



M. Tech Information and Cyber Security

VTR PGE 2023– Curriculum

CBCS - Choice Based Credit System

Department of Information Technology
School of Computing

M. Tech Information and Cyber Security**CBCS VTRPGE2023****(With effect from 2023-2024)****Minimum credits required for regular students in various course categories for
M.Tech(ICS)**

The students shall earn 80 credits in various course categories given below for the award of degree of M.Tech (CSE).

Course Category	Minimum Credits Required – Regular
Program Core	34
Program Elective	18
Open Elective	03
<u>Independent Learning</u> i) Technical Writing Tools /Business English ii) Research Methodology	02 02
<u>Project Work</u> i) Phase – I ii) Phase – II iii) Phase – III	03 06 12
Total	80

Vel Tech RangarajanDr.Sagunthala R&D Institute of Science and Technology

Department of Information Technology

M. Tech Information and Cyber Security- CBCS VTRPGE2023

Program Core (34 Credits)

L – Lecture; T – Tutorial; P – Practical; C – Credits

S. No	Subject Code	Course Name	L	T	P	C
1	20231IT101	Probability and Statistics	4	0	0	4
2	20231IT102	Advanced Data Structures and Algorithms	4	0	0	4
3	20231IT103	Advanced Operating Systems	4	0	0	4
4	20231IT104	Advanced Database Management Systems	4	0	0	4
5	20231IT105	Cryptography and Network Security	4	0	0	4
6	20231IT201	Network Technologies	3	0	2	4
7	20231IT202	Artificial Intelligence	3	0	2	4
8	20231IT203	Vulnerability Assessment and Penetration Testing	3	0	2	4
9	20231IT301	Advanced Data Structures and Algorithms Laboratory	0	0	2	1
10	20231IT302	Advanced Operating Systems Laboratory	0	0	2	1
Total						34

Program Elective (18 Credits)

L – Lecture; T – Tutorial; P – Practical; C – Credits

S. No	Subject Code	Course Name	L	T	P	C
1	20232IT102	Data Privacy and Security	2	0	2	2
2	20232IT201	Cloud Security	3	0	2	4
3	20232IT202	Block Chain Technology	3	0	2	4
4	20232IT203	Identity Access Management	3	0	2	4
5	20232IT204	Forensics in Cyber Security	3	0	2	4
6	20232IT205	Advanced Routing Techniques and Security	3	0	2	4
7	20232IT206	Web and Mobile Application Security*	3	0	2	4
8	20232IT207	Incident Response and Threat Intelligence*	3	0	2	4
9	20232IT208	Cyber Security Policy, Law and Ethics	3	0	2	4
10	20232IT209	Intrusion Detection and Prevention Systems*	3	0	2	4
11	20232IT210	Security Audit, compliance and Policy*	4	0	2	4
12	20232IT211	Malware Analysis and Reverse Engineering*	3	0	2	4

Open Electives (3 Credits)

- ❖ Open electives are the courses offered across the schools to enhance the knowledge breadth and professional competency of the students. The students shall register for appropriate electives offered in other PG programmes based on their area of interest. The courses offered under this category cover the interdisciplinary/ transdisciplinary knowledge.
- ❖ One course (Three credits) shall be taken from the courses offered by the online platform like Swayam, NPTEL.
- ❖ **In the Open Elective category they may enroll the course (3 credits) in MOOCs platform which is approved in the BoS.**

L-Lecture, T-Tutorial, P-Practical, C-credit

S.No	Course Code	Course Name	L	T	P	C
1	20233IT401	Open Elective-1 from NPTEL /Swayam	3	0	0	3

Independent Learning (4 Credits)

S. No	Course Code	Course Name	L	T	P	C	Pg.No
1	20234IT401	Research Methodology	2	0	0	2	
2	20234IT402	Technical Writing Tools /Business English	2	0	0	2	

Project Work (21 Credits)

S. No	Course Code	Course Name	L	T	P	C	Pg.No
1	20234IT701	Project Work Phase 1	-	-	-	3	
2	20234IT702	Project Work Phase 2	-	-	-	6	
3	20234IT703	Project Work Phase 3	-	-	-	12	

Mandatory

Student has to publish/present the project work in a Scopus indexed journals /International Conference

PROGRAM CORE

COURSE CODE	COURSE TITLE	L	T	P	C
20231IT101	Probability and Statistics	4	0	0	4

A.Preamble

To provide an in-depth knowledge about probability, sampling, Correlation and Random process

B.Prerequisite Courses

Nil

C.Course Objectives

Students undergoing this course are expected to

- Be familiar with the basic concepts of probability and random variables.
- Understand the basic concepts of sampling distribution.
- Develop the knowledge of testing of hypothesis for small and large samples which plays an important role in real life problems.
- Apply the Correlation and classifications of design of experiments for statistical quality control.

D.Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Understand the basic concepts of probability	K2
CO2	Apply the basic concepts of different types of sampling	K3
CO3	Utilize the concepts of Hypothesis testing and Chi-square testing to solve simple problems	K3
CO4	Demonstrate the concepts of Correlation	K3
CO5	Develop the concepts of Random process to solve simple problems	K3
Knowledge Level (Based on revised Bloom's Taxonomy) K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create		

E.Correlation of COs with Program outcomes and Programme Specific Outcomes:

COs	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2
CO1	M			M			M	M
CO2	M			M			M	M
CO3	M			M			M	M
CO4	M			M			M	M
CO5	M			M			M	M

H- Strong; M-Medium; L-Low

F.Course Contents**UNIT 1 INTRODUCTION****L-12****Hours**

Axioms of probability - Conditional probability - Total probability - Baye's theorem - Random variable - Probability mass function - Probability density function – Properties – Moments - Moment generating function and their properties - Binomial, Poisson, Geometric, Negative binomial, Uniform, Exponential, Gamma and Weibull distribution and their properties.

UNIT 2 SAMPLING**L-12 Hours**

Sampling: different types of sampling – Sampling distribution – Sampling distribution of Mean Point Estimation of parameters: general concepts of Estimation – Unbiased estimators – Variance of a point Estimator – Standard error – Method of point estimation (method of moments – method of maximum likelihood) – Statistical intervals for a single sample: confidence interval on the mean of a normal distribution with variance known – Confidence interval on the mean of a normal distribution with variance unknown – Confidence interval on the variance and standard deviation of a normal distribution

UNIT 3 TESTING OF HYPOTHESIS**L-12 Hours**

Hypothesis testing: one sample and two sample tests for means and properties of large samples (z-test), one sample and two sample tests for means of small samples (t-test), F-test for two sample standard deviations – Chi-square test for single sample standard deviation – Chi-square tests for independence of attributes and goodness of fit.

UNIT 4 CORRELATION AND REGRESSION**L-12 Hours**

Correlation – Scatter diagram – Karlpearson coefficient of correlation – calculation of the correlation coefficient for a bivariate frequency distribution – rank correlation – repeated rank – Regression – lines of regression – regression curves – regression coefficients – multiple and partial correlation – coefficient of partial correlation – generalization – multiple correlation.

UNIT 5 RANDOM PROCESSES**L-12 Hours**

Classification – Stationary process – Markov Process – Poisson process – Discrete parameter – Markov chain – Chapman Kolmogorov equations – Limiting distributions.

Total : 60 Hours

F.Learning Resources (in IEEE Format)**i.Text Books**

1. Richard A. Johnson and C. B. Gupta, Probability and Statistics for Engineers, (7th Edn.), Pearson Education, Indian Impression – 2011 (Unit 1 to 5)

ii.Online References

- 1.Course on “Probability and statistics” Dec 2021[online],Available:
<https://nptel.ac.in/courses/111/105/111105090>
- 2.Course on “Probabilities and Statistics course “,Dec 2021[online],
Available:<https://stanford.edu/~shervine/teaching/cs-229/refreshers-probabilities-statistics>

COURSE CODE	COURSE TITLE	L	T	P	C
2023IT102	Advanced Data Structures and Algorithms	4	0	0	4

A. Preamble

This course is designed with the purpose of offering comprehensive insights into the practical implementation and effective utilization of Algorithms and Data Structures. Throughout the course, learners will gain a deep understanding of various algorithms and their real-world applications. They will explore the details of designing, analysing, and implementing algorithms to solve a wide range of computational problems efficiently.

B. Prerequisite Courses

NIL

C. Course Objectives

Learners are exposed to

- Analyse complex problems and design efficient algorithms to solve them.
- Enhance problem-solving skills and algorithmic thinking.
- Equip with techniques to create algorithms optimized in terms of complexity.
- Familiarize with different algorithmic paradigms and to approach diverse problem types using various algorithmic techniques.

D. Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Apply the learned principles of algorithms and advanced data structures to real-world scenarios	K3
CO2	Solve complex problems using divide and conquer, greedy and dynamic programming techniques	K3
CO3	Implement appropriate graph-related algorithms for different types of problems	K3
CO4	Utilize advanced algorithms to effectively address complex computational challenges.	K3
CO5	Make use of P, NP completeness, approximation and randomized principles to provide solutions optimization problems	K3
Knowledge Level (Based on revised Bloom's Taxonomy) K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create		

E. Correlation of Cos with Program Outcomes and Programme Specific Outcomes

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2
CO1	3		3	3	3	2	3	3
CO2	3		3	3	3	2	3	3
CO3	3		3	3	3	2	3	3
CO4	3		3	3	3	2	3	3
CO5	3		3	3	3	2	3	3

3- High; 2-Medium; 1-Low

F. Course Contents

Unit 1 Introduction to basic data structures and algorithms

L-12 Hours

Role of Algorithms in Computing - Characterizing Running Times- Recurrences: Substitution Method - Recursion Tree Method - Master Method - Probabilistic Analysis - Randomized Algorithms. Advanced Data Structures: Binomial Heap - Fibonacci Heap - Min-Max Heaps - Weight-Balanced Trees -Tries - Splay Trees - B-Trees - Hashing - Disjoint Set - Union Find Operations

Unit 2 Advanced Design and Analysis Techniques

L-12 Hours

Divide and Conquer: Quick and Merge Sorting Techniques - Linear Time Selection Algorithm – Strassen’s Algorithm for Matrix Multiplication – Closest Pair and Convex-Hull Problem. Greedy Algorithms: Elements – Activity Selection Problem - Job Sequencing with Deadlines - Optimal Storage on Tapes - Container Loading or Bin Packing Problem - Offline Caching. Dynamic Programming: Elements - Rod Cutting - Matrix-Chain Multiplication - Longest Common Sequence – Flow Shop Scheduling – Coin Changing Problem. Amortized Analysis: Aggregate – Accounting Method - Potential Method.

Unit 3 Graph Algorithms

L-12 Hours

Elementary Graph Algorithms: Breadth First Search – Depth First Search. Minimum Spanning Trees: Algorithms for Kruskal and Prim. Single Source Shortest Path – Bellman Ford – Dijkstra’s Algorithm. All Pairs Shortest Path: Floyd-Warshall Algorithm. Network Flow Algorithms: Properties, Ford-Fulkerson Method - Maxflow-Mincut Theorem - Edmonds-Karp Heuristics - Maximum Bipartite Matching.

Unit 4 Advanced Algorithms

L-12 Hours

Number-Theoretic algorithms: GCD algorithm - modular arithmetic - primality testing – Miller Rabin test - Integer factorization - Pollard Rho heuristic. String matching: Rabin-Karp - Knuth-Morris-Pratt algorithms. Probabilistic algorithms: basics of probability theory, pseudorandom generators, Geometric Algorithms: Plane sweep technique, role of sweep-line - status and event-point schedule, line segment intersection problem.

Unit 5 NP-Completeness and Reductions**L-12 Hours**

P and NP Problems, NP- completeness and reducibility, NP-completeness proofs - NP-Complete Problems. Approximation Algorithms: vertex cover – traveling salesperson problem – set covering problem - Randomization and linear programming - subset- sum problem.

Total: 60 Hours**G. Learning Resources****i.Text Books**

1. Thomas H.Cormen, Charles E.Leiserson, Ronald L. Rivest and Clifford Stein, “Introduction to Algorithms”, Fourth Edition, MIT Press, 2022. [Unit 1,2,3,4].
2. Ellis Horowitz, Sartaj Sahni, Susan Anderson Freed, “Fundamentals of Data Structure in C”, Universities Press,2017. [Unit 5].

ii.Reference Books

1. Anany Levitin, “Introduction to the Design and Analysis of Algorithms”, Third Edition, Pearson Education, 2017.
2. V. Aho, J. E. Hopcroft, and J. D. Ullman, “Data Structures and Algorithms”, Pearson Education, First Edition, Reprint 2017.
3. Narasimha Karumanchi, “Data Structures and Algorithms Made Easy”, Fifth Edition, Career Monk, 2021.

iii.Online References:

1. “Introduction to Data Structures and Algorithms”. Accessed on Apr. 4 20, [Online]. Available: <https://nptel.ac.in/courses/106/102/106102064/>.
2. “Data Structures and algorithms”. Accessed on: Apr. 15, 2021 [Online]. Available: <https://www.coursera.org/specializations/data-structures-algorithms>.
3. “Data structures Visualization” 2011. Accessed on: Apr. 15, 2021 [Online]. Available: <https://www.cs.usfca.edu/~galles/visualization/Algorithms.html>
4. “Data Structures Fundamentals” 2021, Accessed on: Apr. 20,2021 [Online]. Available: <https://www.edx.org/course/data-structures-fundamentals>

COURSE CODE	COURSE TITLE	L	T	P	C
20231IT103	Advanced Operating Systems	4	0	0	4

A. Preamble

This course aims to offer students an introductory exploration of advanced concepts in operating systems design. Throughout this course, participants will delve into the architectural aspects and theoretical foundations of OS design, resource allocation, security measures, cluster computing, high-availability considerations, scalability challenges, and various other OS-related topics.

B. Prerequisite Courses

Nil

C. Course Objectives

Learners are exposed to

- Familiarize the concepts of synchronization Mechanisms, Deadlock and Memory Management Techniques.
- Understand the Distributed operating System Concepts and Synchronization methods.
- Solve common issues that may arise when using Windows, such as driver errors, system crashes, and software compatibility issues.
- Implement the Files and Disks management in UNIX environment.

D. Course Outcomes

Upon the successful completion of the course, students will be able to:

CO	Course Outcomes	K - Level
CO1	Understand various synchronization Mechanisms, Process Scheduling and Memory Management Techniques.	K2
CO2	Solve the issues and resolutions related to deadlock detection, centralized, distributed & hierarchical deadlock handling algorithms.	K3
CO3	Explain load distributing algorithms, synchronization techniques, distributed mutual exclusion algorithms & their classifications.	K2
CO4	Apply Diagnostic tools to resolve performance Issues in Windows Operating Systems.	K3
CO5	Implement various File, Disk and Network Management Schemes in Unix Operating System.	K3

Knowledge Level (Based on revised Bloom's Taxonomy)

K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create

E. Correlation of Cos with Program Outcomes and Programme Specific Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2
CO1	3	3	3	3	3		3	3
CO2	3	3	3	3	3		3	2
CO3	3	3	3	3	3		3	3
CO4	3	3		3	3			
CO5	3	3		3	3			

High- 3; Medium-2; Low-1

F. Course Contents**Unit 1 Fundamentals of Operating Systems****L-12 Hours**

Overview – Synchronization Mechanisms: Critical Section Problem, other Problems, and Language Mechanisms for Synchronization (Monitors, Serializers, Path Expressions) – Processes Deadlocks: Preliminaries, Models of Deadlocks, Models of Resources, Systems with only Reusable Resources

Unit 2 Distributed Deadlock Handling**L-12 Hours**

Deadlock handling strategies, Detection: Issues and resolution, Control Organizations, Centralized algorithms (Completely Centralized, The Ho-Ramamoorthy), Distributed algorithms (Path-pushing ,Edge-Chasing, Diffusion computation Based) Hierarchical **algorithms**: The Menasce-Muntz ,Ho-Ramamoorthy Algorithm.

