VAAGDEVI COLLEGE OF ENGINEERING
AUTONOMOUS
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
M.Tech in CSE(CYBER SECURITY)
COURSE STRUCTURE
Applicable from AY 2025-26 Batch

I Year I Semester

Sl.No	Course Code	Course Title	L	T	P	Credits
1	M25CY01	Introduction to Cyberspace Operations and Design	3	0	0	3
2	M25CS17	Cyber Security	3	0	0	3
3		**Professional Elective – I**	3	0	0	3
	M25CY02	Information Security				
	M25CY03	Machine Learning for Cyber Security				
	M25CY04	System and Network Security				
4		**Professional Elective – II**	3	0	0	3
	M25CS06	Applied Cryptography				
	M25CY05	Digital Forensics & Incident Response				
	M25CY06	Wireless & Mobile security				
5	M25CS25	Cyber Security Lab	0	0	4	2
6		**Professional Elective-I Lab**	0	0	4	2
	M25CY07	Information Security Lab				
	M25CY08	Machine Learning for Cyber Security Laboratory				
	M25CY09	System and Network Security Laboratory				
7	M25MC01	Research Methodology & IPR	2	0	0	2
8	M25AC01	Audit Course-I	2	0	0	0
		Total				

* Professional Elective-I and Professional Elective-I Lab must be of same course

VAAGDEVI COLLEGE OF ENGINEERING
AUTONOMOUS
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
M.Tech in CSE(CYBER SECURITY)
COURSE STRUCTURE
Applicable from AY 2025-26 Batch

I Year II Semester

Sl.No	Course Code	Course Title	L	T	P	Credits
1	M25CY10	Ethical hacking	3	0	0	3
2	M25CS04	Natural Language Processing	3	0	0	3
3		**Professional Elective – III**	3	0	0	3
	M25CY11	Vulnerability Assessment And Penetration Testing				
	M25CY12	Data Privacy				
	M25CY13	Cloud Security				
4		**Professional Elective – IV**	3	0	0	3
	M25CY14	Secure Software Engineering				
	M25CY15	Intrusion Detection and Prevention				
	M25CY16	Scripting languages for information security				
5	M25CS12	Natural Language Processing Lab	0	0	4	2
6		**Professional Elective-III Lab**	0	0	4	2
	M25CY17	Vulnerability Assessment And Penetration Testing Lab				
	M25CY18	Data Privacy Lab				
	M25CY19	Cloud Security Lab				
7	M25CY20	Mini Project with Seminar	0	0	4	2
8	M25AC02	Audit Course-II	2	0	0	0
		Total	**14**	**0**	**12**	**18**

* Professional Elective-III and Professional Elective-III Lab must be of same course

VAAGDEVI COLLEGE OF ENGINEERING
AUTONOMOUS
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
M.Tech in CSE(CYBER SECURITY)
COURSE STRUCTURE
Applicable from AY 2025-26 Batch

II Year I Semester

Sl.No	Course Code	Course Title	L	T	P	Credits
1		**Professional Elective – V**	**3**	**0**	**0**	**3**
	M25CY21	Biometric Security				
	M25CY22	Quantum Cryptography				
	M25CY23	Privacy and Security in Online Social Networks				
2		**Open Elective**	3	0	0	3
3	M25CY24	Dissertation Work Review-II	0	0	18	6
		Total	**6**	**0**	**18**	**12**

II Year II Semester

Sl.No	Course Code	Course Title	L	T	P	Credits
1	M25CY25	Dissertation Work Review-III	0	0	18	6
2	M25CY26	Dissertation Viva - Voce	0	0	42	14
		Total	**0**	**0**	**60**	**20**

* For Dissertation Work Review-I, please refer R25 Academic Regulations

Audit Course I & II:

1. Research Paper Writing in English
2. Disaster Management
3. Sanskrit for Technical Knowledge
4. Value Education
5. Constitution of India
6. Pedagogy Studies
7. Stress Management by yoga
8. Personality Development Through Life Enlightenment Skills

Open Electives for other Departments:

1. Cyber Laws and Rights in the digital age – M25CY27
2. Foundations of Blockchain Technology - M25CY28
3. Information Security Risk Management – M25CY29

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 – 26

(M25CY01)- INTRODUCTION TO CYBERSPACE OPERATIONS AND DESIGN

I Year I Sem. **L T P C**
3 0 0 3

Course Outcomes:

1. Understanding of Cyberspace Environment and Design and Cyberspace Operational Approaches
2. Understand Cyberspace Operations.
3. Understanding of Cyberspace Integration
4. Building Cyber Warriors and Warrior Corps
5. Designing Cyber Related Command and Training and Readiness for Cyber Related Commands

UNIT -I

Understanding the Cyberspace Environment and Design- Cyberspace environment and its characteristics, Developing a design approach, Planning for cyberspace operation
Cyberspace Operational Approaches- Foundational approaches that utilize cyberspace capabilities to support organizational missions, The pros and cons of the different approaches

UNIT - II

Cyberspace Operations- Network Operations (NETOPS), Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO), Defense and Diversity of Depth network design, Operational methodologies to conduct cyberspace operations.

UNIT - III

Cyberspace Integration- Design a cyberspace operation and integrate it with a Joint Operations plan, Practice the presented methodologies in a practical application exercise.

UNIT - IV

Building Cyber Warriors and Warrior Corps- The warrior and warrior corps concept as applied to cyber organizations, The challenges of training and developing a cyber- workforce from senior leadership to the technical workforce.

UNIT - V

Designing Cyber Related Commands- Mission statements, Essential tasks, Organizational structures, Tables of organizations
Training and Readiness for Cyber Related Commands- Mission Essential Tasks (METs), Developing the cyber workforce, Plan your own training programs within your organization.

Text books and References:

1. Paulo Shakarian et al. “Introduction of Cyber Warfare: A Multidisciplinary Approach,” syngress, Elsevier 2013.
2. Jeffery carr et al, “Inside Cyber Warfare: Mapping the Cyber Underworld,” O’Reilly Publication December 2012.
3. Jason Andress et al. “Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners” Syngress, Elsevier 2013.
4. R. A. Clarke, Robert Knake “Cyber War: The Next Threat to National Security and What to Do About It” Haper Collins Publisher 2010.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CS17) CYBER SECURITY

I Year I Sem. **L T P C**
3 0 0 3

Course Outcomes:

1. Analyze and evaluate the cyber security needs of an organization.
2. Understand Cyber Security Regulations and Roles of International Law
3. Identify various security challenges phased by mobile devices.
4. Design and develop a security architecture for an organization.
5. Understand fundamental concepts of data privacy attacks

UNIT -I
Introduction to Cyber Security: Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.

UNIT - II
Cyberspace and the Law & Cyber Forensics: Introduction, Cyber Security Regulations, Roles of International Law. The INDIAN Cyberspace, National Cyber Security Policy. Introduction, Historical background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber Forensics and Digital evidence, Forensics Analysis of Email, Digital Forensics Lifecycle, Forensics Investigation, Challenges in Computer Forensics.

UNIT - III
Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication service Security, Attacks on Mobile/Cell Phones, Organizational security Policies and Measures in Mobile Computing Era, Laptops.

UNIT- IV
Cyber Security: Organizational Implications: Introduction, cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for organizations

UNIT - V
Privacy Issues: Basic Data Privacy Concepts: Fundamental Concepts, Data Privacy Attacks, Data linking and profiling, privacy policies and their specifications, privacy policy languages, privacy in different domains- medical, financial, etc Cybercrime: Examples and Mini-Cases Examples: Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions of Rupees, Parliament Attack, Pune City Police Bust Nigerian Racket, e-mail spoofing instances. Mini-Cases: The Indian Case of online Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.

TEXT BOOKS:
1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
2. B.B. Gupta, D.P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335,2018.

REFERENCES:
1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
2. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J. David Irwin, CRC Press T&FGroup.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY02) INFORMATION SECURITY (PE-1)

I Year I Sem. **L T P C**
3 0 0 3

Course Outcomes:

1. Demonstrate the knowledge of cryptography, network security concepts and applications.
2. Ability to apply security principles in system design.
3. Ability to identify and investigate vulnerabilities and security threats and mechanisms tocounter them.
4. Understanding IP Security Concepts.
5. Ability to Learn Intruders, Viruses

UNIT - I

Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms, A model for Internetwork security. Classical Encryption Techniques, DES, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and Modes of operation, Blowfish, Placement of Encryption Function, Traffic Confidentiality, key Distribution, Random Number Generation.

UNIT - II

Public key Cryptography Principles, RSA algorithm, Key Management, Diffie-Hellman Key Exchange, Elliptic Curve Cryptography. Message authentication and Hash Functions, Authentication Requirements and Functions, Message Authentication, Hash Functions and MACs Hash and MAC Algorithms SHA-512, HMAC.

UNIT - III

Digital Signatures, Authentication Protocols, Digital signature Standard, Authentication Applications, Kerberos, X.509 Directory Authentication Service. Email Security: Pretty Good Privacy (PGP) and S/MIME.

UNIT - IV

IP Security: Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management. Web Security: Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security(TLS), Secure Electronic Transaction (SET).

UNIT - V

Intruders, Viruses and Worms Intruders, Viruses and related threats Firewalls: Firewall Design Principles, Trusted Systems, Intrusion Detection Systems.

