SCHEME & SYLLABUS OF UNDERGRADUATE DEGREE COURSE of B. Tech. (Computer Science & Engineering (Cyber Security)) VII & VIII Semester

[Draft Syllabus Subjected to approval]

Effective for the students admitted in year 2021-22 and onwards
Approved by ……. academic council meeting held on …….

Teaching & Examination Scheme
B. Tech. (Computer Science & Engineering (Cyber Security))
4^{rd}Year – VII Semester
(Effective for the students admitted in year 2021-22 and onward)

S. No.	Category	Course Code	Course Title	Hours			Exam Hours	Marks			Credit
				L	T	P		IA	ETE	Total	
	THEORY										
1	DC	7CY4-01	Cybersecurity in Wireless and Mobile Networks	3	-	-	3	30	70	100	**3**
2	UE	**University Elective subject** ***Course code and title to be selected from the university elective pool of subjects***		3	-	-	3	30	70	100	**3**
3	DE	7CY 5-11	Mobile Computing	2	-	-	3	30	70	100	**2**
		7CY5-12	GPU Computing								
		7CY5-13	Generative AI								
Sub Total				**8**	**00**	**00**	**-**	**90**	**210**	**300**	**8**
PRACTICAL & SESSIONAL											
4	DC	7CY4-21	Network Protocols Lab	-	-	2	-	60	40	100	**1**
5	UI	7CY7-30	Industrial Training	-	-	1	-	60	40	100	**3**
	UI	7CY7-50	B.Tech. Project - I	-	-	3	-	60	40	100	**2**
6	CCA	7CY8-00	SODECA / Co-Curricular Activity	-	-	-	-	-	100	100	**1**
Sub Total				**00**	**00**	**06**	**-**	**180**	**220**	**400**	**7**
Total				**8**	**00**	**06**	**-**	**270**	**430**	**700**	**15**

L = Lecture, **T =** Tutorial, **P =** Practical, **IA=**Internal Assessment**, ETE=**End TermExam,**Cr**=Credits

Teaching & Examination Scheme
B. Tech. (Computer Science & Engineering (Cyber Security))
4^{rd}Year – VIII Semester
(Effective for the students admitted in year 2021-22 and onward)

S. No.	Category	Course Code	Course Title	Hours			Exam Hours	Marks			Credit
				L	T	P		IA	ETE	Total	
	THEORY										
1	UE	**University Elective subject** *Course code and title to be selected from the university elective pool of subjects*		3	-	-	3	30	70	100	**3**
Sub Total				**3**	**00**	**00**		**30**	**70**	**100**	**3**
	PRACTICAL & SESSIONAL										
10	UI	8CY7-40	Seminar	-	-	2	-	60	40	100	**2**
	UI	8CY7-50	B.Tech. Project - II	-	-	3	-	60	40	100	**4**
12	CCA	8CY8-00	SODECA / Co-Curricular Activity	-	-	-	-	-	100	100	**2**
Sub Total				**00**	**00**	**05**	**-**	**120**	**180**	**300**	**8**
Total				**03**	**00**	**05**	**-**	**150**	**250**	**400**	**11**

L = Lecture, **T =** Tutorial,   = Practical, **IA**=Internal Assessment**, ETE**=End Term Exam,**Cr**=Credits

VII Semester
B. Tech. (Computer Science & Engineering (Cyber Security))

7CY4-01: Cybersecurity in Wireless and Mobile Networks

Credit: 3	**Max. Marks: 100 (IA:30, ETE:70)**
3L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:

As a result of successfully completing this course, students will be able :

- Get a comprehensive Understanding of Cybersecurity Fundamental
- Understand the Cryptographic Techniques and Access Control Mechanisms
- Identify and Mitigate of Network Security Challenges
- Understand the advanced Security Protocols for Network Protection
- understand the Privacy and Security in Ad-hoc and Vehicular Networks
- Apply the Theoretical Knowledge to Real-world Security Challenges

Course Outcomes:

