CMR COLLEGE OF ENGINEERING & TECHNOLOGY
(Autonomous)

Kandlakoya, Hyderabad – 501 401

B.Tech. Minor Degree in Cyber Security
Course Structure Regulation-R18

V SEMESTER (III YEAR I SEMESTER)

Course Code	Title of the Course	L	T	P	Contact Hours/ Week	Credits
A36229	Principles of Information Security	3	0	0	3	3
A36230	Principles of Information Security Lab	0	0	3	3	1.5
Total		**3**	**0**	**3**	**6**	**4.5**

VI SEMESTER (III YEAR II SEMESTER)

Course Code	Title of the Course	L	T	P	Contac tHours/ Week	Credit s
A36228	Foundations of Cyber Security	4	0	0	4	4
Total		**4**	**0**	**0**	**4**	**4**

VII SEMESTER (IV YEAR I SEMESTER) Either Offline or MOOCS)

Course Code	Title of the Course	L	T	P	Contact Hours/ Week	Credit s
A36210	Concepts of Ethical Hacking	3	0	0	3	3
A36213	Digital Forensics					
A36211	Concepts of Ethical Hacking Lab	0	0	3	3	1.5
A36214	Digital Forensics Lab					
Total		**3**	**0**	**3**	**6**	**4.5**

VIII SEMESTER (IV YEAR II SEMESTER)

Course Code	Title of the Course	L	T	P	Contact Hours/ Week	Credit s
A36218	Incident & Response Management	3	0	0	3	3
A36212	Mobile & Wireless Security					
A36224	OS Security					
A36227	Block Chain Technologies					
A36221	Cloud Security					
A36226	Mini-Project	0	0	4	4	2
Total		**3**	**0**	**4**	**7**	**5**
Total Credits						**18**
NOTE: Above subjects not studied in regular B. Tech. course						

PRINCIPLES OF INFORMATION SECURITY

B.Tech. Cyber Security (Minor) III Year I Sem. **L T P C**
3 0 0 3

UNIT - I

Introduction to Computer Networks, Network hardware, Network software, OSI and TCP/IP Reference models, Securityattacks, Security Services and Mechanisms.

UNIT - II

Integer Arithmetic, Modular Arithmetic, Traditional Symmetric Key Ciphers, Data Encryption Standard (DES), AdvancedEncryption Standard (AES).

UNIT - III

Mathematics of Cryptography: Primes, Primality Testing, Factorization, Chinese Remainder Theorem, Asymmetric
Cryptography: Introduction, RSA Cryptosystem, Rabin Cryptosystem,Elliptic Curve Cryptosystem,

UNIT - IV

Message Integrity and Message Authentication: Message Authentication Code (MAC), SHA-512 - Digital Signatures.

UNIT - V

Security at the Application Layer: PGP and S/MIME. Security at Transport Layer: SSL and TLS. - Principles of IDS andFirewalls.

TEXT BOOKS:

1. Computer Networks, Andrew S Tanenbaum, David. j. Wetherall, 5th Edition. Pearson Education/PHI.
2. Cryptography & Network Security by Behrouz A. Forouzan. Special Indian Edition, TMH.

REFERENCE BOOK:

1. Network Security Essentials (Applications and Standards), William Stallings Pearson Education.

COURSE OUTCOMES:

1. Demonstrate the knowledge of Computer Networks, Cryptography, Information security concepts and
applications.
2. Ability to apply security principles in system design.

PRINCIPLES OF INFORMATION SECURITY LAB

B.Tech.Cyber Security (Minor) III Year I Sem.

L T P C
0 0 0 1.5

Lab Exercises

1. Write a program to perform encryption and decryption using the followingsubstitution ciphers.
2. Caeser cipher
3. Play fair cipher
4. Hill Cipher
5. Write a program to implement the DES algorithm.
6. Write a program to implement RSA algorithm.
7. Calculate the message digest of a text using the SHA-1 algorithm.
8. Working with sniffers for monitoring network communication (Wireshark).
9. Configuring S/MIME for email communication.
10. Using Snort, perform real time traffic analysis and packet logging.