TEXT BOOK:

1. Cryptography and Network Security (principles and approaches) by William Stallings Pearson Education, 4th Edition.

REFERENCE BOOKS:

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.
2. Principles of Information Security, Whitman, Thomson

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY03) Machine Learning for Cyber Security (Professional Elective - I)

I Year I Sem. **L T P C**
3 0 0 3

COURSE OUTCOMES:

On completion of the course, students will be able to
CO1 - Understand basic machine learning concepts.
CO2 - Implement supervised and unsupervised algorithms for cyber security tasks.
CO3 - Apply data pre-processing operations for data cleaning and feature selection.
CO4 - Implement deep learning models for cyber security tasks.
CO5 - Analyze the results of machine learning models in cyber security.

UNIT - I

Data Exploration and Preprocessing:
Data exploration using Pandas and NumPy, Preprocessing of datasets, including handling missing values, scaling, encoding categorical variables, etc.

UNIT-II

Supervised Learning Models:
Linear and Non-linear Regression, Classification Models (KNN, SVM, Naïve Bayes, Decision Tree,
Logistic Regression), Ensemble Techniques (Random Forests, Gradient Boosting), Neural Network, Architecture using Tensor Flow or PyTorch, Hyper parameter Tuning for various machine learning Algorithms.

UNIT-III

Unsupervised Learning and Anomaly Detection:
Network Traffic Anomaly Detection using Clustering Algorithms (K-Means, Hierarchical Clustering, DBSCAN), Phishing Email Dataset Analysis using Clustering Algorithms.
End-to-End Machine Learning Pipeline for Cyber security:
Designing and implementing an end-to-end pipeline encompassing data preprocessing, model training, hyper parameter tuning, and evaluation using real-world cyber security datasets.

UNIT-IV

Adversarial Attacks and Model Security:
Implementing adversarial attacks (FGSM, PGD) on trained models for malware detection, Understanding and defending against adversarial attacks to ensure model security.

UNIT-V

Performance Evaluation and Comparative Analysis:
Evaluating the performance of various machine learning models on cyber security tasks, Comparing the effectiveness of different algorithms and techniques in detecting and preventing cyber security threats.

TEXT BOOKS

1. Aurélien Géron, “Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow”, O'Reilly Media,Inc.
2. Sebastian Raschka, Vahid Mirjalili, “Machine Learning and Deep Learning with Python, Scikit-learn, and TensorFlow”, Packt Publishing

REFERENCE BOOKS

1. Jagannath E. Nalavade, “Machine Learning Approaches in Cyber Security”, Namya Press
2. Soma Halder, Sinan Ozdemir, “Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem”,Packt Publishing.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY04) SYSTEM AND NETWORK SECURITY (Professional Elective - I)

I Year I Sem. **L T P C**
3 0 0 3

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Illustrate the concepts of system software and computer networks.

CO2- Understand the program binaries, debugging and analysis, buffer overflow vulnerabilities, string vulnerabilities and integer exploits.

CO3- Identify the vulnerabilities existing in a program code.

CO4- Apply the mitigation and prevention techniques existing in the system.

CO5- Analyze the vulnerabilities in public networks, potential impact and mitigation strategies.

.

UNIT-I

Vulnerabilities and Exploits in System Software, Introduction to Program Binaries, GDB tool, Buffer Overflow in the Stack, Return to LibC attack, Format String Vulnerabilities, Integer Exploits.

UNIT-II

Prevention and Mitigation Techniques
W^X, Canaries, Address Space Layout Randomization (ASLR), Hardware and compiler mitigations Capability and sandboxing systems: SGX, Trust zone.

UNIT-III

Hardware Security
Power Analysis Attacks, Side-channel attacks, Physically Un-clonable Functions, Hardware Trojan.

UNIT –IV

Network Security -OSI and TCP Model Architecture, Public Networks Vulnerabilities, Network Security Protocols: SSL, Use of Packet Sniffer tool and Intrusion detection technique to detect the cyber attacks.

TEXT BOOKS

1. William Stallings, “Network Security Essentials: Applications and Standards”, Prentice Hall.
2. Michael T. Goodrich and Roberto Tamassia, “Introduction to Computer Security”, Addison Wesley.
3. W. Stallings, “Cryptography and Network Security: Principles and Practice”, Prentice Hall.
4. One, Aleph. "Smashing the stack for fun and profit." Phrack magazine.
5. B. Bierbaumer, K. Julian, K. Thomas, A.Francillon, and A. Zarras. "Smashing the stack protector for fun and profit." In ICT Systems Security and Privacy Protection: 33rd IFIP TC 11 International Conference, SEC 2018, Proceedings 33, pp. 293-306. Springer International Publishing, 2018.

REFERENCE BOOKS

1. D. Ahmad,. "The rising threat of vulnerabilities due to integer errors." IEEE Security & Privacy 1, no. 4 (2003): 77-82.
2. E. Leon, and S. D. Bruda. "Counter-measures against stack buffer overflows in GNU/Linux operating systems." Procedia Computer Science 83 (2016): 1301-1306.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CS06) APPLIED CRYPTOGRAPHY (PROFESSIONAL ELECTIVE - II)

I Year I Sem. **L T P C**
3 0 0 3

Prerequisites: Mathematical maturity with strong foundational knowledge in discrete mathematics.

Course Outcomes:

1. Understand the various cryptographic protocols
2. Analyze key length and algorithm types and modes
3. Illustrate different public key algorithms in cryptosystems
4. Understand special algorithms for protocols and usage in the real world.
5. Understand and apply key real-world cryptographic protocols for secure communication and electronic payment systems.

Unit I

Foundations: Terminology, Steganography, Substitution Ciphers and Transposition Ciphers, Simple XOR, One Time Pads, Computer Algorithms, Large Numbers, Cryptographic Protocols: Protocol Building Blocks Introduction to Protocols, Communications Using Symmetric Cryptography, One-Way Functions, One Way Hash Functions, Communications Using Public-Key Cryptography, Digital Signatures, Digital Signatures with Encryption, Random and Pseudo-Random-Sequence Generation

Unit II

Cryptographic Techniques Key length: Symmetric Key length, Public key length, comparing symmetric and public key length. Algorithm types and modes: Electronic Codebook Mode, Block Replay, Cipher Block Chaining Mode, Stream Cipher, Self-Synchronizing Stream Ciphers, Cipher-Feedback Mode, Synchronous Stream Ciphers, Output-Feedback Mod, Counter Mode, Other Block-Cipher Modes.

Unit III

Public-Key Algorithms Background, Knapsack Algorithms, RSA, Pohlig-Hellman, Rabin, ElGamal, McEliece, Elliptic Curve Cryptosystems, LUC, Finite Automaton Public-Key Cryptosystems Public-Key Digital Signature Algorithms: Digital Signature Algorithm (DSA), DSA Variants, Gost Digital Signature Algorithm, Discrete Logarithm Signature Schemes, Ong-Schnorr-Shamir, ESIGN

Unit IV

Special Algorithms for Protocols Multiple-Key Public-Key Cryptography, Secret-Sharing Algorithms, Subliminal Channel, Undeniable Digital Signatures, Designated Confirmer Signatures, Computing with Encrypted Data, Fair Coin Flips, One-Way Accumulators, All-or-Nothing Disclosure of Secrets, Fair and Failsafe Cryptosystems, Zero Knowledge Proofs of Knowledge, Blind Signatures, Oblivious Transfer, Secure Multiparty Computation, Probabilistic Encryption, Quantum Cryptography

Unit V

Real World Approaches IBM Secret key management protocol, ISDN, Kerberos, Krypto Knight, Privacy enhanced mail (PEM), Message security protocol (MSP), PGP, Public-Key Cryptography Standards (PKCS), Universal Electronic Payment System (UEPS).

TEXT BOOKS:

1. Bruce Schneier, Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth).

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY05) DIGITAL FORENSICS & INCIDENT RESPONSE (PROFESSIONAL ELECTIVE-II)

I Year-I Semester **L/T/P/C**
3/ 0/ 0/ 3

Course Outcomes:

Upon completion of this course, the students will be able to:

1. Understanding of various digital forensics techniques and its usage for the potential countermeasures or incident response.
2. Demonstrate a critical evaluation and use of digital forensics technique to do incident response with an independent project.
3. Understand Evidence duplication and preservation issues.
4.Understand E mail Analysis and Messenger Analysis.
5. Understand Mobile Device Forensics.

UNIT-I

Forensics Overview: Computer Forensics Fundamentals, Benefits of Computer Forensics, Computer Crimes, Computer Forensics Evidence and the Courts, Legal Concerns and Privacy, Issues

UNIT-II

Forensics Process: Forensics Investigation Process, Securing the Evidence and Crime Scene, Chain of Custody, Law Enforcement Methodologies.

UNIT-III

Forensics Evidence, Evidence Sources. Evidence Duplication, Preservation, Handling, and Security, Forensics Soundness, Order of Volatility of Evidence, Collection of Evidence on a Live System, Court Admissibility of Volatile Evidence.

UNIT-IV

Acquisition and Duplication: Sterilizing Evidence Media, Acquiring Forensics Images, Acquiring Live Volatile Data, Data Analysis, Metadata Extraction, File System Analysis, Performing Searches, Recovering Deleted, Encrypted, and Hidden files, Internet Forensics, Reconstructing Past Internet Activities and Events, E-mail Analysis, Messenger Analysis: AOL, Yahoo, MSN, and Chats

UNIT-V

Mobile Device Forensics: Evidence in Cell Phone, PDA, Blackberry, iPhone, iPod, and MP3. Evidence in CD, DVD, Tape Drive, USB, Flash Memory, Digital Camera, Court Testimony, Testifying in Court, Expert Witness Testimony, Evidence Admissibility.