Upon successful completion of the course the students will be able to
CO-1: Identify and Analyze Security Threats and Vulnerabilities
CO-2: Develop and Implement Security Protocols for Wireless Networks
CO-3: Secure IP-based Networks and Ad-hoc Networks
CO-4: Implement Privacy-Preserving Techniques in Network Protocols
CO-5: Understand and Address Ethical and Privacy Issues in Cybersecurity

S. No.	Contents	Hours
1	**Fundamentals of Security and Threats - I**: Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack. Malware Terminology: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots. Active and Passive Security Attacks. IP Spoofing, Tear drop,DoS, DDoS,XSS, SQL injection, Smurf	8
2	**Fundamentals of Security and Threats – II**: Man in middle, Format String attack. Types of Security Vulnerabilities- buffer overflows, Invalidated input, race conditions, access-control problems, weaknesses in authentication, authorization, or cryptographic practices. Access control Problems.	8
3	**Security Challenges and Protocols in Wireless Networks:** Vulnerabilities and Security Challenges of Wireless networks, Trust Assumptions, Adversary models and Protocols, Attacks against naming and addressing in the Internet, Security protocols for address resolution and address auto configuration.	8
4	**Advanced Security Protocols in IP and Ad-hoc Networks:** Security for global IP mobility, IP Security (IP Sec) protocol, Key Establishment and Revocation Protocols in Sensor Networks, Secure Neighbor Discovery, Secure routing protocols in multihop wireless networks, Provable Security for Ad-hoc Network routing protocols	8
5	**Privacy and Security in Ad-hoc and Vehicular Networks:** Privacy-preserving routing in Ad-hoc Networks, Location privacy in vehicular Ad-hoc networks, Secure protocols for behavior enforcement, and Game theoretic model of packet forwarding.	9
	Total	**41**

Suggested Books:

1. Stallings William , Cryptography and Network Security - Principles and Practice, Seventh Edition, Pearson Education; Seventh edition
2. William Stalling, Lawrie Brown, Computer Security: Principles and Practice, Pearson; 4th edition
3. Buttyan, J. P. Hubaux, “Security and Cooperation in Wireless Networks”, Cambridge University Press.
4. O. Goldrich,“Foundation of Cryptography-Vol.1 & Vol.2”, Cambridge University Press.
5. Charlie Kaufman,Radia Perlman, and Mike Speciner, Network Security: Private Communication in a Public World, Prentice Hall; 2nd edition
6. William Stallings, Network Security Essentials: Applications and Standards,   Pearson; 6th edition
7. Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Wiley; 2nd edition
8. James Kempf, “Wireless Internet Security: Architecture and Protocols”, Cambridge University Press.

9. Gunter Ollmann 2007. The Phishing Guide Understanding & Preventing Phishing Attacks. IBM Internet Security Systems.
10. Tyler Wrightson, Wireless Network Security A Beginner's Guide, McGraw-Hill Education; Illustrated edition
11. Subir Kumar Sarkar, ―Ad-Hoc Mobile Wireless Networks: principles, protocols and applications, CRC Press
12. Prasant Mohapatra and Sriramamurthy, ―Ad Hoc Networks: Technologies and Protocols, Springer International Edition, 2009
13. Stefano Basangi, Marco Conti, Silvia Giordano, Ivan Stojmenovic, ―Mobile Ad-Hoc Networking, John-Wiley and Sons Publications, 2004

VII Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
7CY5-11: Mobile Computing	
Credit: 2	**Max. Marks: 100 (IA:30, ETE:70)**
2L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:

As a result of successfully completing this course, students will:

• To make the student understand the concept of the mobile computing paradigm, its novel applications, and limitations.

• To understand the typical mobile networking infrastructure through a popular GSM protocol

• Understand the issues and solutions of various layers of mobile networks, namely MAC layer, Network Layer & Transport Layer

• To understand the database issues in mobile environments & data delivery models.

• Understand the ad hoc networks and related concepts.

• To understand the platforms and protocols used in the mobile environment.

Course Outcomes:

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

CO-1: Think and develop a new mobile application.

