MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

5th Semester

Subject Type	Course Name	Course Code	Credit Points	Credit Distribution			Mode of Delivery			Proposed MOOCs
				Theory	Practical	Tutorial	Offline #	Online	Blended	
CC 11	Cyber Foresics	CYS 501	6	5	0	1	✓			As per MAKAUT notification
CC 12	Malware Analysis	CYS 502	6	5	0	1	✓			
DSE 1 (Any One)	Cloud Computing	CYS 503(A)	6	5	0	1	✓			
	Design and Analysis of Algorithm	CYS 503(B)	6	4	0	0	✓			
		CYS 593(B)		0	2	0	✓			
DSE 2 (Any One)	Information and Coding Theory	CYS 504(A)	6	5	0	1	✓			
	Introduction to AI and Machine Learning	CYS 504(B)	6	4	0	0	✓			
		CYS 594(B)		0	2	0	✓			
Semester Credit			**24**							

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

- **CC 11: Cyber Forensics**
- **Code: CYS 501**
- **Course Objective:**

It enables the students to make use of the knowledge in the field of Computer forensics & Cyber Crime. After completion of the course the students will be able to apply investigation tools and techniques, analysis of data to identify evidence, Technical Aspects & Legal Aspects related to cybercrime.

Sl. No.	Course Summary	Mapped Module
1.	Examine and Discuss Cyber Forensic Science.	M1
2.	Make use of Cyber Crime Scene Analysis.	M2
3.	Infer Evidence Management & Presentation.	M3
4.	Discuss Computer Forensics.	M4
5.	Assess details about Mobile Forensics.	M5
6.	Outline recent trends in mobile forensics techniques and methods.	M6

Module Number	Content	Total Hours	%age of questions	Blooms Level	Remarks
1	Introduction of Cyber Forensic Science.	12	20	1,2	
2	Cyber Crime Scene Analysis	10	20	1,2,3	
3	Evidence Management & Presentation	12	20	2,3,4	
4	Computer Forensics	12	25	2,3,4	
5	System and Network Security	7	10	2,3,4	
6	Recent trends in mobile forensics techniques and methods	7	5	2,3	
		60	100		
	Tutorial	16			

Module 1: Cyber Forensics Science:
Forensics science, computer forensics, and digital forensics. Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber-criminalistics area, holistic approach to cyber-forensics

Module 2: Cyber Crime Scene Analysis:
Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

Module 3: Evidence Management & Presentation:
Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.

Module 4: Computer Forensics:

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

Module 5: Mobile Forensics:

Mobile forensics techniques, mobile forensics tools. Legal Aspects of Cyber Forensics: IT Act 2000, amendment of IT Act 2008.

Module 6: Recent trends in mobile forensic technique and methods:

Recent trends in mobile forensic technique and methods to search and seizure electronic evidence

Suggested Reading:

- 1. John Sammons, The Basics of Digital Forensics, Elsevier Model Curriculum of Engineering & Technology PG Courses [Volume-I]
- 2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

- **CC 12: Malware Analysis**
- **Code: CYS 502**
- **Course Objective:**
- This course provides all the necessary insights about the modern malware and anti-malware landscape. Participants will be able to evaluate about current malware functioning and how it infects companies' IT infrastructures through their weakest points, exploiting these weaknesses after infection.

Sl. No.	Course Summary	Mapped Module
1.	Make use of Fundamentals of Malware Analysis (MA).	M1
2.	Discuss about Malware Forensics.	M2
3.	Examine Malware and Kernel Debugging.	M3
4.	Explain Memory Forensics and Volatility.	M4
5.	Make use of Researching and Mapping Source Domains/IPs.	M5
6.	Assess Case Study(e.g. Finding Artifacts in Process Memory etc.	M6

Module Number	Content	Total Hours	%age of questions	Blooms Level	Remarks
1	Fundamentals of Malware Analysis (MA)	15	25	1,2	
2	Malware Forensics	10	15	1,2,3	
3	Malware and Kernel Debugging	10	20	2,3	
4	Memory Forensics and Volatility	10	20	2,3	
5	Researching and Mapping Source Domains/IPs	7	10	2,3,4	
6	Case Study	8	10	2,3,4,5	
		60	100		
	Tutorial	16			

