SEMESTER -I

CTMTAIDS SI P1: Mathematical and Computational Foundation for Artificial Intelligence

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		Total
					Internal Exams					University Exams		University Exams (LPW)		
					TA-1		MSE		TA-2 *					
L	T	P	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To understand the concepts of Vector space and inner-product spaces.
2. To apply the linear algebra concepts in approximations and matrix. decompositions.
3. To understand functions of several variables, gradients relevant for machine learning.
4. To acquire sound mathematical aspects of machine learning and artificial intelligence.

UNIT -I

Vector spaces, linear independence, basis, dimensions, matrix representation of data, inner products and norms on a vector space, lengths, angles.

UNIT -II

Orthogonal matrices and Gram-Schmidt, projections, least square approximations, Matrix decompositions, Cholesky decomposition, eigen decomposition and diagonalization, singular value decomposition.

UNIT -III

Brief overview of simple linear regression, multiple linear regression, and logistic regression. Linear Regression and parameter estimation; Dimensionality reduction - Principal Component Analysis, linear discriminant analysis; Density estimation with Gaussian mixture models.

UNIT -IV

Classification with support vector machines – separating hyperplanes, primal and dual support vector machines, kernels.

UNIT -V

Brief overview of random variables, known special probability distributions; Functions of one random variable, mean, variance, moment. Covariance and correlation.

Reference Book: -

1. Mathematics for Machine Learning, Mark Peter Deisenroth, A. Aldo Faisal and Cheng Soon Ong, Cambridge University Press, 2020
2. Linear Algebra and Learning from Data, Gilbert Strang, Wellesley-Cambridge Press, 2019
3. Linear Algebra, Stephen H. Friedberg, Arnold J. Insel and Lawrence E. Spence, Pearson
4. Probability, Random Variables, and Stochastic Processes, Athanasios Papoulis and S. Unnikrishnan Pillai, Mc-Graw Hill, 2002, Fourth Edition
5. Applied Statistics and Probability for Engineers, Douglas C. Montgomery and George C. Runger, John Wiley and Sons, 2018, Seventh Edition.

CTMTAIDS SI P2: Network Security and Forensics

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To understand the basics of network vulnerability assessment and penetration testing methodology.
2. To understand the important network communication protocols.
3. To understand the concept of encryption, public key cryptography, message authentication and hash functions.
4. To understand the basics of wireless network protocols and its security concepts.
5. To understand the basics of network forensics.

UNIT–I

ISO/OSI, TCP-IP, Networking devices: Host, Hub, Bridge, Switch, Router and its functioning, Perimeter devices: IDS, IPS, Firewall and its functioning. NOC, SOC, SIEM, Servers: DNS, DHCP, Proxy, Mail and Application servers. Threat, vulnerability, attack surface, attack vector, exploit. Common attacks and countermeasures: Phishing attack, ARP poising, MAC flooding, DoS and DDoS.

UNIT–II

Penetration testing life cycle: Scope, SOW, Reconnaissance, target enumeration, vulnerability identification, assessment, exploitation, and reporting. Information gathering starting at source scrutinizing key employees, Dumpster diving, War driving, analyzing the web, exploring domain ownership- whois, Regional internet registries, server location, Scanning: active and passive, ICMP (Ping), OS and server fingerprinting, scanning tools and port status, TCP and UDP scan. SNMP services enumeration, and countermeasures. Routing devices enumeration and countermeasures. Advanced enumeration: Password cracking, sniffing

password hashes and password protection. Vulnerability exploitation, Buffer overflow, vulnerability assessment tools, source code assessment tools, application assessment tools, system assessment tools, exploit tools.

UNIT–III

Introduction to Security: need for security, principle of security, security approaches. Encryption Techniques: plaintext, cipher text, substitution and transposition techniques, encryption and decryption, key range and size. Symmetric and Asymmetric encryption. Public Key Cryptography and Message Authentication: Public key cryptographic principles, digital signatures, key management, hash function and message digest. Types of attacks and countermeasures.

UNIT–IV

802.11 Protocols, WAP and inherent security issues, promiscuous and monitor mode, Sniffing wireless packets, management, control, and data frames, WLAN authentication and encryption, WEP, WPA and WPA 2. WLAN authentication and security flaws. WLAN based attacks and countermeasures. WLAN Pen testing tools.

