INDIAN INSTITUTE OF INFORMATION TECHNOLOGY KOTTAYAM

Curriculum and Syllabus for the PG Course M.Tech. Programme in Cyber Security for Working Professionals

Contents

M.Tech. in Cyber Security
General Course Structure

Semester- I					
Course Code	Course Name	**L**	**T**	**P**	**C**
CBM511	Mathematical Foundations for Cyber Security	2	0	0	2
DSC512	Programming and Data Structures	2	0	2	3
CBM513	Computer Networks and Security	2	0	2	3
Semester- II					
CBM521	Secure Software Engineering	2	0	0	2
CBM 522	Information Security and Applied Cryptography	2	0	2	3
CBM523/CBM524	Decision Support and Artificial Intelligence/ AI,Machine Learning and Security	2	0	2	2
Semester- III					
CBM611	Cloud Computing and Security	2	0	2	3
CBM612/CBM613/~~CBM614~~	Advanced Database Security/Operating System Security	2	0	2	3
CBM615/CBM616	Blockchain Technology and Applications/ The Internet of Things: A Security Perspective	2	0	2	3
Semester- IV					
CBM621/CBM622	Intrusion Detection Systems and Firewall /Penetration Testing	3	0	2	4
CBM623/CBM624	Information Security Standards,Policies, Strategies & Audits/ Legal Aspects of Computing	2	0	0	2
CBM625	Criminal Psychology and Behaviour Intelligence	1	0	0	1
Semester- V					
CBM711	Project(Phase I)				14
Semester- VI					
CBM721	Project(Phase II)				14
Total Credits					60

L	T	P	C
2	0	0	2

SEMESTER I

CBM511 Mathematical Foundations for Cyber Security

Pre-requisites

Students are expected to have knowledge in basic linear algebra, probability theory, set theory and logic.

Course Objectives

- To provide mathematical background required for cyber security.
- To familiarise the basic building blocks of important cyber security applications.
- To discuss the theoretical aspects of number theory.
- To introduce vital concepts of graph and probability theory which will be useful for data compression, information hiding

Course Outcomes

Students who successfully complete this course will be able to: -

- Visualize abstract concepts, quantitative relationships, and spatial connections.
- Understand, communicate and model using symbols and numbers.
- Illustrate the use of algebraic structures in cryptography.
- Apply probability theory in key generation in an encrypted system.

Syllabus

Mathematical reasoning,Mathematical induction, Graph Theory: Representing Graphs and Graph Isomorphism, graph colouring, Hamilton circuits and Euler cycles, Fleury's algorithm,Weighted graphs, Dijkstra algorithm, Planar graphs.

Algebraic Structures: Groups, Modular arithmetic, Modulo groups, Modular exponentiation, Discrete logarithms, Modular inverse, Primitive roots, Rings, Fields, Galois Fields: GF (P^n),GF (2^n) and their applications in cryptography.

Number Theory: Fundamental theorem of arithmetic, Division algorithm, Prime and relatively prime, Mersenne primes, Euclidean algorithm, Extended Euclidean algorithm, Fermat's theorem, Euler totient function, Euler's Theorem, Congruences and Residue Classes, Chinese Remainder Theorem, Tests for primality-Solovay-Stressen test, Miller-Rabin test.

Probability and Statistics: Introduction to probability concepts, Family of random variables – types, densities and distributions, Statistical inference – Testing of hypothesis.

Game theory and its application in cyber security: Adversarial Modelling.

Learning Resources

1. Discrete Mathematics and its Applications, 7th ed. Author: Kenneth H. Rosen, Publisher: McGraw Hill.
2. Norman L. Biggs, Discrete Mathematics, Oxford University Press, Second Edition, 2003.
3. Papoulis A, Pillai SU. Probability, Random Variables, and Stochastic Processes. Tata McGraw-Hill Education, 2002.
4. Niven I, Zuckerman HS, Montgomery HL. An introduction to the theory of numbers. John Wiley & Sons, 1991.
5. Lewis, Harry, and Rachel Zax. Essential discrete mathematics for computer science. Princeton University Press, 2019.
6. Stinson, Douglas Robert, and Maura Paterson. Cryptography: theory and practice. CRC press, 2018.
7. Vince, John. Foundation Mathematics for Computer Science. Springer International Publishing, Switzerland, 2015.
8. Montgomery, Douglas C., and George C. Runger. Applied statistics and probability for engineers. Seventh Edition, John Wiley & Sons, 2018.
9. Gross, Jonathan L., and Jay Yellen. Graph theory and its applications. CRC press, 2005.
10. Das, Abhijit. Computational number theory. CRC Press, 2016.
11. Rosen KH. Elementary number theory. London: Pearson Education; 2011.
12. Dimitri, and John Tsitsiklis. Introduction to Probability. 2nd ed. Athena Scientific, 2008. ISBN: 9781886529236.
13. Probabilistic systems analysis and applied probability: Prof. John Tsitsiklis (MIT Lectures)

Research Papers

1. Taylor, Ian. "Alan M. Turing: The Applications of Probability to Cryptography." arXiv preprint arXiv:1505.04714 (2015).
2. Priyadarsini, P. L. K. "A survey on some applications of graph theory in cryptography." Journal of Discrete Mathematical Sciences and Cryptography 18, no. 3 (2015): 209-217. https://doi.org/10.1080/09720529.2013.878819

L	T	P	C
2	0	2	3

DSC512 Programming and Data Structures

Course Objectives

The course is intended to provide the foundations of the practical implementation and usage of Algorithms and Data Structures.

