CE/CZ 4001 – Virtual and Augmented Reality

Course Code	CE/CZ 4001							
Course Title	Virtual and Augmented Reality							
Pre-requisites	CZ 2003: Computer Graphics and Visualization							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	24	TEL	0	Tutorials	12	Student presentations	3

Course Aims

Virtual and augmented reality is becoming a powerful technology for engineers to design and implement applications ranging from manufacturing and medical to media and entertainment. Virtual reality refers to techniques that build imaginary worlds in computers. Augmented reality adds cues by overlaying computer-generated images onto the real world. An understanding of the hardware, software and algorithms for virtual and augmented reality allows engineers like you to push the limits of the technology and develop useful applications.

The prerequisite of this course is CZ2003 Computer Graphics and Visualization, which covers fundamentals of 3D modelling and animation.

Intended Learning Outcomes (ILO)

Each lecture module contains the motivation, fundamentals and mathematical background, hardware, software and algorithms in virtual and augmented reality. Practical problems with their solutions will be studied in tutorials. You will gain hands-on experiences through the laboratory assignments. Upon the successful completion of this course, you shall be able to:

1. Explain what is virtual and augmented reality and how it can simulate and interact with the real-world;
2. Identify typical problems associated with virtual and augmented reality;
3. Describe some examples of real-world applications;
4. Design and implement a working system using available tools based on the concepts and mathematics learnt in this course

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)	Presentations (Hours)
1	**Virtual Reality Platform** Project Window; Scene View; Hierarchy Window; Inspector Window; Game View	2	1	0
2	**Graphics** Primitive Shapes, Transforming Shapes; Controlling Appearance with Materials; Lighting, Camera; Shader, Texture; Particle System	2	1	0
3	**Physics** Rigidbody; Colliders; Joints; Character Controllers; Physics Debug Visualization	2	1	0
4	**Animation** Workflow and Setup of Animations: Objects, Characters, Properties; Animation Clips; Humanoid Animation Retargeting	2	1	0
5	**Navigation** Inner Workings; Building NavMesh: Surface Modifier, Volume, Link; NavMesh Agent; NavMesh Obstacle; Creating Off-mesh Link; Building Hight Mesh, Navigation Area and Cost	2	1	0
6	**Particle System** Unified representation for rigid objects, deformable objects, liquid, gas, and cloth; Dynamics	2	1	0
7	**eLearning** Project Development	2	1	0
8	**Introduction to Augmented Reality** Definition and challenges; introduction to augmented reality engine; case study of a specific engine, e.g. ARToolKit.	2	1	0
9	**Displays for Augmented Reality** History; augmented reality display technologies; head-mounted displays; hand-held displays; spatial displays; perceptual issues.	2	1	0
10	**Tracking, Recognition and Registration** Tracking techniques: sensor-based, video-based, hybrid; recognition: feature detection and matching; calibration and registration: projection methods.	2	1	0
11	**Rendering and Augmentation** Geometric model and transformations; rendering framework; augmentation; interaction.	2	1	0
12	**Examples of Augmented Reality System** Example systems to link augmented reality concepts to real-world applications; challenges.	2	1	0

13	**Project Presentation**	0	0	3
	Check for Hours	24	12	3

Assessment (includes both continuous and summative assessment)

a) Final Examination: 60%
b) Project written report: 20%
c) Project oral presentation: 20%

CE/CZ 4003 – Computer Vision

Course Code	CE/CZ 4003							
Course Title	Computer Vision							
Pre-requisites	NIL							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	13	Laboratories	-

Course Aims

This course aims to introduce you basic concepts and technologies of computer vision, and develop skills to implement widely used algorithms to process real vision tasks. This course presents you with digital image acquisition, representation, processing, recognition, and 3D reconstruction, to gain understanding of algorithm/system design, analytical tools, and practical implementations of various computer vision applications. You will be equipped with fundamental knowledge, practical skills and the insights for future development in this area.

Intended Learning Outcomes (ILO)

Upon the successful completion of this course, you shall be able to:

1. Describe the fundamental computer vision concepts;
2. Explain the advantages and disadvantages of the common computer vision techniques;
3. Implement the basic computer vision algorithms;
4. Apply computer vision techniques to solve simple real problems.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)
1	Introduction to computer vision **Background and applications;**	1	
2	Principles of Camera Systems **Imaging systems, basic thin-lens optics, digitization, image representation;**	2	1
3	Image Enhancement in the Spatial domain **Histogram operations, linear and nonlinear filtering;**	3	2
4	Image Enhancement in the Frequency domain **Fourier transform, low-pass, high-pass and band-pass filters;**	3	2
5	Colour **Basics of colour;**	2	1
6	Edge Processing **Edge representations, edge filtering, Canny edge detection, Hough transform;**	3	1
7	Region Processing **Region representations, thresholding, texture-based segmentation;**	3	2
8	Imaging Geometry **3D Coordinate Systems, camera perspective projection, camera parameters and calibration;**	3	1
9	3D Stereo Vision **Parallax and 2D triangulation, appearance-based matching and feature-based matching, 3D reconstruction;**	3	1
10	Object Recognition **Supervised and unsupervised learning, bag-of-words model for general object recognition;**	3	2
	Check for Hours	**=26**	**=13**

Assessment (includes both continuous and summative assessment)

a) Final examination: 60%
b) Project 1: 20%
c) Project 2: 20%

CE/CZ 4013 – Distributed Systems

Course Code	CE/CZ 4013							
Course Title	Distributed Systems							
Pre-requisites	CE/CZ 2005: Operating System CE 3005: Computer Networks OR CZ 3006: Net-Centric Computing							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	13		

Course Aims

This course aims to develop your understanding of the basic architectures, algorithms and design principles of distributed computing systems, and how they meet the demands of contemporary distributed applications.

This course provides an introductory but broad perspective of distributed systems, and is relevant for anyone pursuing a career in the IT/ICT industry – including those in product design and development, network/system administration, as well as, given the proliferation of IT in all walks of our lives, in executive roles across industries and government.

Intended Learning Outcomes (ILO)

This course introduces distributed systems at an elementary level. Upon the successful completion of this course, you shall be able to:

1. Explain the fundamental concepts and main features of distributed systems.
2. Describe the architectures of distributed systems.
3. Describe the functions of software components and common services to support distributed applications.
4. Analyse and apply the basic distributed algorithms.
5. Apply key design principles to an implementation of distributed system.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)	
1	Characteristics of distributed systems and system models Fundamental characteristics of distributed systems, resource sharing, issues and problems in distributed systems, architecture models, fundamental models.	3	1	
2	Interprocess communication Transport services, external data representation, marshalling and unmarshalling, request-reply protocol over UDP, request-reply protocol over TCP.	2	1	
3	Distributed objects and remote invocation Distributed object model, architecture of remote method invocation, Java RMI.	2	2	
4	Distributed file systems **Distributed file system requirements, Sun network file system, Andrew file system, Coda file system.**	3	1	
5	Peer-to-peer systems **Introduction to P2P systems and applications, unstructured P2P file sharing, structured DHT systems.**	3	1	
6	Name services **Names, name services, Domain Name System.**	2	1	
7	Time and global states **Clock synchronization algorithms, logical time, logical clocks, vector clocks, global states, distributed debugging.**	4	2	
8	Coordination and agreement **Distributed mutual exclusion algorithms, election algorithms, consensus problems.**	3	2	
9	Replication and consistency **Benefits of replication, requirements of replication, consistency models, consistency protocols.**	4	2	
	Check for Hours	=26	=13	

Assessment

a) Final Examination: 60%
b) Course Project: 40%

CE/CZ 4015 – Simulation and Modelling

Course Code	CE/CZ 4015							
Course Title	Simulation and Modelling							
Pre-requisites	CE/CZ 1007: Data Structures CE/CZ 1011: Engineering Maths I							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	13	Laboratories	8

Course Aims

Modelling and Simulation (M&S) course aims to equip you with one of the most important techniques to study real-time complex systems. M&S is an essential tool in many areas of science and engineering and has many applications, ranging from system analysis, decision support, to virtual environments. Thus, this course will introduce some fundamental techniques in M&S and build an understanding of the systems and tools of this field.

This course provides an introduction to system simulation and modelling techniques for complex dynamic systems. While the focus of this course is on how to analyze complex systems using computer simulation, some basic mathematical techniques will also be discussed. Various modelling, simulation and performance analysis techniques of complex systems will be discussed in this course with the emphasis on discrete event systems.

Intended Learning Outcomes (ILO)

Upon the successful completion of this course, you shall be able to:

1. Determine the properties of different types of physical systems and different types of simulations that are suitable to analyze their behaviors;
2. Analyze data collected from real world and build input models for simulation studies;
3. Conduct various simulation studies to investigate the behaviors of complex systems;
4. Conduct statistical analysis of the simulation outputs; and
5. Analyze discrete event systems through the competent use of computer simulation methods and mathematical modeling techniques.

