RAJALAKSHMI
ENGINEERING COLLEGE
An AUTONOMOUS Institution
Affiliated to ANNA UNIVERSITY, Chennai

# RAJALAKSHMI ENGINEERING COLLEGE

# CURRICULUM AND SYLLABUS

# DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING REGULATIONS R2019

## VISION

- To promote highly ethical and innovative computer professionals through excellence in teaching, training and research.

## MISSION

- To produce globally competent professionals, motivated to learn the emerging technologies and to be innovative in solving real world problems.
- To promote research activities amongst the students and the members of faculty that could benefit the society.
- To impart moral and ethical values in their profession.

# MINOR DEGREE IN BLOCKCHAIN AND CYBER SECURITY

Blockchain is a way of recording peer-to-peer transactions in a distributed public ledger. The Blockchain Minor explores the fundamentals of the public (and private), transparent, secure, tamper-resistant, and distributed databases known as block chain. Students will learn how to develop smart contracts as self-executing programs that run on the blockchain and be introduced to cutting-edge research results and developments as blockchain technology evolves.

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorised exploitation of systems, networks, and technologies. Students will deepen their understanding of cybersecurity concepts and principles. Learn offensive and defensive cybersecuritytechniques.Develop professional skills to apply cybersecurity knowledge to the general area of their majors.

| S. No. | Subject Code | Subject Name | L | T | P | C |
|---|---|---|---|---|---|---|
| 1 | MCS19045 | Fundamentals of Blockchain | 3 | 0 | 2 | 4 |
| 2 | MCS19046 | Blockchain Security and Performance | 3 | 0 | 2 | 4 |
| 3 | MCS19002 | BlockchainforFinTech | 3 | 0 | 0 | 3 |
| 4 | MCS19047 | Ethical Hacking and Security | 3 | 0 | 2 | 4 |
| 5 | CS19P14 | Information Security And Management | 3 | 0 | 0 | 3 |
| | | **Total** | **15** | **0** | **6** | **18** |

# SYLLABUS

| Subject Code | Subject Name | L | T | P | C |
|---|---|---|---|---|---|
| **MCS19045** | **Fundamentals of Blockchain** | **3** | **0** | **2** | **4** |
| **Course Objectives:** | | | | | |
| • | The students should be able to understand a broad overview of the essential concepts of blockchain technology. | | | | |
| • | To familiarize students with Bitcoin protocol followed by the Ethereum protocol – to lay the foundation necessary for developing applications and programming. | | | | |
| • | Students should be able to learn about different types of blockchain and consensus algorithms. | | | | |

| | | | |
|---|---|---|---|
| **UNIT – I** | **Basics of Blockchain** | | 9 |
| Distributed Database, Two General Problem, Byzantine General Problem and Fault Tolerance, Hadoop Distributed File System, Distributed Hash Table, ASIC resistance, Turing Complete. • Cryptography: Hash function, Digital Signature - ECDSA, Memory Hard Algorithm, and Zero Knowledge Proof. | | | |
| **UNIT – II** | **Technology Stack** | | 9 |
| Introduction, Advantage over conventional distributed database, Blockchain Network, Mining Mechanism, Distributed Consensus, Merkle Patricia Tree, Gas Limit, Transactions and Fee, Anonymity, Reward, Chain Policy, Life of Blockchain application, Soft & Hard Fork, Private and Public blockchain. | | | |
| **UNIT – III** | **Distributed Consensus** | | 9 |
| Nakamoto consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy utilization and alternate. | | | |
| **UNIT – IV** | **Cryptocurrency** | | 9 |
| History, Distributed Ledger, Bitcoin protocols - Mining strategy and rewards, Ethereum - Construction, DAO, Smart Contract, GHOST, Vulnerability, Attacks, Sidechain, Namecoin | | | |
| **UNIT – V** | **Cryptocurrency Regulation** | | 9 |
| Stakeholders, Roots of Bitcoin, Legal Aspects-Crypto currency Exchange, Black Market and Global Economy. Applications: Internet of Things, Medical Record Management System, Domain Name Service and future of Blockchain. | | | |
| | TOTAL HOURS | : | 45 |
| **Course Outcomes:**<br>Upon completion of the course, the students will be able to: | | | |
| • | Explain the basic notion of distributed systems. | | |
| • | Use the working of an immutable distributed ledger and trust model that definesblockchain | | |
| • | Illustrate the essential components of a blockchain platform. | | |
| • | Build their own cryptocurrency | | |
| • | Apply blockchain in various domains | | |

| **Lab Experiments:** |
|---|
| 1. Creating and Building Up Bitcoin Wallet |
| 2. Ethereum Wallet |
| 3. Building a Private Ethereum Network and Deploying Smart Contract |

| |
|---|
| 4. Ethereum Smart Contract |
| 5. Creating and Building Up Crypto Token. |
| 6. Creating a Business Network using Hyperledger |
| 7. Building and Deploying multichain private Blockchain |

