SNJB's

Late Sau. Kantabai Bhavarlalji Jain

College of Engineering

(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

Shri Neminath Jain Brahmacharyashram (SNJB) (Jain Gurukul)

Neminagar, Chandwad - 423101, Dist. Nashik (MS, India).

Tele: (02556) 253750, Web: www.snjb.org, Email: principalcoe@snjb.org

ESTD - 1928

Curriculum and Evaluation Scheme for Third Year B. Tech. in Computer Engineering with Multidisciplinary Minor and Honor

To be implemented for 2024-28 Batch

(With Effect from Academic Year 2026-27)

CHAIRMAN
BOARD OF STUDIES COMPUTER ENGINEERING
SNJB's
LSKBJ COLLEGE OF ENGINEERING
Chandwad Dist.Nashik

SNJB'S COLLEGE OF ENGINEERING Chandwad (Nashik) Pin-423101

CHAIRMAN
ACADEMIC COUCIL
SNJB's
LSKBJ COLLEGE OF ENGINEERING
Chandwad Dist.Nashik

SNJB's Late Sau. K. B. Jain College of Engineering, Chandwad

(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

Curriculum and Evaluation Scheme for Third Year B. Tech. in Computer Engineering with Multidisciplinary Minor and Honor

To be implemented for 2024-28 Batch

(With Effect from Academic Year 2026-27)

Vision of the Institute

Transform young aspirant learners towards creativity and professionalism for societal growth through quality technical education.

Mission of the Institute

1. To transfer the suitable technology, particularly for rural development.
2. To enhance diverse career opportunities among students for building a nation.
3. To acquire the environment of learning to bridge the gap between industry and academics.
4. To share values, ideas, and beliefs by encouraging faculties and students for the welfare of society.

Vision of the Computer Engineering Department

To empower young generations for significant contributions in the field of computer engineering through excellence in knowledge, technical education, and innovation to cater the industrial demands and societal needs.

Mission of the Computer Engineering Department

1. To achieve academic excellence by inculcating basic and latest knowledge in which new ideas flourish.
2. To undertake collaborative training which offers opportunities for long-term interaction with academia and industry.

Program Outcomes (POs) for an engineering graduate:

PO1: Engineering Knowledge: Apply knowledge of mathematics, natural science, computing, engineering fundamentals and an engineering specialization as specified in WK1 to WK4 respectively to develop the solution of complex engineering problems.

PO2: Problem Analysis: Identify, formulate, review research literature and analyze complex engineering problems reaching substantiated conclusions with consideration for sustainable development. (WK1 to WK4)

PO3: Design/Development of Solutions: Design creative solutions for complex engineering problems and design/develop systems/components/processes to meet identified needs with consideration for the public health and safety, whole-life cost, net zero carbon, culture, society and environment as required. (WK5)

PO4: Conduct Investigations of Complex Problems: Conduct investigations of complex engineering problems using research-based knowledge including design of experiments, modelling, analysis & interpretation of data to provide valid conclusions. (WK8).

PO5: Engineering Tool Usage: Create, select and apply appropriate techniques, resources and modern engineering & IT tools, including prediction and modelling recognizing their limitations to solve complex engineering problems. (WK2 and WK6)

PO6: The Engineer and The World: Analyze and evaluate societal and environmental aspects while solving complex engineering problems for its impact on sustainability with reference to economy, health, safety, legal framework, culture and environment. (WK1, WK5, and WK7).

PO7: Ethics: Apply ethical principles and commit to professional ethics, human values, diversity and inclusion; adhere to national & international laws. (WK9)

PO8: Individual and Collaborative Team work: Function effectively as an individual, and as a member or leader in diverse/multi-disciplinary teams.

PO9: Communication: Communicate effectively and inclusively within the engineering community and society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations considering cultural, language, and learning differences

PO10: Project Management and Finance: Apply knowledge and understanding of engineering management principles and economic decision-making and apply these to one's own work, as a member and leader in a team, and to manage projects and in multidisciplinary environments.

PO11: Life-Long Learning: Recognize the need for, and have the preparation and ability for i) independent and life-long learning ii) adaptability to new and emerging technologies and iii) critical thinking in the broadest context of technological change. (WK8)

Program Specific Outcomes

1. **Professional Skills-**The ability to understand, analyze, and develop computer programs in the areas related to algorithms, system software, multimedia, web design, big data analytics, and networking for efficient design of computer-based systems of varying.
2. **Problem-Solving Skills-** The ability to apply standard practices and strategies in software project development using open-ended programming environments to deliver a quality product for business success.
3. **Successful Career and Entrepreneurship -** The ability to employ modern computer languages, environments, and platforms in creating innovative career paths to be an entrepreneur and a zest for higher studies.

