# Kerala University of Digital Sciences, Innovation and Technology

# M.Tech Computer Science & Engineering
# &
# M.Sc Computer Science

Scheme and Syllabus
2021 Admission

October 2021

School of Computer Science & Engineering (SoCSE)

## School of Computer Science & Engineering

The School of Computer Science & Engineering (SoCSE) of the Kerala University of Digital Sciences, Innovation and Technology (KUDSIT) was established in the year 2020, in the Technocity Campus, Trivandrum. The school offers the academic programs M.Tech Computer Science & Engineering, M.Sc Computer Science and Ph.D.

### Vision

To become a world-class centre of advanced learning, research and development, and societal outreach in the field of Computer Science and Engineering

### Mission

To provide an enriching scholastic environment that nurtures innovative and effective ways of knowledge creation, dissemination and application to facilitate world-class education and cutting edge research in the field of Computer Science and Engineering and thereby contributing to the society nationally and globally.

### Objectives

SoCSE targets to focus its activities in the following dimensions:

- World class research and academics with national and international collaborations.
- Nurturing globally competent and socially responsible talent pool through academic programmes.
- Commercialization of research outcomes through consultancy, collaborative new business initiatives and promotion of entrepreneurship.
- Creating an inclusive and collaborative environment to foster local, sustainable and globally relevant knowledge and expertise.

### Master of Technology (M.Tech) in Computer Science & Engineering (intake: 90)

M.Tech in Computer Science & Engineering will be offered with 3 specializations: Artificial Intelligence; Connected Systems and Intelligence; Cyber Security Engineering. The students will have to choose one of the specializations in the second semester. The admission and eligibility requirements for all the 3 specializations are the same.

## Three Specializations:

### Artificial Intelligence

The annual growth rate of artificial intelligence (AI) is predicted to be 33.2% between 2020 and 2027. The market growth of AI is hampered due to lack in the number of experienced and trained professionals. This programme would transform and strengthen the industries across the globe. It focuses on intelligence exhibited by the machines and is a hybrid intelligence, where AI systems and humans work together. The curriculum offers an opportunity to approach AI from a technical perspective that focuses on the understanding, analysis and development of novel AI algorithms as well as social and human perspectives. Decision making, problem solving, perception, understanding human communication (in any language, and translate among them) for the computers would be the key elements taught in this programme. This programme provides the foundation and advanced skills in the principles and technologies that underlie AI including logic, knowledge representation, probabilistic models, and machine learning. Students can pursue topics in depth, with courses available in areas such as robotics, vision, and natural language processing.

### Connected Systems and Intelligence

The future era of digitally connected world envisages to be governed by smart connected devices that are aware of the context and the location, and envisions cognitive decision making through intelligent data analytics. The synergy derived out of the combination of artificial intelligence, big data analytics, the Internet of Things, and cloud and edge computing contributes significantly to realize the automated interaction of real-world physical systems. In 2025, according to the International Data Corporation, 41.6 billion connected IoT devices would generate 79.4 zettabytes of data. Future smartsystems will rely on data intelligence tools and approaches to identify hidden patterns, unknown correlations, and other relevant information from massive amounts of data.

Graduates from this masters programme is expected to develop novel solutions for intelligent and resilient networked systems and contribute to the design of stable digitally connected ecosystems involving distributed systems, computer vision, ubiquitous computing, machine learning, data science, and security services. They will be experts in the field, qualified for exciting careers in industry or doctoral studies.

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION

Three key UN sustainable development goals addressed by this master programme are: industry, innovation and infrastructure (09); sustainable cities and communities (11); and responsible production and consumption (12). Both connected systems and data intelligence play a crucial role in enabling technologies to achieve some of the above-mentioned objectives such as the development of smart cities, safe and efficient transport systems and efficient resource consumption and production.

### Cyber Security Engineering

Cyber security remains one of the most growth-oriented career fields in the computer science domain. The Cyber Security Engineering degree programme focuses on the fundamentals of developing, engineering, and operating secure information systems. Graduates of this programme will be able to solve complex cyber security issues affecting various businesses worldwide and propose new solutions. Graduates are likely to be employed in law enforcement, government or other related agencies as cyber security specialists, in commercial IT departments or security consultancies, or in other computing positions where cyber security is a major issue. Opportunities also exist for further academic study towards a Ph.D and a career in research.

**M.Tech Programs Offered and Eligibility Requirements**

| Programme | Specialization | Duration | Minimum Eligibility for admission |
|---|---|---|---|
| Full-time Master of Technology (M.Tech) in Computer Science & Engineering | Artificial Intelligence | 2 years<br>(4 semesters) | • B.Tech/BE in CS/IT/ECE or related areas/MCA/M.Sc in CS/IT/Mathematics/ Statistics/Physics |
| | Cyber Security Engineering | 2 years<br>(4 semesters) | |
| | Connected Systems and Intelligence | 2 years<br>(4 semesters) | |
| Part-time Master of Technology (M.Tech) in Computer Science & Engineering | Artificial Intelligence | Minimum three years,<br>Maximum three and half years | • B.Tech/BE in CS/IT/ECE or related areas/ MCA/ M.Sc in CS/IT/Mathematics/ Statistics/Physics<br>• Minimum of two years of full-time work experience in a company/industry/ educational or research institute/ any government department/ autonomous organization in the relevant field. |

**Master of Science (M.Sc) in Computer Science (intake: 90)**

M.Sc in Computer Science will be offered with 2 specializations: Cyber Security; Artificial Intelligence. The students will have to choose one of the specializations while taking the admission. The admission and eligibility requirements for all the 2 specializations are the same.

## Two Specializations:

### Cyber Security

The area of cyber security also known as computer security or IT security is security applied to computers, computer networks, and the data stored and transmitted over them. The field is of growing importance due to the increasing reliance of computer systems. Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. The field of cyber security, has grown very rapidly in the recent years. The subject embraces technologies such as cryptography, machine learning, computer security, network security, ethical hacking forensics and fraud detection, as well as management of security and trade-offs while implementing information security.

With the growing volume and sophistication of cyber-attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. By offering the course M.Sc in Computer Science with specialization in Cyber Security we will be able to harness students who are open to challenging job options in corporate and allied sectors, academics, R&D, government and so on.

### Machine Intelligence

Masters programme in Machine Intelligence enables the students to design, implement and analyze intelligent systems. Intelligent decision making and learning, and intelligent web-based systems are areas of growing emphasis in the digital world. Machine learning algorithms can figure out how to perform important tasks by generalizing from examples. This is often feasible and cost-effective when manual programming is not. Machine learning (also known as data mining, pattern recognition and predictive analytics) is used widely in business, industry, science and government, and there is a great shortage of experts in it. This course provides the necessary foundation in Machine Intelligence as well as other core subjects for a graduate level computer science education. Computers are learning to think, read, and write while picking up human sensory function, with the ability to see and hear (arguably to touch, taste, and smell, though those have been of a lesser focus). Machine intelligence technologies cut across a vast array of problem types (from classification and clustering to natural language processing and computer vision) and methods (from support vector machines to deep belief networks). All of these technologies are reflected on this landscape.

### M.Sc Programs Offered and Eligibility Requirements

| Programme | Specialization | Duration | Minimum Eligibility for admission |
|---|---|---|---|
| Full-time Master of Science (M.Sc) in Computer Science | Cyber Security | 2 years (4 semesters) | B.Tech/B.E in any branch or BCA or B.Sc in CS/IT/Mathematics/Statistics/Physics |
| | Machine Intelligence | 2 years (4 semesters) | |

### Course Categorization

- 100 Level - Undergraduate level basic course
- 200 Level - Undergraduate level advance course
- 300 Level- Postgraduate level instruction based course
- 400 Level - Postgraduate level seminar/ research level course
- 500 Level - Research level course

### Credit Requirements for Completing M.Tech

| Level of Course | Minimum Credit | Maximum Credit |
|---|---|---|
| 100 | 0 | 6 |
| 200 | 0 | 15 |
| 300 | 30 | 70 |
| 400 | 9 | 50 |
| 500 | 0 | 9 |

### Credit Requirements for Completing M.Sc

| Level of Course | Minimum Credit | Maximum Credit |
|---|---|---|
| 100 | 3 | 9 |
| 200 | 6 | 28 |
| 300 | 30 | 50 |
| 400 | 9 | 24 |
| 500 | 0 | 9 |
| | | |

- The minimum semester-wise distribution of credits expected in a MSc program are:

| **Semester** | **Minimum Credits** |
|---|---|
| Semester 1 | 20-30 credits |
| Semester 2 | 20-30 credits |
| Mini-Project# | 6 credits |
| Semester 3 | 20-30 credits |
| Semester 4* | 20-30 credits |
| Total (Minimum) | 100 credits |

*Project requires 16-24 credits
#The mini-project can be part of the semester or be offered between the semester as best suitable for the program of study. This can be decided by the schools.

- The minimum semester-wise distribution of credits expected in the M.Tech program are:

| **Semester** | **Minimum Credits** |
|---|---|
| Semester 1 | 20-30 credits |
| Semester 2 | 20-30 credits |
| Mini-Project# | 6 credits |
| Semester 3 | 20-30 credits |
| Semester 4* | 24-30 credits |
| Total (Minimum) | 100 credits |

*Project requires 24 credits of project work, and 6 credits of seminar.
#The mini-project can be part of the semester or be offered between the semester as best suitable for the program of study. This can be decided by the schools.

**Credit requirements for the masters program:**

Students are required to comply with the following credit limits for successfully completing a master’s program.

- Complete a minimum of 100 Credits, with an upper limit of 120 credits.
- The students are allowed to take a maximum of 30 Credits in a semester.
- The students are allowed to take a maximum of 12 Credits through audit courses. These credits do not count towards total credits for the program.
- The students are allowed to obtain a maximum of 12 Credits through challenge exams. These credits count towards total credits for the program.

**Grade Point Calculation**

The University follows grade point system for each course with a scale of 10 defined as:

| Grade | Percentage of Marks | Grade Points | Remarks |
|---|---|---|---|
| S | 95% and above | 10 | Outstanding |
| A+ | 90% to less than 95% | 9 | Excellent |
| A | 80% to less than 90% | 8 | Very Good |
| B+ | 70% to less than 80% | 7 | Good |
| B | 60% to less than 70% | 6 | Above Average |
| C | 50% to less than 60% | 5 | Average |
| D | 40% to less than 50% | 4 | Pass |
| E | 30% to less than 40% | 2 | Low Pass |
| F | Below 30% | 0 | Fail |

- AB will be represented for Absent and its GP is considered as 0
- “ I “ will represent incomplete
- The minimum grade point requires for passing a course is 4
- The cumulative grade point averages (CGPA) are calculated by weighing grade points by the corresponding credit numbers. The thesis grade counts toward the GP by using the same formula, that is, it is weighed by the credit number assigned to the thesis. The Semester Grade Point Average (SGPA) and Cumulative Grade Point Average (CGPA) is calculated using the standard formula.

# M.Tech in Computer Science and Engineering with Specialization in AI or Connected Systems & Intelligence or Cyber Security Engineering

| Semester 1 | | | | |
|---|---|---|---|---|
| **Course Code** | **Course Title** | **Credits** | **Credit Split Lecture/Lab/ Seminar/Project** | **Level** |
| | Digital Experience Laboratory | 4 | 1-3-0-0 | 300 |
| | Design Thinking and Innovation | 3 | 3-0-0-0 | 300 |
| M3010101 | AI & Machine Learning | 4 | 3-1-0-0 | 300 |
| M3010102 | Mathematical Foundations of Computer Science | 4 | 3-0-1-0 | 300 |
| M3010103 | Advanced Data Structures and Algorithms | 4 | 3-1-0-0 | 300 |
| M3010104 | Advanced Distributed Systems | 4 | 3-1-0-0 | 300 |
| | Elective 1 | 4 | | 300 |
| Total Credits | | 27 | | |

| 1st Semester Electives (Open for all specializations) | | | | |
|---|---|---|---|---|
| **Course Code** | **Course Title** | **Credits** | **Credit Split Lecture/Lab/ Seminar/Project** | **Level** |
| M3010105 | Soft Computing | 4 | 3-0-0-1 | 300 |
| M3010115 | Natural Language Processing | 4 | 3-0-0-1 | 300 |
| M3010125 | Cognitive Computing | 4 | 3-0-0-1 | 300 |
| M3010135 | Blockchain Technology | 4 | 3-1-0-0 | 300 |
| M3010145 | Security in Digital Transformation | 4 | 3-0-0-1 | 300 |

| Semester 2 | | | | |
|---|---|---|---|---|
| **Course Code** | **Course Title** | **Credits** | **Credit Split Lecture/Lab/ Seminar/Project** | **Level** |
| | Digital Access Community Empowerment | 3 | 0-0-0-3 | 300 |
| M3010201 | Data & Intelligence | 4 | 3-1-0-0 | 300 |
| | Elective 2 | 4 | | 300 |
| | Elective 3 | 4 | | 300 |
| | Elective 4 | 4 | | 300 |
| | Elective 5 | 4 | | 300 |
| Total Credits | | 23 | | |

| 2nd Semester Electives for Specialization in AI<br>(Four electives need to be selected) | | | | |
|---|---|---|---|---|
| **Course Code** | **Course Title** | **Credits** | **Credit Split Lecture/Lab/Seminar/Project** | **Level** |
| M3010202 | Deep Learning & Reinforcement Learning | 4 | 3-0-0-1 | 300 |
| M3010212 | Data Mining and Big Data | 4 | 3-0-0-1 | 300 |
| M3010222 | Human Computer Interaction | 4 | 3-0-0-1 | 300 |
| M3010232 | Computer Vision | 4 | 3-0-0-1 | 300 |
| M3010242 | AI Ethics and Sustainability | 4 | 3-0-1-0 | 300 |

| | | | | |
|---|---|---|---|---|
| M3010252 | Connected Environments and Enabling Technologies | 4 | 1-3-0-0 | 300 |
| M3010262 | Social Network Analytics and Security | 4 | 3-0-0-1 | 300 |
| M3010272 | Speech Processing | 4 | 3-0-0-1 | 300 |
| M3010282 | Augmented and Virtual Reality | 4 | 3-1-0-0 | 300 |
| M3010292 | Stochastic Processes and Models | 4 | 3-0-0-1 | 300 |
| M3010203 | Image & Video Processing | 4 | 3-0-0-1 | 300 |

**2nd Semester Electives for Specialization in Connected Systems & Intelligence**

(Four electives need to be selected with minimum three from  Group A)

**Group A**

| **Course Code** | **Course Title** | **Credits** | **Credit Split Lecture/Lab/Seminar/Project** | **Level** |
|---|---|---|---|---|
| M3010213 | Cloud and Edge Computing | 4 | 3-0-0-1 | 300 |
| M3010252 | Connected Environments and Enabling Technologies | 4 | 1-3-0-0 | 300 |
| M3010223 | IoT Networks and Endpoint Security | 4 | 2-2-0-0 | 300 |
| M3010233 | Industrial IoT and Digital Twins | 4 | 3-0-0-1 | 300 |
| M3010243 | Software Defined Networking | 4 | 3-0-0-1 | 300 |
| M3010253 | Internet of Drones | 4 | 3-0-0-1 | 300 |
| M3010263 | Cyber Big Data Analytics | 4 | 3-0-0-1 | 300 |
| M3010262 | Social Network Analytics and Security | 4 | 3-0-0-1 | 300 |
| M3010273 | Ubiquitous Computing | 4 | 3-0-0-1 | 300 |
| M3010283 | Biometric Systems Engineering | 4 | 3-1-0-0 | 300 |
| M3010293 | Hardware Security | 4 | 3-1-0-0 | 300 |
| M3010204 | Wireless Networks and Mobile Computing | 4 | 3-0-0-1 | 300 |
| M3010214 | Wireless Sensor Networks | 4 | 3-0-0-1 | 300 |
| M3010224 | Cryptographic Engineering | 4 | 3-1-0-0 | 300 |
| **Group B** | | | | |
| M3010202 | Deep Learning & Reinforcement Learning | 4 | 3-0-0-1 | 300 |
| M3010234 | Quantum Computing & Cryptography | 4 | 3-0-0-1 | 300 |
| M3010244 | Video Analytics | 4 | 3-0-0-1 | 300 |
| M3010222 | Human Computer Interaction | 4 | 3-0-0-1 | 300 |
| M3010282 | Augmented and Virtual Reality | 4 | 3-1-0-0 | 300 |

**2nd Semester Electives for Specialization in Cyber Security Engineering**

(Four electives need to be selected with minimum three from Group A)

| | **Group A** | | | |
|---|---|---|---|---|
| **Course Code** | **Course Title** | **Credits** | **Credit Split Lecture/Lab/ Seminar/Project** | **Level** |
| M3010254 | Network and System Security | 4 | 3-1-0-0 | 300 |
| M3010293 | Hardware Security | 4 | 3-1-0-0 | 300 |
| M3010264 | Ethical Hacking and Network Defense | 4 | 3-1-0-0 | 300 |
| M3010223 | IoT Networks and Endpoint Security | 4 | 2-2-0-0 | 300 |
| M3010274 | AI Based Cyber Attacks and Defenses | 4 | 3-0-0-1 | 300 |
| M3010263 | Cyber Big Data Analytics | 4 | 3-0-0-1 | 300 |
| M3010284 | Malware Analysis and Reverse Engineering | 4 | 3-1-0-0 | 300 |
| M3010283 | Biometric Systems Engineering | 4 | 3-1-0-0 | 300 |
| M3010294 | Advanced Topics in Cryptography | 4 | 3-0-1-0 | 300 |
| M3010262 | Social Network Analytics and Security | 4 | 3-0-0-1 | 300 |
| M3010205 | Cyber Crime Investigation | 4 | 3-0-0-1 | 300 |
| M3010224 | Cryptographic Engineering | 4 | 3-0-0-1 | 300 |
| M3010215 | Secure Software Engineering | 4 | 3-0-0-1 | 300 |

| | | | | |
|---|---|---|---|---|
| M3010234 | Quantum Computing & Cryptography | 4 | 3-0-0-1 | 300 |
| **Group B** | | | | |
| M3010222 | Human Computer Interaction | 4 | 3-0-0-1 | 300 |
| M3010252 | Connected Environments and Enabling Technologies | 4 | 1-3-0-0 | 300 |
| M3010213 | Cloud and Edge Computing | 4 | 3-0-0-1 | 300 |
| M3010202 | Deep Learning & Reinforcement Learning | 4 | 3-0-0-1 | 300 |
| M3010282 | Augmented and Virtual Reality | 4 | 3-1-0-0 | 300 |
| M3010233 | Industrial IoT and Digital Twins | 4 | 3-0-0-1 | 300 |
| M3010244 | Video Analytics | 4 | 3-0-0-1 | 300 |

| **Semester 2 (Internship)** | | | | |
|---|---|---|---|---|
| **Course Code** | **Course Title** | **Credits** | **Credit Split Lecture/Lab/Seminar/Project** | **Level** |
| M3010225 | M. TechSummer Internship/Team Project | 6 | 0-0-0-6 | 300 |
| Total Credits | | 6 | | |

| **Semester 3** | | | | |
|---|---|---|---|---|
| **Course Code** | **Course Title** | **Credits** | **Credit Split Lecture/Lab/ Seminar/Project** | **Level** |
| M4010301/<br>M4010302/<br>M4010303 | Topics in AI/in Connected Systems & Intelligence/ Cyber Security | 20 | Research (20) | 400 |
| Total Credits | | 20 | | |

| **Semester 4** | | | | |
|---|---|---|---|---|
| **Course Code** | **Course Title** | **Credits** | **Credit Split Lecture/Lab/ Seminar/Project** | **Level** |
| M4010401 | M. Tech Thesis | 30 | 0-0-6-24 | 400 |
| Total Credits | | 30 | | |

| **Audit Courses (non - credit courses) -** NPTEL Courses | | |
|---|---|---|
| Computer Networks and Internet Protocol | Sensors and Actuators | Speaking Effectively |
| Cryptography and Network Security | Python for Data Science | Graph Theory |
| Stochastic Modeling and the Theory of Queues | Operating System | The Joy of Computing using Python |
| Big Data Computing / Algorithms for Big Data | Data Mining | Innovation, Business Models and Entrepreneurship |

# M.Sc. in Computer Science with Specialization in Cyber Security

## Semester 1

| Course Code | Title of the Course | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
|---|---|---|---|---|
| | Digital Experience Laboratory | 4 | 1-3-0-0 | 300 |
| | Design Thinking and Innovation | 3 | 3-0-0-0 | 300 |
| M2020101 | Mathematics for Computer Science | 4 | 3-0-1-0 | 200 |
| M3022102 | Cyber Security and Digital Forensics | 3 | 3-0-0-0 | 300 |
| M2020103 | Data Structures and Algorithms | 4 | 3-1-0-0 | 200 |
| M2020104 | Computer Architecture | 3 | 3-0-0-0 | 200 |
| M1020105 | Python for Data Science | 3 | 3-0-0-0 | 100 |
| M3022106 | Cyber Security and Forensics Lab | 1 | 0-1-0-0 | 300 |
| M1020107 | Python Programming Lab | 1 | 0-1-0-0 | 100 |
| Total Credits | | 26 | | |

## Semester 2

| Course Code | Title of the Course | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
|---|---|---|---|---|
| | Digital Access for Community Empowerment | 3 | 0-0-0-3 | 300 |
| M3022201 | Modern Cryptography | 4 | 3-1-0-0 | 300 |
| M3022202 | Cyber Analytics | 3 | 3-0-0-0 | 300 |
| M2020203 | Operating Systems | 3 | 3-0-0-0 | 200 |
| M2022204 | Computer Networks and Security | 3 | 3-0-0-0 | 200 |
| | Elective 1 | 4 | | 300 |
| M2022206 | Security Auditing Lab | 1 | 0-1-0-0 | 200 |
| M3022207 | Cyber Analytics Lab | 1 | 0-1-0-0 | 300 |
| M3020208 | M.Sc.Mini Project 1 | 1 | 0-0-0-1 | 300 |
| Total Credits | | 23 | | |

## Electives for Semester 2

| Course Code | Title of the Course | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
|---|---|---|---|---|
| M3020205 | Augmented and Virtual Reality | 4 | 3-1-0-0 | 300 |
| M3020215 | Biometrics | 4 | 3-1-0-0 | 300 |
| M3020225 | Information Retrieval | 4 | 3-0-0-1 | 300 |
| M3020235 | Malware Analysis and Reverse Engineering | 4 | 3-1-0-0 | 300 |
| M3020245 | Cloud and Edge Computing | 4 | 3-0-0-1 | 300 |
| M3020255 | Hardware Security | 4 | 3-1-0-0 | 300 |
| Total Credits | | 4 | | |

## Semester 2 Internship

| Course Code | Title of the Course | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
|---|---|---|---|---|
| M3020265 | M.Sc.Summer Internship/Team Project | 2 | 0-0-0-2 | 300 |

|  |  |  |  |
|---|---|---|---|
| Total Credits | 2 |  |  |

| Semester 3 |  |  |  |  |
|---|---|---|---|---|
| Course Code | Title of the Course | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
| M3022301 | Database Security | 4 | 3-0-0-1 | 300 |
| M3022302 | Ethical Hacking and Defensive Techniques | 3 | 3-0-0-0 | 300 |
|  | Elective 2 | 4 |  | 300 |
|  | Elective 3 | 4 |  | 300 |
|  | Elective 4 | 4 |  | 300 |
| M3022306 | Ethical Hacking and Penetration Testing Lab | 1 | 0-1-0-0 | 300 |
| M3020307 | IoT Experience Lab | 2 | 0-2-0-0 | 300 |
| M3020308 | M.Sc. Mini Project 2 | 3 | 0-0-0-3 | 300 |
| Total Credits |  | 25 |  |  |

| Electives for Semester 3 |  |  |  |  |
|---|---|---|---|---|
| Course Code | Title of the Course | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
| M3020303 | Applied Cryptography | 4 | 3-0-1-0 | 300 |
| M3020313 | Block Chain Technology | 4 | 3-1-0-0 | 300 |
| M3020323 | Cognitive Computing | 4 | 3-0-0-1 | 300 |
| M3020333 | Artificial Intelligence for Cyber Security | 4 | 3-0-0-1 | 300 |
| M3020343 | Mobile Application Security | 4 | 3-0-0-1 | 300 |
| M3020353 | Embedded Systems | 4 | 3-0-0-1 | 300 |
| M3020363 | Secure Software Engineering | 4 | 3-0-0-1 | 300 |
| M3020373 | Natural Language Processing | 4 | 3-0-0-1 | 300 |
| M3020383 | Quantum Computing & Cryptography | 4 | 3-0-1-0 | 300 |
| M3020393 | Object-Oriented Analysis and Design | 4 | 3-0-0-1 | 300 |
| M3020304 | Security in Digital Transformation | 4 | 3-0-0-1 | 300 |
| M3020314 | Soft Computing | 4 | 3-0-0-1 | 300 |
| M3020324 | Web Technology | 4 | 3-0-0-1 | 300 |
|  |  |  |  |  |

| Semester 4 |  |  |  |  |
|---|---|---|---|---|
| Course Code | Title of the Course | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
| M4020401 | M.Sc.Internship/Project | 24 | 0-0-0-24 | 400 |
| Total Credits |  | 24 |  |  |

# M.Sc. in Computer Science with Specialization in Machine Intelligence

## Semester 1

| Course Code | Title of the Course | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
|---|---|---|---|---|
| | Digital Experience Laboratory | 4 | 1-3-0-0 | 300 |
| | Design Thinking and Innovation | 3 | 3-0-0-0 | 300 |
| M2020101 | Mathematics for Computer Science | 4 | 3-0-1-0 | 200 |
| M3021112 | Machine Learning | 3 | 3-0-0-0 | 300 |
| M2020103 | Data Structures and Algorithms | 4 | 3-1-0-0 | 200 |
| M2020104 | Computer Architecture | 3 | 3-0-0-0 | 200 |
| M1020105 | Python for Data Science | 3 | 3-0-0-0 | 100 |
| M3021116 | Machine Learning Lab - 1 | 1 | 0-1-0-0 | 300 |
| M1020107 | Python Programming Lab | 1 | 0-1-0-0 | 100 |
| Total Credits | | 26 | | |

## Semester 2

| Course Code | Title of the Course | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
|---|---|---|---|---|
| | Digital Access for Community Empowerment | 3 | 0-0-0-3 | 300 |
| M3021211 | Digital Image and Video Processing | 4 | 3-0-0-1 | 300 |
| M2021202 | Database Systems | 3 | 3-0-0-0 | 200 |
| M2020203 | Operating Systems | 3 | 3-0-0-0 | 200 |
| M3021204 | Deep Learning and Reinforcement Learning | 3 | 3-0-0-0 | 300 |
| | Elective 1 | 4 | | 300 |
| M3021206 | Machine Learning Lab - 2 | 2 | 0-1-0-0 | 300 |
| M3020208 | M.Sc. Mini Project 1 | 1 | 0-0-0-1 | 300 |
| Total Credits | | 23 | | |

## Electives for Semester 2

| Course Code | Title of the Course | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
|---|---|---|---|---|
| M3020205 | Augmented and Virtual Reality | 4 | 3-1-0-0 | 300 |
| M3020216 | Computer Vision | 4 | 3-0-0-1 | 300 |
| M3020225 | Information Retrieval | 4 | 3-0-0-1 | 300 |
| M2022204 | Computer Networks and Security | 4 | 3-0-1-0 | 200 |
| M3020217 | Data Analytics | 4 | 3-0-0-1 | 300 |
| M3020218 | AI Ethics and Sustainability | 4 | 3-0-1-0 | 300 |

## Semester 2 Internship

| Course Code | Title of the Course | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
|---|---|---|---|---|
| M3020265 | M.Sc.Summer Internship/Team Project | 2 | 0-0-0-2 | 300 |
| Total Credits | | 2 | | |

## Semester 3

| Course Code | Title of the Course | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
|---|---|---|---|---|
| M3021373 | Natural Language Processing | 4 | 3-0-0-1 | 300 |
| M3021312 | Big Data Technologies | 3 | 3-0-0-0 | 300 |
| | Elective 2 | 4 | | 300 |
| | Elective 3 | 4 | | 300 |
| | Elective 4 | 4 | | 300 |
| M3021316 | Big Data Technologies Lab | 1 | 0-1-0-0 | 300 |
| M3020307 | IoT Experience Lab | 2 | 0-2-0-0 | 300 |
| M3020308 | M.Sc. Mini Project 2 | 3 | 0-0-0-3 | 300 |
| Total Credits | | 25 | | |

## Electives for Semester 3

| Course Code | Title of the Course | Elective No. | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
|---|---|---|---|---|---|
| M3020334 | Artificial Intelligence | Elective 2 | 4 | 3-0-1-0 | 300 |
| M3020314 | Soft Computing | Elective 2 | 4 | 3-0-0-1 | 300 |
| M3020363 | Secure Software Engineering | Elective 2 | 4 | 3-0-0-1 | 300 |
| M3020324 | Web Technology | Elective 2 | 4 | 3-0-0-1 | 300 |
| M3020245 | Cloud and Edge Computing | Elective 3 | 4 | 3-0-0-1 | 300 |
| M3020354 | Optimization Techniques | Elective 3 | 4 | 3-0-0-1 | 300 |
| M3020353 | Embedded Systems | Elective 3 | 4 | 3-0-0-1 | 300 |
| M3020304 | Security in Digital Transformation | Elective 3 | 4 | 3-0-0-1 | 300 |
| M3020323 | Cognitive Computing | Elective 4 | 4 | 3-0-0-1 | 300 |
| M3020383 | Quantum Computing & Cryptography | Elective 4 | 4 | 3-0-1-0 | 300 |
| M3020313 | Block Chain Technology | Elective 4 | 4 | 3-1-0-0 | 300 |
| M3020374 | Object Oriented Analysis and Design | Elective 4 | 4 | 3-0-0-1 | 300 |

## Semester 4

| Course Code | Title of the Course | Credits | Credit Split Lecture/Lab/ Seminar/Project | Level |
|---|---|---|---|---|
| M4020401 | M.Sc. Internship/Project | 24 | 0-0-0-24 | 400 |
| Total Credits | | 24 | | |

# List of Courses and Syllabus

## University Core Courses

1. Design Thinking and Innovation
2. Digital Access Community Empowerment
3. Digital Experience Laboratory

## Theory Courses

1. Advanced Data Structures and Algorithms
2. Advanced Distributed Systems
3. Advanced Topics in Cryptography
4. AI Ethics and Sustainability
5. AI & Machine Learning
6. AI Based Cyber Attacks and Defenses
7. Applied Cryptography
8. Artificial Intelligence
9. Artificial Intelligence for Cyber Security
10. Augmented and Virtual Reality
11. Big Data Technologies
12. Biometric Systems Engineering
13. Biometrics
14. Block Chain Technology
15. Cloud and Edge Computing
16. Cognitive Computing
17. Computer Architecture
18. Computer Networks and Security
19. Computer Vision
20. Connected Environments and Enabling Technologies
21. Cryptographic Engineering
22. Cyber Analytics
23. Cyber Big Data Analytics
24. Cyber Crime Investigation
25. Cyber Security and Digital Forensics
26. Data & Intelligence
27. Data Analytics
28. Data Mining and Big Data
29. Data Structures and Algorithms
30. Database Security
31. Database Systems
32. Deep Learning and Reinforcement Learning
33. Digital Image and Video Processing
34. Embedded Systems
35. Ethical Hacking and Defensive Techniques
36. Ethical Hacking and Network Defense
37. Hardware Security
38. Human Computer Interaction
39. Image & Video Processing
40. Industrial IoT and Digital Twins
41. Information Retrieval
42. Internet of Drones
43. IoT Networks and Endpoint Security
44. Machine Learning

45. Malware Analysis and Reverse Engineering
46. Mathematical Foundations of Computer Science
47. Mathematics for Computer Science
48. Mobile Application Security
49. Modern Cryptography
50. Natural Language Processing
51. Network and System Security
52. Object-Oriented Analysis and Design
53. Operating Systems
54. Optimization Techniques
55. Python for Data Science
56. Quantum Computing & Cryptography
57. Secure Software Engineering
58. Security in Digital Transformation
59. Social Network Analytics and Security
60. Soft Computing
61. Software Defined Networking
62. Speech Processing
63. Stochastic Processes and Models
64. Ubiquitous Computing
65. Video Analytics
66. Web Technology
67. Wireless Networks and Mobile Computing
68. Wireless Sensor Networks

## Research Courses

1. Topics in Connected Systems & Intelligence
2. Topics in AI
3. Topics in Cyber Security

## Laboratory Courses

1. Big Data Technologies Lab
2. Cyber Analytics Lab
3. Cyber Security and Forensics Lab
4. Ethical Hacking and Penetration Testing Lab
5. IoT Experience Lab
6. Machine Learning Lab - 1
7. Machine Learning Lab – 2
8. Python Programming Lab
9. Security Auditing Lab

## Internships, Projects and Thesis

1. M.Sc Internship
2. M.Sc Project
3. M.Sc Mini Project 1
4. M.Sc Mini Project 2
5. M.Sc Summer Internship
6. M.Sc Summer Team Project
7. M.Tech Summer Team Project
8. M.Tech Thesis
9. M.Tech Summer Internship

## Audit Courses (non-credit courses) - NPTEL Courses

1. Big Data Computing/Algorithms for Big Data
2. Computer Networks and Internet Protocol

3. Cryptography and Network Security
4. Data Mining
5. Graph Theory
6. Innovation, Business Models and Entrepreneurship
7. Operating System
8. Python for Data Science
9. Sensors and Actuators
10. Speaking Effectively
11. Stochastic Modeling and the Theory of Queues
12. The Joy of Computing using Python

# Theory Courses

## M3010103 ADVANCED DATA STRUCTURES AND ALGORITHMS

| Course Code | Course Name | Lecture/Lab/Seminar/Project Credits | Year of Introduction |
|---|---|---|---|
| M301103 | **Advanced Data Structures and Algorithms** | **3-1-0-0** | **2021** |

**Prerequisites:** Students should possess the fundamental programming skills in Computer Programming Languages such as Python.

**Course Objective(s):**

Understand fundamental data structures and algorithms, as well as the tradeoffs between various implementations of these abstractions.

**Course Outcomes:**

By the conclusion of this course, students should be able to:

**CO1**: Understand advanced data structures and their applications conceptually.

**CO2**: Implement various algorithms for a variety of applications, and develop an insight on NP-completeness, randomization, approximation, and parameterized complexity.

**CO3**: Design, prove the correctness and analyse new algorithms.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge.

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature.

**PLO 3** Apply scholarship to conduct independent and innovative research.

**PLO 4** Show communication skills in a variety of formats (oral, written).

**PLO 5** Practice ethical standards of professional conduct and research.

**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | | | | | |
| **CO2** | 3 | 2 | | 1 | | |
| **CO3** | 3 | 2 | | 1 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| **1** | Various Algorithm Design Strategies. Revising Asymptotic Complexity Analysis, Sorting, Searching and Divide and Conquer Algorithm strategy. |
| **2** | Balanced Binary Search Trees (AVL trees). Amortized Complexity and Splay Trees. Basic Graph Algorithms (BFS, DFS and applications), Strongly Connected Components, Maximum flow. |
| **3** | Single-Source Shortest Paths and Minimum Spanning Trees: implementation through heaps, Greedy Algorithm design. All Pairs Shortest Paths and other Dynamic Programming |

| | |
|---|---|
| | examples. |
| **4** | Overview of P, NP Problems, NP-Completeness and a brief introduction to Randomization, Approximation and Parameterized Complexity. |

**Lab Exercises:**

Implementation of linked list, stack, queue. Solving programs using recursion, Problems based on Single-Source Shortest Paths and Minimum Spanning Trees. Implementing sorting and searching algorithms, Implementation of hashing. Other interesting problems (from online platforms) where data structures need to be used in an intelligent way.

**References:**

1. Dexter C. Kozen, The Design and Analysis of Algorithms, ISBN 978-0-387-97687-7, Springer.
2. Douglas R. Stinson, Techniques for Designing and Analyzing Algorithms, ISBN 9780367228897, Chapman and Hall/CRC.
3. Gilles Brassard and Paul Bratley, Algorithmic Theory and Practice, ISBN 0-13-023243-2, Prentice Hall.
4. Jon Kleinberg and Eva Tardos, Algorithm Design, ISBN 0-321-29535-8, Pearson Education, 2006.
5. Jonathan L. Gross, Jay Yellen, Graph Theory and Its Applications, ISBN-13: 978-1584885054, Chapman and Hall/CRC.
6. M. H. Alsuwaiyal, Algorithms Design Techniques and Analysis, ISBN: 978-981-02-3740-0, World Scientific Publishing Co. Beijing.
7. Maarten van Steen, Graph Theory and Complex Networks: An Introduction, ISBN-13: 978-9081540612, Maarten van Steen.
8. NarasimhaKarumanchi, Algorithm Design Techniques: Recursion, Backtracking, Greedy, Divide and Conquer, and Dynamic Programming, Kindle Edition
9. OdedGoldreich, P, NP, and NP-Completeness: The Basics of Computational Complexity, ISBN-13: 978-0521192484, Cambridge University Press.
10. R.C.T. Lee, S.S. Tesng, R.C. Cbang and Y.T. Tsai,Design and Analysis of Algorithms, A strategic Approach, ISBN-13 :978-1259025822, McGraw Hill Education
11. Rajeev Motwani, PrabhakarRaghavan, Randomized Algorithms, ISBN 0-521-47465-5, Cambridge University Press.
12. Rodney G. Downey, Michael R. Fellows, Fundamentals of Parameterized Complexity, ISBN-13:978-1447155584, Springer.
13. S. K. Basu, Design Methods and Analysis of Algorithms,ISBN-13: 978-8120347465, Prentice Hall India.
14. T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, Introduction to algorithms, ISBN 978-0-262-03384-8, The MIT Press.
15. https://leetcode.com/

## M3010104 ADVANCED DISTRIBUTED SYSTEMS

| Course Code | Course Name | Lecture/Lab/Seminar/Project Credits | Year of Introduction |
|---|---|---|---|
| **M301104** | **Advanced Distributed Systems** | **3-1-0-0** | **2021** |

**Prerequisites:** Priorknowledge of operating systems, computer networks, distributed systems, DBMS, Graph Theory.

**Course Objectives:**

1. To understand the basic principles ofdistributed systems along with different core problems and their solutions.
2. To introduce the basics of communication technologies used in distributed platforms viz. computer networks, other inter process communications.
3. To explore real-life examples of distributed systems and how core problems related to

distributed systems are solved in those example domains.