Unit 3 Distributed Scheduling**L-12 Hours**

Scheduling: Issues in load distributing, Components of load distributing algorithms, Stability, Load distributing algorithms, Performance Comparison, Selecting load sharing Algorithm- Distributed Mutual Exclusion: Mutual Exclusion algorithms: Lamport's algorithm, The Ricart-Agarwala and Maekawa's Algorithm.

Unit 4 Performance & Storage Management In Windows**L-12 Hours**

Windows Architecture-Support, Diagnostic Tools-Monitoring ,Troubleshooting Computer Performance-SysInternal Tools-key stages in troubleshooting-purpose and benefits of the various tools-File Recovery-Application Troubleshooting-methods of file recovery-Troubleshooting Windows Startup, Operating System Service Issues-recovering from startup issues-advanced startup options-failed services- locked account scenarios- Troubleshooting Device Driver Failures,Hardware,Physical Failures. Remediate driver issues,Peripherals.storage technologies and Usage-different storage topologies, FC & iSCSI-RAID redundancy RAID 0, RAID 1, RAID 5,RAID 10-disk types-iSCSI logical units-iSCSI target instances-ATA basic disk, dynamic disk, mount points, file systems, mounting a virtual hard disk, distributed file system.

Unit 5 File,Disk & Network Management in Unix

L-12 Hours

Understanding Unix file system permission model, File access criteria - users, groups and permissions. Default permissions, changing file permissions, Importance of Backup, Different Backup tools, Backup and restore services, Basic of DAS, NAS and SAN, Physical disk organization, UNIX partition slices, Mounting and unmounting file systems, Checking and repairing file systems, Monitoring free space, Volume management (LVM) (create, remove, modify, resize), FTP Basic, Configuring FTP. NFS Overview, NFS Installation-Configuration-Troubleshooting. Samba Basics, Features of SAMBA, Installing and Configuring, Linux Squid (Proxy), Features of Sqid, Working of Squid, Configuring and Managing Web Server, Domain Name System, Dynamic Host Configuration Protocol, SSH and NTP, Configure key-based authentication, Synchronize time using other NTP peers, Manage security, Firewall Settings, SELinux, Network and Security services

Total : 60 Hours

G. Learning Resources

- . Text Books**
 1. MukeshSinghal, NiranjanaG.Shivaratri, "Advanced concepts in operating systems: Distributed, Database and multiprocessor operating systems", MC Graw Hill education, 2017.[Unit 1,2,3]
 2. Thomas, Orin. 'Windows server 2019 inside out'. Microsoft Press, 2020 [Unit 4]
 3. Ken Hess, "Practical Linux System Administration" O'Reilly Media, Inc,2023, ISBN: 9781098109035 [Unit 5]
- ii. Reference Books**
 1. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, "Operating System Concepts", Seventh Edition, John Wiley & Sons, 2016.
 2. Andrew S.Tanenbaum, "Modern Operating System", Pearson Edition, Fourth Edition, 2016.
- iii. Online References**
 1. Course on "Power of Operating system" ,Aug 2023,Accessed on Aug, 2023 [online], Available: <https://www.coursera.org/learn/os-power-user>.
 2. Course on "Distributed Systems" , Aug 2023 [online],Accessed on Aug, 2023Available: https://onlinecourses.nptel.ac.in/noc23_cs72/preview.
 3. "Windows Server documentation" , Accessed on Aug, 2023 [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/>.

COURSE CODE	COURSE TITLE	L	T	P	C
20231IT104	Advanced Data Base Management Systems	4	0	0	4

A. Preamble

This course deals with in-depth knowledge about maintain, manage and mitigate database systems in the current real-world scenarios via distributed databases, multi version concurrency control. Summarizing data for data analysis and provide statistic-based decision-making with huge databases like warehouses and big data.

B. Prerequisite Courses

Nil

C. Course Objectives

Learners are exposed to

- Describe the fundamental elements of relational database management systems
- Explain the basic concepts of the distributed and object databases.
- Understand the issues of multi-version granularity locks.
- Know how modern databases formulate SQL queries on data.

D. Course Outcomes

Upon successful completion of this course, students will be able to

CO Nos.	Course Outcomes	K - Level
CO1	Understand Object-Oriented concepts in the database.	K2
CO2	Implement object-oriented databases using Object Query Language.	K3
CO3	Explain concurrency control with a distributed database.	K2
CO4	Describe the decision-making through the mining process.	K2
CO5	Implement modern data models relating to real-time scenario.	K3

E. Correlation of COs with Program Outcomes and Programme Specific Outcomes:

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2
CO1	3		3				3	3
CO2	3		3	3	3		3	3

CO3	3		3	3	3		3	3
CO4	3		3	3	3		3	3
CO5	3		3	3	3		3	3

3- High; 2-Medium; 1-Low

F. Course Contents

Unit 1 Review of Data Model and OODBs

L -12 Hours

Relational model concepts; Relational model constraints and relational database schemas; Update operations, anomalies, dealing with constraint violations, Types, and violations. Enhanced entity relationship modeling, Hierarchical modeling, and Network Modeling. Overview of Object-Oriented Concepts – Objects, Basic Properties. Advantages, examples, Abstract data types, Encapsulation, class hierarchies, polymorphism, examples.

Unit 2 Object and Object-Relational Databases

L- 12 Hours

Object Query Language OQL; Conceptual design of Object database. Overview of object-relational features of SQL; Object-relational features of Oracle; Implementation and related issues for extended type systems; syntax and demo examples, Aliasing, Object aliasing. Algebraic operations on databases, Relational Algebra Queries.

Unit 3 Distributed Databases and Concurrency Control

L-12 Hours

Introduction to distributed databases; Distributed DBMS architectures; Storing data in a Distributed DBMS; Distributed catalog management; Distributed Query processing; Updating distributed data; Multi-Version Concurrency Control, Sharding; Distributed transactions; Distributed Concurrency Control and Recovery.

Unit 4 Data Warehousing, Decision Support, and Data Mining

L-12 Hours

Introduction to decision support; OLAP, multidimensional model; Implementation techniques for OLAP; Data Warehousing; Views and Decision Support, View materialization, Maintaining materialized views. Introduction to Data Mining; Counting co-occurrences; Mining for rules; Tree-structured rules; Clustering; Similarity search over sequences; Incremental mining and data streams;

Unit 5 Enhanced Data Models for Some Advanced Applications**L-12 Hours**

NoSQL with Object Oriented Concepts- MongoDB-Mongoose; CRUD operation using Mongo, Graph databases- Neo4j- CRUD operation using Neo4j; Neo4j vs Graph; Query modeling using Graph; Introduction to Big Data, Handling Big Data using MongoDB-Map Reduce using MongoDB-Hadoop Node configuration;

Total: 60 hours**H. Learning Resources****Text Books**

1. Abraham Silberschatz, Henry F. Korth and S. Sudharshan, "Database System Concepts", Seventh Edition, Tata McGraw Hill, 2020. [Units-1,2,3,4,5]
2. Shannon Bradshaw, E Brazil, Kristina Chodorow, "MongoDB: The Definitive Guide - Powerful and Scalable Data Storage", Third Edition, Shroff/O'Reilly Inc., January 2020.[Unit-5].

ii.Reference Books

1. Raghu Ramakrishnan et al, "Database Management Systems", Third Edition, McGraw Hill, 2014.
2. ElmasriRamez, Navathe S, "Fundamentals of Database System", Seventh Edition, Pearson, 2017.
3. J.D.Ullmann et al, "Database Systems: The Complete Book", Second Edition, Pearson Ed, Inc, 2009.

iii.Online References

1. "Designing local library models", Accessed on: May 05, 2021[online]. Available: <https://developer.mozilla.org/en-US/docs/Learn/Server>.
2. Michael Hunger, Ryan Boyd & William Lyon, "The Definitive Guide to Graph Databases for the RDBMS Developer", first Ed, E-book, Accessed on: October 27, 2021 [online & Download]. Available: <https://neo4j.com/whitepapers/rdbms-developers-graph-databases-ebook/>.
3. "Database Management systems", Accessed on: August 29, 2023 [online]. Available [Archive]: <https://archive.nptel.ac.in/courses/106/105/106105175/>.

COURSE CODE	COURSE TITLE	L	T	P	C
20231IT105	Cryptography and Network Security	4	0	0	4

B. Preamble

This course is designed to help learners comprehend various cryptographic methods and protocols, as well as security techniques. The course provides learners to choose the suitable security standards for solving real-world problems.

C. Prerequisite Courses

20231IT201- Network Technologies

D. Course Objectives

Learners are exposed to

- Identify the conceptual basis of cryptography and security.
- Apply the concepts of Symmetric key cryptography principles.
- Explain the modern cryptographic systems using asymmetric key cryptography
- Choose the web security techniques to ensure application-level security
- Utilize the application layer security standards to get acquainted with the real time security practices.

E. Course Outcomes

Upon successful completion of this course, students will be able to

CO Nos.	Course Outcomes	K - Level
CO1	Apply the basics of Cryptography techniques for data and information security	K3
CO2	Choose Symmetric Cryptographic techniques to make block ciphers and stream ciphers.	K3
CO3	Utilize Asymmetric Cryptographic techniques to solve Diffie Hellman exchange, RSA implementations.	K3
CO4	Develop message integrity and confidentiality methods for web application security	K2
CO5	Apply the intrusion detection system and network monitoring for application layer security	K3

G. Correlation of COs with Program Outcomes and Programme Specific Outcomes:

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2

CO1	2		3		2		2	3
CO2	1		3		2		3	1
CO3	1		1		2		2	1
CO4	2		3		2		2	1
CO5	2		3		2		2	1

3- High; 2-Medium; 1-Low

H. Course Contents

Unit 1 Introduction

L -12Hours

OSI Security Architecture, Basics of Symmetric Encryption -classical Ciphers:

Caesar Cipher, Substitution cipher Permutation – mode of operation Perfect Encryption – One time Pad, Encryption Security: Informational Security and Computational Security, Attack models, Security Goals, Security Notions- Asymmetric Encryption - Pseudo-random Number Generators (PRNGs)- Real word PRNGs – Cryptographic PRNGs vs Non-Cryptographic PRNGs - Key Generation: Symmetric Key and Asymmetric Key generation.

Unit 2 Symmetric Cryptography

L- 12 Hours

Data encryption standard (DES)- DES strength , Block ciphers: Design principles ,Slide attack and Round Keys Substitution -Permutation Networks , Feistel schemes – AES: Table based Implementations, Modes of operation , Stream Ciphers:RC4 - Hash functions: SHA512 - MACs, Authenticated Encryption.

Unit 3 Asymmetric Cryptography

L-12 Hours

Computational hardness - Complexity Classes-Factoring problem -Discrete Logarithm problem -RSA trap door Permutation, RSA Key generation and Security, RSA Implementations: Square and Multiply Exponential Algorithm, Chinese Remainder theorem, Diffie-Hellman : Functions – Problems- Protocols – Elliptic Curves.

Unit 4 Web Security

L-12 Hours

The TLS and SSL Family of Protocols: A Brief History, Transport-Layer Protocol suite ,TLS 1.3 improvements over TLS 1.2 , TLS security : Authentication and Forward Secrecy, Secure Shell (SSH) application, IP Security - Internet Key Exchange (IKE) . Kerberos Systems, X.509 Certificates.

Unit 5 Application Layer Security Practices**L-12 Hours**

Electronic Mail Security: Pretty Good Privacy, S/MIME, DomainKeys Identified Mail.
 Wireless Network Security: Mobile Device Security, Firewalls and Intrusion Detection
 Systems: Intrusion Detection Password Management, Firewall Characteristics Types of
 Firewalls, Firewall Basing, Firewall Location and Configurations, Cloud Security.

Total: 60 hours**I. Learning Resources****i.Text Books**

1. Jean-Philippe Aumasson, "Serious Cryptography: A Practical Introduction to Modern Encryption", No starch Press, Inc. 2017. (Unit- 1,2,3,4)
2. W. Stallings, "Cryptography and Network Security: Principles and Practice", 7/E, Prentice Hall, 2017. (Unit- 5)

ii.Reference Books

1. Behrouz A. Ferouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security", 3rd Edition, Tata Mc Graw Hill, 2015.
2. M. Speciner, R. Perlman, C. Kaufman, "Network Security: Private Communications in a Public World", Prentice Hall, 2002.

iii.Online References

1. Cryptography and Network Security , Accessed on: July 2022, [online]. Available: <https://nptel.ac.in/courses/106105162>
2. "Cryptography techniques", Accessed on: July 2022, [online]. Available: <http://Cryptographywilliamstallings.com/Extras/Security-Notes/>
3. "Authentication algorithms", Accessed on: July 2022 [online]. Available: <http://www.cs.bilk.ent.edu.tr/~selcuk/teaching/cs519/>
4. "Network security concepts", Accessed on: July 2022[online]. Available: <http://freevideolectures.com/Course/3027/Cryptography-andNetwork-Security>

COURSE CODE	COURSE TITLE	L	T	P	C
20231IT201	Network Technologies	3	0	2	4

A. Preamble

The objective is to acquaint the students with the knowledge of network technologies and devices. Switching and Routing technologies are intended to understand the interconnection and configuration of different protocols used to provide network access to LAN/WLAN users. It covers both the practical and theoretical aspects of the installation, configuration, and other related technical requirements for WLAN, access point, VLAN, and VoIP. Students will understand different network technologies and challenges in networking environment.

B. Prerequisite Course

20231IT102 – Advanced Data structures and Algorithms.

C. Course Objectives

Learners are exposed to:

- Understand the concept of TCP and UDP services.
- Know the basic properties of VLAN and modes.
- Implement various techniques of advance routing and wireless networks.
- Interpret the importance of an Ultra-wideband wireless setup and its practical applications.

D. Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Develop the working concepts of TCP-IP reference model and UDP services.	K3
CO2	Demonstrate the virtual local area network configuration, access mode and trunk mode services.	K3
CO3	Explain the functions of advance routing and wireless network services.	K3
CO4	Build the scenario for high-speed network technologies.	K3
CO5	Design the configuration of Ultra-wideband wireless setup.	K3
Knowledge Level (Based on revised Bloom's Taxonomy) K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create		

E. Correlation of Cos with Program Outcomes and Programme Specific Outcomes:

Cos	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PSO 1	PSO 2
CO1	3	3	3			1		
CO2	3	3	2			1		
CO3	3	3				1	2	1
CO4	3	3				1		3
CO5	3	3	3	3	1	1		3

3- High; 2-Medium; 1-Low

F. Course Contents**Unit 1 Introduction****L-9 Hours**

History of Networking; Need for Speed and Quality of Service; Advanced TCP/IP Networks Backbone Networks; High Performance Networks; TCP Services; TCP format and connection management; SCTP; Encapsulation in IP; UDP Services, Format and Encapsulation in IP; IP Services; Header format and addressing; Fragmentation and reassembly; classless and subnet address extensions; Subnetting and Supernetting.