Text books:

1. Jason Luttgens, Matthew Pepe, Kevin Mandia, Incident Response & Computer Forensics, McGraw-Hill Osborne Media, 3 rd edition , 2014.
2. Keith J. Jones, Richard Bejtlich, Curtis W. Rose, Real Digital Forensics: Computer Security and Incident Response, Paperback – Import, 2005.

Reference books:

1. John Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics Paperback, February 24, 2012.
2. Hacking Exposed: Network Security Secrets & Solutions, Stuart McClure, Joel Scambray and George Kurtz, McGraw-Hill, 2005.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY06) WIRELESS & MOBILE SECURITY(PROFESSIONAL ELECTIVE - II)

I Year I Sem. **L T P C**
3 0 0 3

Course Outcomes

1.Familiarize with the issues and technologies involved in designing a wireless and mobile system
2.Understanding of the various way through which wireless networks can be attacked and tradeoffs in protecting networks.
3. Design and implement wireless security protocols for source authentication, message integrity, message flow confidentiality, and anonymity.
4**.** Relate with new Threats, Vulnerabilities and Countermeasures in mobile networks.
5.Understand the concepts of wireless security.

UNIT I:

Overview of Wireless LAN physical components Wireless LAN topologies and technologies 802.11 a/b/g/n/ac Features, Understanding, Building and Configuring Wireless Networks Configure and install wireless adapters, access points, bridges and antennas, security features of 802.11 Wireless networks.

UNIT-II:

Wireless Application Protocol Overview, Wireless Transport layer security, WAP End-to-End Security, PSK Authentication, TKIP Encryption and AES-CCMP Encryption, key management in wireless network.

UNIT-III

Vulnerabilities in Cellular Services, Cellular Jamming Attacks & Mitigation, Wireless Jamming Attacks, Security in Cellular VoIP Services, Mobile application security

UNIT-IV

Enterprise Wireless Security, IEEE.11, Enterprise Wireless Security Devices (Thin Access Point) Wireless VLANs, Security threats and vulnerabilities in Wireless networks, Vulnerabilities of IEEE.11 Security, MAC Address Filtering Weaknesses, hacking Personal Wireless Security, WEP, WPA1 and WPA2, Caffe Latte Attack Basics, Caffe Latte Attack Demo , Koreks Chopchop Attack, Fragmentation And Hirte Attack, Cracking PEAP Hotspot Attacks, Hacking Isolated Clients

UNIT-V

Overview of WLAN security, Mobile IP security -, Attacks on 802.11 networks, Introduction/overview of ad hoc networks, Trust & reputation in ad hoc networks , Secure MANET routing, Node replication attacks, Collaborative cross-layer attacks, MAC misbehavior in MANETs, Security in hybrid systems, Location security & privacy , Location security & privacy, Vehicle Network Security, RFID Hacking and Authentication, Smartphone System Security, Smart Grid Security.

Text Book/Reference Books:

1. 802.11 Wireless Networks: The Definitive Guide by Matthew Gast, O'Reilly Media
2. Next Generation Wireless LANs: 802.11n and 802.11ac by EldadPerahia and Robert Stacey, Cambridge University Press
3. Controller-Based Wireless LAN Fundamentals: An end-to-end reference guide to design, deploy, manage, and secure 802.11 wireless networks by Jeff Smith, Jake Woodhams, Robert Marg, Cisco press14
4. Hacking Exposed Wireless, Third Edition: Wireless Security Secrets & Solutions by Joshua Wright , Johnny Cache, McGraw Hill.
5. BackTrack 5 Wireless Penetration Testing Beginner's Guide by Vivek Ramachandran

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 – 26

(M25CS25) CYBER SECURITY LAB

I Year I Sem. **L T P C**
0 0 4 2

Prerequisites

1. A course on "Network Security and Cryptography".

Course Outcomes:

1. Get the skill to identify cyber threats/attacks.
2. Get the knowledge to solve security issues in day to day life.
3. Acquire and analyze digital evidence from disk , mamory and network using forensic tools like Autopsy,FTK imager and Network Miner.
4. Interpret findings and prepare comprehensive reports to support invesitgations.

List of Experiments

1. Perform an Experiment for port scanning with NMAP.
2. Setup a honey pot and monitor the honey pot on the network
3. Install Jcrpt /Cryp tool tool (or any other equivalent) and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital/PKI signatures.
4. Generate minimum 10 passwords of length 12 characters using open SSL command
5. Perform practical approach to implement Foot printing-Gathering target information using Dmitry-Dmagic, UAtester.
6. Working with sniffers for monitoring network communication (Wireshark).
7. Use Snort to perform real time traffic analysis and packet logging.
8. Perform email analysis using Autopsy tool.
9. Perform Registry analysis and get boot time logging using process monitor tool
10. Perform File type detection using Autopsy tool
11. Perform Memory capture and analysis using FTK imager tool
12. Perform Network analysis using the Network Miner tool

TEXT BOOKS

1. Real Digital Forensics for Handheld Devices, E. P. Dorothy, Auerback Publications, 2013.
2. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010

REFERENCES:

1. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.
2. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C. H. Malin, E. Casey and J. M. Aquilina, Syngress, 2012
3. The Best Damn Cybercrime and Digital Forensics Book Period, J. Wiles and A.Reyes, Syngress, 2007.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY07) Information Security Lab (Professional Elective-I LAB)

I Year I Sem. **L T P C**
0 0 4 2

Course Outcomes:
1. Demonstrate the knowledge of cryptography, network security concepts and applications.
2. Ability to apply security principles in system design.
3. Ability to identify and investigate vulnerabilities and security threats and mechanisms to counter them
4. Ability to implement various cryptographic techniques.

List of Experiments:
1. Implementation of symmetric cipher algorithm (AES and RC4)
2. Random number generation using a subset of digits and alphabets.
3. Implementation of RSA based signature system
4. Implementation of Subset sum
5. Authenticating the given signature using the MD5 hash algorithm.
6. Implementation of Diffie-Hellman algorithm
7. Implementation of the ELGAMAL cryptosystem.
8. Implementation of Goldwasser- Micali probabilistic public key system
9. Implementation of Rabin Cryptosystem. (Optional).
10. Implementation of Kerberos cryptosystem
11. Firewall implementation and testing.
12. Implementation of a trusted secure web transaction.
13. Cryptographic Libraries-Sun JCE/OpenSSL/Bouncy Castle JCE.
14. Digital Certificates and Hybrid (ASSY/SY) encryption, PKI.
15. Message Authentication Codes.
16. Elliptic Curve cryptosystems (Optional)
17. PKCS Standards (PKCS1, 5, 11, 12), Cipher modes.

TEXT BOOK:

1.Cryptography and Network Security (principles and approaches) by William Stallings Pearson Education, 4th Edition.

REFERENCES:

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

2. Principles of Information Security, Whitman, Thomson.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY08) Machine Learning for Cyber Security Lab(Professional Elective-I LAB)

I Year I Sem. **L T P C**
0 0 4 2

PREREQUISITES:

Basic knowledge of linear algebra, probability and statistics. Familiarity with programming languages such as Python.

COURSE OUTCOMES

On completion of the course, students will be able to

CO1 - Understand basic machine learning concepts.
CO2 - Implement supervised and unsupervised algorithms for cyber security tasks.
CO3 - Apply data pre-processing operations for data cleaning and feature selection.
CO4 - Implement deep learning models for cyber security tasks.
CO5 - Analyze the results of machine learning models in cyber security.
CO6 - Build machine learning-based solutions for Cyber Security.

LIST OF EXPERIMENT:

1.Data Exploration and Preprocessing: Data exploration using Pandas and NumPy, Preprocessing of datasets, including handling missing values, scaling, encoding categorical variables, etc.

2. Supervised Learning Models: Linear and Non-linear Regression, Classification Models (KNN, SVM, Naïve Bayes, Decision Tree, Logistic Regression), Ensemble Techniques (Random Forests, Gradient Boosting), Neural Network Architecture using Tensor Flow or PyTorch, Hyper parameter Tuning for various machine learning algorithms

3. Unsupervised Learning and Anomaly Detection: Network Traffic Anomaly Detection using Clustering Algorithms (K-Means, Hierarchical Clustering, DBSCAN), Phishing Email Dataset Analysis using Clustering Algorithms

4. End-to-End Machine Learning Pipeline for Cyber security: Designing and implementing an end-to-end pipeline encompassing data preprocessing, model training, hyper parameter tuning, and evaluation using real-world cyber security datasets

5. Adversarial Attacks and Model Security: Implementing adversarial attacks (FGSM, PGD) on trained models for malware detection, Understanding and defending against adversarial attacks to ensure model security

6. Performance Evaluation and Comparative Analysis: Evaluating the performance of various machine learning models on cyber security tasks, Comparing the effectiveness of different algorithms and techniques in detecting and preventing cyber security threats

TEXT/REFERENCE BOOKS

1. Aurélien Géron, “Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow”, O'Reilly Media,Inc.
2. Sebastian Raschka, Vahid Mirjalili, “Machine Learning and Deep Learning with Python, Scikit-learn, andTensorFlow”, Packt Publishing
3. Jagannath E. Nalavade, “Machine Learning Approaches in Cyber Security”, Namya Press
4. Soma Halder, Sinan Ozdemir, “Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem”,Packt Publishing

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY09) System and Network Security Lab(Professional Elective-I)

I Year I Sem. **L T P C**
0 0 4 2

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the consequences of buffer overflow attacks.
CO2- Experiment with the Formatting String exploits.
CO3- Demonstrate the Integer Overflow attacks.
CO4- Understand the prevention and mitigation techniques to withstand against hardware trojans

LIST OF EXPERIMENT:

1. Buffer Overflow Attacks:
Implement buffer overflow to skip the execution of an instruction, buffer overflow to execute a script and start a shell.

