MINOR DEGREES OFFERED UNDER SVEC-19 REGULATIONS

Offering Dept.	Title of the Minor	Students of Eligible Branches
CSE	Artificial Intelligence and Machine Learning	All branches except CSE, IT and CSSE
IT	Internet of Things	All branches except IT
CSSE	Cyber Security	All branches except CSE, IT and CSSE
ECE	VLSI and Embedded Systems	All branches except ECE
EEE	Power Systems and Drives	All branches except EEE
EIE	Instrumentation and Control Engineering	All branches except EIE
ME	Robotics	All branches except ME
CE	Sustainable Engineering	All branches except CE

Academic Regulations for Minor Degree:

The concept of Minor degree is introduced in the curriculum of all B.Tech. programs offering a Major degree. The main objective of Minor degree in a discipline is to provide additional learning opportunities for academically motivated students and it is an optional feature of the B.Tech. Program. To earn a Minor degree in a discipline, a student has to earn 18 extra credits (By studying FIVE theory & THREE laboratory courses or SIX Theory Courses) from the core courses of the minor discipline.

a. Students having a CGPA of 8.0 or above up to II B.Tech I-Semester without any backlogs shall be permitted to register for a Minor degree by paying the requisite fee.

b. In the subsequent semesters, the student has to pass all the courses registered for Major and Minor Degrees in the first attempt i.e., regular examinations without any backlog to keep the Minor Degree registration active or else it shall be cancelled.

c. If a student becomes ineligible for continuing the Minor Degree, the earned credits under Minor Degree cannot be transferred to Major

Degree; they will remain extra. These additional courses will be mentioned in the transcript. However, they are eligible to receive B.Tech. Degree after satisfying its requirements.

d. The evaluation pattern of the courses shall be similar to the evaluation of regular program courses.

e. Minimum strength required for offering Minor Degree in a discipline is 40 students.

f. A student registered for Minor degree shall pass in all subjects that constitute the requirement for the Minor degree program. No class/division (i.e., second class, first class and distinction, etc.) shall be awarded for Minor degree program.

g. The Minor degree shall be mentioned in the degree certificate as Bachelor of Technology in XXX with Minor in YYY. For example, Bachelor of Technology in Computer Science & Engineering with Minor in Title of the Minor Pursued. This shall also be mentioned in the transcripts, along with the list of courses taken for Minor degree program. However, the performance of the student in the Minor courses will not be considered for the calculation of SGPA and CGPA for the award of Major Degree.

h. Separate course/class work and time table shall be arranged for the various Minor degree programs. Attendance regulations for these Minor discipline programs shall be as per regular courses.

i. Students aspiring for Minor degree must register from III B.Tech I-Semester onwards and must opt for a Minor in a discipline other than the discipline he is registered in.

j. A Student shall register for Minor with the following combinations:

Offering Theory and Laboratory Courses: SEVEN credits in a semester starting from III B.Tech I-Semester to III B.Tech II-Semester (TWO theory & ONE laboratory courses) and FOUR credits in IV B.Tech I-Semester (ONE theory & ONE laboratory courses).

Offering Theory Courses only: SIX credits in a semester starting from III B.Tech I-Semester to IV B.Tech I-Semester (TWO theory courses).

NOTE: Interested meritorious students shall be permitted to register either for a Minor degree in a discipline (or) Honors Degree in a discipline only, but not both.

MINOR DEGREE IN
CYBER SECURITY

Offering Department: COMPUTER SCIENCE AND SYSTEMS ENGINEERING
Students of Eligible Branches: ECE, EEE, EIE, ME and CE

COURSE STRUCTURE

Year & Semester	Course Code	Course Title	Contact Periods per week				C	Scheme of Examination Max. Marks		
			L	T	P	Total		Int. Marks	Ext. Marks	Total Marks
III B.Tech. I-Sem (2 Theory + 1 Lab)	19BM51501	Computer Networks	3	-	-	3	3	40	60	100
	19BM51502	Ad hoc and wireless Sensor Networks	3	-	-	3	3	40	60	100
	19BM51503	Operating Systems	3	-	-	3	3	40	60	100
	19BM51531	Computer Networks Lab	-	-	2	2	1	50	50	100
III B.Tech. II-Sem (2 Theory + 1 Lab)	19BM61501	Cloud Computing	3	-	-	3	3	40	60	100
	19BM61502	Modern Cryptography	3	-	-	3	3	40	60	100
	19BM61503	Cyber security	3	-	-	3	3	40	60	100
	19BM61531	Modern Cryptography Lab	-	-	2	2	1	50	50	100
IV B.Tech. I-Sem (1 Theory + 1 Lab)	19BM71501	IoT Security	3	-	-	3	3	40	60	100
	19BM71502	Information Security	3	-	-	3	3	40	60	100
	19BM71531	Information Security Lab	-	-	2	2	1	50	50	100

Note: If any student has chosen a course from the above list in their regular curriculum then, he/she is not eligible to opt the same course/s for the Minor degree. It is the responsibility of the student to acquire/complete prerequisite before taking the respective course.

III B. Tech. - I Semester
(19BM51501) COMPUTER NETWORKS

Int. Marks	Ext. Marks	Total Marks	L	T	P	C
40	60	100	3	-	-	3

PRE-REQUISITES: -

COURSE DESCRIPTION: Introduction to computer networks; Protocols of physical layer, data link layer, medium access control sub layer, network layer, transport layer, application layer.

COURSE OUTCOMES: After successful completion of this course, the students will be able to:

CO1. Analyze the types of network topologies, layers and protocols.
CO2. Evaluate subnetting and routing algorithms for finding optimal paths in networks.
CO3. Solve problems related to flow control, error control and congestion control in data transmission.
CO4. Assess the impact of wired and wireless networks in the context of network protocols Like DNS, SMTP, HTTP, and FTP.
CO5. Apply ethical principles and standards for developing network-based solutions.

DETAILED SYLLABUS:

UNIT- I: INTRODUCTION AND PHYSICAL LAYER (09 Periods)

Network hardware, Network software, Reference models - OSI, TCP/IP; Example networks – Internet; Wireless LANs - 802.11.

Physical Layer - Guided transmission media, Wireless transmission, Switching - Circuit switching, Packet switching.

UNIT- II: DATA LINK LAYER AND MEDIUM ACCESS CONTROL SUBLAYER (09 Periods)

Data Link Layer: Data link layer design issues, Error detection and correction - CRC, Hamming codes; Elementary data link protocols, Sliding window protocols.

Medium Access Control Sub layer: ALOHA, Carrier sense multiple access protocols, Collision free protocols, Ethernet, Data link layer switching - Repeaters, Hubs, Bridges, Switches, Routers, Gateways.