**Text Book(s) / Reference Book(s)**

1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016
2. Kumar Saurabh, AshutoshSaxena, Blockchain Technology: Concepts and Applications, Wiley, 2020

**Reference Book(s)**

1. Andreas Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media; 1st edition, 2014

2. Gavin Wood, “ETHEREUM: A Secure Decentralized Transaction Ledger”, Yellow paper.2014.

3. Tiana Laurence, Blockchain for Dummies, 2nd Edition 2019, John Wiley & Sons.

4. Imran Bashir, Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks,Packt Publishing, 2017

**Online Resources**

1. https://www.coursera.org/specializations/blockchain.

2. https://nptel.ac.in/courses/106105184/

3.Introduction to Blockchain Technology and Applications, https://swayam.gov.in/nd1_noc20_cs01/preview

4. 2. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System

| Subject Code | Subject Name | L | T | P | C |
|---|---|---|---|---|---|
| **MCS19046** | **Blockchain Security and Performance** | **3** | **0** | **2** | **4** |

| **Course Objectives:** | |
|---|---|
| • | Students should be able to understand the security and performance-related issues ofblockchain. |
| • | Students should be able to learn techniques and tools to tackle the security related issues of blockchain. |
| • | Students should be able to learn new approaches required for enhancing blockchainperformance. |

| **UNIT – I** | **Security Issues** | 6 |
|---|---|---|
| Blockchain Related Issues, Higher-Level Language (Solidity) RelatedIssues, EVM Bytecode Related Issues, Real-Life Attacks on Blockchain Applications/Smart Contracts, Trusted Execution Environments. | | |
| **UNIT – II** | **Security Tools for Smart Contracts** | 12 |
| Working, Advantages, And Disadvantages ofTools- Oyente, Securify, Maian, Manticore, Mythril, SmartCheck, Verx. Secure KeyManagement, Quantum Resilience Keys. | | |
| **UNIT – III** | **Performance Related Issues** | 7 |
| Transaction Speed, Transaction Fees, Network Size,Complexity, Interoperability Problems, Lack of Standardization. Lack of SupportiveRegulations Related to Blockchain Applications. | | |
| **UNIT – IV** | **Performance Improvements** | 12 |
| Off-Chain State Channels, Sidechains, Parallels Chains,Concurrent Smart Contract Transactions, Sharding Technique and Its Benefits, AtomicSwaps Between Smart Contracts. | | |
| **UNIT - V** | **Blockchain Applications** | 8 |
| Decentralized Cryptocurrency, Distributed Cloud Storage, E-Voting, Insurance Claims, Cross-Border Payments, Asset Management, SmartAppliances. | | |
| | TOTAL HOURS : | 45 |

| **Course Outcomes:**<br>Upon completion of the course, the students will be able to: | |
|---|---|
| • | Understand the security perspective of blockchain technology. |
| • | Learn and apply security analysis and performance-enhancing techniques related toblockchain. |
| • | Understand the real-life applications of blockchain technology and apply it to provide solutions to some real-life problems. |
| • | Understand the performance of blockchain |
| • | Implement blockchain for various use cases |

| **Lab Experiments:** |
|---|
| 1. User Security |
| 2. Node Security |
| 3. Denial of Service Attacks, Eclipse Attacks, Replay Attacks, Routing Attacks, Sybil Attacks |
| 4. Securing Digital Payment Transactions |
| 5. Smart contract security |

