portal to configure IoT Hub message routing.

BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	II
Course Name	Modern Networking
Course Code	PMSIT204
Type of course	Major Elective
Level of the Subject	Advanced
Credit points	2 Theory + 1 Practical

### Course Objectives:

1. To understand the state-of-the-art in network protocols, architectures and applications & Analyze existing network protocols and networks.
2. To investigate novel ideas in the area of Networking via term-long research projects.

Unit No.	Name of Unit	Content	Hours
1	Elements of Modern Networking	Modern Networking Elements of Modern Networking The Networking Ecosystem ,Example Network Architectures,Global Network Architecture,A Typical Network Hierarchy Ethernet Applications of Ethernet Standards Ethernet Data Rates Wi-Fi Applications of Wi-Fi,Standards Wi-Fi Data Rates 4G/5G Cellular First Generation Second Generation, Third Generation Fourth Generation Fifth Generation, Cloud Computing Cloud Computing Concepts The Benefits of Cloud Computing Cloud Networking Cloud Storage, Internet of Things Things on the Internet of Things, Evolution Layers of the Internet of Things,	10
		Network Convergence Unified Communications, Requirements and Technology Types of Network and Internet Traffic,Elastic Traffic,Inelastic Traffic, Real-Time Traffic Characteristics Demand: Big Data, Cloud Computing, and Mobile	
		TrafficBig Data Cloud Computing,,Mobile Traffic, Requirements: QoS and QoE,,Quality of Service,Quality of Experience, Routing Characteristics, Packet Forwarding, Congestion Control ,Effects of Congestion,Congestion Control Techniques, SDN and NFV Software-Defined Networking,Network Functions Virtualization	

		Modern Networking Elements	
2	Software Defined Networks	<p>Software-Defined Networks SDN: Background and Motivation, Evolving Network Requirements Demand Is Increasing, Supply Is Increasing Traffic</p> <p>Patterns Are More Complex Traditional Network Architectures are Inadequate,</p> <p>The SDN Approach Requirements SDN Architecture Characteristics of Software Defined Networking, SDN- and NFV-Related Standards Standards- Developing Organizations Industry Consortia Open Development Initiatives, SDN Data Plane and OpenFlow SDN Data Plane, Data Plane Functions Data Plane Protocols OpenFlow Logical Network Device Flow Table Structure Flow Table Pipeline, The Use of Multiple Tables Group Table OpenFlow Protocol, SDN Control Plane SDN Control Plane Architecture Control Plane Functions, Southbound Interface Northbound Interface Routing, ITU-T Model, OpenDaylight OpenDaylight Architecture OpenDaylight Helium, REST REST Constraints Example REST API</p>	10
3	Virtualization & Network Functions Virtualization	<p>Virtualization, Network Functions Virtualization: Concepts and Architecture, Background and Motivation for NFV, Virtual Machines The Virtual Machine Monitor, Architectural Approaches Container Virtualization, NFV Concepts Simple Example of the Use of NFV, NFV Principles High-Level NFV Framework, NFV Benefits and Requirements NFV Benefits, NFV Requirements, NFV Reference Architecture NFV Management and Orchestration, Reference Points Implementation, NFV Functionality, NFV Infrastructure, Container Interface, Deployment of NFVI Containers, Logical Structure of NFVI Domains, Compute Domain, Hypervisor Domain, Infrastructure Network Domain, Virtualized Network Functions,</p> <p>VNF Interfaces, VNFC to VNFC Communication, VNF Scaling, NFV Management and Orchestration, Virtualized Infrastructure Manager, Virtual Network Function Manager, NFV Orchestrator, Repositories, Element Management, OSS/BSS, NFV Use Cases Architectural Use Cases, Service-Oriented Use Cases, SDN and NFV Network Virtualization, Virtual LANs ,The Use of Virtual LANs, Defining VLANs, Communicating VLAN Membership, IEEE</p> <p>802.1Q VLAN Standard, Nested VLANs, OpenFlow VLAN Support, Virtual Private Networks, IPsec VPNs, MPLS VPNs, Network Virtualization, Simplified Example, Network Virtualization Architecture, Benefits of Network Virtualization, OpenDaylight's Virtual Tenant Network,</p>	10