4. To give hands on experience of working with and implementing distributed systems.

**Course Outcomes:**

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

**C01**: Understand the basic problems related to distributed systems and different solution algorithms.

**C02**: Apply the knowledge of distributed systems while developing distributed software solutions.

**C03**: Implement and configure the various state-of-the-art distributed systems solutions.

**C04**: Complete a term project, including independent research, oral presentation, and programming on a latest advancement in Distributed Systems.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written)

**PLO 5** Practice ethical standards of professional conduct and research

**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | | | 1 | | |
| **CO2** | 3 | 3 | 3 | 1 | | |
| **CO3** | 3 | 3 | 3 | 3 | 1 | 1 |
| **CO4** | 1 | 3 | 2 | 3 | 2 | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| 1 | Basics of Computer Networks:<br>Concept of layering: OSI and TCP/IP Protocol Stacks, Basics of packet, circuit and virtual circuit switching.Data link layer: framing, error detection, Medium Access Control, Ethernet bridging.Routing protocols, Fragmentation and IP addressing, IPv4, CIDR notation, Basics of IP support protocols (ARP, DHCP, ICMP), Network Address Translation (NAT).Transport layer: flow control and congestion control, UDP, TCP, sockets, Application layer protocols: DNS, SMTP, HTTP, FTP, Email, Introduction to Wireless Network. |
| 2 | Distributed Systems Fundamentals I:<br>Introduction: Distributed computing Issues and Solutions, Examples of distributed systems. Architecture: Types of distributed Architecture Concepts: Process-Threads, Client-Server, Remote Procedure Call (RPC), Remote Method Invocation, Virtualization, Inter-Process Communication. |
| 3 | Distributed Systems Fundamentals II:<br>Synchronization: Clock Synchronization, Mutual Exclusion, Leader Election.Consistency and Replication.Fault Tolerance. Security: secure channels, access control. |
| 4 | Distributed Systems' Examples:<br>*Cloud:* Introduction to Cloud Computing, Cloud Computing Platforms, Parallel Programming in the Cloud, Distributed Storage Systems, Virtualization(Multicore Operating Systems).<br>*Distributed Database Management Systems*: Introduction, Architecture, Design, Query Processing, Concurrency Control, Reliability Protocols.<br>Distributed File Systems, Peer-to-Peer Computing (Bit Torrent), Distributed Network |

| | |
|---|---|
| | (TOR), Distributed Version/Source Control System (Git) |

**Lab Exercises:**

**Module 1:**

Client-Server implementation (preferably using cloud-based virtual machines)

**Module 2:**

Message Queue implementation to communicate among multiple processes

**Module 3:**

Semaphore-based Mutual Exclusion Implementation

**Module 4:**

TOR implementation, Git Implementation, Distributed Data Processing with Apache Hadoop/Spark

**Books and other resources:**

1. A. S. Tanenbaum and M. V. Steen,“Distributed Systems, Principles and Paradigms,” 2nd Edition, 2016,Createspace Independent Pub.
2. S. Ghosh, “Distributed Systems, An Algorithmic Approach,”2nd Edition, 2020, Chapman and Hall/CRC.
3. H.Attiya and J. Welch,“Distributed Computing: Fundamentals, Simulations, and Advanced Topics,” 2nd Edition, 2006, Wiley.
4. G. F. Coulouris, J.Dollimore, T. Kindberg, and G. Blair,“Distributed Systems. Concepts and Design,”5th Edition, 2011, Pearson.
5. A. D. Kshemkalyani and M. Singhal,“Distributed Computing,”1st Edition, 2011, Cambridge University Press.
6. W. Stevens, B.Fenner, A. M. Rudoff, “Unix Network Programming, Volume 1: The Sockets Networking API,” 3rd Edition, 2015,Pearson Education India.
7. W.Stevens,“UNIX Network Programming,Volume2:InterprocessCommunications,”2nd Edition,2015, Pearson Education India.
8. A. S. Tanenbaum, “Computer Networks,”5thEdition, 2013, Pearson Education India.
9. B. A. Forouzan, “Data communication and Networking,”5th Edition,2012, Mc GrawHill, India.
10. J. F. Kurose, K. W. Ross, “Computer Networking: A top down approach,” 6th Edition, 2017, Pearson Education.
11. Recent Publications from top-Tier Conferences and Journals.

## M3010294 ADVANCED TOPICS IN CRYPTOGRAPHY

| Course Code | Course Name | Lecture/Lab/Seminar/Project Credits | Year of Introduction |
|---|---|---|---|
| **M301294** | **Advanced Topics in Cryptography** | **3-0-1-0** | **2021** |

**Prerequisites:** Cryptography Engineering

**Course Objectives**:

1. Learn how to do research in theoretical and applied cryptography.

2. Learn to develop cryptographic algorithms and prove their security.
3. Applying cryptographic algorithms and protocols to solve practical problems.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1**: Determine appropriate cryptographic primitives to solve real-world cyber security problems.

**CO2**: Evaluate security algorithms, protocols and related research works using rigorous approaches, including theoretical derivation, modeling, and simulations.

**CO3**: Formulate research problems in cryptography and cyber security.

**CO4**: Develop solutions to the formulated problems.

**CO5**: Clearly present ideas and research results.

**Program Learning Outcomes:**

**PLO1** Develop strong fundamental disciplinary knowledge

**PLO2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO3** Apply scholarship to conduct independent and innovative research

**PLO4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO5** Practice ethical standards of professional conduct and research;

**PLO6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 3 | 2 | 2 | 3 |
| **CO2** | 3 | 3 | 3 | 2 | 2 | 3 |
| **CO3** | 3 | 3 | 3 | 2 | 2 | 3 |
| **CO4** | 2 | 3 | 3 | 2 | 2 | 3 |
| **CO5** | 2 | 2 | 1 | 3 | 1 | 3 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Secure multi-party computation, zero-knowledge proof, zero-knowledge arguments, oblivious algorithms, trusted-hardware-assisted cryptography, verifiable computation, efficient authentication and verifiable delegation of computation mechanism, homomorphic commitments, searchable encryption, privacy-preserving authentication, privacy-enhancing-technologies, Computing over encrypted data, Fully Homomorhpic Encryption (FHE), Functional Encryption (FE)), Differential privacy. |
| **2** | Post-quantum cryptography, Design of post-quantum cryptographic primitives, Code-based cryptography, Lattice-based cryptography, Multivariate cryptography, Isogeny-based cryptography, physical unclonable functions, true and deterministic random number generators, cryptanalysis of post-quantum cryptosystem, provable security in the ROM and QROM, software and hardware implementations, performance and security analysis NIST candidates, cryptographic processors, efficient software and hardware architectures, secure implementation and optimization in hardware or software. |
| **3** | Machine learning to analyze cryptosystems, machine learning based cryptanalysis, Machine learning based key exchange framework, machine learning based threat and attack model generation, nonlinear aspects of cryptosystems, Attacks on implementations and their countermeasures, such as side-channel attacks, fault attacks, |

| | |
|---|---|
| | hardware tampering and reverse engineering techniques. |
| **4** | Light weight cryptography, optimization for high-Performance and lightweight cryptography, security and privacy issues for resource-constrained devices, security evaluation of real-world cryptographic systems, formal methods and verification tools for secure embedded design that offer provable security, and metrics for measuring security, cryptography for cyber-physical systems composed of analog and digital components, automotive security and trusted computing. |

**Text Books:**

1. David Evans, Vladimir Kolesnikov and Mike Rosulek. A Pragmatic Introduction to Secure Multi-Party Computation, NOW Publishers, 2018
2. Ronald Cramer, Ivan Damgård and Jesper Buus Nielsen. Secure Multiparty Computation and Secret Sharing, Cambridge University Press, 2015
3. Introduction to Modern Cryptography by Katz and Lindell.
4. Graduate Crypto Book by Dan Boneh and Victor Shoup.

**References:**

1. Yehuda Lindell. Secure Multiparty Computation (MPC), Communications of the ACM, January 2021
2. Manoj Prabhakaran and Amit Sahai (Eds.). Secure Multi-Party Computation, IOS Press, 2013
3. Zvika Brakerski, Fundamentals of fully homomorphic encryption, Providing Sound Foundations for Cryptography: On the Work
of Shafi Goldwasser and Silvio MicaliOctober 2019 Pages 543–563https://doi.org/10.1145/3335741.3335762
4. Mohammed M. Alani, Applications of machine learning in cryptography: a survey, ICCSP '19: Proceedings of the 3rd International Conference on Cryptography, Security and PrivacyJanuary 2019 Pages 23–27
5. William J Buchanan, Shancang Li, Shancang, Rameez Asif, Lightweight cryptography methods, March 2018, Journal of Cyber Security Technology.

## M3010242, M3020218 AI ETHICS AND SUSTAINABILITY

| Course Code | Course Name | Lecture/Lab/Seminar/Project Credits | Year of Introduction |
|---|---|---|---|
| **M301242,<br>M302218** | **AI Ethics and Sustainability** | **3-0-1-0** | **2021** |

**Prerequisites:** Nil

Course Objectives:

1. To equip the students with the ability to identify and analyse ethical issues related to the application of artificial intelligence.
2. To impart skills needed for the application of artificial intelligence in building sustainable systems.
3. To impart skills needed to address design issues related to socio ethic design capability with suitability as a major deign machine/deep learning techniques.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Pragmatic knowledge for understanding and analysing the application of artificial intelligence techniques in building sustainable systems

**CO2**: Problem identification and analysis skills on application domains requiring machine/deep learning techniques

**CO3:** Solution design capability with machine/deep learning techniques

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | 2 |
| **CO2** | 2 | 3 | 3 | 2 | | 2 |
| **CO3** | 2 | 3 | 3 | 2 | | 2 |

(Correlation: 1: Slight (Low)   2: Moderate (Medium)    3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | AI and Humans, Super Intelligence and challenges, Data and data intelligence, Privacy and the Other Usual Suspects, Responsible Machines and Unexplainable Decisions. Policy aspects |
| **2** | Explainable AI - Black box models to XAI, An XAI case study, AI Bias and Ethics - role of explainable AI. Machine Learning and explainabily |
| **3** | Sustainability-definition, UN sustainable development goals, role of data on building sustainable models. Automation and scalability - opportunities and challenges. |
| **4** | AI applications in sustainable development - healthcare, natural resources monitoring and management, agriculture. |

**Lab/Assignment:**

A term paper (prepared by a group of two) based on recent literature

**Text Books:**

1. AI Ethics, Mark Coeckelbergh, MIT Press, 2020
2. Hands-On Explainable AI (XAI) with Python: Interpret, visualize, explain, and integrate reliable AI for fair, secure, and trustworthy AI apps, Denis Rothman, Packt Publishing Limited, 2020

**References:**

1. https://sdgs.un.org/
2. The role of artificial intelligence in achieving the Sustainable Development Goals , Ricardo Vinuesa etal., Nature Communications, 2020

## M3010101 AI & MACHINE LEARNING

| **Course Code** | **Course Name** | **Lecture/Lab/Seminar/Project Credits** | **Year of Introduction** |
|---|---|---|---|
| **M301101** | **AI & Machine Learning** | **3-1-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To impart algorithmic skills needed for designing AI and machine learning techniques and solutions.
2. To equip the students with the ability to identify and analyse problems solvable with

AI/machine learning algorithms/techniques.

3. To impart solution design capability with AI/machine learning techniques.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:**Algorithm design/analysis capability in AI/Machine Learning

**CO2**: Problem identification and analysis skills on application domains requiring AI/machine learning techniques

**CO3:** Solution design capability with AI/machine learning techniques

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge.

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature.

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | 2 |
| **CO2** | 2 | 3 | 3 | 2 | | 2 |
| **CO3** | 2 | 3 | 3 | 2 | | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Artificial Intelligence - Turing Test, Rule/Logic based AI and Machine Learning Based AI, Importance of search in AI - uninformed and informed search, local search - gradient descent, modelling the brain - Perceptron, Back Propagation Algorithm, Narrow and General AI. |
| **2** | Machine Learning Paradigms: Supervised, Unsupervised and reinforcement Learning. Generalization performance, Bias-Variance tradeoffs, Feature Engineering - relevance, feature extraction - PCA. Supervised Learning: - Classification - Bayesian, Decision Tree and Random Forests, Ensemble Methods - Boosting and Bootstrap Aggregation, Regression - linear, logistic. |
| **3** | Unsupervised Learning: Density Estimation - Maximum Likelihood and Parzen Windows, Clustering - Partition Based, Subspace Clustering, Incremental Clustering, Spectral Clustering. Sequence Modelling - Hidden Markov Models. |
| **4** | Statistical Learning theory - Empirical Risk Minimization, and Structural Risk Minimisation: VC Dimension. Kernel Machines - Support Vector Machines, Support Vector Clustering, Support Vector Regression, Scalable Kernel Machines, Deep Kernel Machines - Deep Kernels and Multi Kernel Learning |

**Lab Exercises:**

**Module 1:**

Experiments on Google AI Experiments platform, Implementation of Perceptron

**Module 2:**

Implementation of PCA, Nave Bayes Classifier, Logistic Regression

**Module 3:**

Implementation of ML Estimation, K-Means and HMM

**Module 4:**

Experiments with SVM Libraries - SVM and Deep SVM

**Text Books:**

1. Artificial Intelligence: A Modern Approach 4th Edition, Stuart Russell and Peter Norvig, Pearson, 2020
2. Understanding Machine Learning: From Theory to Algorithms, Shai ShalevShwartz, ShaiBen-David, Cambridge University Press, 2014
3. Deep Learning, Ian Good fellow, Yoshua Bengio, Aron Courville, The MIT Press, 2016

**References:**

**1.** Neural Networks and Learning Machines, Simon Haykin, Person, 2009.

2. Mastering Machine Learning Algorithms, Giuseppe Bonaccorso, Ingram short title, 2018

## M3010274 AI BASED CYBER ATTACKS AND DEFENSES

| Course Code | Course Name | Lecture/Lab/Seminar/Project Credits | Year of Introduction |
|---|---|---|---|
| M301274 | AI Based Cyber Attacks and Defences | 3-0-0-1 | 2021 |

**Prerequisites:** Nil

**Course Objectives:**

1. To provide students with a good understanding of the concepts of AI, ML and deep learning for applying to various cyber security problems.
2. To help the students develop the ability to solve cyber security problems using the learned concepts.
3. To help the students to build autonomous cyber defence systems.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Apply the AI, ML and deep learning concepts for solving various cyber security problems.

**CO2**: Employ AI,ML and DL concepts to identify research gaps in cyber security.

**CO3:** Develop autonomous cyber defence systems

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 1 | | | 3 | | 1 |
| CO2 | | | 3 | 3 | | 1 |
| CO3 | | 3 | 3 | 3 | 3 | 3 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | Applications of AI, machine learning and deep learning in cyber security: spam email |

| | |
|---|---|
| | detection, phishing page detection, malware detection, DoS and DDoS attack detection, anomaly detection, SQL injection attack detection, detection of APT, fraud detection, security risk analysis/estimation, vulnerability detection, prediction of cyber attacks, Intrusion Detection and Prevention Systems (IDS/IPS), Spam and Social Engineering Detection, Network Traffic Analysis, User/Machine Behavior Analytics |
| **2** | Adversarial attacks on machine learning based cyber security systems, Offensive AI and counter measures, Autonomous cyber attacks, secure and privacy preserving machine learning, |
| **3** | Explainable AI for Cyber Security, Enhancing the Trustworthiness of Systems: AI-based reasoning aligned with cyber security priorities, AI for reliable software systems and identity management, Autonomous and Semi autonomous Cyber Security, |
| **4** | Autonomous threat hunting, Threat Modelling, Vulnerability and Risk Management, Autonomous cyber defence, Self learning system, Predictive Analytics for Cyber Security, Applications of Game Theory, Human-AI interfaces, Cognitive security |

**Text Books:**

1. Tony Thomas, Athira P. Vijayaraghavan, Sabu Emmanuel, Machine Learning Approaches in Cybersecurity Analytics, Springer 2020.
2. Clarence Chio, David Freeman, Machine Learning & Security, O Reilly, 2018
3. Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein , Adversarial Machine Learning, Cambridge University Press, 2019.
4. Deep Learning Applications for Cyber Security, Alazab, Mamoun, Tang, MingJian (Eds.), Springer
5. Rakesh M. Verma, David J. Marchette, Cybersecurity Analytics, 2019 by Chapman and Hall/CRC
6. Sushil Jajodia et al, Adaptive Autonomous Secure Cyber Systems, Springer 2020
7. Wojciech Samek et al (ed.), Explainable AI: Interpreting, Explaining and Visualizing Deep Learning, Springer 2019
8. Leslie F. Sikos et al (ed.),AI in Cybersecurity, Springer, 2018

**References:**

1. Alexey Kleymeno , AmrThabetv , Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoTattacks ,2019.
2. Monappa KA, Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, Packt Publication, 2018.
3. Xin et al, Machine Learning and Deep Learning Methods for Cybersecurity, IEEE Access 2018
4. Bowei Xi, Adversarial machine learning for cybersecurity and computer vision: Current developments and challenges, WIREs Computational Statistics, April 2020
5. Mohammad Al-Rubaie, Privacy Preserving Machine Learning: Threats and Solutions,IEEE Security and Privacy Magazine
6. Aiyanyo et al, A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning, Applied Sciences, MDPI, Aug 2020
7. Shaukat et al, A Survey on Machine Learning Techniques for Cyber Security in the Last Decade, IEEE Access, Dec 2020.

## M3020303 APPLIED CRYPTOGRAPHY

| Course Code | Course Name | Lecture/Lab/Seminar/Project Credits | Year of Introduction |
|---|---|---|---|
| M302303 | **Applied Cryptography** | **3-0-1-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

- To introduce the fundamental and practical applications of cryptographic algorithms
- To help the students develop the ability to apply cryptographic solutions to cyber

security problems.

- To help the students to build secure cloud, IoT and other systems.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Summarize the cryptographic aspects of Internet protocols

**CO2**: Apply cryptography techniques for securing IoT applications

**CO3:** Apply Cryptography for security and privacy in cloud

**CO4:** Apply cryptographic techniques for many real life and practical applications

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 2 | 2 | 2 | 1 |
| **CO2** | 3 | 3 | 1 | 1 | 1 | 2 |
| **CO3** | 3 | 3 | 1 | 1 | 1 | 2 |
| **CO4** | 3 | 3 | | | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| 1 | Cryptographic aspects of Internet protocols, TLS/SSLsecurity at the transport layer, IPSec-security at the network layer, IEEE802.11 Wireless LAN security, Mobile phone Security, RFIDs and E-Passports, Electronic Payment Systems, Electronic Voting Machines, Web Services Security |
| 2 | Security Requirements in IoT Architecture - Security in Enabling Technologies - Security Concerns in IoT Applications, Authentication/Authorization for Smart Devices, Transport Encryption, security engineering for IoT development |
| 3 | Cryptography for security and privacy in cloud, Privacy preserving authentication, anonym ous credential systems, privacy preserving disclosure of data, privacy preserving access to resources, accesscontrol through encryption, computingon encrypted data, remote data checking, secure data deduplication, searchable encryption |
| 4 | Crypto-currencies, Bitcoin, P2P network, distributed consensus, incentives and proof-of-work, mining, scripts and smart contracts, wallets: hot and cold storage, anonymity, altcoins. |

**Textbooks:**

1. B L Menezes, R. Kumar, Cryptography, Network Security, and Cyber Laws, Cengage, 2019
2. William Stallings, Cryptography and Network Security Principles and Practice, Sixth Edition, Pearson
3. Sunil Cheruvu , Anil Kumar , Ned Smith , David M. Wheeler , Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment , Apress; 1st ed. edition (August 14, 2019)
4. Stefan Rass , Daniel Slamanig , Cryptography for Security and Privacy in Cloud Computing, Artech House (1 November 2013

5. B. Singhal, G. Dhameja, P S Panda, Beginning Block chain, Apress, 2018
6. A.Narayananetal.,"Bitcoin and Cryptocurrency Technologies:AComprehensive Introduction," Princeton University Press, 2016.

**References:**

1. B. Rusell and D. Van Duren, "Practical Internet of Things Security," Packt Publishing, 2016.
2. Johnson Jr, C. Richard, William A. Sethares, and Andrew G. Klein,"Software receiver design: build your own digital communication system in five easy steps,Cambridge University Press, 2011.3
3. A. Antonopoulos, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies," O'Reilly, 2014.
4. T. Alpcan and T. Basar, "Network Security: A Decision and Game-theoretic Approach," Cambridge University Press, 2011

## M3020334 ARTIFICIAL INTELLIGENCE

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M302334** | **Artificial Intelligence** | **3-0-1-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To provide students with a good understanding of the concepts of information theoretic methods of artificial intelligence described in the syllabus.
2. To help the students develop the ability to solve problems using the learned concepts.
3. To connect the concepts to other domain both within and without mathematics such as pattern recognition.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Understand the foundations of modern artificial intelligence theory, problem and state of the art solutions.

**CO2**: Analyze and evaluate critically the building and integration of artificial intelligence.

**CO3:** Design and demonstrate a working artificial intelligence through team research project, and project report, presentation.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge.

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature.

**PLO 3** Apply scholarship to conduct independent and innovative research.

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences.

**PLO 5** Practice ethical standards of professional conduct and research.

**PLO 6**Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | |
| **CO2** | 3 | 3 | 3 | 2 | | |
| **CO3** | 2 | 3 | 3 | 3 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | Introduction to AI, Turing test, Problem Definition -Production systems, Control strategies, Search strategies. Problem solving methods –Problem graphs, Matching, Indexing and Heuristic functions. |
| 2 | Search - Hill Climbing-Depth first and Breath first, Constraints satisfaction. Knowledge representation, Knowledge representation using Predicate logic, Resolution, Knowledge representation under uncertainty |
| 3 | Structured representation of knowledge - Basic plan generation systems – Strips – Expert systems – Architecture - Roles – Knowledge Acquisition – Meta knowledge, Heuristics - Knowledge representation – Production based system, Frame based system. |
| 4 | Inference – Backward chaining, Forward chaining, Fuzzy reasoning, Bayesian ReasoningLearning Machine learning, adaptive learning. Intelligent Agents - agents and environment - types of agents -collaborative agents. |

**Text Books:**

1. Kevin Night and Elaine Rich, Nair SB., Artificial Intelligence Third Edition, McGraw Hill, 2017.
2. Stuart Russel and Peter Norvig, Artificial Intelligence - A Modern Approach 4th Edition, Person Education, 2020

**References:**

1. Peter Jackson, “Introduction to Expert Systems”, 3rd Edition, Pearson Education, 2007.
2. Dan W. Patterson, “Introduction to AI and ES”, Pearson Education, 2007.

## M3020333 ARTIFICIAL INTELLIGENCE FOR CYBER SECURITY

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M302333 | **Artificial Intelligence for Cyber Security** | **3-0-1-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To provide students with a good understanding of the concepts of AI, ML and deep learning for applying to various cyber security problems.
2. To help the students develop the ability to solve cyber security problems using the learned concepts.
3. To help the students to build autonomous cyber defense systems.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Apply the AI, ML and deep learning concepts for solving various cyber security problems.

**CO2**: Employ AI,ML and DL concepts to identify research gaps in cyber security.

**CO3:** Develop autonomous cyber defence systems

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 1 | | | 3 | | 1 |
| CO2 | | | 3 | 3 | | 1 |
| CO3 | | 3 | 3 | 3 | 3 | 3 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Applications of AI, machine learning and deep learning in cyber security: spam email detection, phishing page detection, malware detection, DoS and DDoS attack detection, anomaly detection, SQL injection attack detection, detection of APT, fraud detection, security risk analysis/estimation, vulnerability detection, prediction of cyber attacks, Intrusion Detection and Prevention Systems (IDS/IPS), Spam and Social Engineering Detection, Network Traffic Analysis, User/Machine Behavior Analytics |
| **2** | Adversarial attacks on machine learning based cyber security systems, Offensive AI and counter measures, Autonomous cyber attacks, secure and privacy preserving machine learning, |
| **3** | Explainable AI for Cyber Security, Enhancing the Trustworthiness of Systems: AI-based reasoning aligned with cyber security priorities, AI for reliable software systems and identity management, Autonomous and Semi autonomous Cyber Security, |
| **4** | Autonomous threat hunting, Threat Modelling, Vulnerability and Risk Management, Autonomous cyber defence, Self learning system, Predictive Analytics for Cyber Security, Applications of Game Theory, Human-AI interfaces, Cognitive security |

**Text Books:**

1. Tony Thomas, Athira P. Vijayaraghavan, Sabu Emmanuel, Machine Learning Approaches in Cybersecurity Analytics, Springer 2020.
2. Clarence Chio, David Freeman, Machine Learning & Security, O Reilly, 2018
3. Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein , Adversarial Machine Learning, Cambridge University Press, 2019.
4. Deep Learning Applications for Cyber Security, Alazab, Mamoun, Tang, MingJian (Eds.), Springer
5. Rakesh M. Verma, David J. Marchette, Cybersecurity Analytics, 2019 by Chapman and Hall/CRC
6. Sushil Jajodia et al, Adaptive Autonomous Secure Cyber Systems, Springer 2020
7. Wojciech Samek et al (ed), Explainable AI: Interpreting, Explaining and Visualizing Deep Learning, Springer 2019
8. Leslie F. Sikos et al (ed.),AI in Cybersecurity, Springer, 2018

**References:**

1. Alexey Kleymenov Amr Thabet, Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoTattacks ,2019.
2. Monappa KA, Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, Packt Publication, 2018.
3. Xin et al, Machine Learning and Deep Learning Methods for Cybersecurity, IEEE Access 2018
4. Bowei Xi, Adversarial machine learning for cybersecurity and computer vision: Current developments and challenges, WIREs Computational Statistics, April 2020
6. Mohammad Al-Rubaie, Privacy Preserving Machine Learning: Threats and Solutions, n IEEE Security and Privacy Magazine
7. Aiyanyo et al, A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning, Applied Sciences, MDPI, Aug 2020
8. Shaukat et al, A Survey on Machine Learning Techniques for Cyber Security in the Last Decade, IEEE Access, Dec 2020.

## M3010282, M3020205 AUGMENTED AND VIRTUAL REALITY

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M301282, M302205 | Augmented and Virtual Reality | 3-1-0-0 | 2021 |

**Prerequisites:** Nil

**Course Objectives:**

1. To provide students with an understanding of concepts and frameworks of immersive technologies.
2. To help students get familiarized with hardware and software of AR/VR systems.
3. To help the students develop immersive technology applications.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Apply the concepts of immersive technologies to manage large scale virtual environment in real time.

**CO2**: Employ the AR/VR concepts to identify the research gaps.

**CO3:**Develop AR/VR systems for application in varied areas.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 1 | | | 3 | | 1 |
| CO2 | | 3 | 3 | | | 1 |
| CO3 | | 3 | 3 | 3 | 3 | 3 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | **Familiarisation with Immersive Technologies**<br>Human perception and cognition: Human auditory system, Human visual system, Visual perception, Visual rendering; Motion in real and virtual worlds; 3D Computer graphics: virtual world space, virtual observer positioning, 3D clipping, 3D modelling, illumination and reflection models, shading algorithms; Tracking: 2D orientation, 3D orientation, characteristics, types of trackers, SLAM; Sound in immersive environments: evolution, sound design basics, natural vs. real sound; Milgram's Reality-virtuality Continuum; Ethics, scientific concerns, social consequences, health and safety issues. |
| 2 | **Augmented Reality**<br>History and evolution of AR; Components for visualising AR: sensors, processor, display devices; Software components in AR: environmental acquisition, sensor integration, application engine, rendering software; Types of AR experiences: Marker based, marker-less, projection based; Augmented Reality Markup Languages (ARML): Types; Augmented reality content: Content creation, tools; User interface; Computer vision algorithms for AR: Marker tracking, infrared tracking, feature tracking, incremental tracking, localization and mapping, outdoor tracking; Interaction in real world: Manipulation, Navigation, Communication; Types of AR interaction: Browsing, 3D, |

| | |
|---|---|
| | tangible; Tangible AR; Collaborative AR; Mobile AR: technologies, promises and constraints; Existing challenges; Styles of augmented reality applications: magic books, magic mirrors, magic windows and doors, magic lens, navigation assistance, non-referential augmentation, objective view augmented reality ; Familiarisation with Microsoft HoloLens, ARCore. |
| 3 | **Virtual Reality**<br>Key elements of VR experience; History and evolution of VR; Virtual reality systems: tracking, Aural display, haptic display, vestibular display, visual displays- stationary, head based, hand-held; Rendering the virtual world- Aural representation, haptic representation, rendering systems- visual, aural, haptic; Interaction with virtual world: Manipulation, Navigation, Communication; Virtual reality experience: immersion, types of virtual world; Designing VR experience; Development tools and framework: software development tool frameworks, X3DStandard; VR software integration, game engines; Existing challenges; Familiarisation with OculusRift and Unity 3D. |
| 4 | **Related Technologies, Applications and Potential Research Areas**<br>Related Technologies: Mixed Reality, XR, Comparison of immersive technologies; Areas and industries for immersive technologies: entertainment, education, training, medical, industrial, military; Case-studies: Design and evaluation, Production pipeline: sensing, rendering, mobile, stand alone and high-end computing platforms; Potential research directions: design, prototyping, innovative applications, cloud services, IoT, cyber physical systems. |

**Text Books:**

1. Alan B. Craig, Morgan Kaufmann, "Understanding Augmented Reality, Concepts and Applications", 2013.
2. Alan B. Craig and William R. Sherman, "Understanding Virtual Reality: Interface, Application, and Design", 2002.
3. Steven M. LaValle. Virtual Reality. Cambridge University Press, 2017.
4. Chung Van Le, Dac-Nhuong Le, Jolanda G. Tromp, "Emerging Extended Reality Technologies for Industry 4.0 Early Experiences with Conception, Design, Implementation, Evaluation and Deployment", 2020.
5. Steve Aukstakalnis, "Practical Augmented Reality A Guide to the Technologies, Applications, and Human Factors for AR and VR", Pearson Education, 2016.

**References:**

1. Alan B Craig, William R Sherman and Jeffrey D Will, "Developing Virtual Reality Applications: Foundations of Effective Design", Morgan Kaufmann, 2009.
2. Jung, Timothy, and M. Cluaudia tom Dieck. "Augmented Reality and Virtual Reality." Empowering Human, Place and Business. Cham: Springer International Publishing 2018.
3. D. Schmalstieg and T. Höllerer. Augmented Reality: Principles and Practice. Addison-Wesley, Boston, 2016.
4. Samuel Greengard, "Virtual Reality", MIT Press, 2019.
5. Dennis Vroegop, "Microsoft HoloLens Developer's Guide", Packt Publishing, 2017.
6. Micheal Lanham, "Learn ARCore — Fundamentals of Google ARCore: Learn to build augmented reality apps for Android, Unity, and the web with Google ARCore 1.0", Packet Publishing, 2018.
7. Ong, Sean, "Beginning Windows Mixed Reality Programming For HoloLens and Mixed Reality Headsets", 2021.
8. Philippe Fuchs, "Virtual Reality Headsets - A Theoretical and Pragmatic Approach", CRC Press, 2017.

## M3021312 BIG DATA TECHNOLOGIES

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of<br>Introduction |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **M302312** | **Big Data Technologies** | **3-0-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

- To introduce various technologies related to big data analysis
- To enable the students to design big data analysis systems using machine learning

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Understand the concept of bigdata

**CO2:** Analyze and process bigdata using Apache Spark

**CO3:** Perform mining in data stream

**CO4:** Design bigdata analysis system using machine learning with spark

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 2 | 1 | 2 | 1 |
| **CO2** | 3 | 2 | 1 | 1 | 1 | 1 |
| **CO3** | 3 | 3 | 1 | 1 | 1 | 2 |
| **CO4** | 3 | 3 | 2 | 1 | 2 | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Introduction to Big Data Technology, Hadoop, HDFS and MapReduce, Hadoop Environment, Messaging systems, Distributed SQL Query Engines |
| **2** | Introduction to Apache Spark, Spark Cluster ASpark Core, High level architecture, Spark Context, RDD, Lazy Operation, Caching methods, Spark SQL |
| **3** | Mining data stream, Examples of data stream applications, Sampling in data streams, Filtering streams, Counting distinct elements in stream, Querying on Windows |
| **4** | Machine learning with spark, Spark Machine Learning libraries, Spark ML and Applications, Graph Processing with Spark |

**Text Books:**

1. Data Analytics with Spark Using Python, By Jeffrey Aven, Addison Weley Data & Analytics series, 2018
2. Big Data Analytics with Spark, Mohammed Guller, APress, 2015

**References:**

1. Anand Rajaraman, Jeffrey D Ullman. Mining of Massive Datasets, Cambridge University Press 2010

## M3010283 BIOMETRIC SYSTEMS ENGINEERING

| **Course Code** | **Course Name** | **Credit Split**<br>**Lecture/Lab/Seminar/Project** | **Year of Introduction** |
|---|---|---|---|

| M301283 | Biometric Systems Engineering | 3-1-0-0 | 2021 |
|---|---|---|---|

**Prerequisites:** Nil

**Course Objectives:**

- To provide fundamental knowledge of various biometric systems
- To enable the students to develop prototypes of biometric systems
- To enable the students to do research in biometrics

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Analyze the fundamentals of biometric systems and it’s components, advantages and disadvantages of the existing biometric modalities and emerging biometric traits.

**CO2**: Develop a prototype device to acquire the biometric data

**CO3:** Design a recognition system based on the biometric algorithms using any biometric modality

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 1 | 2 | 2 | 2 | 2 | 1 |
| **CO2** | 2 | 1 | 1 | 1 | 1 | 2 |
| **CO3** | 2 | 1 | 1 | 1 | 1 | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Introduction to Biometric Systems<br>Physiological and behavioral biometrics: fingerprint, face, iris, keystroke dynamics, Signature, Gait; Biometric system components; Stages of operation: enrolment, verification, identification, identification vs verification; Multibiometrics; Information fusion; Emerging biometric modalities: electrophysiological biometrics, DNA, gait, vascular biometrics, ear shape, soft biometrics, molecular biometrics, multispectral biometrics; Overview of design stages and constraints. |
| **2** | Familiarization with sensors<br>Types of acquisition: contact and contactless acquisition of various biometric modalities- advantages, disadvantages;<br>Sensors - components, working and applications: motion sensor, temperature sensor, depth sensor, ultrasonic sensor, swipe sensor, heart rate sensor,<br>Imaging sensor- cameras- working, applications: near-infrared, night vision, thermal, visible light;<br>3D imaging techniques- definition, working, existing techniques and applications in biometric: computed tomography, 3D laser imaging, structured light imaging, interferometry<br>Familiarization with device prototyping- fingerprint scan, face scan, iris scan, hand geometry, vascular imaging: hand vein, palm vein, finger vein |
| **3** | Biometric Algorithms |

| | |
|---|---|
| | Pre-processing: Noise removal, Region of interest extraction, Enhancement<br>Feature extraction: Texture based: LBP and its variants, HoG, Gabor filter, Log Gabor, GLCM, Statistical-based: ICA, LDA, PCA and its variants, Moments, Transform based: DWT, DFT, Hough transform, shearlet, contourlet, MFCC features;<br>Keypoint descriptors: SIFT, SURF, RANSAC, FAST, ML-based: vocabulary learning methods: clustering (K-Means, GMM), Extreme learning machines, deep learning;<br>Matching: Distance-based: Euclidean, Hamming; Classifier based: KNN, SVM, Deep learning<br>Implementation of any of the biometric-based recognition using these techniques |
| **4** | Evaluation, testing, standards, security and privacy issues<br>Biometric system errors: Type I, Type II errors, EER, ROC, DET; Testing - enrolment, verification and identification processes;<br>Biometric standards: overview, standards organizations, approved biometric standards;<br>Privacy issues, Attacks on the biometric system: types of attacks- reconstruction attacks, PA GAN-based attacks;<br>Countermeasures- Sensor level, Software-based techniques, liveness detection, PAD;<br>Template security: biometric cryptosystems: key generation, key binding, feature transformation: non-invertible transform, salting; Biometric encryption, Biometric Applications. |

**Text Books:**

1. Anil K Jain, Patrick Flynn, Arun A Ross, Handbook of Biometrics, Springer, 2008
2. Ted Dunstone and Neil Yager, Biometric System and Data Analysis: Design, Evaluation, and data Mining, Springer
3. R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, Guide to Biometrics, Springer
4. Reid, P., Biometrics for Network Security, Dorling Kingsley (2007)
5. Woodward, J.D. and Orlans, Nicholos M., Biometrics, McGraw Hill (2002)

**References:**

1. Jiang, Richard, et al. Deep Biometrics. Springer-Verlag, 2019.
2. Jain, A.K., Nandakumar, K. and Nagar, A., 2008. Biometric template security. EURASIP Journal on advances in signal processing, 2008, pp.1-17.
3. Alonso-Fernandez, F., Fierrez, J. and Ortega-Garcia, J., 2011. Quality measures in biometric systems. IEEE Security & Privacy, 10(6), pp.52-62.
4. Campisi P. Security and privacy in biometrics. London: Springer; 2013 Jun 28.
5. Ratha, N.K. and Govindaraju, V. Advances in biometrics: sensors, algorithms and systems. Springer Science & Business Media, 2007

## M3020215 BIOMETRICS

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M302215** | **Biometrics** | **3-1-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

- To provide fundamental knowledge of various biometric systems
- To enable the students to develop prototypes of biometric systems
- To enable the students to explore new biometric modalities

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Analyze the fundamentals of biometric systems and it’s components, advantages and disadvantages of the existing biometric modalities and emerging biometric traits.