Module 1: Fundamentals of Malware Analysis (MA):
Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM) Methodology, Brief Overview of Malware analysis lab setup and configuration, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining ClamAVSignatures, Creating Custom ClamAV Databases, Using YARA to Detect Malware Capabilities, Creating a Controlled and Isolated Laboratory, Introduction to MA Sandboxes, Ubuntu, Zeltser'sREMnux, SANS SIFT, Sandbox Setup and Configuration New Course Form, Routing TCP/IP Connections, Capturing and Analyzing Network Traffic, Internet simulation using INetSim, Using Deep Freeze to Preserve Physical Systems, Using FOG for Cloning and Imaging Disks, Using MySQL Database to Automate FOG Tasks, Introduction to Python ,Introduction to x86 Intel assembly language, Scanners: Virus Total, Jotti, and NoVirus

Thanks, Analyzers: Threat Expert, CWSandbox, Anubis, Joebox, Dynamic Analysis Tools: Process Monitor, Regshot, HandleDiff, Analysis Automation Tools: Virtual Box, VM Ware, Python , Other Analysis Tools

Module 2: Malware Forensics:
Using TSK for Network and Host Discoveries, Using Microsoft Offline API to Registry Discoveries, Identifying Packers using PEiD, Registry Forensics with Reg Ripper Plu-gins:, Bypassing Poison Ivy's Locked Files, Bypassing Conficker's File System ACL Restrictions, Detecting Rogue PKI Certificates

Module 3: Malware and Kernel Debugging:
Opening and Attaching to Processes, Configuration of JIT Debugger for Shell code Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Debugging with Python Scripts and Py Commands, DLL Export Enumeration, Execution, and Debugging, Debugging a VMware Workstation Guest (on Windows), Debugging a Parallels Guest (on Mac OS X). Introduction to WinDbg Commands and Controls, Detecting Rootkits with WinDbgScripts, Kernel Debugging with IDA Pro.

Module 4: Memory Forensics and Volatility:
Memory Dumping with MoonSols Windows Memory Toolkit, Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps, Code Injection and Extraction, Detecting and Capturing Suspicious Loaded DLLs, Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA.

Module 5: Researching and Mapping Source Domains/IPs:
Using WHOIS to Research Domains, DNS Hostname Resolution, Querying Passive DNS, Checking DNS Records, Reverse IP Search New Course Form, Creating Static Maps, Creating Interactive Maps

Module 6: Case Study:
Case study of Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA

Suggested Reading:
1. Michael Sikorski, Andrew Honig "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" publisher Williampollo

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

- **Course: Cloud Computing**
- **Code: CYS 503(A)**
- **Course Objective:**
  Students will be able to examine the principles of cloud computing, SaaS, PaaS etc and to explain knowledge of applications of cloud computing.

Sl. No.	Course Summary	Mapped Module
1.	Define Cloud Computing and its Basics Definition of Cloud Computing	M1
2.	Make use of Platforms in Cloud Computing Virtualization technologies.	M2
3.	Take part in Cloud Infrastructure Cloud Management.	M3
4.	Analyse Concepts of Services and Applications Service Oriented Architecture.	M4

Module Number	Content	Total Hours	%age of questions	Blooms Level	Remarks
1	Definition of Cloud Computing and its Basics Definition of Cloud Computing	15	20	1,2	
2	Use of Platforms in Cloud Computing Virtualization technologies	15	30	1,2,3	
3	Cloud Infrastructure Cloud Management	15	30	2,3,4	
4	Concepts of Services and Applications Service Oriented Architecture	15	20	2,3,4	
		60	100		
	Tutorial	16			

Module 1: Definition of Cloud Computing and its Basics Definition of Cloud Computing:
Defining a Cloud, Cloud Types – NIST model, Cloud Cube model, Deployment models (Public , Private, Hybrid and Community Clouds), Service models – Infrastructure as a Service, Platform as a Service, Software as a Service with examples of services/ service providers, Cloud Reference model. Characteristics of Cloud Computing – a shift in paradigmBenefits and advantages of Cloud Computing Cloud Architecture: A brief introduction on Composability, Infrastructure, Platforms, Virtual Appliances, Communication Protocols, Applications, Connecting to the Cloud by Clients . Services and Applications by Type IaaS – Basic concept, Workload, partitioning of virtual private server instances, Pods, aggregations, silos PaaS – Basic concept, tools and development environment with examples SaaS - Basic concept and characteristics, Open SaaS and SOA, examples of SaaS platform Identity as a Service (IDaaS) Compliance as a Service (CaaS)

Module 2: Use of Platforms in Cloud Computing Virtualization technologies:
Types of virtualization (access, application, CPU, storage), Mobility patterns (P2V, V2V, V2P, P2P, D2C, C2C, C2D, D2D) Load Balancing and Virtualization: Basic Concepts, Network resources for load balancing, Advanced load balancing (including Application Delivery