TEXT BOOKS:

1. “Cryptography and Network Security” by William Stallings 3rd Edition, PearsonEducation.
2. “Applied Cryptography” by Bruce Schneier.

REFERENCE BOOK:

1. Cryptography and Network Security by Behrouz A. Forouzan.

COURSE OUTCOMES

1. To apply algorithms on various Symmetric and Asymmetric encryption algorithms.
2. To demonstrate IDS Tools
3. To apply algorithms used for message Integrity and Authentication

FOUNDATIONS OF CYBER SECURITY

B.Tech.Cyber Security (Minor) III Year II Sem

L T P C
4 0 0 4

UNIT - I

Overview: Computer Security Concepts, Threats, Attacks, and Assets, Security Functional Requirements, Fundamental Security Design Principles, Attack Surfaces and Attack Trees, Computer
Security Strategy.

Access Control: Access Control Principles, Subjects, Objects, and Access Rights, Discretionary Access
Control, Example: UNIX File Access Control, Role-Based Access Control, Attribute-Based Access
Control, Identity, Credential, and Access Management, Trust Frameworks, Case Study: RBAC System
for a Bank.

UNIT - II

Malicious Software: Types of Malicious Software (Malware), Advanced Persistent Threat, Propagation—Infected Content— Viruses, Propagation—Vulnerability Exploit—Worms, Propagation— Social Engineering—Spam E-Mail,Trojans , Payload—System Corruption, Payload—Attack Agent— Zombie, Bots, Payload—Information Theft—Keyloggers, Phishing, Spyware, Payload—Stealthing— Backdoors, Rootkits, Counter measures .

Denial-of-Service Attacks: Denial-of-Service Attacks, Flooding Attacks, Distributed Denial-of-Service Attacks, Application-Based Bandwidth Attacks, Reflector and Amplifier Attacks, Defenses Against Denial-of-Service Attacks, Responding to a Denial-of-Service Attack.

Buffer Overflow: Stack Overflows, Defending Against Buffer Overflows, Other Forms of Overflow Attacks.

UNIT - III

Intrusion Detection: Intruders, Intrusion Detection, Analysis Approaches, Host-Based Intrusion Detection, Network-Based Intrusion Detection, Distributed or Hybrid Intrusion Detection, Intrusion Detection Exchange Format, Honeypots, Example System: Snort.

Firewalls and Intrusion Prevention Systems: The Need for Firewalls, Firewall Characteristics and Access Policy, Types of Firewalls, Firewall Basing, Firewall Location and Configurations, Intrusion Prevention Systems, Example: Unified Threat Management Products.

UNIT - IV

Software Security: Software Security Issues, Handling Program Input, Writing Safe Program Code, Interacting with the Operating System and Other Programs, Handling Program Output.

Physical and Infrastructure Security: Overview, Physical Security Threats, Physical Security Prevention and Mitigation Measures, Recovery from Physical Security Breaches, Example: A Corporate Physical Security Policy, Integration of Physical and Logical Security.

UNIT - V

Human Resources Security: Security Awareness, Training, and Education, Employment Practices and Policies, E-Mail and Internet Use Policies, Computer Security Incident Response Teams.

Legal and Ethical Aspects: Cybercrime and Computer Crime, Intellectual Property, Privacy, Ethical Issues.

TEXT BOOK:

1. William Stallings, "Computer Security: Principles and Practice", Prentice Hall. Prentice Hall; 2014.

REFERENCE BOOKS:

1. Ankit Fadia, "The ethical hacking guide to corporate security", McMillan India.
2. G. McGraw, "Software Security: Building Security In", Addison Wesley, 2006.

COURSE OUTCOMES:

1. To introduce security attacks.
2. To get an exposure to malwares.

3. To gain knowledge on Intrusion detection & prevention systems.

(A36210) CONCEPTS OF ETHICAL HACKING

B. Tech (CSE-Cyber Security) –VI Semester

L	T	P	C
3	0	0	3

UNIT- I

Introduction: Hacking Impacts, The Hacker
Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration
Information Security Models: Computer Security, Network Security, Service Security, Application Security, Security Architecture
Information Security Program: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking.