2. Advanced Buffer Overflow Techniques:
Demonstrate Return-to-libc attack, Buffer overflow attack with Return Oriented Programming (ROP).

3. Other Security Vulnerabilities and Attacks:
Demonstrate Integer Overflow Vulnerability, Formatting string vulnerability attacks.

4. Advanced Security Concepts:
Study Hardware Trojans and their implications in security, Study and prepare a report on SSL design, focusing on its security features and vulnerabilities.

5. Network Security Analysis:
Run and analyze results from the Wireshark tool, focusing on network traffic, packet capture, and security analysis.

TEXT/REFERENCE BOOKS

1. James Houston Baxter, “Wireshark Essentials”, Packt Publishing.
2. Dennis Andriesse, “Practical Binary Analysis”, No Starch Press.
3. Greg Hoglund, Gary McGraw, “Exploiting Software How to Break Code”, Addison-Wesley
4. Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte, “The Shellcoder's Handbook Discovering and Exploiting Security Holes”, Wiley.
5. One, Aleph. "Smashing the stack for fun and profit." Phrack magazine.
6. B. Bierbaumer, K. Julian, K. Thomas, A.Francillon, and A. Zarras. "Smashing the stack protector for fun and profit." In ICT Systems Security and Privacy Protection: 33rd IFIP TC 11 International Conference, SEC 2018, Proceedings 33, pp. 293-306. Springer International Publishing, 2018.
7. D. Ahmad,. "The rising threat of vulnerabilities due to integer errors." IEEE Security & Privacy 1, no. 4 (2003):

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25MC01) RESEARCH METHODOLOGY & IPR

I Year I Sem. **L T P C**
2 0 0 2

Prerequisite: None

Course Outcomes:

At the end of this course, students will be able to

1. Understand research problem formulation.
2. Analyze research related information
3. Follow research ethics
4. Understand that today's world is controlled by Computer, Information Technology, but tomorrow world will be ruled by ideas, concept, and creativity.
5. Understanding that when IPR would take such important place in growth of individuals & nation, it is needless to emphasis the need of information about Intellectual Property Right to be promoted among students in general & engineering in particular.

UNIT-I

Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations.

UNIT-II

Effective literature studies approaches, analysis, Plagiarism, Research ethics

UNIT-III

Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee.

UNIT-IV

Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.

UNIT-V

Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications. New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.

TEXT BOOKS:

1. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students"
2. C.R. Kothari, Research Methodology, methods & techniques, 2nd edition, New age International publishers

REFERENCES:

1. Ranjit Kumar, 2nd Edition, "Research Methodology: A Step by Step Guide for beginners"
2. Halbert, "Resisting Intellectual Property", Taylor & Francis Ltd ,2007.
3. Mayall, "Industrial Design", McGraw Hill, 1992.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY10) ETHICAL HACKING

I Year II Sem. **L T P C**

3 0 0 3

Course Outcomes:

1.Describe the vulnerabilities in a system or network

2.Analyze and evaluate techniques used to break into an insecure web application and identify relevant countermeasures.

3.Evaluate the potential countermeasures to advanced hacking techniques.

4.Explain computer forensic fundamentals

5 Learn Hacking Web Browsers

UNIT -I:

Session Hijacking

Introduction to Session Hijacking, Spoofing Versus Hijacking, Types of Session Hijacking, TCP/IP Hijacking, Session Hijacking Tools, Dangers Posed by Hijacking, Countermeasures.

UNIT- II:

Hacking Web Servers

Introduction to Hacking Web Servers, Sources of Security Vulnerabilities in Web Servers, Webmaster's Concern, Network Administrator's Concern, End User's Concern, Risks, Web Site Defacement, Attacks against Internet Information Services, Piggybacking Privileged Command Execution on Back-End Database Queries (MDAC/RDS), Buffer Overflow Vulnerabilities, Privileged Command Execution Vulnerability, WebDAV/RPC Exploits, IIS 7 Components, Unicode Directory Traversal Vulnerability, Netcat, Tool: IIS Xploit, Msw3prt IPP Vulnerability, RPC DCOM Vulnerability, ASP Trojan, IIS Logs, Management, Patches and Hotfixes, Vulnerability Scanners, Online Vulnerability Search Engine, Countermeasures, File System Traversal Countermeasures, Increasing Web Server Security.

UNIT- III:

Web Application Vulnerabilities

Introduction to Web Application Vulnerabilities, Web Applications, Web Application, Anatomy of an Attack, Web Application Threats, Cross-Site Scripting/XSS Flaws, SQL Injection, Command Injection Flaws, Cookie/Session Poisoning, Parameter/Form Tampering,Buffer Overflow, Directory Traversal/Forceful Browsing, Cryptographic Interception, Authentication Hijacking, Log Tampering, Error Message Interception, Attack Obfuscation, Platform Exploits, DMZ Protocol Attacks, Security Management Exploits, Web Services Attacks, Zero-Day Attacks, Network Access Attacks, TCP Fragmentation, Web Application Hacking Tools.
Tool: Instant Source, Wget, WebSleuth, BlackWidow, SiteScope, Tool: WSDigger, CookieDigger, SSLDigger, WindowBomb, Burp Intruder, Burp Proxy, Burp Suite, Tool: cURL, dotDefender, Acunetix Web Vulnerability Scanner, AppScan, AccessDiver, Tool: NetBrute Scanner Suite, Emsa Web Monitor, Tool: KeepNI, Paros Proxy, WebScarab, IBM Rational AppScan, WebWatchBot,Ratproxy, Mapper.

UNIT- IV:

Web-Based Password Cracking Techniques

Introduction to Web-Based Password Cracking Techniques, Authentication, Authentication Techniques, HTTP Authentication, Integrated Windows (NTLM) Authentication, Negotiate Authentication, Certificate-Based Authentication, Forms-Based Authentication, RSA SecurID Token, Biometric Authentication, Password Cracking, Password Cracking Techniques, Password Cracker Programs, Password Cracker Countermeasures,

Tools: Password-Generating Tools, Password Recovery Tools, Password Revealing Tools, Password Security Tools.

UNIT -V:

Hacking Web Browsers

Introduction to Hacking Web Browsers, How Web Browsers Work, Hacking Firefox, Firefox Information Leak Vulnerability, Firefox Spoofing Vulnerability, Firefox Password Vulnerability, Concerns with Saving Forms or Login Data, Cleaning Up Browsing History, Cookies, Cookie Viewer, Cookie Blocking Options.

Tools for Cleaning Unwanted Cookies, Firefox Security, Getting Started, Privacy Settings, Security Settings, Content Settings, Clear Private Data, Firefox Security Features, Hacking Internet Explorer, Redirection Information Disclosure Vulnerability, Window Injection Vulnerability, Internet Explorer Security, Security Zones, Privacy, Specify Default Applications, Internet Explorer Security Features.

Hacking Opera, JavaScript Invalid Pointer Vulnerability, BitTorrent Header Parsing Vulnerability, BitTorrent File-Handling Buffer Overflow Vulnerability, Opera Security and Privacy Features, Hacking Safari, Safari Browser Vulnerability, iPhone Safari Browser Memory Exhaustion Remote DoS Vulnerability, Securing Safari, AutoFill, Security Features.

Text/Reference Books:

Ethical Hacking and Countermeasures: Web Applications and Data Servers by EC-Council.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CS04) NATURAL LANGUAGE PROCESSING

I Year II Sem. **L T P C**

3 0 0 3

Prerequisites:

1. Data structures, finite automata and probability theory. .

Course Outcomes:

1. Show sensitivity to linguistic phenomena and an ability to model them with formal grammars.
2. Understand and carry out proper experimental methodology for training and evaluating empirical NLP systems
3. Able to manipulate probabilities, construct statistical models over strings and trees, and estimate parameters using supervised and unsupervised training methods.
4. Able to design, implement, and analyze NLP algorithms Able to design different language modeling Techniques.
5. Able to design different language modeling Techniques.

UNIT – I

Finding the Structure of Words: Words and Their Components, Issues and Challenges, Morphological Models Finding the Structure of Documents: Introduction, Methods, Complexity of the Approaches, Performances of the Approaches

UNIT – II

Syntax Analysis: Parsing Natural Language, Treebanks: A Data-Driven Approach to Syntax Representation of Syntactic Structure, Parsing Algorithms, Models for Ambiguity Resolution in Parsing, Multilingual Issues

UNIT – III

Semantic Parsing: Introduction, Semantic Interpretation, System Paradigms, Word Sense Systems,Software.

UNIT – IV

Predicate-Argument Structure, Meaning Representation Systems, Software.