Controller and Application Delivery Network), Mention of The Google Cloud as an example of use of load balancing Hypervisors: Virtual machine technology and types, VMware vSphere Machine Imaging (including mention of Open Virtualization Format – OVF) Porting of applications in the Cloud: The simple Cloud API and AppZero Virtual Application appliance Definition of services, Distinction between SaaS and PaaS (knowledge of Salesforce.com and Force.com), Application development Use of PaaS Application frameworks. Discussion of Google Applications Portfolio – Indexed search, Dark Web, Aggregation and disintermediation, Productivity applications and service, Adwords, Google Analytics, Google Translate, a brief discussion on Google Toolkit (including introduction of Google APIs in brief), major features of Google App Engine service. Amazon Web Service components and services: Amazon Elastic Cloud, Amazon Simple Storage system, Amazon Elastic Block Store, Amazon SimpleDB and Relational Database Service Windows Azure platform: Microsoft's approach, architecture, and main elements, overview of Windows Azure AppFabric, Content Delivery Network, SQL Azure, and Windows Live services

Module 3: Cloud Infrastructure Cloud Management:

An overview of the features of network management systems and a brief introduction of related products fromlarge cloud vendors, Monitoring of an entire cloud computing deployment stack – an overview with mention of some products, Lifecycle management of cloud services (six stages of lifecycle) Concepts of Cloud Security Cloud security concerns, Security boundary, Security service boundary Overview of security mapping Security of data: Brokered cloud storage access, Storage location and tenancy, encryption, and auditing and compliance Identity management (awareness of Identity protocol standards)

Module 4: Concepts of Services and Applications Service Oriented Architecture:

Basic concepts of message-based transactions, Protocol stack for an SOA architecture, Event-driven SOA, Enterprise Service Bus, Service catalogs Applications in the Cloud: Concepts of cloud transactions, functionality mapping, Application attributes, Cloud service attributes, System abstraction and Cloud Bursting, Applications and Cloud APIs Cloud-based Storage: Cloud storage definition – Manned and Unmanned Webmail Services: Cloud mail services including Google Gmail, Mail2Web, Windows Live Hotmail, Yahoo mail, concepts of Syndication services.

Suggested Reading:

1. Barrie Sosinsky; Cloud Computing Bible; Wiley India Pvt. Ltd
2. Rajkumar Buyya, Christian Vecchiola, S. Thamarai Selvi; Mastering Cloud Computing; McGraw Hill Education(India) Private Limited
3. Anthony T. Velte; Cloud computing: A practical approach; Tata Mcgraw-Hill

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

- **Course: Design and Analysis of Algorithms**
- **Code: CYS 503B + CYS 593B**
- **Course Objective:**

1	To be familiar with algorithm complexity analysis.
2	To understand and apply several algorithm design strategies.

Sl. No.	Course Summary	Mapped Module
1.	Discuss Complexity Analysis	M1
2.	Demonstrate Algorithm Design by Divide and Conquer.	M2
3.	Analyse Disjoint Set Data Structure.	M3
4.	Make use of Algorithm Design by Greedy Strategy.	M4
5.	Make use of Algorithm Design by Dynamic Programming	M5
6.	Make use of Algorithm Design by Backtracking.	M6

- **Theory (CYS503B)**

Module Number	Content	Total Hours	%age of questions	Blooms Level	Remarks
1	Complexity Analysis	8	20	1,2	
2	Algorithm Design by Divide and Conquer	8	20	2,3	
3	Disjoint Set Data Structure	8	20	2,3	
4	Algorithm Design by Greedy Strategy	8	10	2,3,4	
5	Algorithm Design by Dynamic Programming	8	10	2,3,4	
6	Algorithm Design by Backtracking	8	20	2,3,4	
		48	100		

Practical (CYS593B)

Module Number	Content	Total Hours	%age of questions	Blooms Level (if applicable)	Remarks (If any)
2	Implement Merge sort	3	10	3,4	
2	Implement Quicksort	3	10	3,4	
2	Find maximum and minimum elements from an array of integers using divide and conquer strategy.	2	10	3,4	

4	Implement fractional knapsack	2	10	3,4	
4	Implement Job sequence with deadline	3	10	3,4	
4	Implement Kruskal's algorithm	3	10	3,4	
4	Implement Prim's algorithm	3	10	3,4	
5	Implement Dijkstra's algorithm	3	10	3,4	
5	Implement Matrix Chain Multiplication	3	10	3,4	
5	Implement Floyd Warshall Algorithm	3	10	3,4	
		28	100		

Module 1: Complexity Analysis

Time and Space Complexity, Different Asymptotic notations big O,Ω,Ø , Little o,,ω and their mathematical significance and proof.