Course Content

S/N	Topics	Lecture Hours	Tutorial Hours
1	**Introduction** Nature of simulation, The concept of systems, models and simulation, Steps in a good simulation study,	1	1
2	**Different Types of Simulation** Monte Carlo simulation, Continuous system simulation, Discrete event simulation, Simulation clock, Time advance mechanisms	3	1
3	**Simulation World View and Simulation Software** Event-scheduling world view, Process-interaction world view, General purpose programming language vs. simulation software	3	1
4	**Basic Probability and Statistical Models for Simulation** Random variable, PDF, Mean, Variance, Correlation, The Law of large numbers, Central Limit Theorem, Sampling, Confidence interval, Statistical tests.	2	1
5	**Random Numbers and Random Variate Generation** Middle-square method, LCG, Inverse Transform, Convolution, Composition, Acceptance-rejection,	3	2
6	**Input Modelling** Data collection, Identifying the distribution with data, MLE, Goodness-of-fit tests (Chi-Square Test, Kolmogorov-Smirnov test), Arrival process	3	2
7	**Verification and Validation of Simulation Models** Basic concepts, Verification techniques, Calibration and validation of models	2	1
8	**Output Analysis**	2	1

	Output analysis for terminating simulations, Output analysis for steady-state simulations, Variance Reduction Technique - Antithetic variates		
9	**Comparison of Alternative Designs** Pair-t approach, Multiple comparison problem, Variance Reduction Technique - Common random numbers	2	1
10	**Queueing Models** Basic properties, Performance measures, Kendall notation, Little's Law, Analysis of M/M/1 system	3	2

Assessment (includes both continuous and summative assessment)

a) Final Examination: 60%
b) Practical Lab Assignment: 25%
c) Written Assignment: 10%
d) Presentations/Discussions: 5%

CE/CZ 4016 – Advanced Topics in Algorithms

Course Code	CE/CZ 4016							
Course Title	Advanced Topics in Algorithms							
Pre-requisites	CZ/CE 2001: Algorithms							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	24	TEL	0	Tutorials	11	Quizzes	4

Course Aims

This course aims to develop your ability to identify key structural components in algorithms, problems and domains alike, and to exploit them to create provably computationally efficient solutions. This course builds on basic skills obtained in the prerequisite "Algorithms" course to broaden the range of analysis techniques that you use; provide you with intricate, elegant and actionable algorithmic design patterns; and develop your skill in exploiting salient problem features to facilitate computation.

Algorithms and designs presented in this course were at the beginning of multiple disciplines that now dominate the IT industry, and serve as a stepping stone for your further development for such roles as an algorithms engineer/developer or an applied researcher in computer technologies.

Intended Learning Outcomes (ILO)

This course equips you with additional techniques for algorithmic performance analysis, performance speedup, and algorithm construction based on domain structure or salient features. Upon the successful completion of this course, you shall be able to:

1. Analyse, classify and compare algorithms and problems from the computational effort point of view;
2. Exploit recurring, dynamic and geometric problem structures to facilitate computation;
3. Recognise limitations of exact computational methods, and exploit the benefits of error tolerance.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)	Quizzes (By reference,1h each)
0	Overview Brief overview of concepts and associated problems. Drivers and motivation, including practical links, for principles covered by the course.	1	0	
1	Analysis Techniques Asymptotic bounds on performance of a given algorithm. Solving recurrences, substitution method, iteration method, master theorem for recurrence equations.	2	0.5	QZ-1
2	Lower Bounds Bounds on unspecified algorithms for a given problem. Lower bounds on search and sorting by comparison.	2	0.5	QZ-2
3	NP-completeness Problem classes, and their associated computational complexity. P and NP, decision and optimisation problems, reductions and reducibility, NP-hardness and NP-completeness.	3.5	1	QZ-2
4	Dynamic Programming Exploiting problem sub-structure to facilitate computation. Optimal sub-structure and memorization, sub-problem dependency graph. Dynamic programming instances as design patters: longest common subsequence, optimal matrix multiplication, rod-cutting-style variations.	3	1	QZ-3
5	Search Techniques Ad-hoc search methods and heuristics antecedent. Backtracking and branch-and-bound. Knapsack and assignment problem design pattern.	2	1	QZ-3

6	Computational Geometry Exploiting geometric embedding of a problem. Polygon triangulation, convex hulls in two dimensions, motion planning. Mathematical primer on convexity.	3.5	1	QZ-4
7	Min-Cut/Max-Flow Exploiting problem embedding as a commodity flow in a graph. Fold-Fulkerson method, and Edmonds-Karp variation. Maximum bipartite matching, additional applications as design patterns.	3	1	QZ-4
8	Approximation Algorithms and Heuristics Exploiting error tolerance to facilitate computation. Heuristic (ad-hoc) vs approximate (error bound) algorithms. Approximate solutions to TSP, set covering, knapsack and scheduling as design patterns.	2	1	
9	Randomized Algorithms Monte Carlo and Las Vegas randomisation style of algorithms. Randomised Quicksort, hashing and Bloom filters, string matching.	2	1	
10	Material review Extended Q/A sessions, presentation of examples that require a combination of techniques.		3	
	Check for Hours	=24	=11	=4

Assessment (includes both continuous and summative assessment)

a) Final Examination: 50%
b) Written Quizzes (4 x 1h): 50%

CE/CZ 4021 – Pervasive Networks

Course Code	CE/CZ 4021							
Course Title	Pervasive Networks							
Pre-requisites	NIL							
No of AUs	3							
Contact Hours	Lectures	13	TEL	13	Tutorials	10		

Course Aims

The objective of this course is to introduce you to different types of wireless network technologies and some important mobile services and applications to support pervasive computing. The subject consists of two complementary components, i.e., wireless network protocol and mobility management. In the wireless network protocol part, various protocols in different layers designed to support wireless data transfer will be presented. In the mobility management, the required mechanisms to support data transfer with users' mobility will be discussed. After attending this course, you should be able to address the various technical challenges associated with wireless networking by solving such challenges using the principles learned. In addition, you should be able to solve issues related to location management, and mobile multimedia services. The concepts covered in this course are particularly important for those working in fields such as mobile phone-related services, wireless apps development and location-based services.

Intended Learning Outcomes (ILO)

Upon the successful completion of this course, you should be able to:

1. Design protocols for different network environments by applying concepts of different wireless technologies in pervasive networks
2. Solve handover problems in cellular mobile environments
3. Conduct performance analysis of the pervasive networks using hexagonal coordinate system and calculus-based mathematical models

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)
1	Introduction to Pervasive and Wireless Networks Special features of wireless networks; Effects of mobility; Various Network Topologies; Various types of Networks including cellular, WLAN, MANETs, WSNs, and WMNs	3	1
2	Medium Access Control Fixed assignment techniques: Frequency-division multiple access (FDMA) Time-division multiple access (TDMA) Spread-spectrum multiple access (SSMA) Frequency-hopped spread-spectrum (FHSS) Direct-sequence spread-spectrum (DSSS) / Code-division multiple access (CDMA) Space-division multiple access (SDMA) Random access (RA) techniques: Packet-radio techniques (PR) Controlled random access: Combination of fixed assignment and RA Use RA to obtain fixed resources	7	2
3	Routing in Ad Hoc, Sensor and Mesh Networks Characteristics of ideal routing Protocol; Classification based on various criteria; Protocols studied: DSDV,DSR,AODV,LAR,OLSR, CGSR	4	2
4	Fundamentals of Cellular Network Cellular System Architecture, Frequency Reuse Concept, Hexagon Geometry, Co-Channel Interference Capacity Expansion Techniques	5	2
5	Mobility Management in Cellular System Location Management: Static Location Update and dynamic Location Update; Handoff Management: Different decision algorithms, Handoff within MSC, Handoff over different MSCs	4	2
6	Mobile IP Basic principle of Mobile IP functions; Triangular routing and it's solution; Techniques supporting fast handoff in Mobile IP	3	1

	Check for Hours	=23	=10	

Assessment (includes both continuous and summative assessment)

a) Final Examination: 60%
b) Take home assignment: 25%
c) Quiz: 15%

CE/CZ 4022 – Personal Mobile Networks

Course Code	CE/CZ 4022							
Course Title	Personal Mobile Networks							
Pre-requisites	CE 3005: Computer Networks CZ 3006: Net-Centric Computing							
No of AUs	3							
Contact Hours	Lectures	26	TEL	-	Tutorials	13	Laboratories	-

Course Aims

This course builds upon the foundation network knowledge gained from core courses on Computer Networks (CE3005) or Net-Centric Computing (CZ3006). It aims to introduce both Computer Engineering and Computer Science students to the realm of mobile communications made possible through wireless technologies. It provides a straightforward and broad survey of wireless voice and data network standards and technologies available today for personal communications. It is designed for those of you taking an entry-level wireless technology course or seeking better knowledge of wireless communications and networks. The topics include the technologies being exploited in Bluetooth to Wi-Fi to cell phones to satellite communications. Wireless mobile communication systems including wireless personal networks (WPAN), wireless local area networks (WLAN), wireless wide area networks (WWAN) would also be introduced. This course will complement CE/CZ4021 Pervasive Networks.