- Ensure that the student evolves into a competent programmer capable of designing and analysing implementations of algorithms and data structures for different kinds of problems.
- Expose the student to the algorithm analysis techniques, to the theory of reductions, and to the classification of problems into complexity classes like NP.

Course Outcomes

- Design and analyse programming problem statements.
- Choose appropriate data structures and algorithms, understand the ADT/libraries, and use it to design algorithms for a specific problem.
- Understand the necessary mathematical abstraction to solve problems.
- Come up with analysis of efficiency and proofs of correctness
- Comprehend and select algorithm design approaches in a problem specific manner.

Syllabus

Introduction: Introduction to Data Structures and Algorithms, Review of Basic Concepts, Asymptotic Analysis of Recurrences. Randomized Algorithms. Randomized Quicksort, Analysis of Hashing algorithms.

Algorithm Analysis Techniques - Amortized Analysis. Application to Splay Trees. External Memory ADT - B-Trees. Priority Queues and Their Extensions: Binomial heaps, Fibonacci heaps, applications to Shortest Path Algorithms. Partition ADT: Weighted union, path compression, Applications to MST. Algorithm Analysis and Design Techniques.

Dynamic Programming, Greedy Algorithms -Bellman-Ford. Network Flows-Max flow, min-cut theorem, Ford-Fulkerson, Edmonds-Karp algorithm.

Intractable Problems: Polynomial Time, class P, Polynomial Time Verifiable Algorithms, class NP, NP completeness and reducibility, NP Hard Problems, Approximation Algorithms.

Learning Resources

1. Introduction to Algorithms, by T. H. Cormen, C. E. Lieserson, R. L. Rivest, and C. Stein, Third Edition, MIT Press.
2. Fundamentals of Data Structures in C by Horowitz, Sahni, and Anderson-Freed, Universities Press
3. Algorithms, by S. Dasgupta, C. Papadimitrou, U Vazirani, Mc Graw Hill.
4. Algorithm Design, by J. Klienberg and E. Tardos, Pearson Education Limited.

L	T	P	C
2	0	2	3

CBM513 Computer Networks and Security

Pre-requisites

No prerequisite courses. However, please consult the instructor if you are not sure about the programming requirement.

Course Objectives

- Study of architecture and protocols of computer networks.
- Study the ISO and Internet models; medium access control and retransmission protocols; protocol analysis and verification; data-communication principles.
- Comprehend the necessity of network security along with the basic concept of Network security.
- Investigate various network vulnerabilities like virus, worm, malware, rootkit and devise strategies to mitigate them.
- Analyse privacy threatening behaviour over the internet and formulate defensive techniques to preserve privacy.

Course Outcomes

Students who successfully complete this course will be able to:-

- List all layers and their functionality of the ISO and Internet network architectures.
- Describe the concepts underlying the design and implementation of the major protocols at various network layers.
- Understand the need for network security and have a thorough grasp of the fundamentals of network security.
- Recognise network vulnerabilities and develop Network defensive strategies by utilizing Intrusion Detection Systems, Honeypot etc.
- Identify and defend against various privacy threatening tools and techniques over the internet.

Syllabus

Introduction: Overview and motivation: Telephone Network and the Internet Network, Circuit Switching vs. Packet Switching, History of the Internet. Architecture-OSI, TCP/IP models, Physical and Data link layer protocols: Encoding, Framing, Error detection, HDLC, PPP, sliding window protocols. Network Layer protocols: Internet addressing, IP, ARP, ICMP, CIDR, Routing algorithms. Transport Layer protocols: UDP, TCP, flow control, congestion control. Application Layer protocols: DNS, Web, HTTP, email, authentication, encryption.

Introduction to Network Security: Need for Network Security, Network Security Fundamentals, Principles of Security, Working of internet and DNS Vulnerabilities, Secure Network Communication.

Malware, Insider Attack and Defence, Computer Virus Types and Defence, Computer Worms, Rootkits, Botnet, Denial of Service Attack.

Need For Physical Security, User Authentication Technologies, Environmental Attacks and Accidents, Firewall, Intrusion Detection System, Honeypot, Tunnelling, Virtual Private Network, Privacy Preserving Communication, Anonymity, Onion Routing.

Learning Resources

1. Michael Goodrich, Roberto Tamassia, Introduction to Computer Security: Pearson publications, 2nd edition, 2021, ISBN-13: 978-0133575477. 2
2. L. L. Peterson and B. S. Davie, Computer Networks: A Systems Approach, 6th edition, Elsevier publications, 2021, Paperback ISBN: 9780128182000.
3. A. S.Tanenbaum and D.J. Wetherall, Computer Networks, Pearson publications, 5th Edition, 2013, ISBN-13: 978-8131770221.
4. J. F. Kurose and K. W. Ross, Computer Networking: A Top-Down Approach, 7th Edition, Pearson publications, 2017, ISBN-13: 9780134296159.
5. Kun Peng, Anonymous Communication Networks: Protecting Privacy on the Web, Auerbach publications, 2019, ISBN: 9780367378738.
6. Sagar Rahalkar, Quick Start Guide to Penetration Testing: With NMAP, OpenVAS and Metasploit, 1st Edition, Apress publications, 2019, Softcover ISBN: 978-1-4842-4269-8.
7. Christopher Hadnagy, Social Engineering: The Science of Human Hacking, 2nd Edition, Wiley Publisher, 2018, ISBN-13: 978-1119433385.