UNIT - II

The Business Perspective: Business Objectives, Security Policy, Previous Test Results, Business Challenges
Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement.

UNIT - III

Preparing for a Hack: Technical Preparation, Managing the Engagement
Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance

UNIT - IV

Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase
Exploitation: Intutive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, RootKits, applications, Wardialing, Network, Services and Areas of Concern

UNIT - V

Deliverable: The Deliverable, The Document, Overall Structure, Aligning Findings, Presentation
Integration: Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion.

TEXT BOOK:

1. James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing”, Auerbach Publications, CRC Press

REFERENCE BOOKS:

1. EC-Council, “Ethical Hacking and Countermeasures Attack Phases”, Cengage Learning
2. Michael Simpson, Kent Backman, James Corley, “Hands-On Ethical Hacking and Network Defense”, Cengage Learning.

COURSE OUTCOMES:

1. Gain the knowledge of the use and availability of tools to support an ethical hack
2. Gain the knowledge of interpreting the results of a controlled attack
3. Understand the role of politics, inherent and imposed limitations and metrics for planning of a test
4. Comprehend the dangers associated with penetration testing.
5. Understand the defence planning and incident management

END

(A36211)CONCEPTS OF ETHICAL HACKING LAB

B. Tech (CSE-Cyber Security)-VI Semester

L	T	P	C
0	0	3	1.5

List of Experiments: \

1. Setup a honey pot and monitor the honey pot on network
2. Write a script or code to demonstrate SQL injection attacks
3. Create a social networking website login page using phishing techniques
4. Write a code to demonstrate DoS attacks
5. Install rootkits and study variety of options
6. Study of Techniques uses for Web Based Password Capturing.
7. Install jcrypt tool (or any other equivalent) and demonstrate Asymmetric Crypto algorithm, Hash and Digital/PKI signatures studied in theory Cryptography & Network Security
8. Install jcrypt tool (or any other equivalent) and demonstrate Symmetric Crypto algorithm, Hash and Digital/PKI signatures studied in theory Cryptography & Network Security
9. Implement passive scanning using Burp suit tool
10. Implement active scanning using Burp suit tool
11. Implement session hijacking using Burp suit tool
12. Implement cookies extraction using Burp suit tool

COURSE OUTCOMES:

1. Gain the knowledge of the use and availability of tools to support an ethical hack
2. Gain the knowledge of interpreting the results of a controlled attack
3. Able to understand and run algorithms on crypto tool
4. Understanding about passive and active scanning
5. To learn about session hijacking and cookies

END

(A36213) DIGITAL FORENSICS

B. Tech (CSE-Cyber Security) –VI Semester

L	T	P	C
3	0	0	3

UNIT - I

Digital Forensics Science: Forensics science, computer forensics, and digital forensics. Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber-criminalistics area, holistic approach to cyber-forensics.

UNIT - II

Cyber Crime Scene Analysis: Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

UNIT - III

Evidence Management & Presentation: Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, define and apply probable cause.

UNIT - IV

Computer Forensics: Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, Complete a case, Critique a case. Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data

UNIT - V

Mobile Forensics: mobile forensics techniques, mobile forensics tools. Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008. Recent trends in mobile forensic technique and methods to search and seizure electronic evidence

TEXT BOOKS:

1.B. Nelson, A. Phillips, and C. Steuart, Guide to Computer Forensics and Investigations, 4th Edition, Course Technology, 2010

REFERENCE BOOKS:

1. John Sammons, The Basics of Digital Forensics, 2nd Edition, Elsevier, 2014
2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, Laxmi Publications, 2005.

COURSE OUTCOMES:

1. Understand relevant legislation and codes of ethics.
2. Investigate computer forensics and digital detective and various processes, policies and procedures data
   acquisition and validation, e-discovery tools.
3. Analyze E-discovery, guidelines and standards, E-evidence, tools and environment.
4. Apply the underlying principles of Email, web and network forensics to handle real life problems
5. Use IT Acts and apply mobile forensics techniques.