UNIT–V

Digital evidence, Network based digital evidence, Network Forensic investigation methodology, Sources of network-based evidence, Evidence acquisition, Network traffic capture and analysis, Traffic capture and analysis tools, Event log aggregation, correlation, and analysis. Data in motion investigation

Reference Books: -

1. Stallings, W., Network Security Essentials: applications and standards. 3rd ed. Pearson Education India, 2007.
2. Stallings, W., Cryptography and Network Security: Principles and Practice. 6th ed. Pearson, 2004.
3. Forouzan, B.A., Cryptography and Network Security. Tata McGraw-Hill Education, 2010 2.
4. Kahate, A. Cryptography and Network Security. McGraw-Hill Higher Ed., 2009.
5. Michael Gregg, Build Your Own Security Lab: A Field Guide for

Networking Testing.

6. Sherri Davidoff and Jonathan Ham, Network Forensics Tracking Hackers through Cyberspace.
7. Mastering Wireless Penetration Testing for Highly Secured Environments by Aaron Johns

CTMTAIDS SI P3: Incident Response and Audit Compliances

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		Total
					Internal Exams					University Exams		University Exams (LPW)		
					TA-1		MSE		TA-2 *					
L	T	P	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To learn Security Audit and Compliance.
2. To understand the process of security audit.
3. To understand the industry standard practices for auditing.
4. To learn various security standards.
5. To learn the policy making and organizational structure.
6. To understand the Risk and Continuity planning.

UNIT–I

Cyber Incident Statistics, Computer Security Incident, Information Warfare, Key Concepts of Information Security, Types of Computer Security Incidents, Examples of Computer Security Incidents, How to Identify an Incident, Need for Incident Response, Goals and Purpose of Incident Response, Signs of an Incident, Incident Categories

UNIT–II

Incident Prioritization, Use of Disaster Recovery Technologies, Impact of Virtualization on Incident Response and Handling, Estimating Cost of an Incident, Incident Reporting, Incident Reporting Organizations, Vulnerability Resources, Incident Management, Incident Response Team Roles, Incident Response Team Responsibilities, Dependencies.

UNIT – III

Identifying the Minimum Acceptable Level of Risk and Appropriate Security Baseline Definitions, Seven Domains of a Typical IT Infrastructure, Writing the IT Infrastructure Audit Report Compliance within User Domain: Compliance law requirements and business drivers, Items Commonly Found in the User Domain,

Compliance within the workstation domain: Compliance law requirements and business drivers, devices and components commonly found in the workstation domain, Maximizing C-I-A, Compliance within the LAN Domain: Compliance law requirements and business drivers, devices and components commonly found in the LAN domain, Maximizing C-I-A, Compliance within LAN and WAN Domain: Devices and Components Commonly Found in the Domain , Penetration Testing and Validating Configurations, Compliance within Remote Access and Application Domain: Devices and Components Commonly Found in the Domain, Application Server Vulnerability Management, Application Patch Management.

UNIT – IV

Introduction to Risk Analysis, Risk Identification, Risk Assessment, Risk Response and Mitigation, Risk Reporting, Introduction to Business Continuity Planning (BCP), Overview of BCP Life Cycle, Need for BCP, Identifying and Selecting Business Continuity Strategies, Introduction to Disaster Recovery (DR) planning, Identification of potential disaster status, DR Strategies, Plans for Business Resumption.

UNIT–V

Indian IT ACT with Amendments, Adjudication under Indian IT ACT, Auditing Standards and Frameworks: ISO/IEC 27001/2, COBIT, SOC Compliance, HIPAA, GDPR and PCIDSS.

Reference Books: -

1. Auditing IT Infrastructures for Compliance by Martin M. Weiss, Michael G. Solomon, Jones and Bartlet Learning, 2015
2. The IT Regulatory and Standards Compliance Handbook by Craig S. Wright, Syngress, 2015
3. Information Technology Control and Audit 5th Edition by Angel R. Otero, 2019
4. (Internal Audit and IT Audit Series) The Complete Guide to Cyber Security Risks and Controls by Anne Kohnke, Dan Shoemaker, Ken Sigler, 2016
5. PCI DSS An Integrated Data Security Standard Guide- Press by Jim Seaman, 2020
6. AICPA - Guide_ SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy-Wiley, 2018