Unit 2 Virtual Local Area Network**L-9 Hours**

Virtual LANs and VLAN Trunking Protocol (VTP) Introducing VLAN, Types of VLANs- Native VLAN, Management VLAN, Default VLAN, Voice VLAN, Data VLAN, Access mode and Trunk mode for switch interfaces, Trunking modes-On, Dynamic-desirable, Dynamic-auto, non-negotiate. Configuring VLAN and Trunks, Trouble Shooting VLANs and Trunks, VTP Concept, VTP Operation- VTP server, VTP client and VTP transparent modes, Configuring and Troubleshooting VTP.

Unit 3 Advanced Routing Technologies**L-9 Hours**

Static and Dynamic Routing, Static Routes with —Next Hop, Addresses, Static Routes with Exit Interface, Summary and Default Static Routes, Configuring and Troubleshooting Static Routes; Classifying Dynamic Routing Protocols, Metrics, Administrative Distance, Shortest path algorithms Dijkstra's Algorithm and Bellman-ford Algorithm. Wireless Networks, Wireless Ad Hoc networks, Applications and Challenges, Types of Ad Hoc Networks: Mobile Ad Hoc Network (MANET), Wireless Sensor Networks (WSN).

Unit 4 Advanced High-Speed Network**L-9 Hours**

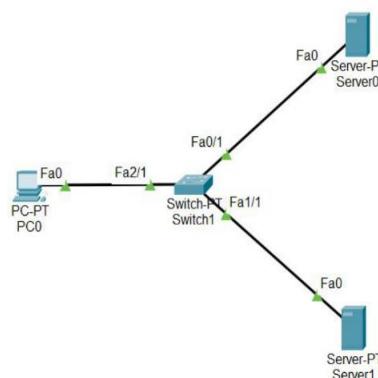
ADSL, other DSL Technologies; Cable Networks: Traditional Cable Networks, Fast Ethernet, Gigabit Ethernet, HFC Networks, Internet Over Cable, Spectrum Allocation, Sharing, Cable Modems, CM & CMTS, Data Transmission Schemes DOCSIS, ADSL versus Cable; FDDI, OFDMA; B-ISDN architecture.

Unit 5 Wireless Technologies**L-9 Hours**

Ultra-wideband Wireless: Overview of ultra-wideband (UWB) wireless, UWB applications, UWB acceptance, VoIP and Voice over WLANs: Overview of voice over IP (VoIP), Components of VoIP, Centralized and distributed VoIP architectures, The ITU-T umbrella protocol: H.323, Session Initiation Protocol (SIP), MGCP and H.248/Megaco, VoIP and Quality of Service (QoS), Mobile Wireless Brief history of mobile wireless, Overview of mobile wireless systems, Roaming in a mobile wireless system.

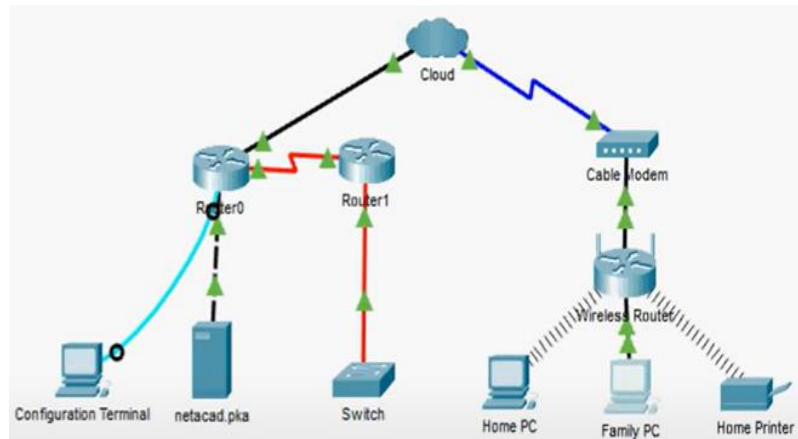
Total: 45 Hours**G. Laboratory Experiments****Total: 30 Hours****Task 1**

Implement a local area network, and to perform an initial configuration of a Cisco Catalyst 2960 switch for the given topology diagram.

**Tool: Cisco Packet Tracer**

Task 2

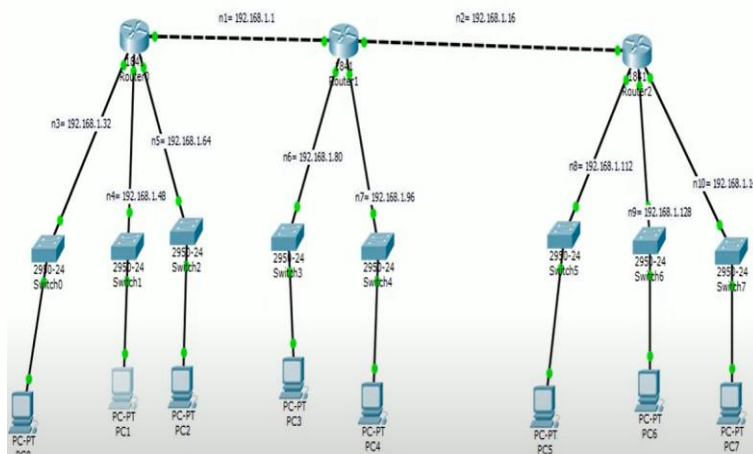
Implement and connect a Wired and Wireless LAN.



Tool: Cisco Packet Tracer

Task 3

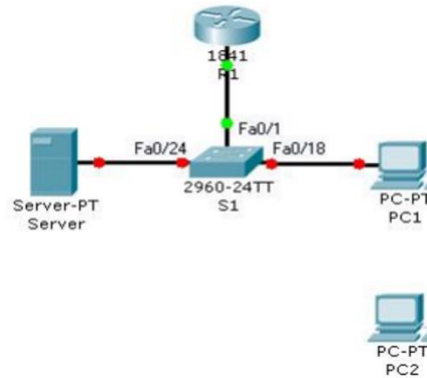
Implement a network using three routers and eight switches and perform subnetting.



Tool: Cisco Packet Tracer

Task 4

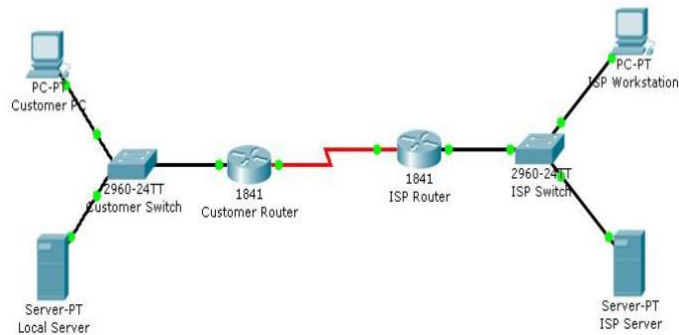
Configuring and troubleshooting a switched (Generic switch) network for the given topology diagram.



Tool: Cisco Packet Tracer

Task 5

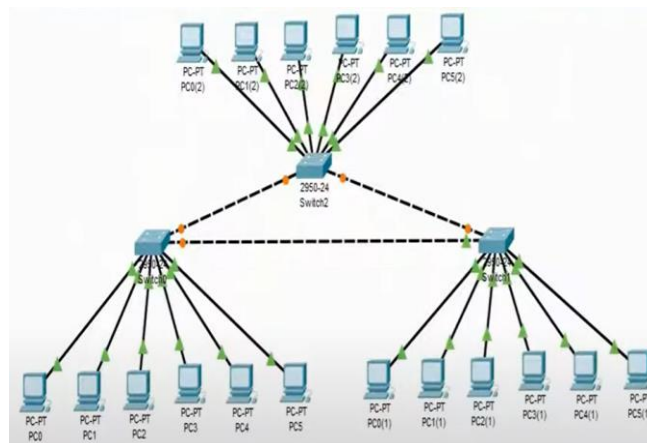
Implement and configure the VLAN1.



Tool: Cisco Packet Tracer

Task 6

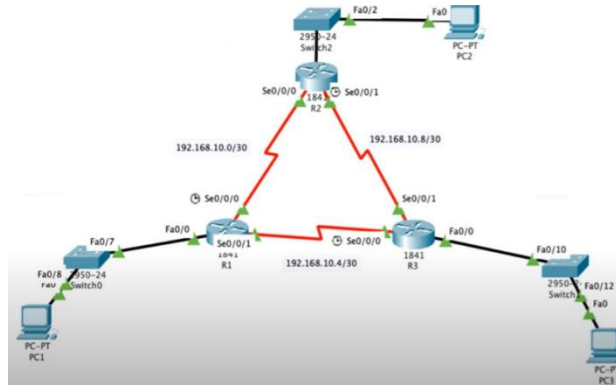
Implement and configure the VLAN2.



Tool: Cisco Packet Tracer

Task 7

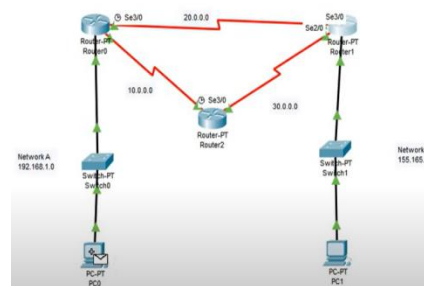
Implement to update OSPF protocol table for the given network.



Tool: Cisco Packet Tracer

Task 8

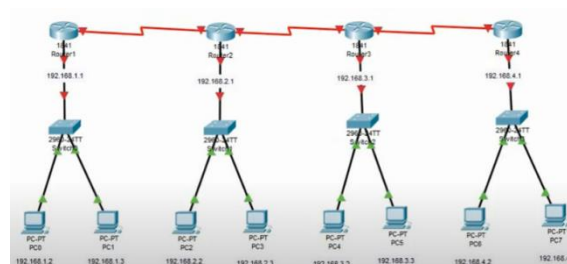
Implement to update routing information protocol table for the given network.



Tool: Cisco Packet Tracer

Task 9

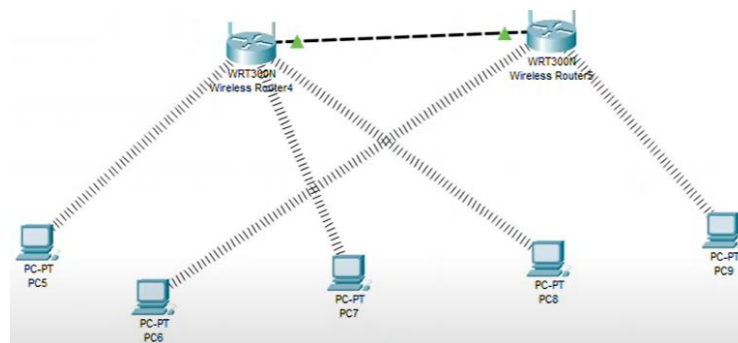
Implement and configure the static routing protocol (RIP).



Tool: Cisco Packet Tracer

Task 10

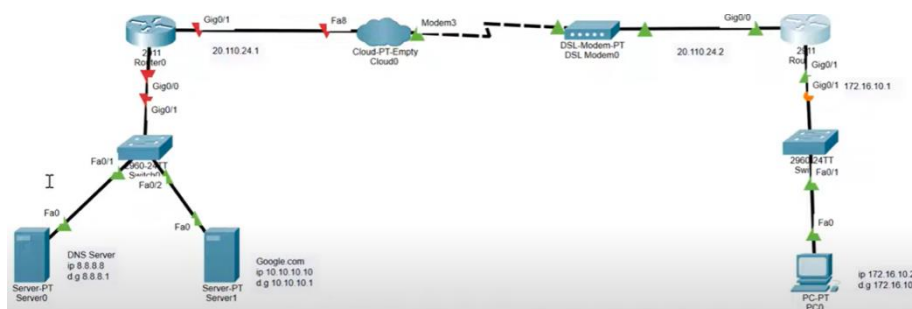
Implement and configure the Ad Hoc network.



Tool: Cisco Packet Tracer

Task 11

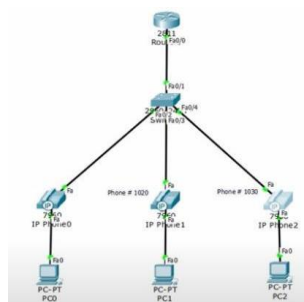
Implement and configure the ADSL connection.



Tool: Cisco Packet Tracer

Task 12

Implement and configure VoIP phones.



Tool: Cisco Packet Tracer

Part-2**Use Cases:****Use Case 1: Ultra-Wideband Technology for Precise Location Tracking:**

The biggest benefit of this pulse-based transfer is that it's possible to calculate time-of-flight information from the received data. UWB can send as many as one billion pulses per second — and each of those pulses can be measured based on how long it takes the data transfer to go from one device to another. Once you know the time taken for the signal to travel between two UWB devices, as well as the speed of the data transfer, it's simple math to work out the

distance between the transmitter and receiver. In the real world, this means UWB eliminates the risk of relay attacks, commonly employed by car thieves that involves intercepting and rebroadcasting radio signals to maliciously gain access to a locked vehicle.

Use Case 2:SPAN:

With Smartphone Ad Hoc Networking-or SPAN-your phone can be a critical communications link. MITRE's prototype solution, SPAN, enables communications in challenged environments. Mesh networks have been a concept for quite a while. With the introduction of smart phones and in particular the Open-Source Android project from Google, the built-in Wi-Fi is actually a vastly underutilized resource that lends itself nicely to building a mesh network. SPAN can be considered one type of implementation of a more generic concept known as a Mobile Ad Hoc Network (MANET).

Total: 75 Hours

G. Learning Resources

i.Text Books

1. Oliver C, "Fundamentals of Data Communication Networks", Wiley Publications, 2017. [Unit 1,2].
2. Behrouz A. Forouzan, "Data Communications and Networking", McGraw Hill Education, 5th Edition, 2017. [Unit 3, 4, 5].

ii. ii.Reference Books

1. Rick Graziani, Allan Johnson, "Routing Protocols and Concepts, CCNA Exploration Companion Guide", Cisco Press, 2011.
2. Jochen Schiller, "Mobile Communications", Second edition, Pearson Education, 2007.
3. McQuerry, Stephen, Jansen, David, Hucaby, David, Cisco LAN Switching Configuration Handbook (Networking Technology) 2nd Edition, Kindle Edition, 2009.

iii.Online References

1. "Introduction to TCP/UDP" [Online]. Accessed on May 2023, Available: https://www.cisco.com/c/en/us/td/docs/ios/sw_upgrades/interlink/r2_0/api_con/act_cp.html
2. "Virtual Area Network". [Online]. Accessed on Feb 2023, Available: <https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html>.
3. "Advanced Routing and Wireless Technologies" [Online]. Accessed on June 2023, Available: <https://www.cisco.com/web/AP/wireless/pdf/overview.pdf>.

COURSE CODE	COURSE TITLE	L	T	P	C
20231IT202	Artificial Intelligence	3	0	2	4

. Preamble

The primary objective of this course is to introduce the basic principles, techniques, and applications of Artificial Intelligence. In this course, students can explore the various search techniques like basic, advanced and heuristic approach were universal problem solving methods to solve a specific problem and provide the best result. Evolutionary algorithms are used to optimize the AI applications. Goal and constraint-based approach, Knowledge reasoning and inference helps the students to develop the decisions making strategies in intelligent agents and expert systems.

B. Prerequisite Course

20231IT102 – Advanced Data Structures and Algorithms

C. Course Objectives

Learners are exposed to:

- Explore the artificial intelligence techniques by using basic and heuristic search approach.
- Understand the basic principles of artificial intelligence concepts towards problem solving, knowledge representation and learning.
- Explore the artificial intelligence techniques in rules and fact-based approach.

D. Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Apply the problem-solving techniques by using State Space and heuristic search approach.	K3
CO2	Use evolutionary and advanced search techniques to provide optimized solution.	K3
CO3	Implement unified planning approach for Constraint-satisfaction problems.	K3
CO4	Apply Logical knowledge representation for rules and fact-based approach.	K3

CO5	Interpret the logic of Uncertainty and Reasoning using resolution methods.	K3
Knowledge Level (Based on revised Bloom's Taxonomy) K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create		

E. Correlation of Cos with Program Outcomes and Programme Specific Outcomes:

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2
CO1	3	3		1	1		2	
CO2	3	3	3	1	1		2	
CO3	3	3	3	1	1		2	
CO4	3	3	2	1	2		1	
CO5	3	3	3	1	2		2	

3- High; 2-Medium; 1-Low

F. Course Contents

Unit – 1 Basic and Heuristic Search Techniques

L-9 Hours

Artificial Intelligence – Introduction - Evolution of AI- State Space Search: Generate and Test- Simple Search- Depth First Search- Breadth First Search- Comparison of BFS and DFS- Depth Bounded DFS- Depth First Iterative Deepening. Heuristic Search: Heuristic Functions- Best First Search- Hill Climbing- N-Puzzle Problem- Block-world Problem - Variable Neighborhood Descent- Beam Search- Tabu Search- Peak to Peak Methods.

Case Studies – Weather Forecasting.

Unit – 2 Evolutionary and Advanced Search Techniques

L-9 Hours

Randomized Search and Emergent Systems: stochastic and evolutionary search algorithms - Simulated Annealing- Emergent Systems- Ant Colony Optimization- Finding Optimal Paths: The Travelling Salesman Problem- Dynamic Programming- Algorithm A*- Iterative Deepening A* - Min-Max- Alpha-Beta Tree search – Monte Carlo Tree Search - Case Studies - Map Navigation - Pruning the OPEN and CLOSED List- Divide and Conquer Beam Stack Search.

Unit – 3 Planning and Strategies**L-9 Hours**

Planning: planning as search, partial order planning - A Unified Planning Framework - Forward and Backwards State Space Planning- Goal Stack Planning- Plan Space Planning - The STRIPS Domain- Constraint Satisfaction Problem: N-Queens-Cryptarithmic-Constraint Propagation- Scene Labeling- Higher Order and Directional Consistency- Algorithm Backtracking: Graph Coloring - Case Studies – Robot traversal.

Unit– 4 Knowledge Representation**L-9 Hours**

Ontologies, foundations of knowledge representation- Logical representation -The Scheme - Frames- Semantic Net- Production rules -Scripts - Inheritance in Taxonomies- Description Logics- Formal Concept Analysis- Conceptual Graphs Knowledge reasoning - Reasoning about objects- relations – events- actions- time and space-reasoning with defaults- Reasoning about knowledge Case studies – Chabot system.

Unit– 5 Knowledge Facets and Logic Inferences**L-9 Hours**

Knowledge Facets: Intelligent agents: reactive, deliberative, goal-driven, utility-driven, and learning agents- The Wumpus World. Logic and Inferences: Formal Logic- Resolution Method in Propositional Logic- Resolution method in First Order Logic- Deductive Retrieval – Horn Clauses – Forward Chaining- Backward Chaining- Uncertain Knowledge - Probabilistic Reasoning- connection to logic- independence- Bayes rule- Bayesian networks probabilistic inference, Case studies – Multi- Agent Decision Making System.

Total: 45 Hours**G. Laboratory Experiments****Total: 30 Hours****Part 1**

Task 1 Implement the Graph search algorithms using Breadth first search and Depth First Search.

Tools- Python, Online Simulator - <https://graphonline.ru/en/>

Task 2 Implement the A * Algorithm to find the optimal path.

Tools- Python, Online Simulator - <https://graphonline.ru/en/>

Task 3 Implement the Mini-Max algorithm that uses recursion to search through the game-tree.

Tools- Python, Online Simulator - <https://graphonline.ru/en/>

Task 4 Write a Program to Implement Tic-Tac-Toe game using Python

Tools- Python, Online Simulator - <https://graphonline.ru/en/>

Task 5 Implement the Ant Colony Optimization to Optimize Ride-Sharing Trip Duration.**Tools- Python, Online Simulator - <https://graphonline.ru/en/>**

Task 6 Solve a Map Coloring problem using constraint satisfaction approach by applying following constraints

- Assign each territory a color such that no two adjacent territories have the same color by considering following parameters: Domains, Variables and Constraints.
- Apply Basic Greedy Coloring Algorithm: Color first vertex with first color, do following for remaining $V-1$ vertices.
- Consider the currently picked vertex and color it with the lowest numbered color that has not been used on any previously colored vertices adjacent to it. If all previously used colors appear on vertices adjacent to v , assign a new color to it.

Tools- Python, Online Simulator - <https://graphonline.ru/en/>

Task 7 Implement the Monkey Banana Problem in Goal Stack planning using prolog by applying following constraints. Imagine a room containing a monkey, chair and some bananas. That have been hanged from the centre of ceiling. If the monkey is clever enough, he can reach the bananas by placing the chair directly below the bananas and climb on the chair. The problem is to prove the monkey can reach the bananas. The monkey wants it, but cannot jump high enough from the floor. At the window of the room there is a box that the monkey can use. The monkey can perform the Following actions: -

- 1) Walk on the floor.
- 2) Climb the box.
- 3) Push the box around (if it is beside the box).
- 4) Grasp the banana if it is standing on the box directly under the banana.

Tools- Python, Online Simulator - <https://graphonline.ru/en/>

Task 8 Implement the N-queen problem using backtracking algorithm. In the 4 Queens problem the object is to place 4 queens on a chessboard in such a way that no queens can capture a piece. This means that no two queens may be placed on the same row, column, or diagonal.

Tools- Python, Online Simulator - <https://graphonline.ru/en/>

Task 9 To Build an Intelligent Chatbot system with Python and Dialog-flow using Interactive Text Mining Framework for Exploration of Semantic Flows in Large Corpus of Text.

Tools- Python, Online Simulator - <https://graphonline.ru/en/>

Task 10 Implement simple fact for following: a. Ram likes mango. b. Seema is a girl. c. Bill likes Cindy. d. Rose is red. e. John owns gold.

Tools- Python, Online Simulator - <https://graphonline.ru/en/>

Task 11 Implement the Bayesian networks probabilistic inference.

Tools- Python, Online Simulator - <https://graphonline.ru/en/>

Part-2 Use Cases:

Use Case – 1:Implement the Map navigation using Heuristic search approach in python.

Use Case – 2:Develop a simple neural network for simulating logic gate operations.

Use Case – 3:Solve Multiple criteria production scheduling problem using Genetic algorithm.

Use Case – 4: Implement the Text Lemmatization using NLTK Python Package.

Use Case – 5: Implement the Intelligent Chat-Bot system using Python and Dialogflow

Use Case – 6: Implement the Block world problem using STRIPS domain precondition rules in prolog.

Total:75 Hours

H. Learning Resources

i.Text books:

1. Stuart. J. Russell, et al. “Artificial Intelligence by Pearson: A Modern Approach” 4th Ed, 2020 [Unit 1 - 5]

ii.Reference books:

1. E. Rich and K. Knight,” Artificial Intelligence”, Mc Graw Hill Publishers Inc, 3rd Edition, 2017.
2. Deepak Khemani, “A First Course in Artificial Intelligence”, McGraw Hill Education, 2013.

iii.Online Reference Links/ Resources:

1. “Artificial Intelligence :Search Methods for Problem Solving”, May. 06, 2014 [Online]. Available: <https://nptel.ac.in/courses/106/106/106106126/> .
2. “Artificial Intelligence: Knowledge representation and reasoning” Jan. 19, 2016. [online] Available :
3. <https://nptel.ac.in/courses/106/106/106106140/>

COURSE CODE	COURSE TITLE	L	T	P	C
20231IT203	Vulnerability Assessment and Penetration Testing	3	0	2	4

A. Preamble

This course will enable the students to understand and apply the underlying principles and many of the techniques associated with the cybersecurity practice such as penetration testing and the exploitation in the networks and host through vulnerability analysis. This course covers penetration testing ranging from passive and active reconnaissance, vulnerability assessment, post exploitation and pivoting.

B. Prerequisite Courses

20231IT102- Advanced Data Structures and Algorithms

Course Objectives

Learners are exposed to

1. Critically interpret the vulnerabilities and exploitation in the system
2. Analyze cyber-attacks and the possible remedial measure undertaken
3. Interpret a management view of system and apply security strategy through efficient vulnerability analysis and cyber security principles.
4. Infer the security threats in context of users, organization and third party risk assessment.

C. Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Understand the basic concepts of vulnerabilities, their terminologies and overview of testing methods	K2
CO2	Apply the penetration testing tools to explore the vulnerabilities in a system	K3
CO3	Explain the management of vulnerabilities including discovery and mitigation	K2
CO4	Discuss the exploitation and the possible threats through various attacking mechanisms	K2
CO5	Apply the vulnerability and scanning tools to detect and avoid vulnerabilities	K3
Knowledge Level (Based on revised Bloom's Taxonomy) K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create		

D. Correlation of COs with Program outcomes and Programme Specific Outcomes:

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2	PSO3
CO1	2					2			
CO2			2	2	2				
CO3		2		2		2			
CO4	2								
CO5			2	2	2				

E. Course Contents**UNIT I Introduction to Vulnerability analysis****9 Hours**

Introduction to vulnerability – Types of Vulnerabilities - Vulnerability assessment (VA) – Security weakness in a system –Host level Vulnerability – Network level vulnerability – Application level vulnerability – Reconnaissance – Active and Passive Reconnaissance – Vulnerability testing – Testing Methodologies.

UNIT-II Penetration Testing**9 Hours**

Introduction to Penetration testing - An Overview of Ethical requirements and legal issues - Penetration test report and components – Scanning network - DNS, web reconnaissance – Patching - Buffer overflow - Introduction to Nessus scanning tool – Introduction to Metasploit framework - Metasploit security vulnerabilities.

Unit 3 Vulnerability management**9****Hours**

Introduction – Information gathering – Active and Passive Information gathering – Scanning for Vulnerabilities - Who is lookup – Introduction to vulnerability management – Vulnerability discovery – Vulnerability Mitigation – Patch and Configuration management – Encountering DoS and DDoS attack – Web application vulnerability scanning – Arachni tool.

Unit 4 Vulnerability and Exploitation**9 Hours**

Introduction - Cyber ethics – Cyberattack – SQL Map – Broken Authentication – Sensitive Data exposure – XML external entity attack – Code Injection – CRLF injection - Broken access control – Security misconfigurations – Cross site Scripting – Deserialization attack – Using components with known vulnerabilities – Logging and auditing dashboard.

Unit 5 Vulnerability Detection and avoidance**9 Hours**

White box and Black box testing in cybersecurity - Introduction to white box, black box and grey box fuzzing – Taint analysis – String analysis and solving – Protection from format string vulnerabilities – Protection from buffer overflow vulnerabilities – Network analysis tools – Port scanning and use of scripts in nmap script engine – Report Writing – Post incident log review.

Total: 45 Hours**F. Lab Experiments****Part - I**

Task 1: Understanding kali linux and retrieving PII of a host such as registrant name, organization, country, name servers, and date of creation, expiry and updation.

Task 2: Perform penetration testing by analysing through ping on IP and Domain using wireshark and kali linux interface and gather information about source, destination, and protocol.

Task 3: To perform Passive Reconnaissance identification which take advantage of unintentional data leaks from an organization using Wireshark.

Task 4: Perform Active Reconnaissance by engaging target systems to gather information about vulnerabilities using Nmap.

Task 5: To perform the scanning operations for services in the target using nmap.

Task 6: To perform analysis on the list of infected files downloaded and their hashes, and analyse the URL/Domain of the infected site using Wireshark.

Task 7: To sniff packets using SSH and Telnet protocol and retrieve the username and password using Wireshark.

Task 8: Introduction to operations on Metasploit framework and Scripting for penetration testing – Recon and Enumeration scripts .

Task 9: To perform offensive security mechanisms by executing port scan, ipscan and vulnerability scan.

Task 10: To analyze the privilege Escalation attack scenario and issues using metasploit

Part -II: Use cases

Use Case 1: Scan an http domain site and assess its vulnerabilities to prepare a detailed vulnerability report including Assessment overview, individual vulnerability details and prioritizing the vulnerabilities.

Use Case 2: Perform a Penetration test on a Web application and detect its vulnerabilities associated and also remediate a solution for the vulnerability

Use Case 3: Analyze the security incidents in a web application and prepare a log and audit table providing the security incidents on a web application.

Use Case 4: Perform a scanning process in network and preparing reports on reverse DNS and IP lookups, PII

Total: 30 Hours 45+30=75 Hours)

G.Learning Resources (in IEEE Format)

i. Text Books:

1. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy", ISBN: 978-1597496551, Syngress, 2013.(Unit I, IV)
2. Stuart McClure, Joel Scambray, George Kurtz, "Hacking Exposed 7: Network Security Secret & Solutions", McGraw Hill, ISBN 978-0-07-178028-5, 2012.(Unit V)
3. Wil Allsopp, "Advanced Penetration Testing: Hacking the World's Most Secure Networks", Wiley Publications, ISBN: 978-1-119-36768-0, 2018. (Unit II, III)

ii. Reference Books:

1. Joakim Kavrestad, "Fundamentals of digital forensics, theory, methods, and real life applications", Second Edition, ISBN 978-3-030-38954-3, Springer, 2020

iii. Online References:

1. “Ethical Hacking”, Accessed on: May 15, 2021 [Online]. Available: <https://nptel.ac.in/courses/106/105/106105217/>
2. “Vulnerability Scanning”, Accessed on: June 5, 2021 [Online]. Available: <https://alison.com/topic/learn/92039/web-application-vulnerability-scanning>
3. “Vulnerability scanning tool: Nessus”, Accessed on: June 5, 2021 [Online]. Available: <https://www.cs.cmu.edu/~dwendlan/personal/nessus.html>
4. “Vulnerability Testing”, Accessed on May 12, 2021 [Online]. Available: <https://us-cert.cisa.gov/bsi/articles/best-practices/white-box-testing/white-box-testing#BandG>

COURSE CODE	COURSE TITLE	L	T	P	C
20231IT301	Advanced Data Structures and Algorithms Laboratory	0	0	2	1

A. Preamble

This course is intended to cultivate the ability to create and evaluate linear and nonlinear data structures. Students gain first hand proficiency in identifying and implementing appropriate data structures for real-world problems. This practical exposure equips them with insights into the tangible applications of these data structures.