		Software-Defined Infrastructure, Software-Defined Storage, SDI Architecture	
4	Quality of Service	<p>Defining and Supporting User Needs, Quality of Service, Background, QoS Architectural Framework, Data Plane, Control Plane, Management Plane, Integrated Services Architecture, ISA Approach ISA Components, ISA Services, Queuing Discipline, Differentiated Services, Services, DiffServ Field, DiffServ Configuration and Operation, Per-Hop Behavior, Default Forwarding PHB, Service Level Agreements, IP Performance Metrics, OpenFlow QoS Support, Queue Structures, Meters, QoE: User Quality of Experience, Why QoE?, Online Video Content Delivery, Service Failures Due to Inadequate QoE Considerations QoE-Related Standardization Projects, Definition of Quality of Experience, Definition of Quality, Definition of Experience Quality Formation Process, Definition of Quality of Experience, QoE Strategies in Practice, The QoE/QoS Layered Model Summarizing and Merging the ,QoE/QoS Layers, Factors Influencing QoE, Measurements of QoE, Subjective Assessment, Objective Assessment, End-User Device Analytics</p> <p>Summarizing the QoE Measurement Methods, Applications of QoE Network Design Implications of QoS and QoE Classification of QoE/ QoS Mapping Models, Black-Box Media-Based QoS/QoE Mapping Models, Glass-Box Parameter-Based QoS/QoE Mapping Models, Gray-Box QoS/QoE Mapping Models, Tips for QoS/QoE Mapping Model Selection, IP- Oriented Parameter-Based QoS/QoE Mapping Models, Network Layer QoE/QoS Mapping Models for Video Services, Application Layer QoE/QoS Mapping Models for Video Services Actionable QoE over IP-Based Networks, The System-Oriented Actionable QoE Solution, The Service-Oriented Actionable QoE Solution, QoE Versus QoS Service Monitoring, QoS Monitoring Solutions, QoE Monitoring Solutions, QoE-Based Network and Service Management, QoE-Based Management of VoIP Calls, QoE-Based Host-Centric Vertical Handover, QoE-Based Network-Centric Vertical Handover</p> <p>Modern Network Architecture: Clouds and Fog, Cloud Computing, Basic Concepts, Cloud Services, Software as a Service, Platform as a Service, Infrastructure as a Service, Other Cloud Services, XaaS, Cloud Deployment Models, Public Cloud Private Cloud Community Cloud, Hybrid Cloud, Cloud Architecture, NIST Cloud Computing Reference Architecture, ITU-T Cloud Computing Reference Architecture, SDN and NFV, Service Provider Perspective Private Cloud Perspective, ITU-T Cloud Computing Functional Reference Architecture, The Internet of Things: Components The IoT Era Begins, The Scope of the Internet of Things</p>	10

		Components of IoT-Enabled Things, Sensors, Actuators, Microcontrollers, Transceivers, RFID, The Internet of Things: Architecture and Implementation, IoT Architecture, ITU-T IoT Reference Model, IoT World Forum Reference Model, IoT Implementation, IoTivity, Cisco IoT System, ioBridge, Security Security Requirements, SDN Security Threats to SDN, Software-Defined Security, NFV Security, Attack Surfaces, ETSI Security Perspective, Security Techniques, Cloud Security, Security Issues and	
<b>Total No. of Lectures</b>			40

### Course Outcomes:

1. Understanding the elements of modern networking.
2. Remember in-depth knowledge in the area of Computer Networking to work with software defined networks.
3. Analyze between virtualization and software network virtualization.
4. Understand the architecture of modern networking.
5. Remember scholarship of knowledge through performing in a group to identify, formulate and solve a problem related to Computer Networks
6. Create a technical document for the identified Networking System Conducting experiments to analyze the identified research work in building Computer Networks

### References:

1. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud William Stallings AddisonWesley Professional October 2015
2. SDN and NFV Simplified A Visual Guide to Understanding Software Defined Networks and Network Function Virtualization Jim Doherty Pearson Education, Inc
3. Network Functions Virtualization (NFV) with a Touch of SDN Rajendra Chayapathi Syed Farrukh Hassan AddisonWesley
4. CCIE and CCDE Evolving Technologies Study Guide Brad dgeworth, Jason Gooley, Ramiro Garza Rios Pearson Education, Inc 2019
5. Computer Networking: A Top-Down Approach" by James F. Kurose and Keith W. Ross