L	T	P	C
2	0	0	2

SEMESTER II

CBM 521 Secure Software Engineering

Course Objectives

- Design and implementation of secure software
- Introduce the role of security in the development lifecycle
- To design secure software
- To learn methodological approaches to improving software security during different phases of software development lifecycle
- To know best security programming practices.

Course Outcomes

Students who successfully complete this course will be able to:-

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

Syllabus

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.

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 Secure Architectural Design: Threat Modelling, 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), 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.

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.

Learning Resources

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.

L	T	P	C
2	0	2	3

CBM522 Information Security and Applied Cryptography

Pre-requisites

Mathematical Foundations for Cyber Security (CBM 511)

Course Objectives

- To lay a foundation on Security in Networks, Classical Cryptosystem and Block Cipher Modes of Operation.
- To analyse various Private and Public key Cryptosystem for encryption, key exchange and hashing, Authentication Protocols.
- To acquire the fundamental knowledge on applications of cryptography.

Course Outcomes

Students who successfully complete this course will be able to:-

- Understand the fundamental concepts of Classical and modern Cryptosystem.
- Compare various private and public key Cryptosystem for encryption, key exchange and authentication algorithms.
- Understand the different applications of cryptography.

Syllabus

Introduction – Cryptography, cryptanalysis, cryptology, classical cryptosystem- shift cipher, affine cipher, Vignere cipher, substitution, transposition techniques.

Block Ciphers and Modes of Operations- DES - Data Encryption Standard-Block cipher principles-block cipher modes of operationAES-TripleDES-Blowfish-RC5.

Public Key Cryptography- Public Key Cryptosystem, Key distribution, Diffie Hellman Key Exchange-MITM Attack - RSA, Random Number Generation-ECC-Key Management.

Hash Functions and Digital Signatures- Authentication requirement– Authentication function – MAC – Hash function – SHA - HMAC - Digital signature and authentication protocols.

Applications- Authentication – Kerberos, IP Security – IPSec, Web Security - SSL, TLS, Blockchain, IoT Security.

Learning Resources

1. William Stallings, Cryptography and Network Security –6th Edition, Pearson Education.
2. Behrouz A. Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, 5nd Edition, Mc Graw Hill Education.
3. Rich Helton, Johennie Helton, Mastering Java Security: Cryptography Algorithms and Practices, John Wiley Publishers.
4. Charles P. Pleeger, "Security in Computing", Pearson Education Asia, 5th Edition.
5. William Stallings, "Network Security Essentials: Applications and standards", Person Education Asia.
6. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security: Private Communication in a public world", Prentice Hall India, 6th Edition.

L	T	P	C
2	0	2	3

CBM523 Decision Support and Artificial Intelligence

Pre-requisites

None.

Course Objectives

- An overview of different Decision support system and Machine Learning models
- Using Machine Learning for effective security
- Various attack on ML models
- Machine Learning and Privacy

Course Outcomes

- Understand the concepts in Machine Learning
- Learn how to use machine learning for solving cyber security issues

Syllabus

Introduction: data science, data analytics, machine learning, and Artificial Intelligence. Programming in Python, Basics of manipulation of Data. Introduction to modern data analysis (Data visualization; probability; histograms; multinomial distributions).

Machine Learning Overview: Types of learning, Supervised, Unsupervised, Application in Security

Deep Learning Overview: Applying Deep Learning in various use cases, anomaly detection.

Artificial Intelligence in Cyber Security: Model Stealing & Watermarking, Network Traffic Analysis, Network Traffic Analysis.

Learning Resources

1. Tom Mitchell. Machine Learning. McGraw Hill, 1997.
2. Machine Learning: A Probabilistic Perspective, Kevin P Murphy, MIT Press.
3. Christopher M. Bishop. Pattern Recognition and Machine Learning. Springer 2006.

4. Deep Learning by Ian Goodfellow, Yoshua Bengio, and Aaron Courville

5. Cathy O'Neil and Rachel Schutt. Doing Data Science, Straight Talk from The Frontline. O'Reilly. 2014.

L	T	P	C
2	0	2	3

CBM524 AI, Machine Learning and Security

Course Objectives

The course aims to:

- Develop foundational skills in Python programming and data manipulation techniques relevant to data-driven security.
- Familiarize students with modern data analysis techniques, including data visualization, probability distributions, and statistical tools.
- Provide an overview of machine learning paradigms, with a focus on supervised and unsupervised learning techniques applied to cybersecurity.
- Introduce deep learning concepts and explore their use in anomaly detection and related security challenges.
- Examine the application of artificial intelligence in cybersecurity, including model security, network traffic analysis, and attack detection.