**Text Book(s) / Reference Book(s)**

1. Mastering Ethereum: Building Smart Contracts and Dapps Book by AndreasAntonopoulos and Gavin Wood, Shroff Publisher/O′Reilly Publisher, 2018.
2. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, “BitcoinandCryptocurrency Technologies: A Comprehensive Introduction”, Princeton University Press, July, 2016.
3. SachinShetty, Charles A. Kamhoua, Laurent L. Njilla, Blockchain for Distributed Systems Security, Wiely, 2019
4. Rahul Neware Dr. Brajesh Kumar, Er. ParagRastogi ,Dr. HarshalPatil, BLOCKCHAIN SECURITY, Book Rivers; 1st edition, 2022
5. YassineMaleh , Mohammad Shojafar , MamounAlazab , ImedRomdhani,Blockchain For Cybersecurity And Privacy: Architectures Challenges And Applications, Taylor & Francis Ltd, 2020
6. Corresponding Online Resources: https://www.edx.org/course/blockchain-and-fintech-basics-applications-and-limitations

| Subject Code | Subject Name | L | T | P | C |
|---|---|---|---|---|---|
| **MCS19002** | **BlockchainforFintech** | **3** | **0** | **0** | **3** |

**Course Objectives:**

| | |
|---|---|
| • | To understand the benefits of using blockchain in financial sector. |
| • | To visualize how decentralized nature of blockchain is impacting banking and financial sector. |
| • | To get an insight on the trading logics in decentralized Markets |
| • | To understand the limitation of cryptocurrency Regulations |
| • | To know how blockchain regulations and future trends related to blockchain to be used in financial sector. |

| | | |
|---|---|---|
| **UNIT – I** | **Introduction** | 9 |
| Concept, Cryptocurrency Mining, Uses of Cryptocurrencies, Tokens, Token vs Crypto Coin, Concept of ICOs (Initial Coin Offerings), Benefits of Using ICOs, STOs (Security token offerings), ICO vs STO, Cryptocurrency wallets. | | |
| **UNIT – II** | **Decentralized Finance** | 9 |
| Concept, Benefits and Risks Associated with DeFi, Centralized vs Decentralized finance, DeFi Projects, DeFi future trends. | | |
| **UNIT – III** | **Decentralized Markets** | 9 |
| Concept of Decentralized markets, impact of decentralization on financial market, Decentralized Exchanges (DEX), Security, control and privacy concerns related to DEX, Liquidity and Usability of DEX, best DEXs for trading, Fund Management and Trading logic of DEX, Concept of Decentralized Web. | | |
| **UNIT – IV** | **Blockchain&Cryptocurrency Regulations** | 9 |
| Introduction, History Stance of the Government, Judicial Approach to Cryptocurrency, Possible Reasons for Ban, Virtual Currency Regulations, Global Perspective of Regulations on Blockchain, Future needs for Regulations. | | |
| **UNIT - V** | **Banking and Blockchain** | 9 |
| Cross-Border Payments Using Blockchain and Its Benefits, Study of blockchain platforms used for cross-border payments, Impact of Blockchain on Banking Services. Stable Coin: Concept, Uses and Types of Stable Coins,Case-Study: Tether and Libra Coins. | | |
| TOTAL HOURS | : | 45 |

**Course Outcomes:**
Upon completion of the course, the students will be able:

| | |
|---|---|
| • | To understand the basic of blockchain and currency in finance sector |
| • | To understand the trading logics in blockchain |
| • | To understand difference between different types of coins and tokens related to blockchain technology. |
| • | To understand the concept of decentralized markets. |
| • | To understand the concept of banking and block chain |

**Text Book(s) / Reference Book(s)**

1. Melanie Swan, Blockchain: Blueprint for a new economy, Shroff Publisher/O'Reilly Publisher, 2015.
2. Ron Quaranta, Blockchain in Financial Markets and Beyond: Challenges and Applications, Risk Books Publisher, 2017.

3. Richard Hayen, Blockchain&FinTech: A Comprehensive Blueprint to Understanding Blockchain& Financial Technology, 2017.
4. Jeff Reed, Bitcoin, FinTech, Smart Contracts, Cryptocurrency, Risk Books Publisher, 2016.
5. David KuoChuen Lee, Linda Low, Inclusive FintechBlockchain, Cryptocurrency and ICO, World Scientific Publishing Company Pvt Limited, 2018.