<b>CASE STUDY</b>	
<b>SR. NO</b>	
<b>1</b>	<p><b>Cisco Digital Network Architecture (Cisco DNA)</b></p> <p>Business Context:</p> <p>In today's fast-paced digital landscape, organizations face the challenge of adapting their networks to meet evolving business needs. Traditional networks struggle to keep up with the demands of mobility, security, and scalability. Cisco recognized this and introduced the Cisco Digital Network Architecture (Cisco DNA) as a solution.</p> <p>Solution Overview:</p> <p>Cisco DNA is a comprehensive framework that combines software-defined networking</p>

(SDN), automation, security, and analytics. It aims to transform the way networks are designed, deployed, and managed. Here are the key components:

1. Software-Defined Access (SD-Access):
  - Simplifies network segmentation, policy enforcement, and provisioning.
  - Enables dynamic policy-based network access.
  - Provides centralized management through Cisco DNA Center.
2. Software-Defined WAN (SD-WAN):
  - Optimizes wide area network connectivity.
  - Enhances application performance by intelligently routing traffic.
  - Simplifies branch office deployments.
3. Wi-Fi 6 (802.11ax):
  - Delivers faster speeds, increased capacity, and improved efficiency.
  - Supports IoT devices and high-density environments.

### Networking Success Stories

In the digital age, networking—both online and offline—is crucial for professional growth. Companies worldwide have harnessed the power of networking to achieve remarkable success. Here are some inspiring case studies:

**Epic Games:** The gaming giant Epic Games leveraged its extensive network to drive innovation. By collaborating with other game developers, artists, and industry experts, they created groundbreaking games like Fortnite. Networking allowed them to access fresh ideas, talent, and partnerships.

**Salesforce:** Salesforce, a leading customer relationship management (CRM) platform, owes much of its success to networking. Their annual events, such as Dreamforce, bring together professionals, customers, and partners. These connections foster knowledge exchange, product enhancements, and business growth.

**Scuderia Ferrari:** The iconic Formula 1 racing team Scuderia Ferrari thrives on networking. Their global network of engineers, sponsors, and fans contributes to their continuous improvement. By collaborating with suppliers and competitors, they stay at the forefront of racing technology.

**NatWest Bank:** NatWest Bank transformed its customer experience through networking. By connecting with fintech startups, they embraced digital innovations. Their partnerships led to streamlined services, personalized banking, and enhanced security measures.

## Practicals

Practical No	Details
1.	Configure IP SLA Tracking and Path Control Topology
2.	Using the AS_PATH Attribute
3.	Configuring IBGP and EBGP Sessions, Local Preference, and MED
4.	Secure the Management Plane
5.	Configure and Verify Path Control Using PBR

<b>6.</b>	IP Service Level Agreements and Remote SPAN in a Campus Environment
<b>7.</b>	Inter-VLAN Routing
<b>8.</b>	Simulating MPLS environment
<b>9.</b>	Simulating VRF
<b>10.</b>	Simulating SDN with OpenDaylight SDN Controller with the Mininet Network Emulator . OFNet SDN network emulator

BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	II
Course Name	Information Security Auditing
Course Code	PMSIT204
Type of course	Major Elective
Level of the Subject	Advanced
Credit points	2 Theory + 1 Practical

### Course Objectives:

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

Unit No.	Unit Name	Content	Hours
1	Basic of Auditing	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, Understanding the Corporate Organizational Structure Governance, Strategy Planning for Organizational Control , Overview of Tactical Management Planning and Performance, Overview of Business Process Reengineering Operations Management Summary , Audit Process Understanding the Audit Program Establishing and Approving an Audit Charter, Preplanning Specific Audits Performing an Audit Risk Assessment ,	10
2	Working with Auditing	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)  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	10



		System Migration, Infrastructure Deployment and Data Conversion, Post-implementation Review,	
3	End- User Computing Data Governance & Disaster Recovery	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 Information Systems Life Cycle ,Governance in Software Development ,Management of Software Quality, Overview of the Executive Steering Committee Change Management,	10
4	Software Project Management	Management of the Software Project ,Overview of the System Development Life Cycle Overview 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  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 Disaster Recovery 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	10
<b>Total No. of Lectures</b>			<b>40</b>

### Course Outcomes:

After completion of the course, a student should be able to:

1. Understand various information security policies and process flow, Ethics of an Information security Auditor.
2. Understand various information systems in an organization, their criticality and various governance and management policies associated with them.
3. Critically analyze various operational strategies like asset management, data governance etc.
4. Suggest requisite changes as per organizations requirements with improvements.