Course Outcomes

Students who successfully complete this course will be able to:

- Write Python programs for data manipulation and basic analysis using libraries relevant to data science and security.
- Apply statistical techniques such as histograms and probability distributions to understand and visualize security-related data.
- Differentiate between supervised and unsupervised learning and identify their applications in threat detection and anomaly analysis.
- Implement basic machine learning models and evaluate their use in cybersecurity scenarios.
- Describe the role of deep learning in security applications and demonstrate its use in tasks like anomaly detection.
- Analyze cybersecurity threats using AI-driven techniques such as model watermarking, model stealing detection, and network traffic analysis.

Syllabus

Introduction: Role of AI in Cyber Security and Security Framework: Artificial Intelligence in Cyber Security, Challenges and Promises, Security Threats of Artificial Intelligence, Use-Cases: Artificial Intelligence Email Observing, Data Manipulation using Python (NumPy, Pandas), Introduction to modern data analysis- Data Visualization, Basic Probability and Statistics, Histograms and Multinomial Distributions.

Machine Learning in Security: Introduction to Machine Learning, Applications of Machine Learning in Cyber Security Domain, Machine Learning: tasks and Approaches, Anomaly Detection, Privacy Preserving Nearest Neighbour Search, Machine Learning Applied to Intrusion Detection, Online Learning Methods for Detecting Malicious Executables.

Deep Learning in Security: Introduction to deep learning, Cyber Security Mechanisms Using Deep Learning Algorithms, Application of Deep Learning in: Anomaly detection, Behavioral analytics, Malware classification, Network Cyber threat Detection.

Artificial Intelligence in Cyber Security: Model Stealing & Watermarking, Network Traffic Analysis, Malware Analysis.

Learning Resources

1. Tom Mitchell. Machine Learning. McGraw Hill, 1997.
2. Gupta, Brij B., and Quan Z. Sheng, eds. Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press, 2019.
3. Artificial Intelligence and Data Mining Approaches in Security Frameworks, Editor(s):Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, Rashmi Agrawal, 2021.
4. Tsai, Jeffrey JP, and S. Yu Philip, eds. Machine learning in cyber trust: security, privacy, and reliability. Springer Science & Business Media, 2009.
5. Machine Learning: A Probabilistic Perspective, Kevin P Murphy, MIT Press. 6. Christopher M. Bishop. Pattern Recognition and Machine Learning. Springer 2006.

L	T	P	C
2	0	2	3

SEMESTER III

CBM611 CLoud Computing and Security

Pre-requisites

Distributed system security, Computer networks and Security

Course Objectives

- Understand the principles of distributed, cluster, and grid computing in relation to cloud environments.
- Analyze security challenges in cloud computing, including virtualization and data protection.
- Explore cloud security frameworks, compliance, and risk management strategies.
- Gain expertise in security tools and threat mitigation techniques across AWS, Azure, and Google Cloud.
- Implement security automation, identity management, and cloud policy enforcement for enterprise environments.

Course Outcomes

- Evaluate and implement security controls for different cloud service and deployment models.
- Apply data security and identity management best practices in multi-cloud environments.
- Utilize cloud-native security tools for threat detection, monitoring, and compliance.
- Automate security policies and incident response across AWS, Azure, and Google Cloud.
- Design and deploy enterprise-grade cloud security architectures for real-world applications.

Syllabus

Introduction - Overview of Distributed Computing, Cluster computing, Grid computing - Cloud Computing – Characteristics -Service and Deployment Models – SLA -Security Challenges - Virtualization - High Availability (HA)/Disaster Recovery (DR) using Virtualization - Cloud Data Security - Data Protection.

Microsoft Defender for Cloud-Azure DDoS Protection-Azure Firewall-Azure Information

Protection- Azure Security Center-Azure Front Door- WAF-Azure Active Directory-Azure Policy-Azure Key Vault.

AWS Security Hub-Amazon Guard Duty -AWS Shield -AWS Firewall Manager-AWS Macie - AWS Config -Amazon CloudFront - AWS Global Accelerator - AWS WAF - AWS Elastic Load Balancing (ELB) -Cloud watch - Cloud Trail - Security automation – Identity and Access Management.

Google Cloud Security Command Center -Chronicle Security Operations-Google Cloud Armor- Google Cloud Firewall -Google Cloud Data Loss Prevention (DLP)-Google Cloud CD - Cloud Load Balancing - Google Cloud Identity and Access Management - Google Cloud Policy Intelligence

Learning Resources

1. Kai Hwang, Geoffrey C. Fox and Jack J. Dongarra, "Distributed and cloud computing from Parallel Processing to the Internet of Things", Morgan Kaufmann, Elsevier – 2012
2. Barrie Sosinsky, "Cloud Computing Bible" , John Wiley & Sons, 2010
3. Tim Mather, Subra Kumaraswamy, and Shahed Latif, "Cloud Security and Privacy An Enterprise Perspective on Risks and Compliance", O'Reilly 2009
4. Vic (J.R.) Winkler, "Securing The Cloud: Cloud Computing Security Techniques and Tactics", Syngress/Elsevier
5. Thomas Erl, "Cloud Computing Design Patterns", Prentice Hall.
6. Dac-Nhuong Le, Raghvendra Kumar, Gia Nhu Nguyen, Jyotir Moy Chatterjee," Cloud Computing and Virtualization", Scrivener Publishing LLC, Wiley digital library, 2018.
7. John R. Vacca, "Computer and Information Security Handbook", Elsevier, 2009. 10. Mark Rhodes -Ousley, "Information Security – The complete reference", McGraw Hill, 2013.
8. $https://cloud.google.com/docs$
9. $https://docs.aws.amazon.com/$
10. $https://learn.microsoft.com/en-us/azure/?product=popular$

L	T	P	C
2	0	2	3

CBM612 Advanced Database Security

Pre-requisites

None.