Module 2: Algorithm Design by Divide and Conquer

Basic concept of divide and conquer, Merge sort, Quick sort ,heap sort and their complexity analysis in best case, worst case and average case.

Module 3: Disjoint Set Data Structure

Set Manipulation Algorithm by Union-Find, Union by Rank, Path Compression

Module 4: Algorithm Design by Greedy Strategy

Basic concept, Activity Selection Problem, Fractional Knapsack problem, Job sequencing with deadline, Prims, Kruskal.

Module 5: Algorithm Design by Dynamic Programming

Basic concept, 0/1 Knapsack Problem, Matrix Chain Multiplication, All Pair Shortest Path - Floyd Warshall Algorithm, Dijkstra's Algorithm.

Module 6: Algorithm Design by Backtracking

Basic concept, Use - N-Queen Problem, Graph Coloring Problem, Hamiltonian Path Problem

Suggested Reading-

Author	Book
E.Horowitz and Sahni	Fundamentals of Computer Algorithms
T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein	Introduction to Algorithms

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

- **Course: Information and Coding Theory**
- **Code: CYS 504(A)**
- **Course Objective:**

1	Outline how error control coding techniques are applied in communication systems.
2	Able to explain the basic concepts of cryptography.
3	To make use of the knowledge of probabilities, entropy, measures of information.

Sl. No.	Course Summary	Mapped Module
1.	Discuss Information Entropy Fundamentals	M1
2.	Examine Data and Voice Coding.	M2
3.	Explain Error Control and Coding.	M3

Module Number	Content	Total Hours	%age of questions	Blooms Level	Remarks
1	Information Entropy Fundamentals	10	25	1,2	
2	Data and Voice Coding	25	35	1,2,3	
3	Error Control Coding	25	40	2,3,4	
		60	100		
	Tutorial	16			

Module 1: INFORMATION ENTROPY FUNDAMENTALS

Uncertainty, Information and Entropy – Sourccoding Theorem – Huffman coding –Shannon Fano coding – Discrete Memory less channels – channel capacity – channel coding Theorem – Channel capacity Theorem.

Module 2: DATA AND VOICE CODING

Differential Pulse code Modulation – Adaptive Differential Pulse Code Modulation – Adaptive subband coding – Delta Modulation – Adaptive Delta Modulation – Coding of speech signal at low bit rates (Vocoders, LPC).

Denial of Service Attacks, DOS-proof network architecture, Security architecture of World Wide Web, Security Architecture of Web Servers, and Web Clients, Web Application Security – Cross Site Scripting Attacks, Cross Site Request Forgery, SQL Injection Attacks, Content Security Policies (CSP) in web, Session Management and User Authentication, Session Integrity, Https, SSL/TLS, Threat Modeling, Attack Surfaces, and other comprehensive approaches to network design for security

Module 3: ERROR CONTROL CODING

Linear Block codes – Syndrome Decoding – Minimum distance consideration – cyclic codes – Generator Polynomial – Parity check polynomial – Encoder for cyclic codes – calculation of

syndrome – Convolutional codes.

Suggested Reading:

List of Books **Text Books:**			
Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Simon Haykin	Communication Systems	4th Edition	John Wiley and Sons, 2001
Fred Halsall	Multimedia Communications, Applications Networks Protocols and Standards		Pearson Education, Asia 2002
Reference Books:			
Mark Nelson	Data Compression Book		Publication 1992
Watkinson J	Compression in Video and Audio		Focal Press, London, 1995

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB
Syllabus of B. Sc. Cyber Security
(Effective for 2020-2021 Admission Session)
Choice Based Credit System
140 Credit (3-Year UG) MAKAUT Framework
w.e.f 2020-21

- **DSE 2: Introduction to AI and Machine Learning**
- **Code: CYS 504(B) & 594(B)**
- **Course Objective:**

1.	Gain a historical perspective of AI and its foundations
2.	Become familiar with basic principles of AI toward problem solving, inference, perception, knowledge representation, and learning.
3.	Investigate applications of AI techniques in intelligent agents, expert systems, artificial neural networks and other machine learning models.
4.	Experience AI development tools such as an 'AI language', expert system shell, and/or data mining tool.
5.	Experiment with a machine learning model for simulation and analysis.
6.	Explore the current scope, potential, limitations, and implications of intelligent systems

Sl. No.	Course Outcome	Mapped Module
1.	Explain Artificial intelligence fundamentals	M1
2.	Make use of Machine learning	M2
3.	Discuss Human language technologies	M3
4.	Assess Intelligent Systems for Pattern Recognition	M4
5.	Examine Smart applications and Robotics	M5