5. Understand the information flow across the organization and identify the weak spots, and also suggest improvements to strengthen them.
6. Come up with strong strategies to protect information assets and come up with an efficient business continuity plan, disaster recovery strategy etc.

**References:**

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
4. IT Auditing: Using Controls to Protect Information Assets" by Chris Davis, Mike Schiller, and Kevin Wheeler:
5. The Basics of Information Security Auditing: A Simple Introduction" by Brian J. Bartlett

<b>CASE STUDY</b>	
<b>1.</b>	<p><b>Practices in Indian IT Organizations</b></p> <p><b>Introduction</b>            In recent years, information security has gained significant attention across diverse businesses and sectors. The rapid adoption of new and innovative ways of handling information (during generation, processing, storage, and distribution) has made organizations agile. Simultaneously, it has posed new challenges. This case study explores and examines the information security management (ISM) practices of two IT development and services organizations in India.</p> <p><b>Methodology</b>            Qualitative Research: The study adopts a qualitative research approach, using semi-structured interviews to understand the current ISM practices of the case organizations.            Descriptive Analysis: Observations from the interviews are analyzed descriptively.            SAP-LAP Method: The Situation, Actor, Process—Learning, Action, Performance (SAP-LAP) method of inquiry is used to analyze the findings.</p>
<b>2.</b>	<p><b>Security Audit in a Medium-Sized Organization</b></p> <p><b>Introduction</b>            In this case study, we delve into the basics of an information systems security audit conducted on a medium-sized organization. The audit served as a security baseline for future assessments. Let’s explore the key aspects:</p> <p><b>Background</b>            Organization: A medium-sized company operating in the technology sector.            Objective: To evaluate the organization’s information security practices and identify vulnerabilities.</p> <p><b>Methodology</b>            Audit Scope Definition: The audit team defined the scope, including critical systems, networks, and data repositories.            Risk Assessment: Identified potential risks and threats.            Audit Execution:            Technical Assessment: Reviewed network configurations, access controls, and system logs.            Policy Compliance: Assessed adherence to security policies and standards.            Vulnerability Scanning: Conducted vulnerability scans on servers and applications.</p> <p><b>Findings and Recommendations:</b>            Discovered vulnerabilities (e.g., outdated software, weak passwords).            Recommended remediation steps.</p>

## Practicals

Practical No	Details
1.	<p>Pre-Audit Checklist Creation:</p> <ul style="list-style-type: none"> <li>○ Develop a comprehensive pre-audit checklist covering aspects such as information gathering, risk assessment, and compliance requirements.</li> </ul>
2.	<p>Understanding Professional Ethics:</p> <ul style="list-style-type: none"> <li>○ Research and analyze professional ethics codes relevant to information security auditing (e.g., ISACA's Code of Professional Ethics).</li> <li>○ Create a presentation or report highlighting key ethical principles.</li> </ul>
3.	<p>Audit Program Development:</p> <ul style="list-style-type: none"> <li>○ Design an audit program for a specific organizational process (e.g., financial transactions, access controls).</li> <li>○ Specify audit objectives, scope, procedures, and resources required.</li> </ul>
4.	<p>Risk Assessment Simulation:</p> <ul style="list-style-type: none"> <li>○ Simulate a risk assessment for an IT system or project.</li> <li>○ Identify potential risks, assess their impact, and prioritize them.</li> <li>○ Propose risk mitigation strategies.</li> </ul>
5.	<p>Audit Evidence Gathering:</p> <ul style="list-style-type: none"> <li>○ Select a real-world organization or system.</li> <li>○ Collect audit evidence (e.g., logs, policies, interviews).</li> <li>○ Document findings and observations.</li> </ul>
6.	<p>Business Continuity and Disaster Recovery Planning Review:</p> <ul style="list-style-type: none"> <li>○ Evaluate an organization's business continuity and disaster recovery plans.</li> <li>○ Identify gaps or areas for improvement.</li> <li>○ Provide recommendations.</li> </ul>
7.	<p>Security Controls Assessment:</p> <ul style="list-style-type: none"> <li>○ Choose a specific security control (e.g., access control, encryption).</li> <li>○ Assess its effectiveness within an organization.</li> <li>○ Propose enhancements or adjustments..</li> </ul>
8.	<p>Post-implementation Review:</p> <ul style="list-style-type: none"> <li>○ Analyze the success of an implemented system or project.</li> <li>○ Assess whether it meets its intended goals.</li> <li>○ Identify any deviations from the original plan.</li> </ul>
9.	<p>Change Management Audit:</p> <ul style="list-style-type: none"> <li>○ Investigate an organization's change management processes.</li> <li>○ Evaluate change request handling, approvals, and documentation.</li> <li>○ Suggest improvements.</li> </ul>
10.	<p>Database Management Security Assessment:</p> <ul style="list-style-type: none"> <li>○ Focus on database security (e.g., user access, encryption, backups).</li> <li>○ Assess the security posture of a database system.</li> <li>○ Generate a report with findings and recommendations..</li> </ul>

BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	II
Course Name	Network Security & Cryptography
Course Code	PMSIT204
Type of course	Major Elective
Level of the Subject	Advanced
Credit points	2 Theory + 1 Practical

**Course Objectives:**

1. Discuss the fundamental ideas of cryptographic algorithms, public-key cryptography, enhancements made to IPv4 by IPSec
2. Generate and distribute a PGP key pair and use the PGP package to send an encrypted email message.

Unit No.	Unit Name	Content	Hours
1	Basic of Security.	Security Concepts: Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms, A model for Network Security Cryptography Concepts and Techniques: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks	10
2	Symmetric & Asymmetric Cryptography	Symmetric key Ciphers: Block Cipher principles, DES, AES, Blowfish, RC5, IDEA, Block cipher operation, Stream ciphers, RC4. Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Elgamal Cryptography, Diffie-Hellman Key Exchange, Knapsack Algorithm. Cryptographic Hash Functions: Message Authentication, Secure Hash Algorithm (SHA-512), Message authentication codes: Authentication requirements, HMAC, CMAC, Digital signatures, Elgamal Digital Signature Scheme. Key	10
3	Management & Distribution of key , Transport level security	Management and Distribution: Symmetric Key Distribution Using Symmetric & Asymmetric Encryption, Distribution of Public Keys, Kerberos, X.509 Authentication Service, Public – Key Infrastructure  Transport-level Security: Web security considerations, Secure Socket Layer and Transport Layer Security, HTTPS, Secure Shell (SSH) Wireless Network Security: Wireless	10

		Security, Mobile Device Security, IEEE 802.11 Wireless LAN, IEEE 802.11i Wireless LAN Security	
4	Security in Email & Case studies	<p><b>AI in Network Security :</b> Applications of AI in NS , Challenge to work with AI</p> <p><b>AI in Cryptography:</b> Applications , Challenges, Neural Cryptography , Neural key exchange protocol and its working. Case study on Key generation process with AI, Secure Inter-branch Payment Transactions</p>	10
<b>Total No. of Lectures</b>			<b>40</b>

### Course Outcomes:

1. Understand basic cryptographic algorithms, message and web authentication and security issues.
2. Understand the basic categories of threats to computers and networks
3. Analyze between Symmetric & Asymmetric cryptography algorithms.
4. Analyze to identify information system requirements for both of them such as client and server.
5. Analyze to understand the current legal issues towards information security.
6. Understand various security like email security, transport security etc.

### References:

1. Cryptography and Network Security - Principles and Practice: William Stallings, Pearson Education, 6th Edition
2. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 3rd Edition
3. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.
4. Cryptography and Network Security: Forouzan Mukhopadhyay, Mc Graw Hill, 3rd Edition
5. Information Security, Principles, and Practice: Mark Stamp, Wiley India.
6. Principles of Computer Security: WM. Arthur Conklin, Greg White, TMH

<b>CASE STUDY</b>	
<b>SR. NO</b>	
<b>1</b>	<p>IP Security (IPsec) Background IP Security (IPsec) is a suite of protocols designed to provide confidentiality, integrity, and authentication for IP packets. It ensures secure communication over IP-based networks, such as the internet.</p> <p>Historical Development Origins: IPsec emerged in the 1990s as a response to the growing need for secure communication in the digital age.</p> <p>Standardization: The Internet Engineering Task Force (IETF) standardized IPsec, making it widely adopted.</p>