Intended Learning Outcomes (ILO)

By the end of this course, the student would be able to:

1. Describe, explain and evaluate the fundamental components and technologies of wireless mobile communication systems.
2. Describe, explain, discuss and analyse the requirements of, as well as issues and challenges on mobile communication systems.
3. Describe, explain, discuss and analyse the effects of mobility on the communication system and how the impacts and impairments can be alleviated and resolved.
4. Factor, analyse and evaluate the various issues, techniques and technologies in the design and development of mobile applications and communication networks.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)
1	**Fundamentals of Wireless Mobile Communications** Fundaments of wireless communication systems: enabling concepts and challenges; components of a wireless communication system; radio frequency transmission, data and carrier signal components; channel bandwidth and data rate; signal propagation (SNR, attenuation, multipath distortion, noise), data transmission (modulation, common channel models, fading mitigation, spread spectrum, multiple access – FDMA, TDMA, CDMA).	9	4
2	**Overview of Mobile Networks** Introduction to different types of mobile networks eg. WPAN, WLAN, WWAN, Ad Hoc networks, MANETS, Meshed networks, vehicular networks, sensor networks etc.	1	1
3	**Wireless Personal Area Networks (WPAN)** Bluetooth applications, classes, network topology, standards, transmission. Introduction to ZigBee, Near Field Communication (NFC), Wearable Technologies, Body Area Networks (BAN).	3	1
4	**Wireless Local Area Networks (WLAN)** IEEE 802.11 standards; WLAN modes; Media Access Control; MAC Layer Operations; Transmission Technology; Wireless Propagation Problems; Wifi Mesh System, Wifi Range Extender, Applications.	6	3
5	**Wireless Wide Area Networks (WWAN)** Cellular communications network: network components; Switching Technology; Organization; Channel reuse; Mobility Management, Handoff; Roaming; Generations of Cellular Technologies. Satellite communications network: Transmission, Service and Type, Satellite Systems, Applications eg. GPS, DGPS, Wifi in flight	6	2
6	**Revision**	1	2
	Check for Hours	=26	=13

Assessment (includes both continuous and summative assessment)

a) Quiz/Quizzes: 40% (if 2 quizzes) to 20% (if 1 quiz)
b) Assignment: 0% (if no assignment) to 20%
c) Final Examination: 60%

CE/CZ 4023 – Advanced Computer Networks

Course Code	CE/CZ 4023							
Course Title	Advanced Computer Networks							
Pre-requisites	CE 3005: Computer Networks, or CZ 3006: Net-Centric Computing							
Pre-requisite for	Nil							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	10	Example class	0

Course Aims

Building upon earlier courses (CE3005 or CZ3006), this subject aims to bring you into the realm of real inter-networking. The subject consists of two complementary components. On one hand, several application layer protocols are to be explained, along with their requirements on the underlying networks. One the other hand, practical network design and management methodologies will be introduced; they aim at meeting the application requirements. Emphasis is mostly placed on the practical use and construction of networks, with a bias toward multimedia applications. Advanced materials, such as, peer-to-peer networking will also be covered to prepare you well for your future career in advanced computer networks.

Intended Learning Outcomes (ILO)

Upon the successful completion of this course, you shall be able to:

1. Identify and explain several application layer protocols and what they may demand from the underlying networks.
2. Identify and explain networks design and management to satisfy various application requirements
3. Conduct quick protocol performance analysis and making critical design decisions
4. Design a network to support a given set of requirements

Course Content

	Topics	Lectures (Hours)	Tutorials and/or Example Classes (Hours)
1	**Top-Down View of Computer Networks** Recapitulate the concepts, emphasizing on the Internet structure (edge, core, access), as well as multiplexing, fragmentation, and delay.	2	1
2	**Application Layer Protocols** Concepts of Application layer protocols; Application layer protocols such as HTTP and SMTP; Network management architecture and protocols (e.g., SNMP); Peer-to- protocols.	6	3
3	**Multimedia Networking** Multimedia applications; Voice-over-IP; Session protocols (e.g. SIP and H.323); Real-Time Streaming Protocol (RTSP), Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP).	5	2
4	**Advanced Network Protocols** Multi-protocol Label Switching (MPLS) protocols; IP Multicasting architecture and protocols.	3	2
5	**QoS and Traffic Management** Quality of Services (QoS) requirements, Best-effort service, Integrated services, Differentiated services. Introduction to traffic management techniques, Connection Admission Control, Traffic Shaping and Policing, and Scheduling.	6	3
6	**Network Deployment and Design** Practical issues in designing commonly used computer networks, ranging from home network to enterprise networks. Some focuses will be given to design wireless networks or hybrid wired-wireless networks.	4	2
		=26	=13

Assessment (includes both continuous and summative assessment)

a) Final Examination: 60%
b) Take home assignment: 20%
c) Take home assignment: 20%

CE/CZ 4024 – Cryptography and Network Security

Course Code	CE/CZ 4024							
Course Title	Cryptography and Network Security							
Pre-requisites	CE 3005: Computer Networks or CZ 3006: Net Centric Computing							
No of AUs	3							
Contact Hours	Lectures	26	TEL	-	Tutorials	13	Lab	-

Course Aims

This course aims to develop your ability to understand how basic cryptographic algorithms work and identify the problems associated with the application of cryptography in real-world security systems, and explain the pros and cons of various cryptographic mechanisms.

This course provides an introduction to basic cryptographic algorithms, along with the underlying mathematical foundations guiding the design of aid algorithms, and explores the usage of these primitives in real world applications, particularly applied to network security.

Intended Learning Outcomes (ILO)

This course provides an understanding of cryptography and network security at an introductory level. Upon the successful completion of this course, you shall be able to:

1. Apply the theoretical (mathematical) tools that form the basis of cryptographic algorithms;
2. Explain and analyze the design of cryptographic algorithms;
3. Identify the typical problems associated with the application of cryptography in real-world systems;
4. Explain the security issues in a Cyberspace environment;
5. Explain the design decisions behind a secure network architecture plan;
6. Design basic secure network strategy based on a combination of cryptographic and network security control mechanisms

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)
1	Introduction Concepts and terminology. Drivers and motivations for cryptographic techniques (what is cryptography, and why is it necessary.) Provide a historical perspective of cryptography, and discourse various related concepts of symmetric cipher, asymmetric cipher, key management and cryptanalysis.	2	1
2	Mathematical Background Finite field theory: modular arithmetic, Euclid algorithm, Galois field; Number theory: prime numbers, Miller-Rabin primality test, Chinese remainder theorem, discrete logarithm.	4	3
3	Secret-Key Cryptography Block cipher: DES, 3DES, AES; Modes of operation: ECB, CBC, CFB, etc; Stream cipher.	3	1
4	**Public Key Cryptography** Public key algorithm: RSA; Digital signatures; Elliptic Curve Cryptography (ECC).	3	1
5	**Hash Functions and MACs** Hash functions: MD5 and SHA, birthday attack; Message Authentication Codes (MAC): HMAC, CMAC.	3	1
6	**Key Management** Security requirement of cryptographic keys, Key generation, key storage, tamper-resistant hardware, Public key certificates, PKI.	3	2
7	Distributed Authentication Security requirement of inter-process communication, challenge-response authentication, Needham-Schroeder Protocol, Diffie-Hellman Key Exchange, ISO/IEC 9798 Entity Authentication	4	2

8	Secure Network Architecture Closed-System Security vs Open-System Security, Multi-tier network security architecture, Defence-in-depth, Perimeter Network, SCADA network, Internet banking network.	4	2
	Check for Hours	=26	=13

Assessment (includes both continuous and summative assessment)

a) Final Examination: 50%
b) Quiz-1: 25%
c) Quiz-2: 25%

CE/CZ4031 - Database System Principles

Course Code	CE/CZ 4031							
Course Title	Database System Principles							
Pre-requisites	CE/CZ 2001: Algorithms CZ 2007: Introduction to Databases							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	13	Student presentations	0

Course Aims

Database management systems (DBMS) are designed to manage large and complex data sets. The fundamentals of the implementation of database management systems must be understood by all Computer Science students. This will help students to develop and design software systems utilizing databases, and equip students with the knowledge of managing data of large scale. Moreover, this should be understood by current and future business leaders so that they can offer strategic guidance based on an informed understanding of database business capabilities. This course provides the basis for achieving this goal.

Intended Learning Outcomes (ILO)

This course introduces the basic concepts and methods of implementing a data management system. Upon the successful completion of this course, you shall be able to:

1. Discuss the importance of, and uses for, databases within organizations.
2. Explain how a relational database is implemented.
3. Describe the principles behind commercial databases and how to manage a relational database system.
4. Communicate knowledgeably about data management using professional language

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)	Presentations (Hours)
1	Overview of Database Management Systems (DBMS): DBMS Architecture, Relational DBMS.	1	0	0
2	Storage of Relational Data Memory Hierarchy, Disks, Representing Relations in Disks, Using Secondary Storage Effectively, How to Move Data to Memory	3	2	0
3	Indexing Techniques Indexes on Sequential Files, Secondary Indexes, B-Trees, Hashing, Multi-dimensional Indexes (R-Trees, kD Trees)	7	4	0
4	Query Processing One-Pass Algorithms, Nested-Loop Joins, Two-Pass Algorithms based on Sorting and Hashing, Index-Based Algorithms, Algebraic Laws	5	2	0
5	Query Optimization Introduction to Physical Query Plan Operators, Logical Query Plans, Physical Query Plans, Join Ordering.	4	2	0
6	Failure Recovery Modelling Resilient Operations, Undo/Redo Logging, Checkpoint, Recoverability, Recovery process	2	1	0
7	Transaction Management and Concurrency Control Transactions, Serial and Serializable Schedules, Conflict-Serializability, Locking, Resolving Deadlocks.	4	2	0
	Check for Hours	=26	=13	0

Assessment

a) Final Examination: 50%
b) Quizzes: 20%
c) Assignments: 30%

CE/CZ 4032 – Data Analytics and Mining

Course Code	CE/CZ 4032							
Course Title	Data Analytics and Mining							
Pre-requisites	CE/CZ 2001: Algorithms							
No of AUs	3							
Contact Hours	Lectures	24	TEL	0	Tutorials	13	Student presentations	4

Course Aims

In the era of big data, large quantities of data are being accumulated. The amount of data collected is said to double every nine months. Seeking knowledge from massive data is one of the most desired attributes of Data Mining. In general, there is a huge gap from the stored data to the knowledge that could be construed from the data. This transition will not occur automatically, that is where Data Mining comes into picture. In Exploratory Data Analysis, some initial knowledge is known about the data, but Data Mining could help in a more in-depth knowledge about the data. Courses on Database systems give methods to extract information, but they fail to extract knowledge that is actionable.