B. Prerequisite Courses

Nil

C. Course Objectives

Learners are exposed to:

- Understand the role of algorithms in computing and their significance in solving various computational problems.
- Familiarize with advanced data structures and algorithmic techniques for solving various applications.
- Acquired advanced algorithms to solve specific types of problems

D. Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Implement advanced data structures to efficiently handle complex data storage and retrieval tasks.	K3
CO2	Design efficient algorithmic techniques for computational problems considering complexity factors	K3
CO3	Analyse appropriate graph-related algorithms to solve computing applications	K3
CO4	Make use of number theoretic and probabilistic algorithms to specific types of problems	K3
CO5	Apply randomization and linear programming concepts to address optimization problems with practical solutions	K3
Knowledge Level (Based on revised Bloom's Taxonomy) K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create		

E. Correlation of Cos with Program Outcomes and Programme Specific Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO12	PSO1	PSO2
CO1	3		3	3	3	3	3	3	2
CO2	3		3	3	3	3	3	3	2
CO3	3		3	3	3	3	3	3	2
CO4	3		3	3	3	3	3	3	2
CO5	3		3	3	3	3	3	3	2

3- High; 2-Medium; 1-Low

F. Course Contents**Part I:****Task 1: Priority Queue Data Structure**

- i) Binomial Heap: Implement the decrease-key operation in a binomial heap and analyze its time complexity
- ii) Fibonacci Heap: Implement a mechanism for lazy deletion in Fibonacci heaps

Task 2: Advanced Data Structures

- i) Splay Tree: Implement the operations to find the kth smallest or largest element in a Splay Tree. Test your implementation with various values of k.
- ii) B Tree: Implement disk-based operations by tracking the number of page accesses required for various B-Tree operations. Experiment with different node sizes and order values to optimize disk I/O efficiency

Task 3: Advanced Hashing

- i) Implement and analyze cryptographic hash functions like SHA-256
- ii) Implement the Rabin-Karp string searching algorithm that uses hashing to efficiently search for a pattern within a text.

Task 4: Algorithmic Techniques

- i) Implement the Strassen's algorithm for matrix multiplication using the divide and conquer approach
- ii) Implement merge sort to count the number of inversions in an array using divide and conquer strategy
- iii) Implement the Huffman coding algorithm for text compression using Greedy technique.

- iv) Implement longest common subsequence among multiple strings using dynamic programming
- v) Solve the coin change problem with a twist: instead of finding the number of ways to make change, find the minimum number of coins needed to make a certain amount

Task 5: Elementary Graph Algorithms

- i) Implement Kruskal's algorithm to find minimum spanning tree of a weighted graph
- ii) Implement Prim's algorithm to find minimum spanning tree using priority queue
- iii) Implement the Bellman-Ford algorithm to find the shortest path from a source vertex to all other vertices, even in graphs with negative-weight edges

Task 6: Network Flow Algorithms

- i) Implement the Ford-Fulkerson algorithm to find the maximum flow in a network. Test it on different flow networks and explore different augmenting path strategies (BFS & DFS)
- ii) Implement the Edmonds-Karp algorithm, a specific implementation of Ford-Fulkerson using BFS for finding augmenting paths
- iii) Implement max-flow min-cut algorithm to image segmentation problems: to partition an image into different segments while minimizing the cut

Task 7: Number Theoretic Algorithms

- i) Implement an algorithm to generate strong pseudoprimes based on the Miller-Rabin primality test
- ii) Implement Pollard's Rho algorithm for integer factorization

Task 8: Probabilistic & Geometric Algorithms

- i) Implement an algorithm generates random passwords using pseudorandom numbers. Users can specify the desired password length and character set
- ii) Implement a basic plane sweep algorithm. Use it to solve a simple geometric problem, such as finding intersections among a set of line segments.

Task 9: Randomization and Linear Programming

- i) Implement a randomized algorithm to select a random subset of elements from a given array with equal probability
- ii) Implement a linear programming model to optimize the construction of a binary search tree with specific access frequencies for the elements. Solve it to find the optimal tree structure.

Part II:**Use Case 1: Emergency Service Dispatch System**

An emergency service organization, such as a fire department or medical response team, needs an efficient system to dispatch emergency vehicles to incidents based on their severity and proximity to the incident location. This system must consider both the urgency of the situation and the availability of nearby vehicles. A combination of hashing and priority queues can be employed to create a real-time emergency service dispatch system. Utilize hashing and priority queue to manage the available emergency vehicles. The priority of each vehicle is determined based on factors such as the vehicle's current location, type of emergency it's equipped to handle, and its availability status.

Develop an algorithm to perform the following operations:

- (i) Real-Time Incident Insertion: As new incidents are reported, hash their locations to determine the appropriate grid cell. Simultaneously, insert the incident into the priority queue based on its severity. The more severe incidents will have higher priority in the queue.
- (ii) Proximity-based Vehicle Assignment: When an incident is reported, retrieve the nearby grid cells using hashing and identify the vehicles available in those cells. Pop the highest-priority vehicle from the queue and assign it to the incident.
- (iii) Dynamic Priority Updates: Update the priority of vehicles in the queue based on their new locations, availability status, and other factors. This ensures that the dispatch system adapts to changing conditions in real-time.

Use Case 2: Network Optimization in Supply Chain Management

A global manufacturing company produces and distributes various products through a complex supply chain network involving multiple suppliers, factories, warehouses, and distribution centers. The company seeks to optimize its supply chain operations to minimize costs and maximize efficiency while meeting customer demands.

Develop and implement an algorithm to perform the following operations:

- (i) Optimal Flow Calculation: Apply network flow algorithms such as the Ford-Fulkerson algorithm or the Edmonds-Karp algorithm to calculate the optimal flow of products through the supply chain network. The goal is to satisfy customer demands while minimizing transportation costs.
- (ii) Minimum Cost Flow: Incorporate transportation costs as edge weights in the graph. Use algorithms like the Minimum Cost Flow algorithm to find the flow that minimizes the total cost of transporting products across the network.

Use Case 3: Tape Storage Optimization

A media production company creates and stores large volumes of video footage for various projects. The company needs an efficient way to store and retrieve video files from tape storage while minimizing the number of tapes used and optimizing data retrieval.

Applying a greedy approach to tape storage optimization can help the media production company efficiently manage their video archive. Develop and implement an algorithm to perform the following operations:

(i) Tape Utilization Greedy Strategy:

Implement a greedy strategy that selects the next video file to store based on the remaining space on the current tape. Choose the file that best fits the available space without wasting significant capacity.

(ii) Greedy File Retrieval:

When retrieving files, use a greedy approach that retrieves files from the tapes with the most free space first. This helps prevent prematurely using tapes with significant storage capacity.

Use Case 4: Approximation Algorithm for Traveling Salesman Problem

A delivery company needs to optimize the routes of its delivery trucks to minimize travel time and fuel costs. The company faces the classic Traveling Salesman Problem (TSP), where a salesman needs to visit a set of cities exactly once and return to the starting city. Implement the approximation algorithm in the delivery company's route planning software. This helps the company optimize routes for its delivery trucks in real-world scenarios.

Develop and implement an algorithm to perform the following operations:

(i) Use the Nearest Neighbor algorithm as an approximation technique. Start from a randomly selected city, and in each step, choose the nearest unvisited city to the current city. Continue until all cities are visited, and then return to the starting city.

(ii) To improve the approximation, consider performing multiple iterations of the Nearest Neighbor algorithm with different starting cities and selecting the best solution among them.

Total: 30 Hours

G. Learning Resources**i. Text Books**

1. Thomas H.Cormen, Charles E.Leiserson, Ronald L. Rivest and Clifford Stein, "Introduction to Algorithms", Fourth Edition, MIT Press, 2022.
2. Ellis Horowitz, Sartaj Sahni, Susan Anderson Freed, "Fundamentals of Data Structure in C", Universities Press,2017.

ii. Reference Books

1. Anany Levitin, "Introduction to the Design and Analysis of Algorithms", Third Edition, Pearson Education, 2017.
2. V. Aho, J. E. Hopcroft, and J. D. Ullman, "Data Structures and Algorithms", Pearson Education, First Edition, Reprint 2017.
3. Narasimha Karumanchi, "Data Structures and Algorithms Made Easy", Fifth Edition, Career Monk, 2021.

iii. Online References

1. “Introduction to Data Structures and Algorithms”. Accessed on Apr. 4. 2020, [Online]. Available: <https://nptel.ac.in/courses/106/102/106102064/>.
2. “Data Structures and algorithms”. Accessed on: Apr. 15, 2021 [Online]. Available: <https://www.coursera.org/specializations/data-structures-algorithms>.

COURSE CODE	COURSE TITLE	L	T	P	C
20231IT302	Advanced Operating Systems Laboratory	0	0	2	1

A. Preamble

This course aims to offer students an introductory exploration of advanced concepts in operating systems design. These tasks aim to explore mutual exclusion, inter-process communication, resource allocation, fault tolerance, client-server applications, task scheduling algorithms, and stateful servers. Through these implementations, students will gain hands-on experience in designing and analyzing essential components of modern computing systems and understand their practical implications in real-world scenarios.

B. Prerequisite Courses

Nil

C. Course Objectives

Learners are exposed to:

- Understand essential algorithms and concepts related to synchronization Mechanisms, Deadlock avoidance.
- Explore and analyze various aspects of distributed systems and client-server applications
- Use performance and monitor tools to trouble shoot windows server.
- Manage File and Disk in UNIX environment.

D. Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Develop algorithms to solve mutual exclusion problem and IPC problems.	K3
CO2	Apply Bakers algorithm to ensure the optimal utilization of resources and prevents system from deadlock.	K3
CO3	Experiment with Performance and monitor tools to enhance Windows Server Performance.	K3
CO4	Organize Files and Disk in UNIX environment.	K3
Knowledge Level (Based on revised Bloom's Taxonomy) K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create		

E. Correlation of Cos with Program Outcomes and Programme Specific Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO12	PSO1	PSO2
CO1	3	3	3	3	3			3	3
CO2	3	3	3	3	3			3	3
CO3	3	3							3
CO4	3	3							3

3- High; 2-Medium; 1-Low

F. Course Contents

Task 1 Implement the Mutual Exclusion Problem Using Dekker's Algorithm. Tools: C/C++/ Java

Task 2 Implement Inter Process Communication Problem (Producer-Consumer / Reader-Writer Problem) Using Semaphores. Tools: C/C++/ Java

Task 3 Implement Banker's algorithm. Tools: C/C++/ Java

Task 4 Implement and study the incremental/decremented growth of response and service times for different number of client and servers for servicing continuous stream(s) of constant sized messages. Tools: C/C++/ Java

Task 5 Implement a name server for registration and identification of services running on another server. Tools: C/C++/ Java

Task 6 Implement a client-server application for a computing problem (of exponential complexity). Compare the performance for a local and remote machine of different speeds. Tools: C/C++/ Java 95

Task 7 Performance and Monitor . Monitoring Reliability and Performance-how to use the Performance Monitor and Resource Monitor to monitor system reliability and performance.

a. Monitoring Events-how to use the Event Viewer tool to monitor events on a Windows Server.

b. Use monitoring tools to establish a performance baseline-As an IT administrator, you have been tasked with identifying the cause of a slow network performance issue in your Windows Server environment. You need to establish a performance baseline and monitor the network to identify potential bottlenecks and areas for optimization. What monitoring tools and techniques can you use to establish a performance baseline and identify potential network performance issues?

c. Optimize performance on Windows 10 clients.-In the lab, you have a Windows 10 client device that is running slow and needs to be optimized for better performance. Use the built-in performance optimization tools and techniques to identify and resolve performance issues, such as disabling unnecessary startup programs, defragmenting the hard drive, and adjusting power settings. Monitor the system performance using Task Manager and other

performance monitoring tools to ensure that the changes have a positive impact on the system's overall performance.

Task 8 Troubleshooting Windows Server . Using Advanced Startup and Windows RE to recover from Boot Failures

- a. Recovering Windows using Reset This PC
- b. Troubleshooting Hardware by Using Windows Memory Diagnostics
- c. Recovering Windows by using a Restore Point

Task 9 File access criteria - users, groups and permissions .

Task 10 Working with Backup using different Backup Tools

- a. Creating, formatting and mounting a partition

Total: 30 Hours

H. Learning Resources

ii. Text Books

1. MukeshSinghal, NiranjanaG.Shivaratri, "Advanced concepts in operating systems: Distributed, Database and multiprocessor operating systems", MC Graw Hill education, 2001.
2. Thomas, Orin. 'Windows server 2019 inside out'. Microsoft Press, 2020.
3. Ken Hess, "Practical Linux System Administration" O'Reilly Media, Inc,2023, ISBN: 9781098109035.

iii. Reference Books

4. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, "Operating System Concepts", Seventh Edition, John Wiley & Sons, 2016.
5. Andrew S.Tanenbaum, "Modern Operating System", Pearson Edition, Fourth Edition, 2016.

iv. Online References

1. Course on "Power of Operating system" ,Aug 2023 [online], Available:<https://www.coursera.org/learn/os-power-user>
2. Course on "Distributed Systems" , Aug 2023 [online],Available: https://onlinecourses.nptel.ac.in/noc23_cs72/preview
3. "Windows Server documentation" , Accessed on Aug, 2023 [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/>

PROGRAM ELECTIVE

COURSE CODE	COURSE TITLE	L	T	P	C
20232IT102	Data Privacy and Security	2	0	0	2

Preamble

This course is to familiarize the students with Basic concepts in security and privacy. This course addresses the security and privacy issues in legacy systems and also covers privacy policies laws, regulations, access control, monitoring, auditing, security information and event management..

B. Prerequisite Courses

20232IT205 - Cryptography and Network Security

C. Course Objectives

Learners are exposed to

- Familiarizes with the basic concepts of privacy in today's environment.
- Demonstrate a detailed of Privacy and Storage security and related Issues.
- Explain the basic concepts of Identity, cloud policy and Access Management.
- Develop the security essentials in IT Sector.
- Know the Monitoring and auditing the applications.

D. Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Understand the concepts of Data privacy and Privacy Policies	K2
CO2	Explain Privacy enabling technologies and Storage Area Network security	K2
CO3	Apply the Access control mechanisms based on role and identity.	K3
CO4	Plan and Organize the protection of data and information system	K3
CO5	Illustrate the proactive monitoring and audit the information systems	K2
Knowledge Level (Based on revised Bloom's Taxonomy) K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create		

E. Correlation of COs with Program outcomes and Programme Specific Outcomes:

Cos	PO1	PO2	PO3	PO4	PO5		PO10	PO11	PSO1	PSO2
CO1	2	2	3							
CO2	3	2	2	2						2
CO3	2	2	2	3					3	2
CO4	2	2	2							2
CO5	3	2	2							2
H- Strong; M-Medium; L-Low										

F. Course Contents

Unit 1 Fundamental of Data Privacy

L-6 Hours

Introduction- Data Privacy Concepts, Data Privacy Attacks, Data linking and profiling, access control models, role-based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy in medical and financial domains.

Unit 2 Privacy and Storage

L-6 Hours

Privacy on the Internet - Privacy Enhancing Technologies - Detection of Conflicts in security policies - privacy and security in environment monitoring systems. Storage Area Network Security - Storage Area Network Security Devices - Risk management - Physical Security Essentials.

Unit 3 Access Control and Identity Management

L-6 Hours

Access control requirements for Cloud infrastructure - User Identification - Authentication and Authorization - Roles-based Access Control - Multi-factor authentication - Single Sign-on, Identity Federation - Identity providers and service consumers - Storage and network access control options - OS Hardening and minimization - Verified and measured boot

Unit 4 Security Management

L-6 Hours

Data Protection strategies: Data retention, deletion and archiving procedures for tenant data, Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key. Components of an Information System, Securing the Components, Balancing Security and Access, Information security essentials for IT Managers.

Unit 5 Monitoring, Auditing and Management**L6 Hours**

Proactive activity monitoring - Incident Response, Monitoring for unauthorized access, malicious traffic, abuse of system privileges - Events and alerts - Auditing – Record generation, Reporting and Management, Tamper-proofing audit logs, Quality of Services, Secure Management, User management, Identity management, Security Information and Event Management.