UNIT – V

Discourse Processing: Cohesion, Reference Resolution, Discourse Cohesion and Structure Language Modeling: Introduction, N-Gram Models, Language Model Evaluation, Parameter Estimation, Language Model Adaptation, Types of Language Models, Language-Specific Modeling Problems, Multilingual and Cross Lingual Language Modeling

TEXT BOOKS:

1. Multilingual natural Language Processing Applications: From Theory to Practice – Daniel M. Bikel and Imed Zitouni, Pearson Publication
2. . 2. Natural Language Processing and Information Retrieval: Tanvier Siddiqui, U.S. Tiwary.

REFERENCES:

3. 1. Speech and Natural Language Processing - Daniel Jurafsky & James H Martin, Pearson Publications.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY11) VULNERABILITY ASSESSMENT & PENETRATION TESTING (PE-III)

I Year II Sem. **L T P C**

3 0 0 3

Course Outcomes:

1. Understand social engineering attacks
2. Learn to handle the vulnerabilities of a Web application.
3. Perform penetration testing
4. Understand the Security Vulnerabilities of Web Application
5. Analyze the malware type and impact.

UNIT-I

Introduction Ethics of Ethical Hacking: Why you need to understand your enemy's tactics, recognizing the gray areas in security, Vulnerability Assessment and Penetration Testing. Penetration Testing and Tools: Social Engineering Attacks: How a social engineering attack works, conducting a social engineering attack, common attacks used in penetration testing, preparing yourself for face-to-face attacks, defending against social engineering attacks.

UNIT-II

Physical Penetration Attacks: Why a physical penetration is important, conducting a physical penetration, Common ways into a building, Defending against physical penetrations. Insider Attacks: Conducting an insider attack, Defending against insider attacks. Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit.

UNIT-III

Managing a Penetration Test: planning a penetration test, structuring a penetration test, execution of a penetration test, information sharing during a penetration test, reporting the results of a Penetration Test. Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process. Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections (XPSP3, Vista, 7 and Server 2008), Bypassing Windows Memory Protections.

UNIT-IV

Web Application Security Vulnerabilities: Overview of top web application security vulnerabilities, Injection vulnerabilities, cross-Site scripting vulnerabilities, the rest of the OWASP Top Ten SQL Injection vulnerabilities, Cross-site scripting vulnerabilities. Vulnerability Analysis: Passive Analysis, Source Code Analysis, Binary Analysis.

UNIT-V

Client-Side Browser Exploits: Why client-side vulnerabilities are interesting, Internet explorer security concepts, history of client-side exploits and latest trends, finding new browser-based vulnerabilities heap spray to exploit, protecting yourself from client-side exploit. Malware Analysis: Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware.

TEXT BOOKS:

1. Gray Hat Hacking-The Ethical Hackers Handbook", Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.
2. The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws", DafyddSuttard, Marcus pinto, 1st Edition, Wiley Publishing.

REFERENCES:

1. Penetration Testing: Hands-on Introduction to Hacking, Georgia Weidman, 1st Edition, NoStarch Press.
2. The Pen Tester Blueprint-Starting a Career as an Ethical Hacker, L. Wylie, Kim Crawly, 1 st Edition, Wiley Publications.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY12) DATA PRIVACY (PE-III)

I Year II Sem. **L T P C**

3 0 0 3

Course Outcomes:

1 Define differential privacy
2.Design techniques to achieve differential privacy for linear queries.
3.Design mechanisms for query release problem using online learning algorithms.
4.Analyze computational complexity of differentially private mechanisms
5. Understand the concepts of private machine learning

UNIT 1:

The Promise of Differential Privacy: Privacy-preserving data analysis; Basic Terms: The model of computation, Towards defining private data analysis, Formalizing differential privacy; Basic Techniques and Composition Theorems: Useful probabilistic tools, Randomized response, The laplace mechanism, The exponential mechanism, Composition theorems, The sparse vector technique;

UNIT-II:

Releasing Linear Queries with Correlated Error: An offline algorithm: SmallDB, An online mechanism: private multiplicative weights; Generalizations: Mechanisms via α-nets, The iterative construction mechanism, Connections;

UNIT-III:

Boosting for Queries: The boosting for queries algorithm, Base synopsis generators; When Worst-Case Sensitivity is Atypical: Subsample and aggregate, Propose test-Release, Stability and privacy; Lower Bounds and Separation Results: Reconstruction attacks,

UNIT-IV:

Lower bounds for differential privacy; Differential Privacy and Computational Complexity: Polynomial time curators, Some hard-to-Syntheticize distributions, Polynomial time adversaries; Differential Privacy and Mechanism Design:

UNIT-V :

Differential privacy as a solution concept, Differential privacy as a tool in mechanism design, Mechanism design for privacy aware agents; Differential Privacy and Machine Learning: The sample complexity of differentially private machine learning, Differentially private online learning, Empirical risk minimization; Additional Models: The local model, Pan-private streaming model, Continual observation, Average case error for query release.

Text Books:

1. C. Dwork and A. Roth, The Algorithmic Foundations of Differential Privacy, now Publishers, 2014.

Reference Books:

1. Charu C. Aggarwal, Privacy-Preserving Data Mining: Models and Algorithms, 1st Edition Springer, 2008.
2. Relevant Research Pape

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY13) CLOUD SECURITY (PE-III)

I Year II Sem. **L T P C**

3 0 0 3

Course Outcome:

1Ability to acquire the knowledge on fundamentals concepts of cloud computing
2. Able to distinguish the various cloud security and privacy issues.
3. Able to analyze the various threats and Attack tools
4. Able to understand the Data Security and Storage
5. Able to analyze the Security Management in the Cloud**.**

UNIT – I

Overview of Cloud Computing: Introduction, Definitions and Characteristics, Cloud Service Models, Cloud Deployment Models, Cloud Service Platforms, Challenges Ahead. Introduction to Cloud Security: Introduction, Cloud Security Concepts, CSA Cloud Reference Model, NIST Cloud Reference Model, NIST Cloud Reference Model

UNIT – II

Cloud Security and Privacy Issues: Introduction, Cloud Security Goals/Concepts, Cloud Security Issues, Security Requirements for Privacy, Privacy Issues in Cloud.
Infrastructure Security: The Network Level, the Host Level, the Application Level, SaaS Application Security, PaaS Application Security, IaaS Application Security

UNIT – III

Threat Model and Cloud Attacks: Introduction, Threat Model- Type of attack entities, Attack surfaces with attack scenarios, A Taxonomy of Attacks, Attack Tools-Network-level attack tools, VM- level attack tools, VMM attack tools, Security Tools, VMM security tools.

UNIT – IV

Information Security Basic Concepts, an Example of a Security Attack, Cloud Software Security Requirements, Rising Security Threats.
Data Security and Storage: Aspects of Data Security, Data Security Mitigation, Provider Data and Its Security.

UNIT – V

Evolution of Security Considerations, Security Concerns of Cloud Operating Models, Identity Authentication, Secure Transmissions, Secure Storage and Computation, Security Using Encryption Keys, Challenges of Using Standard Security Algorithms, Variations and Special Cases for Security Issues with Cloud Computing, Side Channel Security Attacks in the Cloud
Security Management in the Cloud- Security Management Standards, Availability Management, Access Control, Security Vulnerability, Patch, and Configuration Management.

TEXT BOOKS:

1. Cloud Security Attacks, Techniques, Tools, and Challenges by Preeti Mishra, Emmanuel S Pilli, Jaipur R C Joshi Graphic Era, 1 st Edition published 2022 by CRC press.
2. Cloud Computing with Security Concepts and Practices Second Edition by Naresh Kumar Sehgal Pramod Chandra, P. Bhatt John M. Acken, 2nd Edition Springer nature Switzerland AG2020.
3. Cloud Security and Privacy by Tim Mather, Subra Kumaraswamy, and Shahed Lati First Edition, September 2019.

REFERENCES:

1. Essentials of Cloud Computing by K. Chandrasekaran Special Indian Edition CRC press.
2. Cloud Computing Principles and Paradigms by Rajkumar Buyya, John Wiley

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY14) SECURE SOFTWARE ENGINEERING (PE-IV)

I Year II Sem. **L T P C**

3 0 0 3

Course Outcomes:

1. Explain terms used in secured software development and life cycle process
2. Incorporate requirements into secured software development process and test software for security vulnerability
3. Identify vulnerable code in implemented software and describe attack consequences
4. Apply mitigation and implementation practices to construct attack resistant software
5. Apply secure design principles for developing attack resistant software

UNIT-I:

Introduction & Motivation: Hacker vs. Cracker, Historical Background, Mode of Ethical Hacking, Hacker Motive, Gathering Information, Secure Software, Compliance Requirements, C-Level Language, Assets, Threats and Risks, Security Requirements, Confidentiality, Integrity, Availability

UNIT-II:

Secure Software Development Methodologies: Secure Software Development Lifecycle (SSDLC), Guidelines for Secure Software, SD-3 Principles, Security Practices, Secure coding standards, OWASP, ISO15408, Common Criteria (CC), build-insecurity

Requirements Engineering: Availability, Authenticity, Confidentiality, Efficiency, Integrity, Maintainability, Portability, Reliability, Requirements Engineering, Trustworthiness, Threat Analysis and Risk Management

UNIT-III:

Secure Architectural Design: Threat Modeling, Asset, Threat, Attack, Dataflow Diagram (DFD), Threat Tree (Attack Tree), STRIDE, DREAD. Security Architecture, Software Attack Surface, Secure, Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-based Access Control (RBAC),.