**CO2**: Develop a prototype device to acquire the biometric data

**CO3:** Design a recognition system based on the biometric algorithms using any biometric modality

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 1 | 2 | 2 | 2 | 2 | 1 |
| **CO2** | 2 | 1 | 1 | 1 | 1 | 2 |
| **CO3** | 2 | 1 | 1 | 1 | 1 | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Introduction to Biometric Systems<br>Physiological and behavioral biometrics: fingerprint, face, iris, keystroke dynamics, Signature, Gait; Biometric system components; Stages of operation: enrolment, verification, identification, identification vs verification; Multibiometrics; Information fusion; Emerging biometric modalities: electrophysiological biometrics, DNA, gait, vascular biometrics, ear shape, soft biometrics, molecular biometrics, multispectral biometrics; Overview of design stages and constraints. |
| **2** | Familiarization with sensors<br>Types of acquisition: contact and contactless acquisition of various biometric modalities- advantages, disadvantages;<br>Sensors - components, working and applications: motion sensor, temperature sensor, depth sensor, ultrasonic sensor, swipe sensor, heart rate sensor, Imaging sensor-cameras- working, applications: near-infrared, night vision, thermal, visible light;<br>3D imaging techniques- definition, working, existing techniques and applications in biometric: computed tomography, 3D laser imaging, structured light imaging, interferometry |
| **3** | Biometric Algorithms<br>Pre-processing: Noise removal, Region of interest extraction, Enhancement<br>Feature extraction: Texture based: LBP and its variants, HoG, Gabor filter, Log Gabor, GLCM, Statistical-based: ICA, LDA, PCA and its variants, Moments, Transform based: DWT, DFT, Hough transform, shearlet, contourlet, MFCC features;<br>Keypoint descriptors: SIFT, SURF, RANSAC, FAST, ML-based: vocabulary learning methods: clustering (K-Means, GMM), Extreme learning machines, deep learning;<br>Matching: Distance-based: Euclidean, Hamming; Classifier based: KNN, SVM, Deep learning |
| **4** | Evaluation, testing, standards, security and privacy issues<br>Biometric system errors: Type I, Type II errors, EER, ROC, DET; Testing - enrolment, verification and identification processes;<br>Biometric standards: overview, standards organizations, approved biometric standards;<br>Privacy issues, Attacks on the biometric system: types of attacks- reconstruction |

| | |
|---|---|
| | attacks, PA GAN-based attacks;<br>Countermeasures- Sensor level, Software-based techniques, liveness detection, PAD;<br>Template security: biometric cryptosystems: key generation, key binding, feature transformation: non-invertible transform, salting; Biometric encryption, Biometric Applications. |

**Text Books:**

1. Anil K Jain, Patrick Flynn, Arun A Ross, Handbook of Biometrics, Springer, 2008
2. Ted Dunstone and Neil Yager, Biometric System and Data Analysis: Design, Evaluation, and data Mining, Springer
3. R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, Guide to Biometrics, Springer
4. Reid, P., Biometrics for Network Security, Dorling Kingsley (2007)
5. Woodward, J.D. and Orlans, Nicholos M., Biometrics, McGraw Hill (2002)

**References:**

1. Jiang, Richard, et al. Deep Biometrics. Springer-Verlag, 2019.
2. Jain, A.K., Nandakumar, K. and Nagar, A., 2008. Biometric template security. EURASIP Journal on advances in signal processing, 2008, pp.1-17.
3. Alonso-Fernandez, F., Fierrez, J. and Ortega-Garcia, J., 2011. Quality measures in biometric systems. IEEE Security & Privacy, 10(6), pp.52-62.
4. Campisi P. Security and privacy in biometrics. London: Springer; 2013 Jun 28.
5. Ratha, N.K. and Govindaraju, V. eds., 2007. Advances in biometrics: sensors, algorithms and systems. Springer Science & Business Media.

## M3020313 BLOCK CHAIN TECHNOLOGY

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M302313** | **Blockchain Technology** | **3-1-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To provide students with a deeper understanding of the concepts of blockchain technology with due focus on decentralized computing and distributed systems described in the syllabus.
2. To help the students develop the ability to address real-world problems using the learned concepts of smart contracts and Dapps.
3. To connect the learned concepts with other business domains having opportunities of disruptive innovation with blockchain
4. To make students aware of the existing challenges of blockchain and focus on contributing revolutionary solutions of the same

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Apply the science of blockchain technology in modelling better solutions distributed computing.

**CO2**: Analyze the variants of blockchain/DLT and their adoption in respective domains

**CO3:** Visualize the use of blockchain technology and its potential disruptions in multiple business domains in the coming era.

**Program Learning Outcomes:**

**PLO1** Develop strong fundamental knowledge about the underlying concepts of blockchain technology

**PLO 2** Demonstrate in-depth understanding of different blockchain types, architectures and
distributed consensus methods.

**PLO 3** Critically compare and evaluate the need of Blockchain/DLT in industry

**PLO 4** Alert the problems and challenges in deploying blockchain based Dapps and Smart Contracts with a deeper understanding of the multiple tradeoffs in the proposed product.

**PLO 5** Demonstrates the disruptive potential of blockchain technology in revolutionizing the existing business models.

**PLO 6** Acquire research skills to propose better algorithms/solutions for the existing challenges and contribute to the upcoming blockchain protocols.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 2 | 2 | 2 | 3 |
| **CO2** | 2 | 3 | 3 | 3 | 3 | 2 |
| **CO3** | 2 | 3 | 3 | 3 | 3 | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Fundamentals of Blockchain technology : Centralized Vs Decentralized Computing, Concept of Distributed Ledger. Cryptographic principles - Encryption Techniques , Block Ciphers, Hash Functions (SHA), Digital Signatures, Public-Key Cryptography (RSA, ECDSA), Merkle Trees, DAG, PKI. Distributed Systems - Basic principle , design, architecture, Inter-process communication, peer-to-peer networks. Features of Blockchain. Blockchain vs Database, Blockchain vs Internet. |
| **2** | Blockchain network: Byzantine Generals Problem, Consensus Approach - PoW, PoS, pBFT. Working of Bitcoin network - Nodes, Forks, Mining, Wallets, UTXO Model. Challenges of Blockchain Technology. Blockchain Architectures: Public, Private, Hybrid. Potential Threats. - 51% attack, Sybil and Eclipse attacks. |
| **3** | Programmable Blockchains - Smart Contracts, Dapps. Introduction to Ethereum - Architecture, EVM. Token Standards - Fungible and Non-fungible (ERC). Hyperledger Umbrella Projects. Corda DLT. Why or Why Not Blockchain. Next Generation Blockchains - Cardano, Algorand, Polkadot. Application of Blockchain - Banking, Supply chain, Governance |
| **4** | Advanced Concepts - ZKPs, Sharding and sidechains, Layer-2 Protocols solving Blockchain Trilemma. Decentralized Finance (DeFi), Decentralized Autonomous Organizations (DAO). SegWit. BIP and EIP. |

**Lab Experiments:**

Experiments will be done with Ethreum and Hyperledger Fabric

**Text Books:**

1. Mastering Blockchain - Third Edition, Imran Bashir, 2020
2. Blockchain Revolution, Don and Alex Tapscott, 2018.
3. Mastering Ethereum: Building Smart Contracts and DApps, by Andreas M. Antonopoulos and Gavin Wood

**References:**

1. Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, 2009, https://bitcoin.org/bitcoin.pdf.
2. The Basics of Bitcoins and Blockchains, Antony Lewis 2018.

## M3010213, M3020245 CLOUD AND EDGE COMPUTING

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301213, M302245** | **Cloud and Edge Computing** | **3-0-0-1** | **2021** |

**Prerequisites:** Prior knowledge of operating systems, distributed systems, computer networks, machine and deep learning.

**Course Objectives:**

1. To impart a comprehensive and in-depth understanding of Cloud and Edge Computing basics, technologies and applications to M.Tech students by introducing and researching cutting-edge topics, technologies, applications and implementations.
2. To expose the students to frontier areas of Cloud and Edge Computing while providing sufficient foundations for further study and research.

**Course Outcomes:**

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

**C01**: Understand the foundations of distributed algorithms and concepts and issues related tocloud and edge computing through completion of homework, quizzes, and examinations.

**C02**: Prepare students for an industrial programming environment by successfully completingprogramming projects on cloud and edge computing.

**C03**: Expose students to current literature in cloud and edge computing

**C04**: Complete a term project, including independent research, oral presentation, and programming on latest advancement in cloud and edge computing.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written)

**PLO 5** Practice ethical standards of professional conduct and research

**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 1 | 2 | | |
| **CO2** | 3 | 2 | 2 | 2 | | |
| **CO3** | 2 | 2 | 2 | 2 | | |
| **C04** | 2 | 2 | 2 | 3 | 3 | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Introduction to Distributed Algorithms, Cloud Computing Architecture and Management, Cloud Deployment Models, Cloud Service Models, Cloud Development Process Flows, Cloud Service Providers, Virtualization, Orchestration and Messaging,Networking in Cloud Computing, Cloud Storage,Containers, Microservices and Serverless Computing, Programming Models and Languages for Cloud Computing, |
| **2** | Open Source Tools for IaaS, PaaS and SaaS, Open Source Tools for Research such as CloudSim and SimMapReduce, Software Defined Compute, Software-Defined Data Centers, Virtual Private Cloud Networking, Hybrid Cloud and Multi-Cloud Environments, Cognitive Clouds, Mobile Cloud Computing, Green Cloud Computing. |
| **3** | Edge/Fog Computing Paradigms, Edge Architecture, Edge computing Applications, Real-Time Data Analytics through Edge Clouds, Edge Computing for 5G/6G, Cognitive Edge Computing, Context-Awareness, Kubernetes Platform for Edge Environments;Cloudlets, SocialMedia and Mashup Services;IoT Services on cloud, Components, IoT Core, IoT Examples (AWS IoT), IoT Data Analytics Platform on Cloud Environments. |
| **4** | Case studies of Cloud and Edge Computing, Cloud Analytics, AI and ML at the Edge and in the Cloud, Fault Tolerance, Load Balancing, Performance |

| | |
|---|---|
| | and QoS,Security, Trustand Privacy in Cloud and Edge, Future Research Direction/Opportunity in the Cloud and Edge Computing. |

**Books and other resources:**

1. Recent Publications from top-Tier Cloud/System Conferences and Journals
2. Rajiv Misra, Yashwant Singh Patel, Cloud and Distributed Computing: Algorithms and Systems, ISBN: 9788126520275, Wiley
3. Andrew S. Tanenbaum, Maarten Van Steen, Distributed Systems: Principles and Paradigms, 2nd ed. Prentice Hall
4. Gerard Tel, Introduction to Distributed Algorithms, 2nd edition, Cambridge University Press, ISBN:9781139168724
5. K Chandrasekaran, Essentials of Cloud Computing, CRC Press, 2015
6. Rajkumar Buyya, Christian Vecchioola, S ThamaraiSelvi, Mastering Cloud Computing, McGrawHill, 2013
7. Cl Surianarayanan, PethuruRaj Chelliah, Essentials of Cloud Computing: A Holistic Perspective, Springer; 1st ed. 2019 ed.
8. Rajkumar Buyya, Satish N Srirama, Fog and Edge Computing: Principles and Paradigms, 2019, ISBN: 978-1-119-52498-4, Wiley
9. John R. Vacca, Cloud Computing Security: Foundations and Challenges, ISBN-10 : 1482260948, CRC Press
10. Brendan Burns, Joe Beda, Kelsey Hightower, Kubernetes: Up and Running: Dive Into the Future of Infrastructure, O'Reilly Publications, 2019.
11. Alan A. A. Donovan, Brian W. Kernighan, The Go Programming Language, Addison-Wesley, 2015
12. Steve Klabnik, Carol Nichols, The Rust Programming Language, No Starch Press, 2018
13. Jeeva S. Chelladhurai, Vinod Singh, Pethuru Raj, Learning Docker, Packt Publishing, 2 edition, 2017
14. Agus Kurniawan, Learning AWS IoT, Packt Publishing, 2018
15. E. Krishnasamya, S. Varrettea, M. Mucciardib, Edge Computing: An Overview of Framework and Applications, Available Online: https://prace-ri.eu/wp-content/uploads/Edge-Computing-An-Overview-of-Framework-and-Applications.pdf.

## M3010125, M3020323 COGNITIVE COMPUTING

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301125, M302323** | **Cognitive Computing** | **3-0-0-1** | **2021** |

**Prerequisites:** 10th class biology and chemistry, basic background in simple differential equations and probability theory, interest in neuroscience and cognitive science.

**Course Objectives:**

1. To provide students with a basic understanding of the concepts of neuroscience, cognitive science and cognitive computing described in the syllabus.
2. To help them understand how to connect the concepts of cognitive science and neuroscience to the computing domain.
3. To make students aware of the current research trends in cognitive computing and artificial emotional intelligence.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Understand the various cognitive and emotional processes that occur in the brain/mind, and how this knowledge can be applied in the computing domain.

**CO2**: Analyze and evaluate critically the building of cognitive and affective computing models and systems.

**CO3:** Think about research ideas in the field of cognitive science and computing and pursue them.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 1 | | 1 | | 1 |
| **CO2** | 3 | 2 | 1 | 1 | 1 | 1 |
| **CO3** | 2 | 2 | 2 | | 1 | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Basic neuroscience: Neurons, Dendrites and Axons, Synapses, Synaptic and Action Potentials, Action Potential generation and propagation, Brain organization, anatomy and functions, Synaptic integration and plasticity, the Concept of a Basic Circuit, Abstractions of Cortical Basic Circuits, Neocortical Brain Organization. Neuron models - McCulloch-Pitts, Integrate-and-Fire, Hodgkin-Huxley, Compartmental modelling. |
| **2** | Cognitive science: Introduction, interdisciplinary nature. Cognition and human mind. The cognitive perspective of pattern recognition, Cognitive models of memory, Mental Imagery, Understanding a problem, a cybernetic view of cognition. Decision making: cognitive psychology of decision making, neural basis, consciousness and free will. Hierarchical temporal memories, Spiking Neural networks, hardware support for Brain Simulations. Eye Tracking and other modalities for data acquisition. |
| **3** | Introduction to cognitive computing, Cognitive Computing Systems, Representations for Information and Knowledge, Principal Technology Enablers of Cognitive Computing, Cognitive Computing Architecture and Approaches, Applications of Cognitive Computing Systems. Cognitive Computing and Neural Networks: Reverse Engineering the Brain, Scope of Realization of Cognition in Artificial Intelligence, Brain Computer Interface: Introduction, Major Types, Brain Response useful for Building BCIs, Applications. |
| **4** | Emotions and machines: Manifestations, classifications, purpose and importance, theories and models and neural basis of emotions; mood; emotion dynamics and factors that influence it; the need for artificial emotional intelligence; expressing, recognizing, processing and responding to emotions; challenges to accurate emotion perception and recognition; emotion as information in judgement and decision making; making moral judgements; computational models for synthetic emotion simulation; application of artificial emotional intelligence in areas such as smart video surveillance, virtual reality based training, advertising and market research, customer care, healthcare and assistive technologies. |

**References:**

1. Neuroscience: Edited by Dale Purves, George J. Augustine, David Fitzpatrick, William C. Hall, Anthony-Samuel LaMantia, and Leonard E. White. Sinauer Associates Inc.
2. Principles of Neural Science: Edited by Eric Kandel, James Schwartz, Thomas Jessell, Steven Siegelbaum, and A.J. Hudspeth. McGraw-Hill Professional.
3. Cognitive neuroscience: the biology of the mind. Gazzaniga, M., Ivry, R. B., & Mangun, G. R. Cambridge: MIT press.

4. Computational Explorations in Cognitive Neuroscience: Understanding the Mind by Simulating the Brain. R. O'Reilly & Y. Munakata. MIT Press.
5. Theoretical neuroscience: computational and mathematical modelling of neural systems, Dayan, Peter, and Laurence F. Abbott.
6. The Book of GENESIS: Exploring Realistic Neural Models with the GEneralNEural Simulation System, Internet Edition: J. M. Bower and D. Beeman.
7. Pinker S, How the mind works, New york, NY: W W Norton.
8. Cognitive Science: An Introduction to the Science of the Mind: José Luis Bermúdez, Cambridge University Press.
9. Cognitive Science: An Introduction to the Study of Mind: Friedenberg, J. and Silverman. G. W., Sage Publications.
10. A Companion to Cognitive Science: Bechtel, W., & Graham, G. (Eds.), Malden, MA: Blackwell.
11. Mind: Introduction to Cognitive Science. Thagard, P., Cambridge, MA: MIT Press.
12. How the mind comes into being: Introducing cognitive science from a functional and computational perspective. Butz, Martin V., and Esther F. Kutter. Oxford University Press.
13. Computational Modelling in Cognition: Principles and Practice. Lewandowsky, S., & Farrell, S. Thousand Oaks, CA, US: SAGE.
14. Artificial Intelligence and Soft Computing - Behavioral and Cognitive Modelling of the Human Brain: Amit Konar, Publisher: CRC Press.
15. Cognitive Computing Theory and Applications: Venkat N. Gudivada, Vijay V. Raghavan, Venu Govindaraju, C.R. Rao, Publisher: Elsevier B.V.
16. Brain Computer Interfacing: An Introduction by Rajesh P. N. Rao., Publisher: Cambridge.
17. Learning in Energy-Efficient Neuromorphic Computing: Algorithm and Architecture Co-Design. Nan Zheng, Pinaki Mazumder, John Wiley & Sons.
18. Well-Being: The Foundations of Hedonic Psychology: Edited by D. Kahneman, E. Diener, and N. Schwarz. Russell Sage Foundation.
19. Selected journal articles.

## M2020104 COMPUTER ARCHITECTURE

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M202104 | **Computer Architecture** | **3-0-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To help students understand the fundamentals behind a computer and its architecture.
2. To explore the working principles of all the important building blocks of a computer.
3. To understand how these building blocks are put together to design a so-called computer.
4. To explore a few advanced topics in computer architecture.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Know how different components of a computer system are working.

**CO2**: Apply the knowledge of computer architecture while modelling systems for security analysis.

**CO3:** Compare various types of computer architectures and can analyze the design principles.

**CO4:** Use a computer more confidently with the acquired knowledge of its constituent components.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | | 2 | | | |
| **CO2** | | 3 | 3 | 2 | 3 | 3 |
| **CO3** | 2 | 3 | 2 | 1 | 2 | 1 |
| **C04** | 2 | 2 | 3 | 2 | 3 | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Computer Fundamentals: Computer types, functional units, Basic concepts.<br>Von Neumann Architecture<br>Instruction Sets: Machine instructions, Memory operations, Addressing modes, Instructions sets, Stacks, Subroutines, RISC & CISC architectures. |
| **2** | Processing Unit: Components (Registers, ALU, Datapath), Instruction execution, Control signals, Operations of control unit: Hardwired controlled unit, Microprogrammed control unit) - horizontal and vertical micro-programming,<br>Computer Arithmetic: Basic operations on signed numbers, Floating point operations. |
| **3** | Memory Management: Memory Hierarchy, Semiconductor based memory (Internal Organization, SRAM, DRAM), Read only memory,<br>Cache memories – mapping techniques, Performance, Virtual memory (Address translation), Memory management, Secondary storage, RAID introduction<br>Input/output: Accessing I/O devices, Bus Operations, I/O Modules, I/O Control mechanisms – Programmed I/O, Interrupt controlled, Direct Memory Access, I/O Interface (Serial, Parallel), I/O interconnection Standards. |
| **4** | Pipelining: Pipeline concept, Speedup, Throughput, Hazards in pipeline – structural hazard, data hazard, control hazard: Branch hazard; Dealing with hazards - Register Renaming, Branch Prediction.<br>Advanced Computer Architecture: Parallel Processing - Flynn’s classification, Amdahl's law, Characteristics of Multiprocessors, Interconnection Structures, Interprocessor Arbitration, Interprocessor Communication and Synchronization, Cache Coherence, Vector/Array Processing. |

**Text Books:**

1. C. Hamacher, Z. Vranesic, S. Zaky, and N. Manjikian, “Computer Organization,” 6th Edition, 2011, McGraw-HillHigher Education.
2. D. A. Patterson and J. L. Hennessy, “Computer Organization and Design – The Hardware/Software Interface,” 6th edition, 2020, Morgan Kaufmann.
3. William Stallings, “Computer Organization & Architecture designing for performance,”8th Ed., 2009, Pearson
4. P. Pal Chaudhuri,“Computer Organization and Design,” 3rd Edition, 2008, PHI
5. Andrew S. Tanenbaum,“Structured Computer Organization,”6th Edition,2012, Pearson.

**References:**

1. J. P. Hayes, Computer Architecture and Organization, 3rd Ed, 1998, Mcgraw-Hill Education.
2. M. M. Mano,Computer Systems Architecture, 3rd Ed., 1992, Pearson/PHI.

# M2022204 COMPUTER NETWORKS AND SECURITY

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M202204 | Computer Networks and Security | 3-0-1-0 | 2021 |

**Prerequisites:** Nil

**Course Objectives:**

- To introduce the fundamentalaspects of computer networks
- To enable the students to understand various cyber attacks targeted on computer networks
- To enable the students to develop various security mechanism for computer networks
- To enable the students to simulate various network attacks

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Summarize principles of Networks

**CO2:** Describe the layered protocol model.

**CO3:** Discriminate between various protocols

**CO4:** Appraise security threats and resolve effectively

**CO5:** Analyse the challenges in different network architectures

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 3 | 2 | 3 | 2 | | |
| CO2 | 3 | 3 | 3 | 2 | | |
| CO3 | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | Network Basics: The Network Edge, The Network Core, Access Networks, Delay, Loss and Throughput, Protocol Layers and Their Service Models, Application Layer: RPC, P2P, HTTP, FTP, DNS, DHCP, Electronic Mail, WLAN, Socket, Programming with TCP & UDP |
| 2 | Transport Layer: Services, TCP, UDP, Network Layer: Functions, design issues, Internet Protocol (IP), IPV4 & IPv6, Routers, Routing algorithms, Congestion Control Algorithms |

| | |
|---|---|
| **3** | Data Link Layer: Design issues, framing methods, Error Detection and Correction, PPP, Sliding Window Protocols, Multiple Access Protocols, Address Resolution, Protocol (ARP), Ethernet, Link Layer Switches, Spanning Tree Protocol, VLAN |
| **4** | Security Attacks, Security Services, Security Mechanisms, Key Management and Distribution, User Authentication Protocols, SSL, TLS, Wireless Network Security, Electronic Mail Security, Vulnerability Analysis, Attacks in sensor and IoT networks, Endpoint Security, familiarization of Network simulators - NS2/NS3 or Cooja/Contiki and simulation of attacks and analyze network performance. |

**Text Books:**

1. James Kurose and Keith Ross, Computer Networking: A Top-Down Approach, Pearson
2. Andrew S. Tanenbaum, Computer Networks 5th Edition, Pearson
3. William Stallings, Cryptography and Network Security Principles and Practice, Prentice Hall
4. VlasiosTsiatsis, Stamatis Karnouskos, Jan Holler, David Boyle, Catherine Mulligan, Internet of Things: Technologies and Applications for a New Age of Intelligence. Elsevier Academic press.
5. Zaigham Mahmood, Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for IoV, Springer
6. Ian F. Akyildiz, Mehmet Can Vuran-Wireless Sensor Networks. Wiley.

**References:**

1. Peterson L.L, Davie B.S, Computer Networks, A systems approach, 3/E, Harcourt Asia, 2003
2. Keshav S., An Engineering Approach to Computer Networking, Pearson Education, 2000.
3. Shinde S.S, Computer Network, New Age International, 2009
4. Pethuru Raj and Anupama C. Raman, The Internet of Things: Enabling Technologies, Platforms, and Use Cases, CRC Press.
5. Adrian McEwen, Designing the Internet of Things, Wiley, 2013.

## M3010232 COMPUTER VISION

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M301232 | **Computer Vision** | **3-0-0-1** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To provide students with a good understanding of the concepts of computer vision described in the syllabus.
2. To help the students develop the ability to solve problems using the learned concepts.
3. To connect the concepts to other domain both within and without mathematics such asmachine learning and pattern recognition.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Understand the foundations of modern computer vision theory, problem and state of the art solutions.

**CO2**: Analyse and evaluate critically the building and integration of computer vision algorithms and systems.

**CO3:** Design and demonstrate a working computer vision system through team research project, and project report, presentation.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 3 | 2 | 3 | 2 | | |
| CO2 | 3 | 3 | 3 | 2 | | |
| CO3 | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | The Four Rs of Computer Vision, Geometry of Image Formation and Sensing, Single/Two View Geometry, Camera Calibration, Vanishing Points, Planar Scenes and Homography, Interest Point Detection, Robust Correspondence Estimation |
| 2 | Feature Extraction: Edges - Canny, LoG, DoG; Line detectors (Hough Transform), Corners - Harris and Hessian Affine, Orientation Histogram, SIFT, SURF, HOG, GLOH, Scale-Space Analysis- Image Pyramids and Gaussian derivative filters, Gabor Filters and DWT. |
| 3 | Image Segmentation: Region Growing, Edge Based approaches to segmentation, Graph-Cut, Mean-Shift, MRFs, Texture Segmentation; Object detection |
| 4 | Motion Analysis: Background Subtraction and Modelling, Optical Flow, KLT, Spatio-Temporal Analysis, Dynamic Stereo; Motion parameter estimation. |

**Text Books:**

1. Richard Szeliski, Computer Vision: Algorithms and Applications, Springer-Verlag London Limited 2011.
2. Computer Vision: A Modern Approach, D. A. Forsyth, J. Ponce, Pearson Education, 2003.
3. Richard Hartley and Andrew Zisserman, Multiple View Geometry in Computer
4. Vision, Second Edition, Cambridge University Press, March 2004.

**References:**

1. Simon J. D. Prince. 2012. Computer Vision: Models, Learning, and Inference (1st. ed.). Cambridge University Press, USA.
2. E. R. Davies. 2017. Computer Vision, Fifth Edition: Principles, Algorithms, Applications, Learning (5th. ed.). Academic Press, Inc., USA.

## M3010252 CONNECTED ENVIRONMENTS AND ENABLING TECHNOLOGIES

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301252** | **Connected Environments and Enabling Technologies** | **1-3-0-0** | **2021** |

**Prerequisites:** Prior knowledge of Computer Networks, Distributed Computing, DBMS, Programming in Python

**Course Objectives:**

1. To learn the current state of the art in the IoT domain and learn details regarding several necessary principles required for future connected systems.
2. To expose the students to the different application areas of IoT along with providing sufficient foundations for further study and research.
3. To improve the critical reading, presentation, and research skills.

**Course Outcomes:**

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

**C01**: Understand the various building blocks of IoT and its characteristics and the application areas.

**CO2**: Explore the relationship between IoT, cloud computing, and big data and apply basic principles to develop practical skills of IoT and related fields.

**C03**: Complete written paper reviews, an oral paper presentation, and a final course project.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written)

**PLO 5** Practice ethical standards of professional conduct and research

**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 1 | | 1 | | |
| **CO2** | 2 | 2 | 1 | 2 | | 1 |
| **CO3** | 2 | 2 | 1 | 2 | | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus: Connected Environments and Enabling Technologies**

| **Module** | **Content** |
|---|---|
| **1** | Demystifying the IoT Paradigm, IoT Network Architecture and Design, IoT Sensors and Devices, IoT Edge Gateways, IoT Access Technologies, IP as the IoT Network Layer, IoT Standards and Protocols, Machine to Machine Communications, RFID, 5G, Software-defined Networking (SDN), Network Functions Virtualization (NFV), Semantic Technologies, Discovery Services, Industrial IoT, Internet of Medical Things, Semantic Web of Things and Cognitive IoT |
| **2** | Microcontrollers, Single Board Computers (SBCs) and boards based on Arduino and Raspberry PI, Data Transmission and Service Access Protocols such as MQTT, COAP, etc., IoT Graphical user interface: Web servers, HTML, PHP, Scripting languages: - Python, Bash, IoT application development for Android and iOS phones, Embedded Linux and Applications, Cotiki OS, Cooja Simulator, IoT Database management: MySQL, MongoDB |
| **3** | IoT programming languages for Edge devices, gateways and cloud applications, System on Chip (SoC) Technologies and Tools including NVIDIA® Jetson, REST Application programming interfaces (APIs) for Device and Cloud Services, Intelligent IoT Devices and Applications through AI Processing, IoT Data Analytics Platforms, IoT Data Virtualization Platforms, IoT Data Visualization Platform, IoT Edge Data Analytics, IoT-Cloud Integration through AWS IoT for the Edge, Lambda@Edge, etc. |
| **4** | IoT-enabled Applications: Smart Home, Smart Building, Smart City, Smart Health, Smart Transportation, Environmental Monitoring, Smart Industry, Smart Grid, Smart Farming, Public Safety, Case Studies. |

**Books and other resources:**

1. Recent Publications from top-Tier Conferences and Journals
2. Adrian McEwen, Hakim Cassimally, Designing the Internet of Things, ISBN: 978-1-118-43062-0, 2013, Wiley
3. Damon Parker, Arduino Programming, 2020, ISBN-13: 978-1801128001, New Begin Ltd.
4. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry, IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of

Things, Cisco Press, ISBN-13: 978-1-58714-456-1

5. Dawoud Shenouda Dawoud, Peter Dawoud, Microcontroller and Smart Home Networks, 2020, ISBN-13 : 978-8770221566, River Publishers
6. Harry Fairhead, Raspberry Pi IoT In C, 2020, ISBN-13 : 978-1871962635, I/O Press
7. Jean-Philippe Vasseur, Adam Dunkels, Interconnecting Smart Objects with IP: The Next Internet, ISBN-13 : 978-0123751652, 2010, Morgan Kuffmann
8. Maggie Lin and Qiang Lin, Internet of Things Ecosystem, ISBN-13 : 979-8597147208, 2021
9. Ovidiu Vermesan, Peter Friess, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, ISBN: 9788792982735, 2013, River Publishers
10. Pethuru Raj, Anupama C. Raman, The Internet of Things Enabling Technologies, Platforms, and Use Cases, ISBN 9781498761284, Taylor & Francis, 2017
11. Qinghao Tang, Fan Du, Internet of Things Security: Principles and Practice, 2021, Springer
12. Rajesh Singh, Anita Gehlot, Lovi Raj Gupta, Bhupendra Singh, Mahendra Swain, Internet of Things with Raspberry Pi and Arduino, ISBN 9780367248215, 2019, CRC Press
13. Theo Lynn, John G. Mooney, Brian Lee, Patricia Takako Endo, The Cloud-to-Thing Continuum: Opportunities and Challenges in Cloud, Fog and Edge Computing, 2020, ISBN-13: 978-3030411091, Palgrave Macmillan.
14. Vijay Madisetti, ArshdeepBahga, Internet of Things (A Hands-on-Approach), ISBN-13 : 978-8173719547, 2015, Orient Blackswan Private Limited - New Delhi
15. Zach Shelby, Carsten Bormann, 6LoWPAN: The Wireless Embedded Internet, ISBN: 978-0-470-74799-5, Wiley .

## M3010224 CRYPTOGRAPHIC ENGINEERING

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M301224 | Cryptographic Engineering | 3-0-0-1 | 2021 |

**Prerequisites:** A basic understanding of algebra, modular arithmetic, and familiarity with basic cryptography algorithms

**Course Objectives:**

1. Learn modern cryptographic algorithms, their implementations in contemporary computing platforms and security analysis.
2. Analyze countermeasures to thwart implementation-level attacks on cryptographic operations in hardware and software
3. Identify appropriate cryptographic techniques for real world applications

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Apply appropriate cryptographic techniques to solve real-world problems in information security

**CO2**: Analyze the attack surface of a system in order to realize effective mitigation measures against threats

**CO3:** Exploit cryptography standards to create standards-compliant secure software and hardware systems

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 2 | 2 | 1 | 2 |
| **CO2** | 3 | 3 | 3 | 2 | 1 | 2 |
| **CO3** | 2 | 1 | 1 | 2 | 3 | 3 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | Block Ciphers, DES, Triple-DES, AES, Block Cipher Modes, Stream Ciphers, RC4, Hash Functions, SHA-1, SHA3, MAC, HMAC, Practical implementation of symmetric key schemes in software and hardware, Optimization for High-Performance and Lightweight Cryptography |
| 2 | Public-Key Cryptographic Algorithms, RSA, Rabin, ElGamal, ECC, Lattice Cryptography, Diffie Hellman Key Exchange, Kyber Key Exchange Algorithm, Parameter selection and practical implementation of PKC schemes in software and hardware |
| 3 | Digital Signature Algorithms: RSA, DSA, ECDSA with NIST and Brainpool curves, DH, ECDH with NIST and Brainpool curves, Dilithium, HSS, XMSS, XMSSMT, Parameter selection and practical implementation of digital signature schemes<br>Security evaluation of real-world cryptographic systems, provable security, formal methods and verification tools for secure embedded design, metrics for measuring security, |
| 4 | Hash-based deterministic random number generator (DRG.4 acc. AIS 31), True random number generator (PTG.2 acc. AIS 31), protocols like KMIP and API interfaces such as PKC#11, MS CNG, MS CAPI, Java Cryptography Extension (JCE), Microsoft Crypto API (CSP), Cryptography Next Generation (CNG) and SQL Extensible Key Management (SQLEKM), Public Key Infrastructure (PKI) and Hardware Security Module (HSM), X.509, secure key storage, key exchange methods, |

**Text Books:**

1. A Ç. K. Koç. Cryptographic Engineering, Springer, 2009.
2. Joachim von zur Gathen, CryptoSchool, Springer, 2015
3. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson
4. Jean-Philippe Aumasson, Serious Cryptography: A Practical Introduction to Modern Encryption, No Starch Press, 2017
5. David Wong, Real-World Cryptography, Manning Publications, July 2021
6. F. Rodríguez-Henríquez, A. D. Pérez, N. A. Saqib and Ç. K. Koç. Cryptographic Algorithms on Reconfigurable Hardware, Springer 2007.
7. C. Rebeiro, D. Mukhopadhyay, and S. Bhattacharya. Timing Channels in Cryptography, Springer 2015.
8. M. Joye and M. Tunstall. Fault Analysis in Cryptography, Springer 2012.
9. Simon Rubinstein-Salzedo, Cryptography, Springer, 2018

**References:**

1. Alko R. Meijer, Algebra for Cryptologists, Springer, 2016
2. Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 2020
3. Thomas R. Shemanske, A Beginner's Guide, Modern Cryptography and Elliptic Curves, American Mathematical Society, 2017 .