Course Objectives

- Introduce the database and its security issues.
- Compare in details the various state-of-art database security methods and techniques.
- Learn in detail the security features in databases.
- Understand the database security analysis tools.

Course Outcomes

Students who successfully complete this course will be able to

- Understand and characterize modern techniques of database information security threats and techniques for database security assessment.
- Analyze information in a database to identify information security incidents
- Understand and use the main tools for database management systems monitoring.
- Apply build-in database functions to enable database integrity support.
- Create a plan for vulnerabilities detection and identification in databases

Syllabus

Introduction- Database System Applications, Purpose of Database Systems, Introduction to the Relational Model - Querying relational data, Form of Basic SQL Query - Examples of Basic SQL Queries.

Introduction to database security issues- Confidentiality, Integrity, Availability (CIA triad) for databases, Security challenges in databases, Common database vulnerabilities - Insider attacks, Active directory attacks, buffer overflow attacks, Multi-layered security architecture for databases

Database security methods and techniques- Authentication and authorization mechanisms, Access control models (Discretionary Access Control, Access Control, Role Based Access Control), Data masking and redaction (Static and dynamic techniques), Encryption techniques in databases, Database Application firewall, Cloud database security considerations.

SQL injection attack: Introduction to SQL injection attacks, Types of SQL injection attack, SQL injection mitigation using secure coding practices, SQL injection attack detection and prevention using database firewall. Crash recovery mechanisms: Secure database backup and recovery mechanisms, Secure server replication, Load balancing, Change Data Tracking (CDC), Point-in-time- recovery.

Database security analysis tools-Database security scanners. Writing your own security analysis tools. Database auditing and logging, Real-time monitoring and alerting through Security information and event management (SIEM) integration, Penetration testing using sqlmap and burp suite.

Learning Resources

1. Basta A., Zgola M, "Database Security" 3nd Edition, Cengage Learning, US, 2011
2. Ron Ben Natan, "Implementing database security and auditing", Digital Press, 2005.
3. Bhavani Thuraisingham, Database and Applications Security, Auerbach Publications, 2005.
4. Rose Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, John Wiley & Sons, 2001.
5. Michael Gertz, Sushil Jajodia, Handbook of Database Security Applications and Trends, Springer, 2008.
6. Silvana Castano, Database Security, ACM Press. Alfred Basta, Melissa Zgola, Database Security, Cengage Learning.

L	T	P	C
2	0	2	3

CBM613 Operating System Security

Course Objectives

- Learn security of operating systems.
- Learn relevant tools to secure operating systems.
- Learn how to enforce mandatory access control.
- General information security.

Course Outcomes

Students who successfully complete this course will be able to

- Identify and define key terms related to operating systems.
- Learn, and understand the main concepts of advanced operating systems design.
- Develop ability to protect operating systems.
- Improve the security of operating systems from malicious software.

Syllabus

Fundamentals: OS Processes, Synchronization, Memory Management, File Systems Trusted Operating Systems, Assurance in Trusted Operating Systems, Virtualization Techniques. Secure operating systems- Security goals, Trust model, Threat model Access Control Fundamentals – Protection system – Lampson's Access Matrix, Mandatory protection systems, Reference monitor.

Multics: Multics system, Multics security, Multics vulnerability analysis Security in Ordinary OS – Unix, Windows, Verifiable security goals – Information flow, Denning's Lattice model, Bell-Lapadula model, Biba integrity model, Covert channels.

Security Kernels: Secure Communications processor, Securing Commercial OS

Secure Capability Systems – Fundamentals, Security, Challenges-Secure Virtual Machine Systems, Case study - Linux kernel, Android, DVL, Solaris Trusted Extensions.

Learning Resources

1. Andrew S. Tanenbaum, Modern Operating Systems, Third Edition, Prentice Hall, 2007.
2. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, Operating System Concepts with Java", Eighth Edition, Wiley, 2008.
3. Trent Jaeger, Operating System Security, Synthesis Lectures on Information Security, Privacy and Trust, Morgan and Claypool, 2008.
4. C. P. Pfleeger and S. L. Pfleeger, Security in Computing, Prentice Hall Professional, 2003.
5. W. Mauerer, Professional Linux Kernel Architecture, Wiley, 2008.
6. D. P. Bovet and M.Cesati, Understanding the Linux Kernel, Third Edition, O'Reilly Media, Inc., 2005.

L	T	P	C
2	0	2	3

CBM615 Blockchain Architecture and Applications

Pre-requisites

Computer Networks and Security, Information Security and Applied Cryptography.