SNJB's Late Sau. K. B. Jain College of Engineering, Chandwad

(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

Curriculum and Evaluation Scheme for Third Year B. Tech. in Computer Engineering with Multidisciplinary Minor and Honor

To be implemented for 2024-28 Batch

(With Effect from Academic Year 2026-27)

GENERAL COURSE STRUCTURE

A. Definition of Credit:

Table 1: Credit Definition

1 Hour Lecture (L) per week	1 Credit
1 Hour Tutorial (T) per week	1 Credit
2 Hours Practical (P) per week	1 Credit

B. Range of Credits: (B.Tech. or Equivalent) in Tech. with Multidisciplinary Minor:

In the light of the fact that a typical NEP Compliant Model Four-year Undergraduate degree program in Technology has about 176 credits, the total number of credits proposed for the four-year B.Tech. in **Computer Engineering** with Multidisciplinary minor degree is kept as **172.**

Table 2: Range of Credits

Course Category		Credits As PER NEP Guidelines	Proposed Credits
Basic Science Course	BSC/ESC	14-18	15
Engineering Science Course		16-12	14
Programme Core Course (PCC)	Program Courses	44-56	47
Programme Elective Course (PEC)		20	20
Multidisciplinary Minor (MD M)	Multidisciplinary Courses	14	17
Open Elective (OE) Other than a particular program		8	8
Vocational and Skill Enhancement Course (VSEC)	Skill Courses	8	8
Ability Enhancement Course (AEC)	Humanities Social Science and Management (HSSM)	4	6
Entrepreneurship/Economics/ Management Courses		2	4
Indian Knowledge System (IKS)		2	2
Value Education Course (VEC)		4	5
Research Methodology(RM)	Experiential Learning Courses	4	4
Community Engagement Project (CEP)/ Field Project (FP)		2	2
Project		4	5
Internship/ OJT		12	12
Co-curricular Courses (CC)	Liberal Learning Courses	4	3
Total Credits		**160-176**	**172**

C. Semester wise Credit Distribution Structure for Four Year B. Tech in Computer Engineering with Multidisciplinary Minor:

Table3: Semester-wise Credit Distribution Structure

Semester		I	II	III	IV	V	VI	VII	VIII	Total Credits
Basic Science Course	BSC/ESC	8	7	-	-	-	-	-	-	15
Engineering Science Course		7	7	-	-	-	-	-	-	14
Programme Core Course (PCC)	Program Courses	-	3	11	8	9	4	9	3	47
Programme Elective Course (PEC)		-	-	-	-	6	5	6	3	20
Multidisciplinary Minor (MD M)	Multidisciplinary Courses	-	-	3	3	3	2	3	3	17
Open Elective (OE) Other than a particular program		-	-	-	3	2	3	-	-	8
Vocational and Skill Enhancement Course (VSEC)	Skill Courses	2	2	-	2	-	2	-	-	8
Ability Enhancement Course (AEC)	Humanities Social Science and Management (HSSM)	1	-	1	2	2	-	-	-	6
Entrepreneurship/Economics/ Management Courses		-	-	2	2	-	-	-	-	4
Indian Knowledge System (IKS)		2	-	-	-	-	-	-	-	2
Value Education Course (VEC)		-	-	3	2	-	-	-	-	5
Research Methodology	Experiential Learning Courses	-	-	-	-	-	4	-	-	4
Community Engagement Project (CEP)/ Field Project (FP)		-	-	2	-	-	-	-	-	2
Project		-	-	-	-	-	2	3	-	5
Internship / OJT		-	-	-	-	-	-	-	12	12
Co-curricular Courses (CC)	Liberal Learning Courses	1	2	-	-	-	-	-	-	3
Total Credits (Major)		**21**	**21**	**22**	**22**	**22**	**22**	**21**	**21**	**172**

Students can opt for any of the following as per the rules and regulations given by the institute:

1. B. Tech with Multidisciplinary Minor = Total 172 Credits
2. **B. Tech with Multidisciplinary Minor and Honor = Total 190 Credits**

HONORS

- In addition to 172 credits of B. Tech Programmes (Bachelor of Technology) i.e. Major in which the student has taken admission, a student may opt for Honors in the same Tech. discipline/branch / Emerging Areas.
- A student is required to earn an additional 18 credits in the same Tech. discipline/ branch / Emerging Areas for Honors distributed over semesters III to VIII.
- The total number of credits required to complete the Honors in the same Tech. discipline/ Emerging Areas is 18 credits, in addition to 172 credits in Major.
- Students will have to compulsorily choose Honors from the same Tech. discipline/branch.
- Honors Degree in the Bachelor of Engineering programme shall be awarded to students earning additional total credits of all six semesters from the second year to final year, i.e., 18 Credits, in addition to 172 credits or 130 credits respectively. The student admitted in the first year must earn 172 credits and 130 credits admitted in lateral entry (admitted after Diploma or B.Sc.) in the second year.
- Minor Courses can be completed through an online platform.