UNIT- III: NETWORK LAYER (09 Periods)

Network layer design issues, Routing algorithms - Shortest path algorithm, Flooding, Distance vector routing, Link state routing, Hierarchical routing, Broadcast routing, Multicast routing, Anycast routing; Congestion control algorithms, Network layer in the internet - The IP version 4 protocol, IP addresses, IP version 6, Internet control protocols, OSPF, BGP.

UNIT- IV: TRANSPORT LAYER (09 Periods)

UDP – Segment header, Remote procedure call, Real-time transport protocols; TCP – service model, Protocol, Segment header, Connection establishment, Connection release, Sliding window, Timer management, Congestion control.

UNIT- V: APPLICATION LAYER (09 Periods)

Domain Name System (DNS) - Name space, Domain resource records, Name servers; Electronic mail - Architecture and services, User agent, Message formats, Message transfer, Final delivery; The World Wide Web - Architectural overview, HTTP, FTP.

Total Periods: 45

Topics for self-study are provided in the lesson plan

TEXT BOOK(S):

1. Andrew S. Tanenbaum and David J. Wetherall, *Computer Networks*, Pearson, 5th Edition, 2015.

REFERENCE BOOKS:

1. Behrouz A. Forouzan, *Data Communications and Networking*, McGraw Hill, 5th Edition, 2013.
2. James F. Kurose and Keith W. Ross, *Computer Networking: A Top-Down Approach*, Pearson, 7th Edition, 2017.

ADDITIONAL LEARNING RESOURCES:

1. https://www.cisco.com/c/en/us/solutions/small-business/resourcecenter/networking/networking-basics.html
2. https://memberfiles.freewebs.com/00/88/103568800/documents/Data.And.Computer.Communications.8e.WilliamStallings.pdf

CO-PO and PSO Mapping Table:

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	2	-	-	-	-	-	-	-	-	-	-	-	3
CO2	3	2	-	3	-	-	-	-	-	-	-	-	-	-	3
CO3	3	2	-	2	-	-	-	-	-	-	-	-	-	-	3
CO4	-	-	-	-	-	2	-	-	-	-	-	-	-	-	3
CO5	-	-	-	-	-	-	-	3	-	-	-	-	-	-	3
Average	3	2.3	2	2.5	-	2	-	3	-	-	-	-	-	-	3
Level of correlation of the course	3	3	2	3	-	2	-	3	-	-	-	-	-	-	3

Level of Correlation: 3 - High 2 - Medium 1 - Low

III B. Tech. – I Semester
(19BM51502) AD HOC AND WIRELESS SENSOR NETWORKS

Int. Marks	Ext. Marks	Total Marks	L	T	P	C
40	60	100	3	-	-	3

PRE-REQUISITES: -

COURSE DESCRIPTION: Ad hoc Wireless Networks, Medium Access Control Protocols for Ad hoc Wireless Networks, Routing Protocols for Ad hoc Wireless Networks, Wireless Sensor Networks, Medium Access Control Protocols for WSN's.

COURSE OUTCOMES: *After successful completion of the course, students will be able to:*

CO1. Investigate ad hoc and wireless sensor networks to improve the network performance.
CO2. Analyze the issues in MAC, routing protocols in Ad hoc wireless networks.
CO3. Apply routing protocols of MAC Layer in sensor networks to provide networking solutions.
CO4. Follow norms and standards in engineering practice to solve ad hoc and wireless sensor network problems.

DETAILED SYLLABUS:

UNIT–I: AD HOC WIRELESS NETWORKS (08 Periods)

Fundamentals of wireless communication technology, the electromagnetic spectrum, Radio propagation mechanisms, Characteristics of the wireless channel, Applications, Issues, Ad hoc wireless Internet.

UNIT–II: MAC PROTOCOLS FOR AD HOC WIRELESS NETWORKS (08 Periods)

Issues in designing a MAC protocol, Classification of MAC protocols, Contention based protocols, Contention based protocols with reservation mechanisms, and Contention based protocols with scheduling mechanisms.

UNIT–III: ROUTING PROTOCOLS FOR AD HOC WIRELESS NETWORKS (09 Periods)

Issues in designing routing and transport layer protocol for Ad hoc networks, Classification of routing protocols, Table driven routing protocols, On demand routing protocols, Hybrid routing protocols.

UNIT–IV: WIRELESS SENSOR NETWORKS (09 Periods)

Vision of ambient intelligence, Application examples, Types of applications, Challenges of WSN's, Why are sensor networks different, Enabling technologies, Hardware components, Energy consumption of sensor nodes.

UNIT–V: MEDIUM ACCESS CONTROL PROTOCOLS FOR WIRELESS SENSOR NETWORKS (11 Periods)

Fundamentals of MAC protocols, Low duty cycle protocols and wake up concepts, Contention based protocols, Schedule based protocols, IEEE 802.15.4 MAC protocol, 802.11 and Bluetooth, Case study on tele healthcare – Introduction, MASN hardware design, Reliable MASN communication protocols, MASN software design, Integration of RFID and wearable sensors.

Total Periods: 45

Topics for self-study are provided in lesson plan

TEXT BOOKS:

1. C. Siva Ram Murthy, B.S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*, Pearson, 2012.
2. Holger Karl and Andreas Willig, *Protocols and Architectures for Wireless Sensor Networks*, Wiley, 2017.

REFERENCE BOOKS:

1. Fei Hu and Xiaojun Cao, *Wireless Sensor Networks: Principles and Practice*, CRC Press, 2010.
2. Yi Qian, Peter Muller and Hsiao–Hwa Chen, *Security in Wireless Networks and Systems*, Wiley, 2011.

ADDITIONAL LEARNING RESOURCES:

1. https://www.tyndall.ie/wireless-sensor-networks-2
2. https://www.elprocus.com/introduction-to-wireless-sensor-networks-types-and-applications/
3. https://www.analog.com/en/design-center/landing-pages/002/apm/wsn-solution-2014.html

CO-PO and PSO Mapping Table:

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	-	-	-	-	-	-	-	-	-	-	-	-	-
CO2	3	3	2	-	-	-	-	-	-	-	-	-	-	-	-
CO3	2	2	1	-	-	-	-	-	-	-	-	-	-	-	-
CO4	-	-	-	-	-	2	-	2	-	-	-	-	-	-	-
Average	2.6	2.3	1.5	-	-	2	-	2	-	-	-	-	-	-	-
Level of correlation of the course	3	3	2	-	-	2	-	2	-	-	-	-	-	-	-

Level of Correlation: 3 - High 2 - Medium 1 - Low

III B. Tech. – I Semester
(19BM51503) OPERATING SYSTEMS

Int. Marks	Ext. Marks	Total Marks	L	T	P	C
40	60	100	3	-	-	3

PRE-REQUISITES: -

COURSE DESCRIPTION: Operating Systems Operations; Process Scheduling; Process Synchronization, Deadlocks; Paging and Segmentation, Disk Scheduling; File Concepts, I/O Interface; Concepts of Protection and Security.