Manual data analysis has been around for some time now, but it creates a bottleneck for large data analysis. Fast developing computer science and engineering techniques and methodology generates new demands. Data mining techniques are now being applied to all kinds of domains, which are rich in data. Although data mining is partly based on statistical methods, data mining methods give a lot more than the statistical methods. Data mining methods are to a large extent based on machine learning methods. The difference is data mining is meant for huge data whereas machine learning is usually done over relatively small-sized data. Huge data brings completely a new set of problems to be solved.

This course aims to introduce you to the exciting and ever-evolving world of data analytics and mining.

Intended Learning Outcomes (ILO)

This course introduces data mining at an elementary level. Upon the successful completion of this course, you shall be able to:

1. Discuss basic concepts and general knowledge of data analytics, data mining and the KDD process, using professional language associated with data analytics and data mining
2. Pre-process the data so that it can be analyzed further using sophisticated data analytics and mining algorithms
3. Discuss several major data mining tasks (including classification, clustering, and association rule mining, etc) and related algorithms to solve them
4. Apply data mining techniques to tackle real-world big data applications, to perform core data analytics & mining tasks with large amount of data.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)	Presentations (Hours)
1	**Introduction of Data Analytics & Mining** Overview of data mining and knowledge discovery, definitions of data mining and KDD, data sources, categories of data mining tasks, major issues in data mining.	2	1	0
2	**Data Pre-processing** Definitions, Types of data, Types of attributes, Data cleaning, integration, sampling, discretization and transformation, similarity and dissimilarity measures	2	2	
3	**Data Analytics & Visualization** Summary Statistics, Visualization, On-line Analytics Processing and Data Warehouse	4	2	
4	**Predictive Pattern Mining** Concepts and Techniques, Decision tree, Instance-based Classifiers, Support Vector Machines, Ensemble Classification, Predictive evaluation	6	3	
5	**Cluster Pattern Analysis** Concepts and techniques, Partition-based clustering (K-means clustering), Hierarchical clustering, Density-based based clustering, Clustering evaluation	6	2	
6	**Association Rule Mining** Concepts and techniques, Frequent itemset generation, Rule generation, A-priori algorithm, FP-Growth algorithm	4	2	
7	**Anomaly Detection** Definitions and concepts, Statistical approaches, Proximity-based outlier detection, Density-based outlier detection, Clustering-based techniques	2	1	
	Check for Hours	=26	=13	=0

Assessment (includes both continuous and summative assessment)

a) Final Examination: 50%
b) Course written report and presentation: 50%

CE/CZ 4034 – Information Retrieval

Course Code	CE/CZ 4034							
Course Title	Information Retrieval							
Pre-requisites	CE/CZ 2001: Algorithms							
No of AUs	3							
Contact Hours	Lectures	23	TEL	0	Tutorials	8	Student presentations	0

Course Aims

This course aims to involve students in a technical way to understand and build information retrieval systems. They were expected to master the basic concepts and building blocks for information retrieval systems. In addition, applications in artificial intelligence were also introduced to get students acquainted with state of the arts.

Intended Learning Outcomes (ILO)

This course introduces information retrieval at an elementary level. Upon the successful completion of this course, you shall be able to:

1. List and explain each of the modules information retrieval system;
2. Code with necessary packages to build a preliminary search engine;
3. Describe and distinguish various retrieval systems;
4. Apply fundamental clustering, classification and web search techniques to solve problems, such as computations and designs.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)	Presentations (Hours)
1	Introduction to information system Course details and schedule. General introduction to definition and application to information system.	2	1	0
2	Boolean retrieval and tolerant retrieval Term-document incidence; Inverted index; Boolean query; Optimization; Tokenization; Linguistic analysis; Query.	4	1	0
3	Ranked retrieval Term-document count matrix; tf-idf; Vector space ranking.	3	1	0
4	**Efficient retrieval** Efficient vector space representation; Efficient cosine ranking; Computing the K largest cosine values; Parametric and zone indexes; Tiered indexes.	4	1	0
5	Enhancing Retrieval Evaluation, calculating F-measure; Options for improving results using global and local methods.	2	1	0
6	**Classification** Text classification; Techniques; Feature selection.	2	1	0
7	Clustering Document clustering; Clustering algorithms.	2	1	0
8	Web search and IR applications Web search; Link analysis.	4	1	0
	Check for Hours	=23	=8	0

Assessment (includes both continuous and summative assessment)

a) Final Examination: 50%
b) Assignment: 35%
c) Quiz: 15%

CE/CZ 4041 – Machine Learning

Course Code	CE/CZ 4041							
Course Title	Machine Learning							
Pre-requisites	CE/CZ 1011: Engineering Maths I CE/CZ 1007: Data Structures							
No of AUs	3							
Contact Hours	Lectures	22	TEL	0	Tutorials	10	Student presentations	6

Course Aims

This course provides an introductory but broad perspective of machine learning fundamental algorithms, and is relevant for anyone pursuing a career in AI or Data Science. It aims to provide you with the essential concepts and principles of algorithms in machine learning so that you can use various machine learning techniques to solve real-world application problems.

Intended Learning Outcomes (ILO)

This course introduces machine learning at an elementary level. Upon the successful completion of this course, you shall be able to:

1. Explain the motivations and principles behind various machine learning algorithms;
2. Apply or even design specific machine learning algorithms to solve real-world application problems;
3. Identify some state-of-the-art machine learning techniques.
4. Conduct research on machine learning.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)	Presentations (Hours)
1	**Introduction to Machine Learning** Overview of machine learning, supervised learning, unsupervised and applications	2	0	0
2	**Bayesian Classifiers** Bayesian decision theory, Naïve Bayes, Bayesian Brief Networks	4	2	0
3	**Decision Tree** Tree induction, prediction based trees, generalization errors	2	1	0
4	**Artificial Neural Networks** Perceptron, Multi-layer perceptron, backpropagation algorithm	2	1	0
5	**Support Vector Machines (SVMs)** Induction of SVMs, linear SVMs, Kernelized SVMs	1.5	1	0
6	**Regression Models** Linear regression, Kernelized regression	1.5	0.5	0
7	**K-Nearest Neighbor Classifiers (KNN)** KNN with majority voting, KNN with distance-weighted voting	1	0.5	0
8	**Ensemble Learning** Boosting, bootstrapping, model average	2	1	0
9	**Clustering** K-means clustering, hierarchical clustering, performance evaluation for clustering, applications	2	1	0

10	**Density Estimation** Parametric and non-parametric density estimation approaches	2	1	0
11	**Dimension Reduction** Principal component analysis (PCA), linear discriminant analysis (LDA)	1	1	0
12	**Application and Advanced Research Topics** Through course project on a predefined list of applications or research topics	0	0	7
	Check for Hours	=21	=10	7

Assessment (includes both continuous and summative assessment)

a) Final Examination: 60%
b) Course project presentation: 10%
c) Course project report: 30%

CE/CZ 4042 – Neural networks and deep learning

Course Code	CE/CZ 4042							
Course Title	Neural networks and deep learning							
Pre-requisites	CE/CZ 1003: Introduction to computational thinking CE/CZ 1007: Data structures CE/CZ 1011: Engineering mathematics I CE/CZ 1012: Engineering mathematics II							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	12	Student presentations	0

Course Aims

This course aims to provide you with a basic but comprehensive foundation of neural networks and deep learning, including underlying principles, architectures, and learning algorithms of various types of deep neural networks that are essential for future applications of artificial intelligence and data science.

