APJ Abdul Kalam Technological University

Cluster 6: Ernakulam I

M. Tech Programme in Cyber Security

Scheme of Instruction and Syllabus: 2020 Admissions

APJ Abdul Kalam Technological University
SCHEME AND SYLLABUS FOR M. Tech. DEGREE PROGRAMME in CYBER SECURITY

(Cluster 6: Ernakulam I)

Credit requirement : 68 credits (23+19+14+12)

Normal Duration - Regular: 4 semester **Maximum Duration -** Regular: 6 semester

Courses - Core courses: Either 4 or 3 credits courses**; Elective courses:** All of 3 credits

ALLOTMENT OF CREDITS AND EXAMINATION SCHEME

SEMESTER – I (Credits: 23)

Exam Slot	Course Code	Subjects	L-T-P	Internal Marks	End Semester Exam		Credits
					Marks	Duration (hrs)	
A	06DS 6 0 1 3	Mathematical Foundations For Cyber Security	4-0-0	40	60	3	4
B	06DS 6 0 2 3	Advanced Data Structures and Algorithms	4-0-0	40	60	3	4
C	06DS 6 0 3 3	Operating Systems And Security	4-0-0	40	60	3	4
D	06DS 6 0 4 3	Cryptographic Protocols and Standards	3-0-0	40	60	3	3
E	06DS 6 x 5 3	Elective I	3-0-0	40	60	3	3
F	06DS 6 0 6 3	Research Methodology	0-2-0	100	0	0	2
S	06DS 6 0 7 3	Seminar I	0-0-2	100	0	0	2
U	06DS 6 0 8 3	Information Security Lab	0-0-3	100	0	0	1
							23 Credits

Elective-I	
Course Code	**Subjects**
06DS 6 1 5 3	Mobile Network Security
06DS 6 2 5 3	Information Risk Management
06DS 6 3 5 3	Data Mining and Machine Learning
06DS 6 4 5 3	Data Privacy

SEMESTER – II (Credits: 19)

Exam Slot	Course Code	Subjects	L-T-P	Internal Marks	End Semester Exam		Credits
					Marks	Duration (hrs)	
A	06DS 6 0 1 4	Cyber Forensics	4-0-0	40	60	3	4
B	06DS 6 0 2 4	Secure Coding	3-0-0	40	60	3	3
C	06DS 6 0 3 4	Ethical Hacking	3-0-0	40	60	3	3
D	06DS 6 x 4 4	Elective II	3-0-0	40	60	3	3
E	06DS 6 x 5 4	Elective III	3-0-0	40	60	3	3
F	06DS 6 0 6 4	Mini Project	0-0-4	100			2
U	06DS 6 0 7 4	Ethical Hacking And Digital Forensic Tools Lab	0-0-3	100			1
							19 Credits

Elective-II	
Course Code	**Subjects**
06DS 6 1 4 4	Coding and Information Theory
06DS 6 2 4 4	Design of Secured Architectures

06DS 6 3 4 4	Digital Watermarking
06DS 6 4 4 4	Identity and access Management

Elective-III	
Course Code	**Subjects**
06DS 6 1 5 4	Cryptanalysis
06DS 6 2 5 4	Blockchain Technologies
06DS 6 3 5 4	Storage management and Security
06DS 6 4 5 4	Security Monitoring Services

SEMESTER – III (Credits: 14)

Exam Slot	Course Code	Subjects	L-T-P	Internal Marks	End Semester Exam		Credits
					Marks	Duration (hrs)	
A	06DS 7 x 1 3	Elective IV	3-0-0	40	60	3	3
B	06DS 7 x 2 3	Elective V	3-0-0	40	60	3	3
S	06DS 7 0 3 3	Seminar II	0-0-2	100	0	0	2
F1	06DS 7 0 4 3	Project(Phase I)	0-0-8	50	0	0	6
							14 Credits

Elective-IV	
Course Code	**Subjects**
06DS 7 1 1 3	Cloud Security
06DS 7 2 1 3	Cyber Laws and Security Policies
06DS 7 3 1 3	Disaster Recovery
06DS 7 4 1 3	IT Governance
Elective-V	

Course Code	Subjects
06DS 7 1 2 3	Internet Information and application security
06DS 7 2 2 3	Database Security
06DS 7 3 2 3	Dependable Distributed Systems
06DS 7 4 2 3	IoT Security

SEMESTER – IV (Credits: 12)

Exam Slot	Course Code	Subjects	L-T-P	Internal Marks	End Semester Exam		Credits
					Marks	Duration (hrs)	
F2	06DS 7 0 1 4	Project (Phase 2)	0-0-21	70	30	-	12
							12 Credits

Total:68 Credits

APJ Abdul Kalam Technological University
Master of Technology – Course Plan

SEMESTER I

M. Tech Programme in Cyber Security

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6013	MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY	4-0-0-4	2020

COURSE OBJECTIVES:

1. Introduce basic concepts and knowledge in number theory, together with a wide variety of interesting applications of discrete mathematics.
2. Train students to solve problems from algorithm design and analysis, coding theory etc and to apply techniques of number theory in cryptography.

COURSE OUTCOMES:

1. Understand the ideas of group, ring and an integral domain and be aware of examples of these structures in mathematics.
2. Introduce students to number theoretic problems and to different areas of number theory.
3. Apply coding methods to generate error detection and correction codes.
4. Use the concept of randomness in the domain of cryptography.

SYLLABUS: Number theory, Divisibility, Fundamental theorems of arithmetic, Congruences, Algebraic structures, Coding theory, Stochastic processes, pseudo random number generation.

MODULE	COURSE CONTENT (52 hrs)	HRS
I	ALGEBRAIC STRUCTURES: Groups – Subgroup, Cyclic groups, group homomorphisms, Permutation groups, Cosets, Modulo groups – Primitive roots – Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Rings of polynomials, factorization of polynomials over a field. Fields – Finite fields – GF (pn), GF(2n) - Classification – Structure of finite fields.	12
INTERNAL TEST 1 (Module I)		
II	NUMBER THEORY: Introduction - Divisibility - Greatest common divisor - Prime numbers – Fundamental theorem of arithmetic – Mersenne primes - Fermat numbers - Euclidean algorithm - Fermat's theorem - Euler totient function - Euler's theorem. Congruences: Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem. Modular Arithmetic and Caesar cipher, quadratic residues, Legendre symbol, Jacobi symbol. Gauss's lemma, Quadratic Reciprocity.	16
INTERNAL TEST 2 (Module II)		

III	CODING THEORY: Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes – Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes - Hadamard Code - Goppa codes.	12
IV	Stochastic Process and Pseudo random number generation: Random Variables – discrete and continuous- Central Limit Theorem-Stochastic Process- Markov Chain. Pseudorandom number generation: Introduction and examples - Indistinguishability of Probability Distributions - Next Bit Predictors - The Blum-Blum-Shub Generator – Security of the BBS Generator	12
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, 'An introduction to the theory of numbers', John Wiley and Sons 2004.
2. Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006.
3. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
4. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.
5. Fraleigh J. B., 'A first course in abstract algebra', Narosa, 1990.
6. Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa, 1998.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6023	ADVANCED DATA STRUCTURES AND ALGORITHMS	4-0-0-4	2020

COURSE OBJECTIVES:

1. Familiarize with advanced data structures based on trees and heaps.
2. Learn to choose the appropriate data structure and algorithm design method for a specified application.
3. Study approaches used to analyze and design algorithms and to appreciate the impact of algorithm design in practice.
4. Learn different advanced algorithms in dynamic programming, flow network and computational geometry.

COURSE OUTCOMES:

After completion of the course, the students will be able to

1. Compare different implementations of data structures and to recognize the advantages and disadvantages of the different implementations.
2. Determine which algorithm or data structure to use in different scenarios.
3. Design and analyze the performance of an algorithm.
4. Demonstrate different advanced algorithms in dynamic programming, flow network and computational geometry.

SYLLABUS: Trees, Priority queues, Heaps, Analysis of algorithms, Solving recurrence relations, Dynamic Programming, Flow networks, Computational geometry.

MODULE	COURSE CONTENT (52 hrs)	HRS
I	Trees -Threaded Binary Trees, Selection Trees, Forests and binary search trees, Counting Binary Trees, Red-Black Trees, Splay Trees, Suffix Trees, Digital Search Trees, Tries- Binary Tries-patricia, Multiway Tries.	12
INTERNAL TEST 1 (Module I)		
II	Priority Queues - Single and Double Ended Priority Queues, Leftist Trees, Binomial Heaps, Fibonacci Heaps, Pairing Heaps, Symmetric Min-Max Heaps, Interval Heaps.	12
INTERNAL TEST 2 (Module II)		

III	Analysis of Algorithms-review of algorithmic strategies, asymptotic analysis, solving recurrence relations through Substitution Method, Recursion Tree, and Master Method. Dynamic Programming-Rod cutting-top down and bottom up approach, matrix chain multiplication-recursive solution, Longest common subsequence problem	14
IV	Maximum Flow-Flow Networks, Ford-Fulkerson method-analysis of Ford-Fulkerson, Edmonds-Karp algorithm, Maximum bipartite matching, Betweenness Centrality algorithm Computational Geometry- Line segment properties, Finding the convex hull, Finding the closest pair of points. Implementations using Python.	14
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Ellis Horowitz, SartajSahni, Susan Anderson Freed, Fundamentals of Data Structures in C, Second Edition, University Press, 2008
2. Yedidyah Langsam, Moshe J. Augenstein, Aaron M. Tenenbaum, Data Structures using C and C++, Second Edition, PHI Learning Private Limited, 2010
3. Thomas Cormen, Charles, Ronald Rives, Introduction to algorithm,3rd edition, PHI Learning
4. Ellis Horowitz and SartajSahni, Sanguthevar Rajasekaran, Fundamentals of Computer Algorithms,Universities Press, 2nd Edition, Hyderabad .
5. Sara Baase & Allen Van Gelder , Computer Algorithms – Introduction to Design and Analysis, Pearson Education..
6. Anany Levitin, Introduction to The Design & Analysis of Algorithms, Pearson Education, 2nd Edition, New Delhi, 2008.
7. Berman and Paul, Algorithms, Cenage Learning India Edition, New Delhi, 2008.
8. S.K.Basu , Design Methods And Analysis Of Algorithms ,PHI Learning Private Limited, New Delhi,2008.
9. Jon Kleinberg and Eva Tardos, Algorithm Design, Pearson Education, NewDelhi, 2006.
10. Hari Mohan Pandey, Design Analysis And Algorithms, University Science Press, 2008.
11. R. Panneerselvam, Design and Analysis of Algorithms, PHI Learning Private Limited, New Delhi, 2009.
12. UditAgarwal, Algorithms Design And Analysis, Dhanapat Rai & Co, New Delhi, 2009.
13. Aho, Hopcroft and Ullman, The Design And Analysis of Computer Algorithms, Pearson Education, New Delhi, 2007.
14. S.E.Goodman and S. T. Hedetmiemi, Introduction To The Design And Analysis Of Algorithms, McGraw-Hill International Editions, Singapore 2000.
15. Richard Neapolitan, Kumarss N, Foundations of Algorithms, DC Hearth &company.
16. Sanjay Dasgupta, Christos Papadimitriou, Umesh Vazirani, Algorithms, Tata McGraw-Hill Edition.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6033	OPERATING SYSTEMS AND SECURITY	4-0-0-4	2020

COURSE OBJECTIVES:

1. Introduce students to the field of threats and vulnerabilities in OS and how to provide security in different OS.
2. Focuses on the study of techniques of fundamentals of protection systems, Information flow and Security kernels. This course also deals with a couple of case studies.

COURSE OUTCOMES:

Upon completion, the student will be able to

1. Understand the basic of securing an operating system.
2. Understand the principles of trusted systems, Information flow integrity and securing commercial OS.
3. Understand the security challenges with the help of case studies.

SYLLABUS: Secure OS, Trust and threat models, Access control, Multics, Security goals, Information flow, Security kernels.