Table(CYS 504B):-

Module Number	Content	Total Hours	%age of questions	Blooms Level	Remarks
1	Artificial intelligence fundamentals	10	20	1	
2	Machine learning	10	20	1,2	
3	Human language technologies	10	20	2,3	
4	Intelligent Systems for Pattern Recognition	8	10	2,3	
5	Smart applications and Robotics	10	10	3,4	
		48	100		

Table(CYS 594B) :-

Module Number	Content	Total Hours	%age of questions	Blooms Level	Remarks
5	Smart applications and Robotics using Prolog	14	50	3,4	

5	Smart applications and Robotics using Lisp	14	50	3,4	
		28	100		

Module 1: Artificial intelligence fundamentals

A.I. systems integrating approaches and methods.- Advanced search- Constraint satisfaction problems - Knowledge representation and reasoning - Non-standard logics - Uncertain and probabilistic reasoning (Bayesian networks, fuzzy sets).- Foundations of semantic web: semantic networks and description logics. - Rules systems: use and efficient implementation.- Planning systems

Module 2: Machine learning

Computational learning tasks for predictions, learning as function approximation, generalization concept. - Linear models and Nearest-Neighbors (learning algorithms and properties, regularization). - Neural Networks (MLP and deep models, SOM). - Probabilistic graphical models. - Principles of learning processes: elements of statistical learning theory, model validation. - Support Vector Machines and kernel-based models.

- Introduction to applications and advanced models. Applicative project: implementation and use of ML/NN models with emphasis to the rigorous application of validation techniques

Module 3: Human language technologies

Formal and statistical approaches to NLP. Statistical methods: Language Model, Hidden Markov Model, Viterbi Algorithm, Generative vs Discriminative Models Linguistic essentials (tokenization, morphology, PoS, collocations, etc.). Parsing (constituency and dependency parsing).Processing Pipelines. Lexical semantics: corpora, thesauri, gazetteers. Distributional Semantics: Word embeddings, Character embeddings. Deep Learning for natural language.

Applications: Entity recognition, Entity linking, classification, summarization.

Opinion mining, Sentiment Analysis. Question answering, Language inference,

Dialogic interfaces. Statistical Machine

Translation. NLP libraries: NLTK, Theano, Tensorflow

Module 4: Intelligent Systems for Pattern Recognition

Particular focus will be given to pattern recognition problems and models dealing with sequential and time-series data-Signal processing and time-series analysis-Image processing, filters and visual feature detectors-Bayesian learning and deep learning for machine vision and signal processing-Neural network models for pattern recognition on non-vectorial data (physiological data, sensor streams, etc)-Kernel and adaptive methods for relational data-Pattern recognition applications: machine vision, bio informatics, robotics, medical imaging, etc.-ML and deep learning libraries overview: e.g. scikit-learn, Keras, Theano

Module 5: Smart applications and Robotics

Common designs for smart applications examples: fuzzy logic in control systems or cloud analysis of field sensors data streams Make or buy: selecting appropriate procurement strategies example: writing your own RRN architecture vs. using cloud services

Development platforms for smart objects examples: Brillo (IoT devices) or Android TV (Smart TVs)

Development platforms for smart architectures examples: TensorFlow (server-side RNNs), or the Face Recognition API (mobile) Cloud services for smart applications examples: Google Cloud

Machine Learning API, Google Cloud Vision API, Google Cloud Speech API, or Deploying Deep Neural Networks on Microsoft Azure GPU VMs
Deployment and operations examples: cloud hosting vs. device hosting, or harnessing user feedback to drive improvement
Measuring success: methods and metrics examples: defining user engagement and satisfaction metrics, or assessing the naturalness of smart interactions
Introduction to robotics: main definitions, illustration of application domains-Mechanics and kinematics of the robot- Sensors for robotics-Robot Control-Architectures for controlling behaviour in robots-Robotic Navigation-Tactile Perception in humans and robots-Vision in humans and robots-Analysis of case studies of robotic systems-Project laboratory: student work in the lab with robotic systems

Suggested Reading:

Name of Author	**Title of the Book**
Stuart Russell and Peter Norvig	Artificial Intelligence: A Modern Approach
Nils J Nilsson	Artificial Intelligence: A New Sythesis
Negnevitsky	Artificial Intelligence
Akerkar Rajendr	Intro. to artificial intelligence
Anand Hareendran and Vinod Chandra	Artificial Intelligence and Machine Learning