Course Objectives

- Introduce the concept and the basics of blockchain technologies,
- Enable awareness on the different generations of blockchains.
- Provide knowledge on various applications of blockchain technologies

Course Outcomes

Students who successfully complete this course will be able to:

- Understand the basics of blockchain Technologies and its various applications.
- Capable to identifying problems on which blockchains could be applied.

Syllabus

Introduction – Blockchain history, basics, architectures, Types of blockchain, Base technologies – Dockers, Hash function, Digital Signature - ECDSA, Zero Knowledge Proof.

Bitcoins – Fundamentals, aspects of bitcoins, properties of bitcoins, bitcoin transactions, bitcoin P2P networks, block generation at bitcoins, consensus algorithms- Proof of Work, Proof of Stake, Proof of Burn.

Ethereum- Introduction to Ethereum, Consensus Mechanisms, Smart Contracts.

Applications – Blockchain applications, e-governance, smart cities, smart industries, Finance, Medical Record Management System, use cases, trends on Blockchains.

Learning Resources

1. Baxv Kevin Werbach, The Blockchain and the new architecture of Trust, MIT Press, 2018
2. Joseph J. Bambara and Paul R. Allen, Blockchain – A practical guide to developing business, law, and technology solutions, McGraw Hill, 2018.

3. Joseph J. Bambara and Paul R. Allen, Blockchain, IoT, and AI: Using the power of three to develop business, technical, and legal solutions, Barnes & Noble publishers, 2018.

4. Melanie Swan, Blockchain – Blueprint for a new economy, OReilly publishers, 2018.

5. Jai Singh Arun, Jerry Cuomo, Nitin Gaur, Blockchain for Business, Pearson publishers, 2019.

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

L	T	P	C
2	0	2	3

CBM616 The Internet of Things: A Security Perspective

Pre-requisites

- Computer Networks and Security
- Programming and Data Structure

Course Objectives

- Introduce the concepts and basics of Wireless and IoT technologies.
- Analyze various secured Wireless Communication Protocols for IoT Infrastructure.
- Provide knowledge on various applications of IoT based technologies and their associated circuits.
- Enable awareness on the different IoT Vulnerabilities, Attacks, and security methods

Course Outcomes

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

- Learn the basics of communication in wireless sensor network and IoT.
- Compare various secured Wireless Communication Protocols for IoT Infrastructure.
- Understand the various applications of IoT
- Design IoT based applications using Arduino or Raspberry PI boards.
- Understand the various attacks and different security measures in IoT infrastructure.

Syllabus

Introduction - Basics of networking - wired, wireless, MANET, PAN, Wireless Sensor Networks, M2M Communication.

Secured Wireless Communication Protocols for IoT Infrastructure - IPv6 -LowPAN, LoRa, Transport-Bluetooth- LPWAN, Data -MQTT –CoAP.

IoT architectures and programming - basic architectures, Sensor basics, sensing and actuation, sensor communications, connectivity challenges Data processing mechanisms, scalability issues, visualization issues, analytics basics, the utility of cloud computing, fog computing, and edge computing, advanced IoT architectures Raspberry Pi and Arduino programming.

IoT security: Vulnerabilities, Attacks, and countermeasures - security engineering for IoT

development - IoT security lifecycle.

Privacy preservation models in IoT -Trust and Authentication models in IoT - Wireless Communication for Industrial IoT - Security in Industrial IoT, and Best Practices.

Learning Resources

1. Pethuru Raj and Anupama C. Raman, The Internet of Things: Enabling Technologies, Platforms, and Use Cases, CRC Press, First edition, 2017.
2. B. Rusell and D. Van Duren, "Practical Internet of Things Security," Packt Publishing, 2016.
3. Fei HU, "Security and Privacy in Internet of Things (IoTs): Models, Algorithms,and Implementations", CRC Press,2016
4. Honbu Zhou, The Internet of Things in the Cloud: A Middleware Perspective, CRC press, First edition, 2012.
5. Arshdeep Bahga and Vijay Madisetti, Internet of Things: A Hands-on Approach, Universities Press, First edition, 2014.
6. Mung Chiang, Bharath Balasubramanian, Flavio Bonomi, Fog for 5G and IoT (Information and Communication Technology Series, Wiley series, First edition, 2017.
7. Alan A. A. Donovan, Brian W. Kernighan, The Go Programming Language, Addison-Wesley Professional Computing Series, First edition, 2015.

L	T	P	C
3	0	2	4

SEMESTER IV

CBM621 Intrusion Detection Systems and Firewall

Pre-requisites

AI, Machine Learning and Network Security

Course Objectives

- To understand the architecture, configuration, and analysis of specific intrusion detection systems
- To provide the fundamentals, background, and knowledge base required to setup and manage an intrusion detection system on a networked system of computers.
- To analyze the security of an organization and appropriately apply Intrusion Detection tools and firewalls in order to improve their security posture.

Course Outcomes

Students who complete this course will be able to:

- Understand modern concepts related to Intrusion Detection System.
- Do quantitative analysis for determining the best tool or approach to reduce risk from intrusion
- Construct and adapt firewalls and intrusion detectors and analyse their architectures
- Apply security principles to firewalls and intrusion detection systems.