*****END*****

(A36214) DIGITAL FORENSICS LAB

B. Tech (CSE-Cyber Security) –VI Semester

L	T	P	C
0	0	3	1.5

List of Experiments

Week 1:

Performing Forensic Imaging of the evidence using the following
i) Sleuthkit (autopsy) Imaging ii) Encase Imaging iii) Helix Imaging iii) Win hex Imaging iv) Write Blockers

Week 2:

Performing Forensic Analysis of the evidence using the following
i) Configuring the tool ii) Analysis, using Sleuthkit(autopsy)
iii) Analysis using Encase iv) Recovering files

Week 3:

Performing Forensic Analysis of the evidence using the following
i) Bookmarking evidence ii) Keyword searching iii) password cracking

Week 4:

Usage and perform analysis on
i) Steganography

Week 5:

Perform the following in Networking
i) DoS Attacks ii) SQL injection

Week 6:

Perform the following in Networking
i) Web defacement ii) Shell / backdoors

Week 7:

Finding the Email Crimes by using Email Tracing Tool
i) Email Tracer

Week 8:

Investigating Network and logs using
i) IPS/IDS ii) Snorting iii) Gathering logs

Week 9:

Investigating Network and logs using
i) Investigating logs ii) Investigating wireless access point iii) Auditing

Week 10:

Perform Mobile Forensics on
i) Blackberry forensics ii) Android forensics

Week 11:

Perform Mobile Forensics on
ii) iPhone Forensics ii) iPod Forensics

Week 12:

Perform the Forensic Report Writing
i) Report Samples Report ii) writing skills
iii) Common mistakes in report iv) Report submission

REFERENCE BOOKS:

1. Kevin Mandia, Chris Prosise, “Incident Response and computer forensics”, Tata McGrawHill, 2006
2. Nilakshi Jain, D. R. Kalbande, “Digital Forensic: The Fascinating World of Digital Evidences”, Wiley publications,2016.
3. Peter Stephenson, "Investigating Computer Crime: A Handbook for Corporate Investigations", Sept 1999.
4. Eoghan Casey, "Handbook Computer Crime Investigation's Forensic Tools and Technology", Academic Press, 1st Edition, 2001
5. Skoudis. E., Perlman. R. Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses.Prentice Hall Professional Technical Reference. 2001.
6. Norbert Zaenglein, "Disk Detective: Secret You Must Know to Recover Information From a Computer", Paladin Press, 2000
7. Bill Nelson, Amelia Philips and Christopher Steuart, “Guide to computer forensics investigation “Course technology, 4th edition
8. SoufianeTahiri, “Mastering Mobile Forensics”, Packt Publishing,2016.

COURSE OUTCOMES:

1. Student should be able to Analyze E-discovery, guidelines and standards E-evidence, tools and environment.
2. Student should be able Apply the underlying principles of Email, web and network forensics to handle real life problems
3. To investigate the networks and logs
4. Understanding about the steganography
5. Student able to write Forensic Report

END

(A36218) INCIDENT RESPONSE MANAGEMENT

B. Tech (CSE-Cyber Security)

L	T	P	C
3	0	0	3

UNIT - I

Real-World Incidents: What Constitutes an Incident?, What Is Incident Response?, Where We Are Now, Why Should You Care About Incident Response?, Concept of the Attack Lifecycle, IR Management Handbook: What Is a Computer Security Incident?, What Are the Goals of Incident Response?, Who Is Involved in the IR Process?, The Incident Response Process: Initial Response, Investigation, Remediation, Tracking of Significant Investigative Information, Reporting.

UNIT - II

Pre-Incident Preparation: Preparing the Organization for Incident Response, Identifying Risk, Policies That Promote a Successful IR, Working with Outsourced IT, Thoughts on Global Infrastructure Issues, Educating Users on Host-Based Security, Preparing the IR Team, Preparing the Infrastructure for Incident Response, Computing Device Configuration, Network Configuration.