Total : 30 Hours**G. Learning Resources (in IEEE Format)****i. Text Books:**

1. Brij B. Gupta , Dharma P. Agrawal, H. Wang “Computer and Cyber Security: Principles, Algorithm, Application, and Perspectives”, CRC Press, 2022 (Unit 1,2)
2. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, Seventh Edition, Cengage Learning, 2021 (Unit 3, 4 & 5)

ii. Reference Books:

1. Siani Pearson, George Yee "Privacy and Security for Cloud Computing", Computer Communications and Networks, Springer, 2021.
2. Mather, Kumaraswamy and Latif, Cloud Security and Privacy!, OREILLY 2021

iii. Online References:

- 1.“Misinformation and Privacy” Accessed on Apr. 20, 2022 [Online].

Available: <https://nptel.ac.in/courses/106106146>.

- 2.“Data Privacy and Fundamental”. Accessed on: Apr. 15, 2021 [Online].

Available: <https://www.classcentral.com/course/northeastern-data-privacy-20025>.

COURSE CODE	COURSE TITLE	L	T	P	C
20232IT201	Cloud Security	3	0	2	4

A.Preamble

This course covers the basic concepts of cloud security along with the impacts and governance in infrastructure, data and systems, which are widely used in the design of cloud environment. The Infrastructure security has been categorized into Network, Host and application levels. The Identity and storage management in cloud along with the internal and external compliance of the cloud service providers. The issues related with multi-tenancy operation, virtualized infrastructure security and methods to improve virtualization security along with its applications along with examples are also dealt with in this course.

B.Prerequisite Courses

- 20231IT105-Cryptography and Network Security

C.Course Objectives

Learners are exposed to

- Identify the basic concepts of cloud and its deployments
- Apply the different levels of security in cloud including Network, application and host level
- Utilize security and storage management principles along with the necessity of availability management
- Make use of the concepts of policies and governance associated with cloud and its associated applications
- Utilize the necessity of security as a cloud service and hypervisors

D.Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Identify the basic concept of cloud computing.	K3
CO2	Apply the infrastructure security and data security in cloud	K3
CO3	Identify the concepts of security and storage management in cloud	K3
CO4	Make use of concepts about privacy, audit and compliance in cloud	K3
CO5	Utilize the security-as-a-cloud service and Hypervisor Risks-VM.	K3
Knowledge Level (Based on revised Bloom's Taxonomy) K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create		

E. Correlation of Cos with Program Outcomes and Programme Specific Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PSO 1	PSO2
CO1	1	1		1				
CO2	2		2	2	3			2
CO3	2	2	2	2	3	2		
CO4	2	2			2	2		
CO5	2	2		2	3	2		2

High- 3; Medium-2; Low-1

F. Course Contents**UNIT I Cloud Computing fundamenta****L-9****Hours**

Cloud Computing: SPI Framework for Cloud Computing - Traditional Software Model - Cloud Services Delivery Model - Cloud Deployment Models – Virtual Private Cloud - Key Drivers to Adopting the Cloud- Impact of Cloud Computing on Users - Governance in the Cloud.

UNIT II Infrastructure security at Network, Host and application level**L- 9****Hours**

Infrastructure Security: Web application security – Web attacks - The Network Level: Ensuring Data Confidentiality, Integrity and availability – Amazon RDS - Network-Level Mitigation: SaaS and PaaS Host Security. Host Level: Virtualization Software Security- Threats to the hypervisor - Virtual Server Security: The Application Level: Application Security features and requirements - DoS and EDoS - End User Security – PortSwigger

UNIT III Security and Storage Mangement in Cloud**L-9****Hours**

Security issues: Unauthorized exposure – Data leakage - Security Management Standards Security Management in the Cloud – Identity and access management - Cloud Security Vulnerability - Patch and Configuration Management – Key Management in cloud - Availability Management: SaaS, PaaS, IaaS - Storage as a Service (STaaS) – Amazon EBS and S3

UNIT IV Privacy, Audit and Compliance**L- 9****Hours**

Privacy: Data Life Cycle-Key Privacy Concerns- Responsible for Protecting Privacy- Changes to Privacy Risk Management and Compliance -Legal and Regulatory Implication- U.S. Laws and Regulations - International Laws and Regulations. Audit and compliance: Internal Policy Compliance -Governance, Risk, and Compliance - Control Objectives for Cloud Computing Cloud Security Alliance -Auditing the Cloud for Compliance

UNIT V Security-as-a-cloud-service**L-9 Hours**

Security-as-a-[cloud] service: Origins -Email Filtering - Web Content Filtering - Vulnerability Management- Identity Management-As-a-Service-Impact of cloud computing in corporate- Security policy implementation and Types- Hypervisor Risks-VM Security Recommendations.

Total: 45 Hours

G.Laboratory Experiments

Part 1

Task 1: Install the Oracle VM Virtual box hosted hypervisor and mount an open virtual appliance School of Computing Department of Computer Science & Engineering file over the existing operating system. Tools: Oracle VM

Task 2: Import Kali Linux and mount the instance in the Oracle VM virtual box for implementing SQL map to detect SQL based vulnerabilities in web application. Tools: Oracle VM, Kali Linux

Task 3: Perform the security testing of web applications to identify its attack vectors, using burp suite package imported through kali Linux in Virtual machine. Tools: Oracle VM, Kali Linux

Task 4: Perform a 2FA (two factor authentication) bypass using a brute force attack mechanism using portswigger tool by burpsuite. Tools: Portswigger, Burpsuite

Task 5: Perform a Forced Open authentication profile linking by implementing CSRF attack using Portswigger tool by burpsuite. Tools: Portswigger, Burpsuite

Task 6: Implement URL based and Method based access control in the portswigger tool to circumvent the access control process. Tools: Portswigger, Burpsuite

Task 7: Build a Virtual private cloud in amazon web services environment and launch a web server in the sandbox module of AWS. Tools: Amazon web services

Task 8: Launch an Elastic cloud 2 instance in the amazon web service environment, and manage the instance by modifying the security group, resizing the instance and termination protection processes. Tools: Amazon web services

Task 9: Establish an Amazon EBS volume, attach it to an instance, apply a file system to the volume, and then take a snapshot back up in the sandboxed AWS environment. Tools: Amazon web services

Task 10: Launch an Amazon relational database service and configure the database instance to get interacted with a web application ensuring high availability. Tools: Amazon web services

Total: 30 Hours

Total: 45+30= 75 Hours

G.Learning Resources (in IEEE Format)**Text Books:**

1. Tim Mather, Subra Kumaraswamy, Shahed Latif, “Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance” O'Reilly Media; 1 edition [ISBN: 0596802765], 2009.

Reference Books:

1. Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, 201

Online References:

1. Bob Dill, David Smits. (2022, Nov.) [Online]. Available: <https://www.ibm.com/in-en/cloud/security> [Accessed on 25.11.22]
2. Rana Khalil, Michael Sommer (2023, May) Port Swigger[Online]. Available: <https://portswigger.net/web-security/sql-injection/lab-login-bypass> [Accessed on 18.5.23]

COURSE CODE	COURSE TITLE	L	T	P	C
20232IT202	Blockchain Technology	3	0	2	4

A. Preamble

Blockchain technology has become popularly known because of its use in the implementation of Cryptocurrencies such as BitCoin, Ethereum. The technology itself holds much more promise in various areas such as time stamping, logging of critical events in a system, recording of transactions and trustworthy e-governance. This course covers the technical aspects of public distributed ledgers, blockchain systems, cryptocurrencies, and smart contracts. Students will learn how these systems are built, how to interact with them, how to design and build secure distributed applications.

B. Prerequisite Courses

20231IT201–Network Technologies

C. Course Objectives

Learners are exposed to

Access blockchain applications in a structured manner.

Impart knowledge in block chain techniques and able to present the concepts clearly and structured. To get familiarity with future currencies and to create own crypto token.

D. Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Explain Block chain with types of consensus mechanisms and protocol	K2
CO2	Illustrate the concepts of Cryptocurrency and Smart Contracts to build block chain	K3
CO3	Construct Public, Private and Consortium Block chain System for real time implementation	K3
CO4	Use Initial Coin Offering , security and privacy in block chain with Hyper ledger Fabric	K3
CO5	Implement Blockchain applications in real time using solidity.	K3
Knowledge Level (Based on revised Bloom's Taxonomy) K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create		

E. Correlation of Cos with Program Outcomes and Programme Specific Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2														
CO2	3	3											2		
CO3		3													
CO4					3										
CO5			3		3									3	

High- 3; Medium-2; Low-1

F. Course Contents

Unit 1 Introduction to Blockchain, Types and Consensus Mechanism

9 Hours

Fundamentals of Blockchain- Introduction - Origin of Blockchain -Blockchain Solution - Components of Blockchain - Block in a Blockchain - Technology and the Future
Blockchain Types and Consensus Mechanism - Introduction - Decentralization and Distribution -Types of Blockchain - Consensus Protocol

Unit 2 Cryptocurrency and Smart Contracts

9 Hours

Cryptocurrency – Bitcoin, Altcoin and Token -Bitcoin and the Cryptocurrency- Cryptocurrency Basics - Types of Cryptocurrencies - Cryptocurrency Usage
Smart Contracts - Characteristics of a Smart Contract - Types of Smart Contracts -Types of Oracles - Smart Contracts in Ethereum - Smart Contracts in Industry

Unit 3 Types of Blockchain

9Hours

Public Blockchain System - Popular Public Blockchain - Bitcoin Blockchain -Ethereum Blockchain
Private Blockchain System - Key Characteristics of Private Blockchain – Need of Private Blockchain -Private Blockchain Examples- Private Blockchain and Open Source - Various Commands (Instructions) in E-commerce Blockchain -Smart Contract in Private Environment - State Machine -Different Algorithms of Permissioned Blockchain -Byzantine Fault - Multichain
Consortium Blockchain - Key Characteristics of Consortium Blockchain - Need of ConsortiumBlockchain - Hyperledger Platform -Overview of Ripple - Overview of Corda

Unit 4 Security and Application of Blockchain

9 Hours

Initial Coin Offering - Blockchain Fundraising Methods -Launching an ICO - Investing in an ICO - Pros and Cons of Initial Coin Offering - Successful Initial Coin Offerings - Evolution of ICO - ICO Platforms **Security in Blockchain** - Security Aspects in Bitcoin - Security and Privacy Challenges of Blockchain in General - Performance and Scalability – Identity Management and Authentication Regulatory Compliance and Assurance - Safeguarding Blockchain Smart Contract (DApp) - Security Aspects in Hyperledger Fabric

Unit 5 Development Tools and Frameworks

9 Hours

Blockchain Ethereum Platform using Solidity - Remix IDE -Structure of a Smart ContractProgram -Using Remix to Write and Run a Solidity Program – Modifiers – Events - Arrays inSolidity - Function Visibility - Variable Visibility - Function Modifier Keyword - How FundsAre Accepted - Fallback Function - Contract Inheritance -Contract Communicating with Another Contract - External Libraries - ERC20 Token Transfer - Error Handling in Solidity - ApplicationBinary Interface (ABI) - Swarm (Decentralized Storage Platform) - Whisper (DecentralizedMessaging Platform)

Total: 45 Hours

G. Laboratory Experiments

Total: 30 Hours

Task1: Creating Meta Mask wallet and crypto

- Meta Mask Setup
- Deposit the Crypto
- Make a Transaction and Extracting the transaction details
- Ethereum Transaction

Tool: Meta Mask

Task 2:Implement the Smart Contract using Remix, Solidity

- Working With Variables
- Sending Money
- Starting, Pausing, Stopping and Deleting transaction
- Mapping and Struct
- Error Handling
- View/Pure, Receive Function and Fallback Function
- Inheritance, Modifier and Importing
- Events and Return Variables

Tool: Remix, Solidity

Task 3: Installation and Configuration of Node.js and Web3.js

- Transfer Ether

- Interacting with Smart Contract
- Using Web3.js with Chrome to Interact with Smart Contracts

Tool: Node.js and Web3.js

Task 4: Creating the Hyper Ledger Fabric using solidity

- Create the Fabric Test Network
- ringing up the test network
- Creating a channel
- Starting a chain code on the channel
- Interacting with the network
- Bringing down the network

Tool: Node.js and Web3.js

Task 5: Creating the Shared Wallet using solidity

Task 6: Deploying MEW with Ganache

Task 7: Establish the transaction using Remix with Ganache

Tool: Remix with Ganache

Part 2

Use cases:

Use Case 1: Retail - Establishing unconditional transparency in the food supply chain using blockchain Hyperledger fabric

Use Case 2: Banking and Financial Services – Increasing transaction volume and network resilience while maintaining confidentiality requirements for real time gross settlement among different banks of a central banking consortium

Use Case 3: Healthcare - Electronic health records and medical research data digitization

Use Case 4: Energy and Utilities – Renewable energy trading which are locally owned deliver benefits that are environmentally relevant for the communities involved

Use Case 5: Blockchain in Real-estate – The real estate market currently faces several issues related to housing affordability, rising rate and economy, many of which cannot be addressed with blockchain

Total: 45+30= 75 Hours

H. Learning Resources

i. Text Books:

- 1.Chandramouli Subramanian, Asha A George, Abhilash K A and MeenaKarthikeyan, “Blockchain Technology”, Universities Press,2021(Unit1-Unit5)
- 2.Imran Bashir, “Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained”, Birmingham – Mumbai: Packt, 2nd Edition Kindle, 2018 (Unit 1&2)

ii. Reference Books:

1. Narayanan, Arvind, et al. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016.
- 2.Antonopoulos, Andreas M. Mastering Bitcoin: Programming the Open Blockchain. O'Reilly Media, Inc., 2017.
- 3.Antonopoulos, Andreas M. and Wood, Gavin. Mastering Ethereum. O'Reilly Media,Inc., 2018.

iii.Web Resource(s):

- 1.Ethereum project documentation”, Jan 21 2016, Accessed on: Jan 21 2016 [Online]. Available: <https://ethdocs.org/en/latest/>
- 2.“Monero Research Lab papers” 01 April2014, Accessed on: 01 April 2014 [Online].Available: <https://www.getmonero.org/resources/research-lab/>
3. “ZCash documentation”, 10 Jan 2021 Accessed on: 10 Jan 2021 [Online]. Available:<https://z.cash/>

COURSE CODE	COURSE TITLE	L	T	P	C
20234IT203	Identity Access Management	3	0	2	4

A. Preamble

This course focuses on managing and maintaining Identity of the users in an organization and operations. The course helps the learners to understand the access management and role engineering procedures and policies and their applicability over various contexts and situations. The identity and access management's necessity in a cloud environment are also dealt in the course along with its challenges and operations.

B. Prerequisite Courses

1. Computer Networks / Cyber Security/Database Management Systems

C. Course Objectives

Learners are exposed to

- Understand the basic concepts in identity and access management
- Identify the identity based restrictions created over various organization
- Utilize the access control principles and procedures to get acquainted with role engineering process
- Infer the policies and governance associated with identity and access management
- Identify the necessity of identity and access management in cloud environment

D. Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Understand the concepts and functionalities of identity and access management	K2
CO2	Identify the standards and management of identities in IAM environment	K3
CO3	Utilize the Access management controls and principles for end user access management	K3
CO4	Infer the necessity of Policies and governance in identity and access management	K2
CO5	Identify the importance of Cloud based Identity and access management and its standards	K3
Knowledge Level (Based on revised Bloom's Taxonomy) K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create		

E. Correlation of Cos with Program Outcomes and Programme Specific Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
											1				
CO1		1													
CO2		1	1	1	2										
CO3		1	1	1	2										
CO4		1	1		2										
CO5		1			2										

High- 3; Medium-2; Low-1

F. Course Contents**Unit 1 Introduction****9 Hours**

Cybersecurity and its necessity – Context based Cybersecurity – Types of Cyber threats - Introduction to Identity and access management - IAM Concepts and terms - IAM Architecture - IAM Operational activities – User Identification, Authentication and Authorization –Roles in identity and access management – Identity vs Access management – Functional aspects of IAM – Key Service Components of IAM – IAM Risks - Drivers for Identity and access management

Unit 2 Identity Management**9 Hours**

Digital Identity and ID creation – Identity life cycle - Authentication: Security assertion markup language - Open ID - Open ID Connect Protocol Suite –Types of Digital authentication - Joiner, mover, leaver processes - Authorization: Access control lists - Role based, attribute based and identity based – Active Directory -Lightweight directory access protocol - Open Authentication- Extensible access control markup language –Password Management - Biometrics - Federated identity management - Tomcat Server – DB ServerAuth0 tool – Open VAS tool.