## M3022202   CYBER ANALYTICS

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M302202 | Cyber  Analytics | 3-0-0-0 | 2021 |

**Prerequisites:** Nil

**Course Objectives:**

- To introduce various supervised, unsupervised and reinforcement machine learning algorithms
- To enable the students to  apply ML techniques to analyze cyber data
- To enable the students to perform cyber  threat detection, risk estimation, vulnerability detection, and cyber attack detection
- To make the students to design ML based cyber security solutions

**Course Outcomes:** After completion of this course,  the students would be able to:

**CO1:** Compare supervised, unsupervised and reinforcement machine learning paradigms

**CO2:** Design supervised and unsupervised learning algorithms for cyber security problems.

**CO3:** Apply the knowledge of data analytics to analyze cyber data for security threats, risk estimation, vulnerability detection, cyber attack detection and prevention.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 3 | 2 | 3 | 2 | | |
| CO2 | 3 | 3 | 3 | 2 | | |
| CO3 | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low)  2: Moderate (Medium)    3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | Data Ingestion, Data Processing and Cleaning, Data Visualization and Exploratory, Pattern Recognition, Classification, Clustering, Feature extraction, Feature Selection, Random Projections, Modelling, Model Specification, Model Selection and Fitting, Evaluation, Bias, variance and Noise, Strengths and Limitations, Curse of Dimensionality, Applications of Data Analytics to Security Challenges, Cyber security Datasets, Data Science Applications |
| 2 | Unsupervised Learning, Data Collection, Types of Data and Operations, Properties of Datasets, Data Exploration and Pre-processing, Data Representation, Association Rule Mining, Variations on the Apriori Algorithm, Clustering, Partitional Clustering, Hierarchical Clustering, Manifold Discovery, Spectral Embedding, Anomaly Detection, Distance-based Outlier Detection, kNN based approach, Density-based Outlier Detection, Clustering-based Outlier Detection, One-class learning based Outliers, Security Applications, Data Mining for Intrusion Detection, Stepping-stone Detection, Malware Clustering, Directed Anomaly Scoring for Spear Phishing Detection |
| 3 | Supervised Learning, The Bayes Classifier, Naïve Bayes, Nearest Neighbors |

|  |  |
|---|---|
|  | Classifiers, Linear Classifiers, Decision Trees and Random Forests, Random Forest, Support Vector Machines, Semi-Supervised Classification, Perceptron, Neural Networks, Deep Networks, Topological Data Analysis, Ensemble Learning, Adaboost, One-class Learning, Online Learning, Metrics for Unbalanced Datasets, Security Applications, Intrusion Detection, Malware Detection, Spam and Phishing Detection, cyber security risks estimation |
| **4** | Big Data Techniques and Security, Ingesting the Data, Persistent Storage, Computing and Analyzing, Techniques for Handling Big Data, Visualizing, Streaming Data, Big Data Security, Implications of Big Data Characteristics on Security and Privacy, Mechanisms for Big Data Security Goals |

**Text Books:**

1. Cybersecurity Analytics, Rakesh M. Verma, David J. Marchette, Chapman and Hall/CRC, 2019
2. Tony Thomas, Athira P. Vijayaraghavan, Sabu Emmanuel, Machine Learning Approaches in Cybersecurity Analytics, Springer 2020
3. Clarence Chio, David Freeman, Machine Learning & Security, O Reilly, 2018
4. Mark Stamp, Introduction to Machine Learning with Applications in Information Security, CRC Press, 2018
5. D K Bhattacharyya, J K Kalita, Network Anomaly Detection, A machine Learning Perspective, CRC Press, 2014
6. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts By AurélienGéron, "O'Reilly Media, Inc.", 2019
7. P.-N. Tang, M. Steinbach, and V. Kumar: Introduction to Data Mining, Addison Wesley, 2006
8. Jiawei Han and MichelineKamber, Data Mining: Concepts and Techniques, Morgan Kaufman Publishers, Third Edition, 2011**.**

**References:**

1. A Practical Approach for Machine Learning and Deep Learning Algorithms by Abhishek Kumar Pandey, Pramod Singh Rathore, S Balamurugan, BPB Publications, 2019
2. Soma Halder, Sinan Ozdemir, Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem, Packt Publishing (December 31, 2018)
3. Alazab, Mamoun, Tang, MingJian, Deep Learning Applications for Cyber Security, Springer 2019

## M3010263 CYBER BIG DATA ANALYTICS

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301263** | **Cyber Big Data Analytics** | **3-0-0-1** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To impart skills needed for understanding and applying machine learning and big data technologies
2. To equip the students with the ability to identify and analyze problems solvable with machine learning and big data technologies
3. To impart solution design capability with data mining and big data technologies

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Apply the knowledge of data analytics to analyze cyber data for security threats, risk estimation, vulnerability detection, cyber attack detection and prevention.

**CO2:** Design supervised and unsupervised learning algorithms for cyber security problems.

**CO3:** Solution design capability with data mining and big data technologies

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences.

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | |
| **CO2** | 3 | 3 | 3 | 2 | | |
| **CO3** | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Volume, velocity and variety of cyber data, Familiarization of cyber security datasets such as DARPA, KDD'99 Cup, NSL-KDD, CAIDA, ISOT'10, ISCX'12, CTU-13, UNSW-NB15, CIC-IDS2018 CIC-IDS2017, CIC-DDoS2019, ADFA IDS, CERT, Bot-IoT, Data Ingestion, Data Processing and Cleaning, Data Visualization , Handling quality problems in cyber security datasets, feature engineering, Dimensionality reduction and sampling techniques for valuable cybersecurity data extraction, recency analysis of datasets, Representation of cyber-attack data for cross-platform processing |
| **2** | UnsupervisedLearning, Association RuleMining, Clustering, Partitional Clustering, Hierarchical Clustering, Manifold Discovery, Spectral Embedding, Supervised Learning, Naïve Bayes, Nearest Neighbors Classifiers, Linear Classifiers, Decision Trees and Random Forests, RandomForest, Support Vector Machines, Semi-Supervised Classification Perceptron, Neural Networks, Deep Networks, Topological Data Analysis, Ensemble Learning, Adaboost,<br>Applications of ML techniques in various cyber security problems such as intrusion detection, malware detection, spam and phishing detection, cyber security risks estimation etc. |
| **3** | Introduction to Big Data Technology, Hadoop, HDFSand MapReduce, Hadoop Environment, Messaging systems, Distributed SQL Query Engines, Introduction to Apache Spark, Spark Cluster ASpark Core, High level architecture, Spark Context, RDD, Lazy Operation, Caching methods, Spark SQL<br>Machine learning with spark, Spark Machine Learning libraries, Spark ML and Applications, Graph Processing with Spark |
| **4** | Application of big data technologies in various cyber security problems such as anomaly detection, DDoS detection, intrusion detection, network monitoring, malware detection, phishing detection, network monitoring, cyber threat intelligence, behavioral analytics, advanced persistent threat (APT) detection, fake news detection in social media networks |

**Text Books:**

1. Cybersecurity Analytics, Rakesh M. Verma, David J. Marchette, Chapman and Hall/CRC, 2019
2. Tony Thomas, Athira P. Vijayaraghavan, Sabu Emmanuel, Machine Learning Approaches

in Cybersecurity Analytics, Springer 2020

3. Clarence Chio, David Freeman, Machine Learning & Security, O Reilly, 2018
4. Mark Stamp, Introduction to Machine Learning with Applications in Information Security, CRC Press, 2018
5. D K Bhattacharyya, J K Kalita, Network Anomaly Detection, A machine Learning Perspective, CRC Press, 2014
6. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts By AurélienGéron, "O'Reilly Media, Inc.", 2019
7. P.-N. Tang, M. Steinbach, and V. Kumar: Introduction to Data Mining, Addison Wesley, 2006
8. Jiawei Han and MichelineKamber, Data Mining: Concepts and Techniques, Morgan Kaufman Publishers, Third Edition, 2011**.**
9. Data Analytics with Spark Using Python, By Jeffrey Aven, Addison Weley Data & Analytics series, 2018
10. Big Data Analytics with Spark, Mohammed Guller, APress, 2015

**References:**

1. A Practical Approach for Machine Learning and Deep Learning Algorithms by Abhishek Kumar Pandey, Pramod Singh Rathore, S Balamurugan, BPB Publications, 2019
2. Soma Halder, Sinan Ozdemir , Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem, Packt Publishing (December 31, 2018)
3. Alazab, Mamoun, Tang, MingJian, Deep Learning Applications for Cyber Security, Springer 2019
4. Anand Rajaraman, Jeffrey D Ullman. Mining of Massive Datasets, Cambridge University Press 2010

## M3010205 CYBER CRIME INVESTIGATION

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301205** | **Cyber Crime Investigation** | **3-0-0-1** | **2021** |

**Prerequisites:**

- Basic understanding of Computer Architecture, Computer Organisation, OS and Networking
- Basic understanding of Programming Skills

**Course Objectives:**

1. The main objective of the course is to introduce the students to bring awareness in crimes and tracing the attackers.
2. Understanding Laws relating to cyber rime investigations.
3. Describe how to prepare for digital evidence investigations and explain the differences between law enforcement agencies and corporate investigations.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1**: Knowledge of cybercrimes and able to perform cyber rime investigation.

**CO2**: Perform digital forensics analysis upon OS, networks and network devices.

**CO3**: Utilize various forensic tools to collect digital evidence.

**Program Learning Outcomes:**

**PLO 1**Develop strong fundamental disciplinary knowledge

**PLO 2**Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4**Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences

**PLO 5** Practice ethical standards of professional conduct and research

**PLO 6**Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 2 | 2 | 2 | |
| **CO2** | 3 | 3 | 3 | 2 | 3 | 2 |
| **CO3** | 3 | 2 | 3 | 2 | 3 | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Overview of Cyber Crimes: Definition, Tools and Techniques used to commit Cyber Crimes, Types of Cyber Crimes. Digital Evidence - Source and Nature of Digital Evidence. Digital Evidence in the Courtroom<br>Pre-investigation Assessment: Preliminary review of the Scene of Offence, Pre-investigation Technical Assessment, Issuance of Prevention Notice, Containment of Incident / Offence. |
| **2** | Digital Evidence Examination Guideline, Standard Operating Procedure (SOP) for Investigation, Collection of Digital Evidence, Physical Drives Imaging, Network Drives Imaging and Logical File Collection, Chain of Custody, Gathering Information from External Agencies / Companies.<br>OS Forensics: Registry Analysis, Timestamp Analysis, Event Viewer Analysis.<br>Memory Forensics: Volatile Data Collection, Memory Dump, Volatility Framework and Plugins, Bulk Extractor and YARA tools. |
| **3** | Network Forensics: Understanding Network Protocols with Wireshark, Packet Capturing using Wireshark, Packet Filtering, Extracting of Data from PCAP file, Analysis of Logs. Email Investigation.<br>Virtual Machine Forensics: Importance of Virtual Machines in Forensic Analysis, Imaging of a Virtual Machine, Identification and Extraction of supporting VM files in the host system. |
| **4** | Cloud Forensics: Cloud Storage Forensic Framework, Evidence Source Identification and Preservation in the Cloud Storage, Cloud Storage Forensic Analysis, Issues in Cloud Forensics. Dropbox and Google Drive analysis.<br>IoT Forensics: Challenges and Case Studies<br>Investigations of Darknet, Illegal Usage of Crypto Currencies, Investigation of Crimes in Social Media and Online Financial Transactions, Machine Learning Applications in Cyber Crime Detection and Investigation. |

**Text Books:**

1. Bill Nelson, Amelia Phillips, Christopher Steuart, “Guide to Computer Forensics and Investigations”, Sixth Edition (2020)
2. Karanam Satyanarayana, "Step by Step in Cyber Crimes Investigation, Challenges and Solutions", Asia Law House; 1st Edition (2020).
3. Angus M. Marshall, “Digital Forensics: Digital Evidence in Criminal Investigation”, John – Wiley and Sons, 2008.
4. Dr. Rukmani Krishnamurthy, "Introduction to Forensic Science in Criminal Investigation", Selective & Scientific Books (2015)
5. Niranjan Reddy, "Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations", New York, Apress, 1st Edition (2019)

**References:**

1. Thomas J. Holt (Author), Adam M. Bossler (Author), Kathryn C. Seigfried Spellar, "Cybercrime and Digital Forensics: An Introduction", Routledge, 2nd Edition (2017)
2. Computer Forensics: Investigating Network Intrusions and Cyber Crime (EC Council Press

Series: Computer Forensics)

3. Cyber Forensics: Understanding Information Security Investigations (Springer's Forensic Laboratory Science Series) by Jennifer Bayuk

## M3022102 CYBER SECURITY AND DIGITAL FORENSICS

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M302102 | Cyber Security and Digital Forensics | 3-0-0-0 | 2021 |

**Prerequisites:** Nil

**Course Objectives:**

1. Familiarize with cyber crimes and cyber security
2. Understand various techniques of cyber attacks and defences
3. Perform digital forensic investigations

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1** Understand various cyber attacks/crimes and cyber security mechanisms.

**CO2**: Perform digital forensics analysis on OS, memory, networks and network devices etc.

**CO3**: Utilize various cyber security and forensic tools to understand cyber attacks and collect digital evidence.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2**Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3**Apply scholarship to conduct independent and innovative research

**PLO 4**Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6**Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 2 | | | |
| **CO2** | 3 | 3 | 3 | | 3 | |
| **CO3** | 3 | 3 | 3 | | 3 | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | Cybercrimes and Information Security, Tools and Techniques used to commit Cyber Crimes, Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Phishing Attack, Spam, Social Engineering, Cyberstalking, Credit Card Frauds, Financial crimes , Security mechanisms against these attacks and crimes . |
| 2 | Darknet, Crypto Currencies and Crimes, Crimes in Social Media and Online Financial Transactions, Attacks on Wireless Networks, Security issues in mobile platforms and applications, Security issues in cloud, Security issues in IoT networks, Security mechanisms against various attacks in these networks |
| 3 | Digital Evidence, Source and Nature of Digital Evidence, Collection of Digital Evidence, Physical Drives Imaging, Network Drives Imaging and Logical File Collection, Chain of |

| | |
|---|---|
| | Custody, Gathering Information from External Agencies / Companies,<br>OS Forensics: Registry Analysis, Timestamp Analysis, Event Viewer Analysis.<br>Memory Forensics: Volatile Data Collection, Memory Dump, Volatility Framework and Plugins, Bulk Extractor and YARA tools. |
| **4** | Network Forensics, Understanding Network Protocols with Wireshark, Packet Capturing using Wireshark, Packet Filtering, Extracting of Data from PCAP file, Analysis of Logs, Email Investigation.<br>Virtual Machine Forensics: Importance of Virtual Machines in Forensic Analysis, Imaging of a Virtual Machine, Identification and extraction of supporting VM files in the host system. |

**Text Books:**

1. Bill Nelson, Amelia Phillips, Christopher Steuart,"Guide to Computer Forensics and Investigations", Sixth Edition (2020)
2. Karanam Satyanarayana, "Step by Step in Cyber Crimes Investigation, Challenges and Solutions", Asia Law House; 1st Edition (2020).
3. Nina Godbole , Sunit Belapure, Cyber Security: Understanding Cyber Crimes, Computer For ensics and Legal Perspectives, 2011,
4. John Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital For ensics Elsevier, 2014.
5. P.W. Singer, Allan Friedman, Cyber security and Cyber war: What Everyone Needs to Know, Oxford University Press, 2014,
6. Angus M. Marshall, "Digital Forensics: Digital Evidence in Criminal Investigation", John – Wiley and Sons, 2008.
7. Dr. Rukmani Krishnamurthy, "Introduction to Forensic Science in Criminal Investigation", Selective & Scientific Books (2015)
8. Niranjan Reddy, "Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations", New York, Apress, 1st Edition (2019)

**References:**

1. Thomas J. Holt (Author), Adam M. Bossler (Author), Kathryn C. Seigfried Spellar , "Cybercrime and Digital Forensics: An Introduction", Routledge, 2nd Edition (2017)
2. Computer Forensics: Investigating Network Intrusions and Cyber Crime (EC Council Press Series: Computer Forensics)
3. Cyber Forensics: Understanding Information Security Investigations (Springer's Forensic Laboratory Science Series) by Jennifer Bayuk

## M3010201 DATA & INTELLIGENCE

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301201** | **Data and Intelligence** | **3-1-0-0** | **2021** |
| **Prerequisites:** Nil | | | |

**Course Objectives:**

1. To impart skills needed to identify and understand data problems
2. To equip with analytical thinking on problems solvable with data intelligence

3. To impart solution design capability with data intelligence

**Course Outcomes:** After completion of this course, the students would be able to:
**CO1:** Understand and develop techniques in data intelligence
**CO2**: Problem identification and analysis skills on data intelligence problems
**CO3:** Solution design capability with data intelligence

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | 2 |
| **CO2** | 2 | 3 | 3 | 2 | | 2 |
| **CO3** | 2 | 3 | 3 | 2 | | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Data Intelligence and Decision Making, Collaborative Intelligence - Humans and AI. Data Architecture, Data Profiling and Storage, Data Quality and Integration, ETL process |
| **2** | Data Analytics Thinking, Exploratory Analysis, Multidimensional Analysis, OLAP, Data Visualization, Data Modelling, Overfitting and Underfitting |
| **3** | Decision Analytic Thinking - Applications of Clustering, Classification and Association Mining. Big Data Environments and Knowledge Extraction. Enterprise Data Management - Collibra case study. |
| **4** | Realistic AI and Digital Transformation. Intelligence in CRM - Telenor case study, Healthcare Intelligence - VideaHealth Case study, Retail Intelligence - Vispera case study, HR Intelligence - Recruit Japana case study, Manufacturing Intelligence - Dow Chemicals case study. |

**Lab/Assignment:**
A case study presentation and discussion (by a group of three)

**Text Books:**

**1.** Provost, F. and Fawcett, T., Data Science for Business, Shroff Publishers andDistributors Pvt. Ltd, 2014

2. Daniel T. Larose, Chantal D. Larose, Data Mining and Predictive Analytics, John Wiley and Sons, 2016.

3. HBR Case Studies

**References:**

1. Erl, T., Khattak, W. and Buhler, P., Big Data Fundamentals: Concepts, Drivers and Techniques, Pearson Education India, July 2016
2. Seth Stephens-Davidowitz, Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are, HarperLuxe, 2017.

## M3020217 DATA ANALYTICS

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M302217 | Data Analytics | 3-0-0-1 | 2021 |

**Prerequisites:** Basic knowledge in Machine learning, statistics and Python

**Course Objectives:**

1. To provide students with a good understanding of the concepts of Data Analytics described in the syllabus.
2. To help the students develop the ability to solve problems using the learned concepts.
3. To connect the concepts to the domain both within and without data analytics such as machine learning and pattern recognition.

**Course Outcomes:** After completion of this course, the students would be able to:
**CO1:** Understand the Data analytics techniques and state of the art solutions.
**CO2**: Analyze and evaluate critically the building and integration ofData analytics.
**CO3:** Design and demonstrateData analytics through team research project, and project report presentation.

**Program Learning Outcomes:**
**PLO1** Develop strong fundamental disciplinary knowledge
**PLO2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO3** Apply scholarship to conduct independent and innovative research
**PLO4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO5** Practice ethical standards of professional conduct and research;
**PLO6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course out comes with program learning out comes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 2 | 2 | 1 | 2 |
| **CO2** | 3 | 3 | 3 | 2 | 1 | 2 |
| **CO3** | 2 | 1 | 1 | 2 | 3 | 3 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | Data pre-processing and Normalization: Types of data and data models, active and passive models, explanatory and predictive models, static and continuously learning models; missing data, stages of data preparation, data characterization, Missing values, conversion of data, Normalizing variable ranges, redistribution of values, retaining and replacing missing value information, sparse variables, Dimensionality Reduction and PCA |
| 2 | Clustering : Distance Measures, Clustering, Hierarchical clustering, k-means clustering, Kohonen networks, DBSCAN, Measuring cluster goodness, Association rules, Affinity and Market Basket analysis, support and Confidence, Apriori and FP- |

| | |
|---|---|
| | growth, Pattern-sequential, frequent sequence mining |
| **3** | Regression and Classification: Linear regression, the least square estimates, Inference in regression, Multiple Regression, Inference in multiple regression, Logistic regression, regression with categorical predictors, Supervised learning methods, Classification, KNN algorithm, choosing k, Decision trees, Classification and regression trees, Decision Trees, SVM, Neural network, Activation functions, Gradient descent methods, ,Maximum Likelihood estimation, Naive Bayes Algorithm, Model evaluation techniques-Application |
| **4** | Applications on Data Science: Sentiment Analysis, recommendation systems, social network analysis, Data Analytics using NumPy, Data Manipulation and Visualization with Pandas and Tableau. R programming for Data Science, Deep Learning based on medical data analysis/Business data Analysis |

**TextBooks:**

1. Joao Moreira, Andre De Carvalho, Tomas Horvath “ A general Introduction to Data Analytics” Wiley, 2019
2. Ian H. Witten, Eibe Frank, Mark A. Hall , Data Mining: Practical Machine Learning Tools and Techniques, Third Edition (The Morgan Kaufmann Series in Data Management Systems), Morgan Kaufmann; 3 edition (January 20, 2011)
3. Abhishek Kumar Pandey, Pramod Singh Rathore, S Balamurugan, A Practical Approach for Machine Learning and Deep Learning Algorithms, BPB Publications, 2019
4. By Hadley Wickham, Garrett Grolemund, R for Data ScienceImport, Tidy, Transform Visualize, and Model Data, O’reilly, 2016

**References:**

1. Advanced Analytics with R and TableauBy Jen Stirrup, Ruben Oliva Ramos · 2017
2. Data Preparation for Data Mining by Dorian Pyle, Morgan Kaufmann Publishers, Inc. 1999 (ebook)

## M3010212 DATA MINING AND BIG DATA

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/ Project | Year of Introduction |
|---|---|---|---|
| **M301212** | **Data Mining and Big Data** | **3-0-0-1** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To impart skills needed for understanding and applying data mining and big data technologies
2. To equip the students with the ability to identify and analyse problems solvable with data mining and big data technologies
3. To impart solution design capability with data mining and big data technologies

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Understand and develop techniques in data mining and big data management
**CO2**: Problem identification and analysis skills on data mining and big data applications
**CO3:** Solution design capability with data mining and big data technologies

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 1 | 2 | 2 |
| **CO2** | 2 | 3 | 3 | 1 | 1 | 3 |
| **CO3** | 2 | 2 | 3 | 2 | 2 | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Introduction to data warehousing - ETL process,OLAP, Data mining - Market Basket Analysis, Association rue mining: frequent pattern mining, FP Tree, Apriori algorithm, Decision Trees - Classification and Regression Trees - Tree induction. Recommender Systems - Collaborative Filtering, Content Based Recommendation, Knowledge Based Recommendation. |
| **2** | Visualisation of social graphs, Social network exploration/ processing: graph classification, clustering of social-network graphs, centrality measures, community detection and mining, outlier detection. Information diffusion in graphs: Cascading behaviour, spreading, epidemics, heterogeneous social network mining, influence maximisation. |
| **3** | Introduction to Big Data Technology - Hadoop, HDFS, MapReduce. Apache Spark -Spark Core, High Level Architecture, Spark Context, RDD, Lazy Operation, Caching methods, Spark SQL. |
| **4** | Mining data stream, Examples of data stream applications, Sampling in data streams, Filtering streams, Counting distinct elements in stream, Spark ML and Applications. |

**Text Books:**

1. Ian H. Witten and Eibe Frank, Data Mining: Practical Machine Learning Tools and Techniques (Second Edition), Morgan Kaufmann, 2005
2. Data Analytics with Spark Using Python, By Jeffrey Aven, Addison Weley Data & Analytics series, 2018
3. Analysing Social Networks, Steven Borgatti, Martin Everett and Jeffrey Johnson, Sage, 2013

**References:**

1. Jannach D., Zanker M. and FelFering A., Recommender Systems: An Introduction, Cambridge University Press, 2011
2. Understanding Social Networks: Theories, Concepts and Findings, Charles Kadushin, Oxford University Press, 2011

## M2020103 DATA STRUCTURES AND ALGORITHMS

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/ Project | Year of Introduction |
|---|---|---|---|
| **M202103** | **Data Structures and Algorithms** | **3-1-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

- To impart the basic concepts of data structures and algorithms
- To understand concepts about searching and sorting techniques
- To understand basic concepts about stacks, queues, lists, trees and graphs
- To enablewriting algorithms and doing a step by step approach in solving problems with the help of fundamental data structures

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Analyze a given algorithm and express its time and space complexities in asymptotic notations.

**CO2**: Summarize the operations and applications of abstract and concrete data structures.

**CO3:** Apply the concept of recursion and heap in problem solving.

**CO4:** Show data representation and manipulation using nonlinear data structures like trees and graphs.

**CO5:** Explainvarioustechniquesforsearching, sorting, hashing and patternmatching

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | |
| **CO2** | 3 | 3 | 3 | 2 | | |
| **CO3** | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | Introduction to ADT and Algorithms: Principles of DSA, ADT, computationalproblem,algorithmnotion, Analysisofalgorithms – timecomplexity,spacecomplexity,asymptoticnotations - Big-Ohnotation, Big-Omega notation, Theta notation, Small-Ohnotation, Small-Omega notation; Notion of best, worst and average casecomplexity. |

| | |
|---|---|
| | Overview of algorithm design techniques –incrementaldesign, Divide and conquer technique, Greedy technique, Dynamic Programming.<br>Recursion:<br>Closedform,recursiveform,problemsolving,Fibonacciseries,TowersofHanoi, Writing recurrence relation for a given problem and solution using substitution technique. |
| **2** | Implementation Lists and Linked List: Lists ADT, Linked list - basic operations, doublylinked list,<br>Introduction to stack, basic operations, Applications of stack data structure – parenthesis matching, Conversion from Infix notation to Polish and reverse Polish notations, Evaluation of expression using stack<br>Introduction to queues - basic operations. Circular queues, Priority Queues.<br>Heap: Introduction,max heap,minheap,representation, applications<br>Complexity of basic operations on LL, stack, queue and heap data structures |
| **3** | Non-linear data structures: Complexities of basic operations<br>Binarytree,traversalinatree,binary search tree, notion of height balancedtrees, AVL trees, B-tree, red black tree.<br>Graph: Weighted graph, spanning tree,Kruskal’salgorithm,Prim’salgorithm, graph traversal techniques – DFSandBFS, shortest path problem - Dijkstra’salgorithm |
| **4** | Searchingalgorithms:LinearandBinary search.<br>Sorting techniques – bubble sort, selection sort, insertion sort, merges sort, heap sort, quick sort.<br>Hashing:openaddresshashing,doublehashing,chaining.Patternmatchingandstring/ text<br>Dynamic Programming techniques – Optimal substructure property, Overlapping sub-problems property, Memorization; Matrix chain Multiplication Problem, Longest Common Subsequence Problem |

**Lab Exercises:**

**Module 1:**
Array-based stack implementation, plotting complexity values to show the asymptotic behavior

**Module 2:**
Implementation of linked list, stack, queue, heap

**Module 3:**
Determining shortest path from a graph

**Module 4:**
Implementing sorting and searching algorithms, Implementation of hashing

Other interesting problems (from online platforms like https://leetcode.com/) where data structures need to be used in an intelligent way.

**Text Books:**

1. T.H. Cormen Introduction to algorithms, MIT Press. 2009
2. Bradley N. Miller, David L. Ranum Problem Solving with Algorithms and Data Structures Using Python, Franklin, Beedle & Associates, 2011

**References:**

1. A.D Aho, J. E. Hopcroft and J. D. Ullman, Data Structures and Algorithms, Pearson

education Asia, 1983.
2. Y. Langsam, M. J. Augenstein and A. M. Tenenbaum, Data Structures using C, PearsonEducation Asia, 2004
3. Adam Drozdek, Data Structures and Algorithms in Java, Published by Brooks/Cole, 2nd edition2002.

## M3022301 DATABASE SECURITY

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/ Project | Year of Introduction |
|---|---|---|---|
| **M302301** | **Database Security** | **3-0-0-1** | **2021** |

**Prerequisites: Nil**

**Course Objectives:**

- To teach different types of databases.
- To teach the security aspects of databases
- To perform data auditing

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Discriminate between different Types of Databases
**CO2:** Develop and designs EntityRelationship Models
**CO3:** Summarize concepts related to applications of SQL
**CO4:** Identify differential attributes of Structured Data, Unstructured Data & Semi-Structured Data
**CO5**: Apply principles of Database Security for efficient Data auditing.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | |
| **CO2** | 3 | 3 | 3 | 2 | | |
| **CO3** | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Different Types of Databases, Entity Relationship Models, Relational Models,RelationalAlgebra,Calculus,ACIDProperties,RelationalDatabases,ConcurrencyControl,ProcessofDatabaseDesign,Dependenciesand NormalizationforRelationalDatabases,Object-oriented/Object-RelationalModels, Threats to the Database, Principles of Database Security, Levels of DatabaseSecurity, Database Security Issues, |
| **2** | IntroductiontoSQL,SQLFeatures,SQLOperators,SQLDatatypes,SQLParsing,Typesof SQLCommands,AdvancedStudyofStructuredQueryLanguage,QueryingDatafromthedatabase,CorrelatedSub-queries,Joins,HierarchicalQueries,BindVariables,Cursors,Functions,StoredProcedures,<br>MySQL,BasicsofNewSQLDatabases, SQLInjectionandMitigation, |
| **3** | StructuredData,UnstructuredData,Semi-StructuredData,LimitationsofTraditional RDBMSs, SQL and Structured Data, SQL and Semi-Structured Data,SQLandUnstructuredData,TheEmergenceofNoSQL,NoSQLDatabasefeatures,TypesofNoSQLDatabases,SearchEngineDatabases,Basicsof MongoDBandNeo4j, DataAuditing,StatisticalDatabaseSecurity,Semantic Integrity Control, Privilege Analysis, Virtual Private Database(VPD),DataRedaction,SensitiveDataProtection, |
| **4** | Authentication and Authorization in DBMS,PropertiesandBasicPrinciplesofAccess ControlMechanisms, Viewsfor AccessControl, Classical Database Access Control: Discretionary Access Control, Role-Based Access Control and Mandatory Access Control; Access Control in OpenEnvironments suchasAttributeBased EncryptionandIdentityBasedEncryption, Access Control in SQL, Network DataEncryption,StrongAuthentication,PrivateDataAggregation,SearchinEncryptedData:Searchable EncryptionOverview,Selected SchemesonSearchable Encryption |

**Text Books:**

1. Abraham Silberschatz, Henry F. Korth, S. Sudharshan, Database System Concepts, 6th Ed., Tata McGraw Hill, 2011.
2. Andreas Meier, Michael Kaufmann, SQL & NoSQL Databases: Models, Languages, Consistency Options and Architectures for Big Data Management, Springer, 2019
3. Guy Harrison, Next Generation Databases: NoSQL, NewSQL, and Big Data, Apress
4. Ramez Elmasri, Shamkant B. Navathe, Fundamentals of Database Systems, 6th Ed., Pearson Education, 2011.
5. Ron Ben Vatan, Implementing Database Security & Auditing

**References:**

1. C. J. Date, A.Kannan, S.Swamynathan, An Introduction to Database Systems, 8th Ed.n, Pearson Education, 2006
2. Elmasri, Ramez; Navathe, Shamkant B, Fundamentals of Database Systems, Pearson, 2000
3. G.K. Gupta, Database Management Systems, Tata McGraw Hill, 2011
4. Hellerstein, Joseph, Michael Stonebraker, Readings in Database Systems (The Red Book),

5. 4th ed., MIT Press, 2005
6. Jan L Harrington, Object Oriented Database Design Clearly Explained, Harcourt, 2000
7. Raghu Ramakrishnan, Database Management Systems, 4th Ed, McGraw-Hill, 2015
8. Raghu, and Johannes Gehrke, Database Management Systems, 3rd ed. McGraw-Hill, 2002
9. Stefano Ceri, Giuseppe Pelagatti, Distributed Databases: Principles and Systems, Universities Press, 2000
10. Vijay Atluri, Pierangela Samarati, Security of Data and Transaction.

## M2021202 DATABASE SYSTEMS

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M202202** | **Database Systems** | **3-0-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To provide students with a good understanding of the concepts of information theoretic methods of database systems described in the syllabus.
2. To help the students develop the ability to solve problems using the learned concepts.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Understand the foundations of modern database systems theory, problem and state of the art solutions.

**CO2**: Analyze and evaluate critically the building and integration of database algorithms and systems.

**CO3:** Design and demonstrate a working database system through team research project, and project report, presentation.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge.

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature.

**PLO 3** Apply scholarship to conduct independent and innovative research.

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences.

**PLO 5** Practice ethical standards of professional conduct and research.

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | |
| **CO2** | 3 | 3 | 3 | 2 | | |
| **CO3** | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| **1** | Introduction to Database Management Systems: Abstraction, Independence, ACID Properties, DBMS Architecture, Comparison with File Server Model.<br>Data Modeling: E-R Modeling, Relational Model: Concepts, Tables, Keys, Data Integrity and Constraints, Normalization |
| **2** | Introduction to SQL: SQL Features, SQL Operators, SQL data types, SQL Parsing, Types of SQL Commands, Advanced Study of Structured<br>Query Language, Querying Data from the database, Correlated Sub-queries, Joins, |

|  |  |
|---|---|
|  | Hierarchical Queries, Cursors, Functions, Stored Procedures. |
| **3** | Distributed Databases: Architectures, Replication and Fragmentation, Query Processing in Distributed Databases, Commit Protocols, Concurrency control, Deadlock Handling and Recovery in Distributed Database Management Systems. |
| **4** | Overview, and History of NoSQL. The Emergence of NoSQL, MongoDB, Cassandra, HBASE, Neo4j use and deployment, Application, Challenges NoSQL<br>approach, Key-Value and Document Data Models, Column-Family Stores, Aggregate-Oriented Databases, Replication and sharding |

**Text Books:**

1. Database Management System, MonelliAyyavaraiah, ArepalliGopi, Horizon Books,2017
2. SQL & NoSQL Databases: Models, Languages, Consistency Options and Architectures for Big Data Management, Andreas Meier, Michael Kaufmann, Springer,2019
3. Abraham Silberschatz; Henry F Korth, Database System Concepts, McGraw Hill Publication, 2002
4. Hellerstein, Joseph, and Michael Stonebraker. Readings in Database Systems (The Red Book). 4th ed. MIT Press, 2005.
5. Raghu, and Johannes Gehrke. Database Management Systems. 3rd ed. McGraw-Hill, 2002.

**References:**

1. Stefano Ceri; Giuseppe Pelagatti, Distributed Databases: Principles and Systems, Universities Press, 2000
2. Jan L Harrington, Object Oriented Database Design Clearly Explained, Harcourt, 2000
3. Elmasri,Ramez; Navathe, Shamkant B, Fundamentals of Database Systems, Pearson, 2000

## M3021204 DEEP LEARNING AND REINFORCEMENT LEARNING

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M302204** | **Deep Learning and Reinforcement Learning** | **3-0-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To provide students with a good understanding of the concepts of deep learning and reinforcement learning described in the syllabus.
2. To help the students develop the ability to solve problems using the learned concepts.
3. To connect the concepts to other domain both within and without mathematics such as pattern recognition.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Understand the foundations of modern deep learning and reinforcement learning theory, problem and state of the art solutions.

**CO2**: Analyze and evaluate critically the building and integration of deep learning and reinforcement learning algorithms and systems.

**CO3:** Design and demonstrate a working deep learning and reinforcement learning system through team research project, and project report, presentation.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | |
| **CO2** | 3 | 3 | 3 | 2 | | |
| **CO3** | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low)   2: Moderate (Medium)    3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Deep Networks: Deep FeedForward Networks, Regularization in Deep Learning, Optimization for Training Deep Models. Convolutional Neural Networks, Sequence Modeling - Recurrent and Recursive Nets. Concept of Attention and  Transformer Architectures.  Generative Adversarial Networks. |
| **2** | Autoencoders- Transfer learning-Few Shot Learning, Zero-shot Learning . Practical Methodology. Applications of Deep Learning in domains involving natural language text/speech, Images and videos. |
| **3** | Introduction to Reinforcement Learning, Markov Processes Markov Reward Processes (MRPs) Markov Decision Processes (MDPs), MDP Policies, Policy Evaluation, Policy Improvement, Policy Iteration, Value operators. Model-free learning - Q-learning, SARSA, Scaling up: RL with function approximation, RL with function approximation. |
| **4** | Imitation learning in large spaces, Policy search, Exploration/Exploitation, Meta-Learning, Batch Reinforcement Learning, Bandit problems and online learning. Solution methods: dynamic programming, Monte Carlo learning, Temporal difference learning, Eligibility traces, Value function approximation, Models and planning. |

**Text Books:**

1. Sutton, R. S. & Barto, A. G. (1998), Reinforcement Learning: An Introduction , MIT Press .
2. Csaba Szepesvari. 2010. Algorithms for Reinforcement Learning. Morgan and Claypool Publishers.
3. Josh Patterson and Adam Gibson, "Deep learning: A Practitioner's Approach", O'Reilly, 2017.
4. Ian Goodfellow, Y. Bengio and A. Courville, "Deep Learning", MIT Press, 2016.

**References:**

1. Kevin P. Murphy. 2012. *Machine Learning: A Probabilistic Perspective*. The MIT Press.
2. Martin L. Puterman. 1994. *Markov Decision Processes: Discrete Stochastic Dynamic Programming* (1st. ed.). John Wiley & Sons, Inc., USA.
3. Michael A. Nielsen, "Neural Networks and Deep Learning", Determination Press, 2015.
4. Li Deng and Dong Yu, "Deep Learning: Methods and Applications", 2013.

## M3021211 DIGITAL IMAGE AND VIDEO PROCESSING

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M302211 | Digital Image and Video Processing | 3-0-0-1 | 2021 |

**Prerequisites**

**CourseObjectives:**

1. Toprovidestudentswithagoodunderstandingoftheconceptsof Image processing described in the syllabus.
2. Tohelpthestudentsdeveloptheabilitytosolveproblemsusingthelearnedconcepts.
3. Toconnecttheconceptstootherdomainbothwithinandwithout image processing suchasmachine learningandpattern recognition.