UNIT-IV:

Access Matrix Secure Coding and Security Testing: Introduction to Vulnerabilities, Vulnerability Patterns,Secure Coding Practices, Code Checking, Tools, Cross Site Scripting, Injection Flaws, Cross Site Request Forgery, Denial of Service, Test Cases, Security Test Plan, White Box Test, Black Box Test, Penetration Testing, Code Review, Test Report.

UNIT-V:

Secure Deployment: Secure Default Configuration, Product Life Cycle, Automated Deployment Process, Secure Target Environment, Secure Delivery of Code, Trusted Origin, Code Signing, Least Privilege Permissions, ITIL Release and Deployment Management Security Response: Security Response, Security Bulletins, Vulnerabilities, Security Patches, Disclosure, Responsible Disclosure, Patch Tuesday, Security Response Policy, Security Response Process, Common Vulnerability Scoring System, CVSS Code & Resource Protection: Introduction to Back Door, Time Bomb, Four-Eyes Principle, Confidentiality Classification, Background Screening, Security Clearance, Offline and Online Licensing, Mechanisms, Code Obfuscation

Text/Reference Books:

1. Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw and Nancy Mead Software Security Engineering: A Guide for Project Managers by. Addison-Wesley, (2004).
2. Gary McGraw, Software Security: Building Security, Addison-Wesley (2006)
. 3. Threat Modelling: Designing for Security by Adam Shostack, John Wiley and Sons Inc.
4. Mano Paul ,7 Qualities of Highly secure Software Taylor and Francis, CRC Press (2012) 5. Mark Merkow and Lakshmikanth Raghavan, Secure and Resilient Software, CRC Press, ISBN 9781439826973.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY15) INTRUSION DETECTION AND PREVENTION (PE-IV)

I Year II Sem. **L T P C**

3 0 0 3

Course Outcomes:

1.Analyze several security threats and the significance of security needs.
2.Describe various foundations on which detection approaches can be built.
3.Explain several types of IDS and IPS, their use and implementation, and also how to evaluate their performance.
4.Ability to learn Intrusion Detection and Prevention
5.Ability to learn IDS Tools

UNIT I

Network Attacks, Understanding Intrusion Detection and Intrusion Prevention System, Detection Approaches (Misuse Detection, Anomaly Detection, etc.),Uses of IDPS Technologies, Key Functions of IDPS Technologies, Stateful Protocol Analysis.

UNIT II

Data Collection (Host-Based, Network-Based, Application-Based, Application-Integrated and Hybrid), Theoretical Foundations of Detection - Taxonomy of anomaly detection system, fuzzy logic, Bayes theory, Artificial Neural networks, Support vector machine, Evolutionary computation, Association rules, Clustering, Architecture and Implementation.

UNIT III

IDS Challenges, Alert Management & Correlation (Data Fusion, Alert Correlation, Cooperative Intrusion Detection), Evaluation Criteria- Accuracy, Performance, Completeness, Timely Response, Adaptation and Cost-Sensitivity, Intrusion Tolerance and Attack Resistance, Test. Intrusion Response.

UNIT IV

Security and IDS Management (Data Correlation, Incident Response, Policy and Procedures, Law, Standards and organizations, Security Business issues, Future of Intrusion Detection and Prevention).

UNIT V

Implementation and Deployment: Internet Security System's Real Source, Snort, NFR Security, IDS Tools. Detail case study of IDS in different networks like Ethernet Networks, 802.11 Networks, Mobile Networks, Ad-hoc Networks, and Wireless Sensor Networks.

Text/ Reference Book:

1. Network Intrusion Detection and Prevention by Ali A. Ghorbani, Wei Lu MahbodTavallaee, Springer.
2. Intrusion Detection & Prevention by Carl Endorf, Eugene Schultz, and Jim Mellander, TMH.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY16) SCRIPTING LANGUAGES FOR INFORMATION SECURITY (PE-IV)

I Year II Sem. **L T P C**

3 0 0 3

Course Outcomes:

1 .Understand, analyze and build dynamic, interactive and secure web sites.
2 .Understand current and evolving Web languages for integrating media and user interaction in both front end and back end elements of a Web site.
3 .Analysis and reporting of web data and minimizing cyber risks.
4 .Applying different testing and debugging techniques and analyzing the web site effectiveness.
5 .Applying different cyber security tools and scripting languages to mitigate frequent cyber attacks.

UNIT-I

HTML: Introduction to HTML, What is HTML, HTML Documents, Basic structure of an HTML document, Creating an HTML document, Mark up Tags, Heading-Paragraphs, Line Breaks, HTML Tags. Elements of HTML: Introduction to elements of HTML, Working with Text, Working with Lists, Tables and Frames, Working with Hyperlinks, Images and Multimedia, Working with Forms and controls.

UNIT-II

Java Script: Introduction to JavaScript, Basic Syntax, Control Structures, Writing Functions, Working with Arrays, The Document Object Model, Events Handling, Client-side Validation, Form Validation & RegExps, ASP, Perl CGI, & Form Methods, SSI & Cookies, Frames & Windows, mimeTypes, plugins, & Java

UNIT-III:

PHP: PHP installation and Introduction, Loops String Functions in PHP, PHP Email Function, PHP Basics, Variables Arrays in PHP with Attributes Date & Time, Image, Uploading File handling in PHP Functions in PHP, Errors handling in PHP.

UNIT-IV:

Python: Introduction to Python, Python basics, Data Types and variables Operators, Looping & Control Structure List, Modules Dictionaries, String Regular Expressions, Functions and Functional Programming, Object Oriented Linux Scripting Environment – Classes, Objects and OOPS concepts, File and Directory Access, Permissions and Controls Socket, Libraries and Functionality Programming, Servers and Clients Web Servers and Client scripting, Exploit Development techniques, Writing plugins in Python, Exploit analysis, Automation Process, Debugging basics, Task Automation with Python.

UNIT-V:

Perl & NodeJS: Introduction to Perl – Overview of Perl Features, Getting and Installing Perl, Accessing Documentation via perldoc, HTML-Format Reference Documentation, Perl Strengths and Limitations, Security Issues in Perl Scripts. Introduction to Node.js; Events; Streams; Modules; Express; Socket.io; Persisting Data.

Text Books:

1. Deitel, Deitel and Nieto, Internet and Worldwide Web - How to Program, 5th Edition, PHI, 2011.
2. Bai and Ekedhi, The Web Warrior Guide to Web Programming, 3rd Edition, Thomson, 2008.

Reference Books:

1. Computer Programming And Cyber Security for Beginners: Zack Codings (Python Machine Learning, SQL, Linux, Hacking with Kali Linux, Ethical Hacking)

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CS12) NATURAL LANGUAGE PROCESSING LAB

I Year II Sem. **L T P C**

0 0 4 2

Prerequisites: Data structures, finite automata and probability theory

Course Outcomes:

1. Show sensitivity to linguistic phenomena and an ability to model them with formal grammars.
2. Able to manipulate probabilities, construct statistical models over strings and trees, and estimate parameters using supervised and unsupervised training methods.
3. Able to design, implement, and analyze NLP algorithms
4. Apply cognitive and statistical models to language tasks by combining rule-based and machine learning approaches to better understand sentence structure, meaning, and context.

List of Experiments

Implement the following using Python

1. Tokenization
2. Stemming
3. Stop word removal (a, the, are,.)
4. Word Analysis
5. Word Generation
6. Pos tagging
7. Morphology
8. chunking
9. N-Grams
10. N-Grams Smoothing

TEXT BOOKS:

1. Multilingual natural Language Processing Applications: From Theory to Practice – Daniel M. Bikel and Imed Zitouni, Pearson Publication

2. Natural Language Processing and Information Retrieval: Tanvier Siddiqui, U.S. Tiwary

REFERENCES:

1. Speech and Natural Language Processing - Daniel Jurafsky & James H Martin, Pearson Publications

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY17) VULNERABILITY ASSESSMENT & PENETRATION TESTING LAB(PE-III)

I Year II Sem. **L T P C**

0 0 4 2

Course Outcomes:

1. Design for monitoring network traffic
2. Perform different penetration testing methods
3. Design different types of vulnerabilities scanning
4. Understand web application assessment

List of Experiments:

1. Monitoring Network Traffic
2. Host & Services Discovery using Nmap
3. Vulnerability Scanning using OpenVAS
4. Internal Penetration Testing
    a. Mapping
    b. Scanning
    c. Gaining access through CVE's
    d. Sniffing POP3/FTP/Telnet Passwords
    e. ARP Poisoning
    f. DNS Poisoning
5. External Penetration Testing
    a. Evaluating external Infrastructure
    b. Creating topological map & identifying IP address of target
    c. Lookup domain registry for IP information
    d. Examining use of IPV6 at remote location
6. Different types of vulnerability scanning
7. Vulnerability scanning with Nessus
8. Web application assessment with nikto & burp suite

TEXT BOOKS:

1. Gray Hat Hacking-The Ethical Hackers Handbook, Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.
2. The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws, Dafydd Suttard, Marcus pinto, 1st Edition, Wiley Publishing.