Intended Learning Outcomes (ILO)

Upon the successful completion of this course, you shall be able to:

1. Interpret artificial neuron as an abstraction of biological neuron and explain how it can be used to build deep neural networks that are trained to perform various tasks such as regression and classification;
2. Identify the underlying principles, architectures, and learning algorithms of various types of neural networks;
3. Select and design a suitable neural network for a given application;
4. Implement deep neural networks that can efficiently run on computing machines.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)
1	**Introduction to neural networks** Biological neural networks, artificial neuron, activation functions, history of neural networks	2	1
2	**Regression** Gradient descent learning, stochastic gradient descent learning, linear neuron, linear regression, perceptron, perceptron learning algorithm	2	1
3	**Classification** Pattern recognition, discrete perceptron, discrete perceptron learning, logistic regression, learning a logistic neuron	2	1
4	**Neuron layers** Softmax layer, softmax learning algorithm, perceptron layers, learning algorithms	2	1
5	**Feedforward networks** Feedforward neural networks, multilayer perceptron, backpropagation algorithm, deep feedforward neural networks	2	1
6	**Model selection and overfitting** holdout method, K-split resampling technique, K-fold cross-validation, three-way data splits, overfitting and underfitting of neural networks, early stopping, regularization and weight decay, drop-outs	2	1
7	**Convolution neural networks (CNN)** Feature extraction by convolution, pooling of feature maps, convolutional neural networks, deep CNN, learning with momentum	2	1
8	**Recurrent neural networks (RNN)** Recurrent neural networks with hidden recurrence (Elman type) and with output recurrence (Jordan type), learning deep RNN	2	1
9	**Gated recurrent networks (GRN)** Vanishing and exploding gradient problem in RNN, memory cells and gating, long short-term memory (LSTM) units, gated recurrent units (GRU), sequence-to-sequence models	2	1
10	**Autoencoders** Learning of autoencoders, denoising autoencoders, sparse autoencoders, building stacked and deep autoencoders	2	1
11	**Restricted Boltzmann machines (RBM)** Energy based models, restricted Boltzmann machines, sampling in RBM, contrastive divergence	2	1
12	**Deep belief networks (DBN)** Unfolding RBM into deep belief networks, Layer-wise greedy learning, joint unsupervised training	2	1
13	**Revision**	2	
		=26	=12

Assessment (includes both continuous and summative assessment)

a) Final Examination: 50%
b) Project 1 (report and codes): 25%
c) Project 2 (report and codes): 25%

CE/CZ 4045 – Natural Language Processing

Course Code	CE/CZ 4045					
Course Title	Natural Language Processing					
Pre-requisites	CE/CZ 2001: Algorithms					
No of AUs	3					
Contact Hours	Lectures	26	TEL	0	Tutorials/Example classes	13

Course Aims

Natural language processing is becoming a very hot topic in both industrial practices and academic research. It finds many real-world applications such as information extraction, sentiment analysis, machine translation, question answering, and summarization. Hence, it is an important subject to prepare you to cope with the huge amount of unstructured information in text, for example, in web pages and business documents. This subject covers the basic concepts and computational methods for natural language processing. Techniques covered should be biased toward those generally accepted established traditional practices recommended by practitioners.

This course will equip you with the basic concepts and techniques in natural language processing on different levels including words, syntax, and semantics. You will be able to apply the techniques to real-world problems and conduct evaluations of your solutions.

Intended Learning Outcomes (ILO)

You will learn natural language processing at a basic level, establishing a solid understanding on the theory of morphological, syntactic, and semantic analysis. With that, you will gain skills to apply the NLP techniques to real-world problems by using NLP packages and toolkits.

Upon completion of the course, you should be able to:

1. Identify and analyse the linguistic characteristics of written English
2. Design and develop a NLP system to analyze and process a general corpus
3. Troubleshoot for domain-specific NLP applications

Course Content

	Topics	Lectures (Hours)	Tutorials/example classes (Hours)
1	**Regular expressions and Word-level Analysis** Introduction to NLP, Finite State Automata (Deterministic and Non-deterministic), Stemming, Tokenizing, Segmentation, Spelling Checking	3	1
2	**N-gram Language Model** Word Prediction, N-gram Language Models (Counting and basic concepts), Evaluation, Smoothing for Language Models	3	2
3	**Word Classes and Part-of-speech Tagging** Word classes, POS tagging, Hidden Markov Model and its Application to Part-of-speech Tagging, the Viterbi Algorithm	4	2
4	**Formal Grammars** Constituency, grammatical relations, subcategorization, phrase structure, dependency structure, context free grammar (CFG), dependency grammar	3	2
5	**Syntactic Parsing** Top-down parsing, bottom-up parsing, parse tree, CKY algorithm, Earley algorithm, syntactic ambiguities, probabilistic CFG, treebank, attachment ambiguities, lexicalized CFG	4	2
6	**Computational Semantics** First-order logic, model-theoretic semantics, representing linguistic concepts, semantic augmentation to CFG, compositional semantic analysis	3	1
7	**NLP Applications** Introduction to Classification Methods, Evaluation, Introduction to Sentiment Analysis (Concept and Basic Methods). Information extraction. Word sense disambiguation	3	2
8	**Machine Translation** Introduction to Machine translation (Alignment Models, Decoding)	2	1
9	**Review**	1	0
	Check for Hours	=26	=13

Assessment (includes both continuous and summative assessment)

a) Final Examination: 50%
b) Midterm quiz: 15%
c) Assignment: 35%

CE/CZ 4046 – Intelligent Agents

Course Code	CE/CZ 4046							
Course Title	Intelligent Agents							
Pre-requisites	None							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	13	Student presentations	0

Course Aims

Intelligent agents are a new paradigm for developing software applications and the focus of intense interest as a sub-field of Computer Science and Artificial Intelligence. Multi-agent systems arise when these agents co-exist, interact and cooperate with each other. Agents and multi-agent systems are being used in an increasingly wide variety of applications, such as personal assistants, e-commerce, traffic control, workflow and business process management systems, etc. This course will equip you with the skills and knowledge on the design and implementation of intelligent agents and multi-agent systems to solve large-scale, complex, and dynamic real-world problems.

Intended Learning Outcomes (ILO)

Upon the successful completion of the course, you should be able to:

1. Describe the variety of connotations that agent-based computation implies and describe how the field fits into Artificial Intelligence and more broadly, Computer Science.
2. Identify the typical problems associated with intelligent agents and multi-agent systems.
3. Describe and debate the ways for solving problems related to intelligent agents and multi-agent systems.
4. Analyse real world and (possibly) new problems related to intelligent agents and multi-agent systems, and propose and evaluate possible mitigations.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)	Presentations (Hours)
1	Introduction to Intelligent Agents What is an agent; Principles of autonomy and agency; Views of the field from different aspects: Software engineering/simulation/AI; Relationship with AI/distributed systems/game theory/social science	2	1	0
2	Deductive Reasoning Agents Symbolic research agents; Planning systems; Planning agents	3	1	0
3	Practical Reasoning Agents Intentions and practical reasoning; Means-end reasoning; A Procedural reasoning system	4	2	0
4	Reactive and Hybrid Architectures Reactive vs hybrid; Brooks subsumption architecture; Limitations and hybrid architectures	4	2	0
5	Introduction to Multi-Agent Systems and Applications Definition of multi-agent systems; Applications of intelligent agents and multi-agent systems; Some demos	2	0	0
6	Working Together Benevolent agents; Cooperative distributed problem solving; Contract Net; Task sharing and result sharing; Coordination	3	1	0
7	Multi-Agent Interaction Utilities and preferences, Payoff matrices; Solution concepts, Game Theory; Nash equilibrium; Prisoners Dilemma	2	2	0
8	Allocating Scarce Resources - Auctions Definition of auctions; Categorization of auctions; English auction; Dutch auction; First-price sealed bid auction; Vickrey auctions; Combinatorial auctions; Bidding languages; The VCG Mechanism; Some examples	2	2	0
9	Making Group Decisions Social Choice; Preference aggregation; Social Welfare; Voting procedures	2	1	0
10	Forming Coalitions Cooperative games; Computational and representational issues; Modular representations; Coalition games with goals; Coalition structure formation	2	1	0

	Check for Hours	=26	=13	0

Assessment (includes both continuous and summative assessment)

a) Final Examination: 60%
b) Course project: 40%

CE/CZ 4055 – Cyber Physical System Security

Course Code	CE/CZ 4055							
Course Title	Cyber Physical System Security							
Pre-requisites	CE/CZ 1006: Computer Organisation And Architecture							
No of AUs	3							
Contact Hours	Lectures	26	TEL	-	Tutorials	12	Laboratories:	3

Course Aims

Cyber physical systems are typically designed as a network of interacting elements with physical input and output, and are characterized by the interaction between the physical world (sensors, user inputs, actuators) and the cyber world (processing, decision making). Cyber physical systems are the driving force behind modern civilization, being integral part of technologies, such as additive manufacturing, smartcard-based payment, power delivery systems, drone-based operations, and smart home automation. Cyber physical systems are characterized by stringent performance requirements, such as, extremely low energy budget, small area footprint and often hard real-time constraints. Due to the pervasive nature of the cyber physical systems in our everyday lives, it also runs the risk of huge security hazards.

In this course, we will learn about the basics of cyber physical systems, including the design principles and methodologies. Further, there will be a detailed treatment of the security challenges for cyber physical systems, which vary in practice due to the diverse nature of the application environment of cyber physical systems. These different forms of security breaches, observed across diverse cyber physical systems, will be put in a well-characterized taxonomy, to be systematically identified as attack surfaces. The techniques to handle these attacks will be described in a generic manner, including key management and wireless/RFID communication. The attack surfaces and protection/mitigation principles will then be elaborated with practical case studies, from the representative cyber physical systems such as automotive, smart card systems and smart grid.