MODULE	COURSE CONTENT (52 hrs)	HRS
I	Introduction: Secure OS, Security Goals, Trust Model, Threat Model. Access Control Fundamentals: Protection system, Lampson's Access Matrix, Mandatory protection system. Multics: Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis.	14
	INTERNAL TEST 1 (Module I)	
II	Verifiable security goals: Information flow, information flow secrecy models, information flow integrity model, the challenges of trusted process, covert channels.	12
	INTERNAL TEST 2 (Module II)	
III	Security Kernels: The Security Kernels, secure communications processor, Securing commercial OS: Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX Era- IX, domain and type enforcement	12
IV	Case study - Solaris Trusted extensions: Trusted extensions access control, Solaris compatibility, trusted extension mediations, process rights management, role based access control Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux.	14

END SEMESTER EXAM (All Modules)
REFERENCES: 1. Trent Jaeger, Operating system security, Morgan & Claypool Publishers, 2008 2. Michael Palmer, Guide to Operating system Security Thomson 3. Andrew S Tanenbaum, Modern Operating systems, 3rd Edition 4. Secure Operating Systems. John Mitchell. Multics-Orange Book-Claremont 5. Paxson, Bro: A System for Detecting Network Intruders in Real-Time. Proc. 7th USENIX Security Symposium, San Antonio, TX, January 1998.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06 DS 6043	CRYPTOGRAPHIC PROTOCOLS AND STANDARDS	3-0-0-3	2020

COURSE OBJECTIVES:

- To provide learners with the concepts of symmetric and asymmetric cipher models.
- To enable learners to understand fundamental concepts of authentication.

COURSE OUTCOMES:

At the end of the course, students will be able

- To explain classical encryption techniques.
- To demonstrate encryption techniques and key exchange methods.
- To differentiate between types of cryptosystems.
- To compare various authentication techniques and signature schemes.

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Introduction to concepts of security, Cryptographic goals, Classical encryption techniques: Shift cipher, Substitution cipher,Vigenere cipher, Hill cipher, Permutation cipher, Stream ciphers, LFSR, Cryptanalysis of Vigenere cipher and LFSR.	10
INTERNAL TEST1(Module 1)		
II	Modern Block Ciphers: Block ciphers principles, Shannon's theory of confusion and diffusion, Feistel cipher, Data Encryption Standard, 3- DES, Advanced Encryption Standard and Modes of operation, IDEA.	10
INTERNAL TEST2(Module 2)		
III	Hash Functions and Data Integrity: Classification and framework, Cryptographic hash functions, message authentication code, Hash based MAC, Case study: SHA 256. Introduction to Public Key Cryptography: Integer factorization problem, Discrete logarithm problem.	11
IV	Public key cryptosystems- RSA cryptosystem, Attacks on RSA, Diffie-Hellman Key agreement scheme, ElGamal cryptosystem, Elliptic curve cryptography. Signature schemes: RSA signature, Digital Signature Algorithm, ECDSA. X.509 certification standard.	11
END SEMESTER EXAM(All Modules)		

REFERENCES:

1. William Stallings, Cryptography and Network Security, Pearson Education, 2014.
2. Behrouz A. Forouzan, Cryptography and Network Security, Tata McGraw-Hill. 2010.
3. Charlie Kaufman, Radia Perlman, Mike Speciner, “Network security”, 2nd edition, Pearson India Education Services.
4. Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
5. Abhijith Das and C.E. VeniMadha van, "Public-key Cryptography, Theory and Practice", Pearson Education, 2009.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6153	MOBILE NETWORK SECURITY	3-0-0-3	2020

COURSE OBJECTIVES:

1. Creates Understanding about the basics of wireless technologies and security.
2. Gain in - depth knowledge on wireless and mobile network security and its relation to the new security based protocols
3. Apply proactive and defensive measures to counter potential threats, attacks and intrusions
4. Design secured wireless and mobile networks that optimise accessibility whilst minimising vulnerability to security risks.

COURSE OUTCOMES:

Upon completion, the student will be able to

1. Identify and investigate in-depth both early and contemporary threats to mobile and wireless networks security.
2. Apply proactive and defensive measures to deter and repel potential threats, attacks and intrusions.
3. Develop a clear view of integrated security environments consisting of both similar and diverse wireless access technologies and security architectures.

SYLLABUS: Transmission fundamentals, Wireless network standards, Threats, challenges and attacks, Authentication, Access point based security measures.

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Transmission Fundamentals: Antennas and Wave Propagation. Cellular Wireless networks, Third Generation Systems, 4G Long Term Evolutions, Signal Encoding Techniques, Spread Spectrum, Coding and Error Control, Multiple Access in Wireless Systems	11
INTERNAL TEST 1 (Module I)		
II	Satellite Networks, Wireless System Operations and Standards, Wi-Max an Ultra Wide Band technologies, Mobile IP and Wireless Access Protocol. Wireless LAN Technology, Wi-Fi and IEEE 802.11 Wireless LAN Standard, Blue-tooth and IEEE 802.15 standard.	11
INTERNAL TEST 2 (Module II)		

III	Threats to Wireless networks, ESM, ECM and ECCM, Proliferation of device and technologies, Practical aspects, Wireless availability, Privacy Challenges, Risks: Denial of Service, Insertion Attacks, Interception and monitoring wireless traffic, MIS configuration, Wireless Attacks, Surveillance, War Driving, Client-to-Client Hacking, Rogue Access Points, Jamming and Denial of Service.	10
IV	Authentication, Encryption/Decryption in GSM, Securing the WLAN, WEP Introduction, RC4 Encryption, Data Analysis, IV Collision, Key Extraction, WEP Cracking, WPA/ WPA2, AES, Access Point-Based Security Measures, Third- Party Security Methods, Funk's Steel-Belted Radius, WLAN Protection Enhancements, Blue-tooth Security Implementation, Security in Wi- MAX, UWB security, Satellite network security.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. KavehPahlavan and PrashantKrishnamurthy,"Principles of Wireless Networks", Prentice Hall, 2006.
2. Cyrus Peikari and Seth Fogie, "Maximum Wireless Security" Sams, 2002.
3. Hideki lmai, Mohammad Ghulam Rahman and Kazukuni Kobari "Wireless Communications Security", Universal Personal Communications of Artech House, 2006.
4. Stallings William, "Wireless Communications and Networks" Second Edition, Pearson Education Ltd, 2009.
5. Jon Edney and William A. Arbaugh, " Real 802.11 Security: Wi-Fi Protected Access and 802.11i" , Addison-Wesley Professional, 2003.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6253	INFORMATION RISK MANAGEMENT	3-0-0-3	2020

COURSE OBJECTIVES:

1. To understand the processes and measures that is used to manage risk to business critical information in an increasingly challenging cyber security environment.
2. Examine the way in which business and society make an assessment of, control and transfer risk.
3. To engage students in active discovery of risk management principles.

COURSE OUTCOMES:

Upon completion, the student will be able to

1. Understand the structured process that is used to manage risk to information and data.
2. Realise what a business must, should or could do to address its risks.
3. Recognise the challenges unique to deploying the security measures.

SYLLABUS: Security components, Government models and standards, Risk analysis and management, Security architectures and designs, Business continuity and disaster recovery, Business impact analysis.

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Information Risk Management: Definitions and relationships among different security components - threat agent, threat, vulnerability, risk, asset, exposure and safeguards; Governance models such as COSO and COBIT, ISO 27000 series of standards for setting up security programs.	11
	INTERNAL TEST 1 (Module I)	
II	Risk analysis and management, policies, standards, baselines, guidelines and procedures as applied to Security Management program, Information strategy objectives.	11
	INTERNAL TEST 2 (Module II)	
III	Security awareness and training. Security Architecture and Design: review of architectural frameworks (such as Zachman and SABSA), concepts of Security Models (such as Bell-LaPadula, Biba and Brewer-Nash), vulnerabilities and threats to information systems (such as traditional on-premise systems, web based multi-tiered applications, distributed systems and cloud based services), application of countermeasures to mitigate against those threats and security products evaluation.	10

IV	Business Continuity and Disaster Recovery: Business Continuity Management (BCM) concepts, Business Impact Analysis, BC/ DR Strategy development, backup and offsite facilities and types of drills and tests. An introduction to Operational Security and Physical security aspects.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Alan Calder and Steve G. Watkins, "Information Security Risk Management for IS027001 /IS027002", IT Governance Ltd, 2010.
2. Susan Snedaker, "Business Continuity and Disaster Recovery Planning for IT Professionals", Elsevier Science & Technology Books, 2007.
3. Harold F Tipton and Micki Krause, "Information Security Management Handbook", Volume 1, Sixth Edition, Auerbach Publications, 2003.
4. Andreas Von Grebmer, "Information and IT Risk Management in a Nutshell: A Pragmatic Approach to Information Security" Books on Demand, 2008.
5. Evan Wheeler, " Security Risk Management" ,Elsevier, 2011.
6. Ian Tibble,"Security De-Engineering: Solving the Problems in Information Risk Management", CRC Press, 2012.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6353	DATA MINING AND MACHINE LEARNING	3-0-0-3	2020

COURSE OBJECTIVES:

1. Introduce students to the field of data mining and machine learning process.
2. Focuses on the study of techniques of clustering, classification, association finding, feature selection and visualisation to real world data and determining whether a real world problem has a data mining solution
3. Introduce students to areas where data mining and machine learning can be applied to provide solutions to cyber security problems.

COURSE OUTCOMES:

Upon completion, the student will be able to

1. Understand the basic data mining and machine learning algorithms.
2. Apply supervised and unsupervised learning algorithms to prediction problems.
3. Accurately evaluate the performance of algorithms, as well as formulate and test hypotheses.

SYLLABUS: Introduction to data mining, Machine learning process, Machine learning in misuse/ signature detection, Anomaly detection, Hybrid detection and Network profiling, Data mining for privacy preservation, Intrusion detection.

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Introduction- Cybersecurity, Data Mining, Machine Learning. Classical Machine Learning Paradigms for Data Mining - Fundamentals of Supervised Machine Learning Methods, Popular Unsupervised Machine Learning Methods, Improvements on Machine Learning Methods, Challenges in Data Mining, Challenges in Machine Learning	11
INTERNAL TEST 1 (Module I)		
II	Supervised Learning for Misuse/Signature Detection - Machine Learning Applications in Misuse Detection- Rule-Based Signature Analysis, Artificial Neural Network, Support Vector Machine, Genetic Programming, Decision Tree and CART, Bayesian Network. Machine Learning for Anomaly Detection - Anomaly Detection - Machine Learning in Anomaly Detection Systems	11
INTERNAL TEST 2 (Module II)		

III	Machine Learning for Hybrid Detection - Hybrid Detection, Machine Learning in Hybrid Intrusion Detection Systems, Machine Learning Applications in Hybrid Intrusion Detection - Anomaly-Misuse sequence Detection System, Association Rules in Audit Data Analysis and Mining. Machine Learning for Scan Detection - Scan and Scan Detection, Machine Learning in Scan Detection, Machine-Learning Applications in Scan Detection, Other Scan Techniques	10
IV	Machine Learning for Profiling Network Traffic - Network Traffic Profiling and Related Network Traffic Knowledge, Machine Learning and Network Traffic Profiling, Data Mining and Machine Learning Applications in Network Profiling. Emerging Challenges in Cyber security - Network Monitoring, Profiling, and Privacy Preservation, Challenges in Intrusion Detection.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Sumeet Dua and Xian Du, "Data Mining and Machine Learning in Cyber security" CRC press, Auerbach Publications 2011.
2. Christopher Westphal," Data Mining for Intelligence, Fraud & Criminal Detection: Advanced Analytics & Information Sharing Technologies" CRC Press, 2008.
3. Marcus A. Maloof, "Machine Learning and Data Mining for Computer Security: Methods and Applications" Springer Science & Business Media, 2006.
4. Jesus Mena," Machine Learning Forensics for Law Enforcement, Security, and Intelligence", CRC Press, 2011.
5. Ian H. Witten, Eibe Frank, Mark A. Hall," Data Mining: Practical Machine Learning Tools and Techniques", Elsevier, 2011.
6. Ian Goodfellow, Yoshua Bengio, Aaron Courville, Deep Learning, MIT Press, 2016.
7. Tom M Mitchell, Machine Learning, McGraw Hill, 1997.
8. Jiawei Han, Micheline Kamber, Jian Pei, Data Mining: Concepts and Techniques, 3rd edition, 2011.
9. D. K. Bhattacharyya and J. K. Kalita, Network Anomaly Detection: A Machine Learning Perspective, 1st Edition, Chapman and Hall/CRC, 2013.
10. T. Dunning and E. Friedman, Practical Machine Learning - A New Look at Anomaly Detection, O'Reilly, 1st edition, 2014.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6453	DATA PRIVACY	3-0-0-3	2020

COURSE OBJECTIVES:

1. To create architectural, algorithmic and technological foundations for the maintenance of the privacy of individuals, the confidentiality of organisations, and the protection of sensitive information, despite the requirement that information be released publicly or semi-publicly.