Unit 3 User Access Management**9 Hours**

User management: Service provisioning markup language - User identity and attribute management –Role Engineering -Access Control Models: Discretionary access control – Mandatory access control - Role based access control –Rule based access control — Multi factor Authentication - Privileged access management–Provisioning management and its types - Kerberos authentication protocol for access management –Open SSL- Okta access management tool

Unit 4 IAM Policy Management**9 Hours**

Policy management in IAM - Types of policies: Identity based policy – Resource based Policy - Session Policy –Admin roles vs IAM policies –Admin and Break glass accounts - Effective Permission Boundaries – Difference between rule and policy - Role of IAM in UEM unified endpoint management –Data governance and protection –Auditing and logging - Compliance and Governance administration.

Unit 5 Identity and access management for Cloud**9 Hours**

Cloud Identity and access management - Comparison of Enterprise and Consumer Authentication Standards and Protocols– IAM practices in cloud - Cloud Identity administration: Single Sign on – Federated SSO - Identity management as a service – Cloud Authorization management: Tag based access control - Replication and Disaster recovery – Availability Management in cloud – Access management in AWS Cloud.

Total: 45 Hours**Part-2****Lab tasks:**

Task1: Install and run the tomcat server and DB server and test whether the server is started and running.

Task 2: Create a user identity and manage the credential and its associated vulnerability using green bone security assistant in OpenVAS through Kali Linux Platform.

Task 3: Create and manage keys in ‘Openssl’ for certificate management including identification of certificate information and verification of SSL through Kali Linux.

Task 4: Create multiple user accounts with its credentials and manage to retrieve those created credentials through the command line interface password cracking built-in tool in Kali Linux and audit the passwords.

Task 5: Implement the firewall rules for access control management and create restrictions for ‘services’ based on their ‘names’ and ‘port numbers’ using kali Linux.

Task 6: Create new user accounts and groups and manage the access control/levels of authorization or ownership between different users under each created groups using kali Linux.

Task 7: Getting administrator rights using Burp Suite.

Authentication Bypass: Getting access to server-side script and changing the password and access the server-side applications.

Task 8: Identity management using Auth0

- i) Creation of customer managed policy
- ii) Permit users to manage their credentials

Task 9: Delegate access Management across AWS console using following roles.

- i) User identity creation
- ii) User roles
- iii) Admin roles

Task 10: Manage the access on AWS console and add the created users to different user groups based on which access restrictions will be created to other users using attribute-based access control. Check the Permissions of each user created, using 'IAM users' sign in link in AWS console to check the access restrictions over the instances created over S3, EC2 for validating the access restriction.

Task 11: Develop a web application to use Social Login using open Authentication to authenticate

Task 12: Develop a web application to authenticate using SAML protocol by creating an account with Okta and registering SAML application for authentication.

G. Learning Resources (in IEEE Format)

i. Text Books:

1. Ertem Osmanoglu, "Identity and Access Management: Business performance through connected Intelligence", Second Edition, Syngress, O'Reilly ISBN: 9780124104334 2013.
2. Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy, An Enterprise perspective on risk and compliance", O'Reilly ISBN: 978-0-596-80276-9, 2017.

ii. Reference Books:

1. Ken Hess, "Unified Endpoint management for Dummies", IBM Limited edition Pearson Education, John Wiley and Sons, 2017.
2. Atlice Labs, "Identity and Access Management", by Atlice labs Whitepaper, 2017.

COURSE CODE	COURSE TITLE	L	T	P	C
2023IT204	Forensics in Cyber Security	3	0	2	4

A. Preamble

Forensics in cyber security is a specialized course in the stream of Computer Science & Engineering. This Course gives the comprehensive understanding of computer forensics and investigation tools and techniques in acquisition, recovery, documentation, and analysis of information contained within and created with computer systems and computing devices. Digital evidence methods and standards, techniques and standards for preservation of data, application forensics, web forensics, network forensics, mobile device forensics, and information security audit. This course discusses about various tools, incident response, report writing and gives the introduction about the different digital forensics methods such as network forensics, email forensics, cloud forensics

B. Prerequisite Courses

- 2023IT105-Cryptography and Network Security

C. Course Objectives

Learners are exposed to

- Identify the basic concepts of cloud and its deployments
- Apply the different levels of security in cloud including Network, application and host level
- Utilize security and storage management principles along with the necessity of availability management
- Make use of the concepts of policies and governance associated with cloud and its associated applications
- Utilize the necessity of security as a cloud service and hypervisors

D. Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Outline and Explore the fundamentals of cyber forensic analysis.	K3
CO2	Infer and conduct basic network forensic analysis	K3
CO3	Classify the evidence acquisition and forensics duplication	K3
CO4	Evaluate and validate the types of Forensic tools	K3
CO5	Detect cyber security incidents and its response	K3
Knowledge Level (Based on revised Bloom's Taxonomy) K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create		

E. Correlation of Cos with Program Outcomes and Programme Specific Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PSO ₁	PSO2
CO1	1	1		1				
CO2	2		2	2	3			2
CO3	2	2	2	2	3	2		
CO4	2	2			2	2		
CO5	2	2		2	3	2		2

High- 3; Medium-2; Low-1

F. Course Contents**UNIT I Forensic Science****L-9****Hours**

Principles and Methods: Scientific approach to Forensics, Identification and Classification of Evidence, Location of Evidence: Storage Media, Hard drives, Hardware Interfaces, Recovering Data, Media File Forensic Steps-Forensic Analysis: Planning, Case Notes and Reports, Quality Control

UNIT II Network Forensics**L- 9**

Hours Network forensics overview-Securing a Network- Developing procedures for network forensics- Investigating virtual networks-Examining Honeynet projects-E-mail Investigations: Role of client and server in E-mail, Investigating E-mail crimes and violations, E-mail Servers, E-mail Forensic tools.

UNIT III Digital Forensics Approach and Duplication**L-9 Hours**

Introduction to Forensic Duplication - Rules of Forensic Duplication (Thumb Rule) - Necessity of Forensic Duplication - Forensic Duplicates as Admissible Evidence - Important Terms in Forensic Duplicate - Forensic Duplication Tool Requirements - Creating a Forensic Duplicate of a Hard Drive - Creating a Qualified Forensic Duplicate of a Hard Drive.

UNIT IV Forensics Tools**L- 9 Hours**

Evaluating Forensics Tool Needs- Tasks performed by forensics tools- Forensics Software Tools: Command-line forensic tools, Linux forensic tools- Forensics Hardware Tools: Forensic workstation, Write-Blocker- Validating and Testing Forensics Software

UNIT V Incident Response and Tool**L-9****Hours**

Incidence Response Goals of Incident Response - People Involved in Incident Response Process - Incident Response Methodology - Activities in Initial Response - Phases after

Detection of an Incident - Report Writing and Presentation - Tools: Internet and E-Mail Examinations - Mobile Forensics Tools – Write Blockers -Imaging – Visual Analysis – Secured Storage – Damaged Media.

Total: 45 Hours

G.Laboratory Experiments

Part 1

Task1: Study of Computer Forensics and different tools used for forensic investigation.

Task 2: To extract Exchangeable image file format (EXIF) Data from Image Files.

Task 3: Forensics Case Investigation using live data

Task 4: To Recover Deleted Files using Forensics Tools

Task 5: To Find Last Connected USB on your system

Task 6: To View Last Activities on Your PC

Task7: To analyze network-related incident

Task 8: To make the forensic image of the hard drive to find the suspicious activity

Task 9: To Restore the Evidence Image to find criminal activity

Task 10: To hide and extract any text file behind an image file/ Audio file using Comma

Task 11: To capture the physical memory of a computer and analyze artifacts in memory

Task 12: To Collect Email Evidence in Victim PC

Part 2

Use Cases:

Use case 1: You are on-site, conducting a preliminary examination of a Linux system. The hardware suite includes a 56KB modem. What areas of search should be included in your examination? Prepare an examination plan that details what you will look for, and why.

Use case 2: You receive a Windows OS X system and are asked to summarize the applications and data on the hard drive. In addition, you are asked to report any recent system usage and any signs of encryption, external storage media, or clock tampering.

Use case 3: As a security investigator, you have been asked to determine if company confidential information (intellectual property) has been copied from enterprise computers. Investigation centers on a particular computer that has shown a high volume of network traffic at unusual times. In the course of conducting your investigation you discover that large

capacity removable media has been attached to the suspect computer. A preview examination reveals that software used for secure deletion had been downloaded to the desktop. Prepare an investigative plan listing the lines of investigation that you plan to pursue.

Use case 4: A large accounting MNC company is going to audit certain activities by officers of a medium size, publicly traded bank. During the investigation, the appointed auditor needed to examine several computer systems used by certain Bank employees. After collecting the evidence, the digital forensic examiners were immediately dispatched and sent in to arrange for the formal investigation of those systems to search for corroborating evidence in support of the audit team's suspicions and findings.

Use case 5: Discover you have known the existence of threatening e-mails being sent to the CEO of your company at that time predict will you do the examination of the e-mails revealed that they originated from outside of the country? Describe the steps you would take in your investigation. In particular, address the issue of jurisdiction and locating your counterparts in the target country.

Total: 30 Hours

Total: (45+30)75 Hours

G.Learning Resources (in IEEE Format)

- i. Text Books:**
 - a. Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" O'Reilly Media; 1 edition [ISBN: 0596802765], 2009.
- ii. Reference Books:**
 - a. Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, 201
- iii. Online References:**
 - a. Bob Dill, David Smits. (2022, Nov.) [Online]. Available: <https://www.ibm.com/in-en/cloud/security> [Accessed on 25.11.22]
 - b. Rana Khalil, Michael Sommer (2023, May) Port Swigger[Online]. Available: <https://portswigger.net/web-security/sql-injection/lab-login-bypass> [Accessed on 18.5.23]

COURSE CODE	COURSE TITLE	L	T	P	C
20232IT205	Advanced Routing Techniques and Security	2	0	2	3

A. Preamble

This course covers network configuration, operation, and examining IPv4 and IPv6 networks. It also includes network access, IP connectivity, IP services, network security, automation, and programmability.

B. Prerequisite Courses

1. 20231IT201–Network Technologies

C. Course Objectives

Learners are exposed to

- Examine the Network Configuration.
- Design and optimize the various routing protocols.
- Implement various IP connectivity and services.
- Implement the remote access and authentication protocols.

D. Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Explain the role and function of Routing Configuration.	K3
CO2	Configure IP Routing.	K3
CO3	Interpret the IGRP and EIGRP.	K3
CO4	Dynamic Routing Protocols.	K3
CO5	Border Gateway Protocol.	K3

Knowledge Level (Based on revised Bloom's Taxonomy)

K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create

E. Correlation of Cos with Program Outcomes and Programme Specific Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PSO1	PSO2
CO1	2	2	1				3	
CO2	2	3	2	1			3	
CO3	2	3	2	1			3	
CO4	2	2	2				3	
CO5	2	2	3	1			3	

High- 3; Medium-2; Low-1

F.Course Contents**Unit 1 Routing Configuration****L - 9****Hours**

Introduction: The Internal Components of a Cisco Router and Switch, The Router and Switch Boot Sequence, Configuring DHCP, DHCP Relay, Network Time Protocol, Configuring IP Routing, Static Routing, Default Routing, Dynamic Routing, Routing Protocol Basics, Routing Information Protocol.

Unit 2 IGRP and EIGRP**L-9****Hours**

IGRP (Interior Gateway Routing Protocol) - Configuration, Timers, Loop Avoidance Mechanisms. EIGRP (Enhanced Interior Gateway Routing Protocol) - Neighbors, Topology Table, Packet Types.

Unit 3 Dynamic Routing Protocols**L- 9****Hours**

OSPF (Open Shortest Path First) - Neighbors, Designated Routers, Network Types and Metric. Border Gateway Protocol (BGP) – Peers, Neighbors, Synchronization, Routing Table.

Unit 4 Introduction to Security Hours

L-9

Introduction: Security Trends; Overview of Firewall–Needs for Firewall and Types; Infrastructure security- Port Security, Access Control List, Device Hardening.

Unit 5 Remote Access and Authentication Hours

L- 9

Introduction - Remote Access–Secure socket layer–VPN–IPSEC–Port Address

Translator –Network Address Translator (NAT) –Access policies; Authentication: Authentication- Radius, AD, TACACS, Directory Access Protocol (DAP), Lightweight directory access protocol (LDAP), DAP, Link layer discovery protocol (LLDP).

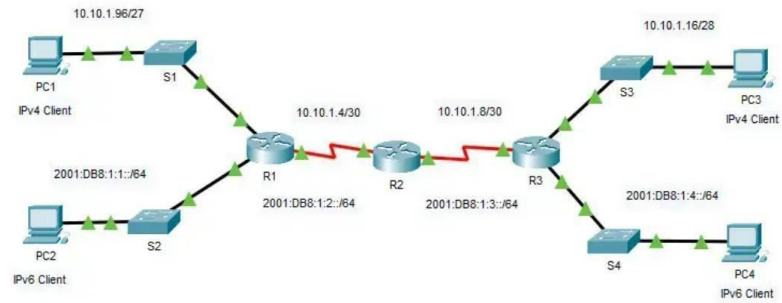
Total: 45 Hours

G. Laboratory Task: Hours

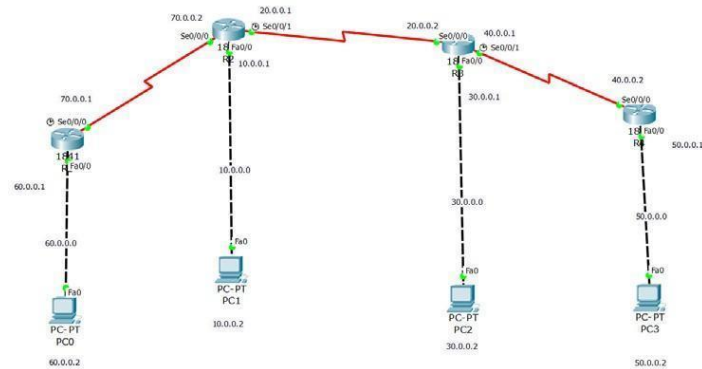
Total: 30

Task 1: Study of network command and configuration commands.

Task 2: Interpreting Ping and Traceroute Output.