COURSE OUTCOMES: *On successful completion of this course, the students will be able to:*

CO1. Analyze performance of CPU scheduling algorithms.
CO2. Design solutions for process synchronization problems by using semaphores and monitors.
CO3. Devise solutions for deadlocks using deadlock handling mechanisms.
CO4. Solve memory management problems using page replacement and disk scheduling algorithms.
CO5. Identify efficient file allocation methods for optimal disk utilization.
CO6. Analyze services of I/O subsystems and mechanisms of security & protection.

DETAILED SYLLABUS:

UNIT I: INTRODUCTION TO OPERATING SYSTEM AND PROCESS MANAGEMENT (08 Periods)

INTRODUCTION: Definition, Operating System Structure and Services, System Calls.

PROCESS MANAGEMENT: Process Scheduling, Process Control Block, Inter Process Communication, Threads, Multithreading Models, CPU Scheduling Criteria, Scheduling Algorithms, Multiprocessor Scheduling.

UNIT II: PROCESS SYNCHRONIZATION AND DEADLOCKS (10 Periods)

PROCESS SYNCHRONIZATION: Critical Section Problem, Peterson's Solution, Synchronization Hardware, Semaphores, Synchronization Problems, Monitors.
DEADLOCKS: System Model, Deadlock characterization, Methods for handling deadlocks, Prevention, Detection, Avoidance, Recovery from deadlock.

UNIT III: MEMORY MANAGEMENT AND SECONDARY STORAGE (10 Periods)

MEMORY MANAGEMENT: Swapping, Contiguous Allocation, Paging, Segmentation, Segmentation with Paging.

VIRTUAL MEMORY: Demand Paging, Page Replacement Algorithms, Copy-on-Write, Thrashing.
SECONDARY STORAGE STRUCTURE: Overview of Mass Storage Structure, Disk Structure, Disk Scheduling, Disk Management.

UNIT IV: File and I/O Systems (08 Periods)

FILE SYSTEM: File concept, Access Methods, Directory Structure, File System Structure, i-node, File System Implementation, Directory Implementation, Allocation Methods.
I/O SYSTEM: I/O Hardware, Application I/O Interface, Kernel I/O subsystem

UNIT V – PROTECTION AND SECURITY (09 Periods)

PROTECTION: Goals, Principles, Domain of Protection, Access Matrix, Implementation of Access Matrix, Access Control, Revocation of Access Rights.

SECURITY: Security Problem, Program Threats, System and Network Threats, User Authentication, Implementing Security Defenses, Firewalling to Protect Systems and Networks, Computer-Security Classifications.

Total Periods: 45

Topics for Self Study are provided in Lesson Plan

TEXT BOOKS:

1. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, *Operating System Concepts*, Wiley India Edition, 9th Edition, 2016.

REFERENCE BOOKS:

1. William Stallings, *Operating Systems, Internals and Design Principles*, Pearson Education, 7th Edition, 2013.
2. Andrew S. Tanenbaum, *Modern Operating Systems*, PHI, 3rd Edition, 2009.

CO-PO and PSO Mapping Table:

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2	3	2	2	2	-	-	-	-	-	-	-	3	-	-
CO2	2	2	3	-	2	-	-	-	-	-	-	-	3	-	-
CO3	2	2	3	-	2	-	-	-	-	-	-	-	3	-	-
CO4	2	2	3	-	2	-	-	-	-	-	-	-	3	-	-
CO5	3	3	-	-	-	-	-	-	-	-	-	-	3	-	-
CO6	2	3	-	3	-	-	-	-	-	-	-	-	3	-	-
Average	2.16	2.5	2.75	2.5	2	-	-	-	-	-	-	-	3	-	-
Level of correlation of the course															

Level of Correlation: 3 - High 2 - Medium 1 - Low

III B. Tech. - I Semester
(19BM51531) COMPUTER NETWORKS LAB

Int. Marks	Ext. Marks	Total Marks	L	T	P	C
50	50	100	-	-	2	1

PRE-REQUISITES:A course on Computer Networks

COURSE DESCRIPTION: Hands on practice with NS3; Packet Tracer network simulation tools; Simulation of network topologies; ARP protocol; CSMA/CD protocol; Distance Vector/Link State Routing protocols; Transmission errors; Sliding window protocol; TCP; UDP.

COURSE OUTCOMES: *After successful completion of this course, the students will be able to:*

CO1. Apply mathematical foundations to solve computational problems in computer networks.
CO2. Select and apply network simulation tools like NS3, Packet Tracer to simulate networking protocols.
CO3. Simulate and analyze network topologies, network protocols to provide efficient networking solutions.
CO4. Work independently and communicate effectively in oral and written forms.

LIST OF EXERCISES:

1. a) Study of network devices and network IP in detail.
   b) Simulate a peer to peer topology of a computer network.
   c) Simulate IPv4 addressing in a computer network (give IP Address of different classes in given Network id).

Exercises on Packet Tracer Simulator Tool:

2. Introduction to Packet Tracer
3. a) Study of basic network commands and network configuration commands.
      i) ping ii) nslookup iii) netstat iv) ifconfig
   b) Create a network topology and configure a network topology with four PCs, two switches, and two routers.

Exercises on NS3 Simulator Tool:

4. a) Introduction to NS3 tool.
   b) Create a network with three nodes namely 0, 1 and 2. Establish a TCP connection between node 0 and node 2 such that node 0 will send TCP packets to node 2 via node 1.
5. a) Create a simple topology of two nodes (Node1, Node2) separated by a point-to-point link. Setup a UDP Client on one Node1 and a UDP Server on Node2. Consider a fixed data rate Rate1.
      i) Measure end to end throughput whilst varying the latency of the link.
      ii) Add another client application to Node1 and a server instance to Node2. What do you need to configure to ensure that there is no conflict?
      iii) Repeat step 3 with the extra client and server application instances. Show screenshots of pcap traces which indicate that delivery is made to the appropriate server instance.

b) Simulate a Local Area Network. Consider a local area network formed by nodes 3, 4, and 5. This LAN communicates with the external world through a router denoted by node 2. There are two servers connected to the router and represented by nodes 0 and 1. Node 0 is running an application over TCP, which is accessed by node 4. Node 1 is running an application on UDP, which is accessed by node 5. Analyze the trace file.

6. Simulate link errors. Presence of link errors cause one or more packets to be retransmitted. Consider the following topology.

Node #2 act as a router. Any traffic to or from the LAN passes through it. Consider node #1 running a FTP server, and node #5 is downloading a file of size 4 MB. However, the link between node #2 and #3 is fault. It drops packets with a fixed probability of 0.2. Implement a link error model to reflect this. Try different values of the simulation time to ensure that the file has been entirely transferred. Has the plot of bytes received a linear curve or non-linear? Why?