CO-2: Take any new technical issue related to this new paradigm and come up with a solution(s).

CO-3: Develop new ad hoc network applications and/or algorithms/protocols.

CO-4: Understand & develop any existing or new protocol related to the mobile environment

S. No.	Contents	Hours
1	**Introduction:** Mobile Communications, Mobile Computing – Paradigm, Promises/Novel Applications and Impediments and Architecture; Mobile and Handheld Devices, Limitations of Mobile and Handheld Devices. GSM – Services, System Architecture, Radio Interfaces, Protocols, Localization, Calling, Handover, Security, New Data Services, GPRS	**5**
2	**(Wireless) Medium Access Control (MAC):** Motivation for a specialized MAC (Hidden and exposed terminals, Near and far terminals), SDMA, FDMA, TDMA, CDMA, Wireless LAN/(IEEE 802.11)	**6**
3	**Mobile Network Layer:** IP and Mobile IP Network Layers, Packet Delivery and Handover Management, Location Management, Registration, Tunneling and Encapsulation, Route Optimization, DHCP	**6**
4	**Mobile Transport Layer:** Conventional TCP/IP Protocols, Indirect TCP, Snooping TCP, Mobile TCP, Other Transport Layer Protocols for Mobile Networks. Database Issues: Database Hoarding & Caching Techniques, Client-Server Computing & Adaptation, Transactional Models, Query processing	**6**
5	**Data Dissemination and Synchronization:** Communications Asymmetry, Classification of Data Delivery Mechanisms, Data Dissemination, Broadcast Models, Selective Tuning and Indexing Methods, Data Synchronization – Introduction, Software, and Protocols.	**5**
	Total	**28**

Suggested Books:

1. Jochen Schiller, “Mobile Communications”, Addison-Wesley, Second Edition, 2009.
2. Raj Kamal, “Mobile Computing”, Oxford University Press, 2007, ISBN: 0195686772
3. ASOKE K TALUKDER, HASAN AHMED, ROOPA R YAVAGAL, “Mobile Computing, Technology Applications and Service Creation” Second Edition, Mc Graw Hill.
4. UWE Hansmann, Lother Merk, Martin S. Nicklaus, Thomas Stober, “Principles of Mobile Computing,” Second Edition, Springer.
5. “GENESIS : Personal Communication Device”. GENESIS 191A321 Document, 1993.

6. “Intelligent Vehicle Highway Systems Projects”. Department of Transportation, Minnesota Document, March 1994.

VII Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
7CY5-12: GPU Computing	
Credit:2	**Max. Marks: 100 (IA:30, ETE:70)**
2L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:

As a result of successfully completing this course, students will:

- Understand parallel programming with graphics processing units (GPUs).
- Understand Memory management and mechanism for parallel computing

Course Outcomes:

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

CO-1: Define and understand terminology commonly used in parallel computing.

CO-2: Describe common GPU architectures and programming models.

CO-3: Understand a Given problem and develop an efficient parallel algorithm to solve it.

CO-4: Understand CUDA memory access mechanism.

S. No.	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	**1**
2	**GPU Introduction**: To study architecture and capabilities of modern GPUs and learn programming techniques for the GPU such as CUDA programming model. Heterogeneous Parallel Computing, Architecture of a Modern GPU, Speeding Up Real Applications, Parallel Programming Languages and Models.	**6**
3	**History of GPU Computing**: Evolution of Graphics Pipelines, The Era of Fixed-Function Graphics Pipelines, Evolution of Programmable Real-Time Graphics, Unified Graphics and Computing Processors, GPGPU, Scalable GPUs, Recent Developments, Future Trends.	**5**
4	**Introduction to Data Parallelism and CUDA C:** Data Parallelism, CUDA Program Structure, A Vector Addition Kernel, Device Global Memory and Data Transfer, Kernel Functions and Threading.	**5**
5	**Data-Parallel Execution Model:** CUDA Thread Organization, Mapping Threads to Multidimensional Data, Matrix-Matrix Multiplication—A More Complex Kernel, Synchronization and Transparent Scalability, Assigning Resources to Blocks, Thread Scheduling and Latency Tolerance.	**6**
6	**CUDA Memories:** Importance of Memory Access Efficiency, CUDA Device Memory Types, A Tiled Matrix – À Matrix Multiplication Kernel, Memory as a Limiting Factor to Parallelism.	**5**
	Total	**28**

Suggested Books:

1. Sanders, J. and Kandrot, E., CUDA by Example: An Introduction to General-Purpose GPU Programming, Addison-Wesley Professional (2012) 4th Edition.