COURSE OUTCOMES:

After successful completion of this course, students will be able to:

1. Understand the concepts of privacy in today's environment.
2. Obtain the understanding of how automation is changing the concepts and expectations concerning privacy and the increasingly interconnected issue of security.
3. Obtain the knowledge of the role of private regulatory and self-help efforts.
4. Have an understanding of how emerging issues are affecting society and business, with a concentration on how information security must shape corporate practices.

SYLLABUS: Fundamentals, Data privacy attacks, Data linking and profiling, Access control models, Mathematical model for data sharing, Protection models, Medical privacy legislations, Privacy in World Wide web.

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Introduction- Fundamental Concepts, Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy in different domains- medical, financial, etc	10
	INTERNAL TEST 1 (Module I)	
II	Data explosion- Statistics and Lack of barriers in Collection and Distribution of Person-specific information. Mathematical model for characterizing and comparing real-world data sharing practices and policies and for computing privacy and risk measurements, Demographics and Uniqueness.	10
	INTERNAL TEST 2 (Module II)	
III	Protection Models- Null-map, k-map, Wrong map Survey of techniques- Protection models (null-map, k-map, wrong map), Disclosure control, Inferring entity identities, Strength and weaknesses of techniques, entry specific databases. Computation systems for protecting delimited data- MinGen, Datafly, Mu-Argus, k-Similar, Protecting textual documents: Scrub.	12

IV	Technology, Policy, Privacy and Freedom- Medical privacy legislation, policies and best practices, Examination of privacy matters specific to the World Wide Web, Protections provided by the Freedom of Information Act or the requirement for search warrants.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. B. Raghunathan, The Complete Book of Data Anonymization: From Planning to Implementation, Auerbach Pub, 2013.
2. L. Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection, MIT Computer Science, 2002.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6063	RESEARCH METHODOLOGY	0-2-0-2	2020

COURSE OBJECTIVES:

1. To prepare the student to do the M. Tech project works with a research bias.
2. To formulate a viable research question.
3. To develop skill in the critical analysis of research articles and reports.
4. To analyze the benefits and drawbacks of different methodologies.
5. To understand how to write a technical paper based on research findings.

COURSE OUTCOMES:

Students should be able to

1. Understand research concepts in terms of identifying the research problem
2. Propose possible solutions based on research
3. Write a technical paper based on the findings
4. Get a good exposure to a domain of interest
5. Get a good domain and experience to pursue future research activities

SYLLABUS: Introduction to Research Methodology - Types of research - Ethical issues - Copy right - royalty - Intellectual property rights and patent law - Copyleft - Open access - Analysis of sample research papers to understand various aspects of research methodology : Defining and formulating the research problem - Literature review - Development of working hypothesis - Research design and methods - Data Collection and analysis - Technical writing - Project work on a simple research problem

MODULE	COURSE CONTENT (28 hrs)	HRS
I	**Introduction to Research Methodology:** Motivation towards research - Types of research: Find examples from literature. **Professional ethics in research** - Ethical issues-ethical committees. Copy right - royalty - Intellectual property rights and patent law - Copy left- Open access -Reproduction of published material - Plagiarism - Citation and acknowledgement. **Impact factor**. Identifying major conferences and important journals in the concerned area. Collection of at least 4 papers in the area.	6
INTERNAL TEST 1 (Module I)		

II	**Defining and formulating the research** problem -Literature Survey- Analyze the chosen papers and understand how the authors have undertaken literature review, identified the research gaps, arrived at their objectives, formulated their problem and developed a hypothesis.	8
INTERNAL TEST 2 (Module II)		
III	**Research design and methods**: Analyze the chosen papers to understand formulation of research methods and analytical and experimental methods used. Study of how different it is from previous works. **Data Collection and analysis.** Analyze the chosen papers and study the methods of data collection used. - Data Processing and Analysis strategies used– Study the tools used for analyzing the data.	7
IV	**Technical writing** - Structure and components, contents of a typical technical paper, difference between abstract and conclusion, layout, illustrations and tables, bibliography, referencing and footnotes-use of tools like Latex. Identification of a simple research problem – Literature survey- Research design- Methodology –paper writing based on a hypothetical result.	7
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. C. R. Kothari, Research Methodology, New Age International, 2004
2. Panneerselvam, Research Methodology, Prentice Hall of India, New Delhi, 2012.
3. J. W. Bames, Statistical Analysis for Engineers and Scientists, Tata McGraw-Hill, New York.
4. Donald Cooper, Business Research Methods, Tata McGraw-Hill, New Delhi.
5. Leedy P. D., Practical Research: Planning and Design, McMillan Publishing Co.
6. Day R. A., How to Write and Publish a Scientific Paper, Cambridge University Press, 1989.
7. Manna, Chakraborti, Values and Ethics in Business Profession, Prentice Hall of India, New
   Delhi, 2012.
8. Sople, Managing Intellectual Property: The Strategic Imperative, Prentice Hall ofIndia, New Delhi, 2012.
9. Vinod Chandra S. S., Anand H. S. Research Methodology, Pearson Education, ISBN: 978-93-528-6351-8, 2017

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6073	SEMINAR-I	0-0-2-2	2020

COURSE OBJECTIVES:

1. To introduce the students to research, make them understand research papers and prepare presentation material
2. To understand cutting edge technology in the chosen area
3. To improve oral communication skills through presentation
4. To prepare original technical write up on the presentation

COURSE OUTCOMES:

After completion of course, students will be able to:

1. Develop skills in doing literature survey, technical presentation and report preparation
2. Improve the proficiency in English
3. Improve presentation skills
4. Improve analytical and reasoning ability
5. Improve technical writing skills

SYLLABUS:

The aim of this course is to introduce the student to research, and to acquaint him with the process of presenting his work through seminars and technical reports. Students have to register for the seminar and select a topic in consultation with any faculty member offering courses for the programme. The student is expected to do an extensive literature survey and analysis in an area related to computer science (other than the area of specialisation). The study should preferably result in design ideas, designs, algorithms, and theoretical contributions in the form of theorems and proofs, new methods of proof, new techniques or heuristics with analytical studies, implementations and analysis of results.

The presentation shall be of 30 minutes duration and a committee with the Head of the Department as the chairman and two faculty members from the department as members shall evaluate the seminar based on the coverage of the topic, presentation and ability to answer the questions put forward by the committee.

Students shall individually prepare and submit a seminar report based on experimental study / industrial training on the corresponding topic, in the prescribed format given by the Department. The reference shall include standard journals (ACM/ IEEE), conference proceedings and equivalent documents, reputed magazines and textbooks, technical reports and web based material, approved by the supervisor. The references shall be incorporated in the report following IEEE standards reflecting the state-of-the-art in the topic selected.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6083	INFORMATION SECURITY LAB	0-0-3-1	2020

COURSE OBJECTIVES:

1. The main objective of this practical session is that students will get the exposure to various tools and programming methods using in information security.

COURSE OUTCOMES:

By the completion of this laboratory session student

1. Will gain the knowledge on perl and Shell scripting languages to implement various security attacks.
2. Will get the ideas in various ways to trace an attacker.
3. Will get the practical exposure to software firewall, port monitoring

SYLLABUS:

Transmission, functions and security attacks implementation with Perl and shell scripting, Cryptographic algorithms and security protocols in C/C++, Firewall, Port monitoring.

The following programs should be implemented preferably on platform Windows/ Linux through perl, shell scripting language and other standard utilities available with LINUX systems.

Sl No	List of Experiments
1	Write a perl script to concatenate ten messages and transmit to remote server a. Using arrays b. Without using arrays.
2	Write a perl script to implement following functions: a. Stack functions b. File functions c. File text functions d. Directory functions e. Shift, unshift, Splice functions.
3	Write a Perl script to secure windows operating systems and web browser by disabling Hardware and software units.
4	Write a perl script to implement Mail bombing and trace the hacker.
5	Write a shell script to crack LINUX login passwords and trace it when breaking is happened.
6	Working with Sniffers for monitoring network communication (Ethereal)

7	Understanding of cryptographic algorithms and implementation of the same in C or C++.
8	Using open SSL for web server - browser communication
9	Using GNU PGP
10	Performance evaluation of various cryptographic algorithms
11	Using IP TABLES on Linux and setting the filtering rule
12	Configuring S/MIME for e-mail communication
13	Understanding the buffer overflow and format string attacks
14	Using NMAP for ports monitoring
15	Implementation of proxy based security protocols in C or C++ with features like confidentiality, integrity and authentication
Twelve experiments to complete mandatory	

REFERENCES:

1. http://linuxcommand.org/man_pages/openssl1.html
2. http://www.openssl.org/docs/apps/openssl.html
3. http://www.queen.clara.net/pgp/art3.html
4. http://www.ccs.ornl.gov/~hongo/main/resources/contrib/gpg-howto/gpghowto.html
5. https://netfiles.uiuc.edu/ehowes/www/gpg/gpg-com-0.htm
6. http://www.ethereal.com/docs/user-guide/

APJ Abdul Kalam Technological University
Master of Technology – Course Plan

SEMESTER II

M. Tech Programme in Cyber Security

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6014	CYBER FORENSICS	4-0-0-4	2020

COURSE OBJECTIVES:

1. The main objective of the course is to introduce the students to bring awareness in crimes and tracing the attackers.
2. Define digital forensics from electronic media.
3. Describe how to prepare for digital evidence investigations and explain the differences between law enforcement agency and corporate investigations.
4. Explain the importance of maintaining professional conduct

COURSE OUTCOMES:

Upon completion, the student will be able to

1. Utilise a systematic approach to computer investigations.
2. Utilise various forensic tools to collect digital evidence.
3. Perform digital forensics analysis upon networks and network devices.
4. Perform web based investigations.

SYLLABUS: Introduction, Computer forensics, Security investigations, Digital evidences, Evidence collection, data seizure, analysis and preservation, Network intrusion and web based investigations, Countermeasures, Cyber forensic tools.

MODULE	COURSE CONTENT (52 hrs)	HRS
I	Cyber forensics Introduction to Cyber forensics, Type of Computer Forensics Technology- Type of Vendor and Computer Forensics Services. Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases, Analyzing Malicious software	14
INTERNAL TEST 1 (Module I)		
II	Digital Evidence in Criminal Investigations. The Analog and Digital World, Training and Education in digital evidence, the digital crime scene, Investigating Cybercrime, Duties Support Functions and Competencies. Computer Forensics Evidence and Capture- Data Recovery-Evidence collection and Data Seizure-Duplication and preservation of Digital Evidence-Computer image verification and Authentication	14
INTERNAL TEST 2 (Module II)		

III	Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks, Router Forensics. Computer Forensics Analysis- Discovery of Electronic Evidence- Identification of data- Reconstructing Past events-networks	12
IV	Countermeasure: Information warfare- Surveillance tool for Information warfare of the future-Advanced Computer Forensics. Cyber forensics tools and case studies.	12
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Understanding Cryptography: A Textbook for Students and Practitioners: Christofpaar, Jan Pelzl.
2. Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts Ali Jahangiri
3. Handbook of Digital and Multimedia Forensic Evidence [Paperback] John J. Barbara
4. Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press Series: Computer Forensics)
5. Cyber Forensics: Understanding Information Security Investigations (Springer's Forensic Laboratory Science Series) by Jennifer Bayuk
6. Information warfare : Information warfare and security: (ACM Press) by Dorothy Elizabeth Robling Denning
7. Cyberwar and Information Warfare : Springer's by Daniel Ventre
8. Computer forensics: computer crime scene investigation, Volume 1 (Charles River Media, 2008) By John R. Vacca

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6024	SECURE CODING	3-0-0-3	2020

COURSE OBJECTIVES:

1. Students shall understand vulnerabilities in coding, identify, and remediate them.

COURSE OUTCOMES:

Upon completion, the student will be able

1. To utilise a systematic approach to secure coding and web applications.

SYLLABUS: Security architecture, Secure coding with strings, pointers etc. in C/C++, Dynamic memory management, Formatted outputs, Web related vulnerabilities, Hidden form fields.