7. The EU General Data Protection Regulation (GDPR) A Practical Guide by Paul Voigt and Axel von dem Bussche, 2017
8. PCI DSS, SAQ Instructions and Guidelines (Available online)
9. Bob Hayes, Kathleen Kotwica, “Business Continuity 2nd Edition”, Elsevier Pub.2013.
10. Governance, risk, and compliance by Microsoft, 2019.
11. Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response by Leighton Johnson
12. Incident Handling and Response: A Holistic approach for an efficient security incident management by Jithin Aby Alex
13. Blue Team Handbook: Incident Response Edition by Don Murdoch
14. The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk by N. K. McCarthy
15. Critical Incident Management: A Complete Response Guide, Second Edition by John McNall, Thomas T. Gillespie, Vincent F. Faggiano

CTMTAIDS SI P4: Fundamentals of Data Science and Machine Learning

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		Total
					Internal Exams					University Exams		University Exams (LPW)		
					TA-1		MSE		TA-2 *					
L	T	P	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To explore the fundamental concepts of data science and machine learning.
2. To understand data analysis techniques for applications handling large data.
3. To visualize and present the inference using various tools.

UNIT -I

Introduction to core concepts and technologies: Introduction, Terminology, data science process, data science toolkit, Types of data, Example applications, Introduction to Statistical Methods: basic and some advanced concepts of probability and statistics; Concepts of statistics in solving problems arising in data science.

UNIT -II

Data preprocessing, Data cleaning, data integration, Data Reduction Data Transformation and Data Discretization. Evaluation of classification methods, Confusion matrix, Students T-tests and ROC curves-Exploratory Data Analysis Basic tools (plots, graphs and summary statistics) of EDA, Philosophy of EDA.

UNIT -III

Basic Machine Learning Algorithms: Association Rule mining, Linear Regression, Logistic Regression. Classification, k-Nearest Neighbors (k-NN), k-means, Decision tree, Naive Bayes, Ensemble Methods Random Forest. Feature Generation and Feature Selection, Feature Selection algorithms, Filters, Wrappers, Decision Trees, Random Forests.

UNIT -IV

Clustering, Choosing distance metrics, Different clustering approaches, hierarchical agglomerative clustering, k-means, DBSCAN, Relative merits of each method, clustering tendency and quality. Computer science and engineering applications Data mining, Network protocols, analysis of Web traffic.

UNIT -V

Data visualization introduction, Types of data visualization, Data types. Applications of Data Science, Technologies for visualization, Tools for data visualization, recent trends in various data collection and analysis techniques, various visualization techniques, application development methods used in data science.

Reference Books: -

1. Cathy O'Neil, Rachel Schutt, "Doing Data Science", Straight Talk from The Frontline, O'Reilly, 2013.
2. Han, J., Pei, J. and Tong, H., "Data mining: concepts and techniques.", 2022.
3. Davy Cielen, Arno D. B. Meysman, Mohamed Ali, "Introducing Data Science," Manning Publications Co., 3 rd edition, 2016.
4. Mohammed J. Zaki and Wagner Miera Jr, "Data Mining and Analysis: Fundamental Concepts and Algorithms", Cambridge University Press, 2014.
5. Gareth James, Daniela Witten, Trevor Hastie, Robert Tibshirani, "An Introduction to Statistical Learning: with Applications in R," Springer, 1st edition, 2013.
6. Jure Leskovek, Anand Rajaraman, Jeffrey Ullman, "Mining of Massive Datasets", v2.1, Cambridge University Press, 2014.
7. Joel Grus, O'Reilly, "Data Science from Scratch: First Principles with Python", 1st edition, 2015.

CTMTAIDS SI P5: Introduction to Forensic Science and Cyber Law

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
04	00	00	04	04	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. About the significance of forensic science to human society and criminal investigation.
2. The fundamental principles of forensic science.
3. The divisions in a forensic science laboratory.
4. The working of the forensic establishments in India and abroad.
5. Legal aspects of forensic investigations.

UNIT-I

History of Development of Forensic Science in India. Functions of forensic science. Historical aspects of forensic science. Definitions and concepts in forensic sciences. Scope of forensic science. Various contemporary disciplines of forensic sciences and their applications in different approaches with theoretical concepts Need of forensic science. Basic principles of forensic science.