7. Simulate Address Resolution Protocol (ARP) to associate a logical address with a physical address and Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address.

8. Simulate packet transmission over a CSMA/CD based LAN with NS3. Consider the LAN with seven nodes to be an isolated one i.e. not connected to the Internet. Node #0 in the LAN acts as a UDP traffic source, and node #6 is the destination node. Assume CBR traffic to be flowing between the nodes. The simulation lasts for 25 seconds. In Ethernet a packet is broadcasted in the shared medium, and only the destination node accepts the packet. Other nodes simply drop it. What should be the number of hops a packet from node #0 to node # 6 travel? Verify this from the "Hop Count" plot.

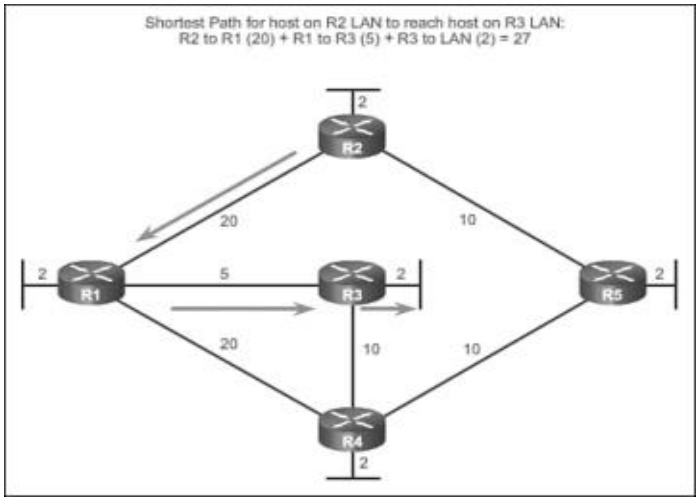
9. a) UDP uses a simple connectionless communication model with a minimum of protocol mechanism. The implementation provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. Simulate half duplex chat User Datagram Protocol.

   b) TCP model supports a full bidirectional TCP with connection setup and close logic. Simulate full duplex chat Transmission Control Protocol.

10. a) In a typical FTP session, the user is sitting in front of one host (the local host) and wants to transfer files to or from a remote host. Implement File Transfer Protocol
    to move files between local and remote file systems.

    b) Sliding window protocol supports reliable and efficient transmission between nodes and it also obtains higher throughput than that of stop-n-wait protocol. Simulate sliding window protocol normal operation and timeout operations.

11. Configure the following network to find shortest path between R2 LAN to R3 LAN using Distance Vector / Link State Routing Protocol.



REFERENCE BOOKS:

1. Andrew S. Tanenbaum and David J. Wetherall, *Computer Networks*, Pearson, 5th Edition, 2015.
2. A. Jesin, *Packet Tracer Network Simulator*,Packt Publishing, 2014.
3. Jack L. Burbank, *An Introduction to Network Simulator 3,* Wiley, 2018.

Software/Tools used:

1. Network simulator tools - NS3, Packet Tracer
2. Virtual Labs (Computer Networks Lab – http://vlabs.iitb.ac.in/vlabs-dev/labs_local/ computer-networks/ labs/explist.php)
3. Virtual Labs (Advanced Network Technologies Virtual Lab - http://vlabs.iitkgp.ernet.in/ant)

CO-PO and PSO Mapping Table:

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	-	-	-	-	-	-	-	-	-	-	-	-	-
CO2	-	-	-	-	3	-	-	-	-	-	-	-	-	-	-
CO3	1	3	3	3	3	-	-	2	-	-	-	-	-	-	-
CO4	-	-	-	-	-	-	-	3	3	-	-	-	-	-	-
Average	2	3	3	3	3	-	-	2	3	3	2	-	-	-	-
Level of correlation of the course	3	2	-	-	-	-	-	-	-	-	-	-	-	-	-

Level of Correlation: 3 - High 2 - Medium 1 - Low

III B. Tech. – II Semester
(19BM61501) **CLOUD COMPUTING**

Int. Marks	Ext. Marks	Total Marks	L	T	P	C
40	60	100	3	-	-	3

PRE-REQUISITES: -

COURSE DESCRIPTION: Fundamental Cloud Computing and Virtualization; Understanding Cloud Models and Architectures; Understanding Cloud Services, Applications and Capacity Planning; Exploring Platform as a Service (PaaS); Exploring Infrastructure as a Service (IaaS).

COURSE OUTCOMES: After successful completion of this course, the students will be able to:

CO1. Demonstrate knowledge on basic concepts and terminologies of Cloud Computing and Virtualization.
CO2. Select appropriate Cloud deployment models, Service models and Architectures in Cloud Application development.
CO3. Analyze Cloud services, Applications and Capacity Planning.
CO4. Apply different PaaS application frameworks to construct Cloud applications.
CO5. Develop web applications through Google, Microsoft and Amazon web services as per societal needs.

DETAILED SYLLABUS:

UNIT I–FUNDAMENTAL CLOUD COMPUTING AND VIRTUALIZATION (10 Periods)

Cloud Computing: Origin and influences, Basic concepts and terminology, Goals and benefits, Risks and challenges, Roles and boundaries and Cloud characteristics.

Introduction to Virtualization: Characteristics, Taxonomy of virtualization technologies, Pros and cons of virtualization, Virtualization Technologies:Xen**,** VMware and Hyper-V.

UNIT II– UNDERSTANDINGCLOUD MODELS AND ARCHITECTURES (08 Periods)

Cloud Models: NIST model, Cloud Cube model, Deployment models: Public, Private, Hybrid and Community; Service models: IaaS, PaaS and SaaS.

Understanding Cloud Architecture: Exploring the Cloud Computing Stack: Composability, Infrastructure, Platforms, Virtual Appliances, Communication Protocols, Applications; Connecting to the Cloud: The Jolicloud Netbook OS and Chromium OS - The Browser as an Operating System.

UNIT III – UNDERSTANDING CLOUD SERVICES, APPLICATIONS AND CAPACITY PLANNING (09 Periods)

Understanding Cloud Services and Applications Infrastructure as a Service (IaaS): IaaS workloads, Pods, aggregation, and silos; Platform as a Service (PaaS), Software as a Service (SaaS): SaaS characteristics, Open SaaS and SOA, Salesforce.com and CRM SaaS; Identity as a Service (IDaaS): Identity, Networked identity service classes, Identity system codes of conduct, IDaaS interoperability; Compliance as a Service (CaaS).

CapacityPlanning: Defining Baseline and Metrics: Baseline measurements, System metrics, Load Testing, Resource ceilings, Server and instance types; Network Capacity and Scaling.

UNIT IV – EXPLORING PLATFORM AS A SERVICE (PaaS) (10 Periods)

PaaS Application Frameworks: Drupal, Eccentex AppBase 3.0, Long Jump, Square space, WaveMaker and Wolf Frameworks.