REFERENCES:

1. Penetration Testing: Hands-on Introduction to Hacking, Georgia Weidman, 1st Edition, No Starch Press.
2. The Pen Tester Blueprint-Starting a Career as an Ethical Hacker, L. Wylie, Kim Crawly, 1st Edition, Wiley Publications.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY18) DATA PRIVACY LAB (PE-III)

I Year II Sem. **L T P C**

0 0 4 2

Course Outcomes:

1 Implementation of differential privacy mechanism for numeric, non-numeric and linear queries.
2 Implement composition techniques in the design of mechanisms.
3 Implement utility measurement of differential privacy to evaluate mechanisms.
4 Classify the existing mechanisms into several types: transformation, partitioning of dataset, query separation and iteration.

List of Experiments:

1. Implement differential privacy using the Laplace mechanism for numeric data
2. Implement differential privacy using the Exponential mechanism for non-numeric data
3. Implement differential privacy using the Gaussian mechanism for linear queries
4. Implement Sequential/parallel composition theorems in the design of the above mechanisms
5. Implement the utility measurements such as Noise size and error for data publishing and analysis to evaluate the performance of differential privacy mechanisms.
6. Use Machine learning approach to classify the mechanisms into several types

Text Books:

1. C. Dwork and A. Roth, The Algorithmic Foundations of Differential Privacy, now Publishers, 2014.

Reference Books:

1. Tianqing Zhu, Gang Li, Wanlei Zhou, Philip S. Yu, Differential Privacy and Applications, Springer International Publishing AG 2017.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY19) CLOUD SECURITY LAB (PE-III)

I Year II Sem. **L T P C**

0 0 4 2

Course Outcomes:

1. Ability to acquire the knowledge on fundamentals concepts of cloud computing.
2. Able to distinguish the various cloud security and privacy issues.
3. Able to analyze the various threats and Attack tools
4. Able to understand the Data Security and Storage

List of Experiments:

This lab mainly relies on Amazon Web Service (AWS), an IaaS cloud provider. Students are required to register an AWS account. Following task should be performed for different case studies

1. Infrastructure Security: *Network Architecture Design on Cloud: Design a secure network architecture on cloud:* Setup Virtual Private Cloud (VPC), Configure Subnet and Associate to VPC, Security Configuration on VPC
2. Instance Launching: Provide secure communication between Application server and Database server
3. Provisioning of Network level security, Host level security, Application level security in cloud
4. Illustrate Data security and Storage on cloud
5. Data privacy and security Issues, Jurisdictional issues raised by Data location
6. Identity & Access Management
7. Access Control
8. Trust, Reputation, Risk
9. Authentication in cloud computing, Client access in cloud, Cloud contracting Model, Commercial and business consideration

TEXT BOOKS:

1. Cloud Security Attacks, Techniques, Tools, and Challenges by Preeti Mishra, Emmanuel S Pilli, Jaipur R C Joshi Graphic Era, 1st Edition published 2022 by CRC press.

2. Cloud Computing with Security Concepts and Practices Second Edition by Naresh Kumar Sehgal Pramod Chandra, P. Bhatt John M. Acken,2nd Edition Springer nature Switzerland AG 2020.

3. Cloud Security and Privacy by Tim Mather, Subra Kumaraswamy, and Shahed Lati First Edition, September 2019.

REFERENCES:

1. Essentials of Cloud Computing by K. Chandrasekaran Special Indian Edition CRC press.

2. Cloud Computing Principles and Paradigms by Rajkumar Buyya, John Wiley.

3. https://www.nielit.gov.in/sites/default/files/cl.pdf

4. www.Sans.org

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY21) BIOMETRIC SECURITY (PE-V)

II Year I Sem. **L T P C**

3 0 0 3

Course Outcome (CO)

1. Understand and analyze biometric systems at the component level and be able to analyze and design basic biometric system applications.
2. Review technical challenges of biometric systems to build biometric identification systems.
3. Identify the sociological and acceptance issues associated with the design and implementation of biometric systems.
4. Apply knowledge to design security systems using biometrics.
5. Develop applications with intelligent biometric security systems with machine learning

UNIT I:

Overview of Biometrics: Biometric modalities, basic applications, benefits of biometrics over traditional authentication systems, Key biometric terms and processes, biometric characteristic, biometric systems: Identification, Verification. Biometric System Modules, Biometric system Errors: FAR/FRR. Threshold,Score distribution,. Applications of biometrics.

UNIT II:

Performance Measure of a biometric system, Accuracy, Confusion Matrix, Precision and Recall, null and alternative hypothesis h0, h1,Error type I/II, Matching score distribution, FM/FNM, ROC curve, DET curve, FAR/FRR curve.

UNIT III:

Physiological Biometrics, Fingerprint: Fingerprint Sensing, Feature extraction(Local ridge orientation and frequency, Segmentation, Singularity detection, Enhancement and binarization, Minutiae extraction), Matching(Correlation-based techniques, Minutiae-based methods, Ridge Feature-based techniques), Performance evaluation.

UNIT IV:

Introduction to Multi biometrics, Limitations of uni modal systems, levels of fusion, Feature level fusion techniques: concatenation, PCA, LDA , Score fusion techniques: sum rule, product rule, min rule, max rule, hamature t-norm, Normalization techniques, Multi biometrics Using Face and Ear.- Incorporating Ancillary Information in Multi biometric Systems.

UNIT V:

Biometric Template Security, Biometric system vulnerability, template protection schemes: Feature Transformation, Biometric Cryptosystem, Salting (e.g., Biohashing) , Non-invertible Transform, Key Binding, Key Generation.

Text books and References:

1. John Chirillo and Scott Blaul : “Implementing Biometric Security”, 1st Edition, Wiley Eastern Publication, 2005.
2. Anil K jain, Patrick Flynn, Arun A. (Eds.), Handbook of Biometrics, Springer, 2008.
3. Julian D. M. Ashbourn, Biometrics: Advanced Identify Verification: The Complete Guide,
   a. Springer-verlag, 2000.

Davide Maltoni, Handbook of Fingerprint Recognition.
Biometric Systems: Technology, Design and Performance Evaluation, Editors: J. Wayman, Jain, D. Maltoni and D. Maio, Springer, 2005

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY22) QUANTUM CRYPTOGRAPHY (PE-V)

II Year I Sem. **L T P C**

3 0 0 3

Course Outcomes: Graduates after completing the course shall gain**:**

1. Ability to understand concepts of quantum cryptography and cryptographic techniques.
2. To work in research institutions / Industry in the field of quantum cryptography.
3. To design new or modify existing quantum cryptographic techniques.
4. To understand quantum cryptography encryption and decryption schemes.
5. To understand the Quantum-Cryptographic Networks and the Ring of Trust models

.

UNIT I

Quantum Information Theory, Unconditional Secure Authentication, Entropy, Quantum Key Distribution, Quantum Channel, Public Channel, QKD Gain, Finite Resources

UNIT II

Adaptive Cascade Introduction, Error Correction and the Cascade Protocol, Adaptive Initial Block-Size Selection, Fixed Initial Block-Size, Dynamic Initial Block-Size, Examples

UNIT III

Attack Strategies on QKD Protocols: Introduction, Attack Strategies in an Ideal Environment, Individual Attacks in an Realistic Environment QKD Systems: Introduction, QKD Systems

UNIT IV

Statistical Analysis of QKD Networks in Real-Life Environment: Statistical Methods, Statistical Analysis QKD Networks Based on Q3P: QKD Networks, PPP, Q3P, Routing, Transport

UNIT V

Quantum-Cryptographic Networks from a Prototype to the Citizen: The SECOQC Project, How to Bring QKD into the “Real” Life

The Ring of Trust Model: Introduction, Model of the Point of Trust, Communication in the Point of Trust Model, Exemplified Communications, A Medical Information System Based on the Ring of Trust

TEXT BOOKS:

1. Kollmitzer C., Pivk M. (Eds.), Applied Quantum Cryptography, Lect. Notes Phys. 797 (Springer, Berlin Heidelberg 2010)

REFERENCES:

1. Quantum Cryptography by Donald J. Barrett.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY23) PRIVACY AND SECURITY IN ONLINE SOCIAL NETWORK (PE-V)

II Year I Sem. **L T P C**

3 0 0 3

Course Outcomes:
At the end of the course, a student should:

1. Explain the core concepts of the OSN, the properties, advantages and challenges brought about by the various models and applications.
2. Describe fundamental concepts of OSN security threats and attacks
3. Design solutions for mitigating the attack on OSN.
4. Evaluate the OSN analysis tools such as UCINET and NodeXL
5. Understanding OSN Application areas and UCINET and NodeXL

Unit I: Introduction
Online social Media and Policing, Online Social Networks, OSN architecture and components, OSN challenges, opportunities, and pitfalls in online social networks, privacy and security problems, Collecting data from Online Social Media

Unit II: OSN Security privacy
Trust, credibility, and reputations in social systems, Leakages and linkages of user information and content, Attacks and threats on the OSN, privacy issues on social media sites, Protecting user data from the OSN, Attacks from compromised accounts, Information privacy disclosure, revelation and its effects in OSM, Phishing in OSM & Identifying fraudulent entities in online social networks

Unit III: OSN Security solutions
Fine-grained Privacy Settings, View-centric Privacy Settings, Anonymizing social data, Third-party
Platforms, Information Hiding, Encryption, Crawling Behavior Exploitation, Semantic-based Approach, Exposure-based Access Controls

Unit IV: OSN attacks solutions
Random Walk based Detection, Centrality based Detection, Monitoring User Behavior based Detection, Credit Networks based Resistance, Trust Networks based Resistance, Community based Detection, Regulated APIs, Reputation Systems, Focused Hub, Behavioral Deviation, Anomaly Detection Principal Component Analysis, Social Honeypots, Feature based Detection