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Introduction, Security concepts, Security Architecture - Principles, coding in C and C++, Strings - String Characteristics, Common String Manipulation Errors, String Vulnerabilities, Process Memory Organization, Stack Smashing, Code Injection, Arc Injection, Notable Vulnerabilities. Pointer Subterfuge - Data Locations, Function Pointers, Data Pointers, Modifying the Instruction Pointer, Global Offset Table, The .dtors Section , Virtual Pointers, The atexit() and on_exit() Functions, Thelongjmp() Function, Exception Handling.	11
INTERNAL TEST 1 (Module I)		
II	Dynamic Memory Management - Common Dynamic Memory Management Errors, Doug Lea's Memory Allocator, RtlHeap, Integer Security - Integers, Integer Conversions, Integer Error Conditions, Integer Operations, Vulnerabilities, Non-exceptional Integer Logic Errors, Notable Vulnerabilities in Dynamic Memory Management and Integer Security.	11
INTERNAL TEST 2 (Module II)		
III	Formatted Output - Variadic Functions, Formatted Output Functions, Exploiting Formatted Output Functions, Stack Randomization. File I/O - Concurrency, Time of Check, Time of Use, Files as Locks and File Locking, File System Exploits.	10

IV	Web Application, SQL Injection, Web Server–Related Vulnerabilities (XSS, XSRF, and Response Splitting), Web Client–Related Vulnerabilities(XSS), Use of Magic URLs, Predictable Cookies, and Hidden Form Fields:- Overview, CWE References, Affected Languages, Spotting the Pattern, Code Review, Testing Techniques, Redemption Steps.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Robert C. Seaford, "Secure Coding in C and C++", Addison-Wesley Professional, 2005.
2. Mark G. Graff, Kenneth R. van Wyk, "Secure Coding: Principles & Practices" O'Reilly, 2003
3. Michael Howard, David LeBlanc, and John Viega, "24 DEADLY SINS OF SOFTWARE SECURITY" McGraw-Hill Companies, 2010.
4. James A. Whittaker and Herbert H. Thompson, "How to Break Software Security",
5. Addison Wesley, 2003. John C. Mitchell and Krzysztof Apt, "Concepts in Programming Languages", Cambridge University Press, 2001.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6034	ETHICAL HACKING	3-0-0-3	2020

COURSE OBJECTIVES:

1. To understand steps in ethical hacking.
2. To render all the techniques used for penetration testing for performing security auditing.
3. To transform the internet security industry by infusing professionalism and efficiency.

COURSE OUTCOMES:

By the end of the course students will

1. Learn various hacking methods.
2. Perform system security vulnerability testing.
3. Perform system vulnerability exploit attacks.
4. Produce a security assessment report
5. Learn various issues related to hacking.

SYLLABUS: Introduction to hacking, hacking methods, footprinting, enumeration, Securing files and folders, Voice mail and VPN hacking, Network devices, Wireless hacking, Firewalls, DoS attacks, Remote Control Insecurities

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Introduction, Casing the establishment- What is footprinting- Internet Footprinting. - Scanning-Enumeration - basic banner grabbing, Enumerating Common Network services. Case study-Network security monitoring securing permission. Securing file and folder permission using the encrypting file system.	11
INTERNAL TEST 1 (Module I)		
II	Dial-up ,PBX, Voicemail, and VPN hacking - Preparing to dial up. War- Dialing. Brute-Force Scripting. Voice mail hacking . VPN hacking. Network Devices – Discovery, Autonomous System Lookup. Public Newsgroups. Service Detection. Network Vulnerability. Detecting Layer 2 Media.	10
INTERNAL TEST 2 (Module II)		

III	Wireless Hacking - Wireless Foot printing. Wireless Scanning and Enumeration. Gaining Access. Tools that exploiting WEP Weakness. Denial of Services Attacks. Firewalls- Firewalls landscape- Firewall Identification-Scanning Through firewalls- packet Filtering- Application Proxy Vulnerabilities . Denial of Service Attacks - Motivation of Dos Attackers. Types of DoS attacks. Generic Dos Attacks. Unix and Windows DoS	11
IV	Remote Control Insecurities - Discovering Remote Control Software. Connection. Weakness. VNC . Microsoft Terminal Server and Citrix ICA .Advanced Techniques Session Hijacking. Back Doors. Trojans. Cryptography . Subverting the systems Environment. Social Engineering. Web Hacking. Web server hacking web application hacking. Hacking the internet User - Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global Counter measures to Internet User Hacking.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security
Secrets & Solutions”, Tata Mcgrawhill Publishers, 2010.
2. Bensmith, and Brian Komer, “Microsoft Windows Security Resource Kit”, Prentice Hall of India, 2010.
3. Michael T. Simpson, “Ethical Hacking and Network Defense”, Cengage Learning, New Delhi, 2012.
4. Kevin Beaver, “Hacking for Dummies”, Wiley Publication, India, 2007.
5. Ankit Fadia, “Unofficial Guide to Ethical Hacking”, Macmillan Company, New Delhi, 2001.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6144	CODING AND INFORMATION THEORY	3-0-0-3	2020

COURSE OBJECTIVES:

1. Covers information theory and coding within the context of modern digital communications applications.
2. To help students in quantify the notion of information in a mathematically and intuitively sound way.
3. Explaining how this quantitative measure of information may be used in order to build efficient solutions to multitudinous engineering problems

COURSE OUTCOMES:

By the end of the course students will

1. Learn various coding methods.
2. Learn various error control methods.

SYLLABUS:

Source coding, Information theory, Coding methods, Channel capacity and coding, Error control coding, Cyclic codes, Convolutional codes, Modulation.

MODULE	COURSE CONTENT (42hrs)	HRS
I	Source Coding - Introduction to information theory, uncertainty and information, average mutual information and entropy, source coding theorem, Shannon-fano coding, Huffman coding, Arithmetic coding, Lempel-Ziv algorithm, run-length encoding and rate distortion function.	11
INTERNAL TEST 1 (Module I)		
II	Channel capacity and coding - channel models, channel capacity, channel coding, information capacity theorem, random selection of codes. Error control coding: linear block codes and their properties, decoding of linear block code, perfect codes, hamming codes, optimal linear codes and MDScodes.	11
INTERNAL TEST 2 (Module II)		

III	Cyclic codes - polynomials, division algorithm for polynomials, a method for generating cyclic codes, matrix description of cyclic codes, burst error correction, fire codes, golay codes, CRC codes, circuit implementation of cyclic codes. BCH codes: minimal polynomials, generator polynomial for BCH codes, decoding of BCH codes, Reed-Solomon codes and nested codes.	10
IV	Convolutional codes - tree codes and trellis codes, polynomial description of convolutional codes, distance notions for convolutional codes, generation function, matrix description of convolutional codes, Viterbi decoding of convolutional codes, distance bounds for convolutional codes, turbo codes and turbo decoding. Trellis Coded Modulation - concept ofcoded modulation, mapping by set partitioning, ungerboeck's TCM design rules, TCM decoder, Performance evaluation for Additive White Gaussian Noise (AWGN) channel, TCM for fading channels.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Lin S. and D. J. Costello, "Error Control Coding — Fundamentals and Applications", Second Edition, Pearson Education Inc., NJ., USA, 2004
2. Shu Lin and Daniel J. Costello, "Error Control Coding", Second Edition, Prentice Hall, 1983.
3. E. R. Berlekamp, "Algebraic Coding Theory", McGraw-Hill, New York, 1968.
4. R. E. Blahut, "Algebraic Codes for Data Transmission", Cambridge University Press Cambridge, UK, 2003.
5. Ranjan Bose, "Information theory, coding and cryptography", Tata McGraw Hill, 2002.
6. Viterbi, "Information theory and coding", McGraw Hill, 1982.
7. John G. Proakis, "Digital Communications", 2nd Edition, McGraw Hill, 1989.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6244	DESIGN OF SECURED ARCHITECTURES	3-0-0-3	2020

COURSE OBJECTIVES:

1. Students shall gain an understanding of the techniques and architectural components used to provide a secure computing environment.

COURSE OUTCOMES:

Upon completion, the student will be able

1. To know the strengths and weaknesses of different security design techniques.
2. To specify a security solution to fulfill specific design requirements.

SYLLABUS: Security architecture overview, Software process and architecture models, Architecture review, Low level architecture, Buffer overflow attacks, Mid-level architecture, High level architecture, Enterprise security architecture, Tools for data management.

MODULE	COURSE CONTENT (42hrs)	HRS
I	Architecture and Security - Architecture Reviews-Software Process-Reviews and the Software Development Cycle-Software Process and Architecture Models-Software Process and Security-Architecture Review of System-Security Assessments-Security Architecture Basics- Architecture Patterns in Security.	11
INTERNAL TEST 1 (Module I)		
II	Low-Level Architecture - Code Review-importance of code review- Buffer Overflow Exploits- Counter measures against Buffer Overflow Attacks patterns applicable- Security and Perl-Byte code Verification in Java- Good Coding Practices Lead to Secure Code- Cryptography- Trusted Code - Secure Communications	11
INTERNAL TEST 2 (Module II)		

III	Mid-Level Architecture - Middleware Security- Middleware and Security-The Assumption of Infallibility. High-Level Architecture – Security Components-Secure Single Sign-On-Public-Key Infrastructures- Firewalls- Intrusion Detection Systems-LDAP and X.500 Directories-Kerberos- Distributed Computing Environment-The Secure Shell, or SSH The Distributed Sandbox- Security and Other Architectural Goals-Metrics for Non-Functional Goals-Force Diagrams around Security- High Availability- Robustness- Reconstruction of Events- Ease of Use- Maintainability, Adaptability, and Evolution- Scalability- Interoperability- Performance- Portability.	10
IV	Enterprise Security Architecture - Security as a Process-Security Data- Enterprise Security as a Data Management Problem- Tools for Data Management- David Isenberg and the "Stupid Network"-Extensible Markup Language- The XML Security Services Signaling Layer-XML and Security Standards- The Security Pattern Catalog Revisited-XML-Enabled Security Data-HGP: A Case Study in Data Management. Business Cases and Security: Building Business Cases for Security	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Jay Ramachandran, "Designing Security Architecture Solutions", Wiley Computer Publishing, 2010.
2. Markus Schumacher, "Security Patterns: Integrating Security and Systems Engineering", Wiley Software Pattern Series, 2010.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6344	DIGITAL WATERMARKING	3-0-0-3	2020

COURSE OBJECTIVES:

1. To make the students aware of the basic mathematical concept behind watermarking theory and its main applications.
2. Provides the knowledge about the applications of watermarking techniques used and teaches about Watermark security and cryptographic methods used.

COURSE OUTCOMES:

Upon completion, the Students will be able to

1. Understand and identify digital watermarking from other related fields.
2. Explain different types of watermarking applications and watermarking frameworks.
3. Design digital watermarking systems according to application domains.
4. Analyze the different type of watermarking security issues.

SYLLABUS:

Watermarking signals, Models of watermarking, Basic message coding, Detecting multi-symbol watermarks, Watermarking with side information, Information embedding, Information coding, Analyzing errors, Analysis of normalized correlation, Using perceptual mode, Perceptual models, Watermark security and cryptography.