Syllabus

Introduction: Introduction to Intrusions, Need of Intrusion Detection, Classification of Intrusion Detection Systems, Sources of Vulnerabilities, Attacks against various security objectives, countermeasures of attacks.

Intrusion Detection and Prevention Technologies: Host-based intrusion detection system (HIDS), Network-based IDS, Information Sources for IDS, Host and Network Vulnerabilities and Countermeasures. Intrusion detection techniques, misuse detection: pattern matching, rule-based and state-based anomaly detection: statistical based, machine learning based, data mining-based hybrid detection.

IDS infrastructure:IDS Architecture, IDS/IPS Management and Architecture Issues with

regard to deploying IDS/IPS systems, end point approach to security, system approach to security, Case study on commercial and open-source IDS.

Firewall: Introduction, Firewall Operational Models, Firewall architecture, Process of Firewall Design, Implementation, and Maintenance, Firewall Policy Formalization with Rules, Firewalls Evaluation and Current Developments

Learning Resources

1. The Ultimate Kali linux Book, Glen D. Singh, Second Edition, 2022, packt Publishing.
2. Ethical Hacking and Penetration Testing Guide, Rafay Baloch, 2025, CRC Press Taylor & Francis Group
3. Ali A. Ghorbani, Network intrusion detection and prevention concepts and techniques, Springer, 2010
4. Brij Gupta, Srivathsan Srinivasagopalan, Handbook of Research on Intrusion Detection Systems, IGI Global, 2020, ISBN: 9781799822431.
5. C. Endorf, E. Schultz and J. Mellander, Intrusion Detection & Prevention, McGraw-Hill/Osborne, 2004
6. Chris Sanders and Jason Smith, Applied Network Security Monitoring: Collection, Detection, and Analysis, Syngress, 2013
7. Rebecca Gurley Bace, Intrusion Detection, Macmillan, 2000.
8. David J. Marchette, Computer Intrusion Detection and Network Monitoring - A Statistical Viewpoint, Springer Verlag, 2001.
9. Richard Bejtlich, Extrusion Detection - Security Monitoring for Internal Intrusions, Addison-Wesley, 2005.
10. Michael E. Whitman, Herbert J. Mattord, and Andrew Green, Guide to Firewalls and VPNs, Third Edition. Course Technology, Cengage Learning, 2012, ISBN-13 978-1-111-13539-3.

L	T	P	C
3	0	2	4

CBM622 Penetration Testing

Pre-requisites

Student should have a passing Grade in CBM 513 (Computer Networks and Security) and CBM522 (Information Security and Applied Cryptography) or the instructor's approval.

Course Objectives

- Introduces the concepts of Penetration testing.
- Gives the students the opportunity to learn about different tools and techniques for penetration testing and security.
- Practically apply penetration testing tools to perform various activities.

Course Outcomes

Students who successfully complete this course will be able to:

- Understand the core concepts related to vulnerabilities and their causes.
- Understand ethics behind hacking and vulnerability disclosure.
- Comprehend the impact of Hacking.
- Exploit the vulnerabilities related to computer system and networks using state of the art tools and technologies.

Syllabus

Introduction and Information Security Overview, Hacking and Ethical hacking concepts, Hacker behaviour & mindset, Hacking Methodology. Methodology. MITRE ATT & CK framework, Cyber Kill Chain.

Reconnaissance and foot printing, Passive reconnaissance, Active reconnaissance Methodology-IP spoofing, DNS spoofing. Active scanning, Enumerating Common services. Network Penetration Testing, Understanding shells, Profiling Target Systems,Network Infrastructure Vulnerabilities, Exploiting Basic Services, Post Exploitation using Meterpreter

Social Engineering attacks and countermeasures, Phishing, Password attacks, Techniques for wordlist Creation, Privilege Escalation. Network Infrastructure Vulnerabilities, IP spoofing, DNS spoofing.

DoS attacks. Web server and application vulnerabilities, SQL injection attacks, DoS attacks. Client-side exploits, privilege escalation.

Metasploit framework, Metasploit Console, Payloads, Metrpreter, Introduction to Armitage.

Learning Resources

1. Baloch, R., Ethical Hacking and Penetration Testing Guide, Auerbach Publications, CRC Press, 2015.

2. David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, Metasploit: The Penetration Tester's Guide, No Starch Press, 2011, ISBN: 159327288X,9781593272883.

3. Sagar Rahalkar, Quick Start Guide to Penetration Testing: With NMAP, OpenVAS and Metasploit, 1st Edition, Apress publications, 2019, Softcover ISBN: 978-1-4842-4269-8.

4. Christopher Hadnagy, Social Engineering: The Science of Human Hacking, 2nd Edition, Wiley Publisher, 2018, ISBN-13: 978-1119433385.

5. Glen D. Singh, Learn Kali Linux 2019: Perform Powerful Penetration Testing Using Kali Linux, Metasploit, Nessus, Nmap, And Wireshark, Packt Publishing, 2019, ISBN: 1789611806.