Exploring Platform as a Service using Google Web Services: Surveying the Google Application Portfolio, Google Toolkit and Working with the Google App Engine.

Exploring Platform as a Service using Microsoft Cloud Services: Exploring Microsoft Cloud Services, Defining the Windows Azure Platform, Windows Live: Windows Live Essentials, Windows Live Home and Windows Live for Mobile.

UNIT V – EXPLORING INFRASTRUCTURE AS A SERVICE (IaaS) (08 Periods)

Understanding Amazon Web Services, Amazon Web Service Components and Services, Working with the Elastic Compute Cloud (EC2): Amazon Machine Images, Pricing models, System images and software, Creating an account and instance on EC2; Working with Amazon Storage Systems: Amazon Simple Storage System (S3), Amazon Elastic Block Store (EBS) and CloudFront; Understanding Amazon Database Services: Amazon SimpleDB, Amazon Relational Database Service (RDS) and Choosing a database for AWS.

Total Periods: 45

Topics for Self-study are provided in the Lesson Plan.

TEXT BOOKS:

1. Barrie Sosinsky, *Cloud Computing Bible,* Wiley India Pvt Ltd, 2011 (Reprint 2017).
2. Thomas Erl and RicardoPuttini, *Cloud Computing- Concepts, Technology and Architecture,* Pearson, 2014 (Seventh Impression 2017).

REFERENCE BOOKS:

1. Rajkumar Buyya, Christian Vecchiloa and S Thamarai Selvi, *Mastering Cloud Computing*, McGraw Hill Education, 2013 (Reprint 2017).
2. George Reese, *Cloud Application and Architectures*, O'Relly, 2009 (Reprint 2017).

ADDITIONAL LEARNING RESOURCES:

1. *"Exploring the Google Toolkit",*https://code.google.com/, drafted on 23 December, 2019.
2. "*Understanding Amazon Web Services*", https://aws.amazon.com/, drafted on 23 December, 2019.
3. "*Exploring Microsoft Cloud Services",*https://www.microsoft.com/windowsazure, drafted on 23 December, 2019.

CO-PO and PSO Mapping Table:

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CO2	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CO3	2	3	3	2	-	-	-	-	-	-	-	-	-	-	-
CO4	1	2	3	-	3	-	-	1	-	-	-	-	-	-	-
CO5	1	2	3	-	-	1	1	-	-	-	-	-	-	-	-
Average	2	2.33	3	2	3	1	1	1	-	-	-	-	-	-	-
Level of correlation of the course	2	3	3	2	3	1	1	1	-	-	-	-	-	-	-

Level of Correlation: 3 - High 2 - Medium 1 - Low

III B. TECH. - II SEMESTER
(19BM61502) **MODERN CRYPTOGRAPHY**

Int. Marks	Ext. Marks	Total Marks	L	T	P	C
40	60	100	3	-	-	3

PRE-REQUISITES: -

COURSE DESCRIPTION: Cryptographic protocols; Encryption techniques for confidentiality; Mathematics of symmetric and asymmetric algorithms; Hash functions for integrity; digital signature schemes.

COURSE OUTCOMES: After successful completion of this course, the students will be able to:

CO1. Apply cryptographic protocols to ensure authentication in network systems.
CO2. Analyze the efficiency of cryptographic techniques based on security attacks.
CO3. Choose suitable key management scheme for efficient key exchange between the authenticated parties.
CO4. Implement algorithms using information, complexity, and number theories for ensuring the security requirements-CIA.
CO5. Evaluate Message Digest and Secure Hash Algorithms using hash functions for data Integrity.
CO6. Analyze well-known digital signature algorithms for securing communication.

DETAILED SYLLABUS:

UNIT I – FOUNDATIONS OF CRYPTOGRAPHY (08 Periods)

FOUNDATIONS OF CRYPTOGRAPHY: Steganography, Substitution ciphers and Transposition Ciphers, One Time Pads. **Protocol Building Blocks:** Introduction to protocols, communications using symmetric Cryptography, One-Way Hash Functions, Communications Using Public-Key Cryptography, Digital Signatures with Encryption, Random and Pseudo-Random-Sequence Generation, **Basic Protocols**: Key Exchange, Authentication and key Exchange.

UNIT II- CRYPTOGRAPHIC TECHNIQUES (08 Periods)

CRYPTOGRAPHIC TECHNIQUES: Key Management, Electronic Codebook Mode, Block Replay, Cipher Block Chaining Mode, Stream Ciphers, Self-Synchronizing Stream Ciphers, Cipher-Feedback Mode, Synchronous Stream Ciphers, Output-Feedback Mode, Counter Mode, Choosing a Cipher Mode, Interleaving, Block Ciphers versus Stream Ciphers.

UNIT III- MATHEMATICS FOR CRYPTOGRAPHIC ALGORITHMS (12 Periods)

MATHEMATICS FOR CRYPTOGRAPHIC ALGORITHMS: Mathematical background:Information Theory, Complexity Theory, Number Theory, Factoring, Prime Number Generation, Discrete Logarithms in a Finite Field, Data **Encryption** Standard (DES), DES decryption, Security of DES, DES variants, Public Key Algorithms: RSA, Pholig-Hellman, RABIN, Elliptic Curve Cryptosystems.

UNIT IV- HASH FUNCTIONS (08 Periods)

HASH FUNCTIONS: One Way Hash Functions, Snefru hash function, N- Hash, MD4, MD5, Secure Hash Algorithm (SHA), Security of SHA, One Way Hash Functions Using Symmetric Block Algorithms, Using Public-Key Algorithms, Message Authentication Codes (MAC).

UNIT V- DIGITAL SIGNATURES **(09 Periods)**

DIGITAL SIGNATURES: Digital Signature Algorithm (DSA), Security of DSA, Discrete Logarithm Signature Schemes, Ongchnorr-Shamir, SCHNORR authentication and signature scheme, Diffie-Hellman Key exchange, Station-to-Station Protocol, Shamir's Three-Pass Protocol.

Total Periods 45

Topics for self-study are provided in lesson plan

TEXTBOOKS:

1. Bruce Schneier, *"Applied Cryptography: Protocols, Algorithms and Source Code in C",*John Wiley and Sons, New York, 2009.