	<p>Major Goals</p> <p>Confidentiality: Protect data from unauthorized access by encrypting it.</p> <p>Integrity: Ensure data integrity by detecting any unauthorized modifications.</p> <p>Authentication: Verify the identity of communication peers.</p> <p>Key Components</p> <p>Authentication Header (AH): Provides integrity and authentication.</p> <p>Encapsulating Security Payload (ESP): Offers confidentiality, integrity, and optional authentication.</p> <p>Security Associations (SAs): Define security parameters for communication.</p> <p>Protocols and Procedures</p> <p>IKE (Internet Key Exchange): Establishes secure communication channels by negotiating cryptographic keys.</p> <p>Diffie-Hellman Key Exchange: Used within IKE to securely exchange keys.</p> <p>AES (Advanced Encryption Standard): Commonly used for encryption.</p> <p>SHA (Secure Hash Algorithm): Ensures data integrity.</p>
2	<p>Kerberoasting is an attack vector aimed at the Kerberos authentication protocol. Kerberos is a type of network authentication protocol that allows a client and server to conduct mutual verification before providing requested resources to the client. In a successful Kerberoasting attack, an adversary leverages the architectural limitations of Kerberos to gain access to user password hashes. These hashes can then be subjected to offline cracking, potentially revealing user passwords.</p> <p>Attack Scenario</p> <p>Objective: Obtain user password hashes.</p> <p>Method: Exploit the way Kerberos handles service tickets.</p> <p>Process:</p> <p>The adversary identifies service accounts (such as Active Directory service accounts) that use Kerberos for authentication.</p> <p>The adversary requests a service ticket for a specific service account.</p> <p>The service ticket contains the encrypted user password hash.</p> <p>The adversary captures the service ticket and extracts the hash.</p> <p>The adversary can then attempt to crack the hash offline to reveal the user's password.</p> <p>Implications</p> <p>Persistence: A cracked user password provides the adversary with the ability to maintain persistence within the system.</p> <p>Lateral Movement: The attacker can move laterally within the network, potentially compromising other systems.</p> <p>Privilege Escalation: Access to user accounts may allow privilege escalation.</p> <p>Real-World Cases</p> <p>Ransomware: Adversaries may use Kerberoasting as part of a ransomware attack.</p> <p>Data Theft: Stealthy removal of data from a system.</p> <p>Backdoors: Building a back door for future access.</p> <p>Detection and Mitigation</p> <p>Detection:</p> <p>Monitor for unusual service ticket requests.</p> <p>Look for patterns indicative of Kerberoasting attacks.</p>

## Practicals

Practical No	Details
1.	Write programs to implement the following Substitution Cipher Techniques: - * Caesar Cipher - Encryption and Decryption
2.	Write programs to implement the following Substitution Cipher Techniques: * Playfair Cipher * Vernam Cipher
3.	Write programs to implement the following Transposition Cipher Techniques: - Rail Fence Cipher - Simple Columnar Technique
4.	Write program to encrypt and decrypt strings using - DES Algorithm - AES Algorithm
5.	Write program to encrypt and decrypt strings using - AES Algorithm
6.	Write a program to implement an IDEA algorithm to perform encryption / decryption of a given string.
7.	Write a program to implement the Diffie-Hellman Key Agreement algorithm to generate symmetric keys.
8.	Write a program to implement the MD5 algorithm to compute the message digest.
9.	Write a program to calculate HMAC-SHA1 Signature
10.	Write a Python program to illustrate ElGamal encryption

BOS	INFORMATION TECHNOLOGY
Class	M.Sc. I.T. Part - I
Semester	II
Course Name	On Job Training: Internship/ Apprenticeship
Course Code	PMSIT207
Type of course	OJT/FP
Level of the Subject	Advanced
Credit points	4

The syllabus proposes an internship for about 7 weeks to 8 weeks (min. 90Hrs) to be done by a student. It is expected that a student chooses a Data Analytics or IT-related industry and formally works as a full time/ part time intern during the period. The student should subject oneself with an internship evaluation with proper documentation of the attendance and the type of work he or she has done in the chosen organization. Proper certification (as per the guidelines given in Appendix 1 and 2) by the person, to whom the student was reporting, with the Organization's seal should be attached as part of the documentation.