**CourseOutcomes:**Aftercompletionofthiscourse,thestudentswouldbeableto:

**CO1:** Understandthe digital image processing techniques andstateoftheartsolutions.

**CO2**: Analyzeandevaluatecriticallythebuildingandintegrationof digital image processing.

**CO3:**Designanddemonstrate digital image processingthroughteamresearchproject,andprojectreport,presentation.

**ProgramLearningOutcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge.
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature.
**PLO 3** Apply scholarship to conduct independent and innovative research.
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences.
**PLO 5** Practice ethical standards of professional conduct and research.
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mappingofcourseoutcomeswithprogramlearningoutcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 3 | 3 | 2 | 2 | 1 | 2 |
| CO2 | 3 | 3 | 3 | 2 | 1 | 2 |
| CO3 | 2 | 1 | 1 | 2 | 3 | 3 |

(Correlation:1:Slight(Low)2:Moderate(Medium)3:Substantial(High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | Introduction to Image Processing Systems, Image Acquisition, Sampling and Quantization, Pixel Relationships, Color Fundamentals and Modules, File Formats, Image Enhancement and Restoration, Spatial Domain Gray Level Transformations, Histogram Processing, Spatial Filtering, Smoothing and Sharpening. |
| 2 | Frequency Domain: Filtering in Frequency Domain, DFT, FFT, DCT, Smoothing and Sharpening Filters, Homomorphic Filtering. Noise Models: Spatial and Frequency Properties of Noise, Important Noise Probability Density Functions, Periodic Noise, Estimation of Noise Parameters, Constrained and Unconstrained. |
| 3 | Restoration Models, Image Deblurring Algorithms. Morphological Image Processing: Erosion and Dilation, Opening and closing, Hit or miss transformation, basic morphological algorithms, gray scale morphology. Image Segmentation and Feature Analysis, Detection of Discontinuities, Edge Operators, Edge Linking and Boundary Detection, Thresholding, Region based Segmentation: Region Growing, Region Splitting and Merging. Representation and description: boundary and regional descriptors, Image Compression: classification of lossy and lossless image compression schemes. |
| 4 | Video Formation, Perception and Representation: Video Capture and Display, Analog Video Raster, Digital Video, Fourier Analysis of Video Signals and Frequency Response of the Human Visual System. Video Sampling: Basics of the Lattice Theory, Sampling of Video Signals Over Lattices, Filtering Operations in Cameras and Display Devices. Video Sampling Rate Conversion, Different Video Modeling.Video Object Tracking and segmentation. Object recognition, pattern and pattern classes, recognition based on decision- theoretic methods, structural methods, case studies –image analysis, image coding. |

**Textbooks:**

1. Refael C Gonzalez and Richard E Woods, Digital Image Processing, Third Edition, Pearson Education, 2008.
2. Alan C. Bovik. 2005. Handbook of Image and Video Processing (Communications, Networking and Multimedia). Academic Press, Inc., USA.
3. Anil K. Jain, Fundamentals of Digital Image Processing, Prentice Hall India, 2008.

**References:**

1. Madhuri A Joshi, Digital Image Processing: An Algorithmic Approach, Prentice Hall India,

2006.

2. Rafael C. Gonzalez, Richard E woods, Steven L Eddins, Digital Image Processing Using MATLAB, First Edition, Pearson Education, 2004.
3. Milan Sonka, Vaclav Hlavac and Roger Boyle, Image Processing, Analysis and Machine Vision, Third Edition, Brooks Cole, 2008.

## M3020353 EMBEDDED SYSTEMS

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M302353** | **Embedded systems** | **3-0-0-1** | **2021** |

**Prerequisites:** Students should have already taken or are currently taking the following courses
1. Digital Experience Lab

**Course Objectives:**

1. To introduce concepts of embedded systems: microcontroller platforms, memory, registers, interrupts and interaction with peripherals.
2. To train students to develop basic programming skills required using the ARM IDE of instructors choice and introduce debugging.
3. To train students to leverage the skills acquired to solve real world problems using embedded systems.

**Course Outcomes:** After completion of this course, the students would be able to:
**CO1:** knowledge on Microcontroller platforms for building embedded applications
**CO2:** Learn basic programming on embedded systems using assembly and embedded C
**CO3:** Understanding on interfacing peripherals in the microcontrollers and how to choose the appropriate family of ARM microcontrollers based on real world applications.
**CO4:** Learn interfacing external I/O and sensors for various applications.
**CO5:** Introduction to ML in resource constrained applications.

**Program Learning Outcomes:**
**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3**Apply scholarship to conduct independent and innovative research
**PLO 4**Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences
**PLO 5** Practice ethical standards of professional conduct and research
**PLO6**Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 3 | 3 | 3 | 1 | 2 | 2 |
| CO2 | 3 | 2 | 3 | 2 | 3 | 2 |
| CO3 | 3 | 3 | 2 | 2 | 3 | 2 |
| CO4 | 3 | 2 | 3 | 2 | 1 | 1 |
| CO5 | 2 | 2 | 2 | 1 | 1 | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | Introduction to Embedded Systems and its Architecture: Introduction & overview, characteristics of embedded computing applications, concept of real time systems, challenges in embedded systems. Instruction set architecture, CISC and RISC instruction set architecture, basic embedded processor, microcontroller architecture, CISC examples, 8051, RISC example, DSP processors, ARM Cortex M Controllers. |
| 2 | Memory Management and Designing Embedded Computing Platforms: virtual memory, memory management, unit and address translation, I/O sub-system, busy-wait I/O, DMA, interrupt driven I/O, co-processors and hardware accelerators, processor performance enhancement, pipelining, super-scalar execution, CPU Bus and organization. Types of memory. |
| 3 | Introduction to the ARM architecture: operation modes and states - Programmer’s model, ARM and Thumb instruction sets, Internal Memory - registers, special function registers, Program Status Registers, flags, memory map, stack memory, Exceptions and Interrupts, nested vectored interrupt controller (NVIC), vector table, Fault handling. Introduction to ARM programming environments, Introduction to IDE *, Basic programming and Debugging. |
| 4 | Designing Using ARM Cortex M3: Introduction to ARM Cortex M family, STM/Ti Microcontrollers*, I/O devices, timers and counters, watchdog timers, interrupt controllers, Serial Communication, ADC and DAC converters, Interfacing peripherals: displays, keyboards, Sensor interfacing, memory interfacing, I/O device interfacing, ARM Mbed Platform and Introduction to ML in embedded platforms. |

**Text Books :**

1. Joseph Yiu, ” The Definitive Guide to ARM Cortex-M3 and Cortex®-M4 Processors”,Newnes, 3rd Edition,
2. Trevor Martin, The Designer's Guide to the Cortex-M Processor Family, Elsevier
3. Jonathan W. Volvano, Embedded Microcomputer Systems: Real-Time Interfacing, 2nd edition, CENGAGE-Engineering
**4.** Muhammed Ali Mazidi, Janice Mazidi and Rolin McKinlay, 8051 Microcontroller and Embedded Systems, 2nd edition, Prentice Hall

**References:**

1. Kenneth J. Ayala, 8051 Microcontroller, 3rd edition, Thomson, 2005.
2.Joseph Yiu, "The Definitive Guide to ARM CORTEX-M3 and CORTEX®-M4 Processors, 2nd Edition”, Elsevier
3. Perry Xiao, ”Designing Embedded Systems and the Internet of Things (IoT) with the ARM mbed” ,Wiley

**Note :**

* Instructors Choice : Based on availability.
* Engage students with Mini projects, if ES lab is not available to provide hands-on experience and better understanding of the concepts.

# M3022302 ETHICAL HACKING AND DEFENSIVE TECHNIQUES

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M302302 | Ethical Hacking and Defensive Techniques | 3-0-0-0 | 2021 |

**Prerequisites:** Nil

**Course Objectives:**

1. To help the students apply tools and techniques to explore cyber security breaches.
2. To provide students with a knowledge of the need for protecting the cyber assets from an adversary.
3. To provide students with a knowledge of employing machine learning techniques for vulnerability assessment.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Apply tools and techniques to evaluate whether the computer systems, critical infrastructures, IoT and networks are vulnerable to cyber attacks.

**CO2**: Understand the need for protecting network and computer systems from cyber attacks.

**CO3:** Analyze the vulnerabilities present in the networks and computer systems using machine learning techniques.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 3 | | 3 | | 3 | |
| CO2 | 3 | 2 | | | 1 | |
| CO3 | 3 | 3 | | 3 | | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | Introduction to Ethical Hacking, Hacking Concepts, Hacking Life Cycle, Information Security Laws and Standards, Domains in Cyber Security, Footprinting Concepts, Footprinitng Countermeasures. |

| | |
|---|---|
| | Network Scanning Concepts, Ports, Services & Protocols, OS Discovery, Enumeration Concepts & Techniques, Enumeration Countermeasures, Vulnerability Scanning & Identification, Vulnerability Assessment Report Preparation, |
| **2** | Hacking Concepts, Gaining Access, Escalating Privileges, Maintaining Access, Clearing Logs<br>Malware Concepts, APT Concepts, Fileless Malware Concepts, Malware Analysis, Countermeasures to Malware, Sniffing Concepts & Techniques, Countermeasures to Sniffing, Detection mechanisms to sniffing, Social Engineering Concepts & Techniques, Identify Theft, Countermeasures to Social Engineering. |
| **3** | DoS & DDoS Attacks, Countermeasures to DoS & DDoS, Session Hijacking & Countermeasures, Hacking Web Applications, OWASP Top 10, Countermeasures to Web App Attacks, Web Shells, Patch Management. IDS, IPS, Firewall & NG- Firewall Concepts, DMZ Architecture, Network Infra Devices (Web Proxy, Reverse Proxy, SIEM Solutions, EDR & AV, WAF), Honeypots, SIEM Architecture, SOAR Concept, Use Cases in Network Defense, Use of Workbooks and Playbooks in Network Defense. |
| **4** | Wireless Threats, Hacking Wireless Networks, Vulnerabilities in Wireless Networks, Countermeasures to wireless Hacking, Hacking Mobile Platforms, Vulnerabilities in Mobile Apps, Cloud Computing Concepts & Technologies, Cryptography Concepts, Disk Encryption, Email Encryption, Vulnerabilities in Encryption, Countermeasures. |

**Text Books:**

1. Phillip L. Wylie , The PentesterBluePrint, Wiley Publication, 2021.
2. James Corley, Kent Backman , Michael Simpson , Hands on Ethical Hacking and Network Defense, DelmarCengage Learning.
3. Patrick Engebretso, The Basics of Hacking and Penetration Testing, Second Edition, Syngress Publication.
4. Sean-Philip Oriyano, CEH Certified Ethical Hacker Version 8 Self-study Guide, Wiley / Sybex, 2014
5. Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte, The Shell Coder's handbook Discovering and Exploiting Security Holes, 2nd Edition. John Wiley & Sons, 2011
6. Justin Seitz, Black Hat Python, No Starch Press, Inc. 2014
7.

**References:**

1. Peter Kim, The Hacker Playbook 2: Practical Guide to Penetration Testing, Createspace Independent Pub, 2015
2. Michael T Simpson, Hands-On Ethical Hacking and Network Defense 2nd Edition, Cengage Learning, 2012
3. Rafay Baloch, Ethical hacking and Penetration Testing Guide, CRC Press 2014.
4. Kevin Beaver, Hacking for Dummies 5th Edition. John Wiley & Sons, 2013
5. Stuart McClure, Joel Scambray and Goerge Kurtz, "Hacking Exposed Network Security Secrets & Solutions", Tata Mc

## M3010264 ETHICAL HACKING AND NETWORK DEFENSE

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M301264 | Ethical Hacking and Network Defense | 3-1-0-0 | 2021 |

**Prerequisites:** Nil

**Course Objectives:**

1. To help the students apply tools and techniques to explore cyber security breaches.
2. To provide students with a knowledge of the need for protecting the cyber assets from an adversary.
3. To provide students with a knowledge of employing machine learning techniques for vulnerability assessment.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Apply tools and techniques to evaluate whether the computer systems, critical infrastructures, IoT and networks are vulnerable to cyber attacks.

**CO2**: Understand the need for protecting network and computer systems from cyber attacks.

**CO3:** Analyze the vulnerabilities present in the networks and computer systems using machine learning techniques.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

|  | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 |  | 3 |  | 3 |  |
| **CO2** | 3 | 2 |  |  | 1 |  |
| **CO3** | 3 | 3 |  | 3 |  | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| **1** | Introduction to ethical hacking: Types of hackers, Ethical hacking steps, Social engineering, Phishing, Website cloning, Whatsapp Phishing, spywares and backdoors, Password cracking, Cookie stealing, Botnets, Dos/DDoS attacks, MITM attack. Investigating statistical weaknesses in TCP/IP Initial Sequence numbers, |

| | |
|---|---|
| | Implementing ML based Trojan and spyware detection mechanisms. |
| **2** | Network scanning and Web application Penetration testing:-Information gathering, Banner grabbing tools, Foot printing and reconnaissance, Recon-ng framework, Enumeration, Scanning the networks, Advanced IP Scanner, Port scanning using Nmap, vulnerability scanning using Openvas and Nessus, Network packet capturing, Wireshark, Python for hackers, Scapy, Buffer overflow attacks, Exploit development, Immunity debugger, Shell coding in Linux, Metasploit framework, Routersploit, Pentesting web applications, Web Vulnerability scanners, Cross site scripting, SQL injection attacks, Local file inclusion, Remote file inclusion, Cross site request forgery, Burp suite application, Websploit framework, Bug bounty platforms, Wireless protocols, Hacking WLAN Authentication, Wireless MITM, WEP Cracking, WPA/WPA2-PSK hacking, Hacking Mobile Devices:- Vulnerabilities in Mobile Apps, OWASP top 10 vulnerabilities for mobile application, Investigating SQL injection attack challenges, Investigating Padding Oracle Attack in a PHP website, ML based vulnerability assessment in networks. |
| **3** | IoT hacking:- Detecting open and poorly protected communication ports, Sniffing: Capture and analysis of radio signals in IoT, Detecting firmware modification attacks and buffer overflow attacks, Identifying buses and Interfaces of the IoT device, NandGlitching, JTAG debugging and Exploitation. Investigating software and hardware attacks in IoT.<br>Critical Infrastructure hacking and penetration testing: - Passive enumeration, Active enumeration, Physical inspection, Active port scanning, Active testing of network isolation, Raspberry PI, Arduino, Honeypot using Raspberry Pi, Investigating different software and hardware attacks in SCADA systems, ML based vulnerability assessment in IOT and critical infrastructures. |
| **4** | Network Defense:- Understanding Routers, Routing Protocols, Hardware Routers, Access control Lists, Understanding Firewalls:- Firewall Technology , Understanding Intrusion detection systems and Prevention systems:- Network based and Host based IPS/IDS, Web Filtering, Security Incident Response Team, Investigating Honeypot Mechanisms for Network Defense, Building ML based network defense mechanisms. |

**Text Books:**

1. Phillip L. Wylie, The PentesterBluePrint, Wiley Publication, 2021.
2. James Corley, Kent Backman , Michael Simpson , Hands on Ethical Hacking and Network Defense, DelmarCengage Learning.
3. Patrick Engebretso, The Basics of Hacking and Penetration Testing, Second Edition, Syngress Publication.

**References:**

1. Peter Kim, The Hacker Playbook 2: Practical Guide to Penetration Testing, Createspace Independent Pub, 2015.

## M3010293, M302255HARDWARE SECURITY

| Course | Course Name | Credit Split | Year of |
|---|---|---|---|

| Code | | Lecture/Lab/Seminar/Project | Introduction |
|---|---|---|---|
| M301293,<br>M302255 | Hardware Security | 3-1-0-0 | 2021 |

**Prerequisites:** Prior knowledge of computer networks, cryptography, sensor networks and basics of computer hardware.

**Course Objectives:**

This course aims to:

1. Provide knowledge of the state-of-the-art security methods and devices.
2. Familiarize the range of hardware-level attack techniques and countermeasures.
3. Make students aware of potential hardware vulnerabilities and provide them with the knowledge and skills needed to build trustworthy hardware.

**Course Outcomes:**

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

- **C01**: Describe the vulnerabilities in current digital system design flow and the physical attacks to these systems.
- **C02**: Demonstrate proficiencies in understanding hardware security issues.
- **C03**: Apply the tools and skills to build secure and trusted hardware
- **C04**: Discuss the recent trends in the domain of hardware security and apply their knowledge in research and development.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written)
**PLO 5** Practice ethical standards of professional conduct and research
**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

## Mapping of course outcomes with program learning outcomes:

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 2 | 1 | | 2 | | |
| **CO2** | 2 | 1 | 1 | 1 | | |
| **CO3** | 2 | 2 | 1 | 2 | 1 | |
| **C04** | | 2 | 2 | 2 | 3 | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | Hardware Security threats, Vulnerabilities, and Attacks. Challenges in Securing Hardware, Threats to Hardware. Hardware Security Vulnerability Assessment. Hardware-Assisted Computer Security: ARM TrustZone, Intel SGX. Hardware Root of Trust, Trusted Platform Module (TPMs), TPM Cryptographic Hardware, Hardware Accelerators, Cryptographic Coprocessors. Implementing Security in Reprogrammable Hardware. FPGA Basics, Applications and Uses, FPGA Based Security Solutions. |
| **2** | Modern IC Design and Manufacturing Practices and Their Implications: Hardware |

| | |
|---|---|
| | Intellectual Property (IP) Piracy and IC Piracy, Design Techniques to Prevent IP and IC Piracy, Physically Unclonable Functions (PUFs), PUF Implementations and using PUFs to prevent Hardware Piracy, Model Building Attacks on PUFs (Case Study: SVM Modeling of Arbiter PUFs, Genetic Programming based Modeling of Ring Oscillator PUF).JTAG Protection**.** |
| **3** | Side-channel Attacks (SCA) on Cryptographic Hardware: Current-measurement based Side-channel Attacks, power, electromagnetic SCA. Design Techniques to Prevent Side-channel Attacks, Improved Side-channel Attack Algorithms and Cache Attacks. Fault-tolerance of Cryptographic Hardware, Fault Attacks. Hardware Trojan based SCA. |
| **4** | Hardware Trojans: Hardware Trojan Nomenclature and Operating Modes, Countermeasures-Design and Manufacturing Techniques to Prevent/Detect Hardware Trojans, Logic Testing and Side-channel Analysis based Techniques for Trojan Detection. Case study: Hardware security issues and solutions in vehicles, hardware security of fog end-devices for the internet of things. |

**Books and other resources:**

1. Recent Publications from top-Tier Conferences and Journals
1. Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, Hardware Security: Design, Threats, and Safeguards, Chapman and Hall/CRC.
2. Debdeep Mukhopadhyay, Rajat Subhra Chakraborty, Hardware Security: Design, Threats, and Safeguards Hardcover, ISBN-13: 978-1439895832, Chapman and Hall/CRC.
3. Jin Y. Introduction to hardware security. Electronics. 2015 Dec; 4(4):763-84.
4. Sidhu S, Mohd BJ, Hayajneh T, Hardware security in IoT devices with emphasis on hardware Trojans. Journal of Sensor and Actuator Networks. 2019 Sep; 8(3):42.
5. Butun I, Sari A, Österberg P. Hardware Security of Fog End-Devices for the Internet of Things. Sensors. 2020 Jan; 20(20):5729.
6. Labrado C, Thapliyal H. Hardware security primitives for vehicles. IEEE Consumer Electronics Magazine. 2019 Oct 31; 8(6):99-103.
7. Prinetto P, Roascio G, Hardware Security, Vulnerabilities, and Attacks: A Comprehensive Taxonomy. InITASEC 2020 Aug 4 (pp. 177-189).

## M3010222 HUMAN COMPUTER INTERACTION

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301222** | **Human Computer Interaction** | **3-0-0-1** | **2021** |

**Prerequisites:** Students should possess the fundamental programming skills in Computer Programming Languages such as Python and have prior experience in handling software scripting, prototyping and code management tools.

**Course Objectives:**

1. Understand the fundamentals of Human-Computer Interaction and design technologies and recognize the theoretical perspectives of human factors that influence the acceptance of computer interfaces.
2. Understand the critical aspects of implementation of human-computer interfaces and identify the various tools and techniques for interface analysis, design, and evaluation and develop comprehensive, user-friendly andinteresting interfaces.
3. Introduce the student to the literature and research aspectsof human-computer interaction.

**Course Outcomes:**

By the conclusion of this course, students should be able to:

**C01**: Explain and apply core theories and models from the field of HCI.
**CO2**: Apply theoretical concepts to design and develop useful and usable interfaces.
**C03**: Discuss and critique research in the field of HCI and report research findings in scientific articles.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge.
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature.
**PLO 3** Apply scholarship to conduct independent and innovative research.
**PLO 4** Show communication skills in a variety of formats (oral, written).
**PLO 5** Practice ethical standards of professional conduct and research.
**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

## Mapping of course outcomes with program learning outcomes:

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 1 | | 1 | | |
| **CO2** | 2 | 2 | 1 | 2 | | |
| **CO3** | 1 | 2 | 2 | 2 | | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Introduction to HCI, History of HCI, Factors in HCI, Disciplines contributing to HCI, User Interface Design: Models, Principles, Practices. Direct Manipulation. Input and Interaction Techniques, Tangible and Embodied User Interactions, Mobile Interactions, Crowdsourcing, Augmented/Virtual Reality and HCI, Web Interfaces, Assistive and Accessible Interfaces. |
| **2** | Cognitive Framework of HCI. Mental models. Perception & Representation. Attention and Interface Design. Memory in Interface Design. Knowledge Representation. User Modeling, Understanding Users, Cognitive and Affective Factors.User Interface for Games,Social Issues influencing HCI Design and Use. Modelling Social and Emotional Processes.Context Awareness in HCI. |
| **3** | Interaction with Natural Languages, Next Generation Interface.Interfaces Design and Prototyping, Usability Testing & Analytic Evaluation: Introduction, Cognitive Walkthrough. Heuristic Evaluation. Evaluation with Cognitive Models, Evaluation with Users, Model-based Design and evaluation. HCI and Data Visualization. |
| **4** | Modeling Interaction: Descriptive and Predictive Techniques, Digital and Physical Prototyping, Research Methods in HCI, Quantitative research, Accessibility Research, Research Ethics. Future of HCI, Non- WIMP/ Natural/Multimodal Interfaces, Mobile and Wearable Computing, High End Cloud Service and Multimodal Client Interaction. HCI for IoT enabled Systems. HCI and Usable Security. |

**Books and other resources:**

1. Recent Publications from top-Tier Conferences and Journals.
2. Alan Dix, Janet Finlay, Gregory Abowd, & Russell Beale, Human-Computer Interaction (3rd ed.), Prentice Hall, 2003.
3. Andrew Sears, Julie A. Jacko, Julie A. Jacko, The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Applications, CRC Press, eBook ISBN9780429163975

4. Ben Shneiderman, Designing the user interface strategies for effective human computer interaction, Pearson, New Delhi. 2004
5. Cooper, Reimann, Cronin, &Noessel, About Face: The Essentials of Interaction Design, Fourth Edition, 2014.
6. Donald Norman, The Design of Everyday Things, Basic Books, 2002.
7. Human Computer Interaction (HCI) – NPTEL Course
8. J. Preece, Y.RogersandH. Sharp, Interaction design: Beyond Human- Computer Interaction, John Wiley &Sons. 2015.

## M3010203 IMAGE & VIDEO PROCESSING

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301203** | **Image & Video Processing** | **3-0-0-1** | **2021** |

**Prerequisites:** Nil

Course Objectives:

1. To provide students with a good understanding of the concepts of video
2. processing tasks described in the syllabus.
3. To help the students develop the ability to solve problems using the learned concepts.
4. To connect the concepts to other domain both within and without mathematics such asmachine learning and pattern recognition.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:**Understand the foundations of modern image/video signal processing theory, problem and state of the art solutions.
**CO2**: Analyse and evaluate critically the building and integration of image/video signal processing algorithms and systems.
**CO3:** Design and demonstrate a working image/video signal processing system through team research project, and project report, presentation.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | |

|  |  |  |  |  |
|---|---|---|---|---|
| **CO2** | 3 | 3 | 3 | 2 |
| **CO3** | 2 | 3 | 3 | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| 1 | Steps in Image Processing Systems, Image Acquisition, Sampling and Quantization, Pixel Relationships, Color Fundamentals and Modules, File Formats. Image Enhancement and Restoration, Spatial Domain Gray Level Transformations, Histogram Processing, Spatial Filtering, Smoothing and Sharpening, Frequency Domain, Filtering in Frequency Domain, Smoothing and Sharpening Filters, Homomorphic Filtering |
| 2 | Image Segmentation and Feature Analysis, Detection of Discontinuities, Edge Operators, Edge Linking and Boundary Detection, Thresholding, Region based Segmentation: Region Growing, Region Splitting and Merging. Image Compression: classification of lossy and lossless image compression schemes, image segmentation and object recognition, image coding. |
| 3 | Video Formation, Perception and Representation: Video Capture and Display, Analog Video Raster, Digital Video, Fourier Analysis of Video Signals and Frequency Response of the Human Visual System. Video Sampling: Basics of the Lattice Theory, Sampling of Video Signals Over Lattices, Filtering Operations in Cameras and Display Devices. Video Sampling Rate Conversion, Different Video Modeling. |
| 4 | Two-Dimensional Motion Estimation: Block-Based Transform Coding, Predictive Coding. Video Compression Standards. Video Object Tracking and segmentation, Video Filtering, enhancement, Video stabilization and super-resolution, Video coding, representation, Content based Video retrieval, Video based Rendering. |

**Text Books:**

1. Gonzalez, R. C. & Woods, R. E. (2008), Digital Image Processing, Prentice Hall, Upper Saddle River, N.J.
2. Anil K. Jain. 1989. Fundamentals of Digital Image Processing. Prentice-Hall, Inc., USA.
3. John W. Woods. 2011. Multidimensional Signal, Image, and Video Processing and Coding, Second Edition (2nd. ed.). Academic Press, Inc., USA.
4. Y. Wang, J. Ostermann and Y.-Q. Zhang, Video Processing and Communications. Signal Proc. Series, Prentice Hall, 2002.

**References:**

1. William K. Pratt. 2007. Digital Image Processing: PIKS Scientific Inside. Wiley-Interscience, USA.
2. Scott E. Umbaugh. 2010. Digital Image Processing and Analysis: Human and Computer Vision Applications with CVIPtools, Second Edition (2nd. ed.). CRC Press, Inc., USA.
3. A. Murat Tekalp. 2015. Digital Video Processing (2nd. ed.). Prentice Hall Press, USA.
4. Alan C. Bovik. 2005. Handbook of Image and Video Processing (Communications, Networking and Multimedia). Academic Press, Inc., USA.

# M3010203 INDUSTRIAL IOT AND DIGITAL TWINS

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301203** | **Industrial Internet of Things (IIoT) and Digital Twins** | **3-0-0-1** | **2021** |

**Prerequisites:** Basic knowledge in computer networks, operating systems, distributed systems, machine learning and programming in Python.

**Course Objectives:**

1. To provide students with a thorough understanding of the fundamentals, technologies, and applications of IIoT and Digital Twins.
2. To expose students to cutting-edge fields of IIoT and Digital Twins while providing sufficient foundations for further study and research.

**Course Outcomes:**

At the end of this course, students are expected to be able to understand:

**C01**: The evolution and revolution of the future Internet, and control, networking and computing requirements for IIoT.
**C02**: How to establish and sustain digital twins for complicated yet sophisticated systems on various environments.
**C03**: Complete paper reviews, oral presentations, and a final course project.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written)
**PLO 5** Practice ethical standards of professional conduct and research
**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 2 | 2 | 2 | 2 | | 1 |
| **CO2** | 1 | 2 | 2 | 2 | | 1 |
| **CO3** | | 2 | 2 | 2 | 1 | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:** Industrial IoT and Digital Twins

| Module | |
|---|---|
| I | The History and Evolution of Industry 4.0, Basics of Industry 4.0, Key Technologies in Industry 4.0, **Industry 4.0 Design Principles, The Challenges of Industry 4.0,** IIoT and Industry 4.0, Basics of IIoT, Reference Architecture of IIoT, Review of Enabling Technologies of IIoT: IIoT Sensors, Actuators, Industrial Data Transmission and Industrial Data Acquisition. Standardization Progress: IIC, IEEE, and NIST. |
| **II** | Control Systems in IIoT. Networking Systems in IIoT. IIoT Network Protocols. Computing |

| | |
|---|---|
| | Systems in IIoT. Machine Learning for IIoT. Resource Management. Data Management In IIoT. Security and Privacy in IIoT. Collaborations between Heterogeneous IIoT Systems. Public Safety in IIoT. Research Directions of Control, Networking and Computing for IIoT. |
| **III** | Introduction to Digital Twins. Applications of Digital Twins. Digital Twin Conceptual Architecture. Challenges and Enabling Technologies associated with Digital Twins. The combination of Digital Twins, Data Analytics Platforms, AI Frameworks and Libraries, Data Lakes Running on Cloud Environments (Public, Private or Hybrid). Open Research and Challenges with Digital Twins.<br>Applications: Digital Twins for Factory Automation and Smart Manufacturing. Preventive and Predictive Maintenance of Industrial Assets. Design, Development, and Management of Systems such as Medical Instruments, Robots, Drones, etc. |
| **IV** | Review of different IIoT Platforms (Open source and Commercial): Zetta, ThingsBoard, Distributed Services Architecture (DSA), OpenRemote, Node-RED, M2MLabs Mainspring, Thinger, ThingSpeak; GE Predix, AWS IoT, Bosch IoT Suite, ThingSpace and ThingWorx.<br>Applications and Case Studies (Smart Agriculture, Smart Healthcare, Smart Manufacturing, Smart Cities, Smart home, Environment and Sustainability, Smart Grid etc..). |

**Books and other resources:**

1. Recent Publications from top-Tier Conferences and Journals.
2. Sudip Misra, Chandana Roy, Anandarup Mukherjee, Introduction to Industrial Internet of Things and Industry 4.0, ISBN 9780367897581, CRC Press.
3. Houbing Song, Glenn A Fink, Sabina Jeschke, Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications, ISBN: 9781119226048, Wiley & Sons Ltd.
4. Pethuru Raj, Preetha Evangeline, The Digital Twin Paradigm for Smarter Systems and Environments: The Industry Use Cases, Volume 117, ISBN: 9780128187562, Academic Press.
5. Arvind Ravulavaru, Enterprise Internet of Things Handbook, ISBN: 9781788838399, Packt Publishing.
6. Anand Tamboli, Build Your Own IoT Platform: Develop a Fully Flexible and Scalable Internet of Things Platform in 24 Hours, ISBN-13: 978-1484244975, Apress.
7. Louis Schrenk, Digital Twin Technology: Twins Digital Technology And Industries: Digital Twin Deployment, Kindle Edition.
8. Vijay Raghunathan, Digital Twin: A Complete Guide For The Complete Beginner, Kindle Edition.

## M3020225 INFORMATION RETRIEVAL

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M302225** | **Information Retrieval** | **3-0-0-1** | **2021** |
| **Prerequisites:** Nil | | | |
| **Course Objectives:**<br>To impart skills needed for understanding and applying data mining and big data technologies | | | |

To equip the students with the ability to identify and analyse problems solvable with data mining and big data technologies

To impart solution design capability with data mining and big data technologies

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Understand and develop techniques in data ming and big data management

**CO2**: Problem identification and analysis skills on data mining and big data applications

**CO3:** Solution design capability with data mining and big data technologies

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 3 | 1 | 1 | 1 |
| **CO2** | 3 | 3 | 3 | 2 | 1 | 2 |
| **CO3** | 3 | 3 | 3 | 1 | 1 | 3 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Introduction to Information Retrieval - Relevance of Information retrieval, The nature of the unstructured and semi-structured text, traditional IR mechanisms - Inverted index and Boolean queries |
| **2** | Text encoding: tokenization, stemming, stop words, phrases, Retrieval Models - Boolean, vector space, TF-IDF, Okapi, cosine measure, IR Performance Evaluation - User happiness, precision, recall, F-measure. |
| **3** | Word Embeddings and Applications - Word2Vec, Glove, Concept2Vec, Sentiment and Emotion Analysis in Text - rule based and learning based approaches. Single Document and multi document Summarization. Ontology and applications |
| **4** | Search Engine Architecture - web crawlers, indexing, query processing, retrieval models - ranking algorithm. Link Analysis - Page Rank, Federated Search, Enterprise Search Engines |

**Text Books:**

1. Introduction to Information Retrieval, Christopher D. Manning, PrabhakarRaghavan, HinrichSchütze, 2008
2. Modern Information Retrieval, Baeza-Yates & Ribeiro-Neto, 1999

**References:**

1. Search Engines: Information Retrieval in Practice. Bruce Croft, Donald Metzler, and Trevor Strohman, Pearson Education, 2009.
2. Information Retrieval: Implementing and Evaluating Search Engines. Stefan Buttcher, Charlie Clarke, Gordon Cormack, MIT Press, 2010.

## M3010253 INTERNET OF DRONES

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301253** | **Internet of Drones** | **3-0-0-1** | **2021** |

**Prerequisites:** Prior knowledge of computer networks, cryptography, sensors and basics of computer hardware.

**Course Objectives:**
This course aims to:

1. 1. Give knowledge about the Internet of Drones and the challenges associated.
2. 2. Learn the issues and attacks and their countermeasures in IoD.
3. 3. Give insight into the AI enabled UAV networks and the challenges associated.

**Course Outcomes:**
Upon successful completion of this course, students will be able to:

**C01**: Describe the issues, challenges in IoD.
**C02**:Apply the tools and skills to build secure frameworks for IoD.
**C03**:Demonstrate proficiencies in understanding IoD design with blockchain and AI.
**C04**: Discuss the recent trends in the domain of drone technology and apply their knowledge in research and development.

**Program Learning Outcomes:**
**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written)
**PLO 5** Practice ethical standards of professional conduct and research
**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| **CO1** | 2 | 1 | | 2 | | |
| **CO2** | 2 | 1 | 1 | 1 | | |
| **CO3** | 2 | 2 | 1 | 2 | 1 | |
| **C04** | | 2 | 2 | 2 | 3 | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| 1 | Application Areas, Current Scenario. Drone Subsystems, Classification of Drones, Network Architecture, Components, Layers, Operation Model, Taxonomy of IoD, Communication Protocols, Drones Distribution and Deployment-Related Challenges, Routing, Localization, Energy-Aware Solutions for IoD Networks, Drones And 5G, 6G and Connected Sky, Edge Computing, Drone-Enabled Aerial Computing. Resource Management. |
| **2** | Drone Security: Issues and Challenges, Security Requirements, Classification of Cyber- Attacks and Mitigation Techniques.Behavior and Vulnerability Assessment. Addressing the Privacy Issues. Trust Management. Authentication Techniques. Secure Data Dissemination. Blockchain Based Solutions. Drone Forensics. UAV Network Simulators: AVENS, NS3. |
| **3** | Application of Machine and Deep learning, Lightweight AI Techniques for UAV. Edge AI and IoD. Drone Programming. Drone Data Analytics. Drones as the Internet of Video Things. Internet of Underwater Things. |
| **4** | Ethical Frameworks. Drone Standards. Case study: Early Forest Fire Detection, Pandemic Situation Supervision, Intelligent Delivery Systems, Surveillance and Data Acquisitionetc.Simple Projects. Networking with Drone Startups in India. |

**Books and other resources:**

1. Recent Publications from top-Tier Conferences and Journals
2. Butun I, Sari A, Österberg P. Hardware Security of Fog End-Devices for the Internet of Things. Sensors. 2020 Jan; 20(20):5729.
3. Islam A, Rahim T, Masuduzzaman MD, Shin SY. A Blockchain-Based Artificial Intelligence-Empowered Contagious Pandemic Situation Supervision Scheme Using Internet of Drone Things. IEEE Wireless Communications. 2021 Apr 20.
4. Fadi Al-Turjman, Drones in Smart-Cities: Security and Performance, 978-0-12-819972-5, Elsevier
5. Kinaneva D, Hristov G, Raychev J, Zahariev P. Early forest fire detection using drones and artificial intelligence. In2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) 2019 May 20 (pp. 1060-1065). IEEE.
6. Krishnamurthi, Rajalakshmi, Nayyar, Anand, Hassanien, Aboul Ella (Eds.), Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead, Hardcover ISBN 978-3-030-63338-7, Springer
7. Labrado C, Thapliyal H. Hardware security primitives for vehicles. IEEE Consumer Electronics Magazine. 2019 Oct 31; 8(6):99-103.
8. Lahmeri MA, Kishk MA, Alouini MS. Artificial intelligence for UAV-enabled wireless networks: A survey. IEEE Open Journal of the Communications Society. 2021 Apr 23; 2:1015-40.
9. Prinetto P, Roascio G, Hardware Security, Vulnerabilities, and Attacks: A Comprehensive Taxonomy. InITASEC 2020 Aug 4 (pp. 177-189).
10. Sidhu S, Mohd BJ, Hayajneh T, Hardware security in IoT devices with emphasis on hardware Trojans. Journal of Sensor and Actuator Networks. 2019 Sep; 8(3):42.
11. Wu Y, Dai HN, Wang H, Choo KK. Blockchain-based privacy preservation for 5g-enabled drone communications. IEEE Network. 2021 Feb 16;35(1):50-6.
12. Yahuza M, Idris MY, Ahmedy IB, Wahab AW, Nandy T, Noor NM, Bala A. Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges. IEEE Access. 2021 Apr 9; 9:57243-70.

## M3010223 IOT NETWORKS AND ENDPOINT SECURITY

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301223** | **IoT Networks and Endpoint Security** | **2-2-0-0** | **2021** |

**Prerequisites:** Prior knowledge of distributed systems, computer networks, cryptography, sensor networks and basics of connected systems.

**Course Objectives:**

1. To impart a comprehensive and in-depth understanding of network security, IoT Networks, endpoint security and various security mechanisms.
2. To expose the students to frontier areas of IoT security while providing sufficient foundations for further study and research.

**Course Outcomes:**

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

**C01**: Understand network security threats, security services, and countermeasures.

**C02**: Understand vulnerability analysis and risk mitigation strategies and prepare a sample Vulnerability Assessment Report.