6. Michael Hixon, Justin Hutchens, Kali Linux. Network Scanning Cookbook, Packt Publishing, 2017, ISBN: 139781787287907

L	T	P	C
2	0	0	2

CBM 623 Information Security Standards, Policies, Strategies & Audits

Pre-requisites

None.

Course Objectives

- Enable a clear understanding and knowledge of Security Analyst foundations.
- Expose students to various IT auditing techniques.
- Understand the significance of Risk Management.

Course Outcomes

- Students who successfully complete this course should have a comprehensive understanding of Information Security Standards, auditing process and Risk Management.

Syllabus

Introduction and IT Audit, IT Environment, Methods for Business Advisory Audits, Role of the IT Audit Team, IT Audit Process, Stages of Auditing.

Auditing Techniques, Auditing Entity-Level Controls, Auditing Cybersecurity Programs, Auditing Data Centers and Disaster Recovery, Auditing Networking Devices, Auditing Web Servers and Web Applications, Auditing Databases, Auditing Storage, Auditing End-User Computing Devices, Auditing Applications, Auditing Company Projects.

Frameworks, Standards, Regulations, and Risk Management, Benefits of Risk Management, Risk Analysis.

Learning Resources

1. Mike Kegerreis, Mike Schiller, Chris Davis, IT Auditing Using Controls to Protect Information Assets, 3rd Edition, Publisher: McGraw-Hill Education, 2019, ISBN-10: 1260453227.
2. Angel R. Otero, Information Technology Control and Audit, 5th Edition, Publisher: Auerbach Publications, 2020, ISBN-10: 1498752284.
3. Martin Weiss, Michael G. Solomon, Auditing IT Infrastructures for Compliance, 2(nd)Edition, Publisher: Jones & Bartlett Learning, 2015, ISBN- 10:1284090701.

4. Stephen D. Gantz, The Basics of IT Audit: Purposes, Processes, and Practical Information, Publisher: Syngress, 2013, ISBN-10: 0124171591.

L	T	P	C
2	0	0	2

CBM624 Legal Aspects of Computing

Pre-requisites

None.

Course Objectives

- Cover various aspects of Cyber law as per Indian/IT act.
- Gives an overview of E-commerce Laws and Consumer Protection laws in Indian IT/Act.
- Determining the impact of Privacy Laws on Information Security.

Course Outcomes

Students who successfully complete this course will be able to:

- Demonstrate an understanding of the Cyber law with respect to Indian IT/Act.
- Comprehend the intricacies of E-commerce Laws and Consumer Protection laws in India.
- Understand the importance and significance of Data Privacy Law.

Syllabus

Introduction and Challenges associated with Cyber Crimes Evolution of the IT Act, IT Act, 2000, Components of Cyber law, Penalties & Offences, amendments.

Case Laws on Cyber Space Jurisdiction and Jurisdiction issues under IT Act, E –commerce and Laws in India and challenges, Digital / Electronic Signature in Indian Laws.

Online payment and Security issues, Consumer Protection Act and E-commerce, E-Record and E-Contracts, Sensitive Personal Data or Information in Cyber Law, Cyber Law an International Perspective.

Learning Resources

1. Sushma Arora, Raman Arora, Cyber Crimes & Laws, 4th Edition 2021, Publisher: Taxmann, ISBN-10: 9390712491
2. N S Nappinai, Technology Laws Decoded, 1st Edition, Publisher: Lexis Nexis, ISBN: 9789350359723
3. Suresh T. Vishwanathan, The Indian Cyber Law, Bharat Law House New Delhi

4. P.M. Bukshi and R.K. Suri, Guide to Cyber and E –Commerce Laws, Bharat Law House, New Delhi

5. Rodney D. Ryder, Guide to Cyber Laws; Wadhwa and Company, Nagpur

6. The Information Technology Act, 2000; Bare Act –Professional Book Publishers, New Delhi

L	T	P	C
1	0	0	1

CBM625 Criminal Psychology and Behaviour Intelligence

Pre-requisites

None.

Course Objectives

- To makes the students familiar with the field of Criminal Psychology.
- To make the students understand the origins of Criminal Behaviour.

Course Outcomes

- Students who successfully complete this course should have a comprehensive understanding of Criminal Behaviour and Psychological aspects of various crimes.

Syllabus

Nature and History of Criminal and Forensic Psychology, Social context of Crime: Extent of Criminality, Changing nature of Crime: Conservative and Radical interpretations in complexity of victimization.

Types of Offenders, Violent Offenders: Media influences and Research Statistics, Theories of Homicide: Psychological Disposition, Socio-Biological theory and Multi-Factorial Approach.

Mental Illness and Crime: Problem of evidence; Mental illness and Crime in general.

Eyewitness Testimony: Accuracy of witness evidence in Court, Witness confidence and improving the validity of line-up, Clinical approaches in Risk and danger assessment.

Learning Resources

1. Dennis Howitt, Introduction to Forensic and Criminal Psychology, 6th Edition, Publisher: Pearson, 2018
2. Wayne Petherick Brent Turvey Claire Ferguson, Forensic Criminology, 1st Edition, Publisher: Elseiver, ISBN: 9780123750716
3. Bruce Arrigo Stacey Shipley, Introduction to Forensic Psychology, 2nd Edition, Publisher: Academic press, ISBN: 9780080468532