UNIT - III

Incident Detection and Characterization: Collecting Initial Facts, Checklists, Maintenance of Case Notes, Building an Attack Timeline, Understanding Investigative Priorities, What Are Elements of Proof?, Setting Expectations with Management, Initial Development of Leads, Defining Leads of Value, Acting on Leads, Turning Leads into Indicators, The Lifecycle of Indicator Generation, Resolving Internal Leads, Resolving External Leads.

UNIT - IV

Data Collection: Live Data Collection, When to Perform a Live Response, Selecting a Live Response Tool, What to Collect, Live Data Collection on Microsoft Windows Systems, Prebuilt Toolkits, Do It Yourself, Memory Collection, Live Data Collection on Unix-Based Systems, Live Response Toolkits, Memory Collection.

UNIT - V

Forensic Duplication: Forensic Image Formats, Complete Disk Image, Partition Image, Logical Image, Image Integrity, Traditional Duplication, Hardware Write Blockers, Image Creation Tools, Live System Duplication, Duplication of Enterprise Assets, Duplication of Virtual Machines.

TEXT BOOKS:

1. “ Incident Response and Computer Forensics”, Kevin Mandia, Mathew Pepe, Jason Luttgens, 3rd Edition, McGraw-Hill Osborne Media, 2014.

REFERENCE BOOKS:

1. "Handbook Computer Crime Investigation's Forensic Tools and Technology", Eoghan Casey, Academic Press.
2. “A Step-by-Step Guide to Computer Attacks and Effective Defenses”, Skoudis. E., Perlman.

R. Counter Hack, Prentice Hall Professional Technical Reference.
3. "Disk Detective: Secret You Must Know to Recover Information From a Computer", Norbert Zaenglein, Paladin Press.
4. "Guide to computer forensics and investigations", Bill Nelson, Amelia Philips and Christopher Steuart, Cengage Learning.

COURSE OUTCOMES:

1.To know the real world incidents
2.To make a pre incident preparation
3.To understand about incident detection and characterization
4. Able to understand data collection
5. To understand about forensic duplication

*****END*****

(A36212) MOBILE & WIRELESS SECURITY

B. Tech (CSE-Cyber Security) – VI Semester **L T P C**

3 0 0 3

UNIT- I

Security in General Wireless/Mobile Networks: High Performance Elliptic Curve Cryptographic Co-processor, An Adaptive Encryption Protocol in Mobile Computing

UNIT- II

Security in Wireless LANs: Cross Domain Mobility Adaptive Authentication, AAA Architecture and Authentication for wireless LAN Roaming, Experimental Study on Security Protocols in WLANs

UNIT-III

Security in Ad Hoc Networks: Pre-authentication and authentication models in Ad Hoc Networks, Promoting Identity-based key management, attacks and countermeasures, Secure and resilient data aggregation, Secure routing in MANET, Intrusion Detection System in MANET

UNIT- IV

Security in Mobile Cellular Networks: Security issues in GSM, 3G and 4G networks, Authentication and encryption, Security concerns in 5G networks.

UNIT- V

Security in Sensor Networks and IoT: Security Issues, Key Management Schemes, Secure Routing in Sensor Networks, Energy-aware security mechanisms, Security and privacy issues in IoT, Identity and access management, Data Integrity, Best practices for IoT security.

TEXT BOOKS:

1. Lei Chen, JiahuangJi, Zihong Zhang, Wireless Network Security, Springer Science & Business Media
2. W. Stallings. Cryptography & Network Security: Principles and Practice, Prentice Hall Noureddine Boudriga, Security of Mobile Communications, CRC Press

REFERENCE BOOKS:

1. Levente Buttyán and Jean-Pierre Hubaux, Security and Cooperation in Wireless Networks, Cambridge University Press
2. James Kempf, Wireless Internet Security: Architectures and Protocols, Cambridge University Press
3. Patrick Traynor, Patrick McDaniel, and Thomas La Porta, Security for Telecommunications Networks, Springer
4. Frank Adelstein, Sandeep K.S. Gupta, Golden G. Richard III, and Loren Schwiebert, Fundamentals of Mobile and Pervasive Computing, McGraw-Hill Professional