2. Kirk, D. and Hwu, M., W., Programming Massively Parallel Processors: A Hands-on Approach. Morgan Kaufmann (2016) 3rd Edition.

3. Hwu, M., W., A GPU Computing Gems Emerald Edition (Applications of GPU Computing Series), Morgan Kaufmann (2011) 1st Edition.

VII Semester
B. Tech. (Computer Science & Engineering (Cyber Security))

7CY5-13: Generative AI

Credit: 2	**Max. Marks: 100 (IA:30, ETE:70)**
2L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:
As a result of successfully completing this course, students will be:

- Understand the fundamentals of generative AI and its applications in computer vision and natural language processing.
- Develop skills in designing and implementing generative models using deep learning frameworks.
- Analyze and evaluate the performance of generative models in various applications.

Course Outcomes:

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

CO-1: Design and implement generative models for image and text generation, and other applications.

CO-2: Understand the strengths and limitations of various generative models and be able to select appropriate models for specific tasks.

CO-3: Develop problem-solving skills using generative AI and be able to apply them to real-world problems.

CO-4: Critically evaluate the performance of generative models and develop strategies for improvement.

S. No.	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course	**1**
2	**Overview of Generative AI**: Types of Generative Models (VAE, GAN, RNN, etc.), Applications of Generative AI (Image Generation, Text Generation, etc.)	**6**
3	**Generative Models for Computer Vision** : Convolutional Neural Networks (CNNs) for image processing, Generative Adversarial Networks (GANs) for image generation, Variational Autoencoders (VAEs) for image compression and generation, Case studies: Image generation, Image-to-image translation, etc.	**7**
4	**Generative Models for Natural Language Processing:** Recurrent Neural Networks (RNNs) for text processing, Transformers for text generation and language modeling, Generative models for text summarization, chatbots, and language translation	**7**
5	**Advanced Generative AI Topics:** Generative models for multimodal data (images, text, audio, etc.), Generative models for sequential data (time series, videos, etc.), Advanced techniques: Style transfer, CycleGAN	**7**
	Total	**28**

Suggested Books:

1. Generative Deep Learning: Teaching Machines to Paint, Write, Compose, and Play by David Foster, O'Reilly Media
2. Deep Learning by Ian Goodfellow, Yoshua Bengio, and Aaron Courville
3. Generative Adversarial Networks by Ian Goodfellow, Yoshua Bengio, and Aaron Courville
4. Natural Language Processing (almost) from Scratch" by Collobert et al.
5. Neural Network Methods for Natural Language Processing" by Yoav Goldberg
   Deep Learning for Computer Vision with Python" by Adrian Rosebrock

VII Semester
B. Tech. (Computer Science & Engineering (Cyber Security))

7CY4-21: Network Protocols Lab

Credit: 1	**Max. Marks: 100 (IA:60, ETE:40)**
0L+0T+ 2P	**End Term Exams: 2 Hours**

Course Objectives:
As a result of successfully completing this course, students will:

- Able to understand basic working principle of UDP Network Protocol.
- Able to understand basic working principle of TCP Network Protocol.
- Able to install various Network simulation and perform Network Simulation.