Intended Learning Outcomes (ILO)

Upon the successful completion of this course, you shall be able to:

1. Describe the basic concepts of cryptography are used for ensuring security of cyber-physical systems
2. Describe the basic design, architecture and design principles of cyber physical systems
3. Identify the sources of vulnerability in a cyber physical system systematically via attack surfaces
4. Determine how security is incorporated at different abstractions and at different components of cyber physical systems
5. Articulate the principles behind the detection and mitigation of attacks for different attack surfaces of a cyber-physical system
6. Compare and contrast practical cyber physical system security such as for smart grid, smart vehicle, and smart card systems
7. Determine the performance overheads to consider for incorporating security in a cyber-physical system

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)
1	**Basics of Cyber Physical System (CPS)** Examples of CPS (Avionics, Health, Grid, etc.), Design Principles, and Characteristics: Robustness, Real Time Constraints, Distributed Control, Human Intervention. Deployment: Wireless Sensor Nodes, Internet-of-Things (IoT), Practical Examples. Security Aspects.	4	1
2	**Basics of Security** Confidentiality, Integrity, Availability, Authenticity. Basics of Cryptography - symmetric-key algorithm, message authentication code, mode of operations, key diversification, Public Key Infrastructure (PKI) and Certificate Authority (CA), hash function and signature, authentication, fingerprint, certification, secured messaging, security token principle of the operation. Security challenges in cyber physical systems. Risk Assessment. CPS Security Characteristics.	4	2
3	**Attack Surfaces of Cyber Physical Systems** Attack surfaces based on network, distributed control, distributed storage, real-time constraints. Attack surfaces based on computing and communication. Hierarchy of vulnerabilities.	2	1
4	**Device-level Security** CPS Platforms. Security by Design. Microprocessor Security, Security Accelerators.	2	2
5	**Key Management in Cyber Physical Systems** Key generation system, key injection system, key management in distributed cyber physical systems, smart device personalization system with biometric security.	3	1
6	**Secure Communication in Cyber Physical Systems** Communication standards and performance requirements. Vulnerability issues in prominent communication protocols, Ethernet, SCADA, NFC.	3	2
7	**Cyber Physical System Security: Smart Cards** Smart cards (contact, contactless): Attack Surfaces, Attack Example: Side-channel Attack, Privacy Intrusion, Mifare RFID hack. Attack Detection and Mitigation.	3	1
8	**Cyber Physical System Security: Smart Grid** Smart grid overview: Attack Surfaces, Attack Example: GPS Spoofing, False Data Injection, and Deadline Violation. Attack Detection and Mitigation.	3	1
9	**Cyber Physical System Security: Smart Vehicle** Automotive systems overview: Attack Surfaces, Attack Example: LIDAR spoofing, Keeloq attack, Malware injection. Attack Detection and Mitigation.	2	1
	Check for Hours	= 26	= 12

Assessment (includes both continuous and summative assessment)

a) Final Examination: 50%
b) Quizzes: 20%
c) Project: 20%
d) Assignment: 10%

CE/CZ 4057 – Time-Critical Computing

Course Code	CE/CZ 4057							
Course Title	Time-Critical Computing							
Pre-requisites	CE/CZ 1006: Computer Organisation And Architecture CE/CZ 2005: Operating Systems							
No of AUs	3							
Contact Hours	Lectures	26	TEL	-	Tutorials	13	Laboratories:	5

Course Aims

Cyber-Physical Systems (CPS) are a large-scale network of computing systems characterized by their interaction with the physical world (sensors and actuators). CPS are the driving force behind modern civilization, being an integral part of technologies such as avionics including drones, autonomous vehicles, etc. These systems generally have ***hard real-time constraints*** that require the cyber components to process physical inputs and generate appropriate physical outputs within pre-defined temporal requirements. For example, think about obstacle detection and avoidance in autonomous vehicles. Such systems, also called ***time-critical computing systems,*** are the primary focus of this course.

In this course, you will learn the fundamental concepts of a Real-Time Operating System (RTOS). RTOS is the core software platform used in time-critical computing, just like an OS in a general-purpose computing system. You will learn RTOS techniques for processor scheduling, process synchronization, etc. You will also learn how such time-critical computing platforms are networked together using protocols that support real-time communication. Building on this foundation, you will also learn how to implement a time-critical system using a drone-based platform.

Intended Learning Outcomes (ILO)

Upon successful completion, you should be able to:

7. Describe and analyze the three fundamental RTOS concepts: processor scheduling, process synchronization and process budgeting.
8. Describe and analyze the fundamental concepts of real-time communication: bounded latency, priority-based scheduling and Time-Division Multiple Access (TDMA).
9. Describe how these concepts are realized in practice, and discuss the associated implementation trade-offs.
10. Describe and analyze how these concepts affect the design of a CPS application in terms of satisfying its real-time requirements.
11. Design and implement a CPS application with real-time requirements, making efficient use of RTOS and real-time network features.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)
1	**Basics of Cyber Physical Systems (CPS), Operating Systems (OS) and Networks** Definition and examples of CPS, computing and communication requirements for CPS (real-time, limited resources, etc.), CPS case-studies to understand requirements, introduction to OS (process concept, process scheduling, semaphores, deadlocks, priority-inversion), introduction to networks (OSI layer, TDMA).	3	1
2	**Worst-Case Execution Time Estimation (Process Budgeting)** Definition of Worst-Case Execution Time (WCET), components affecting WCET in a single-core processor, loop bounds, cache analysis, value analysis, implicit path enumeration technique (IPET).	4	2
3	**Processor Scheduling** Real-time workload model, fixed-priority scheduling (Rate Monotonic and Deadline Monotonic), dynamic-priority scheduling (Earliest Deadline First), scheduling extensions for multi-cores (partitioned and global), introduction to schedulability tests and their relevance in CPS.	4	2
4	**Resource-Sharing Protocols (Process Synchronization)** Key challenges for process synchronization in an RTOS, priority inheritance protocol, priority ceiling protocol, stack resource policy, challenges in extending these protocols to multi-cores, spin-locks for multi-cores.	3	2
5	**Introduction to a Commercial RTOS** Introduction to Micrium-OSIII/FreeRTOS, detailed review of scheduler and synchronization implementations.	2	1
6	**Real-Time Networking** Challenges in meeting real-time requirements in a distributed computing system, fundamentals of priority-based communication, introduction to commercial protocols Controller Area Network (CAN) and TTEthernet (Time-Triggered Ethernet).	4	2
7	**Case Study: Automotive real-time CPS** Introduction to Autoware (autonomous driving simulator), Texas Instruments Hercules Electronic Control Unit, cyber-system design (using CAN and FreeRTOS), implemented automotive applications (cruise control, steering control, collision avoidance), impact of different cyber-system design on application performance.	4	2
8	**Case Study: Drone-based (crazyflie quadcopter) real-time CPS** Introduction to crazyflie quadcopter, FreeRTOS-based design of control for drone operations.	2	1
	Check for Hours	=26	13

Assessment (includes both continuous and summative assessment)

a) Final Examination: 30%
b) Project: 45%
c) Literature Review: 10%
d) In-class activity (Quiz): 15%

Note: The final examination is closed book. The in-class activity involves open book or take home quizzes.

CE/CZ 4062 – Computer Security

Course Code	CE/CZ 4062							
Course Title	Computer Security (System Security)							
Pre-requisites	CE/CZ 2005: Operating Systems							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	13	Student presentations	0

Course Aims

This course aims to equip you with foundational knowledge on issues and techniques required for the cyber security.

You will have the knowledge of different security policies and security models, and have the ability to recognise security features and discover pitfalls in computing systems, including the operating system and softwares.

Intended Learning Outcomes (ILO)

Upon successful completion of this course, you should be able to:

1. Explain the principles of access control and security models in computer systems.
2. Interpret different security mechanisms in modern operating systems.
3. Distinguish different vulnerabilities associated with computer systems.
4. Reproduce and detect vulnerable scenarios in existing software.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)	Presentations (Hours)
1	Introduction, Concepts, and Terminology Security, confidentiality, integrity, and availability; Access control; Security models; Security policies; Data and information; Information flow; Attacks and attackers.	2	1	0
2	Identification and Entity Authentication Passwords; Password security; Biometrics; User tokens; Identity management; Single sign-on.	2	1	0
3	Access-Control Capability-based models; Access control list-based models; Mandatory Access Control (MAC); Role Based Access Control (RBAC); Discretionary Access Control (DAC); Rule Based Access Control (RB-RBAC).	3	1	0
4	Security Models Basic theory of multi-level security systems; the Bell-LaPadula model for confidentiality protection and the Biba model for integrity protection.	3	2	0
5	Reference Monitors Operating system integrity (driver signing, secure boot chain); hardware security features (secure enclave, TPM); Memory protection.	3	1	0
6	Unix Security Security principals; access control model; permission model for file system; controlled invocation; security extensions in modern Unix-like OS, e.g. Linux, and SELinux.	4	2	0
7	Windows Security Security principals; access control model; registry; security descriptors; security policies management.	2	1	0
8	System Software Security Overview of basic software vulnerabilities such as memory corruption and exploits, integer overflow and related exploits, and shell code injection; Interplay between software security and system security such as mechanisms for controlled invocation and file system security.	3	2	0

9	Mobile Operating System Security Security mechanisms and vulnerabilities in Android and iOS: system-level security, application-level security and data protection.	4	2	0
	Check for Hours	=26	=13	=0

Assessment (includes both continuous and summative assessment)

a) Quiz: 20%
b) Final Examination: 60%
c) Case study written report: 20%

CE/CZ 4064 – Security Management

Course Code	CE/CZ 4064							
Course Title	Security Management							
Pre-requisites	CZ/CE 2006: Software Engineering							
No of AUs	3							
Contact Hours	Lectures	23	TEL	0	Tutorials	4	Student presentations	12

Course Aims

This course aims to develop your ability to identify the problems associated with (cyber and information) security management and understand using case studies that to effectively address them, one needs to design solutions that encompass multiple dimensions, including technology, people, processes and (internal as well as external) regulations.