**Online Resources**

1. https://www.accenture.com/in-en/insight-blockchain-technology-how-banks-building-real-time
2. https://medium.com/search?q=decentralized%20exchange
3. Emerging Technology Projection: The Total Economic Impact™ Of IBM Blockchain https://www.ibm.com/downloads/cas/QJ4XA0MD
4. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/india#chaptercontent1
5. https://www.eduonix.com/blockchain-and-cryptocurrencies-for-beginners
6. https://www.coursera.org/learn/cryptocurrency

| Subject Code | Subject Name | L | T | P | C |
|---|---|---|---|---|---|
| **MCS19047** | **Ethical Hacking and Security** | **3** | **0** | **2** | **4** |

**Course Objectives:**

| | |
|---|---|
| ● | To introduce the basic concepts of Ethical Hacking and Penetration Testing |
| ● | To acquire knowledge about gathering information about the victim |
| ● | To demonstrate Enumeration and Port Scanning |
| ● | To learn about vulnerability scanning |
| ● | To learn about Malware |

| | | |
|---|---|---|
| **UNIT – I** | **Introduction to Ethical Hacking** | 9 |
| Important Terminologies Categories of Penetration Test Writing Reports Structure of PT report Vulnerability Assessment Summary Risk Assessment Methodology - Detailed Findings Reports | | |
| **UNIT – II** | **Information Gathering** | 9 |
| Active and Passive Information Gathering Sources Copying Website locally yougetsignal.com NeoTrace Intercepting a Response Acunetix Vulnerability Scanner NetCraft Google Hacking Interacting with DNS Servers DNS Cache Snooping | | |
| **UNIT – III** | **Enumeration And Port Scanning** | 9 |
| Host Discovery Scanning for Open Ports and Services Types of Port Scanning TCP Three-way handshake TCP Flags Port Status Types TCP SYN Scan TCP Connect Scan NULL, FIN and XMAS SCAN NULL Scan FIN Scan XMAS Scan TCP ACK Scan Responses UDP Port Scan Scanning a vulnerable host Performing an IDLE scan with NMAP Service Version Detection OS Fingerprinting | | |
| **UNIT – IV** | **Vulnerability Scanning** | 9 |
| Working with Vulnerability Scanners Nmap Testing SCADA Environments - Nessus Vulnerability Scanner Installing Nessus Adding a user Creating a new policy Safe Checks Silent Dependencies Port Range Preferences | | |
| **UNIT - V** | **Malware Analysis** | 9 |
| Classification of Malware-Environment Setup for Safe Analysis-Malware Analysis in Virtual Machines-Static analysis-Dynamic analysis-Anonymous and stealthy analysis -Malware classification and functionality -Anti Reverse-engineering. | | |
| TOTAL HOURS | : | 45 |

**Course Outcomes:**
Upon completion of the course, the students will be able to:

| | |
|---|---|
| ● | Understand the basic concepts of Ethical Hacking and Penetration Testing and will be able to prepare penetration testing reports. |
| ● | Demonstrate information gathering about the victim using various tools such acunetix, netcraft and google hacking |
| ● | Enumerate and perform different types of scanning and demonstrate nmap. |
| ● | Explore the vulnerability scanners: nmap and Nessus. |
| ● | Understand and demonstrate sniffing, MITM attacks, ARP attacks and DoS attacks. |

**Lab Experiments:**

1. Footprinting and Reconnaissance
2. Scanning Networks
3. Enumeration

| |
|---|
| 4. Vulnerability Analysis |
| 5. System Hacking |
| 6. Malware Threats |
| 7. Sniffing |
| 8. Social Engineering |
| 9. Denial of Service |
| 10. Session Hijacking |
| 11. Evading IDS Firewalls and Honeypots |
| 12. Hacking Web Servers |
| 13. Hacking Web Applications |
| 14. SQL Injection |
| 15. Hacking Wireless Networks |
| 16. Hacking Mobile Platforms |

**Text Book(s) / Reference Book(s)**

1. RafayBaloch, Ethical Hacking and Penetration Testing Guide, CRC Press Taylor & Francis Group, 2015.

2. Hilary Morrison, hein smith, Ethical Hacking a Comprehensive Beginner's Guide to Learn and Master Ethical Hacking, 2018