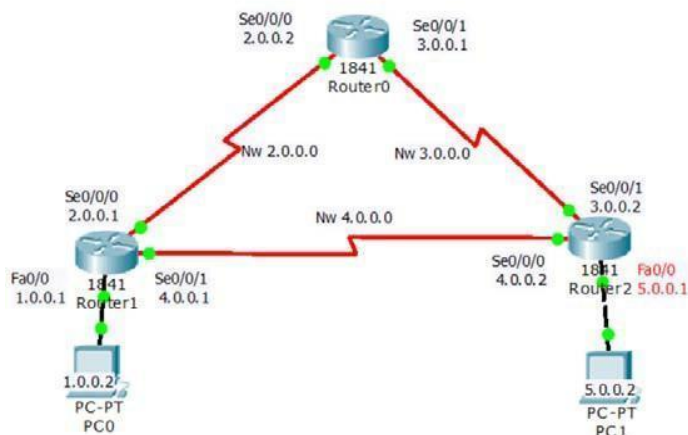


Task 3: Examining and observing Static and Dynamic Routing.

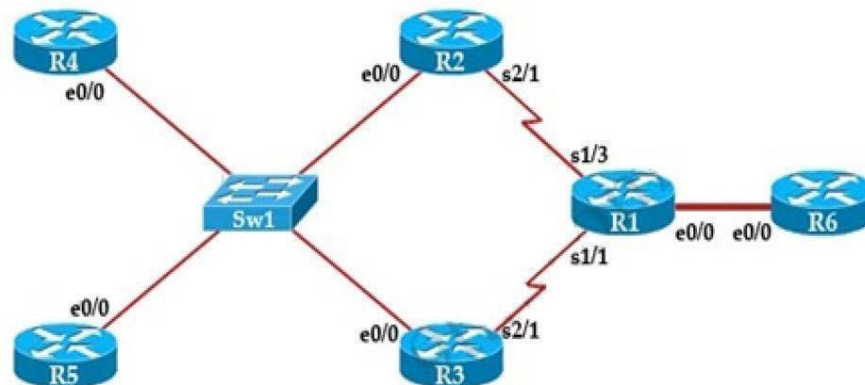


Task 4: Implementing and configuring a Default Route.

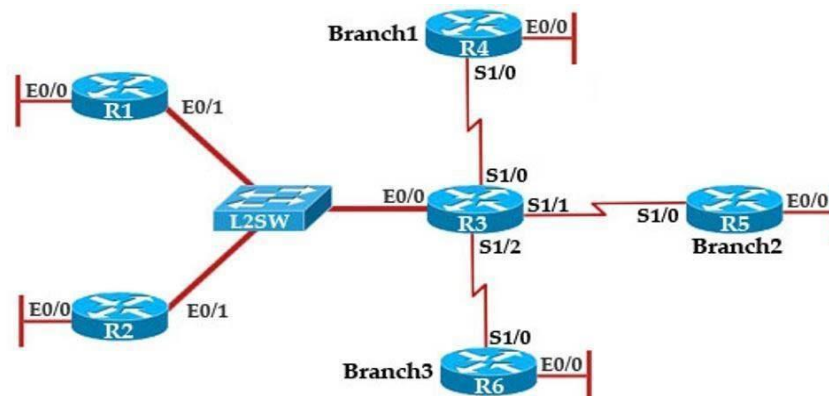
Task 5: Configuring RIP.



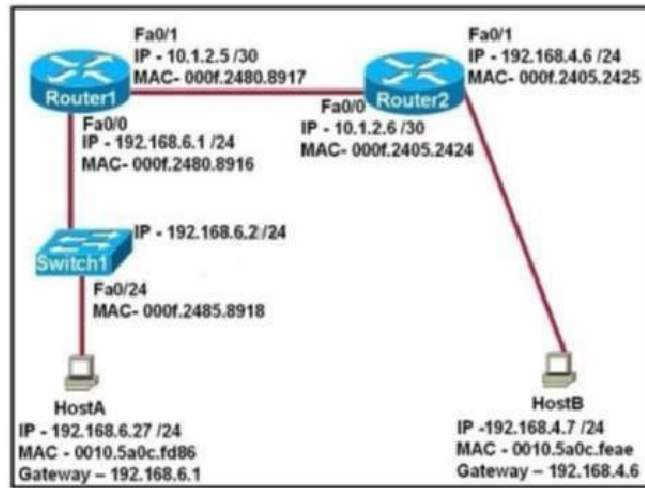
Task 6: The topology below is running EIGRP. You are required to troubleshoot and resolve the EIGRP issues between the various routers. Use the appropriate show commands to troubleshoot the issues.



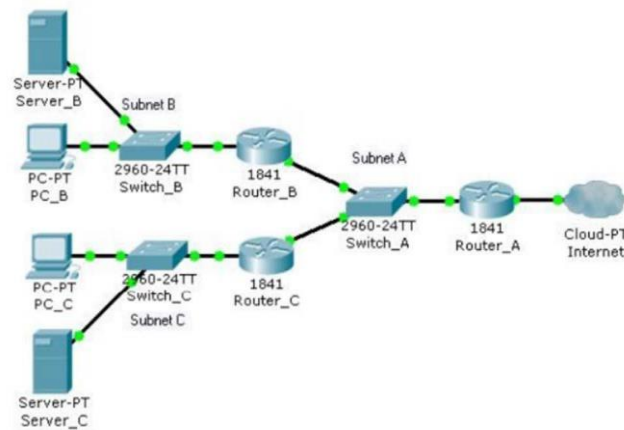
Task 7: The topology below is running OSPF. You are required to troubleshoot and resolve the OSPF issues between the various routers. Use the appropriate show commands to troubleshoot the issues.



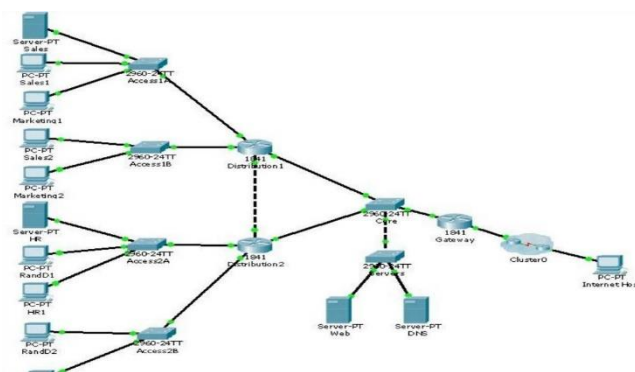
Task 8: After HostA pings HostB, which entry will be in the ARP cache of HostA to support this transmission?



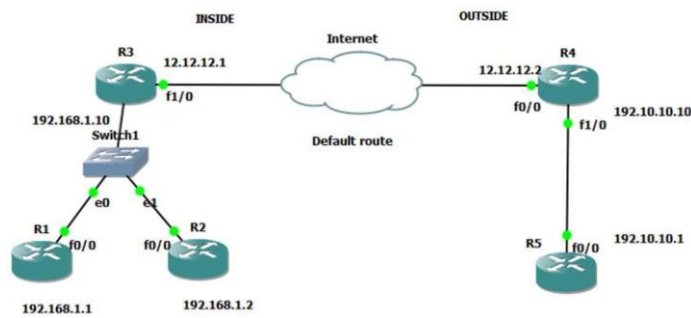
Task 9: Implement Firewall in The Given Network to Enhance Security.



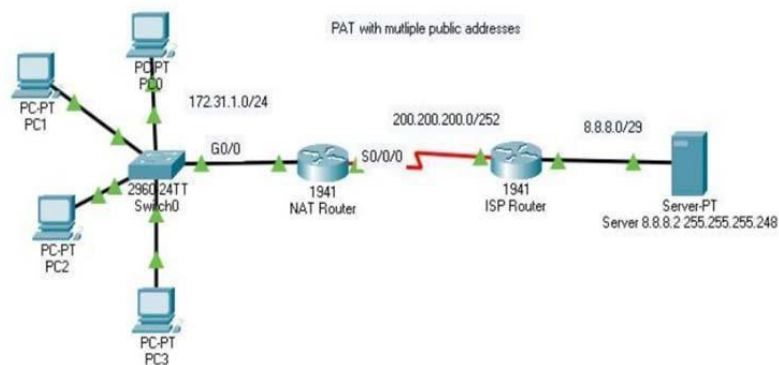
Task 10. Implement The ACLs and verify that the appropriate traffic is permitted or denied.



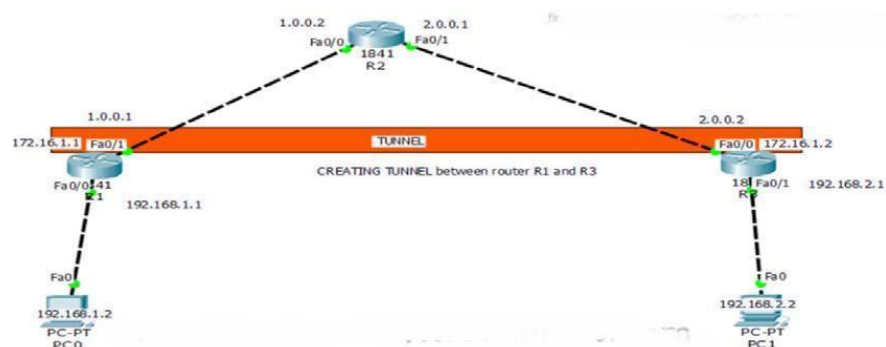
Task 11. Implement the Static NAT.



Task 12. Implement the Static PAT.



Task 13. Implement The VPNtunnels in the network using routers.



G. Learning Resources (in IEEE Format)**i. Text Books:**

1. Behrouz Forouzan, “Data Communications and Networking”, Tata McGraw Hill, 5th Edition, 2021.
2. Kurose and K.W. Ross, “Computer Networking: A Top-Down Approach Featuring the Internet”, Addison-Wesley, 2017

ii. Reference Books:

1. Richard Deal, “CCNA Cisco Certified Network Associate Study Guide”, DOI: 10.1036/0071497285.
2. Todd Lammle, “CCNA Routing and Switching Guide”, Sybex, 2016.

iii Online References:

2. <https://www.gratisexam.com/cisco/200-120/Cisco.Actualtests.200-120.v2014-02-12.by.GillBeast.299q.pdf>
3. <http://examsforall.com/exams/cisco/200-120/Cisco.Actualtests.200-120.v2013-12-09.by.Watson.314q.vce/#.ZD94AXZBzic>
4. <http://ppdi.stmik-banjarbaru.ac.id/data.bc/24.%20Mc%20Graw%20Hill%20Series/McGraw.Hill.Cisco.Certified.Network.Associate.Study.Guide.Ex.pdf>

COURSE CODE	COURSE TITLE	L	T	P	C
2023IT208	Cyber Security Policy, Law and Ethics	4	0	0	4

A.Preamble

This course will enable the students to operate effectively in the cybersecurity governance arena, starting from introduction to cybersecurity by implementing frameworks and developing policy responses to issues that arise with respect to the cyber laws and regulations. The course will give deep insight about the changing nature of cybersecurity threats and the requirement for managers to maintain an up-to-date tool kit in relation to cyber law and policy. The significance of ethics in various cybersecurity applications are catered in this course.

B.Prerequisite Courses

- 2023IT105-Cryptography and Network Security

C.Course Outcomes

Upon the successful completion of the course, students will be able to:

CO No's	Course Outcomes	K - Level
CO1	Interpret the need of Cybersecurity policy and its operation	K3
CO2	Classify the cyber laws and the restrictions in cybersecurity	K3
CO3	Understand the Cybersecurity regulations and risk management	K3
CO4	Infer the vulnerabilities and threats in cybersecurity and exploitation	K3
CO5	Summarize the concept of cyber ethics, and the accountability standards	K3
Knowledge Level (Based on revised Bloom's Taxonomy) K1-Remember K2-Understand K3-Apply K4-Analyze K5-Evaluate K6-Create		

E.Correlation of Cos with Program Outcomes and Programme Specific Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PSO 1	PSO2
CO1	2		2					
CO2			2					
CO3		2	3					
CO4	2	2						
CO5								

High- 3; Medium-2; Low-1

F.Course Contents

Unit 1 Introduction to Cybersecurity**12 Hours**

Essential Terminologies: The hierarchy of standards and policies – Need of Security Policies – Firewall Policy - Host Integrity policy - Service level agreement – Risk based approach – Information Gathering - Collection limitation principles – Transfer and accountability principles - Social Engineering. Case study: Scan a network and determine whether the remote host has a firewall enabled.

Unit 2 Cyber Laws**12 Hours**

Introduction to Cyber Law - An Overview of Cyber law in India - Cybercrime and Legal perspectives - Need of Improvement in Indian Cyber Law - International perspective on Cyber Laws – Investigations on Cyber laws – Phases of digital crime investigation - Governance of cybercrime and the internet - Corporate policy- Policy framework – Intellectual property issues – Legal aspects of Digital contracts. Case study: Reporting of network breach in sensitive domains such as banks and their impact in cyber laws

Unit 3 Cyber Security Regulations**12 Hours**

Introduction - Roles of International Law - the state and Private Sector in Cyberspace - Cyber Security Standards - National Cyber Security Policy - Continuous improvement principles - Privacy Acts- ISO/IEC 27,000 – Systrust – Webtrust – Statement on auditing standards 70 – Sabanes oxley Act – HIPAA - Information Technology Act -Information Security Governance and Risk Management – NIST: Standard reference data – National Vulnerability database

Case Study on implementation of secure architecture for financial services adhering to the regulations

Unit 4 Cybercrimes and laws**12 Hours**

Introduction – Cyberattack - An Important Commonality for Exploitation and Attack - Inherent Vulnerabilities of Information Technology –Cyber Lawyers – Cyber law advantages – Two sides of cyber law – Computer crime and insecurity – IT amendment act 2008 – Role of Computer emergency response team (CERT) – Digital products and federal policy – Intellectual property rights considerations – Bayh-Dole Act – Patents and Trade secrets on digital products.

Unit 5 CyberEthics**12 Hours**

Introduction to dimensions of cyberethics in cybersociety – Significance of Cyberethics- Corevalues and virtues – Cyberethics by norms, laws and relations – Artificial Intelligence Ethics: AI for good – Ethics in information society: Nine P's- CyberBullying – Limiting

access of technology – Accountability and Liability. Case study: Analyse and judge the cybercrimes in e-commerce and social media.

Total: 60 Hours

G.Learning Resources (in IEEE Format)

Text Books:

1. Jeff Kosseff, “Cybersecurity Law”, ISBN: 978-1-119-23150-9, Wiley Publications, 2017. (Unit II, III, IV)
2. David Clark, Thomas Berson and Herbert, “At the Nexus of Cybersecurity and public policy, Basic concepts and issues”, National academic press, ISBN 13: 978-0-309-30318-7, 2014. (Unit I, IV)
3. Christopher Stuckelbergerc, Pavan Duggal, “Cyber Ethics 4.0, Serving humanities with values”, Globalethics publications 4th edition, ISBN 978-2-88931-265-8 2018 (Unit V)

Reference Books:

1. Joakim Kavrestad, “Fundamentals of digital forensics, theory, methods, and real life applications”, Second Edition, ISBN 978-3-030-38954-3, Springer, 2020

Online References:

1. “Cybersecurity”. Accessed on: June 20, 2021 [Online]. Available: <https://www.nap.edu/catalog/18749/at-the-nexus-of-cybersecurity-and-public-policy-some-basic>.
2. “ISO 27000 standards”. Accessed on: June 15, 2021 [Online]. Available: <https://www.iso.org/standards.html>.
3. “Cyber Conflicts”. Accessed on: June 20, 2021 [Online]. Available: <https://www.coursera.org/lecture/cyber-conflicts/introduction-to-cybercrime-and-fundamental-issues-xndSq>.
4. “Cyber Laws”. Accessed on: July 2, 2021 [Online]. Available: <https://www.cyberlawsindia.net/2sides.html>