This course provides an introductory but broad perspective of cyber and information security, and is relevant for anyone pursuing a career in the IT/ICT industry – including those in product design and development, security engineering, penetration testing, network/system administration, as well as, given the proliferation of IT in all walks of our lives, in executive roles across industries and government.

Intended Learning Outcomes (ILO)

This course introduces security management at an elementary level. Upon the successful completion of this course, you shall be able to:

1. Explain the need for effective security management;
2. Identify the typical problems associated with security management;
3. Describe and debate the ways in which various organizations solve these problems;
4. Analyse real world and (possibly) new security incidents or problems, and propose and evaluate possible mitigations.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)	Presentations (Hours)
1	Introduction Concepts and terminology. Drivers and motivations for security management (what is security, and why is it necessary.) Discourse various related concepts of security, including data security, information security, technology risk, information risk, and Cyber security.	2	0.5	0
2	Information Security, Governance, and the Law Principles and practices of information security governance, policy, and programme. Laws and regulations affecting information security governance, policy, and programme.	3	0.5	2
3	Model, Framework, and Approach Systems, models, and frameworks pertaining to security management. Information classification. Industry standards, best practices, and certifications (e.g., ISO/IEC 27001). Performance measurement. Economics of information security.	4	0.5	2
4	Organization and People Organization and reporting structure. People aspects of security management, including third-party personnel, and temporary employees. Information owner and custodian. Security awareness, training, and competency. Security communications.	4	0.5	2
5	Risk Analysis and Assessments Principles, methods and practices of risk analysis and assessments, including common problems and resolutions. Managing information security risks in outsourcing and other business alliances.	2	0.5	2

6	Security Operations Operations management, effectiveness and efficiency. Incident handling. Change management. Vulnerability management.	4	0.5	2
7	Internal Control, Audit, and Security Principles and practices of Internal Control and Audit in organizations. How Internal Control and Audit relates to Security in practice. Common challenges and resolutions.	2	0.5	1
8	Contingency Planning and Management Principles and practices relating to incident management, crisis management, business continuity planning and management, and disaster recovery planning and management.	2	0.5	1
	Check for Hours	=23	=4	12

Assessment (includes both continuous and summative assessment)

a) Final Examination: 60%
b) Case study written report: 15%
c) Case study oral presentation: 25%

CE/CZ 4065 – Digital Forensics

Course Code	CE/CZ 4065							
Course Title	Digital Forensics							
Pre-requisites	CE/CZ1001, CE3005/CZ3006, CE/CZ4062							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	13	Laboratories	8

Course Aims

Digital forensics has become increasingly relied upon to obtain evidence suitable for admission to a court of law. Such a process involves the gathering, recovery, and analysis of electronic traces to procure electronic evidence; this done in a manner that maintains a well-documented chain of custody such that the integrity of the electronic evidence can be validated by external parties.

This course provides an introductory but broad perspective of digital forensics and is relevant for anyone pursuing a career in the IT/ICT industry – including those in product design and development, security engineering, penetration testing, network/system administration, as well as, given the proliferation of IT in all walks of our lives, in executive roles across industries and government.

Intended Learning Outcomes (ILO)

This course introduces digital forensics at an elementary level. Upon the successful completion of this course, you shall be able to:

1. Explain the knowledge about what is stored in digital systems and how to retrieve and use such data/information to procure evidence;
2. Describe the different anti-forensic techniques, and how anti-forensics can be detrimental to a forensic analyst's effort in recovering evidence;
3. Describe network forensics, including techniques used to capture data and information on networks, and how to use such data to reconstruct a system/user activity scenario;
4. Explain how data is retained in storage systems;
5. Present the investigative findings in an objective manner.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)	Presentations (Hours)
1	Introduction Overview of forensic science; Steps from collecting data to preserving evidence; Framework for digital forensic evidence collection and processing; Role and responsibility of first responders; Legal considerations in digital forensics.	4	2	
2	Crime Scene Investigation Overview of the investigative approaches, the do's and the don'ts; Introduction to forensic toolkit; Types of crime – traditional and cyber. (Use cases for discussions)	4	2	
3	Digital Evidence Overview of digital evidence handling and introduction to the evidence file hash value.	2	1	
4	Reviewing a Case Overview of reviewing a case using a forensic toolkit. (Introduction to Guidance Software EnCase and other potential toolkits)	2	1	2
5	Host Forensics – Disk Types and Structures Host forensics independent of the operating system, examination of the disk types (e.g. BIOS, MBR, RAM); Block devices and file systems, HDDs and SSDs, information extraction and tools for host forensics.	2	1	2
6	Host Forensics Operating System – Windows Fundamentals of host forensics for Microsoft Windows;	2	1	2
7	Host Forensics Operating System - Mac & Unix Fundamentals of host forensics for Unix derivatives using the Linux operating system as an example - Information extraction and tools for host forensics.	2	1	2

8	Information Hiding – Steganography Steganographic techniques for images, videos, textual data, and audio; Steganalytical techniques for selected media types; Covert and subliminal channels; Cryptographic techniques and tools for information hiding.	2	1	
9	Non-standard Storage Mechanisms and Devices Survey of non-standard storage mechanisms; Retention characteristics; Mobile and smart phones; Vehicular systems; Network-based search and storage mechanism; Cloud based storage	2	1	
10	Reporting and Expert Witness The Do's and Don't's of reporting, with possible litigation outcome; Insight to developing interview questions and how to identify culpable subjects.	2	1	
11	Industry review and concerns Review the current technology landscape, concerns, limitations, legal concerns, professional certifications and training/development.	2	1	
	Check	26	13	8

Assessment (includes both continuous and summative assessment)

a) Final Examination: 50%
b) Laboratories and written report: 50%

CE/CZ 4067 – Software Security

Course Code	CE/CZ 4067							
Course Title	Software Security							
Pre-requisites	CZ/CE 2002: Object Oriented Design & Programming or CZ/CE 2005: Operating Systems							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	13	Laboratories	-

Course Aims

This course aims to develop skills in software security. It focuses on security attacks launched by supplying specially crafted inputs to software components that modify the intended behaviours of those components, and the secure coding techniques (defences). The modified behaviours of the software components become security critical in a connected world where application systems are constructed from a collection of software components. Software developers who are not familiar with software security are likely to omit suitable defences out of ignorance.

As such, this course will equip you with the deep knowledge about software security attack and defence techniques, a skill necessary to become IT security experts or professional software developers.

Intended Learning Outcomes (ILO)

Upon the successful completion of this course, you shall be able to:

1. Describe the causes for common software vulnerabilities.
2. Include basic defences in their code.
3. Make use of software security tools
4. Describe the importance and the recommended phases of a software development process geared towards writing secure code

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)
1	Introduction to Secure Software Development Definitions. Why software security? Secure development lifecycle approach; Software threat modelling, risk analysis, and impact analysis. Defensive programming concepts and principles.	2	1
2	Buffer overrun attacks Buffer overruns; the call stack and stack frames; classes of stack overrun attacks; defences: canaries, DEP, ASLR; integer overflows; safe integer arithmetic; refined attacks: return-oriented programming, jump-oriented programming; overrun attacks on the heap	3	1.5
3	Targeted overwrite attacks Format string attacks; memory allocation and deallocation; double-free attacks; attack targets; defences	3	1.5
4	Input security Sources of input: Environment variables; object reuse and storage residues; uninitialized memory corruption attacks;	2	1
5	Type safety and race conditions **Type-safe languages; type confusion attacks; race conditions**	2	1
6	Character and integer representations **Meta characters; UTF-8 encoding of Unicode characters and the challenges posed to filtering input; input filtering: Regular expressions; wrappers; HTML encoding.**	2	1
7	Data access security HTTP parameter pollution attacks; SQL injection attacks: Principles of SQL injection attacks; defences: escaping, filtering, bound parameters;	4	2
8	**Generation and handling of cryptographic material** Session security; cross-site request forgery attacks; use of cryptographic mechanisms, and security protocols in software; software key generation and handling; code signing and verification of loadable modules.	4	2
9	Code review, software testing and taint analysis Static and dynamic taint analysis; data flow and information flow analysis; fuzzing; regression testing; black/white box testing; data mutation.	4	2
	Check for Hours	=26	=13

Assessment (includes both continuous and summative assessment)

a) Final Examination: 60%
b) One Quiz: 20%
c) Project/Assignment: 20%

CE/CZ 4068 – Application Security

Course Code	CE/CZ 4068							
Course Title	Application Security							
Pre-requisites	CE/CZ 2005: Operating Systems CE 3005: Computer Networks (for CE) or CZ 3006: Net-Centric Computing (for CSC)							
No of AUs	3							
Contact Hours	Lectures	26	TEL	-	Tutorials	13	Laboratories	-

Course Aims

The internet has become a convenient platform for commercial transactions executed by application systems. Commercial transactions are obvious targets for criminal activities. Securing such transactions involves multiple parties, hardware components, and protocols which are important to the security of the underlying application systems. Practitioners in this field need to be familiar with current security technologies and appreciate the respective management tasks and responsibilities of the parties involved. This course would support you in fulfilling these expectations.