3. Jon Erickson, Hacking The Art of Exploitation, No Starch Press, San Francisco ,2nd Edition,2008.

4. Shon Harris, Allen Harper, Chris Eagle and Jonathan Ness, Gray Hat Hacking: The Ethical

5. Hackers Handbook, TMH ,3rd Edition, 2011.

<table>
<tr><th colspan="2">Subject Code</th><th colspan="2">Subject Name</th><th>L</th><th>T</th><th>P</th><th>C</th></tr>
<tr><td colspan="2"><b>CS19P14</b></td><td colspan="2"><b>Information Security And Management</b></td><td><b>2</b></td><td><b>0</b></td><td><b>2</b></td><td><b>3</b></td></tr>
<tr><td colspan="8"><b>Course Objectives:</b></td></tr>
<tr><td>●</td><td colspan="7">To understand the basics of Information Security and legal and ethical issues in Information Security.</td></tr>
<tr><td>●</td><td colspan="7">To understand the information security policy and concepts of access control.</td></tr>
<tr><td>●</td><td colspan="7">To learn about intrusion detection and prevention techniques and tools.</td></tr>
<tr><td>●</td><td colspan="7">To learn about auditing techniques and tools.</td></tr>
<tr><td>●</td><td colspan="7">To Learn to analyze and validate forensics data</td></tr>
<tr><td><b>UNIT – I</b></td><td colspan="5"><b>Introduction</b></td><td colspan="2">6</td></tr>
<tr><td colspan="8">Security Trends, OSI security architecture, Security attacks, security services, security mechanisms, Security System Development Life cycle – Legal, Ethical and Professional issues.</td></tr>
<tr><td><b>UNIT – II</b></td><td colspan="5"><b>Security Analysis</b></td><td colspan="2">6</td></tr>
<tr><td colspan="8">Risk Management - Identifying and Assessing Risk - Assessing and Controlling Risk. Blueprint for Information Security - Information Security Policy</td></tr>
<tr><td><b>UNIT – III</b></td><td colspan="5"><b>Security Technology</b></td><td colspan="2">6</td></tr>
<tr><td colspan="8">Intrusion Detection and Prevention Systems(IDPS)-Terminology-Types-Detection methods. Honeypots, Honeynets and padded cell systems. Scanning and Analysis Tools-Port scanners-Firewall analysis tools, Operating system detection tools-Vulnerability scanners-Packet sniffers-Wireless security tools.</td></tr>
<tr><td><b>UNIT – IV</b></td><td colspan="5"><b>Auditing</b></td><td colspan="2">6</td></tr>
<tr><td colspan="8">Overview, Access control, IT Audit, Authentication. Open Web Application Security Project (OWASP), Web Site Audit and Vulnerabilities assessment-Case study: Wireshark, FAW</td></tr>
<tr><td><b>UNIT - V</b></td><td colspan="5"><b>Analysis And Validation</b></td><td colspan="2">6</td></tr>
<tr><td colspan="8">Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition – Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics. - Case Study: Toolsley</td></tr>
<tr><td colspan="5">TOTAL HOURS</td><td>:</td><td colspan="2">30</td></tr>
<tr><td colspan="8"><b>Course Outcomes:</b><br>Upon completion of the course, the students will be able to:</td></tr>
<tr><td>●</td><td colspan="7">Discuss the basics of information security and legal and ethical issues in Information Security.</td></tr>
<tr><td>●</td><td colspan="7">Analyse the risk management and information security policy.</td></tr>
<tr><td>●</td><td colspan="7">Implement intrusion detection and prevention techniques using different tools.</td></tr>
<tr><td>●</td><td colspan="7">Perform auditing of logs.</td></tr>
<tr><td>●</td><td colspan="7">Analyze and validate forensics data</td></tr>
</table>

| **List of Experiments:** |
|---|
| 1 Implementation to gather information from any PC‟s connected to the LAN using whois, port scanners, network scanning, Angry IP scanners etc. |
| 2 Implementation of Steganography |
| 3 Implementation of Mobile Audit and generate the report of the existing Artifacts. |
| 4 Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report. |

| |
|---|
| 5 Implementation of Cyber Forensics tools for Disk Imaging, Data acquisition, Data extraction and Data Analysis and recovery. |
| 6 Perform mobile analysis in the form of retrieving call logs ,SMS log ,all contacts list using the forensics tool like SAFT |
| 7 Implementation to identify web vulnerabilities, using OWASP project. |
| **Contact Hours : 30** |

**Text Book(s) / Reference Book(s)**

1. Michael E Whitman and Herbert J Mattord, “Principles of Information Security”, Cengage Learning, Fourth Edition, 2011.

2 Nelson, Phillips, Enfinger, Steuart, “Computer Forensics and Investigations”, Cengage Learning, India Edition, 2008.

**Reference Book(s)/Web link(s):**

1 Micki Krause, Harold F. Tipton, “Handbook of Information Security Management”, CRC Press; 6th Edition, 2007.

2 John R.Vacca, “Computer Forensics”, Cengage Learning, 2005

3 MarjieT.Britz, “Computer Forensics and Cyber Crime”: An Introduction”, 3rd Edition, Prentice Hall, 2013.