MODULE	COURSE CONTENT (42hrs)	HRS
I	Watermarking host signals: Image, Video, and Audio. Multimedia compression and decompression, Lossless compression, Models watermarking, Communication-based models of watermarking, Geometric models of watermarking, modeling watermark detection by correlation	11
	INTERNAL TEST 1 (Module I)	
II	Basic message coding, Mapping message in message vectors, Error correction coding, Detecting multi-symbol watermarks, Watermarking with side information, Information embedding, Informed coding.	11
	INTERNAL TEST 2 (Module II)	
III	Structured dirty-paper codes, Analyzing errors, Message errors, ROC curves, The effect of whitening on error rates, Analysis of normalized correlation, Using perceptual mode, Evaluating perceptual impact of watermarks.	10

IV	General forms of perceptual model, Perceptual adaptive watermarking, Robust watermarking, Watermark security, Watermark security and cryptography, Content authentication, Exact authentication, Selective, authentication, Localization, Restoration.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Cox I., M. Miller, J. Bloom, J. Fridrich and T Kalker, "Digit Watermarking and Steganography", Second Edition, Morg Kaufmann Publishers, 2008.
2. E. Cole, R. Krutz, and J. Conley, Network Security Bible, Wiley-Dreamtech, 2005.
3. W. Stallings, Cryptography and Network Security Principles and practice, 3/e, Pearson Education Asia, 2003.
4. C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 3/e, Pearson Education, 2003.
5. M. Bishop, Computer Security: Art and Science, Pearson Education, 2003.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6444	IDENTITY AND ACCESS MANAGEMENT	3-0-0-3	2020

COURSE OBJECTIVES:

1. To provide basics of Identity and Access Management and its concepts
2. Understand multi-factor Authentication to configure strong authentication for users at sign-in.
3. To Manage and secure web applications with OAuth 2.0.

COURSE OUTCOMES:

Students should be able to

1. Understand the semantics and principles behind terms and concepts in Identity & Access Management
2. Understand the players and building blocks of Identity Management frameworks
3. Identify different components of IAM in a given implementation.
4. Implement secure networking solutions using OAuth 2.0.

SYLLABUS: IAM overview, Framework, Implementation methodology, Life cycle for Identity and access, IAM data management, RBAC model, Authentication method, Strong authentication, Implementing identity management, Authorization, OAuth 2.0.

MODULE	COURSE CONTENT (42hrs)	HRS
I	Introduction to IAM, Types of business cases for IAM, IAM Framework, IAM Capability maturity framework, Differences from traditional IT.	3
	Implementation Methodology and Approach - Plan and Diagnose, Define and Design, Develop and Deliver, Adopt and Sustain, IAM Implementation Toolkit, Life cycle for Identity and Access - Request, Approve, Create, Grant, Delete, Revoke, Request system, Workflow system, Provisioning system, HR system, IAM Data Management.	6
INTERNAL TEST 1 (Module I)		

II	Identity and Access Intelligence - Risk based approach to IAM, Roles and Rules - RBAC Key concepts, Rules and enforcement, RBAC Model and Access management, RBAC implementation considerations. Authentication methods - Cloud IAM identities, B2C and B2E, MFA, Passwords and API keys, Shared IDs, Federated identity, Instance Metadata, Identity documents, Secrets management, LDAP - basics, LDIF, LDAP security, LSC, SAML - assertions, protocols, bindings, profiles, OAuth - roles, tokens, grants, Overview of OpenID and connection chains.	3 8
INTERNAL TEST 2 (Module II)		
III	Strong authentication - OTPs, HOTP, TOTP, Mutual SSL/TLS, FIDO, User managed access - UMA Grant, Federated authorization. Implementing identity management - SSO, Credential management systems, Integrating identify services, Managing sessions, AAA protocols.	5 5
IV	Need of OAuth 2.0, Roles, Authorisation flow, Tokens, Clients and endpoints, Security considerations, Additional security with SAML. Case study : OAuth 2.0 for web server applications, Client side applications, Mobile applications.	12
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Ertem Osmanoglu, “Identity and Access Management: Business Performance Through Connected Intelligence”, Elsevier Syngress 2014
2. Mike Chapple, James Michael Stewart, Darril Gibson, “(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide”, Wiley Sybex, 2018
3. Chris Dotson, “Practical Cloud Security: A Guide for Secure Design and Deployment”, O’Reilly 2019
4. Michael Schwartz, Maciej Machulak, “Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software”, APress, 2018
5. Steve Martinelli, Henry Nash, Brad Topol, “Identity, Authentication, and Access Management in OpenStack”, O’Reilly, 2016
6. Martin Spasovski, “OAuth 2.0 Identity and Access Management Patterns”, Packt Publishing.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6154	CRYPTANALYSIS	3-0-0-3	2020

COURSE OBJECTIVES:

1. To enable learner to understand various risks, threats and vulnerabilities in a system.
2. Also gives security awareness and countermeasures to mitigate various risks, threats and vulnerabilities in a system.

COURSE OUTCOMES:

1. Students will be able to design and analyse the security architecture designed for any system.
2. Students will be able to identify the security flows in any multi-tiered applications, distributed systems and cloud based services and mitigate it.

SYLLABUS: Classical ciphers, Linear Shift Register Random Bit generator, ORYX-Cryptanalysis, Block ciphers, Algorithmic number theory, Algorithms for DLP, Index calculus for DLP algorithms, Lattice based cryptanalysis, Attacks on cryptographic hash functions.

MODULE	COURSE CONTENT (42hrs)	HRS
I	Cryptanalysis of classical ciphers: Vigenere cipher, Affine cipher, Hill cipher, Linear Shift Register Random Bit Generator: Berlekamp- Massey algorithm for the cryptanalysis of LFSR, Correlation attack on LFSR based stream ciphers, Cryptanalysis of ORYX, Fast algebraic attack.	11
	INTERNAL TEST 1 (Module I)	
II	Cryptanalysis of Block Ciphers: Man in the middle attack double DES, Linear and Differential cryptanalysis. Algorithmic Number Theory: Stein's binary greatest common divisor algorithm, Shanks Tonelli algorithm for square roots in Fp, Stein's greatest common divisor algorithm for polynomials.	11
	INTERNAL TEST 2 (Module II)	
III	Algorithms for DLP: Pollard Rho method for DLP, Shank's baby step Giant step algorithm for DLP Silver-Pohling-Hellman algorithm for DLP, Index calculus for DLP algorithms: Trial division, Fermat method, Legendre-congruence, Continued fraction method, Pollard Rho method, Elliptic curve method, Quadratic sieve.	10

IV	Lattice based Cryptanalysis. Direct attacks using lattice reduction, Coppersmith's attacks. Attacks on cryptographic hash functions: Birth day paradox, Birthday for paradox for multi collisions, Birthday paradox in two groups, Application of Birthday paradox in Hash functions, Multicollisions attack on hash functions.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Antoine Joux, "Algorithmic Cryptanalysis", Chapman & Hall/CRC Cryptography and Series, 2009.
2. Song Y Yang, "Number Theory for Computing", Second Edition,SpringerVerlag, 2010.
3. Gregory V. Bard, "Algebraic Cryptanalysis", Springer, 2009.
4. Hoffstein, Jeffray, Pipher, Jill and Silverman, "An Introduction to Mathematical Cryptography",Springer, 2010.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6254	BLOCKCHAIN TECHNOLOGIES	3-0-0-3	2020

COURSE OBJECTIVES:

1. Understand blockchain as the underlying technology of cryptocurrency.
2. Identify the role of decentralization in maintaining security.
3. Identify areas of application for conventional cryptographic algorithms in the blockchain ecosystem.

COURSE OUTCOMES:

Students will be able to

1. Understand emerging abstract models for Blockchain Technology.
2. Familiarize the functional and operational aspects of cryptocurrency ecosystem.
3. Identify major research challenges in cryptocurrency domain.

SYLLABUS: Consensus problem, Distributed consensus, Nakamoto consensus, PoW, PoS, PoB, Cryptocurrencies, Bitcoins, Technologies in blockchain, Mining, ethereum, Smart contracts.

MODULE	COURSE CONTENT (42hrs)	HRS
I	Distributed Databases- Two general problem- Byzantine General problem and Fault Tolerance, The consensus problem - Asynchronous Byzantine Agreement - AAP protocol and its analysis. Distributed Consensus: Nakamoto consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy utilization and alternate. Technologies Borrowed in Blockchain – hash pointers, consensus, byzantine fault-tolerant distributed computing, digital cash etc.	12
INTERNAL TEST 1 (Module I)		
II	Cryptographic basics for cryptocurrency - a short overview of Hashing, signature schemes, encryption schemes and elliptic curve cryptography. Zero Knowledge proofs and protocols in Blockchain - Succinct non interactive argument for Knowledge (SNARK) - pairing on Elliptic curves.	10
INTERNAL TEST 2 (Module II)		

III	Bitcoin and Blockchain History, Bitcoin Mechanics and Optimizations: A Technical Overview, Bitcoin IRL: Wallets, Mining - Blocks - Merkley Tree - hardness of mining - transaction verifiability - anonymity - forks - double spending - mathematical analysis of properties of Bitcoin. Private and Public blockchain. Game Theory and Network Attacks: How to Destroy Bitcoin.	10
IV	Ethereum and Smart Contracts: Enabling a Decentralized Future - Ethereum Virtual Machine (EVM) - Wallets for Ethereum - Solidity - Smart Contracts - Some attacks on smart contracts. Scaling Blockchain: Cryptocurrencies for the Masses, Enterprise Blockchain: Real-World Applications, Anonymity: Mixing and Altcoins, Future of Blockchains.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, 2016.
2. Andreas Antonopoulos, "Mastering Bitcoin", O'Reilly
3. Joseph Bonneau et al, SoK: Research perspectives and challenges for Bitcoin and cryptocurrency, IEEE Symposium on security and Privacy, 2015
4. J.A.Garay et al, The bitcoin backbone protocol - analysis and applications EUROCRYPT 2015 LNCS VOl 9057
5. R.Pass et al, Analysis of Blockchain protocol in Asynchronous networks , EUROCRYPT 2017
6. R.Pass et al, Fruitchain, a fair blockchain, PODC 2017.
7. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6354	STORAGE MANAGEMENT AND SECURITY	3-0-0-3	2020

COURSE OBJECTIVES:

1. To enable students to understand, explore and acquire a critical understanding about managing information in storage system and effective security implementation on the corresponding platforms.

COURSE OUTCOMES:

1. Introduce the students to various types of storage systems available and understand the importance of storage networking.
2. To explain the basic information storage and retrieval concepts in a storage system.
3. To understand the issues those are specific to efficient information retrieval.
4. To implement security issues while storing and retrieving information.

SYLLABUS:

Storage systems, Storage networking, Storage industry organizations, Components, Data organization, Error management, Large storage systems, Securing storage infrastructure, framework, managing and monitoring storage infrastructure.

MODULE	COURSE CONTENT (42hrs)	HRS
I	Introduction, History: computing, networking, storage, Need for storage networking, SAN,NAS,SAN/NAS Convergence, Distributed Storage Systems, Mainframe/proprietary vs. open storage, Storage Industry Organizations and Major Vendors Market, Storage networking strategy (SAN/NAS) Technology	11
INTERNAL TEST 1 (Module I)		
II	Storage components, Data organization: File vs. Block, Object; Data store; Searchable models; Storage Devices (including fixed content storage devices), File Systems, Volume Managers, RAID systems, Caches, Prefetching. Error management: Disk Error Management, RAID Error Management, Distributed Systems Error Management	11
INTERNAL TEST 2 (Module II)		

III	Large Storage Systems: Google FS/Big Table, Cloud/Web - based systems (Amazon S3), FS+DB convergence, Programming models: Hadoop. Archival Systems: Content addressable storage, Backup: server less, LAN free, LAN Replication issues, Storage Security, Storage Management, Device Management, NAS Management, Virtualization, Virtualization solutions, SAN Management: Storage Provisioning, Storage Migration	10
IV	Securing the storage Infrastructure, Storage Security Framework, Risk Triad, Storage Security Domains, Security Implementation in Storage Networking. Managing the Storage Infrastructure, Monitoring the Storage Infrastructure, Storage Management Activities, Developing an Ideal Solution, Concepts in Practice.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. EMC Education Services “Information Storage and Management: Storing, Managing, and Protecting Digital Information” , John Wiley & Sons, 2010.
2. John Chirillo, ScottBlaul“ Storage Security: Protecting SANs, NAS and DAS”, Wiley, 2003.
3. David Alexander, Amanda French, Dave Sutton “Information Security Management Principles” BCS, The Chartered Institute, 2008.
4. Gerald J. Kowalski, Mark T. Maybury“ Information Storage and Retrieval Systems: Theory and Implementation, Springer, 2000.
5. Foster Stockwell , “A history of information storage and retrieval” McFarland, 2001.
6. R. Kelly Rainer, Casey G. Cegielski , “Introduction to Information Systems: Enabling and Transforming Business, John Wiley & Sons, 2010.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6454	SECURITY MONITORING SERVICES	3-0-0-3	2020

COURSE OBJECTIVES:

1. Understand the key techniques and principles of Security Monitoring
2. Understand Essential Components of a defensible network security architecture and SOC
3. Identify Endpoint systems with detective capabilities and resilient to attack.
4. Assess vulnerability of systems using active and passive methods.