Course Outcomes:
Upon successful completion of the course, students will be able to
CO-1: Simulate different network topologies.
CO-2: Implement various framing methods of Data Link Layer.
CO-3: Implement various Error and flow control techniques.
CO-4: Implement network routing and addressing techniques.
CO-5: Implement transport and security mechanisms

List of Experiments

1. Implementation of Stop and Wait Protocol and Sliding Window Protocol.
2. Study of Socket Programming and Client – Server model
3. Write a code simulating ARP /RARP protocols.
4. Write a code simulating PING and TRACEROUTE commands
5. Create a socket for HTTP for web page upload and download.
6. Write a program to implement RPC (Remote Procedure Call)
7. Implementation of Subnetting.
8. Applications using TCP Sockets like ***a. Echo client and echo server b. Chat c. File Transfer***
9. Applications using TCP and UDP Sockets like ***d. DNS e. SNMP f. File Transfer***
10. Study of Network simulator (NS).and Simulation of Congestion Control Algorithms using NS
11. Perform a case study about the different routing algorithms to select the network path with its optimum and economical during data transfer. i. Link State routing ii. Flooding iii. Distance vector
12. To learn handling and configuration of networking hardware like RJ-45 connector, CAT-6 cable, crimping tool, etc.
13. Configuration of router, hub, switch etc. (using real devices or simulators)
14. Running and using services/commands like ping, traceroute, nslookup, arp, telnet, ftp, etc.
15. Network packet analysis using tools like Wireshark, tcpdump, etc.
16. Network simulation using tools like Cisco Packet Tracer, NetSim, OMNeT++, NS2, NS3, etc.
17. Socket programming using UDP and TCP (e.g., simple DNS, data & time client/server, echo client/server, iterative & concurrent servers)

Note: The Instructor may add/delete/modify/tune experiments, wherever he/she feels in a justified manner It is also suggested that open source tools should be preferred to conduct the lab (C , C++ , Java , NS3, Mininet, Opnet, TCP Dump, Wireshark etc.

VII Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
7CY7-50 : B.Tech. Project – I	
Credit: 2	Max. Marks: 100 (IA:60, ETE:40)
0L+0T+3P	Mode of evaluation: Report and presentation

Assessment or Evaluation

The evaluation criteria for B. Tech. Project - I

S. No.	Category	Internal Assessment Max Marks in %	End Term Examinations Max Marks in %
1	Project Motivation, Conceptual Design, Innovativeness, and utility in actual life application	10%	10%
2	Project Ideation, Project Formulation, and Design	10%	10%
3	Project Prototyping & Finalization, Project Planning & Timeline (Project Viability for 2 semesters)	10%	10%
4	Technology Used and Method	10%	10%
5	Project Execution, Development, Deployment, Demonstration and Delivery (Working and completeness) required to justify current semester work and presentation	30%	30%
6	Report writing and project documentation (organization of the report, clarity, use of figure/diagram, writing skills, presentation of result, paper publication, patent application, etc.)	20%	20%
7	Professional ethics (teamwork, punctuality, novelty, etc.)	10%	10%
Total		**100%**	**100%**

VIII Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
8CY7-50 : B.Tech. Project -II	
Credit: 4	**Max. Marks: 100 (IA:60, ETE:40)**
0L+0T+3P	**Mode of evaluation: Report and presentation**

Assessment or Evaluation

The evaluation criteria for B. Tech. Project - II

S. No.	Category	Internal Assessment Max Marks in %	End Term Examinations Max Marks in %
1	Project Motivation, Conceptual Design, Innovativeness, and utility in actual life application	10%	10%
2	Project Ideation, Project Formulation, and Design	10%	10%
3	Technology Used and Method	10%	10%
4	Project Execution, Development, Deployment, Demonstration and Delivery (Working and completeness) required to justify current semester work and presentation	30%	30%
5	Report writing and project documentation (organization of the report, clarity, use of figure/diagram, writing skills, presentation of result, paper publication, patent application, etc.)	20%	20%
6	Professional ethics (teamwork, punctuality, novelty, etc.)	10%	10%
7	Paper Published in reputed journals (SCE, SCIE, Scopus, UGC care or any peer-reviewed journal), Paper publications (International or National conferences [IEEE, ACM, Springer, etc]), and presentations at Hackathon (Institute level or SIH) or any institute, state or national level project presentation competitions.	10%	10%
Total		**100%**	**100%**