The student has to choose One Honor out of the Two Honor groups provided below

Honors offered by Computer Engineering are as follows:

Table 4: Honors

Sr No	Name of Honors Offered by Department
A.	Blockchain Technologies
B.	Cyber Security

The detailed syllabus structure for the same is as follows:

Table 5A: Specialization Honors in Blockchain Technologies

Sr. No	Category	SEM	Course Code	Course Name	Teaching Scheme				
					Hours				Credits
					L	T	P	Total Hours	
01	HOC	III	24-HOC-CS-2-01A	Foundation of Blockchain Technology	3	-	-	3	3
02	HOC	IV	24-HOC-CS-2-02A	Decentralize and Blockchain Technologies	3	-	-	3	3
03	HOC	V	24-HOC-CS-3-03A	Blockchain Architecture Design	3	-	-	3	3
04	HOC	VI	24-HOC-CS-3-04A	Smart Contract and Cryptocurrency	3	-	-	3	3
05	HOC	VII	24-HOC-CS-4-05A	Blockchain Security	3	-	-	3	3
06	HOC	VIII	24-HOC-CS-4-06A	Blockchain Applications	3	-	-	3	3
Total					**18**	-	-	**18**	**18**

Table 5B: Specialization Honors in Cyber Security

Sr. No	Category	SEM	Course Code	Course Name	Teaching Scheme				
					Hours				Credits
					L	T	P	Total Hours	
01	HOC	III	24-HOC-CS-2-01B	Cryptography and Network Security	3	-	-	3	3
02	HOC	IV	24-HOC-CS-2-02B	Information Security	3	-	-	3	3
03	HOC	V	24-HOC-CS-3-03B	Ethical Hacking	3	-	-	3	3
04	HOC	VI	24-HOC-CS-3-04B	Digital Forensic	3	-	-	3	3
05	HOC	VII	24-HOC-CS-4-05B	Network Forensics and Cyber Threat Analysis	3	-	-	3	3
06	HOC	VIII	24-HOC-CS-4-06B	Cyber Physical Systems	3	-	-	3	3
Total					**18**	-	-	**18**	**18**

#Note for NPTEL/SYAYAM: Approved courses and platforms will be enlisted timely by authorities along with rules and regulations

SNJB's Late Sau. K. B. Jain College of Engineering, Chandwad

(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

Curriculum and Evaluation Scheme for Third Year B. Tech. in Computer Engineering with Multidisciplinary Minor and Honor

To be implemented for 2024-28 Batch

(With Effect from Academic Year 2026-27)

Honors Syllabus for SEM V

24-HOC-CS-3-03A : Blockchain Architecture Design

Teaching Scheme: Theory: 3 Hours/Week	**Credit:** 3	**Examination Scheme:** **SEE** : 100 Marks

Prerequisites Courses: 24-HOC-CS-2-01A Foundation of Blockchain Technology

Companion Course: NA

Course Objectives:

- To provide in-depth understanding of blockchain architecture, transaction lifecycle, and system design.
- To explore consensus protocols and analyze their applicability in different blockchain environments.
- To familiarize students with enterprise blockchain platforms and frameworks such as Hyperledger Fabric.
- To understand blockchain applications across domains like finance, supply chain, governance, and healthcare.
- To study advanced security, privacy, and interoperability challenges in blockchain systems.
- To understand different blockchain ecosystems and identify emerging trends for future applications.

Course Outcomes:

After completion of the course, learners should be able to

CONo	CO	BL
1	Study and understand blockchain architecture, transaction flow, and scalability challenges.	2
2	Understand various consensus protocols and study their performance in permissioned and permissionless environments.	2
3	Implement enterprise blockchain solutions using Hyperledger Fabric and Composer.	3
4	Interpret blockchain use cases in industries such as finance, supply chain, and e-governance.	2
5	Understand different blockchain platforms (Ethereum, Quorum, Corda) and identify future trends like Web3, CBDCs, and blockchain with AI/IoT.	2

Course Contents

Unit I	**Blockchain Architecture and System Design**	**8 Hours**

Layered blockchain architecture, Transaction flow and lifecycle, Block structure and validation, Network nodes and peer-to-peer communication, Scalability challenges and solutions

#Exemplar/Case Studies- Study Bitcoin block structure and transaction validation.