COURSE OUTCOMES:

Students will be able to

1. Understand different threat models in networks.
2. Apply security analysis mechanisms to collect and analyse data about threats.
3. Understand methods to secure virtualised systems.
4. Analyse network vulnerability using passive and active methods.
5. Understand methods to identify and mitigate threats.

SYLLABUS: Security Operation Centres, Security Architectures, Risk management, Prevetive and reactive measures, Data collection and analysis in SOC, Security event generation, SOC capabilities assessment, Threats to virtualised environment, SOC Infrastructure, Security technologies, Vulnerability assessment, Security hardening.

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Security Operations Centers and Security Architecture, Network Security Architecture, Network Security Monitoring, Endpoint Security Architecture, Audit Security Operations and SOC - Information assurance, Risk management, Information Security Incident Response. Network Security Axioms, Threats - attack process, attacker types, vulnerability types, attack results, attack taxonomy. Guarding against Network Intrusions - Reconnaissance and Attacks, Malicious software, Intrusion monitoring and detection, Preventive and Reactive measures, Network based intrusion protection. Automation and Continuous Security Monitoring	5 5
INTERNAL TEST 1 (Module I)		

II	Data collection and Analysis in SOC - syslog protocol, telemetry data, Vulnerability management, OWASP Risk Rating Methodology, Threat intelligence, Attack signatures. Security Event Generation and Collection - Calculating EPS, Ubuntu Syslog server, Network Time Protocol, Logging - Apache logs, Database logs, Antivirus and HIDS logs, Network device logs, Netflow. Endpoint Security Architecture - Defining endpoints, Endpoints and network integration, Cast Study: Microsoft Windows.	7 4
INTERNAL TEST 2 (Module II)		
III	Assessing SOC capabilities - Identify business and IT goals, Assessing capabilities, Collect information, Analyse maturity levels, Formalize findings. Threats to virtualised environment, Hypervisor configuration and security, Virtual network security considerations, Cloud VM Reconnaissance, Virtual Disk manipulation, VM Encryption, Case Study of VMware ESXi - configuration, vSphere, vCenter.	4 6
IV	SOC Infrastructure - Internal layout, Active infrastructure. Security Technologies - Identity technologies, Host and Application security, Network firewalls, Content filtering, Network Intrusion Detection systems, Cryptography, Hybrid Host solutions, Application firewalls. Vulnerability assessment, Information gathering - Reverse IP lookup, site metadata, Enumerating services - HTTP, SMTP, FTP, SMB, DNS, SSH, VNC, nmap scripts, Privilege escalation, Security hardening.	6 5
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Joseph Muniz, Gary McIntyre, Nadhem AlFardan, “Security Operations Center: Building, Operating, and Maintaining your SOC”, Cisco Press
2. Chris Fry, Martin Nystrom, “Security Monitoring: Proven Methods for Incident Detection on Enterprise Networks”, O’Reilly 2009
3. Sean Convery, “Network Security Architectures”, Cisco 2004
4. John R. Vacca, “Network and System Security”, Elsevier Syngress, 2014
5. Dave Shackleford, “Virtualization Security: Protecting Virtualized Environments”, John Wiley and Sons, 2013
6. Sagar Rahalkar, “Network Vulnerability Assessment: Identify security loopholes in your network’s infrastructure”, Packt Publishers.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6064	MINI PROJECT	0-0-4-2	2020

COURSE OBJECTIVES:

1. To apply engineering knowledge in practical problem solving
2. To foster innovation in design of products, processes or systems
3. To develop creative thinking in finding viable solutions to engineering problems
4. Design and develop a system or application in the area of their specialisation.

COURSE OUTCOMES:

Student should be able to
1. Identify and solve various problems associated with designing and implementing a intelligent system or application.
2. Test the designed system or application.

Approach

The mini project is designed to develop practical ability and knowledge in tools/ techniques to solve problems related to the industry, academic institutions and computer science research. Students can take up any application level/system level project pertaining to a relevant domain. Projects can be chosen either from the list provided by the faculty or in the field of interest of the student. The topic should be approved by the Programme Co-ordinator / Faculty member before carrying out the work. For external projects, students should obtain prior permission after submitting the details of the guide and synopsis of the work. At the end of each phase, presentation and demonstration of the project should be conducted, which will be evaluated by a panel of examiners. A detailed project report duly approved by the guide in the prescribed format should be submitted for end semester assessment. Marks will be awarded based on the report and their performance during presentations and demonstrations. Students need to do two presentations, first one highlight the topic, objectives, methodology, design and expected results and the second one is the demo of the work done/hardware implementation/ prototype. Publishing the work in Conference Proceedings/Journals with National/ International status with the consent of the guide will carry an additional weightage in the evaluation process.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS6074	ETHICAL HACKING AND DIGITAL FORENSIC TOOLS LAB	0-0-3-1	2020

COURSE OBJECTIVES:

1. The main objective of this practical session is that students will get the exposure to various hacking and forensic tools.

COURSE OUTCOMES:

By the completion of this laboratory session Student

1. Will gain the knowledge to implement various security attacks.
2. Will get the ideas in various ways to trace an attacker.
3. Will get the practical exposure to forensic tools.

SYLLABUS: Ethical hacking- Trojans, backdoors, DoS, Session hijacking, DDoS, Password guessing and cracking. Santhoku Linux operating system , Forensic tools- Helix3pro tool, exiftool , deft_6.1 tool, Courier tool, Ghostnet tool, kgbkey logger etc.

Part A: Ethical hacking

1. Working with Trojans, Backdoors and sniffer for monitoring network communication
2. Denial of Service and Session Hijacking using Tear Drop, DDOS attack.
3. Penetration Testing and justification of penetration testing through risk analysis
4. Password guessing and Password Cracking.
5. Malware – Keylogger, Trojans, Keylogger countermeasures
6. Understanding Data Packet Sniffers
7. Windows Hacking – NT LAN Manager, Secure 1 password recovery
8. Implementing Web Data Extractor and Web site watcher.
9. Email Tracking.
10. Configuring Software and Hardware firewall.
11. Firewalls, Packet Analyzers, Filtering methods.

Part B: Exposure on Digital Forensic tools

1. Backup the images file from RAM using Helix3pro tool and show the analysis.
2. Introduction to Santhoku Linux operating system and features extraction.
3. Using Santoku operating system generates the analysis document for any attacked file from by taking backup image from RAM.
4. Using Santoku operating system generates the attacker injected viewing java files.
5. Using Santoku operating system shows how attackers opened various Firefox URL‟s and
pdf document JavaScript files and show the analysis.
6. Using Santoku operating System files show how an attacker connected to the various network inodes by the specific process.
7. Using exiftool (-k) generate the any picture hardware and software.
8. Using deft_6.1 tool recover the attacker browsing data from any computer.
9. Using Courier tool Extract a hacker secret bitmap image hidden data.
10. Using sg (Stegnography) cyber Forensic tool hide a message in a document or any file.
11. Using sg cyber Forensic tool unhide a message in a document or any file.
12. Using Helix3pro tool show how to extract deleted data file from hard disk or usb device.
13. Using Ghostnet tool hide a message into a picture or any image file.
14. Using kgbkey logger tool record or generate an document what a user working on system
15. Using pinpoint metaviewr tool extract a metadata from system or from image file.
16. Using Bulk Extractor tool extract information from windows file system.

Nine experiments from Part A and Thirteen experiments from Part B need to be complete mandatory

APJ Abdul Kalam Technological University
Master of Technology – Course Plan

SEMESTER III

M. Tech Programme in Cyber Security

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS7113	CLOUD SECURITY	3-0-0-3	2020

COURSE OBJECTIVES:

1. To understand the Security aspects of cloud computing which have always been subjected to many criticisms.
2. Explaining the importance for any security professional to possess an understanding of the cloud architecture and study the methods to secure the same.

COURSE OUTCOMES:

Upon completion, the student will be able to

1. Understand the fundamentals of cloud computing and its architecture.
2. Understand the requirements for an application to be deployed in a cloud.
3. Become knowledgeable in the methods to secure cloud.
4. Analyse the issues and challenges faced to secure information in a cloud.

SYLLABUS:

Cloud computing Fundamentals and Architecture, Cloud architecture models, Deployment models, Cloud software security fundamentals, Design principles, Cloud Risk Issues and Challenges, Virtualization Security management, Cloud Security Architecture

MODULE	COURSE CONTENT (42 hrs)	HRS
I	**Cloud computing Fundamentals and Architecture**:- Essential characteristics, Architectural influences, Technological Influences, Operational influences, Outsourcing legal issues, BPO issues, IT server Management. Cloud architecture model – Cloud delivery model, SPI framework, SaaS, PaaS, IaaS, Deployment models – Public, community, Private, Hybrid Cloud. Alternative deployment models.	11
INTERNAL TEST 1(Module I)		
II	**Cloud software security fundamentals**: – Security objective, security service, Cloud security design principles, Secure cloud software requirements, Secure development practice, Approaches of cloud software requirements engineering, Security policy implementation, Secure cloud software testing, penetration testing, Disaster recovery, Cloud for BCP/DCP.	11
INTERNAL TEST 2 (Module II)		

III	**Cloud Risk Issues and Challenges**:- CIA triad, Privacy and Compliance Risk, PCIDSS, Information privacy and privacy law, Common threats and vulnerabilities, Access control issues, service provider Risk. Security policy Implementation, Computer Security incident response team (CSIRT), Virtualization security Management- virtual threats, VM security recommendations, VM security techniques – hardening, securing VM remote access.	10
IV	**Cloud Security Architecture** :- General issues, Trusted cloud, Secure execution environments and communications, Micro architecture, Identity management, Access control, Autonomic security, protection, self-healing. Cloud life cycle issues – cloud standards, DMTF, ISO, ETSI, OASI, SNIA, OGF, OWASP, Incident response, Internet Engineering Task Force Incident-Handling Guidelines, Computer security and response team, Encryption and key management, VM Architecture, Key Protection, Hardware protection, VM life cycle.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Ronald L. Krutz, Russell Dean Vines, Cloud Security, Wiley publication 2010.
2. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, Inc., 2009.
3. Toby Velte, Anthony Velte, Robert Elsenpeter, Cloud Computing, A Practical Approach, Tata McGraw-Hill Education, 2009.
4. Gautam Shroff, Enterprise Cloud Computing Technology Architecture Applications, Cambridge University Press, 2010.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS7213	CYBER LAWS AND SECURITY POLICIES	3-0-0-3	2020

COURSE OBJECTIVES:

1. To enable learner to understand, explore, and acquire a critical understanding cyber law.
2. Develop competencies for dealing with frauds and deceptions (confidence tricks, cams) and other cyber crimes for example, child pornography etc.

COURSE OUTCOMES:

Learner will be able to

1. Be conversant with the social and Intellectual Property issues emerging from Cyberspace.
2. Explore the legal and Policy developments in various countries to regulate Cyberspace
3. Develop the understanding of relationship between commerce and cyberspace
4. Gain in-depth knowledge of Information Technology Act And legal framework of Right to Privacy, Data Security and Data Protection.