COURSE OUTCOMES:

1. Understanding the modern concept and foundation of Mobile security.
2. Understand and classify various next generation networks
3. Identity various sources of vulnerabilities from Mobile.
4. Analyse network security attacks and its countermeasures.
5. Understanding the key management schemes

***END**

(A36224)OS Security

B. Tech (CSE-Cyber Security)	**L**	**T**	**P**	**C**
	3	**0**	**0**	**3**

Unit-I

Processes – Processes, Threads, Inter Process Communications (IPC) , Synchronization – Semaphores, Monitors, Scheduling, Classical IPC problems, Case study – Process in Linux, User and Kernel threads,

Unit-II

Memory Management – Memory abstraction, Virtual memory, Page replacement algorithms, Design issues for paging system, Segmentation.

Unit-III

File Systems – Files, Directories, File System Management and Optimization. Virtualization Techniques.

Unit-IV

Introduction to OS Security.Linux Kernel Modules.Linux Security Modules, SELinux.Malwares.

Unit-V

Introduction to Kernel exploitation – User space vs. Kernel space Attacks, Kernel Stack Vulnerabilities. Case study – Linux kernel

Text Books

1. Andrew S. Tanenbaum, “Modern Operating Systems”, Third Edition, Prentice Hall, 2009.
2. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, “Operating System Concepts with Java”, Ninth Edition, Wiley, 2012.
3. Trent Jaeger ,”Operating System Security”, Morgan and Claypool, 2008
4. Enrico Perla, MassimilianoOldani, “A Guide to Kernel Exploitation – Attacking the Core”, VElsevier, Syngress, 2011
5. Wolfgang Mauerer, “Professional Linux Kernel Architecture”, Wiley, 2008.
6. Daniel P. Bovet and Marco Cesati, “Understanding the Linux Kernel”, Third Edition,O’Reilly, 2006.
7. W. Richard Stevens, Stephen A. Rago, “Advanced Programming in the Unix Environment”, Third Edition, 2013.

COURSE OUTCOMES:

1. Operating Systems Fundamentals
2. Popular Operating Systems
3. The Central Processing Unit (CPU)
4. File Systems
5. Installing and Upgrading Operating Systems
6. Configuring Input and Output Devices

*****END*****

(A30545) BLOCK CHAIN TECHNOLOGIES

B. Tech (CSE-Cyber Security)

L	T	P	C
3	0	0	3

UNIT-I

Introduction: Overview of Block chain, Public Ledgers, Bitcoin, Smart Contracts, Block in a Block chain, Transactions, Distributed Consensus, Public vs Private Block chain, Understanding Crypto currency to Block chain, Permissioned Model of Block chain, Overview of Security aspects of Block chain Basic Crypto Primitives: Cryptographic Hash Function, Properties of a hash function, Hash pointer and Merkle tree, Digital Signature, Public Key Cryptography, A basic cryptocurrency.

UNIT–II

Bitcoin and Block chain: Creation of coins, Payments and double spending, Transaction in Bitcoin Network, Block Mining. Working with Consensus in Bitcoin: Distributed consensus in open environments, Consensus in a Bitcoin network, Proof of Work (PoW) – basic introduction, HashcashPoW, BitcoinPoW, Proof of Stake, Proof of Burn and Proof of Elapsed Time, The life of a Bitcoin Miner, Mining Difficulty, Mining Pool.

UNIT–III

Enterprise application of Block chain: Cross border payments, Know Your Customer (KYC), Food Security, Block chain enabled Trade, We Trade – Trade Finance Network, Supply Chain Financing, and Identity on Block chain.

UNIT-IV

Attacking the Blockchain with a Framework Approach: Technical Challenges, Market/Business Challenges, Legal /Regulatory Barriers and Behavioral/Educational Challenges, Blockchain in Financial Services: Blockchain Applications in Financial Services, Strategic Questions for Financial Services.