***Mapping of Course Outcomes**	**CO1**

Unit II	**Consensus Protocols**	**7 Hours**
Byzantine Fault Tolerance models (PBFT, RAFT, Tendermint), Proof-of-Stake and Delegated PoS, Hybrid consensus models, Consensus scalability and performance trade-offs, Security and attack models		
#Exemplar/Case Studies- Analyze PBFT consensus in Hyperledger Fabric.		
***Mapping of Course Outcomes**	**CO2**	
Unit III	**Enterprise Blockchain Frameworks**	**8 Hours**
Hyperledger Fabric architecture and components (peers, orderers, channels), Transaction endorsement and validation, Hyperledger Composer for business networks, Chaincode development and deployment, Blockchain-as-a-Service platforms		
#Exemplar/Case Studies- Implement Walmart supply chain solution using Hyperledger Fabric.		
***Mapping of Course Outcomes**	**CO3**	
Unit IV	**Security and Privacy in Blockchain**	**In 8 Hours**
Access control and identity in blockchain networks, Privacy mechanisms in Fabric (channels, SideDB), Zero-Knowledge Proofs (ZKPs) and advanced cryptographic techniques, Interoperability challenges, Scalability solutions (sharding, Layer-2)		
#Exemplar/Case Studies- Study Zero-Knowledge Proofs in Zcash privacy transactions.		
***Mapping of Course Outcomes**	**CO1, CO2, CO5**	
Unit V	**Comparative Ecosystems and Future Trends**	**7 Hours**
Ethereum (EVM, smart contracts, gas model), Quorum (enterprise-grade Ethereum), Corda (design philosophy and transaction model), Blockchain with AI, IoT, and Big Data, Emerging trends: Web3, Metaverse, Central Bank Digital Currencies (CBDCs)		
#Exemplar/Case Studies: Compare Corda adoption in R3 banking consortia.		
***Mapping of Course Outcomes**	**CO4,CO5**	
Unit VI	**Blockchain Applications in Industry**	**7 Hours**
Financial services and digital payments, Supply chain and provenance tracking, Healthcare data management, E-governance and identity management, Case studies of blockchain adoption		
#Exemplar/Case Studies- Evaluate Estonia's e-Governance blockchain identity system.		
***Mapping of Course Outcomes**	**CO3, CO4**	
Text Books		
T1: Imran Bashir, *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained*, Packt Publishing, 2018.		

T2: Narayan Prusty, *Foundations of Blockchain: The pathway to cryptocurrencies and decentralized blockchain applications*, Packt Publishing, 2019.
T3: Joseph Holbrook, *Architecting Enterprise Blockchain Solutions*, Wiley, 2020.

Reference Books :

R1: Kavita Saini, Pethuru Chelliah, Deepak Saini, *Essential Enterprise Blockchain Concepts and Applications*, CRC Press, 2022**.**
R2: Udai Pratap Rao, Piyush Kumar Shukla, Chandan Trivedi, Sweta Gupta, Zelalem Sintayehu Shibeshi, Blockchain for Information Security and Privacy, CRC Press, 2021.
R3: Zhengxiang Shi, Xiaoqing Feng, *Advanced Blockchain Technology: Frameworks and Enterprise-Level Practices*, Springer, 2022.

Additional Resources: (Books, e-Resources)

1. https://intellipaat.com/blog/tutorial/blockchain-tutorial/how-does-blockchain-work/
2. https://www.youtube.com/watch?v=rCjVfuR93dk
3. https://www.youtube.com/watch?v=cFVGBxYiBFo
4. https://www.youtube.com/watch?v=KltWJERR6u4

E-Resources:

1. https://blockchain.cse.iitk.ac.in/slides-NPTEL-BlockchainTechnologyApplications.pdf
2. https://users.cs.fiu.edu/~prabakar/cen5079/Common/textbooks/Mastering_Blockchain_2nd_Edition.pdf
3. https://mrcet.com/downloads/digital_notes/CSE/IV%20Year/17062023/BLOCK%20CHAIN%20TECHNOLOGY[R20A0522].pdf (DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY)

MOOC Courses links :

1. NPTEL Course "Introduction to Blockchain Technology & Applications"(NPTEL)
https://nptel.ac.in/courses/106/104/106104220/
2. NPTEL Course on "Blockchain Architecture & UseCases"(NPTEL)
https://nptel.ac.in/courses/106/105/106105184/
3. Blockchain and its Applications, IIT Kharagpur(NPTEL)
https://nptel.ac.in/courses/106105235
4. Blockchain, By Dr.Mayank Aggarwal (Swayam)
https://onlinecourses.swayam2.ac.in/aic21_ge01/preview

24-HOC-CS-3-03B: Ethical Hacking

Teaching Scheme: Theory: 3 Hours/Week	**Credit:** 3	**Examination Scheme:** **SEE**: 100 Marks

Prerequisites Courses: 24-HOC-CS-2-01B: Cryptography and Network Security, 24-HOC-CS-2-02B: Information Security

Companion Course: NA

Course Objectives:

- To Understand the fundamentals of ethical hacking and networking.
- To Demonstrate reconnaissance and information-gathering techniques to identify
- To Demonstrate vulnerability analysis and system exploitation using standard tools.
- To implement appropriate methods to mitigate risks from network-based attacks and social engineering techniques.
- To Describe the use of cryptographic algorithms for ensuring confidentiality, integrity, and authenticity.
- To Apply advanced cryptographic techniques to solve problems in network security