SYLLABUS:

Cyberspace, Cyber Jurisprudence, Civil and criminal jursidictions, IT Act 2000, Digital signatures, Cryptogaphic algorithms, Cyber crimes and offences, Laws, Intellectual property rights, E-commerce-Evolution, development, models

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Emergence of Cyber space. Cyber Jurisprudence, Jurisprudence and law, Doctrinal approach, Consensual approach, Real Approach, Cyber Ethics, Cyber Jurisdiction, Hierarchy of courts, Civil and criminal jurisdictions, Cyberspace-Web space, Web hosting and web Development agreement, Legal and Technological Significance of domain Names, Internet as a tool for global access..	11
INTERNAL TEST 1 (Module I)		
II	Overview of IT Act 2000, Amendments and Limitations of IT Act, Digital Signatures, Cryptographic Algorithm, Public Cryptography, Private Cryptography, Electronic Governance, Legal Recognition of Electronic Records, Legal Recognition of Digital Signature Certifying Authorities, Cyber Crime and Offences, Network Service Providers Liability, Cyber Regulations Appellate Tribunal, Penalties and Adjudication.	11
INTERNAL TEST 2 (Module II)		

III	Patent Law, Trademark Law, Copyright, Software – Copyright or Patented, Domain Names and Copyright disputes, Electronic Data Base and its Protection, IT Act and Civil Procedure Code, IT Act and Criminal Procedural Code, Relevant Sections of Indian Evidence Act, Relevant Sections of Bankers Book Evidence Act, Relevant Sections of Indian Penal Code, Relevant Sections of Reserve Bank of India Act, Law Relating To Employees And Internet, Alternative Dispute Resolution , Online Dispute Resolution (ODR).	10
IV	Evolution and development in E-commerce, paper vs paper less contracts E-Commerce models- B2B, B2C, E security. Application area: Business, taxation, electronic payments, supply chain, EDI, E-markets, Emerging Trends. Case Study On Cyber Crimes: Harassment Via E-Mails, Email Spoofing (Online A Method Of Sending E-Mail Using A False Name Or E-Mail Address To Make It Appear That The E-Mail Comes From Somebody Other Than The True Sender, Cyber Pornography (Exm.MMS),Cyber-Stalking.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. K.Kumar," Cyber Laws: Intellectual property & E Commerce, Security",1st Edition, Dominant Publisher,2011.
2. Rodney D. Ryder, "Guide To Cyber Laws", Second Edition, Wadhwa And Company, New Delhi, 2007.
3. Information Security policy &implementation Issues, NIIT, PHI.
4. Vakul Sharma, "Handbook Of Cyber Laws" Macmillan India Ltd, 2nd Edition, PHI, 2003.
5. Justice Yatindra Singh, "Cyber Laws", Universal Law Publishing, 1st Edition, New Delhi, 2003.
6. Sharma, S.R., "Dimensions Of Cyber Crime", Annual Publications Pvt. Ltd., 1st Edition, 2004.
7. Augastine, Paul T.," Cyber Crimes And Legal Issues", Crecent Publishing Corporation, 2007.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS7313	DISASTER RECOVERY	3-0-0-3	2020

COURSE OBJECTIVES:

1. Understanding of the roles of the various phases of disaster management and issues concerning planning and policies in those phases.
2. Understanding of comprehensive emergency management from a planning and policy Perspective, role of federal, state, and local governments in disaster planning and policies.
3. Knowledge of mitigation planning and policy strategies.
4. Understanding of comprehensive emergency management and related plans.
5. Understanding of the factors that give rise to disaster vulnerabilities (e.g. natural, physical, social, economic, policies, and governance, factors that give rise to differential vulnerabilities and levels of community resilience
6. Data, methods, tools, and geospatial techniques (including GIS) that can enhance vulnerability assessments and knowledge building.

COURSE OUTCOMES:

After completing this course, you will be able to:

1. Affirm the usefulness of integrating management principles in disaster mitigation work
2. Distinguish between the different approaches needed to manage pre- during and post-disaster periods
3. Explain the process of risk management
4. Relate to risk transfer

SYLLABUS:

Introduction, Disaster migration planning and policies, Measuring and mapping vulnerability, Communication and risk management, Disaster response, Disaster Recovery and Rebuilding.

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Introduction: Hazards and Disasters: Planning and Policies, Disaster Mitigation Policies and Planning. Mitigation Planning and Policy Strategies: Local, State, and Federal Level.	11
INTERNAL TEST 1 (Module I)		

II	Measuring and Mapping Vulnerability, Social, Economic, and Political Vulnerabilities, Community Resilience, Emergency Management Planning Communication and Risk Management (Policies and Plans)	11
INTERNAL TEST 2 (Module II)		
III	Disaster Response: Planning for Response, Supporting Emergency Response Operations using Geospatial Technologies Collaboration and Coordination in Emergency Response Planning & Management	10
IV	Disaster Recovery and Rebuilding, Long-term recovery, Post-Disaster Recovery Planning and Reconstruction, Post-Disaster Housing Planning.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Waugh, William L. Jr. (2000). Living with Hazards, Dealing with Disasters: An Introduction to Emergency Management. Armonk, New York: M.E. Sharpe.
2. Burby, Raymond (1998). Cooperating with Nature: Confronting natural hazards with landuse planning for sustainable communities. Joseph Henry Press.
3. Birkland, Thomas. 2006. Lessons of Disaster: Policy Change after Catastrophic Events. Washington,D.C.: Georgetown University Press.
4. Drabek, Thomas. 2010. The Human Side of Disaster. Taylor and Francis

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS7413	IT GOVERNANCE	3-0-0-3	2020

COURSE OBJECTIVES:

1. Definition, establishment, and management of a framework for the governance of enterprise IT in alignment with the mission, vision and values of the enterprise
2. Enterprise objectives through the integration and alignment of IT strategic plans with enterprise strategic plans.
3. Performance measurement are established, evaluated and the reporting of progress to stakeholders
4. IT risk management is in alignment with the enterprise risk management (ERM) framework

COURSE OUTCOMES:

After learning this course, students will be able to

1. Identify the requirements and objectives for the framework for governance of enterprise IT.
2. Understand frameworks like COBIT, ITIL, and COSO for governance.
3. Apply Service Oriented Architectures for proper governance.
4. Understand the concept of KPIs and their application in planning.
5. Apply continuity planning for risk mitigation.

SYLLABUS:

IT governance- Strategies and models, Relevance of IT governance, Frameworks-COBIT, ITIL , COSO, Enterprise Risk Management, Service Oriented Architecture and IT Governance, Key Performance indicators, IT Continuity management.

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Strategies and Models for IT Governance - IT Governance explained, Role of IT Governance, Structures, Processes, and Relational Mechanisms, Process measurement, Implementation Status, Sarbanes - Oxley Rules.	6
	COBIT Framework, Control objectives, Management guidelines, Maturity Models, Adaptation.	4
	INTERNAL TEST 1 (Module I)	
II	Service Oriented Architecture - SOA applications and Service-driven IT applications, SOA Governance, Internal control, Risks, SOA Implementation blueprint, SOA and IT governance, Operation-level agreement, Service-level agreement, Analysis models - SWOT, BCG Matrix.	9

INTERNAL TEST 2 (Module II)		
III	IT Governance and COSO internal controls, ITIL - fundamentals, service strategy components, service design, service translation management, service operation process, best practices. COSO ERM - definitions and objectives, ERM framework, other dimensions. Key Performance Indicators - Four types of performance measures, 10/80/10 Rule, Importance of timely measurement, Relation between Critical Success Factors and KPIs.	8 5
IV	IT Continuity management - Effective IT Security environment, IT continuity planning, Business continuity plan and IT governance. IT Governance in Practice : Case Studies - KBC,AGF Belgium, Huntsman, Sidemar Arcelor.	5 5
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Alan Calder, IT Governance: A Pocket Guide, IT Governance publishing
2. David Clifford, ISO/IEC 20000: An Introduction to the global standard for service management, IT Governance Publishing, 2011.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS7123	INTERNET INFORMATION AND APPLICATION SECURITY	3-0-0-3	2020

COURSE OBJECTIVES:

1. To give exposure to various security threats to web applications/ servers and providing security to web servers.

COURSE OUTCOMES:

By the completion of this course, Student will

1. Understand security concepts, security professional roles, and security resources in the context of systems and security development life cycle
2. Understand the business need for security, threats, attacks, top ten security vulnerabilities, and secure software development
3. Understand information security policies, standards and practices, the information security blueprint.
4. Analyze and describe security requirements for typical web application scenario.

SYLLABUS: Web application security, Web server security, Attacks on web applications and web servers, SQL injection, Mod security.

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Web application security- Key Problem factors – Core defence mechanisms- Handling user access- handling user input- Handling attackers– web spidering – Discovering hidden content. Transmitting data via the client – Hidden form fields – HTTP cookies – URL parameters – Handling client-side data securely – Attacking authentication – design flaws in authentication mechanisms –securing authentication Attacking access controls – Common vulnerabilities – Securing access controls.	11
INTERNAL TEST 1 (Module I)		
II	Web server Hacking - Source code disclosure – Canonicalization attacks –Denial of service – Web application hacking – Web crawling Database Hacking – Database discovery – Database vulnerabilities	10
INTERNAL TEST 2 (Module II)		

III	SQL Injection - How it happens - Dynamic string building – Insecure Database Configuration - finding SQL injection – Exploiting SQL injection – Common techniques – identifying the database – UNION statements – Preventing SQL injection Platform level defenses- Using run time protection - web application Firewalls – Using ModSecurity -Intercepting filters- Web server filters - application filters – securing the database – Locking down the application data – Locking down the Database server	11
IV	Mod Security - Blocking common attacks – HTTP finger printing – Blocking proxies requests – Cross-site scripting – Cross-site request forgeries – Shell command execution attempts – Null byte attacks – Source code revelation – Directory traversal attacks – Blog spam – Website defacement – Brute force attack – Directory indexing – Detecting the real IP address of an attacker.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook, 2nd Edition, Wiley Publishing, Inc.
2. Stuart McClure Joel, Scamb Ray, George Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, Seventh Edition, 2012, The McGraw-Hill Companies
3. Justin Clarke, SQL Injection Attacks and Defense, 2009, Syngress Publication Inc.
4. Magnus Mischel , ModSecurity 2.5, Packt Publishing

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS7223	DATABASE SECURITY	3-0-0-3	2020

COURSE OBJECTIVES:

1. To explore topics related to database security and auditing.
2. The main areas of study is on the key components of information assurance as it relates to database systems – confidentiality, integrity, and availability, and how these components can be managed and measured.

COURSE OUTCOMES:

Upon completion, the student will be able to

1. Identify access control methods for secure database application development
2. Analyze vulnerabilities in the database.
3. Understand common attacks used against database confidentiality and explain how to defend against the attack.
4. Apply security audit methods to database communication and design secure database schema.

SYLLABUS: Database modeling and design, Access control in database, Authentication mechanisms, Password security, Statistical inferences in database, Security in database communication, Auditing strategies.

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Introduction to databases: database modelling, conceptual database design, overview of SQL and relational algebra, Access control mechanisms in general computing systems: Lampson's access control matrix. Mandatory access control.	10
INTERNAL TEST 1 (Module 1)		
II	Authentication mechanisms in databases, DAC in databases: Griffiths and Wade, MAC mechanisms in databases: SeaView. RBAC in databases. Authentication and password security – Weak authentication options, Implementation options, Strong password selection method, Implement account lockout, Password profile.	11
INTERNAL TEST 2 (Module 2)		
III	SQL Injection, Auditing in databases, Statistical inference in databases, Private information retrieval viewed as a database access problem. Privacy in data publishing, Virtual Private Databases, Security of outsourced databases.	10

IV	Securing database to database communication – Monitor and limit outbound communication, Protect link usernames and passwords – Secure replication mechanisms. Trojans- Types of DB Trojans, Monitor for changes to run as privileges, Traces and event monitors. Encrypting data in transit, Encrypt data-at-rest. Database security auditing categories.	11
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Ron Ben Natan, "Implementing Database Security and Auditing", Elsevier, 2005.
2. Hassan A. Afyouni, "Database Security and Auditing: Protecting Data Integrity and Accessibility", Course Technology, 2005.
3. Michael Gertz and SushilJajodia, "Handbook of Database Security-Applications and Trends", Springer, 2008.
4. Database Security, Cengage Learning; 1 edition (July 12, 2011),Alfred Basta . Melissa Zgola.
5. Data warehousing and data mining techniques for cyber security, Springer's By Anoop Singha.
6. Carlos Coronel, Steven A. Morris, Peter Rob, "Database Systems: Design, Implementation, and Management", Cengage Learning, 2011.
7. Vijay Atluri, John Hale, "Research Advances in Database and Information Systems Security", Springer, 2000.
8. Pierangela Samarati, Ravi Sandhu," Database Security X: Status and prospects, Volume 10",Springer, 1997.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS7323	DEPENDABLE DISTRIBUTED SYSTEMS	3-0-0-3	2020

COURSE OBJECTIVES:

1. To explore the state-of-the art principles, methods, and techniques for devising adaptive and dependable distributed systems.
2. Also explains the importance of learning the working of computers in a banking system and creates an awareness of various Biometric systems, their performance and the issues related to the security.