REFERENCE BOOKS:

1. Alfred J Menezes, Paul C van Oorschot and Scott A.Vanstone, *"Handbook of Applied Cryptography"*, CRC Press, New York, 2010.
2. Wenbo Mao, *"Modern Cryptography Theory and Practice",* Pearson Education, 2004

ADDITIONAL LEARNING RESOURCES:

1. https://www.coursera.org/specializations/applied-crypto
2. https://www.udacity.com/course/applied-cryptography--cs387
3. https://www.classcentral.com/course/udacity-applied-cryptography-326
4. https://www.classcentral.com/course/udacity-applied-cryptography-326
5. https://wiki.openssl.org/index.php/Command_Line_Utilities
6. https://www.sslshopper.com/article-most-common-openssl-commands.html

CO-PO and PSO Mapping Table:

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	2	-	-	-	-	-	-	-	-	-	-	-	3
CO2	1	3	1	-	1	-	-	-	-	-	-	-	-	-	3
CO3	3	3	1	-	-	-	-	-	-	-	-	-	-	-	3
CO4	2	2	3	1	1	-	-	-	-	-	-	-	-	-	1
CO5	2	2	3	1	1	-	-	-	-	-	-	--	-	-	2
CO6	3	3	-	-	-	-	-	-	-	-	-	-	-	-	3
Average	2.3	2.6	2	1	1	-	-	-	-	-	-	-	-	-	2.5
Level of correlation of the course	3	3	2	1	1	-	-	-	-	-	-	-	-	-	3

Level of Correlation: 3 - High 2 - Medium 1 - Low

III B. Tech.–II Semester
(19BM61503)**CYBER SECURITY**

Int. Marks	Ext. Marks	Total Marks	L	T	P	C
40	60	100	3	-	-	3

PRE-REQUISITES: -

COURSE DESCRIPTION: Cybercrime, Cyberoffenses, Phishing, Identity theft, Cybercrime in mobile and wireless devices, Organizational measures for handling mobile devices, Security implications on using mobile devices, Tools and methods used in cybercrime, Forensics of computer and handheld devices, Real-life examples of cybercrime.

COURSE OUTCOMES: *After successful completion of this course, the students will be able to:*

CO1. Analyze methods of cybercrime, cyberoffenses to maintain cybersecurity.
CO2. Investigate tools used for cybercrime to protect computational assets.
CO3. Apply appropriate authentication mechanisms to reduce attacks on mobile and wireless devices.
CO4. Use appropriate cyberforensics tools and techniques to maintain cybersecurity.
CO5. Recognize the need for cybersecurity and practice ethics to protect privacy, property rights in cyberspace.

DETAILED SYLLABUS:

UNIT–I: CYBERCRIME (08 Periods)

Cybercrime and information security, Cybercriminals, Classifications of cybercrimes, Need for Cyberlaws in Indian context, Legal perspectives of cybercrime, Indian perspective of cybercrimes, Cybercrime and the Indian ITA 2000, Positive aspects andweak areas of ITA 2000, Amendments made in Indian ITA 2000 for admissibility of e-records, Amendments to the Indian IT Act, Global perspective on cybercrimes, Intellectual property in cyberspace, Ethical dimension of cybercrimes.

UNIT–II: CYBEROFFENSES (11 Periods)

Categories of cybercrime, How criminals plan the attacks, Social engineering, Cyberstalking, Cybercafe and cybercrimes, Botnets, Attack vector, Cloud computing, Phishing – Methods, Techniques, Spear phishing, Phishing scams, Phishing toolkits, Spy phishing, Countermeasures; Identity Theft – Personally identifiable information, Types, Techniques, Countermeasures, Effacing online identity.

UNIT–III: CYBERCRIME IN MOBILE AND WIRELESS DEVICES (07 Periods)

Proliferation of mobile and wireless devices, Trends in mobility, Credit card frauds in mobile and wireless computing era, Security challenges posed by mobile devices, Registry settings for mobile devices, Authentication service security, Attacks on mobile/cell phones, Security implications of mobile devices for organizations, Organizational measures for handling mobile devices related security issues.

UNIT–IV: TOOLS AND METHODS USED IN CYBERCRIME (10 Periods)

Proxy servers and anonymizers, Password cracking, Keyloggers and spywares, Virus and worms, Trojan horses and backdoors, Steganography, DoS and DDoS attacks, SQL Injection, Buffer Overflow, Attacks on wireless networks.

UNIT–V: CYBERFORENSICS, CYBERCRIMEIN REAL-WORLD (09 Periods)

Forensics of Computer and Handheld Devices: Cyberforensics, Cyberforensics and digital evidence, Forensics analysis of e-mail, Forensics and social networking sites, Forensics of handheld devices – Smartphone forensics, EnCase, Device Seizure, MOBILedit.

Cybercrime examples, mini-cases, online scams: Real-life examples - Official website of Maharashtra Government hacked, Indian banks lose millions of rupees, Game source code stolen; Mini-cases - Indian Case of online gambling, Indian case of intellectual property crime;Online scams - Cheque cashing scam, Charity scams.

Total Periods: 45

Topics for self-study are provided in lesson plan

TEXT BOOK:

1. Nina Godbole, SunitBelapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley, 2013.

REFERENCE BOOKS:

1. Nilakshi Jain, Ramesh Menon, *Cyber Security and Cyber Laws*, Wiley, 2020.
2. Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short, *Cybersecurity Essentials*, 1st Edition, Sybex, 2018.
3. ErdalOzkaya,*Cybersecurity: The Beginner's Guide*, 1st Edition,Packt Publishing, 2019.

ADDITIONAL LEARNING RESOURCES:

1. Yuri Diogenes, ErdalOzkaya, *Cybersecurity: Attack and Defense Strategies*, 2nd Edition, Packt Publishing, 2019.
2. http://www.ignou.ac.in/upload/Announcement/programmedetails.pdf
3. Alessandro Parisi, *Hands-On Artificial Intelligence for Cybersecurity*, Packt Publishing, 2019.

CO-PO and PSO Mapping Table:

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	-	-	-	-	-	-	-	-	-	-	-	-	-
CO2	3	2	-	-	2	-	-	-	-	-	-	-	-	-	-
CO3	3	2	1	-	-	-	-	-	-	-	-	-	-	-	-
CO4	3	2	-	-	2	-	-	-	-	-	-	-	-	-	-
CO5	-	-	-	-	-	2	-	2	-	-	-	-	-	-	-
Average	3	2	1	-	2	2	-	2	-	-	-	-	-	-	-
Level of correlation of the course	3	2	1	-	2	2	-	2	-	-	-	-	-	-	-

Level of Correlation: 3 - High 2 - Medium 1 - Low

III B. Tech. - II Semester
(19BM61531)MODERN CRYPTOGRAPHY LAB

Int. Marks	Ext. Marks	Total Marks	L	T	P	C
50	50	100	-	-	2	1

PRE-REQUISITES:A Course on Modern Cryptography

COURSE DESCRIPTION:
Mono-alphabetic Ciphers; Poly-alphabetic Ciphers; Block modes; Block ciphers; Public Key Algorithms, Message Digest Algorithms, Diffie-Hellman Key Exchange; SHA; Digital Signature Standards.