Course Outcomes:

After completion of the course, learners should be able to

CONo	CO	BL
1	**Understand** the fundamentals of ethical hacking, networking concepts, and related legal/ethical aspects.	2
2	**Apply** reconnaissance and information-gathering techniques using tools such as Nmap	3
3	**Conduct** vulnerability scanning and system exploitation using standard tools like Nessus and Metasploit.	3
4	**Apply** techniques to identify network-based attacks and social engineering strategies in given scenarios.	3
5	**Describe** cryptographic algorithms for ensuring confidentiality, integrity, and authenticity of information.	2
6	**Use** advanced cryptographic methods to secure and protect modern network environments	3

Course Contents

Unit I	**Foundations of Ethical Hacking and Networking**	**7 Hours**

Introduction to Ethical Hacking, Basic Concepts of Networking, TCP/IP Protocol Stack,IP addressing and routing ,TCP and UDP, IP subnetting,Routing protocols: IP version 6

#Exemplar/Case Studies : Routing Protocol Behavior Analysis Using Cisco/Juniper Configurations and Packet Captures

***Mapping of Course Outcomes**	**CO1**

Unit II	**Reconnaissance & Information Gathering**	**7 Hours**

Information Gathering (Reconnaissance) – Concepts & Methods,Nmap Features & Capabilities, Exploration of Nmap Features

,Introduction to Port Scanning with Nmap, Port-Scanning Techniques Using Nmap, Software Installation and Network Setup		
#Exemplar/Case Studies: Comparative study of Nmap scanning modes		
***Mapping of Course Outcomes**	**CO2**	
Unit III	**Vulnerability Scanning & System Exploitation**	**7 Hours**
Security Scanning and Proxy Preparation,System Hacking, Malware, Trojans, Virus and Worms,Miscellaneous Attacks,Elements of Hardware Security,Side Channel Attacks,Physical Unclonable Function,Hardware Trojan,Metasploit Framework, SQL Injection Error Based from Web Application, SQLMAP, Cross Site Scripting		
#Exemplar/Case Studies: Attack Demonstrations using Metasploit		
***Mapping of Course Outcomes**	**CO2,CO3**	
Unit IV	**Network Attacks & Social Engineering**	**7 Hours**
Packet Sniffing:Fundamentals of packet sniffing and network traffic monitoring,Working of packet sniffing tools,**Social Engineering Attack**:Overview of social engineering and human-based exploitation techniques,Types of social engineering attacks,**Denial of Service Attack:**Introduction to DoS and Distributed DoS (DDoS) attacks,Types of DoS attacks		
#Exemplar/Case Studies : The NMAP Tool: A Relook		
***Mapping of Course Outcomes**	**CO4**	
Unit V	**Cryptography Fundamentals**	**7 Hours**
Basic concepts of cryptography, Private-key cryptography ,Public-key cryptography, Public-key cryptography ,Cryptographic hash functions,Digital signature and certificate, Applications		
#Exemplar/Case Studies: Describe how RSA digital signatures are used to secure online banking transactions		
***Mapping of Course Outcomes**	**CO5**	
Unit VI	**Advanced Cryptographic Applications**	**7Hours**
Steganography: techniques, tools for detection. **Biometrics:**principles of biometric systems, common vulnerabilities, methods to enhance their security, various network-based attacks, DNS and Email Security		
#Exemplar/Case Studies: Describe how Wireshark is used for network analysis		
***Mapping of Course Outcomes**	**CO6**	
Learning Resources		
Text Books		
T1. Krutz Ronald L, " The Ceh Prep Guide - The Comprehensive Guide To Certified", John Wiley And Sons; 2008, ISBN: 06558 **T2.**Fadia Ankit, "Network Intrusion Alert - An Ethical Hacking Guide To Intrusion Detection", Vikas Publishing House Pvt Ltd;		

2007, ISBN: 04268..

Reference Books :

R1. Fadia Ankit,"An Unofficial Guide To Ethical Hacking", Macmillan India Ltd; 2006
R2. Fadia Ankit," Google Hacking - An Ethical Guide", Vikas Publishing House Pvt Ltd; 2007
R3. Georgia Weidman, Penetration Testing: A Hands-On Introduction to Hacking, No Starch Press, 2014.
R4. William Stallings, Cryptography and Network Security: Principles and Practice (8th Edition), Pearson, 2019.