UNIT-II

Contemporary development in the academic and practices in forensic sciences- advantage of scientific investigations- Tools and Techniques in Forensic Science- Branches of forensic science. Forensic science in international perspectives, including set up of INTERPOL, and FBI. Duties of forensic scientists. Code of conduct for forensic scientists. Qualifications of forensic scientists. Data depiction. Report writing.

UNIT-III

Academic institutions involvement -Organizational set up of Forensic Science Laboratories in India Hierarchical set up of Central Forensic Science Laboratories, State Forensic Science Laboratories, Government Examiners of Questioned Documents, Fingerprint Bureaus, National Crime Records Bureau, Police and Detective Training Schools, NIA, CCNTS, Bureau of Police Research and Development, Directorate of Forensic Science and Mobile Crime Laboratories. Police Academies. National investigation agency and other agencies involved in the criminal investigations- agencies referred for the additional information and requisite examinations

UNIT-IV

Definition of Law, Court, Judge, Basic Terminology in Law, Introduction to Criminal Procedure Code, FIR, Difference between civil and Criminal Justice, Object of Punishment, Kinds of Punishment, Primary and Sanctioning Rights Primary and Secondary functions of Court of Law. Law to Combat Crime-Classification – civil, criminal cases. Essential elements of criminal law. Constitution and hierarchy of criminal courts. Criminal Procedure Code: Cognizable and non-cognizable offences. Bailable and nonbailable offences. Sentences which the court of Chief Judicial Magistrate may pass. Laws specific to Forensic Science: Indian Penal Code pertaining to offences against persons – Section 121A, 299, 300, 302, 304A, 304B, 307, 309, 319, 320, 324, 326, 351, 354, 359, 362.Sections 375 and 377 and their amendments. Indian Evidence Act – Evidence and rules of relevancy in brief. Expert witness. Cross examination and re-examination of witnesses. Sections 32, 45, 46, 47, 57, 58, 60, 73, 135, 136, 137, 138, 141. CrPC – Sections 291,291A, 292 and 293 in the code of criminal procedure.

UNIT-V

Introduction to Computer and its components, different types of storage media, Category to Cyber-crime, Cyber Law, IT Act 2000 and its amendments, International Cyber Laws, Cyber Ethics, Child Sexual Abuse Material related to cyber domain, various acts related to social media, privacy and security on cyber domain, case studies.

Reference Books: -

1. B.B. Nanda and R.K. Tiwari, Forensic Science in India: A Vision for the Twenty First Century, Select Publishers, New Delhi (2001).
2. M.K. Bhasin and S. Nath, Role of Forensic Science in the New Millennium, University of Delhi, Delhi (2002).
3. S.H. James and J.J. Nordby, Forensic Science: An Introduction to Scientific and Investigative Techniques, 2nd Edition, CRC Press, Boca Raton (2005).
4. W.G. Eckert and R.K. Wright in Introduction to Forensic Sciences, 2nd Edition, W.G. Eckert (ED.), CRC Press, Boca Raton (1997).
5. R. Saferstein, Criminalistics, 8th Edition, Prentice Hall, New Jersey (2004).
6. W.J. Tilstone, M.L. Hastrup and C. Hald, Fisher's Techniques of Crime Scene Investigation, CRC Press, Boca Raton (2013)
7. Tallinn Manual on The International Law Applicable to Cyber Warfare, International Group of Experts and NATO by Michael N. Schmitt
8. IT Act 2000 and 2008 bare acts documents Cyber Law in India, Satish Chandra (2017)

CTMTAIDS SI L1: Mathematical and Computational Foundation for Artificial Intelligence Laboratory

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
00	00	01	01	02	--	--	--	--	--	--	--	100	3	100

Syllabus:

Experiments / Practicals to support the associated theory course.

CTMTAIDS SI L2: Network Security and Forensics Laboratory

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
					Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
L	T	P	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
00	00	01	01	02	--	--	--	--	--	--	--	100	3	100

Syllabus:

Experiments / Practicals to support the associated theory course.

CTMTAIDS SI L3: Incident Response and Audit Compliances Laboratory

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
00	00	01	01	02	--	--	--	--	--	--	--	100	3	100

Syllabus:

Experiments / Practicals to support the associated theory course.

CTMTAIDS SI L4: Fundamentals of Data Science and Machine Learning Laboratory

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
					Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
L	T	P	C	TCH	Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
00	00	01	01	02	--	--	--	--	--	--	--	100	3	100

Syllabus:

Experiments / Practicals to support the associated theory course.