**C03**: Expose students to current literature in IoT networks and endpoint security and understand various security challenges and issues.

**C04**: Complete a term project, including independent research, oral presentation, and programming on latest advancement in the related areas.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written)

**PLO 5** Practice ethical standards of professional conduct and research

**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 1 | 3 | | |
| **CO2** | 3 | 2 | 2 | 2 | 2 | |
| **CO3** | 2 | 2 | 2 | 2 | 2 | |
| **C04** | 2 | 2 | 2 | 3 | 3 | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus: IoT Networks and Endpoint Security**

| **Module** | **Content** |
|---|---|

| | |
|---|---|
| 1 | Overview of TCP/IP, TCP/IP networks, Network Vulnerabilities, Zero-day vulnerabilities, Malwares, Threat and Risk Assessment, Network Vulnerability Assessment, Vulnerability Naming Schemes, Information Infrastructure Defense, Reverse Engineering and Code Obfuscation. Network Access Control. Firewalls. DMZ Network. Router Security. Enterprise Wireless Network Security Protocols. Security in 5G & 6G. Endpoint Devices, Security of Endpoint Devices, Endpoint Device Security Challenges. Case Studies: Cyber Attacks on Critical Infrastructure. |
| **2** | IoT Architecture, Resource Management, Interoperability in IoT, IoT Communication Protocols, Network and Transport Layer Challenges, IoT Threats and Security Challenges, Attacks on Different Layers and Categorization of IoT Attacks, IoT Gateway Security, IoT Routing Attacks, Secure Data Aggregation Mechanisms*, Security Analytics and Threat Prediction*. IoT Endpoint Devices, Threats to IoT Endpoints, General Attacks on IoT Endpoint Devices, IoT Endpoint Security Mechanisms, Security of AIOT Devices. Endpoint Security Best Practices. Case Studies. |
| **3** | Security Frameworks for IoT networks, Intrusion Detection and Prevention, Lightweight Cryptography, Key Management and Authentication, Privacy Enhancing and Anonymization Techniques, Trust and Identity Management, Access Control, IoT Simulators to simulate IoT Networks and Attacks on IoT networks, IoT Operating Systems and Security, IoT Forensics. IoT Security Standards. |
| **4** | Case Studies: Internet of Vehicles (IoV), Unmanned Aerial Vehicle (UAV) Networks, Industrial IoT Networks. Future Research Direction/Opportunity in the IoT Networks and Endpoint Security. |

**Books and other resources:**

1. Recent Publications from top-Tier Conferences and Journals
2. Catherine H. Gebotys, Security in Embedded Devices, ISBN 978-1-4419-1529-0, Springer
3. Chwan-Hwa (John) Wu , J. David Irwin, Introduction to Computer Networks and Cybersecurity, CRC Press, 2013
4. Edward A. Lee and Sanjit A. Seshia, Introduction to Embedded Systems, A Cyber-Physical Systems Approach, Second Edition, MIT Press, ISBN 978-0-262-53381-2, 2017.
5. Fei Hu, Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations, ISBN 9780367574925, 2020, CRC Press
6. Namuduri, K., Chaumette, S., Kim, J., & Sterbenz, J., UAV Networks and Communications. Cambridge University Press, 2017
7. Nishu Gupta, Arun Prakash, Rajeev Tripathi, Internet of Vehicles and its Applications in Autonomous Driving, ISBN 978-3-030-46334-2, 2021, Springer
8. Rajkumar Buyya, Amir Vahid Dastjerdi, Internet of Things Principles and Paradigms, 2016, ISBN 978-0-12-805395-9, Elsevier
9. Rajkumar Buyya, Amir Vahid, Internet of Things Principles and Paradigms, Elsevier, 2016.
10. Rajkumar Buyya, Satish N Srirama, Fog and Edge Computing: Principles and Paradigms, 2019, ISBN: 978-1-119-52498-4, Wiley
11. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson education, 2013.
12. Zaigham Mahmood, Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for the IoV, ISBN 978-3-030-36166-2, Springer.

## M3021112 MACHINE LEARNING

| **Course Code** | **Course Name** | **Credit Split<br>Lecture/Lab/Seminar/Project** | **Year of Introduction** |
|---|---|---|---|
| **M302112** | **Machine Learning** | **3-0-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To impart algorithmic skills needed for designing machine learning techniques and solutions.
2. To equip the students with the ability to identify and analyse problems solvable with machine learning algorithms/techniques.
3. To impart solution design capability with machine learning techniques.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:**Algorithm design/analysis capability in Machine Learning

**CO2**: Problem identification and analysis skills on application domains requiring machine learning techniques

**CO3:** Solution design capability with machine learning techniques

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge.

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature.

**PLO 3** Apply scholarship to conduct independent and innovative research.

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences.

**PLO 5** Practice ethical standards of professional conduct and research.

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | |
| **CO2** | 3 | 3 | 3 | 2 | | |
| **CO3** | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Machine Learning Paradigms: Supervised, Unsupervised and reinforcement Learning. Generalisation performance, Supervised Learning: - Classification - Bayesian, Decision Trees, Artificial Neural Networks, Perceptrons, Multilayer networks, Back-Propagation. |
| **2** | Regression: Linear and Logistic Regression, Feature Engineering - relevance, feature selection, feature extraction - Principal Component Analysis. Unsupervised Learning - Clustering - Partition based (K-means, K-mediods), Hierarchical (BIRCH), and Sub-Space Clustering (CLIQUE). |

| | |
|---|---|
| **3** | Kernel Machines - Support Vector Machines - Concept of Kernels, Kernel Trick, Support Vector Regression, Support Vector Clustering. Scalability of Kernel Machines - Core Vector Machine |
| **4** | Ensemble Learning - AdaBoost and Gradient Boosting, Expectation-Maximization(EM) Algorithm, Sequence Modelling - Hidden Markov Models. Graphical Models - Bayesian Networks. |

**Text Books:**

1. Understanding Machine Learning: From Theory to Algorithms, Shai ShalevShwartz, Shai Ben-David,Cambridge University Press, 2014.
1. Introduction to Machine Learning, Third Edition, Ethem Alpaydin, MIT Press, 2014.

**References:**

1. Neural Networks and Learning Machines, Simon Haykin, Person, 2009.
2. Mastering Machine Learning Algorithms, Giuseppe Bonaccorso, Ingram short title, 2018.
2. Machine learning Hands on for Developers and Technical Professionals, First Edition, Jason Bell, Wiley, 2014.
3. Machine Learning: The Art and Science of Algorithms that Make Sense of Data, First Edition, Peter Flach, Cambridge University Press, 2012.

4. Machine Learning – An Algorithmic Perspective, Second Edition, Stephen Marsland, Chapman and Hall/CRC Machine Learning and Pattern Recognition Series, 2014.

5. Machine Learning, First Edition, Tom M Mitchell, McGraw Hill Education, 2013.

## M3010284, M3020235 MALWARE ANALYSIS AND REVERSE ENGINEERING

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301284,<br>M302235** | **Malware Analysis and Reverse Engineering** | **3-1-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To provide students with a knowledge of various malware types and families.
2. To help the students apply tools and techniques to detect malware.
3. To provide the students with an understanding of the need for protecting computer systems against malware attacks.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:**Analyze Windows, Android,Linux and IoTmalware types and families.<br>
**CO2**: Apply tools and techniques to find out the presence of malware.<br>
**CO3:**Understand how malware evades detection and develop suitable defensive mechanism against malware attacks using machine learning and other techniques.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 1 | 2 | 2 | | | |
| **CO2** | 1 | 3 | | | 3 | |
| **CO3** | 1 | 2 | 2 | | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Android malware analysis: - Introduction to Android malware, Android operating system, Android application components, Android security model, Evolution of Android malware, Android malware types and families, Reverse engineering Android Applications:- Disassembling and Decompiling Android applications, Understanding the source code of Android application, Android security assessment tools. Static Analysis of Android Malware: - Static features for Android malware detection, Permission and Intent analysis, Static API call analysis, Dalvik Opcode analysis. Dynamic Analysis of Android Malware: -Setting up a Sandbox for Android malware analysis, Dynamic analysis of Android malware using API calls, system calls and network packets. Investigating Android malware evasion and current trends in Android malware detection, Investigating Android malware obfuscation, Machine learning for Android malware detection using static and dynamic features. Investigating the effectiveness of deep learning for automated Android malware analysis, Investigating adversarial malware evasion in Android malware detection mechanisms, Investigating adversarial Android malware creation techniques. |
| **2** | Windows malware analysis: - Introduction to Windows Malware, Windows operating system, Windows malware types and families, Reverse engineering Windows Applications: - Disassembling Windows applications, Debugging Windows applications, Decompiling Windows applications, Static analysis of Windows malware: - Analysing Win API and Windows internals. Analysing Windows PE files, Dynamicanalysis of Windows malware: - Setting up a VM for Windows malware analysis, Process monitoring for dynamic analysis of Windows malware, Windowsregistrymonitoring, Windows network protocol analysis. Investigating Windows malware obfuscation, Machine learning for Windows malware detection using static and dynamic features. Investigating the effectiveness of deep learning for detecting malware from raw PE files. Investigating adversarial malware evasion in Windows malware detection mechanisms, Investigating adversarial Windows malware creation techniques. |

| | |
|---|---|
| **3** | Linux malware analysis:- Types of Linux malware, Reverse Engineering Linux malware:- Disassembling and debugging the binaries, Examining the memory snapshots, Abusing macros such as unlink() and frontlink(), Static and Dynamic analysis of Linux malware, Investigating the security of Linux kernel against malware attacks, Machine Learning for linux malware detection, Investigating adversarial malware evasion in Linux malware detection mechanisms,Investigating adversarialLinux malware creation techniques. |
| **4** | IoT malware analysis: -IoT malware types and families, Reverse Engineering IoT malware: - Reverse engineering IoT firmware. IoT implant toolkit for malware implantation, Implantation of Trojans in smart speakers and camera. Static analysis of IoT malware: - Static analysis based on function call graph, strings and elf structure. Dynamic analysis of IoT malware: - Detecting IoT malware using network traffic analysis, IoT botnet detection. Machine learning for IoT malware detection using static and dynamic features,IoT malware obfuscation, Investigating adversarial malware evasion in IoT malware detection mechanisms, Investigating adversarial IoT malware creation techniques. |

**Text Books:**

1. Alexey Kleymenov , AmrThabet , Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoTattacks ,2019.
2. Monappa KA, Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, Packt Publication, 2018.
3. Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein , Adversarial Machine Learning, Cambridge University Press, 2019.
4. Tony Thomas, Athira P. Vijayaraghavan, Sabu Emmanuel, Machine Learning Approaches in Cybersecurity Analytics, Springer 2020.
5. Dunham Ken, Android Malware and Analysis, Auerbach Publications; 1 edition, 2014.

**References:**

1. Clarence Chio, David Freeman, Machine Learning & Security, O Reilly, 2018
2. Xiang Fu, Malware Analysis Tutorials: A Reverse Engineering Approach, Online

## M3010102 MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301102** | **Mathematical Foundation of Computer Science** | **3-0-1-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To provide students with a good understanding of the essential concepts of number theory, algebra, linear algebra, probability, random variables, optimization techniques, graph theory and game theory.

2. To help the students develop the ability to solve problems using the learned concepts.
3. To connect the concepts to various topics in computer science.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Understand the mathematical foundations of computer science, artificial intelligence, cyber security and connected systems.
**CO2**: Analyze and evaluate critically the appropriate mathematical techniques required for solving various computer sciences and engineering problems.
**CO3:** Apply various mathematical techniques in computer science and engineering problems.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 2 | 2 | | |
| **CO2** | 1 | 3 | 3 | 2 | | |
| **CO3** | 1 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Basic Properties of the integers, Divisibility and primality, Congruence, Residue classes, Euler's phi function, Fermat's little theorem<br>Groups, Subgroups, Group homomorphisms and isomorphisms, Cyclic groups, Lagrange's theorem, Field, Galois fields |
| **2** | Matrices, Systems of Linear Equations, Solving Systems of Linear Equations, Eigenvalues and Eigenvectors, Cholesky Decomposition Eigen decomposition and Diagonalization, Singular Value Decomposition<br>Vector Spaces, Basis, Linear Mappings, Inner Products, Orthogonality, Orthonormal Basis, Orthogonal Projections, Cauchy Shwartz inequality, Gram Schmidt Orthogonalization, Norms |
| **3** | Random Variables, Expectation and variance, Distribution Function, Discrete Random Variables, Continuous Random Variables, Mean and Variance, probability distributions: uniform, Bernoulli, binomial, Poisson, Exponential, and Gaussian, multivariate normal distribution, MAP, MLE<br>Graph terminology and special types of graphs, representation of graphs, Graph |

| | |
|---|---|
| | Isomorphism, Connected Graphs, Eulerian and Hamiltonian graphs, trees, weighted trees |
| **4** | Convex sets, convex functions, Linear Optimization, Farkas' lemma, Duality theory, The Simplex method, Convex Optimization, Gradient descent, Non linear optimization, Karush-Kuhn-Tucker conditions, Lagrangian duality<br>Introduction to game theory. Two player games with zero-sum payoffs, Two player games with nonzero-sum payoffs, Nash equilibrium in pure and mixed strategies, basic algorithms to find the Nash equilibrium, dynamic and repeated games, Sequential game. |

**References**

1. I N Herstein, Topics in Algebra, Wiley India, 2nd Edition, 2006
2. Neal Koblitz,. A Course in Number Theory and Cryptography, Springer Verlag (low price edition), 2nd Edition, 1994
3. Kenneth Hoffman, Ray Kunze, Linear Algebra, Prentice-Hall of India Pvt.Ltd
4. Hsu HP. Theory and problems of probability, random variables, and random processes. New York: McGraw-Hill; May 2014.
5. M. Mignotte, Mathematics for computer algebra, Springer-Verlag, 1992.
6. Boyd, S. & Vandenberghe, L. (2004), *Convex Optimization* , Cambridge University Press .
7. Suvrit Sra, Sebastian Nowozin, and Stephen J. Wright. 2011. *Optimization for Machine Learning*. The MIT Press.
8. Bertsimas, D. & Tsitsiklis, J. (1997), Introduction to linear optimization , Athena Scientific .
9. An Introduction to Optimization- E. Chong, S. Zak, Wiley
10. Hastie, T.; Tibshirani, R. & Friedman, J. (2001), *The Elements of Statistical Learning*, Springer New York Inc. , New York, NY, USA .
11. Donald F. Stanat and David F. McAllister, Discrete mathematics in Computer Science.
12. Thomas Koshy, Elementary number theory with Applications, Elsevier
13. G**.** ChartrandandP**.** Zhang**,** Introduction to Graph Theory, McGraw-Hill Companies,
14. Douglas B. West, Introduction to Graph Theory, Prentice Hall of India.
15. N. Nisan, T. Roughgarden, V. Vazirani and E. Tardos, Algorithmic Game Theory, Cambridge University Press, 2007.
16. M. J. Osborne and A. Rubinstein, A Course in Gam Theory, The MIT press, 1994.
17. K. R. Apt and E. Graedel, Lectures in Game Theory for Computer Scientists, Cambridge University Press, 2011.

## M2020101 MATHEMATICS FOR COMPUTER SCIENCE

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M202101** | **Mathematics for Computer Science** | **3-0-1-0** | **2021** |
| **Prerequisites:** Nil | | | |
| **Course Objectives:** | | | |

1. To provide students with a good understanding of the essential concepts of number theory, algebra, linear algebra, probability, random variables, optimization techniques, graph theory.
2. To help the students develop the ability to solve problems using the learned concepts.
3. To connect the concepts to various topics in computer science, cyber security and machine learning.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Understand the mathematical foundations of computer science and cyber security.
**CO2**: Analyze and evaluate critically the appropriate mathematical techniques required for solving various computer sciences and cyber security problems.
**CO3:** Apply various mathematical techniques in computer science, cyber security, and machine learning problems.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 2 | 2 | | |
| **CO2** | 1 | 3 | 3 | 2 | | |
| **CO3** | 1 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Basic Properties of the integers, Divisibility and primality, Congruence, Residue classes, Euler’s phi function, Fermat’s little theorem<br>Groups, Subgroups, Group homomorphisms and isomorphisms, Cyclic groups, Lagrange’s theorem, Field, Galois fields |
| **2** | Matrices, Systems of Linear Equations, Solving Systems of Linear Equations, Eigenvalues and Eigenvectors, Cholesky Decomposition Eigen decomposition and Diagonalization, Singular Value Decomposition<br>Vector Spaces, Basis, Linear Mappings, Inner Products, Orthogonality, Orthonormal Basis, Orthogonal Projections, Cauchy Shwartz inequality, Gram Schmidt Orthogonalization, Norms |

|   |   |
|---|---|
| **3** | Probability, sample space, events, axioms of probability, conditional probability, independent events, Bayes Theorem,<br>Random Variables, Expectation and variance, Distribution Function, Discrete Random Variables, Continuous Random Variables, Mean and Variance, probability distributions: uniform, Bernoulli, binomial,Poisson, Exponential, and Gaussian, MAP, MLE |
| **4** | Graph terminology and special types of graphs, representation of graphs, Graph Isomorphism, Connected Graphs, Eulerian and Hamiltonian graphs,<br>Convex sets, convex functions, Linear Optimization, Farkas' lemma, Duality theory, The Simplex method, Convex Optimization, Gradient descent, Non linearoptimization, Karush-Kuhn-Tucker conditions, Lagrangian duality. |

**References**

1. I N Herstein, Topics in Algebra, Wiley India, 2nd Edition, 2006
2. Neal Koblitz,. A Course in Number Theory and Cryptography, Springer Verlag (low price edition), 2nd Edition, 1994
3. Kenneth Hoffman, Ray Kunze, Linear Algebra, Prentice-Hall of India Pvt.Ltd
4. Hsu HP. Theory and problems of probability, random variables, and random processes. New York: McGraw-Hill; May 2014.
5. M. Mignotte, Mathematics for computer algebra, Springer-Verlag, 1992.
6. Boyd, S. & Vandenberghe, L. (2004), Convex Optimization , Cambridge University Press .
7. Suvrit Sra, Sebastian Nowozin, and Stephen J. Wright. 2011. Optimization for Machine Learning. The MIT Press.
8. Bertsimas, D. & Tsitsiklis, J. (1997), Introduction to linear optimization , Athena Scientific
9. An Introduction to Optimization- E. Chong, S. Zak, Wiley
10. Hastie, T.; Tibshirani, R. & Friedman, J. (2001), The Elements of Statistical Learning, Springer New York Inc. , New York, NY, USA .
11. Donald F. Stanat and David F. McAllister, Discrete mathematics in Computer Science.
12. Thomas Koshy, Elementary number theory with Applications, Elsevier.
13. G**.** ChartrandandP**.** Zhang**,** Introduction to Graph Theory, McGraw-Hill Companies,
14. Douglas B. West, Introduction to Graph Theory, Prentice Hall of India.

## M3020343 MOBILE APPLICATION SECURITY

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M302343** | **Mobile Application Security** | **3-0-0-1** | **2021** |
| **Prerequisites:** Nil | | | |
| **Course Objectives:**<br>• To introduce the security aspects mobile applications<br>• To enable the students to perform static and dynamic analysis of Android applications<br>• To enable the students to perform security analysis of windows and iOS applications | | | |
| **Course Outcomes:** After completion of this course, the students would be able to: | | | |

**CO1:** Describetheneedsand threats of smart phonesecurity
**CO2**: Illustratethearchitecture ofandroidanditssecurity
**CO3:** Analyze the Android virtual device, android memory analysis, and intercepted network traffics
**CO4:** Examine the decompilation of android and iOS applications, recovering java code from apk.
**CO5:** ExplainthearchitectureofiOS,jailbreakingandXcode

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 1 | | | | |
| **CO2** | 2 | 1 | | | | |
| **CO3** | 3 | 3 | 3 | | | |
| **CO4** | 2 | 3 | 3 | | | |
| **CO5** | 3 | 2 | | | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Smartphone operating systems, importance of smartphone security, different types and categories of mobile applications. History of Android, features of Android, architecture of Android, components of Android - activity, service, content provider, broadcast receiver, fragment, intent, resource. |
| **2** | Android security models - app sandboxing, app signing, app permission, data encryption, Securing Android Device.<br>Android SDK -Android SDK tools, Android emulator, Platform tools, Android Debug Bridge (adb), AVD and actual devices, interact with devices, logcat mechanism, Android Studio |
| **3** | Mobile vulnerabilities, methods to avoid the vulnerabilities, Features of Android applications, identification of vulnerable features Android applications, Decompiling Android applications, smali files, recovering java code from APK, Android asset packaging tool, risk in Android applications, risk analysis and classification, tools used in mobile malware analysis, Android malware analysis approaches - static analysis, dynamic analysis, network analysis, hybrid analysis. |
| **4** | iOS Security Model, Security Model of the Windows Phone<br>Architecture of iOS, jailbreaking, Xcode, File system and device interaction, |

|  |  |
|---|---|
|  | decompiling iOS application, Intercepting network traffic. |

**Text Books:**

1. Erik Hellman, “Android Programming: Pushing the Limits”, Wiley 2013.
2. Aditya Gupta, “Learning Pentesting for Android Devices”, Packt Publishing (March 26, 2014)
3. Donny Walls, “Mastering iOS Programming”, Packt Publishing Limited.
4. Kunal Relan, iOS Penetration Testing, APress.

**References:**

1. James Edward Keogh, J2ME The Complete Reference McGraw-Hill/Osborne, 2003.
2. Erik Hellman, Android Programming: Pushing the Limits, Wiley 2013.
3. K. Dunham, Shane Hartman, Manu Quintans, Jose Andre Morales, Tim Strazzere, AndroidMalware and Analysis, CRC Press 2014.
4. Jonathan Zdziarski, Hacking and Securing IOS Applications, O&#39;Reilly Media, Inc. 2012.

## M3022201 MODERN CRYPTOGRAPHY

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M302201 | Modern Cryptography | 3-1-0-0 | 2021 |

**Prerequisites:** A basic understanding of algebra, linear algebra, modular arithmetic

**Course Objectives:**

- Learn modern cryptographic algorithms, their implementations in contemporary computing platforms and security analysis.
- Analyze countermeasures to thwart implementation-level attacks on cryptographic operations in hardware and software
- Identify appropriate cryptographic techniques for real world applications

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Apply appropriate cryptographic techniques to solve real-world problems in information security

**CO2**: Analyze the attack surface of a system in order to realize effective mitigation measures against threats

**CO3:**Exploit cryptography standards to create standards-compliant secure software and hardware systems

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 2 | 2 | 1 | 2 |
| **CO2** | 3 | 3 | 3 | 2 | 1 | 2 |
| **CO3** | 2 | 1 | 1 | 2 | 3 | 3 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Block Ciphers, DES, Triple-DES, AES, Block Cipher Modes, Stream Ciphers, RC4, Hash Functions, SHA-1, SHA3, MAC, HMAC |
| **2** | Public-Key Cryptographic Algorithms, RSA, Rabin, ElGamal, ECC, Lattice Cryptography, Diffie Hellman Key Exchange |
| **3** | Digital Signature Algorithms: RSA, DSA, ECDSA, Dilithium, HSS, XMSS, XMSSMT, |
| **4** | Hash-based deterministic random number generator (DRG.4 acc. AIS 31), True random number generator (PTG.2 acc. AIS 31), protocols like KMIP and API interfaces such as PKC#11, MS CNG, MS CAPI, Java Cryptography Extension (JCE), Microsoft Crypto API (CSP), Cryptography Next Generation (CNG) and SQL Extensible Key Management (SQLEKM), Public Key Infrastructure (PKI) |

**Text Books:**

1. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson
2. Jean-Philippe Aumasson, Serious Cryptography: A Practical Introduction to Modern Encryption, No Starch Press, 2017
3. David Wong, Real-World Cryptography, Manning Publications, July 2021
4. Sunil Cheruvu , Anil Kumar , Ned Smith , David M. Wheeler , Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment , Apress; 1st ed. edition (August 14, 2019)
5. Stefan Rass , Daniel Slamanig , Cryptography for Security and Privacy in Cloud Computing, Artech House (1 November 2013
6. B. Singhal, G. Dhameja, P S Panda, Beginning Block chain, Apress, 2018
7. Narayanan et al., “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,” Princeton University Press, 2016.

**References:**

1. Alko R. Meijer, Algebra for Cryptologists, Springer, 2016
2. Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 2020
3. Thomas R. Shemanske, A Beginner's Guide, Modern Cryptography and Elliptic Curves, American Mathematical Society, 2017
4. B. Rusell and D. Van Duren, “Practical Internet of Things Security,” Packt Publishing, 2016.
5. Johnson Jr, C. Richard, William A. Sethares, and Andrew G. Klein,“Software receiver

design: build your own digital communication system in five easy steps,”Cambridge University Press, 2011

6. A. Antonopoulos, “Mastering Bitcoin: Unlocking Digital Cryptocurrencies,” O’Reilly, 2014.
7. T. Alpcan and T. Basar, “Network Security: A Decision and Game-theoretic Approach,” Cambridge University Press, 2011

## M3010115, M3021373, M3020373 NATURAL LANGUAGE PROCESSING

| **Course Code** | **Course Name** | **Credit Split Lecture/Lab/Seminar/Project** | **Year of Introduction** |
|---|---|---|---|
| **M301115,<br>M302373** | **Natural Language Processing** | **3-0-0-1** | **2021** |

**Prerequisites:** Prior knowledge of Python, Probability and Statistics and Machine Learning

**Course Objectives:**

1. To introduce the fundamental concepts of Natural Language Processing.
2. To impart the principles, concepts and theory behind Language Modeling from an algorithmic point of view.
3. To get insights into the conceptual and application levels of Natural Language Processing.

**Course Outcomes:**

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

- **C01**: understand the fundamental theories and application levels of Natural Language Processing.
- **C02**: Develop language models based on the practical knowledge acquired from the subject area.
- **C03**: Understand the latest advancements and research opportunities within this domain.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written)
**PLO 5** Practice ethical standards of professional conduct and research
**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 1 | 1 | 2 | | |
| **CO2** | 2 | 2 | 2 | 2 | 1 | 1 |
| **CO3** | 2 | 2 | 1 | 2 | 2 | 2 |

(Correlation: 1: Slight (Low)   2: Moderate (Medium)    3: Substantial (High))

**Syllabus:Natural Language Processing**

| **Module** | **Content** |
|---|---|
| 1 | Introduction to Natural Language Processing : History of NLP - Study of Human Languages, The problem of ambiguity and uncertainty in language, Phases of Natural Language analysis – Syntax – Semantics and Pragmatics, Domain-specific NLP Applications.<br>Language Modeling: Defining language models - Corpus, Token, and Lexicon, Probabilistic Language Modeling, n-gram models. Word Level Analysis: Regular Expressions- Finite-State Automata- Morphological Parsing, Syntactic Analysis: Parsing - Constituency Grammar - Dependency Grammar - Context Free Grammar, Semantic Analysis: Elements of Semantic Analysis - Meaning Representation - Lexical Semantics. |
| **2** | NLP using Python**-** Getting started with NLTK, Tokenization, Stemming, Lemmatization, Morphological Segmentation, Chunking, Stop Word Removal, Named Entity Recognition.<br>Parts-of-Speech (POS) Tagging - Rule-based POS Tagging, Stochastic POS Tagging and Transformation-based Tagging, Probabilistic Approaches for POS Tagging- Hidden Markov Model (HMM) - Viterbi algorithm and Conditional Random Fields(CRF), Word Sense Disambiguation(WSD). |
| **3** | Applications of NLP: Information Retrieval, Text Categorization and Summarization, Sentiment Analysis, Topic Modeling- LDA, Machine Translation - Statistical Machine Translation (SMT) - Rule-Based Machine Translation (RBMT) – Hybrid Machine Translation and Neural Machine Translation (NMT), Dealing with Multiliguality, Machine learning of cross-lingual mappings, Learning representations using cross-lingual supervision, Challenges in using NLP with multilingual resources.<br>Spam filtering: Existing NLP models - N-gram modeling- Word Stemming - Bayesian Classification, Statistical Learning Methods, Topic Modeling - Latent Semantic Analysis (LSA) - Overview - Singular Value Decomposition (SVD), Latent Dirichlet Allocation (LDA). |
| **4** | NLP using Deep Learning: Introduction to Word Vectors and Word Senses, Matrix Calculus and Back Propagation, Dependency Parsing, Recurrent Neural Networks and Language Models, Convolutional Neural Networks for NLP, Developing Chatbots, Future of NLP and Deep Learning, Linguistic Theories, Cognitive Modeling and Psycholinguistics. Understanding Application development using NLP - Question Answering, Social Networks, and Agent Communication. |

**Books and other resources:**

1. Recent Publications from top-Tier Conferences and Journals.
2. Emily M. Bender, Linguistic Fundamentals for Natural Language Processing: 100 Essentials from Morphology and Syntax,  ISBN-13 : 978-1627050111, Morgan and Claypool Life Sciences, 2013
3. Grant S. Ingersoll, Thomas S. Morton, Drew Farris, Taming Text: How to Find, Organize, and Manipulate It, ISBN-13 : 978-1491981658, O'Reilly Media; 2017
4. Hobson Lane, Hannes Hapke, Cole Howard, Natural Language Processing in Action:

Understanding, analyzing, and generating text with Python, ISBN-13: 978-1617294631, Manning Publications, 2019.

5. Jacob Eisenstein, Introduction to Natural Language Processing, ISBN-13 : 978-0262042840, The MIT Press, 2019
6. NitinIndurkhya and Fred J. Damerau, Handbook of Natural Language Processing, Second Edition, Taylor and Francis, ISBN-13 : 978-1420085921, 2010
7. Palash Goyal, Sumit Pandey, Karan Jain, Deep Learning for Natural Language Processing-Creating Neural Networks with Python. ISBN-13: 978-1-4842-3684-0, Apress, 2018
8. Rada Mihalcea, Dragomir Radev, Ann Arbor, Graph-based Natural Language Processing and Information Retrieval, Cambridge University Press. doi:10.1017/CBO9780511976247
9. Sowmya Vajjala, Bodhisattwa Majumder, Anuj Gupta, Harshit Surana, Practical Natural Language Processing: A Comprehensive Guide to Building Real-World NLP Systems, ISBN-13 : 978-1492054054, O'Reilly Media,2020
10. Steven Bird, Ewan Klein, and Edward Loper, Natural Language Processing with Python – Analyzing Text with the Natural Language Toolkit, O'Reilly Media, ISBN: 978-0-596-51649-9, 2009.
11. Tomek Strzalkowski, Natural Language Information Retrieval, ISBN 978-90-481-5209-4, Springer.
12. Yoav Goldberg, Graeme Hirst, Neural Network Methods for Natural Language Processing, ISBN-13: 978-1627052986, Morgan and Claypool Life Sciences, 2017.

## M3010254 NETWORK AND SYSTEM SECURITY

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301254** | **Networks and System Security** | **3-0-0-3** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

- To impart a comprehensive and in-depth understanding of computer networks, operating systems, web browsers, mobile platforms, critical infrastructure, and the security issues associated with them
- To enable the students to discover security vulnerabilities and design security mechanism for networks, systems and critical infrastructure.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Discover software bugs that pose cyber security threats, explain and recreate exploits of such bugs in realizing a cyber attack on such software, and explain how to fix the bugs to mitigate such threats

**CO2:** Discover cyber attack scenarios to web browsers, and web servers, explain various possible exploits, recreate cyber attacks on browsers, and servers with existing bugs, and explain how to mitigate such threats

**CO3:** Discover and explain cyber security holes in standard networking protocols, both in network architecture, standard protocols, explain mitigation methods and revisions of standards based on cyber threats.

**CO4:** Discover and explain mobile software bugs posing cyber security threats, explain and recreate exploits, and explain mitigation techniques.

**CO5:** Articulate the urgent need for cyber security in critical computer systems, critical infrastructure, networks, and world wide web, and explain various threat scenarios

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 3 | 2 | 3 | | 2 | |
| CO2 | 3 | 3 | 3 | | 2 | |
| CO3 | 3 | 3 | 3 | | 2 | |
| CO4 | 3 | 3 | 3 | 3 | 2 | 2 |
| CO5 | 3 | 3 | 3 | 3 | | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Network Basics, Network Edge, Network Core, Access Networks, Delay, Loss and Throughput, Protocol Layers and their Service Models, Application Layer, Transport Layer, Network Layer, Internet Protocol (IP), IPV4 & IPv6, Routers, Routing algorithms , Data Link Layer, Error Detection and Correction, Address Resolution Protocol (ARP), Ethernet |
| **2** | Security Issues in TCP/IP, Https, SSL/TLS, IPsec, BGP Security, DNS Cache poisoning etc, Firewalls, Intrusion Detection, Filtering, DNSSec, NSec3, Distributed Firewalls, Intrusion Detection tools, Threat Models, Denial of Service Attacks, DOS-proof network architecture<br>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 |
| **3** | Control hijacking attacks – buffer overflow, integer overflow, bypassing browser memory protection, Tools and techniques for writing robust application software, Security vulnerability detection tools, and techniques – program analysis (static, concolic and dynamic analysis, Privilege, access control, and Operating System Security, Exploitation techniques, and Fuzzing, Hardening, Logging, Virtualization, sandboxing, protection of execution space |

| | |
|---|---|
| **4** | Android vs. ioS security model, threat models, information tracking, rootkits, Threats in mobile applications, security vulnerabilities, viruses, Trojans, spywares, and keyloggers and malware detection<br>Security issues in SCADA, Security in Cyber Physical System Security, Threat models in SCADA and various protection approaches, Machine learning approaches for SCADA Security |

**Text Books:**

1. James Kurose and Keith Ross, Computer Networking: A Top-Down Approach, Pearson
2. Andrew S. Tanenbaum, Computer Networks 5th Edition, Pearson
3. William Stallings, Cryptography and Network Security Principles and Practice, Prentice Hall
4. VlasiosTsiatsis, Stamatis Karnouskos, Jan Holler, David Boyle, Catherine Mulligan, Internet of Things: Technologies and Applications for a New Age of Intelligence. Elsevier Academic press.
5. Zaigham Mahmood, Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for IoV, Springer
6. Ian F. Akyildiz, Mehmet Can Vuran-Wireless Sensor Networks. Wiley.
7. Wenliang Du. Computer Security: A Hands-on Approach, CreateSpace Independent Publishing, 2017. ISBN-13: 978-1548367947
8. Andrew Hoffman, Web Application Security, O'Reilly Media, Inc., 2020
9. Pascal Ackerman, Industrial Cybersecurity: Efficiently secure critical infrastructure systems, Packt Publishing Limited , 2017
10. Tony Thomas, Athira P. Vijayaraghavan, Sabu Emmanuel, Machine Learning Approaches in Cybersecurity Analytics, Springer 2020.

**References:**

1. Peterson L.L, Davie B.S, Computer Networks, A systems approach, 3/E, Harcourt Asia, 2003
2. Keshav S., An Engineering Approach to Computer Networking, Pearson Education, 2000.
3. Shinde S.S, Computer Network, New Age International, 2009
4. Pethuru Raj and Anupama C. Raman, The Internet of Things: Enabling Technologies, Platforms, and Use Cases, CRC Press.
5. Adrian McEwen, Designing the Internet of Things, Wiley, 2013.

## M3020393 OBJECT-ORIENTED ANALYSIS AND DESIGN

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/ Project | Year of Introduction |
|---|---|---|---|
| **M302393** | **Object Oriented Analysis and Design** | **3-0-0-1** | **2021** |
| **Prerequisites:** Nil | | | |
| **Course Objectives:** | | | |

- To teach the concepts of object oriented design
- To enable the students to construct run time architecture of a system using deployment diagrams

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Illustrate the use of UML for object oriented analysis and design
**CO2**: Apply concepts of a system by doing use case analysis.
**CO3:**Sketchinteraction diagrams ofagivensystem
**CO4:** Choose appropriate design elements for architectural analysis.
**CO5:** Construct run time architecture of a system using deployment diagrams.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 1 | | | | |
| **CO2** | 2 | 1 | | 1 | | |
| **CO3** | 3 | 3 | 3 | | | |
| **CO4** | 2 | 3 | 3 | 1 | | |
| **CO5** | 3 | 2 | | | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| 1 | OOSE: Best Practices in Software Engineering, Iterative model, Unified ModelingLanguage<br>ObjectOrientation:ObjectOrientedModeling,IntroductiontoUML,FeaturesofObject Orientation, Abstraction, Encapsulation, Hierarchy, ModularityRelationships: Association, Dependency, Generalization,<br>Multiplicity,Aggregation,Modeling class |
| 2 | OOAD Requirement Analysis: UseCasemodel, Flow of Events, Actors, Analysisand Design Overview, Design MechanismUsecase Analysis: Use case Realization,AnalysisClasses,BoundaryClasses, Control Classes, EntityClasses<br>InteractionDiagrams:SequenceandCollaborationDiagrams,ActivityDiagrams,Activity States, State Chart Diagrams,Synchronization bars, ClassDiagrams,Process and |

|   |   |
|---|---|
|  | Threads |
| 3 | Design Elements:Design classes, Subsystems, Interfaces, Packages, LayeringDesignElements,BusinessandDataLayer,IdentifyDesignMechanism-DesignPattern,Frame works<br>ArchitecturalAnalysis:ArchitectureandDesignImplementation,4+1viewarchitecture ,Concurrency,Synchronization,Collaborations,Componentdiagrams,PLayeredApproach, Architectural Mechanism |
| 4 | RuntimeArchitecture:ConcurrencyMechanism,DistributionofmodelElements,Distribution Patterns, OORDBMS Deployment Diagram: Distribution diagrams,runtimearchitecture,concurrency,configurations,process,nodes,networks, Deploymentdiagrams. |

**Text Books:**

1. GradyBooch,JamesRambaugh,IvarJacobson,TheUnitedModelingLanguageUserGuide- Published byAddison-Wesley, 2005
2. JamesRambaugh et.al., ObjectModelingandDesign PrenticeHall,1991

**References:**

1. MeilierPageJones,FundamentalsofObjectOrientedDesigninUML,PearsonEducation, Asia, 2002
2. Ivar Jacobson,The Road totheUnifiedSoftwareDevelopmentProcess,CambridgeUniversityPress, 2000.