Additional Resources: (Books, e-Resources)
https://drive.google.com/drive/folders/1n2ZfPKxOuS-qhFRnUzVOMbngcneI_DTC?usp=drive_link

MOOC Courses links :

- SWAYAM / NPTEL Course – Ethical Hacking (National Open University, India)
  https://onlinecourses.swayam2.ac.in/nou22_cs05/preview
- Coursera-Introduction to Cyber Security Specialization (by NYU)
  https://www.coursera.org/specializations/intro-cyber-security
- edX –Cybersecurity Fundamentals (by Rochester Institute of Technology)
  https://www.edx.org/course/cybersecurity-fundamentals
- Udemy – Practical Ethical Hacking – The Complete Course
  https://www.udemy.com/course/practical-ethical-hacking/

SNJB's Late Sau. K. B. Jain College of Engineering, Chandwad

(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

Curriculum and Evaluation Scheme for Third Year B. Tech. in Computer Engineering with Multidisciplinary Minor and Honor

To be implemented for 2024-28 Batch

(With Effect from Academic Year 2026-27)

Honors Syllabus for SEM VI

24-HOC-CS-3-04A : Smart Contract and Cryptocurrency

Teaching Scheme: Theory: 3 Hours/Week	**Credit:** 3	**Examination Scheme:** **SEE** : 100 Marks

Prerequisites Courses: 24-HOC-CS-2-01A Foundation of Blockchain Technology

Companion Course: NA

Course Objectives:

- To provide a comprehensive understanding of smart contracts, their design, lifecycle, and deployment on blockchain platforms.
- To develop practical skills in programming and deploying smart contracts using Solidity, Hyperledger Fabric, and related tools.
- To study the architecture, functioning, and transaction mechanisms of cryptocurrencies like Bitcoin and Ethereum.
- To implement and analyze various consensus mechanisms and token contracts (PoW, PoS, ERC-20, ERC-721).
- To understand security vulnerabilities, privacy concerns, and emerging trends in smart contracts and cryptocurrencies.
- To study and assess different blockchain platforms, frameworks, and real-world use cases for decision-making.

Course Outcomes:

After completion of the course, learners should be able to

CONo	CO	BL
1	Study and understand smart contracts, their lifecycle, and deployment process	2
2	Implement smart contracts on Ethereum and Hyperledger Fabric using Solidity/chaincode	3
3	Understand cryptocurrency architecture, wallets, and transaction flows	2
4	Implement consensus algorithms (PoW, PoS) and token contracts (ERC-20, ERC-721)	3
5	Interpret security, privacy issues, and emerging trends like NFTs, DeFi, and Web3	2
6	Explore blockchain platforms and smart contract frameworks for real-world use cases.	2

Course Contents

Unit I	**Introduction to Smart Contracts**	**8 Hours**

Concept & origin of smart contracts, Contract lifecycle: creation, deployment, execution, Advantages & limitations compared to traditional contracts.

#Exemplar/Case Studies- Study the "Hello Blockchain" smart contract deployment and execution on Remix IDE

***Mapping of Course Outcomes**	**CO1**

Unit II	**Smart Contract Programming & Tools**	**7 Hours**
Solidity basics: data types, functions, modifiers, events, Development environments: Remix, Truffle, Ganache, Oracles and external data integration.		
#Exemplar/Case Studies- Implement a voting smart contract on Ganache using Truffle and Solidity		
***Mapping of Course Outcomes**	**CO1, CO2**	
Unit III	**Smart Contract Platforms & Use Cases**	**8 Hours**
Ethereum Virtual Machine (EVM) & gas model, Hyperledger Fabric chaincode basics, Case studies: supply chain, voting, healthcare, finance.		
#Exemplar/Case Studies-Analyze Ethereum supply chain smart contract and Hyperledger Fabric chaincode for asset tracking		
***Mapping of Course Outcomes**	**CO2,CO6**	
Unit IV	**Foundations of Cryptocurrency**	**7 Hours**
Smart Contracts: Evolution of digital money & cryptocurrencies, Bitcoin architecture: transactions, blocks, mining, Wallets, keys, and addresses.		
#Exemplar/Case Studies- Study Bitcoin wallet creation, transaction simulation, and ledger verification using Python		
***Mapping of Course Outcomes**	**CO3**	
Unit V	**Consensus Mechanisms and Crypto Economics**	**8 Hours**
Consensus in cryptocurrencies (PoW, PoS, DPoS, PBFT), Tokenomics: coins vs tokens, stablecoins, governance tokens, ICOs, DeFi, DAOs, and exchanges.		
#Exemplar/Case Studies- Implement Proof-of-Work and Proof-of-Stake algorithms and ERC-20 token contract in Solidity		
***Mapping of Course Outcomes**	**CO4**	
Unit VI	**Security, Privacy and Future of Cryptocurrency**	**7 Hours**
Attacks: double spending, 51% attack, Sybil attack, Smart contract vulnerabilities in crypto (reentrancy, overflow), Privacy coins (Monero, Zcash), CBDCs, NFTs, Web3 trends.		
#Exemplar/Case Studies: Evaluate a vulnerable smart contract for reentrancy attack and implement fixes; deploy simple NFT (ERC-721) contract		
***Mapping of Course Outcomes**	**CO4,CO5,CO6**	
Text Books		
T1: Joseph Holbrook, *Architecting Enterprise Blockchain Solutions*, Wiley, 2020, ISBN: 978-1119557692 **T2:** Narayan Prusty, *Foundations of Blockchain: The pathway to cryptocurrencies and decentralized blockchain applications*, Packt		