COURSE OUTCOMES: *After successful completion of this course, the students will be able to:*

CO1. Analyze attack resiliency of classical encryption algorithms to provide security.
CO2. Develop block cipher modes of operations and stream ciphers to achieve confidentiality in network systems.
CO3. Analyze the strength of RSA using cryptanalysis.
CO4. Use Key Exchange algorithm to ensure security primitives.
CO5. Implement different Message digest algorithms and DSS to achieve authentication.
CO6. Work independently or communicate effectively in oral and written forms.

LIST OF PROGRAMMING EXERCISES:

1. Implement the following monoalphabetic Ciphers and analyze its attack resiliency.
   a. Shift Cipher
   b. Affine cipher
2. Implement the following Poly-alphabetic Ciphers and analyze its attack resiliency.
   a. Hill cipher
   b. Vigenere
3. Implement the following block cipher modes and analyze the role of Initialization Vector(IV)
   a. counter mode
   b. Output Feedback mode
4. Write a program to implement the Data Encryption Standard (DES).
5. Implement a stream cipher algorithm with running key generator.
6. Write a program to Implement RSA algorithm.
7. Write a program to find prime factors of a given large number and analyze the time complexity.
8. Write a program to determine the message digest of a given message using the SHA-1 algorithm.
9. Write a program to implement Diffie-Hellman Key Exchange mechanism.
10. Write a program to implement Digital Signature Standard.

REFERENCE BOOKS:

1. William Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson Education, 7th Edition, 2017.
2. Douglas R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 3rd Edition, 2005.

ADDITIONAL LEARNING RESOURCES:

1. https://www.classcentral.com/course/udacity-applied-cryptography-326
2. https://www.classcentral.com/course/udacity-applied-cryptography-326
3. https://wiki.openssl.org/index.php/Command_Line_Utilities
4. https://www.sslshopper.com/article-most-common-openssl-commands.html

CO-PO and PSO Mapping Table:

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2	3	3	-	2	-	-	-	-	-	-	-	3	-	3
CO2	1	3	3	-	2	-	-	-	-	-	-	-	3	-	3
CO3	1	2	1	2	1	1	-	-	-	-	-	-	3	-	3
CO4	2	3	2	2	2	2	-	-	-	-	-	-	3	-	3
CO5	2	3	3	-	3	-	-	-	-	-	-	-	3	-	3
CO6	-	-	-	-	-	-	-	-	3	3	2	-	3	-	3
Average	-	-	-	-	-	-	-	-	3	-	-	-	3	-	3
Level of correlation of the course	-	-	-	-	-	-	-	-	-	-	-	-	3	-	3

Level of Correlation: 3 - High 2 - Medium 1 - Low

IV B. Tech. – I Semester

(19BM71501) **IoT SECURITY**

Int. Marks	Ext. Marks	Total Marks	L	T	P	C
40	60	100	3	-	-	3

PRE-REQUISITES: -

COURSE DESCRIPTION:
Securing the Internet of Things; Cryptographic Fundamentals for IoT; Identity & Access Management Solutions for IoT; Mitigating IoT Privacy Concerns; Cloud Security for IoT

COURSE OUTCOMES: After successful completion of this course, the students will be able to:

CO1. Analyze Attacks, threats and vulnerabilities to secure IoT devices.
CO2. Design IoT messaging and communication protocols using Cryptographic primitives
CO3. Apply authentication credentials and Identity Access Management infrastructure to manage IoT
CO4. Analyze privacy concerns in IoT devices by using PIA
CO5. Examine IoT threats in the cloud for effective utilization of cloud services
CO6. Analyze different cloud service providers to IoT computing

DETAILED SYLLABUS:

UNIT I– Securing the Internet of Things (09 Periods)
Security Requirements in IoT Architecture - Security in Enabling Technologies -Security Concerns in IoT Applications. Security Architecture in the Internet of Things -Security Requirements in IoT - Insufficient Authentication/Authorization – Insecure Access Control - Threats to Access Control, Privacy, and Availability - Attacks Specific to IoT. Vulnerabilities – Secrecy and Secret-Key Capacity -Authentication/Authorization for Smart Devices - Transport Encryption – Attack & Fault trees

UNIT II –Cryptographic Fundamentals for IoT (09 Periods)
Cryptographic primitives and its role in IoT – Encryption and Decryption – Hashes –Digital Signatures – Random number generation – Cipher suites – key management fundamentals – cryptographic controls built into IoT messaging and communication protocols – Zigbee, Bluetooth-LE, Near Field Communication (NFC).

UNIT III – Identity & Access Management Solutions for IoT (09 Periods)
Identity lifecycle – authentication credentials– passwords, Symmetric keys, certificates, Biometrics, IoTIAM infrastructure Authorization and Access controls within publish/Subscribe protocols, access controls within communication protocols

UNIT IV – Mitigating IoT Privacy Concerns (09 Periods)
Privacy challenges introduced by IoT- A complex sharing environment- wearable's, smart homes, Guiding to perform an IoT PIA-Authorities, characterizing collected information, use of collected information, Security, Notice, Data retention Information sharing, redress, auditing and accountability

UNIT V –Cloud Security for IoT (09 Periods)
Cloud services and IoT – offerings related to IoT from cloud service providers – Cloud IoT security controls – An enterprise IoT cloud security architecture – New directions in cloud enabled IoT computing

Total Periods: *45*

Topics for self-study are provided in lesson plan

TEXT BOOK:

1. Brian Russell and Drew Van Duren, *Practical Internet of Things Security: Design a security framework for an Internet connected ecosystem,* 2nd Edition, *O'Reilly, 2*016.

REFERENCE BOOKS:

1. Fei Hu, *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations,* CRC Press2016.
2. ShancangLi LiDaXu, *Securing the Internet of Things*,1st Edition, Elsevier,2017.

CO-PO and PSO Mapping Table:

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2	3	-	3	-	-	-	-	-	-	-	-	-	-	3
CO2	2	3	-	-	1	-	-	-	-	-	-	-	-	-	3
CO3	3	3	3	-	2	-	-	-	-	-	-	-	-	-	2
CO4	2	3	-	-	1	-	-	-	-	-	-	-	-	-	2
CO5	2	2	-	-	-	-	-	-	-	-	-	-	-	-	2
CO6	2	3	-	-	-	2	2	-	-	-	-	-	-	-	2
Average	2.2	2.8	3	3	1.3	2	2	-	-	-	-	-	-	-	2.3
Level of correlation of the course	3	3	3	3	2	2	2	-	-	-	-	-	-	-	3

Level of Correlation: 3 - High 2 - Medium 1 - Low

IV B. TECH. – I SEMESTER
(19BM71502) **INFORMATION SECURITY**

Int. Marks	Ext. Marks	Total Marks	L	T	P	C
30	70	100	3	-	-	3

PRE-REQUISITES: -

COURSE DESCRIPTION:
Computer security; Need of Security; Access Control; Security policies; Software vulnerabilities; Secure Electronic transactions; Secure socket layer; transport layer security; Privacy.