## M2020203 OPERATING SYSTEMS

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/ Project | Year of Introduction |
|---|---|---|---|
| **M202203** | **Operating System** | **3-0-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To help students understand the necessity and fundamental concepts of an Operating System.
2. To explore all the important building blocksin an Operating System.
3. To build practical skills for developing application programming in an Operating System.
4. Explore the different types of Operating Systems in different domains and analyse the security aspects.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:**Analyze various concepts and building blocks associated with Operating System.

**CO2**: Applythe concepts, building blocks, principles and best practicesapplicable to the software development.

**CO3:**Illustrate security aspects in Operating System through its predefined features.

**CO4:**Design application programmingwith multi-processing concepts.

**CO5:**Analyze different types of Operating Systems available and develop applications.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | | | 2 | |
| **CO2** | 2 | 3 | 3 | | 3 | 3 |
| **CO3** | | 3 | | | 3 | 3 |
| **C04** | 2 | 3 | 3 | | 3 | 3 |
| **C05** | 3 | 3 | 3 | | 3 | 3 |

(Correlation: 1: Slight (Low)   2: Moderate (Medium)    3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | OS services, system calls, types, system programs, design and implementation, system structure, debugging, system boot, process concept, IPC(inter process communication), client-server systems, multithreaded programming, symmetric multiprocessing (SMP), process scheduling, Linux Scheduling, Windows Scheduling, Process Migration, Distributed Global States, Distributed Mutual Exclusion, Distributed Deadlock, Linux & Android inter process communication and concurrency mechanisms, scheduling criteria, algorithms, thread scheduling, multiple processor scheduling, exercises<br>Process: process states, process description, process control, synchronization, mutual exclusion, semaphores, synchronization monitors, conditional variables, deadlock. |
| **2** | Contiguous memory allocation, paging, segmentation, virtual memory, demand paging, structure of page table, page replacement, thrashing, exercises<br>File concepts, access methods, file system structure, implementation, mounting, file sharing, allocation methods, free space management, NFS(network file system), disk structure, scheduling, management, swap space management, RAID file systems, I/O systems, distributed file systems, exercises - demand paging, Ext4 |

| | |
|---|---|
| | filesystems.<br>Characteristics of Embedded Systems, Embedded Linux, and Application specific OS. Basic services of NACH Operating System, Principles of protection, domain of protection, access matrix, access control, language based protection, program threats, system and network threats, user authentication, implementing security defenses, firewalling, exercises - man-in-the middle attacks. |
| **3** | FreeRTOS: architecture, distribution, management of heap memory, task, queue, software timer, interrupt, resource management, memory management, task notification, low power support, porting, FreeRTOS+, FreeRTOS Labs, Exercises. |
| **4** | Linux commands, kernel architecture, memory management, virtual process memory, locking, IPC in Linux, system programming with device drivers, kernel modules, kernel threads, virtual file system, extended filesystem, networks, system calls, interrupts, time management,boot methods, SELinux, Raspberry pi, Exercises - Build Linux kernel for Raspberry Pi and board bring up. |

**Text Books:**

1. William Stallings, Operating System: Internals and Design Principles, Prentice Hall, 8th Edition, 2014.
2. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, Operating System Concepts, John Wiley & Sons ,Inc., 9th Edition,2012.
3. Qing Li, Carolyn Yao,Real-Time Concepts for Embedded Systems.
4. Richard Barry, Mastering the FreeRTOS™ Real Time Kernel -A Hands-On Tutorial Guide.
5. Wolfgang Mauerer, Professional Linux® Kernel Architecture.

**References:**

1. Ellen Siever, Stephen Figgins, Robert Love, Arnold Robbins,Linux in a nutshell, Sixth edition.
2. Daniel P. Bovet, Marco Cesati, Understanding the Linux Kernel, 3rd Edition.
3. Frank Mayer, Karl MacMillan, David Caplan**,** SELinux by Example: Using Security Enhanced Linux.

**Web References:**

1. https://freertos.org/FreeRTOS-Plus/index.html
2. http://www.sl2.hu/sexample.pdf
3. https://tldp.org/LDP/lkmpg/2.6/lkmpg.pdf
4. https://www.ibm.com/docs/en/aix/7.2?topic=programming-writing-reentrant-threadsafe-code
5. https://www.omscs-notes.com/operating-systems/distributed-file-systems/
6. https://searchstorage.techtarget.com/definition/RAID
7. https://www.unf.edu/public/cop4610/ree/Notes/PPT/PPT8E/CH15-OS8e.pdf
8. https://people.cs.rutgers.edu/~pxk/416/notes/content/21-crypto-slides.pdf
9. https://www.jigsawacademy.com/blogs/cyber-security/symmetric-and-asymmetric-key-cryptography
10. https://bootlin.com/doc/training/linux-kernel/linux-kernel-slides.pdf
11. http://www.cs.unca.edu/~bruce/Fall14/360/RPiUsersGuide.pdf

12. https://www.raspberrypi.org/help/

## M3020354 OPTIMIZATION TECHNIQUES

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M302354 | Optimization Techniques | 3-0-0-1 | 2021 |

**Prerequisites:** Nil

**Course Objectives:**

- To provide students with a good understanding of the concepts of optimization techniques described in the syllabus.
- To help the students develop the ability to solve problems using the learned concepts.
- To connect the concepts to other domain both within and without theory of optimization techniques such as machine learning and pattern recognition.

**Course Outcomes:** After completion of this course, the students would be able to:
**CO1:**Understand the optimization techniquesproblem and state of the art solutions.
**CO2**: Analyze and evaluate critically the building and integration of optimization techniques.
**CO3:** Design and demonstrate optimization techniques through team research project, and project report, presentation.

**Program Learning Outcomes:**
**PLO 1** Develop strong fundamental disciplinary knowledge.
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature.
**PLO 3** Apply scholarship to conduct independent and innovative research.
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences.
**PLO 5** Practice ethical standards of professional conduct and research.
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | |
| **CO2** | 3 | 3 | 3 | 2 | | |
| **CO3** | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| **1** | Optimization - sequences and limits, derivative matrix, level sets and gradients, Taylor series. |
| **2** | Unconstrained optimization - necessary and sufficient conditions for optima, convex |

| | |
|---|---|
| | sets, convex functions, optima of convex functions, steepest descent, Newton and quasi Newton methods, conjugate direction methods. |
| **3** | Constrained optimization - linear and non-linear constraints, equality and inequality constraints, optimality conditions. |
| **4** | Constrained convex optimization projected gradient methods, penalty methods. |

**Text Books:**

1. E. K. P. Chong and S. H. Zak, An Introduction to Optimization, 2nd Edn., Wiley India Pvt. Ltd., 2010.
2. D. G. Luenberger and Y. Ye, Linear and Nonlinear Programming, 3rd Edn., Springer, 2010.

**References:**

1. Suvrit Sra, Sebastian Nowozin and Stephen J. Wright Optimization for Machine Learning. MIT Press, 2012.
1. Roberto Battiti, Mauro Brunato. The LION Way: Machine Learning plus Intelligent Optimization. Createspace Independent Pub, 2014.

## M1020105  PYTHON FOR DATA SCIENCE

| Course Code | Course Name | Lecture/Lab/Seminar/Project Credits | Year of Introduction |
|---|---|---|---|
| **M102105** | **Python for Data Science** | **3-0-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

- To help students learn the problem-solving techniques.
- To help students understand the fundamental concepts of programming using the Python programming language and introduce the basic concepts of Object-Oriented programming in Python.
- To introduce students to the database concepts and simple data science tools.
- To help students build practical skills for solving problems computationally.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Explain the basic concepts of computational problem solving, and proceduralandobject-oriented programmingparadigms and database programming.
**CO2:**Use algorithms and flowcharts to layout the procedure to solve a problem**.**
**CO3:**Explainthebasicsofpythonsuchasvariables,datatypes,control structures,functions andfilesand apply the knowledge of python to solve computational problems.
**CO4:**Explain coding and analyzing data with Python using tools like Pandas, NumPy, and Matplotlib and understand the basics of cybersecurity data analytics.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants,

entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 3 | | | | | |
| CO2 | 3 | | | | | 1 |
| CO3 | 3 | | | | | |
| CO4 | 3 | | | 2 | | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Computational Problem Solving. Algorithms and Flowcharts, Introduction to Computer Programming. Programming Paradigms and Programming Languages. Introduction to Object Oriented Programming. Introduction to Database Programming and Scripting. Software Development Process. Programming Code of Ethics. Introduction to Python. Real-world Applications of Python. Features of Python Programming Language. Implementations of Python. Python Career Opportunities. |
| **2** | Python Data Types, Variables, Basic Input-Output Operations, Basic Operators. Boolean Values, Conditional Execution, Loops, Lists and List Processing, Logical and Bitwise Operations. Functions, Tuples, Dictionaries, and Data Processing. Modules, Packages, String and List Methods, and Exceptions. |
| **3** | The Object-Oriented Approach: Classes, Methods, Objects, and Exception Handling.A brief introduction to OO Design. File Handling in Python. Introduction to Data Science. Tools for Data Science (GitHub, Jupyter Notebooks).Database Concepts and SQL. SQL using Python. |
| **4** | Data Handling using NumPy and Pandas. Data Visualization in Python. Simple projects. Case studies. |

**Text Books:**

1. Charles Dierbach, “Introduction to Computer Science Using Python: A Computational Problem-Solving Focus”, Wiley, 2017.
2. Ashok NamdevKamthane, Amit Ashok Kamthane, “Programming and Problem Solving with Python”, McGraw Hill Education, 2018.
3. Steven F. Lott, “Object Oriented Python”, Packt Publishing.
4. Wes McKinney, Python for Data Analysis: Data Wrangling with Pandas, NumPy, and IPython, ISBN-13: 978-1449319793, O'Reilly Media.

**References:**

1. Reema Thareja, “Python Programming using Problem Solving Approach”, Oxford Higher Education, 2017.
2. Bradley N. Miller, David L. Ranum Problem Solving with Algorithms and Data Structures Using Python, Franklin, Beedle& Associates, 2011.
3. David D. Riley, Kenny A. Hunt, “Computational Thinking for the Modern Problem Solver”, CRC Press, 2014.
4. Jake VanderPlas, Python Data Science Handbook, Github
5. Fabio Nelli, Python Data Analytics: With Pandas, NumPy, and Matplotlib 2nd Edition, Kindle Edition.

# M3010234, M3020383 QUANTUM COMPUTING & CRYPTOGRAPHY

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/ Project | Year of Introduction |
|---|---|---|---|
| **M301234, M302383** | **Quantum Computing and Cryptography** | **3-0-1-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To provide students with a good understanding of the concepts of quantum mechanics, quantum computing, quantum machine learning, and quantum cryptography described in the syllabus.
2. To help the students develop the ability to solve problems using the learned concepts.
3. To connect the concepts to other domain both within such as machine learning, pattern recognition and cryptography.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Apply the concepts of quantum computing for solving computational problems.
**CO2**: Analyze the use of quantum algorithms for machine learning problems.
**CO3:** Applying quantum cryptography for securing data and communication.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

|  | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 3 | 2 | 3 | 2 | 2 | 2 |
| CO2 | 3 | 3 | 3 | 2 | 2 |  |
| CO3 | 2 | 3 | 3 | 2 | 2 | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| 1 | Elements of quantum mechanics, States and Superposition, Uncertainty Relations, Tunneling, Adiabatic Theorem, No-Cloning Theorem, Hilbert space, Unitary and |

| | |
|---|---|
| | stochastic dynamics, Density Matrix Representation and Mixed States, Probabilities and measurements, Composite Systems and Entanglement, Density operators and correlations, Classical Computation Models and Quantum Gates |
| 2 | Quantum bits – qubits, Combining qubits using the tensor product, Measuring qubits, Performing operations on qubits, Classical gates versus quantum gates, Quantum Circuit, Quantum No Cloning Theorem and Teleportation ,The Bloch Sphere representation,Adiabatic Quantum Computing, Deutsch's Algorithm, Deutsch-Jozsa Algorithm, Simon's periodicity algorithm, Grover's search algorithm, Shor's Factoring algorithm |
| 3 | Quantum Computing in Clustering, Quantum Principal Component Analysis, Quantum K-Means,Quantum K-Medians, Quantum Hierarchical Clustering, Quantum Neural Networks, Quantum Pattern Recognition,Quantum Associative Memory, Quantum Perceptron, Quantum Neural Networks, Quantum Classification, Support Vector Machines with Grover's Search, |
| 4 | Key distribution with a limited Eve and perfect Bob , Key distribution with noise on the channel , Quantum key distribution, BB84 Protocol, Purifying protocols using entanglement, Security from a guessing game, Authentication, Device-independent quantum cryptography Security from quantum uncertainty, Quantum computing in the cloud, Sharing a quantum secret, Secure computations on a remote quantum computer, Practical realization of a quantum computer |

**Text Books:**

1. M. A. Nielsen and I. L. Chuang. Quantum Computation and Quantum Information , Cambridge University Press, 2000
2. Mikio Nakahara and Tetsuo Ohmi,"Quantum Computing", CRC Press (2008).
3. Michele Mosca, An Introduction to Quantum. Computing, Oxford U. Press, New York, 2007.
4. Peter Wittek, Quantum Machine Learning, Academic Press; Reprint edition, 2016

**References:**

1. M. Le Bellac , A Short Introduction to Quantum Information and Quantum Computation", Cambridge University Press, 2006
2. P. Kaye, R. Laflamme, and M. Mosca. An Introduction to Quantum Computing. Oxford, 2007.
3. Peres, Asher, Quantum Theory: Concepts and Methods. New York, NY: Springer, 1993. ISBN: 9780792325499.
4. Presskil Lecture notes. Available online: http://www.theory.caltech.edu/~preskill/ph229/.
5. N. David Mermin, Quantum Computer Science, Cambridge University Press 2007

## M3010215, M3020363 SECURE SOFTWARE ENGINEERING

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/ Project | Year of Introduction |
|---|---|---|---|
| M301215,<br>M302363 | Secure Software Engineering | 3-0-0-1 | 2021 |

**Prerequisites:** Nil

**Course Objectives:**

1. To help students understand the necessity of security in software development
2. To introduce the fundamental concepts and methods of Secure Software Development.
3. To build practical skills for developing and testing secure software.
4. Explore the different software vulnerabilities and attack patterns to handle the recent problems in this domain.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:**Analyze various security problems associated with software

**CO2**: Apply secure software engineering concepts, principles and best practicesapplicable to the software industry.

**CO3:**Illustrate security risks in software's through code reviews andsoftware tools.

**CO4:**Design software solutions with appropriate security engineering

**CO5:**Analyze security vulnerabilities of software's and applications and model defensive countermeasures.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

|  | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 3 | 3 |  |  | 2 |  |
| CO2 | 2 | 3 | 3 |  | 3 | 3 |
| CO3 |  | 3 |  |  | 3 | 3 |
| C04 | 2 | 3 | 3 |  | 3 | 3 |
| C05 | 3 | 3 | 3 |  | 3 | 3 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | The security problem, The Trinity of Trouble, Security problems in software, The problem with application security, Three pillars of software security, Core and influential properties of secure software, Software security roles, Influencing the security properties of software - defensive and attackers perspective, Attack patterns, Leveraging attack patterns in requirements, design, implementation and testing, Security assurance case, The heartbleed bug and attack, Android security bulletin. |
| 2 | Secure SSDLC overview, Risk management framework, Seven touch points for software security, Requirement engineering for secure software, Misuse and Abuse cases, SQUARE process model, Secure software architecture and design, Architectural risk analysis methodologies, Threat modeling - STRIDE, CVSS, Common software code vulnerabilities, Source code review, Coding practises, Software security testing - risk-based testing, penetration testing, Applying RMF on KillerAppCo's iWare 1.0 Server, Model a threat using OWASP Threat Dragon tool, The OWASP top security risks, Tailored threat modeling for the automotive industry – HEAVENS. |
| 3 | Secure coding guidelines, Stack and heap-based buffer overflow, Strings, Pointer subterfuge, Dynamic memory management, Integer security, Formatted output, Concurrency, FileIOWeb security - Cross-site scripting attack, Network security - TCP protocol attack, OS security - Secure boot, KASLR, SELinux, Familiarization of software security attacks - Shellshock attack, Return-to-libc attack, Dirty COW attack. |
| 4 | Graphical representation of programs - CFG, PDG, Call graphs, CPG, Static Analysis, Dynamic analysis,Tracing, Slicing,Code Coverage, Statement coverage, Branch coverage, Condition coverage, Path coverage, Secure programming tools - Splint, Valgrind, SecureUML and UMLSec, Vulnerability analysis on OWASP 1.1 and construct CFG, Vulnerability of the day, Build It- Break It-Fix It, Vulnerability analysis using deep neural networks. |

**Text Books:**

1. Gary McGraw, Software Security: Building Security In, Addison-Wesley Professional, 2006
2. Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, Software Security Engineering, Addison-Wesley Professional, 2008
3. Robert C. Seacord, Secure Coding in C and C++,SEI Series in Software Engineering, 2005
4. Helfrich, James N, Security for software engineers, Chapman & Hall/CRC, 2019
5. Ari Takanen, Charles Miller, and Jared D Demott, Fuzzing for Software Security Testing and Quality Assurance, Artech House 2018

**References:**

1. Wenliang Du, Computer Security: A Hands-on Approach, 2017.
2. C. Warren Axelrod, Engineering safe and secure software systems, Artech House, 2012
3. Nhlabatsi, A., Bandara, A., Hayashi, S., Haley, C., Jurjens, J., Kaiya, H., ...& Yu, Y. (2011). Security patterns: Comparing modeling approaches. In Software engineering

for secure systems: Industrial and research perspectives (pp. 75-111). IGI Global.

4. Yamaguchi, F., Golde, N., Arp, D., & Rieck, K. (2014, May). Modeling and discovering vulnerabilities with code property graphs. In 2014 IEEE Symposium on Security and Privacy (pp. 590-604). IEEE.
5. LaToza, T. D., & Myers, B. A. (2011, September). Visualizing call graphs. In 2011 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC) (pp. 117-124). IEEE.
6. Abadi, M., Budiu, M., Erlingsson, U., & Ligatti, J. (2009). Control-flow integrity principles, implementations, and applications. ACM Transactions on Information and System Security (TISSEC), 13(1), 1-40.
7. Fairley, R. E. (1978). Tutorial: Static analysis and dynamic testing of computer software. Computer, 11(4), 14-23.
8. Nethercote, N., & Seward, J. (2007). Valgrind: a framework for heavyweight dynamic binary instrumentation. ACM Sigplan notices, 42(6), 89-100.
9. Ruef, A., Hicks, M., Parker, J., Levin, D., Mazurek, M. L., & Mardziel, P. (2016, October). Build it, break it, fix it: Contesting secure development. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 690-703).

**Web References:**

1. https://heartbleed.com/
2. https://source.android.com/security/bulletin
3. https://owasp.org/www-community/Vulnerability_Scanning_Tool
4. https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot
5. https://lwn.net/Articles/569635/
6. https://source.android.com/security/selinux
7. http://www.cs.umd.edu/~nelson/classes/resources/cdebugging/
8. https://splint.org/
9. https://splint.org/manual/manual.html
10. https://www.valgrind.org/docs/manual/manual-core.html/
11. https://autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf
12. https://owasp.org/www-project-threat-dragon/

## M3010145, M3020304 SECURITY IN DIGITAL TRANSFORMATION

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/ Project | Year of Introduction |
|---|---|---|---|
| **M301145, M302304** | **Security in Digital Transformation** | **3-0-0-1** | **2021** |
| **Prerequisites:** Nil | | | |
| **Course Objectives:**<br>1. To provide students with a good understanding of the requirements of cyber security in digital transformation.<br>2. To help the students to develop security solutions in digital transformation using the learned concepts | | | |

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Apply the cyber security concepts in various digital transformation domains.

**CO2**: Understand the requirement of security in various domains such as IoT, connected vehicles,5G, AI, and automation

**CO3:** Complete a term project, including independent research, oral presentation, and programming on a latest advancement in digital transformation.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | 3 |
| **CO2** | 3 | 3 | 3 | 2 | | 3 |
| **CO3** | 2 | 3 | 3 | 2 | 3 | 3 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| 1 | AI powered automation and security, big data analytics, data highways,challenges related to data security, the volume of data, data explosion, unstructured data, data integration,Risks of switching database models, Outsourcing data control, auditing big data, AI-based monitoring of business processes, hyper automation, cognitive automation, AI-driven biometric security solutions, automated machine learning, explainable and conversational AI, RPA, AI-driven automation, AIOps (artificial intelligence for IT operations), confluence of AI and IoT. |
| 2 | Hybrid and multi cloud in digital transformation, Cloud Storage security: Limited control of third-party services, Exposing data to public, on-cloud data auditing, Exploitable Application programming interfaces, managing operational risks leveraging automation testing, UI and UX modernization, DevOps, APIs, and Microservices, AI in cloud, Serverless computing, containers, and kubernetes, As-A-Service Revolution, XaaS. |
| 3 | Automation In ERP, Robotic Process Automation (RPA), GPS tracking, RFID |

| | |
|---|---|
| | technology, robotics, Drones, and Vehicle Automation, Extended Reality (XR),<br>Mobile security: Resource-limited security mechanisms: Varied use cases of mobile attacks, Platform obscurity, Diverse set of testing configurations, Attacks through varied Communication channels.<br>Security in IoT: Cross-layer security approaches, Flexible system architecture, Hardware-based versus software-based security solutions. |
| 4 | 5G and enhanced connectivity: connected vehicles, smartphones, streaming, and entertainment, elevated user experiences, remote working setup, video conferencing, and digital collaborations across domains, WiFi 6.<br>Private, public, and hybrid block chains, Block chain with AI. |

**References:**

1. William Stallings, 5G Wireless: A Comprehensive Introduction, Addison-Wesley Professional; 1st edition (24 July 2021)
2. Shaoliang Peng, Blockchain for Big Data: AI, IoT and Cloud Perspectives, CRC Press; 1st edition (30 August 2021)
3. Parikshit N. Mahalle et al., The Convergence of Internet of Things and Cloud for Smart Computing, CRC Press; 1st edition (3 August 2021)
4. Sunil Cheruvu, Anil Kumar, Ned Smith, David M. Wheeler, Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment
5. Hanky Sjafrie, Introduction to Self-Driving Vehicle Technology, Chapman and Hall/CRC; 1st edition (11 December 2019)

## M3010262 SOCIAL NETWORK ANALYTICS AND SECURITY

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301262** | **Social Network Analytics and Security** | **3-0-0-1** | **2021** |

**Prerequisites:** Prior knowledge of Computer Networks, Natural Language Processing (NLP), DBMS, Graph Theory and Machine Learning

**Course Objectives:**

1. To impart a comprehensive and in-depth understanding of the basics of social networks, research challenges and social media analytics to M.Tech students by researching and providing insights into the cutting-edge topics, technologies, applications and implementations.
2. To expose the students to the frontier areas of social networks along with providing sufficient foundations for further study and research.

**Course Outcomes:**

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

**C01**: Summarize social network concepts and security issues and apply basic principles behind network analysis algorithms to develop practical skills of network analysis

**C02**: Summarize human cognition and social networks and analyse the techniques used for behaviour analysis in social networks

**C03**: Apply mechanisms on how big data technologies, machine and deep learning algorithms are employed in social networks

**C04**: Understand how the social technologies impact society and vice versa and examine the ethical and legal implications of leveraging social media data

**C05**:Complete a term project, including independent research, oral presentation, and programming on a latest advancement in the related areas.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written)

**PLO 5** Practice ethical standards of professional conduct and research

**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 1 | 1 | 1 | | |
| **CO2** | 2 | 2 | 2 | 2 | 2 | 1 |
| **CO3** | 2 | 2 | 1 | 2 | | |
| **C04** | 1 | 2 | 2 | 2 | 2 | 2 |
| **C05** | 2 | 2 | 2 | 2 | 2 | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| 1 | Online Social Networks- Introduction, Types of networks, Properties of nodes and networks, Social Network Analysis: Graph Structure of Social Networks, Centrality Measures- Degree, Closeness, Betweenness, Eigenvector centrality, Idea of small worlds, Networks and Groups- Identifying actors, Activating and mobilizing ties, Understanding how people form communities. System Architectures of OSN- Client Server, P2P. |
| **2** | Privacy and Security in Social Networks: Security Threats- Malware attacks, Sybil attacks, Phishing in OSN, Fake Profiles, Social Engineering Attacks, Information Leakage, Dark Web and Social Media. Social Network Analysis and its applications – Influence Maximization-How Information is being created and distributed, Information diffusion among people in a network, How Online Social Networks are formed and evolve over time, Visualizing complex relationships, Identifying powerful and influential participants, Community Detection, Link Prediction. Big Data Analytics and Deep Learning for Social Network Security. |
| **3** | Data extraction from Online Social Media, APIs, Modeling and Visualizing Social Network graphs - Tools- Gephi, Graphviz, and NodeXL. Dataset Collection for Social Media Analytics – Visualizing data using Ne04j. Challenges in collecting social media data.<br>Research in Social Networks: Design of novel algorithms for analyzing social networks, Improving the performance of information sharing in social networks. Rumor Detection, Semantic Analysis, Online Sentiment Analysis- opinion mining, feature based sentiment |

| | |
|---|---|
| | analysis, Trust, credibility, and reputations in social systems. Emerging Areas in OSN: Decentralized Social Networks- When Blockchain meets social networks, Mobile Social Networks, Social Internet of Things (SIoT), Internet of Behavior (IoB) and Social Networks, Cognitive and AI in Social Network Security. |
| **4** | Human Cognition and Social Networks: Human Social Networks and ego networks, Analysis of ego networks in online social networks, Applying structural knowledge to Online Social Networking services.<br>User Behavior Analysis in Social Networks: Psychology of social media users, Personality theories and User Behavior Prediction – Five Factor Theory- TPB-MBTI, Relationships between Personality and Interactions in social networks, Cognitive Psychology and Social Network Usage. |

**Books and other resources:**

1. Recent Publications from top-Tier Conferences and Journals
2. Social Media Security - Leveraging Social Networking While Mitigating Risk-1st Edition, Michael Cross. eBook ISBN: 9781597499873.
3. Kazienko, Przemyslaw, Chawla, Nitesh (Eds.) Applications of Social Media and Social Network Analysis, Springer, 2015. eBook ISBN: 978-3-319-19003-7.
4. Stanley Wasserman; Katherine Faust, Social network analysis: methods and applications, Cambridge; New York: Cambridge University Press, 1994.
5. Federico Alberto Pozzi ElisabettaFersini Enza Messina Bing Liu,Sentiment Analysis in Social Networks, 1st Edition - Elsevier,2016. eBook ISBN: 9780128044384.
6. Valerio Arnaboldi, Andrea Passarella, Marco Conti, Robin I. M. Dunbar, Online Social Networks: Human Cognitive Constraints in Facebook and Twitter Personal Graphs Elsevier - 1st Edition. eBook ISBN: 9780128030424.
7. Derek Hansen, Ben Shneiderman, and Marc A. Smith, Analyzing Social Media Networks with NodeXL: Insights from a Connected World.
8. Missaoui, Rokia, Sarr, Idrissa (Eds.), Social Network Analysis - Community Detection and Evolution, Springer, 2014.
9. Missaoui, Rokia, Abdessalem, Talel, Latapy, Matthieu (Eds.), Trends in Social Network Analysis - Information Propagation, User Behavior Modeling, Forecasting, and Vulnerability Assessment, Springer, 2017.

## M3010105, M3020314 SOFT COMPUTING

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301105,<br>M302314** | **Soft Computing** | **3-0-0-1** | **2021** |
| **Prerequisites:** Nil | | | |
| **Course Objectives:** | | | |

1. To impart algorithmic skills needed for designing soft computing techniques and solutions.
2. To equip the students with the ability to identify and analyse problems solvable with soft computing techniques.
3. To impart solution design capability with soft computing techniques.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:**Algorithm design/analysis capability in Soft Computing

**CO2**: Problem identification and analysis skills on application domains requiring soft computing techniques

**CO3:** Solution design capability with soft computing techniques

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 1 | 1 | 2 |
| **CO2** | 3 | 2 | 3 | 1 | 1 | 2 |
| **CO3** | 3 | 3 | 3 | 2 | 1 | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Difference between Soft and Hard computing, Overview of different components of soft computing techniques - Fuzzy Logic, Rough Logic, ANNs, Genetic Algorithms, Swarm Intelligence |
| **2** | Introduction to Fuzzy logic, Fuzzy membership functions, Operations on Fuzzy sets, Fuzzy relations, Fuzzy propositions, Fuzzy implications, Fuzzy inferences, De-fuzzyfication, Fuzzy logic controller. |

| | |
|---|---|
| **3** | Genetic algorithms basic concepts, encoding, fitness function, Parent Selection - Roulette wheel, Rank, Tournament, Mutation and Crossover operators, Convergence of GA, Applications of GA, Case studies. |
| **4** | Swarm Intelligence - agent systems, social agents, Particle Swarm Optimisation - path planning applications, Ant Colony Optimisation - solving travelling sales man problem with ACO, introduction to Artificial Immune Systems |

**Text Books:**

1. R. Rajasekaran and G. A and Vijayalakshmi Pa, Neural Networks, Fuzzy Logic, and Genetic Algorithms: Synthesis and Applications, Prentice Hall of India, 2011
2. T. Ross, Fuzzy Logic with Engineering Applications, Tata McGraw Hill, 1997
3. Swarm Intelligence Algorithms, Adam Slowik, CRC press, 2020

**References:**

1. D. E. Goldberg, Genetic Algorithms in Search, Optimisation, and Machine Learning, Addison-Wesley, 1989
2. Swarm Intelligence: From Natural to Artificial Systems by Eric Bonabeau, Marco Dorigo and Guy Theraulaz, Oxford University Press, 1999
3. Rough Sets: Mathematical Foundations, Lech Polkowski, Physica-Verlag Heidelberg, 2002

## M3010243 SOFTWARE DEFINED NETWORKING

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301243** | **Software Defined Networking** | **3-0-0-1** | **2021** |

**Prerequisites:** Basic knowledge in computer networks, operating systems, distributed systems, machine learning and programming in Python.

**Course Objectives:**

1. To instill a thorough and in-depth understanding of SDN fundamentals, technologies, and applications through the introduction and investigation of cutting-edge topics, technologies, applications, and implementations.
2. To expose students to cutting-edge research in SDN and NFS while providing sufficient foundation for further study and research.

**Course Outcomes:**

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

**C01**: Analyze the evolution of SDNs, express the various components of SDN and their uses, explain the use of SDN in the current networking scenario and develop various applications.
**C02**: Describe Network Functions Virtualization and investigate emerging SDN models and security aspects of SDN and NFV.
**C03**: Complete paper reviews, oral presentations, and a final course project.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written)

**PLO 5** Practice ethical standards of professional conduct and research

**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 1 | | 1 | | |
| **CO2** | 2 | 2 | 1 | 2 | | |
| **CO3** | 1 | 2 | 1 | 2 | 1 | 1 |

(Correlation: 1: Slight (Low)   2: Moderate (Medium)   3: Substantial (High))

**Syllabus:** Software Defined Networking

| **Module** | |
|---|---|
| I | Networking Basics - Switching, Addressing, Routing, The history of SDN, SDN Architecture, Data, Control, and Management Planes, Distributed Control Planes, Centralized Control Planes, Hardware Lookup, Forwarding Rules, Dynamic Forwarding Tables, Autonomous Switches and Routers, Network Automation and Virtualization, SDN Network Updates, SDN Scalability, SDN Applications. |
| **II** | OpenFlow: Switch-Controller Interaction, Flow Table, Packet Matching, Actions and Packet Forwarding, Extensions and Limitations, Mininet: A simulation environment for SDN; White-box Switching, Open Sourcing SDN, Open Networking Foundation, OpenDaylight, ONOS, OpenStack, OpenSwitch; Programming Languages, Verification Techniques, Debugging Tools for SDN, Virtual appliances on SDN, Virtualization and SDN. |
| **III** | Emerging SDN Models: Protocol Models: NETCONF, BGP, MPLS; Controller Models; Application Models: Proactive, Declarative, External; SDN in Datacenters: Multitenancy, Failure Recovery; SDN in Internet eXchange Points (IXPs); SDN-Powered Mobile Edge Computing, IoT–SDN.<br>Network Function Virtualization (NFV): Introduction to Network Functions, SDN vs. NFV, NFV Reference Architecture, OPNFV, Inline Network Functions, Service Creation and Chaining, NFV Orchestration, Network Slicing, Developing Virtual Network Functions, Deploying Virtualized Network Functions. |
| **IV** | Security Threats and Vulnerabilities Introduced by NFV and SDN, Threat Detection and Mitigation through SDN and NFV;, Authentication, Authorization, and Access Control (AAA), Anomaly Detection and Prevention Mechanisms, Intrusion Detection and Prevention Systems, Security of applying SDN to Wireless and Mobile Networks, Security of applying NFV and SDN to IoT and Cloud/Edge Computing, Security of SDN API, Security Architecture for SDN, Security of SDN Data Plane, Control Plane and Application Plane, Security of Routing in SDN, Security of Network Slicing, Security as a Service for SDN, Machine and Deep Learning for SDN Security, Secure SDN with Blockchain. |

**Books and other resources:**

1. Recent Publications from top-Tier Conferences and Journals
2. Paul Goransson and Chuck Black, Software Defined Networks: A Comprehensive Approach, Morgan Kaufmann Publications, 2017
3. Thomas D. Nadeau & Ken Gray, SDN - Software Defined Networks, O'Reilly, 2013
4. K. Gray and T. D. Nadeau. Network Function Virtualization. Morgan Kaufmann, ISBN: 978-0-12-802119-4, 2016.
5. Shao Ying Zhu, Sandra Scott-Hayward, Ludovic Jacquin, Richard Hill, Guide to Security in SDN and NFV: Challenges, Opportunities, and Applications, Springer, 2017, ISBN-13 : 978-3319646527
6. Dijiang Huang, Ankur Chowdhary, Sandeep Pisharody, Software-Defined Networking and Security from Theory to Practice, ISBN 9780367780647, CRC Press, 2021.
7. Jason Gooley, Dana Yanch, Dustin Schuemann, John Curran, Cisco Software-Defined Wide Area Networks: Designing, Deploying and Securing Your Next Generation WAN with Cisco SD-WAN, ISBN-13: 978-0-13-653317-7, 2020, Cisco Press.

## M3010272 SPEECH PROCESSING

| **Course Code** | **Course Name** | **Credit Split Lecture/Lab/Seminar/Project** | **Year of Introduction** |
|---|---|---|---|
| **M301272** | **Speech Processing** | **3-0-0-1** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To provide students with a good understanding of the concepts of speech processing tasks described in the syllabus.
2. To help the students develop the ability to solve problems using the learned concepts.
3. To connect the concepts to other domain both within and without mathematics such asmachine learning and pattern recognition.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:**Understand the foundations of modern speech processing theory, problem and state of the art solutions.

**CO2**: Analyze and evaluate critically the building and integration of speech signal processing algorithms and systems.

**CO3:** Design and demonstrate a working speech signal processing system through team research project, and project report, presentation.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | |
| **CO2** | 3 | 3 | 3 | 2 | | |
| **CO3** | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| **1** | The human vocal and auditory systems. Characteristics of speech signals: phonemes, prosody, IPA notation. Lossless tube model of speech production. Time and frequency domain representations of speech; window characteristics and time/frequency resolution tradeoffs. Properties of digital filters: mean log response, resonance gain and bandwidth relations, bandwidth expansion transformation, all-pass filter characteristics. |
| **2** | Autocorrelation and covariance linear prediction of speech; optimality criteria in time and frequency domains; alternate LPC parametrisation. Speech coding: PCM, ADPCM, CELP. Speech synthesis: language processing, prosody, diphone and formant synthesis; time domain pitch and speech modification. |
| **3** | Speech recognition: hidden Markov models and associated recognition and training algorithms. Language modelling. Large vocabulary recognition. Acoustic preprocessing for speech recognition. |
| **4** | Speech Processing: Spectral and non-spectral analysis techniques, Model- based coding techniques, Noise reduction and echo cancellation, Synthetic and coded speech quality assessment. Selection of recognition unit, Model-based recognition, Language modeling, Speaker Identification, Text analysis and text-to-speech synthesis. |

**Text Books:**

1. Lawrence Rabiner and Ronald Schafer. 2010. Theory and Applications of Digital Speech Processing (1st. ed.). Prentice Hall Press, USA.
2. Ben Gold, Nelson Morgan, and Dan Ellis. 2011. Speech and Audio Signal Processing: Processing and Perception of Speech and Music (2nd. ed.). Wiley-Interscience, USA.