Publishing, 2019, ISBN: 978-1788834047
T3: Andreas M. Antonopoulos, *Mastering Ethereum: Building Smart Contracts and DApps*, O'Reilly, 2018, ISBN: 978-1491971949

Reference Books :

R1: Imran Bashir, *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained*, Packt Publishing, 2nd Edition, 2018, ISBN: 978-1788839044
R2: Udai Pratap Rao, Piyush Kumar Shukla, Chandan Trivedi, Sweta Gupta, Zelalem Sintayehu Shibeshi, *Blockchain for Information Security and Privacy*, CRC Press, 2021, ISBN: 978-0367654481
R3: Andreas M. Antonopoulos, *Mastering Blockchain*, O'Reilly, Second Edition, ISBN: 978-1-491-95438-6.

Additional Resources: (Books, e-Resources)

1. https://intellipaat.com/blog/tutorial/blockchain-tutorial/how-does-blockchain-work/
2. https://www.youtube.com/watch?v=rCjVfuR93dk
3. https://www.youtube.com/watch?v=cFVGBxYiBFo
4. https://www.youtube.com/watch?v=KItWJERR6u4

E-Resources:

1. https://blockchain.cse.iitk.ac.in/slides-NPTEL-BlockchainTechnologyApplications.pdf
2. https://users.cs.fiu.edu/~prabakar/cen5079/Common/textbooks/Mastering_Blockchain_2nd_Edition.pdf
3. https://mrcet.com/downloads/digital_notes/CSE/IV%20Year/17062023/BLOCK%20CHAIN%20TECHNOLOGY[R20A0522].pdf (DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY)

MOOC Courses links :

1. NPTEL Course "Introduction to Blockchain Technology & Applications"(NPTEL)
https://nptel.ac.in/courses/106/104/106104220/
2. NPTEL Course on "Blockchain Architecture & UseCases"(NPTEL)
https://nptel.ac.in/courses/106/105/106105184/
3. Blockchain and its Applications, IIT Kharagpur(NPTEL)
https://nptel.ac.in/courses/106105235
4. Blockchain, By Dr.Mayank Aggarwal (Swayam)
https://onlinecourses.swayam2.ac.in/aic21_ge01/preview

24-HOC-CS-3-04B: Digital Forensic		
Teaching Scheme: Theory: 3 Hours/Week	**Credit:** 3	**Examination Scheme** **SEE**: 100 Marks

Prerequisites Courses: 24-PCC-CS-3-02 Computer Network, 24-PEC-CS-3-01B Information and Network Security.

Companion Course:

Course Objectives:

- Understand the fundamental concepts of computer forensics, cybercrime, and the evolution of digital investigations.
- Gain knowledge of digital evidence, investigation processes, and the roles of first responders in handling cyber incidents
- Analyse various file systems and operating system artefacts to extract, preserve, and examine digital evidence.
- Develop practical skills in Windows, Linux, and network forensics using standard forensic tools and techniques.
- Apply password cracking, web, wireless, and email forensic techniques to investigate cyber incidents effectively.
- Prepare professional forensic reports, document evidence, and understand legal and ethical aspects of digital forensic investigations.

Course Outcomes:

After completion of the course, learners should be able to

CONo	**CO**	**BL**
CO 1	Understand the principles of computer forensics, cybercrime types, and the investigation lifecycle.	2
CO 2	Identify, acquire, and preserve digital evidence using appropriate tools and techniques to ensure its integrity and authenticity.	3
CO 3	Analyse Windows, Linux, and network systems to recover deleted files, partitions, and volatile/non-volatile information.	4
CO 4	Conduct network traffic analysis, packet sniffing, and web vulnerability assessment using different forensic tools	4
CO 5	Perform password cracking, email forensics, mobile device investigations, and metadata analysis to gather actionable evidence.	5
CO 6	Prepare comprehensive forensic reports and present findings in a professional and legally admissible manner.	6