COURSE OUTCOMES: After successful completion of this course, the students will be able to:

CO1. Apply the security requirements like confidentiality, integrity, and availability to secure network assets from threats and attacks.
CO2. Analyze virus, malicious software and worms for detecting distributed Daniel of service attacks.
CO3. Apply handshaking, alert and change cipher spec protocols and Coding function to secure SSL and TLS.
CO4. Apply PGP model and canonical forms to secure E-Mail data at transport layer.
CO5. Design firewall to secure the system by applying various intrusion detection systems.
CO6. Apply privacy techniques to protect information in the network.

DETAILED SYLLABUS:

UNIT I–INTRODUCTION (08 Periods)
Computer Security Concepts, the OSI Security Architecture, Security Attacks, Security Mechanism, Standards.

Malicious Software: Types of Malicious Software, Viruses, Worms, Distributed Denial of Service Attacks.

UNIT II – SECURITY AT TRANSPORT LAYER: SSL & TLS (09 Periods)
Web Security Consideration, Secure Socket Layer and Transport Layer Security, Transport Layer Security, HTTPS, Secure Shell.

Wireless Network Security: IEEE 802.11 Wireless LAN Overview, IEEE 802.11i LAN Security, Wireless Application Protocol Overview, Wireless Transport Layer Security, WAP end-to-end Security

UNIT III – SECURITY AT APPLICATION LAYER: PGP AND S/MIME (08 Periods)
Pretty Good Privacy, S/MIME, Domainkeys Identified Mail

IP Security: IP Security Overview, IP Security Policy, IP Security Architecture, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange.

UNIT IV– INTRUDERS AND FIREWALLS (08 Periods)
Intrusion Detection System: Intruders, Intrusion Detection, Password Management.

Firewalls: The Need for Firewalls, Firewall Characteristics, Types of Firewalls, Firewall Basing, Firewall location and configuration.

UNIT V- PRIVACY **(09 Periods)**

Evade Traffic analysis, Tunnel SSH through Tor, Encrypt you file seamlessly, Guard against Phishing, Use the web with fewer passwords, Encrypt your E-mail with Thunderbird, Encrypt you E-mail in Mac OS X

Total Periods: 45

Topics for self-study are provided in lesson plan.

TEXT BOOKS:

1. William Stallings "*Network Security Essentials (Applications and Standards)*", 4th Edition, Pearson Education 2011.
2. Andrew Lockhart "*Information security Hacks (Tips and Tools for protecting your privacy)*", 2nd Edition, 2004.

REFERENCE BOOKS:

1. Behrousz A Forouzan, D Mukhopadhyay, "*Cryptography and network Security*", 1st Edition, McGraw Hill,2010.
2 CharlieKaufman, Radia Perlman and Mike Speciner, *Network Security – Private Communication in a Public World,*2nd Edition, Pearson/PHI.

ADDITIONAL RESOURCES:

1. http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014 1/Stallings/Stallings_Cryptography_and_Network_Security.pdf.
2. http://www.ijcsmc.com/docs/papers/January2015/V4I1201544.pdf.

http://nptel.ac.in/syllabus/106105031/

CO-PO and PSO Mapping Table:

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	-	-	2	-	-	-	-	-	-	-	-	-	3
CO2	2	3	-	-	-	-	-	-	-	-	-	-	-	-	3
CO3	3	3	2	-	2	2	3	2	-	-	-	-	-	-	3
CO4	3	3	2	2	2	-	-	-	-	-	-	-	-	-	3
CO5	2	2	3	2	1	-	2	-	-	-	-	-	-	-	3
CO6	3	3	2	2	2	-	3	-	-	-	-	-	-	-	3
Average	2.7	2.8	2.25	2	1.8	2	2.7	2	-	-	-	-	-	-	3
Level of correlation of the course	3	3	3	2	2	2	3	2	-	-	-	-	-	-	3

Level of Correlation: 3 - High 2 - Medium 1 - Low

IV B. TECH. – I SEMESTER
(19BM71531)**INFORMATION SECURITY LAB**

Int. Marks	Ext. Marks	Total Marks	L	T	P	C
50	50	100	-	-	2	1

PRE-REQUISITES:A Course on Information Security

COURSE DESCRIPTION:
Windows Firewall Security Features, Introduction to wireshark tool, Pretty Good Privacy (PGP), Intrusion Detection System, SSL Certificate, and TSL.

COURSE OUTCOMES: After successful completion of this course, the students will be able to:

CO1. Apply the tools and techniques to ensure the information security and privacy for network applications.
CO2. Analyze SSL Certificate and encryption in web applications for security.
CO3. Analyze SSL and TLS protocols to secure TCP connections.
CO4. Implement IP Packet filtering for blocking in-bound packets.
CO5. Work independently or communicate effectively in oral and written forms.

List of Exercises/List of Experiments:

1. Find the Packet Information using Wireshark on our network.
2. Simulate traffic analyzing using wireshark.
3. Study of SSL (HTTPS) over HTTP to secure TCP connections.
4. Simulate Transport Layer Security protocol.
5. Create a simple web application and deploy it in Apache tomcat server and secure it using SSL certificates.
6. Simulate Pretty Good Privacy security protocol for email messages and individual files.
7. Simulate IP Packet filtering at host system in user Network.
8. Study windows firewall security features on the system allotted to you.
9. Create firewalls using ip tables in linux.

REFERENCE BOOKS/LABORATORY MANUALS:

1. Computer Security: Principles and Practices, William Stallings and Lawrie Brown, Pearson Education, ISBN 13-9780134794396
2. Computer Security: Art and Science, by Matt Bishop, Pearson Education, ISBN:9788177584257

SOFTWARE/Tools used:

1. Windows Fire Wall
2. PGP
3. SSL
4. Tomcat 7.0.104
5. Snort
6. Java
7. Wireshark

ADDITIONAL LEARNING RESOURCES:

1. https://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf
2. https://www.cmu.edu/iso/aware/presentation/tepperphd.pdf
3. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

4. https://www.cs.unibo.it/babaoglu/courses/security/resources/documents/intro-to-crypto.pdf

http://www.cs.kent.edu/~mallouzi/ccn%20Spring%202014/

CO-PO and PSO Mapping Table:

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	2	-	2	-	-	-	-	-	-	-	-	-	3
CO2	2	2	3	2	1	2	3	-	-	-	-	-	-	-	3
CO3	2	2	3	-	3	1		-	-	-	-	-	-	-	3
CO4	2	2	3	-	1	2	3	-	-	-	-	-	-	-	3
CO5	-	-	-	-	-	-	-	-	3	3	2	-	-	-	3
Average	2.25	1.75	2.75	2	1.75	1.6	3		3	3	2		-	-	3
Level of correlation of the course	3	2	3	2	2	2	3		3	3	2	-	-	-	3

Level of Correlation: 3 - High 2 - Medium 1 - Low