UNIT–V

Hyperledger Fabric- Architecture, Identities and Policies, Membership and Access Control, Transaction Validation, Bitcoin Security, Limitations and How to Overcome Blockchains, Reinventing the Blockchain, The Ten Rules to Never Break on the Blockchain.

TEXT BOOKS:

1. Melanie Swan, “Block Chain: Blueprint for a New Economy”, O’Reilly, 2015
2. Josh Thompsons, “Block Chain: The Block Chain for Beginners- Guide to Block chain Technology and Leveraging Block Chain Programming”
3. Daniel Drescher, “Block Chain Basics”, Apress; 1stedition, 2017
4. AnshulKaushik, “Block Chain and Crypto Currencies”, Khanna Publishing House, Delhi.

REFERENCE BOOKS:

1. Blockchain for Dummies by Manav Gupta, John Wiley & Sons publication
2. Mastering Bitcoin Unlocking Digital Crypto currencies‖, by Andreas M. Antonopoulos, O ‘Reilly Publication, 1st Edition.

3. RiteshModi, “Solidity Programming Essentials: A Beginner’s Guide to Build Smart Contracts for Ethereum and Block Chain”, Packt Publishing
4. Imran Bashir, “Mastering Block Chain: Distributed Ledger Technology, Decentralization and Smart Contracts Explained”, Packt Publishing
5. Salman Baset, Luc Desrosiers, Nitin Gaur, Petr Novotny, Anthony O’Dowd, Venkatraman Ramakrishna, “Hands-On Block Chain with Hyperledger: Building Decentralized Applications with Hyperledger Fabric and Composer”, Import, 2018.

COURSE OUTCOMES

1. Describe Block chain Technology.
2. Explain Block chain with Crypto currency
3. Build and deploy block chain applications
4. List the obstacles, challenges of Blockchain
5. Analyze hashing applications in real time scenarios

END

(A36221) CLOUD SECURITY

B. Tech (CSE-Cyber Security)	**L**	**T**	**P**	**C**
	3	**0**	**0**	**3**

UNIT I

Cloud Computing Fundamentals: Cloud Computing definition, private, public and hybrid cloud.
Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs private clouds,
role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture.

UNIT II

Cloud Applications: Technologies and the processes required when deploying web servicesDeploying a web service from inside and outside a cloud architecture, advantages and disadvantages- Development environments for service development; Amazon, Azure, Google App.

UNIT – III

Securing The Cloud: Security Concepts - Confidentiality, privacy, integrity, authentication, nonrepudiation, availability, access control, defence in depth, least privilege- how these concepts apply in the cloud and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud

UNIT - IV

Virtualization Security: Multi-tenancy Issues: Isolation of users/VMs from each other- How the cloud
provider can provide this- Virtualization System Security Issues: e.g. ESX and ESXi Security, ESX file
system security- storage considerations, backup and recovery- Virtualization System Vulnerabilities.

UNIT - V

Cloud Security Management: Security management in the cloud – security management standardsSaaS, PaaS, IaaS availability management- access control- Data security and storage in cloud.

REFERENCES:

1. GautamShroff, “Enterprise Cloud Computing Technology Architecture Applications”, Cambridge University Press; 1 edition [ISBN: 978- 0521137355], 2010.
2. Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach”, Tata McGraw-Hill Osborne Media; 1 edition 22, [ISBN: 0071626948], 2009.
3. Tim Mather, SubraKumaraswamy, ShahedLatif, “Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance”, O'Reilly Media; 1 edition, [ISBN: 0596802765], 2009.
4. Ronald L. Krutz, Russell Dean Vines, “Cloud Security”, Wiley [ISBN: 0470589876], , 2010.

COURSE OUTCOMES:

1.Understand the fundamentals of cloud computing.
2.Understand the requirements for an application to be deployed in a cloud.
3. Become knowledgeable in the methods to secure cloud.

*****END*****