Course Contents		
Unit I	**Introduction to Digital Forensics**	**6 Hours**
Definition of Computer Forensics, Cyber Crime, Evolution of Computer Forensics, Objectives of Computer Forensics, Roles of Forensics Investigator, Forensics Readiness, Steps for Forensics. **Computer Forensics Investigation Process**: Digital Forensics Investigation Process, Digital Forensics Investigation Process-Assessment Phase, Acquire the Data, Analyse the Data, Report the Investigation		
#Exemplar/Case Studies - Unauthorised File Deletion in a Student Lab Computer using Recuva (File Recovery Tool)		
***Mapping of Course Outcomes**	**CO1**	
Unit II	**Digital Evidence and File System**	**6 Hours**
Digital Evidence, Digital Evidence Investigation Process, First Responders Toolkit, Issues Facing Computer Forensics, Types of Investigation, and Techniques in Digital Forensics. **File System:** Digital Evidence, Digital Evidence Investigation Process, First Responders Toolkit, Issues Facing Computer Forensics, File System, Types of File Systems		
#Exemplar/Case Studies - Unauthorised File Copying Using a USB Drive in a College Lab using - FTK Imager, Autopsy (Sleuth Kit), USBDeview tools		
***Mapping of Course Outcomes**	**CO2**	
Unit III	**Windows Forensics & Recovering Deleted Files and Partitions**	**6 Hours**
Windows Forensics, Volatile and Non-Volatile Information, Recovering deleted files and partitions, Windows Forensics Summary, **Digital Forensics Roadmap:** FTK Imager, Static Data Acquisition from Windows using FTK Imager, Live Data Acquisition using FTK Imager, Installation of KALI Linux, RAM Dump Analysis using Volatility, Static Data Acquisition from Linux OS. **Recovering Deleted Files and Partitions:** Digital Forensics Tools, Overview of EnCase Forensics, **Deep Information Gathering Tool:** Dmitry Page, Computer Forensics Live Practical by using Autopsy and FTK Imager		
#Exemplar/Case Studies - Recovering Deleted Assignment Files from a Windows Computer - Volatility (RAM dump analysis)		
***Mapping of Course Outcomes**	**CO3**	
Unit IV	**Network Forensics, Logs, and Event Analysis**	**6 Hours**
Introduction to Network Forensics, Network Components and their forensic importance, OSI Internet Layers and their Forensic importance, **Tools Introduction Wireshark and TCPDUMP:** Packet Sniffing and Analysis using Ettercap and Wireshark, Network Forensics, Wireshark Packet Analyser, Packet Capture using TCP DUMP, **Website Penetration:** WHOIS, nslookup. **Logs & Event Analysis:** Forensic Analysis using AUTOPSY: Linux and Windows, Forensics and Log analysis, Compare and AUDIT Evidences using Hashdeep Page, **Data Carving using Bulk Extractor:** Kali Linux and Windows, Recovering Evidence from Forensic Images using Foremost		

#Exemplar/Case Studies - Detecting Data Exfiltration through Suspicious Network Traffic - Wireshark, TCPDUMP, WHOIS, nslookup, Bulk Extractor, Hashdeep		
***Mapping of Course Outcomes**	**CO4**	
Unit V	**Application Password Cracking & Wireless and Web Attacks**	**6 Hours**
Introduction to Password Cracking, Password Cracking using John the Ripper, Password Cracking using Rainbow Tables, PDF File Analysis, Remote Imaging using E3 Digital Forensics. **Wireless and Web Attacks:** WiFi Packet Capture and Password Cracking using Aircrack-ng, Introduction to Web Attacks, Website Copier: HTTRACK, SQL Injection, **Site Report Generation:** Netcraft, **Vulnerability Analysis:** Nikto, Wayback Machine, Deep Information Gathering Tool: Dmitry, Image Metadata Extraction using Imago		
#Exemplar/Case Studies: authorised campus security investigation/penetration test using tools John the Ripper, HTTrack, Nikto, sqlmap, Dmitry, Netcraft, Wayback Machine		
***Mapping of Course Outcomes**	**CO5**	
Unit VI	**Email and Mobile Device Forensics**	**6 Hours**
Email Forensics Investigations, Mobile Forensics, Preparation for Digital Forensic investigation, Introduction to Report Writing, Forensic Reports & Expert Witness, Demonstration of Some Forensics Tools		
#Exemplar/Case Studies: Investigation of Phishing Email and Mobile Device in an Insider Data Leak using MailXaminer, Cellebrite		
***Mapping of Course Outcomes**	**CO6**	
Learning Resources		
Text Books		
T1. "Guide to Computer Forensics and Investigations" – Bill Nelson, Amelia Phillips, Christopher Steuart, 6th Edition, Cengage Learning. **T2.** "Network Forensics: Tracking Hackers through Cyberspace" – Sherri Davidoff, Jonathan Ham, Prentice Hall. **T3.** "Incident Response & Computer Forensics" – Jason Luttgens, Matthew Pepe, Kevin Mandia, 3rd Edition, McGraw-Hill.		
Reference Books :		
R1. "Computer Forensics: Cybercriminals, Laws, and Evidence" – Marjie T. Britz, 4th Edition, Cengage Learning. **R2.** "Practical Computer Forensics" – David Cowen, Wiley, 3rd Edition. **R3.** "Digital Evidence and Computer Crime" – Eoghan Casey, 4th Edition, Academic Press.		
Additional Resources: (Books, e-Resources)		
MOOC Courses links : • https://onlinecourses.swayam2.ac.in/nou22_cs05/preview