Intended Learning Outcomes (ILO)

Upon the successful completion of this course, you shall be able to:

1. Describe the various security technologies used for protecting commercial transactions conducted by application systems
2. Describe the fundamentals of risk analysis and security management
3. Determine how and where commercial transactions may be compromised in the web architecture
4. Identify current attack patterns
5. Determine the protection mechanisms appropriate for a given threat

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)
1	Introduction Definitions. Concepts and principles; Scope of application security (versus software security); Application security lifecycle management (reference ISO/IEC 27034); Application threat modelling.	2	1
2	Application Vulnerabilities Concepts and methodologies for application risk assessment and penetration testing. Vulnerabilities disclosure and response procedures. [Possibly invite vendor to demo related products]	2	1
3	Application Security Framework and Architecture Definition and purpose. Common application security services (e.g., crypto, identity and single sign-on, access control, audit), processes, and methodologies. Third parties' developments and open source security considerations.	2	1
4	Email security First case study that illustrates an application involving multiple parties and protocols and discusses where protection mechanisms might be applied. Spam and phishing emails challenges, solutions, and limitations. Sender Policy Framework (SPF), Domain Key Identified Mails (DKIM), S/MIME, PGP.	2	1
5	Web architecture and its security challenges Overview of the web architecture; essential aspects of http; focus on server-side scripting and client-side scripting for delivering dynamic web pages. TLS/SSL security and challenges. Security issues in web protocols (Http parameter pollution attacks, cross-site request forgery, and SQL injection attacks; recommended security mechanisms.)	3	2
6	Origin-based access control in the Web Same Origin Policy; third party cookies; mashups, Cross-origin resource sharing (CORS), and Cross-site scripting attack.	2	1
7	Roots of Trust Foundations for securing end systems; Trusted Platform Modules, Trusted Execution Environment, ARM TrustZone, Intel TXT, Hardware Security Modules; Web/application server attestation (using TPM).	3	1
8	Decentralized implementation of trust Notion of trust without a central authority, decentralized implementation of trust, distributed ledger, Blockchain, digital currencies, Bitcoin, smart contract.	2	1

9	Security of mobile and cloud as application platforms Mobile and cloud as platforms for application systems; strengths and weaknesses of cloud-based application systems; security requirements and security objectives of cloud-based applications in different industries (e.g. financial, retail, manufacturing); applicable laws, regulations, organization security policies and industries practices.	4	2
10	Security of payment card system Overview of payment card applications, card-present retail transactions and Point-of-Sales (POS) devices; remote attacks against payment card transaction systems and POS devices (identify security vulnerabilities of the interconnected systems, how attacks may work to compromise and control the POS devices); security requirements and security objectives of payment card systems; countermeasures to protect payment card systems from remote attacks.	4	2
	Check for Hours	=26	=13

Assessment (includes both continuous and summative assessment)

a) Final Examination: 60%
b) One Quiz: 20%
c) Project: 20%

CE/CZ 4071 – Network Science

Course Code	CE/CZ 4071							
Course Title	Network Science							
Pre-requisites	CE/CZ 2001: Algorithms							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	13	Student presentations	0

Course Aims

We live in a world where we are surrounded by systems that are incredibly complex, from the society, a collection of billions individuals, to communications systems, integrating billions of devices, from computers to cell phones. In fact, the existence of living beings in this planet depends on the ability of thousands of proteins to work together in a seamless fashion. Furthermore, our ability to comprehend our surroundings is heavily influenced by the activity of billions of neurons in our brain. Such *complex systems* can be represented as static or dynamic *networks* of many interacting components. These components are typically much simpler in terms of behavior or function than the overall system, implying that the additional complexity of the latter is an *emergent network property.*

Network science is a new discipline that investigates the topology and dynamics of such complex networks, aiming to better understand the behavior, function and properties of the underlying systems. In this course, we will study algorithmic, computational, and statistical methods of network science, as well as its applications in solving real-world problems in communications, biology, sociology, and cyber security. The specific topics include network metrics, properties, and models, network querying and analytics, network dynamics, and distributed graph engines. Another pervasive goal of this course is to guide students into the future by presenting research that reveals the “next big thing” in network science.

Intended Learning Outcomes (ILO)

This course introduces network science at a foundation level. Upon the successful completion of this course, you shall be able to:

1. Explain the importance of, and uses for, network science in human society;
2. Describe various network analysis metrics;
3. Describe various static and dynamic properties and models of real-world networks;
4. Formulate basic network search queries and evaluate these in order to search and analyse underlying network data;
5. Describe the working and usage of various network analytics algorithms;
6. Describe the architecture and characteristics of distributed graph engines;
7. Explain the significance of network science models, properties, and algorithms in today's world;

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)	Presentations (Hours)
1	Overview of network science: Definition and importance of network science, history of network science, relation to graph theory	1	0	0
2	Network analysis metrics: Paths, components, degree distributions, clustering, degree correlations, centrality measures, algorithms to compute metrics	3	1	0
3	Properties of real-world networks: Scale-free networks, small-world phenomenon, modularity, network motifs	4	2	0
4	Network models: Random networks, Watts-Strogatz model, preferential attachment, Kleinberg's duplication-based model	4	2	0
5	Network querying: Types of network queries, query evaluation techniques, applications in various domains such as social, biological, and transportation	2	1	0
6	Network analytics: Network partitioning, community detection, statistical analytics, PageRank, clustering and summarization, pattern mining, network sampling, applications in various domains such as social, biological, and cyber security.	5	4	0
7	Network dynamics: Percolation and network resilience to random and targeted attacks, growth and densification, rewiring, network epidemics model, social influence propagation and maximization.	3	2	0
8	Massive graph/network engines: Architecture and characteristics of various distributed graph engines (e.g., Pregel, GraphLab, GraphX/Spark), applications in solving real-world big network querying and analytics problems.	3	1	0

9	Conclusion: Summary of the course content, network science challenges ahead	1	0	0
	Check for Hours	=26	13	0

Assessment (includes both continuous and summative assessment)

a) Final Examination: 50%
b) Term Project: 30%
c) Quiz: 20%

CE/CZ 4073 – Data Science for Business

Course Code	CE/CZ 4073							
Course Title	Data Science for Business							
Pre-requisites	CE/CZ 1007: Data Structures and CE/CZ 1011: Engineering Mathematics I or CE/CZ 1007: Data Structures and CE/CZ 1008: Engineering Mathematics							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	20	TEL	0	Tutorials	9	Presentations	0

Course Aims

Summary: *"Data is the new Oil"* in the modern era of Information. It is of paramount importance in each sector of Business to collect, maintain, visualize, explore, analyse, and model data, in every form and shape, to garner crucial inferential information about the scope and target audience, performance and potential optimizations, predictions and forecasting, as well as practical data-driven business decisions.

The Aim: This elective course in Computer Science and Engineering aims to introduce you, hands-on, to the core techniques of data manipulation, visualization, statistical modelling, inference, and digital data presentation, which constitute the business analytics toolbox for any practicing Data Scientist in the industry in order to make fundamental data-driven decisions in diverse Business scenarios.

Intended Learning Outcomes (ILO)

By the end of the semester, the students should be able to

1. Recognize and identify data-oriented problems in practical Business scenarios,
2. Discuss and explain the type of data required to solve the aforesaid problems,
3. Illustrate and articulate aforesaid problems in terms of relevant data exploration,
4. Devise machine learning models for prediction, classification, clustering, forecasting,
5. Assess and justify the inferential information extracted from data using the models,
6. Compose an engaging "data-story" to communicate the problem and the inference.

Course Content

	Topics	Lectures (Hours)	Tutorials (Hours)
1	Motivation and Introduction What is Data Science? – The core problems and solutions. Basic concepts of Statistics. Basics of Data Handling in R.	2	1
2	Prediction in Business Introduction to Linear Models and Linear Regression. Training and Minimization of Variance in Regression. Model-Fitting, Parameter Estimation and Inference.	4	2

3	Classification in Business Decision Trees, Information Gain, and Optimal Splits. Classification using Random Forests and Ensembles. Performance of Classification – Accuracy and ROC.	3	1.5
4	Choosing a Model How to avoid Overfitting and/or Underfitting of a Model? Bias-Variance Trade-off, Validation and Cross-Validation.	2	1
5	Clustering in Business Notion of Distance and concept of Nearest Neighbours. Regression and Classification using Nearest Neighbours. Neighbourhoods to Clusters – k-Means and Dendograms.	3	1.5
6	Forecasting in Business Fundamentals of Time Series – Trends, Seasonality, Cycles. Time Series Models – Moving Average, ARMA and ARIMA.	2	1
7	Visualizing Data Principal Component Analysis, Low-Dimensional Embedding. Storyboarding – Dashboards and Data Visualizations in R.	2	1
8	Data Analytic Thinking Practical examples of Data Science from Businesses. Ethical considerations in applications of Data Science.	2	0
	Check for Hours	= 20	= 9

Assessment (includes both continuous and summative assessment)

a) Final Exam: 40%
b) Assignments: 60%