COURSE OUTCOMES:

Upon completion, the student will be able to

1. Understand the Architectural and infrastructural principles for adaptive and dependable distributed systems.
2. Understand the Approaches to improve the scalability of dependable and adaptive systems.
3. Understand about the basic banking systems and the bookkeeping practices followed.
4. Gain a broader knowledge and understand the different Biometric techniques.

SYLLABUS:

Basic concepts of dependability, Fault detection, Fault tolerance, Distributed systems, Security policy models, Security in banking, book keeping, Biometrics, Telecom security.

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Dependability concepts - Faults and Failures – Redundancy – Reliability – Availability – Safety – Security – Timeliness - Fault-classification – Fault detection and location - Fault containment - Byzantine failures – Fault injection - Fault-tolerant techniques - Performability metrics. Fault-tolerance in real-time systems - Space-time tradeoff - Fault-tolerant techniques (N-version programming - Recovery block – Imprecise computation; (m,k)-deadline model) – Adaptive fault-tolerance – Fault detection and location in real-time systems. Security Engineering – Protocols - Hardware protection - Cryptography – Introduction – The Random Oracle model – Symmetric Crypto- primitives – modes of operations – Hash functions – Asymmetric crypto primitives.	11
INTERNAL TEST 1 (Module I)		

II	Distributed systems - Concurrency - fault tolerance and failure recovery – Naming. Multilevel Security – Security policy model – The Bell Lapadula security policy model – Examples of Multilevel secure system – Broader implementation of multilevel security system. Multilateral security – Introduction – Comparison of Chinese wall and the BMA model – Inference Control – The residual problem.	10
INTERNAL TEST 2 (Module II)		
III	Banking and bookkeeping – Introduction – How computers systems works – Wholesale payment system – Automatic teller Machine – Monitoring systems – Introduction – Prepayment meters – Taximeters, Tachographs and trunk speed limits. Nuclear Command and control – Introduction – The kennedy memorandum – unconditionally secure authentication codes – shared control security – tamper resistance and PAL – Treaty verification. Security printing and seals – Introduction – History – Security printing – packaging and seals – systemic vulnerability – evaluation methodology.	11
IV	Bio metrics – Introduction – Handwritten signature – face recognition –fingerprints – Iris codes – Voice recognition. Emission Security – Introduction – Technical Surveillance and countermeasures – Passive Attacks – Active Attacks. Electronic and Information warfare – Introduction – Basics – Communication system – Surveillance and target acquisition – IFF system – Directed Energy Weapon – Information Warefare. Telecom Security – Introduction – Phone Breaking – Mobile phones – Network attack and defense - Protecting E-commerce systems- E – policy – Management issues – systems evaluation and assurance.	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Ross J Anderson and Ross Anderson, “Security Engineering: A guide to building dependable distributed systems”, Wiley, 2001.
2. David Powell, “A generic fault-Tolerant architecture for Real-Time Dependable Systems”, Springer, 2001.
3. Hassan B Diab and Albert Y. Zomaya, “Dependable computing systems: Paradigm, Performance issues and Applications”, Wiley series on Parallel and Distributed

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS7423	IoT SECURITY	3-0-0-3	2020

COURSE OBJECTIVES:

1. To give an overview of security in IoT system in security.
2. To provide knowledge about security risks IoT domain faces and countermeasures available for the known issues

COURSE OUTCOMES:

On successful completion of this course the student will be able to

1. Understand IoT general models and security challenges
2. Recognize IoT security and vulnerability threats.
3. Understand different IoT protocols and their security measures.
4. Interpret how to secure an IoT environment
5. Interpret different types of attacks

SYLLABUS:

Introduction to IoT, Architecture, Characteristics, IoT protocols, Security requirements in IoT, IoT vulnerabilities and attacks, Threat modeling, Authentication, Authorization and access control in IoT systems.

MODULE	COURSE CONTENT (42 hrs)	HRS
I	Fundamentals, Architecture of IoTs, Sensing, Actuation; Basics of networking IoT devices; Interoperability in IoT; IoT design methodology, Domain specific IoTs: Home automation, Agriculture, Smart cities; IoT enabling technologies-WSNs, Cloud computing, Big data analytics, Embedded systems; WSN and IoT.	11
INTERNAL TEST 1 (Module I)		
II	IoT protocols-Link layer protocols, Network layer protocols-IPV4, IPV6, 6LoWPAN, Transport layer protocols , Infrastructure-IPv6 -LowPAN , Identification-Electronic Product Code -uCode, Transport-Bluetooth - LPWAN, Data -MQTT – CoAP.	10
INTERNAL TEST 2 (Module II)		

III	IoT Security Requirements -Data Confidentiality -Data Encryption -Data Authentication -Secured Access Control –IoT-Vulnerabilities – Secret-Key Authentication/Authorization for Smart Devices - Constrained System Resources -Device Heterogeneity -Fixed Firmware. IoT Attacks -Side-channel Attacks -Reconnaissance -Spoofing -Sniffing -Neighbour -Discovery -Rogue Devices-Man-in-Middle	11
IV	Threat modelling in an IoT system; Secure IoT system implementation life cycle, Identity and access management solutions for IoT- IoT life cycle, authentication credentials, Authorization and access control; Identity relationship management and context in IoT	10
END SEMESTER EXAM (All Modules)		

REFERENCES:

1. Fei HU, “Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations”, CRC Press,2016.
2. Russell, Brian and Drew Van Duren, “Practical Internet of Things Security”, Packt Publishing, 2016.
3. Ollie Whitehouse, “Security of Things: An Implementers' Guide to Cyber-Security forInternet of Things Devices and Beyond”, NCC Group, 2014.
4. "Internet of Things: A Hands-on Approach", by ArshdeepBahga and Vijay Madisetti (Universities Press).
5. Online Resources
   https://www.postscapes.com/internet-of-things-protocols/
   https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/index.html
   https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS7033	SEMINAR – II	0-0-2-2	2020

COURSE OBJECTIVES:

1. To introduce the students to research, make them understand research papers and prepare presentation material.
2. To understand cutting edge technology in the chosen area
3. To improve oral communication skills through presentation.
4. To prepare original technical write up on the presentation.

COURSE OUTCOMES:

After completion of course, students will be able to:

1. Develop skills in doing literature survey, technical presentation and report preparation
2. Improve the proficiency in English
3. Improve presentation skills
4. Improve analytical and reasoning ability
5. Improve technical writing skills

SYLLABUS:

The aim of this course is to introduce the student to research, and to acquaint him with the process of presenting his work through seminars and technical reports. Students have to register for the seminar and select a topic in consultation with any faculty member offering courses for the programme. The student is expected to do an extensive literature survey and analysis in an area related to the area of specialisation. The study should preferably result in design ideas, designs, algorithms, and theoretical contributions in the form of theorems and proofs, new methods of proof, new techniques or heuristics with analytical studies, implementations and analysis of results.

The presentation shall be of 30 minutes duration and a committee with the Head of the Department as the chairman and two faculty members from the department as members shall evaluate the seminar based on the coverage of the topic, presentation and ability to answer the questions put forward by the committee.

Students shall individually prepare and submit a seminar report based on experimental study / industrial training on the corresponding topic, in the prescribed format given by the Department. The reference shall include standard journals (ACM/ IEEE), conference proceedings and equivalent documents, reputed magazines and textbooks, technical reports and web based material, approved by the supervisor. The references shall be incorporated in the report following IEEE standards reflecting the state-of-the-art in the topic selected.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS7043	PROJECT PHASE I	0-0-8-6	2020

COURSE OBJECTIVES:

1.To undertake research in an area related to the program of study.

2. To acquaint students to literature survey and design of a project.

COURSE OUTCOMES:

Student should be able to

1. Identify the topic, objectives and methodology to carry out the project.
2. Finalise the project plan for their course project.

SYLLABUS:

Every student should carry out project, related to areas of Data Sciences, under the supervision of a Supervisor(s). The project work shall commence in the third semester and shall be completed by the end of fourth semester. Candidates are required to undertake a suitable research project work; the topic shall be approved by a committee constituted by the Head of the concerned Department. Every student will be required to present the topic at the beginning of the Phase-I to illustrate the scope of the work and to finalize the topic. The third semester includes the design phase and the fourth semester includes the implementation and final thesis submission.

The student should report the status of their progress weekly to the concerned supervisor. Students should submit the project report at the end of the respective semesters, on dates announced by the college/department. Project evaluation will be based on presentations, viva voce, demonstration, review reports, design reports and final thesis. Progress of the project work is to be evaluated at the end of the third semester. For this a committee headed by the head of the department with two other faculty members in the area of the project, of which one shall be the project supervisor. If the project is done outside the college, the external supervisor associated with the student will also be a member of the committee.

Normally students are expected to do the project within the college. However they are permitted to do the project in an industry or in a government research institute under a qualified supervisor from that organization. This is only possible in the fourth semester and the topic of investigation should be in line with the project part planned in the 3rd semester. Student should apply for this through the project supervisor indicating the reason for this well in advance, preferably at the beginning of the 3rd semester.

Project evaluation marks shall be as follows:-

Total marks for the Project: 150

In the 3rd Semester: Marks:50

Project Progress evaluation:

Progress evaluation by the Project Supervisor : 20 Marks

Presentation and evaluation by the committee : 30 Marks

APJ Abdul Kalam Technological University
Master of Technology – Course Plan

SEMESTER IV

M. Tech Programme in Cyber Security

COURSE CODE	COURSE NAME	L-T-P-C	YEAR
06DS7014	PROJECT PHASE II	0-0-21-12	2020

COURSE OBJECTIVES:

1. To undertake research in an area related to the program of study.
2. To enable students to implement and deploy a system and carry out performance analysis.

COURSE OUTCOMES:

Student should be able to

1. Get a good exposure to a domain of interest.
2. Get a good domain and experience to pursue future research activities.

SYLLABUS:

The Phase II work shall be based on the work in Phase I. Normally students are expected to do the project within the college. However they are permitted to do the project in an industry or in a government research institute under a qualified supervisor from that organization; the topic of investigation should be in line with the project part planned in the 3rd semester. Student should apply for this through the project supervisor indicating the reason for this well in advance, preferably at the beginning of the 3rd semester. This application is to be vetted by a departmental committee constituted for the same by the Principal and based on the recommendation of the committee the student is permitted to do the project outside the college. The same committee should ensure the progress of the work periodically and keep a record of this. The application for this shall include the following:- Topic of the Project, Project work plan in the 3rdSemester, Reason for doing the project outside, Institution/Organization where the project is to be done, External Supervisor Name, Designation, Qualification and Experience, Letter of consent of the External Supervisor as well as from the organization.

Final evaluation of the project will be taken up only on completion of the project in the fourth semester. This shall be done by a committee constituted for the purpose by the principal of the college. The concerned head of the department shall be the chairman of this committee. It shall have two senior faculty members from the same department, project supervisor and the external supervisor, if any, of the student and an external expert either from an academic/R&D organization or from Industry as members.

Final project grading shall take into account the progress evaluation done in the third semester and the project evaluation in the fourth semester. If the quantum of work done by the candidate is found to be unsatisfactory, the committee may extend the duration of the project up to one more semester, giving reasons for this in writing to the student. Normally further extension will not be granted and there shall be no provision to register again for the project.

Project work is to be evaluated both in the third and the fourth semesters. Based on these evaluations the grade is finalized in the fourth semester.
Project evaluation marks shall be as follows:-
Total marks for the Project: 150
In the 4th Semester: Marks:100

Project evaluation by the supervisor/s : 30 Marks
Presentation& evaluation by the Committee : 40 Marks
Evaluation by the External expert : 30 Marks

Students are required to publish their work in reputed national/ International Journals/ Conference Proceedings etc which will carry weightage in final marks.