Unit V: OSN Applications
OSN application area, Online Social networking service, Applications of k-Anonymity and ℓ-Diversity in Publishing Online Social Networks, An Analysis of Anonymity in the Bitcoin System, understanding UCINET and NodeXL software for social network analysis

Text/Reference Books:

1. Security and Privacy in Social Networks by Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N., Pentland, A. (Eds.)
2. Social and Economic Networks by Matthew O. Jackson, Princeton University Press, 2010.
3. Social Media Security: Leveraging Social Networking While Mitigating Risk by Michael Cross
4. Security and Trust in Online Social Networks (Synthesis Lectures on Information Security, Privacy, and Trust), 2014 by Barbara Carminati, Elena Ferrari, Marco Viviani
5. Security, Privacy, and Anonymization in Social Networks: Emerging Research and Opportunities (Advances in Information Security, Privacy, and Ethics), 2018 by B. K. Tripathy, Kiran Baktha.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY27) CYBER LAWS AND RIGHTS IN THE DIGITAL AGE (OPEN ELECTIVE)

II Year I Sem. **L T P C**

3 0 0 3

Course Outcomes:

At the end of the course, a student should:

1. Explain the cybercrime and legal consequences in information technology.
2. Describe the ways of precaution and prevention of Cyber Crime
3. Evaluate the techniques used in cybercrime.
4. Analyze legal obligations in cyberspace and legal issues in cyber operations and in the use of related tools, techniques, technology, and data.
5. Understand the Cybercrime Examples and mini cases

UNIT I

Cyber Security Fundamentals: Introduction, cybercrime and Information Security, Classification of Cybercrimes, Cybercrime the legal Perspective, Cyber offences,, Cyber-attacks, Social engineering, Cyber stalking, Botnets, Attack Vector, Cybercrime and cloud computing, Cybercrimes on mobile and wireless devices, Attacks on mobile/cell phones, Authentication service security, Organizational security policies and measures in mobile computing

UNIT II

Ethics in Cyber Security: Privacy, Intellectual Property in the cyberspace, Professional Ethics, Freedom of Speech, Fair User and Ethical Hacking, Trademarks, Internet Fraud, Electronic Evidence, forensic Technologies, Digital Evidence collectionTools and Methods

UNIT III

Used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Phishing and Identity Theft, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer overflows

UNIT IV

Cybercrimes and Cyber security: Cybercrime and Legal Landscape around the world, Cyber laws, The Indian IT Act, Challenges, Digital Signatures and Indian IT Act, Amendments to the Indian IT Act, Cybercrime and punishment, Cost of Cybercrimes and IPR Issues, Web threats for Organizations, Social Computing and associated Challenges for Organizations.

UNIT V

Cybercrime Examples and Mini-Cases: Career Paths in Cyber security, Honey pots, Case study (Official Website Hacking, E-mail spoofing, Banking related Frauds, Credit Card related Frauds)

Text/Reference Books:

1. Cyber Security by Nina Godhole, Sunit Belapure, Wiley India.
2. Cyber Security Essentials by James Graham, Ryan Olson, Rick Howard CRC Press, Taylor & Francis Group, 2011 ISBN: 978-1-4398-5123-4

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY28) FOUNDATIONS OF BLOCKCHAIN TECHNOLOGY (OPEN ELECTIVE)

II Year I Sem. **L T P C**

3 0 0 3

Course Outcomes:

1. To understand the essential concepts and structural components of block chain and the rationale behind its implementation.
2. To understand the core technology, many types of block chains and protocols that operate the block chain.
3. To articulate and develop and test block chain-compatible diverse applications with smart contracts.
4. To understand and analyze the advantages and disadvantages of employing block chain technology in various industries and technologies
5. To understand the attacks and counter measures on block chain.

UNIT-I

Introduction to Block chain- Key Concepts of Block chain, Features of Block chain, Importance of Block chain, Block chain 1.0, 2.0, and 3.0, Issues to Centralized System, Centralized to Decentralized and Distributed System, Building Blocks of Block chain-Distributed Ledgers & P2P Networks, Block Header, Transaction Organization.

UNIT-II

Cryptographic Primitives, Basic Crypto Primitives- Hash Functions- Properties of Hash Function, Nonce, Merkle Trees, Hash Pointers, Public Key Cryptography- Public/private keys, Signature schemes, Signature correctness, Aggregate Signature, Threshold Signature

Decentralization- Distributed shared ledger, Distributed Consensus-Distributed Consensus Protocol. The classical theory of consensus, Byzantine General's Problem possibility and impossibility results, Asynchronous consensus, and Byzantine Fault Tolerance

UNIT-III

Types of Block chain- Permission-less Block chain- Bitcoin-Introduction to Bitcoin, Bitcoin Transaction, Bitcoin Protocol, Bitcoin Wallets, Bitcoin Block, Bitcoin Scripts, Bitcoin Network, Bitcoin Mining-Nakamoto Consensus- Proof-of-work, Mining target T, Proof-of-work equation, Mining Algorithm, Mining and reward, Block freshness, Partial and full nodes, Attacks on Bitcoin- Double-spend attacks, Selfish mining, **Ethereum Blockchain**, Introduction to Ethereum, Ethereum Networks, Ethereum Wallets, Ethereum Clients, Ethereum accounts, Transactions and State, Smart contracts, Privacy preserving smart contracts, Proof-of-stake, Variants of Ethereum blockchain

UNIT-IV

Permissioned Block chain- Hyperledger Fabric-, State Machine Replication, Distributed State Machines, MSP, Consensus- Raft Consensus Algorithm, Safety and liveness, Privacy based block chain, ZCash, Zero-knowledge-proof, R3 Corda, Corda Network .

UNIT-V

Block chain Security- Attacks on Block chain and their Countermeasures Block chain (BoT) Advantages of integrating Block chain to IoT, Trust Building, Cost Reduction, Accelerate Data Exchanges, Scaled Security for IoT, IoT Security using BC, Edge Security using BC, Cloud Security using BC, and E2E IoT Security using BC

Text Books:

1. Bitcoin and Cryptocurrency Technologies, A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, Princeton University Press. Henceforth termed as PUP (Princeton university press).
2. Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more, 3rd Edition, Imran Bashir, Packt Publishing, 2020, ISBN: 9781839213199. 3. Introduction to Cryptocurrencies, a basic online course by Haseeb Qureshi.Reference Books:

Reference Books:

1. William Magnuson, “Blockchain Democracy- Technology, Law and the Rule of the Crowd”, Cambridge University Press, 2020.
2. Pethuru Raj, Kavita Saini, Chellammal Surianarayanan, “Blockchain Technology and Applications”, CRC Press, 2021.

3. Chandramouli Subramanian, “Blockchain Technology”, Universities Press, 2020. 4. Relevant Research Paper and While Papers.

VAAGDEVI COLLEGE OF ENGINEERING

(AUTONOMOUS)

M. Tech. CSE(CYBER SECURITY)

EFFECTIVE FROM ACADEMIC YEAR 2025 - 26

(M25CY29) INFORMATION SECURITY RISK MANAGEMENT (OPEN ELECTIVE)

II Year I Sem. **L T P C**

3 0 0 3

Course Outcomes:
After completion of this course, students will be able to learn:

1. the importance of managing IS-related risk and security issues in organizations, and the relationship between these and the achievement of business value from IS/IT investments
2. evaluate the costs of not appropriately identifying and managing risk and security concerns in projects and organizations, resulting in IS/IT failures, dysfunctional systems, and systems which fail to deliver value to key stakeholders
3. The cognitive skills and practical ability to develop and document IS/IT risk and security management plans that detail contingency planning strategies and practices
4. The cognitive skills and ability to identify, analyze, synthesize and articulate the major• theories and concepts associated with IS failure
5. Evaluate the management of IS risk, including factors argued to lead to unsatisfactory outcomes with respect to IS/IT and Information Security

UNIT-I
An Introduction to Risk Management: Introduction to the Theories of Risk Management; The Changing Environment; The Art of Managing Risks.

UNIT-II
The Threat Assessment Process: Threat Assessment and its Input to Risk Assessment; Threat Assessment Method; Example Threat Assessment;

UNIT-III

Vulnerability Issues: Operating System Vulnerabilities; Application Vulnerabilities; Public Domain or Commercial Off-the-Shelf Software; Connectivity and Dependence; Vulnerability assessment for natural disaster, technological hazards, and terrorist threats; implications for emergency response, vulnerability of critical infrastructures;

UNIT-IV

The Risk Process: What is Risk Assessment? Risk Analysis; Who is Responsible?

UNIT-V

Tools and Types of Risk Assessment: Qualitative and Quantitative risk Assessment; Policies, Procedures, Plans, and Processes of Risk Management; Tools and Techniques; Integrated Risk Management; Future Directions: The Future of the Risk Management

Text books: 1. Malcolm Harkins, Managing Risk and Information Security, Apress, 2012.
2. Daniel Minoli, Information Technology Risk Management in Enterprise Environments, Wiley, 2009.

Reference books:
1. Andy Jones, Debi Ashenden ,Risk Management for Computer Security: Protecting Your Network & Information Assets, , 1st Edition, Butterworth-heinemann, Elsevier, 2005.
2. Andreas Von Grebmer, Information and IT Risk Management in a Nutshell: A pragmatic approach to Information Security, 2008, Books On Demand Gmbh.