**References:**

1. O'Shaughnessy, D. (1987). Speech Communication: Human and Machine. Addison-Wesley.
2. Tokunbo Ogunfunmi, Roberto Togneri, and Madihally (Sim) , Narasimha. 2014. Speech and Audio Processing for Coding, Enhancement and Recognition. Springer Publishing Company, Incorporated
3. Benesty, J.; Sondhi, M. M. & Huang, Y., ed. (2008), *Springer Handbook of*

*Speech Processing* , Springer , Berlin.

## M3010292 STOCHASTIC PROCESSES AND MODELS

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M301292 | **Stochastic Processes and Models** | **3-0-0-1** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

- To provide students with a good understanding of the concepts of information theoretic methods, stochastic processes and models described in the syllabus.
- To help the students develop the ability to solve problems using the learned concepts.
- To connect the concepts to other domain both within and without mathematics such as pattern recognition.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:**Understand the foundations of modern stochastic models theory, problem and state of the art solutions.

**CO2**: Analyze and evaluate critically the building and integration of stochastic models algorithms and systems.

**CO3:** Design and demonstrate a working stochastic models system through team research project, and project report, presentation.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | |
| **CO2** | 3 | 3 | 3 | 2 | | |
| **CO3** | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|

| | |
|---|---|
| **1** | Introduction to Probability Theory: sample space, events, Algebra of sets, Notion and Axioms of probability, Equally Likely events, Conditional probability, independent events, concepts of random variables, PMF, PDFs, CDFs, Expectation. Concepts of joint and multiple random variables, joint, conditional and marginal distributions. Correlation and independence. |
| **2** | Bayesian belief networks (BBN): Representation, Independence and conditional independence, Partial independence and other structure. Exact inference in BBN: Variable elimination, Pearl's algorithm, Junction tree, Recursive decomposition, Using additional structure. |
| **3** | Approximate inference: Monte Carlo approximations, Loopy belief propagation, Variational methods. Learning of BBNs: learning parameters, learning structure, Bayesian averaging, EM (learning with hidden variables and missing values), structural EM |
| **4** | Dynamic belief networks: Particle filtering. Markov random fields (Markov networks):Representation (potentials), Independence and conditional independence, Trees, Boltzman machines, Conditional Markov random fields. Inference in Markov networks. Learning Markov networks: Iterative proportional fitting, Cluster variational methods, Other approximations. Relational graphical models |

**Text Books:**

1. Hsu HP. Theory and problems of probability, random variables, and random processes. New York: McGraw-Hill; May 2014.
2. Leon-Garcia, Probability, Statistics, and Random Processes for Electrical Engineering, Third Edition, Prentice-Hall, 2008.
3. Koller D. and Friedman, N., Probabilistic Graphical Models: Principles and Techniques , The MIT Press (2009).
4. Barber, D., Bayesian Reasoning and Machine Learning , Cambridge Univ. Press (2012).

**References:**

1. Feller W. An introduction to probability theory and its applications. John Wiley & Sons; 2008.
2. A. Papoulis, Probability, Random Variables, and Stochastic Processes, Mc-Graw Hill, 2005.
3. David J.C. Mackay. Information theory, inference, and learning algorithms. Cambridge, UK:Cambridge University Press.
4. Judea Pearl. Probabilistic Reasoning in Intelligent Systems. Morgan Kaufman.

## M3010273 UBIQUITOUS COMPUTING

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M301273 | Ubiquitous Computing | 3-0-0-1 | 2021 |

**Prerequisites:** Basic knowledge in computer networks, operating systems, distributed systems, computer vision

**Course Objectives:**

1. To impart fundamental concepts in the areas of wireless networks and mobile computing.
2. To introduce advanced topics in wireless networks and mobile computing.

**Course Outcomes:**

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

**C01**: Understand the general principles of Ubiquitous Computing and the key technical and social factors driving the change towards modern ubiquitous systems.
**CO2**: Understand different approaches used in Ubiquitous Computing and evaluate their applicability in specific application scenarios.
**C03**: Complete application development, paper reviews, oral presentations, and a final course project.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written)
**PLO 5** Practice ethical standards of professional conduct and research
**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 1 | | 1 | | |
| **CO2** | 2 | 2 | 1 | 2 | | |
| **CO3** | 2 | 2 | 1 | 2 | | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:** Ubiquitous Computing

| **Module** | **Content** |
|---|---|
| I | Introduction to Ubiquitous and Pervasive Computing, Ubiquitous Computing Examples, Research Opportunities, Impact of Ubiquitous Computing, Architecture for Ubiquitous Computing, Sensors, Ambient Displays, Tangibles, Middleware, Wireless Standards&Protocols for Ubiquitous Networks, Personal Assistants, Location Aware Computing, Location Tracking, Architecture, Location Based Service and Applications, Location Based Social Networks (LBSN), LBSN Recommendation. |
| **II** | Integrating the Physical and the Virtual Worlds: Sensing and Actuation; Awareness and Perception, Urban Sensing and Mobile Crowdsensing, Participatory and Social Sensing, Crowd Sourcing Platforms and Applications, Internet of Things and Ubiquitous Sensing, Social Network Applications, Context and Location Aware Applications and Services, Ubiquitous Data Access, Context-aware Computing, Issues and Challenges, Mobility, and Location and Context Awareness, Context Prediction, Developing Context-aware Applications. |

| | |
|---|---|
| **III** | Energy Constraints in Ubiquitous Computing, Wearable Computing, Body Area Networks, Privacy and Security in Ubiquitous Computing, Sensor Cloud, Mixed Reality, Contact-free Sensing, Glass and Augmented Reality, Eye-Tracking, Digital Pen and Paper, Mobile Social Networking, Event Based Social Network, Mobile P2P Computing, AI and Big Data Analytics in Ubiquitous Computing. |
| **IV** | Illustration of Some Existing Application Domains for Ubiquitous Computing in such areas as Gaming, Workplaces, Domestic Spaces, Museums and Educational Communities. Adaptive Human Activity and Behaviour Recognition Models, Pervasive Healthcare, Urban Computing and Reality Mining, Ambient Assisted Living, Cyber-Physical Social Systems, Mobile HCI, Internet of Thinking. |

**Books and other resources:**

1. Recent Publications from top-Tier Conferences and Journals
2. A. Genco and S. Sorce, Pervasive Systems and Ubiquitous Computing, ISBN: 978-1-84564-482-6, 2010, WIT Press
3. Aline Godfroid, Eye Tracking in Second Language Acquisition and Bilingualism: A Research Synthesis and Methodological Guide, 2020 ISBN 9781138024670, Routledge
4. Conklin, K., Pellicer-Sánchez, A., & Carrol, G. (2018). Eye-Tracking: A Guide for Applied Linguistics Research. Cambridge: Cambridge University Press, ISBN: 9781108401203
5. Cristian Borcea, Manoop Talasila, Reza Curtmola, Mobile Crowdsensing, ISBN 9780367658304, 2020.
6. Jon Peddie, Augmented Reality: Where We Will All Live, 2017, Springer International Publishing, ISBN 978-3-319-54501-1
7. Laurence T. Yang, Evi Syukur, Seng W. Loke, Handbook on Mobile and Ubiquitous Computing Status and Perspective, 2016, ISBN 9781138198593, CRC Press.
8. Mohammad S. Obaidat, Mieso Denko, Isaac Woungang, Pervasive Computing and Networking, 2011, ISBN: 978-0-470-74772-8, Wiley
9. Samuel Greengard, Virtual Reality, The MIT Press, 2019, ISBN-13 : 978-0262537520
10. Saravanan, P. Shanthi and S. R. Balasundaram. Privacy and Security Challenges in Location Aware Computing. IGI Global, 2021, ISBN13: 9781799877561
11. Stefan Poslad, Ubiquitous Computing: Smart Devices, Environments and Interactions, ISBN:9780470035603, 2009, John Wiley & Sons
12. Tom Lovett, Eamonn O'Neill, Mobile Context Awareness, 2012, Springer-Verlag London, ISBN 978-0-85729-624-5
13. Ubiquitous Computing Fundamentals, John Krumm, CRC Press, 2018
14. Yun Fu, Human Activity Recognition and Prediction, 2016, Springer International Publishing, ISBN 978-3-319-27002-9
15. Zaigham Mahmood, Guide to Ambient Intelligence in the IoT Environment: Principles, Technologies and Applications, 2019, Springer International Publishing, ISBN 978-3-030-04172-4

## M3010244 VIDEO ANALYTICS

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301244** | **Video Analytics** | **3-0-0-1** | **2021** |

**Prerequisites:** Introduction to Signal and Image Processing, Basic proficiency in Python, Introduction to Machine Learning and Deep Learning, Introduction to Networks and Wireless Sensor Networks.

**Course Objectives:**

1. To introduce the basics of video analytics and its applications
2. To develop an awareness about the algorithms and deep learning architectures for video analytics
3. To provide an understanding of recent advancements in video analytics
4. To design and evaluate complex video analytics systems with design decisions and empirical evidence.

**Course Outcomes:**

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

**CO1**: Understand the fundamentals of video processing and familiarize motion-based algorithms and python libraries for segmentation, object recognition, and tracking.
**CO2**: Gain knowledge about the deep learning models for video analytics.
**CO3**: Identify recent developments in real-time video analytics; design and analyze algorithms for real-world problems.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written)
**PLO 5** Practice ethical standards of professional conduct and research
**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 1 | | 1 | | |
| **CO2** | 3 | 2 | 1 | 2 | | |
| **CO3** | 1 | 2 | 2 | 2 | | 2 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:** Video Analytics

| **Module** | **Content** |
|---|---|
| I | Introduction - Image Processing/Computer Vision, Video Processing- Basics of Video-Time-Varying Image Formation Models, Spatio-Temporal Sampling, Sampling Structure Conversion, Three-Dimensional Motion Estimation and Segmentation, Methods Using Point Correspondences, Optical Flow and Direct Methods, Motion Segmentation, Stereo and Motion Tracking, Background Modeling, Local Features, Object Detection and Recognition, Programming Image and Video Analysis Methods in Python + Associated Libraries, OpenCV and Keras. |
| **II** | Segmentation, Kalman, Particle Filter based tracking, Multi-target/Multi- |

| | |
|---|---|
| | camera tracking, Motion Estimation, Action Recognition, Demonizing, Image and Video enhancement, Image and Video compression, Privacy-preserving Techniques for Video Processing, Stereo and Mono Depth Estimation, Decision Trees/Random Forest, Deep Learning for Intelligent Video Analytics--CNN, GAN, Autoencoder, LSTM-Object Detection-Transfer Learning-Multiple Objects Tracking. Open Source Models-Luminoth, Detectron2, YOLO. |
| **III** | Video Analytics Measuring Accuracy/Accuracy Issues, Architecture, Hardware, Video Analytics Demographics (Age, Clothing, Emotion, Gender, Race), Digital Video Security, Networks and Networked Video, Wireless Networked Video, Video Analytics in WSN, IoT Video Analytics Architectures, Edge Intelligence for Video Analytics, Autonomous Real-Time on-Board Video Analytics, Live Video Analytics with FPGA-based Smart Cameras. |
| **IV** | Case Study: Face Detection and Recognition, Natural Scene Videos, Video Surveillance: Crowd Analysis, Traffic Monitoring, Intelligent Transport System; Remote Sensing, Robotics, Healthcare, Live Video Analytics for Drones, Social Media Video Analytics and Metrics. |

**Books and other resources:**

1. Recent Publications from top-Tier Conferences and Journals.
2. Debjyoti Paul, Charan Puvvala, Video Analytics Using Deep Learning: Building Applications with TensorFlow, Keras, and YOLO, 1st Edition, 2020.
3. Murat Tekalp, Digital Video Processing, Prentice Hall Signal Processing Series, 2nd Edition, 2015.
4. IPVM, Video Analytics Book 2021.
5. Richard Szeliski, Computer Vision: Algorithms and Applications, Springer, 2011.
6. Jayavardhana Gubbia, Rajkumar Buyya, Slaven Marusic , Marimuthu Palaniswami., Internet of Things (IoT): A vision, architectural elements, and future directions", Journal Future Generation Computer Systems, Elsevier, 2013.
7. Ching-Tang Fan, Yuan-Kai Wang and Cai-Ren Huang, Heterogeneous Information Fusion and Visualization for a Large-Scale Intelligent Video Surveillance System, IEEE Transactions On Systems, Man, And Cybernetics: Systems, Vol. 47, No. 4, April 2017.
8. Caifeng Shan, Fatih Porikli, Tao Xiang, Shaogang Gong, Video Analytics for Business Intelligence, Springer, 2012.
9. Asier Perallos, Unai Hernandez-Jayo, Enrique Onieva, Ignacio Julio García Zuazola, Intelligent Transport Systems: Technologies and Applications, Wiley, 2015.
10. Plamen Angelov ,Pouria Sadeghi-Tehran, Christopher Clarke, AURORA: Autonomous Real-time On-board Video Analytics, Springer, 2017.

## M3020324 WEB TECHNOLOGY

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M302324** | **Web Technology** | **3-0-0-1** | **2021** |
| **Prerequisites: Nil** | | | |

**Course Objectives:**

1. To help students understand the web application fundamentals.

2. To explore the architecture and design principles of web based applications.

3. To understand the most suitable application stack for a requirement and its implementation.

4. To explore a few related concepts like Microservices, common web application security issues, REST API

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Understand the web technology fundamentals
**CO2**: Develop web application using MEAN and MERN stack
**CO3:** Analyze and evaluate critically the building and integration of different web technology stacks
**CO4:** Develop web applications without known/published security risks and issues

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 3 | 1 | 2 | 2 | | |
| CO2 | 3 | 2 | 3 | 2 | 1 | |
| CO3 | 3 | 3 | 1 | 2 | 1 | |
| CO4 | 3 | 3 | 2 | | 2 | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Fundamentals of TCP/IP protocol, Stateless protocol, HTTP, HTTPS, Web servers, Web server architecture, Application Server, Request/response paradigm, The structure of HTTP messages, Request methods, HTTP Header structure, Status codes. Characteristics of Modern Web Applications, HTML Responsive Web Design, HTML5 |

| | |
|---|---|
| | Elements, Attributes and elements, Type of Style sheets: Internal Style Sheet, Inline Style sheet, External Style Sheet, CSS3 Elements and features, CSS frameworks, Content delivery network, Selectors, XML Schema, Presenting XML Using XML Processors: DOM and SAX. |
| **2** | Introduction to Java Script, Object in JavaScript, Dynamic HTML with Java Script, JavaScript Object Notation, JSON vs XML, JSON Parsing, Data types, Arrays, Decisions and Loops, Functions and scope, JavaScript libraries, JavaScript Frameworks, ECMAScript, TypeScript, Single page applications (SPA),Cookies, Sessions management, Cleint side processing. The Web Services based on technologies such as SOAP, REST, WSDL, Django Framework: Architecture, MVT Architecture Pattern in Django Structure |
| **3** | Basics of angular Framework, Basics of React Web Framework, Nodejs and Expressframework, Introduction to MongoDB, Sample MERN Stack application, Sample MEAN stack application, Node js design patterns – Singleton, Factory, Builder, Prototype, |
| **4** | Data Visualization Techniques for small and large data, OWASP Top Ten Web Application Security Risks, Fundamentals of web application architecture (1Tier, 2-Tier,3-Tier, N Tier and MVC) and components, User interface app components, Structural components, Microservices, Monolithic vs. Microservices |

**TeText Books:**

1. Jeffrey C. Jackson, Web Technologies - A Computer Science Perspective, Pearson Education – 2009.
2. Amos Q. Haviv,Adrian Mejia,Robert Onodi - Web Application Development with MEAN
3. Vasan Subramanian - Pro MERN Stack: Full Stack Web App Development with Mongo, Express, React, and Node 2nd ed. Edition
4. Joseph B. Mille, Internet Technologies and Information Services, ABC-CLIO - 2014.
5. Jim Morrish , Rishi M. Bhatnagar, Enterprise IoT: Strategies and Best Practices for Connected Products and Services - Dirk Slama, Frank Puhlmann , O-Reilly Media (2015).

**References:**

1. Leon Shklar, Richard Rosen , Web Application Architecture - Principles, Protocols and Practices, Wiley – 2009.
2. Laura Lemay, Rafe Colburn, Jennifer Kyrnin, Mastering HTML, CSS &Javascript Web Publishing Paperback 2016.
3. Giacomo Veneri Antonio Capasso, Hands-On Industrial Internet of Things Paperback, Packt Books 2018.
4. Pabbathi, Quick Start Guide to Industry 4.0: One-stop reference guide for Industry 4.0, 2018.

## M3010204 WIRELESS NETWORKS AND MOBILE COMPUTING

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M301204** | **Wireless Networks and Mobile Computing** | **3-0-0-1** | **2021** |
| **Prerequisites:** Basic knowledge in computer networking and digital communications, Programming in Python | | | |
| | | | |

**Course Objectives:**

1. To impart fundamental concepts in the areas of wireless networks and mobile computing.
2. To introduce advanced topics in wireless networks and mobile computing.

**Course Outcomes:**

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

**CO1**: Understand the fundamentals of wireless networks and mobile computing.
**CO2**: Understand the selected recent paradigm-shifting concepts being developed in the research community.
**CO3**: Complete written paper reviews, an oral paper presentation, and a final course project.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written)
**PLO 5** Practice ethical standards of professional conduct and research
**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 1 | | 1 | | |
| **CO2** | 2 | 2 | 1 | 2 | | |
| **CO3** | 2 | 2 | 1 | 2 | | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus: Wireless Networks and Mobile Computing**

| **Module** | **Content** |
|---|---|
| I | 802.11 Wireless LANs, Personal Area Networks: Bluetooth and Zigbee, Near Field Communication (NFC), Cellular Internet Access: 3G, 4G, & 5G; Mobile IP, Location and Handoff Management, Routing, Wireless Multicasting, Topology Control in Wireless, Traffic and Congestion Control, Resource Management, Energy-efficient Protocols for Wireless Networks, Smart Antennas, MIMO and OFDM Based PHY Layer Technologies, Mobility and QoS Management, Policy Based Management in Wireless LANS, 6G, 7G and 8G |
| **II** | Voice-Oriented Wireless Networks, Data-Oriented Wireless Networks, Mobile Ad Hoc Networks and Multi-Hop Wireless, Ultra-wideband and Short-Range Networks, High Altitude Platforms and Satellites, Emergency Wireless Communications, Wireless Real-Time Communications, RFID systems, Service Discovery in Mobile Environments, On-demand Mobility, Cross-layer Design and Optimization, Opportunistic Networks, Wireless Mesh Networks, Delay Tolerant Networks, Wireless Access Networks, Space Networks, Virtualization in Wireless Networks, Software Defined Wireless Networks, Big Data and Mobile Networks, Energy-aware in Mobile Networks; Cellular Cognitive Networks, Cooperative and Cognitive Vehicular Networks, Drone networking, Connected and |

| | |
|---|---|
| | Autonomous Cars. |
| **III** | Indoor and Outdoor Localization, Smartphone Localization, WiFi Fingerprinting, Non-WiFi Localization, Device-Free Sensing with Radio Frequency, Next Generation (5G) Wireless Technologies, Upper Gigahertz and Terahertz Wireless Communications, Millimeter Wave Networking, Visible Light Communication, Sensing Through Visible Light, Visible Light Indoor Localization and Positioning, Indoor and Outdoor Navigation, Machine Learning in Mobile Computing. |
| **IV** | Security in Wireless LANs, Security in Cellular Networks, Bluetooth Security, Mobile Security, Threat and Vulnerability Management, Ad hoc Network Security, Authentication Protocols, Identity Management, Cross-layer Design Security, Cryptographic Algorithms and Applications, Key Distribution and Management; Intrusion Detection and Prevention, Network Security Protocol Design, Physical Layer Security, Security and Privacy of Location-based Services, Trust Management. |

**Books and other resources:**

1. Recent Publications from top-Tier Conferences and Journals
2. Andre Perez, Mobile Networks Architecture, 2012, Wiley, ISBN: 9781848213333
3. D. P. Agrawal and Qing-An Zeng, Introduction to Wireless & Mobile Systems, 4th Ed., Cengage Learning, 2014.
4. Georgios Kambourakis, Félix Gómez Mármol, Guojun Wang, Security and Privacy in Wireless and Mobile Networks, ISBN 978-3-03842-780-3, 2018, MDPI
5. Gerardus Blokdyk, Mobile Network A Complete Guide, 2021, ISBN-13 : 978-1867402572, 5STARCooks
6. Guowang Miao, Fundamentals of Mobile Data Networks, Cambridge University Press, 2016, ISBN-13 : 978-1107143210
7. Haesik Kim, Design and Optimization for 5G Wireless Communications, 2020, ISBN:9781119494553, John Wiley & Sons Ltd
8. James F. Kurose, Keith W. Ross, Computer Networking A Top-Down Approach, Pearson
9. Jonathan Rodriguez, Fundamentals of 5G Mobile Networks, ISBN: 9781118867525, 2015, Wiley
10. Khaldoun Al Agha Guy Pujolle Tara Ali-Yahiya, Mobile and Wireless Networks, 2016, ISBN: 9781848217140, Wiley.
11. Lin, Yi-Bing, Wireless and Mobile All-IP Networks, 2005, ISBN 0471749222, John Wiley & Sons
12. Sherine Mohamed Abd El-Kaderand Hanan Hussein, Fundamental and Supportive Technologies for 5G Mobile Networks, 2019, ISBN13: 9781799811527, IGI Global
13. Steve Rackley, Wireless Networking Technology from Principles to Successful Implementation, ISBN 13: 978-0-7506-6788-3, Elsevier
14. Yan Zhang, Honglin Hu, Masayuki Fujise, Resource, Mobility, and Security Management in Wireless Networks and Mobile Communications, 2006, ISBN 9780849380365, Auerbach Publications
15. Yan Zhang, Jijun Luo, Honglin Hu, Wireless Mesh Networking: Architectures, Protocols and Standards, 2006, ISBN 9780849373992, Auerbach Publications.
16. Zabih Ghassemlooy, Luis Nero Alves, Stanislav Zvanovec, Mohammad-Ali Khalighi, Visible Light Communications Theory and Applications, 2017, ISBN 9780367878108, CRC Press.

## M3010214 WIRELESS SENSOR NETWORKS

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M301214 | Wireless Sensor Networks | 3-0-0-1 | 2021 |

**Prerequisites:** Prior knowledge of operating systems, computer networks, distributed systems, DBMS, Graph Theory.

**Course Objectives:**

1. To understand the fundamentals of wireless sensor networks and their application to real-world scenarios.
2. To investigate the various protocols at various layers and their differences with traditional protocols.
3. To understand the issues pertaining to sensor networks and the challenges involved in managing a sensor network.
4. To introduce students to cutting-edge areas of wireless sensor networks while providing foundations for further study and research.

**Course Outcomes:**

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

**CO1**: Understand the basis of sensor networks, sensor node hardware and software, architecture and placement strategies of sensors, analyze routing and congestion algorithms.
**CO2**: Explore and implement solutions to real world problems using sensor networks.
**CO3**: Expose students to current literature in wireless sensor networks and related areas.
**CO4**: Complete a term project, including independent research, oral presentation, and programming on a latest advancement in Wireless Sensor Networks.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written)
**PLO 5** Practice ethical standards of professional conduct and research
**PLO 6** Acquire professional skills such as collaborative skills and write articles for scholarly journals.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 3 | 2 | 1 | 1 | | |
| CO2 | 3 | 2 | 2 | 2 | | |
| CO3 | 2 | 2 | 2 | 2 | | |
| C04 | 2 | 2 | 2 | 3 | 2 | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus: Wireless Sensor Networks**

| Module | Content |
|---|---|
| 1 | Introduction to Wireless Sensor Networks: Motivations, Application domains of sensor networks, Design Challenges. Operational and Computational Models, Performance metrics, Network Architecture: Traditional Layered Stack, Cross-Layer Designs, Sensor Network Architecture. Single-Node Architecture. Sensor node hardware: mica2, micaZ, telosB, cricket, Imote2, tmote, btnode; Sensor Node Software (Operating System): tiny0S, MANTIS, Contiki, and Ret0S. Introduction to Simulation tools- TOSSIM, OPNET, NS2, NS3, Description of the NS-3 core module and simulation examples and projects. |
| 2 | Middleware for WSN, Protocol Stack in WSN, Medium Access Control in WSN, MAC Protocols, Node Discovery Protocols, Network Clustering, Introduction to Markov Chain: Discrete time Markov Chain definition, Properties, Classification and Analysis; MAC Protocol Analysis; Programming in WSNs, Programming Tools: C, nesC. Challenges and Limitations of Programming WSNs. |
| 3 | Robust Route Setup, Routing Protocols for WSN, Coping with energy constraints, Clustering in WSNs, QoS Management, Topology Management. Network Bootstrapping: Sensor deployment mechanisms, Issues of Coverage. Localization Schemes. Fault Tolerance. Mobile WSN, Synchronization, Congestion and Flow Control; Sensor Data Storage, Retrieval, Processing. Sensor Fusion and Aggregation: Sensor Fusion Paradigms, Probabilistic, Dempster-Shafer Based, Centralized and Distributed Kalman filter, Q-digest. Compressive Sensing and Data Gathering in WSN. |
| 4 | Underwater Acoustic Sensor Networks: Issues and Challenges, Simulation Tools, Application Areas. Body Area Sensor Networks. IoT-Enabled Sensor Networks. Sensor Cloud. Sensor Networks and Edge Computing. Security, Trust and Privacy. Key Management. Real Life Deployment of WSN and Underwater Sensor Networks. |

**Books and other resources:**

1. Recent Publications from top-Tier Conferences and Journals
2. Aggeliki Prayati, Problem Solving for Wireless Sensor Networks, ISBN:9781848002036, 2008, Springer London
3. Agus Kurniawan, Practical Contiki-NG: Programming for Wireless Sensor Networks, ISBN:9781484234082, 2018, APress
4. Anna Forster, Introduction to Wireless Sensor Networks, ISBN:9781119079958, 2016, Wiley
5. Anna Hac, Wireless Sensor Network Designs, ISBN-13 : 978-0470867365, John Wiley & Sons, December 2003.
6. Edgar H. Callaway, Jr. and Edgar H. Callaway, Wireless Sensor Networks: Architectures and Protocols, ISBN 9780849318238, CRC Press, August 2003.
7. Holger Karl and Andreas Willig, Protocols and Architectures for Wireless Sensor Networks, ISBN-13: 978-0470519233, Wiley-Interscience, 2007.
8. Hossam Mahmoud Ahmad Fahmy, Wireless Sensor Networks: Concepts, Applications, Experimentation and Analysis, ISBN: 9789811004124, 2021, Springer Singapore.
9. Ibrahiem M. M. El Emary, S. Ramakrishnan, Wireless Sensor Networks: From Theory to Applications, ISBN 9781138198821, CRC Press, 2016.
10. Jun Zheng, Abbas Jamalipour, Wireless Sensor Networks: A Networking Perspective, Wiley-IEEE Press, 2009, ISBN: 0470167637.

11. Kazem Sohraby, Daniel Minoli, Taieb Znati, Wireless Sensor Networks: Technology, Protocols, and Applications, John Wiley & Sons, ISBN 978-0-471-74300-2, 2007
12. Mauro Conti, Secure Wireless Sensor Networks: Threats and Solutions, ISBN:9781493934607, 2015, Springer New York
13. Mohammad Matin, Wireless Sensor Networks - Technology and Protocols, ISBN 978-953-51-0676-0, InTech, 2012.
14. Shuang-Hua Yang, Wireless Sensor Networks: Principles, Design and Applications, ISBN:9781447155058, 2013, Springer London
15. Waltenegus Dargie, Christian Poellabauer, Fundamentals of Wireless Sensor Networks: Theory and Practice, Wiley, ISBN: 978-0-470-99765-9, July 2010

# Laboratory Courses

## M3021316 BIG DATA TECHNOLOGIES LAB

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M302316 | Big Data Technologies Lab | 0-1-0-0 | 2021 |

**Prerequisites:** Nil

**Course Objectives:**

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Use MapReduce and Hadoop
**CO2:** Analyze and process bigdata using Apache Spark
**CO3:** Develop methods to work with big data
**CO4:** Apply machine learning with pySpark

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 2 | 1 | 2 | 1 |
| **CO2** | 3 | 2 | 1 | 1 | 1 | 1 |
| **CO3** | 3 | 3 | 1 | 1 | 1 | 2 |
| **CO4** | 3 | 3 | 2 | 1 | 2 | 1 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| 1 | Hadoop Hands-on<br>Getting Started with MapReduce and Hadoop<br>MapReduce Exercises |
| 2 | HDFS Introduction<br>Hbase/Cassandra HandsOn [ NoSQL] |
| 3 | Working with Large data sets |
| 4 | Working with pySpark<br>Machine Learning with pySpark |

**Text Books:**

1. Data Analytics with Spark Using Python, By Jeffrey Aven, Addison Weley Data & Analytics series, 2018
2. Big Data Analytics with Spark, Mohammed Guller, APress, 2015
3. Hadoop: The Definitive Guide, Tom White, 3rdedition, O'Reilly Media , 2012.
4. Beautiful Data, Toby Segaran, Jeff Hammerbacher, O'Reilly Media, 2009.

**References:**

1. Mining of Massive Datasets, Anand Rajaraman, Jeffrey D Ullman. Cambridge University Press 2010

## M3022207 CYBER ANALYTICS LAB

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M302207** | **Cyber Analytics Lab** | **0-1-0-0** | **2021** |

**Prerequisites:**

- Nil

**Course Objectives:**

1. To introduce basic machine learning techniques.
2. To develop the skills in using recent machine learning software/tools for solving
3. cyber security problems
4. To develop the skills in applying appropriate supervised, semi-supervised or
5. unsupervised learning algorithms for solving practical cyber security problems.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1**: Identify appropriate machine learning techniques for cyber security analytics.

**CO2**: Apply recent machine learning software/tools for solving cyber security problems

**CO3**: Apply appropriate supervised, semi-supervised or unsupervised learning algorithms for solving practical cyber security problems.

**Program Learning Outcomes:**

**PLO 1**: Develop strong fundamental disciplinary knowledge

**PLO 2**:Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3**: Apply scholarship to conduct independent and innovative research

**PLO 4**: Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5**: Practice ethical standards of professional conduct and research;

**PLO 6**: Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 2 | | | |
| **CO2** | 3 | 3 | 3 | | 3 | |
| **CO3** | 3 | 3 | 3 | | 3 | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | 1. Familiarize with Python Libraries- Numpy, Pandas, Matplotlib, Scikit<br>2. Familiarize with Scikit-Learn, Keras, and TensorFlow<br>3. Perform Data exploration and preprocessing in Python |
| **2** | 1. Implement regularised Linear regression<br>2. Implement Naive Bayes classifier for dataset stored as CSV file.<br>3. Implement regularized logistic regression<br>4. Apply these techniques to various cyber security datasets |
| **3** | 1. Build models using different Ensembling techniques<br>2. Build models using Decision trees<br>3. Build model using SVM with different kernels<br>4. Apply these techniques to various cyber security datasets |
| **4** | 1. Implement K-NN algorithm to classify a dataset.<br>2. Build model to perform Clustering using K-means after applying PCA and determining the value of K using Elbow method.<br>3. Implement CNN for image classification<br>4. Apply these techniques to various cyber security datasets |

**References**

1. Cybersecurity Analytics, Rakesh M. Verma, David J. Marchette, Chapman and Hall/CRC, 2019
2. Tony Thomas, Athira P. Vijayaraghavan, Sabu Emmanuel, Machine Learning Approaches in Cybersecurity Analytics, Springer 2020
3. Clarence Chio, David Freeman, Machine Learning & Security, O Reilly, 2018
4. Mark Stamp, Introduction to Machine Learning with Applications in Information Security, CRC Press, 2018
5. D K Bhattacharyya, J K Kalita, Network Anomaly Detection, A machine Learning Perspective, CRC Press, 2014Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts By AurélienGéron, "O'Reilly Media, Inc.", 2019
6. P.-N. Tang, M. Steinbach, and V. Kumar: Introduction to Data Mining, Addison Wesley, 2006
7. Jiawei Han and MichelineKamber, Data Mining: Concepts and Techniques, Morgan Kaufman Publishers, Third Edition, 2011.
8. A Practical Approach for Machine Learning and Deep Learning Algorithms by Abhishek Kumar Pandey, Pramod Singh Rathore, S Balamurugan, BPB Publications, 2019
9. Soma Halder, Sinan Ozdemir , Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem, Packt Publishing (December 31, 2018)

## M3022106 CYBER SECURITY AND FORENSICS LAB

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introducti on |
|---|---|---|---|
| M302106 | Cyber Security and Forensics Lab | 0-1-0-0 | 2021 |

**Prerequisites:**
Nil

**Course Objectives:**

1. Perform various cyber security attacks
2. Test tools to detect and prevent cyber attacks
3. Perform digital forensic investigations using various tools

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1** Simulate cyber attacks/crimes and cyber security mechanisms.

**CO2**: Perform digital forensics analysis on OS, memory, networks and network devices etc.

**CO3**: Utilize various cyber security and forensic tools to understand cyber attacks and collect digital evidence.

**Program Learning Outcomes:**

**PLO 1**: Develop strong fundamental disciplinary knowledge

**PLO 2**:Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3**: Apply scholarship to conduct independent and innovative research

**PLO 4**: Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5**: Practice ethical standards of professional conduct and research;

**PLO 6**: Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 2 | | | |
| **CO2** | 3 | 3 | 3 | | 3 | |
| **CO3** | 3 | 3 | 3 | | 3 | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| Module | Content |
|---|---|
| **1** | Testing strengths of passwords using password cracking tools, Monitoring using key loggers, Familiarization with malwares: creating test malwares and detecting them, Using steganographic tools for hiding data, Launching SQL injection attacks and prevention, Studying XSS and XSRF attacks, Studying phishing attacks, Implementing buffer over flows and analyzing the vulnerabilities, Familiarization with major open source cyber security tools, Investigating on latest trends in the cyber attacks. |
| **2** | Familiarize with Android application .apk files. By performing static and dynamic analysis on the app find the vulnerable application and document the inferences, perform mobile device forensics,<br>Investigate crimes in Darknet, crimes involving crypto currencies, crimes in social media and crimes in online financial transactions<br>Perform social media forensics, Perform email forensics |
| **3** | File carving for digital forensics, Familiarization of various tools used in disk forensics, OS Forensics, Perform Registry Analysis, Timestamp Analysis, Event Viewer Analysis.<br>Familiarization of various tools used in Memory Forensics, Perform Volatile Data Collection, Memory Dump<br>Familiarize with volatility Framework and Plugins, Bulk Extractor and YARA tools. |
| **4** | Familiarization of various tools used Network forensics, Familiarization of various tools used for Image, audio and video forensics, Familiarization of various anti forensics tools. |

**Text Books:**

1. Michael Gregg, Build Your Own Security Lab: A Field Guide for Network

Testing, 1st Edition, Wiley 2008.

2. Michael Gregg, The Network Security Test Lab: A Step-by-Step Guide, 1st Edition, Wiley 2015.
3. Bill Nelson, Amelia Phillips, Christopher Steuart,"Guide to Computer Forensics and Investigations", Sixth Edition (2020)
4. Karanam Satyanarayana, "Step by Step in Cyber Crimes Investigation, Challenges and Solutions", Asia Law House; 1st Edition (2020).
5. Nina Godbole , Sunit Belapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, 2011,
6. John Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics Elsevier, 2014.
7. P.W. Singer, Allan Friedman, Cyber security and Cyber war: What Everyone Needs to Know, Oxford University Press, 2014,
8. Angus M. Marshall, "Digital Forensics: Digital Evidence in Criminal Investigation", John – Wiley and Sons, 2008.
9. Dr. Rukmani Krishnamurthy, "Introduction to Forensic Science in Criminal Investigation", Selective & Scientific Books (2015)
10. Niranjan Reddy, "Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations", New York, Apress, 1st Edition (2019)

**References:**

1. Thomas J. Holt (Author), Adam M. Bossler (Author), Kathryn C. Seigfried Spellar , "Cybercrime and Digital Forensics: An Introduction", Routledge, 2nd Edition (2017)
2. Computer Forensics: Investigating Network Intrusions and Cyber Crime (EC Council Press Series: Computer Forensics)
3. Cyber Forensics: Understanding Information Security Investigations (Springer's Forensic Laboratory Science Series) by Jennifer Bayuk

## M3022306 ETHICAL HACKING AND PENETRATION TESTING LAB

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M302306** | **Ethical Hacking and Penetration Testing Lab** | **0-1-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To help the students to apply tools and techniques to explore vulnerabilities in systems.
2. To enable the students to perform ethical hacking and penetration of systems and networks

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Apply tools and techniques to evaluate whether computer systems, and networks are vulnerable to cyber attacks.

**CO2**: Understand the need for protecting network and computer systems from cyber attacks.

**CO3:** Analyze the vulnerabilities present in the networks and computer systems using various tools and techniques.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 2 | | 3 | 2 |
| **CO2** | 3 | 3 | 2 | | 3 | |
| **CO3** | 3 | 3 | 2 | | 3 | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | 1. Foot printing Lab - 1 (OSINT)<br>2. Foot printing Lab - 2 (Recon-NG)<br>3. Scanning Lab -1 (Nmap)<br>4. Scanning Lab - 2 (Nmap \| Scanning Scripts \| Online Scanning Tools) Enumeration Lab |
| **2** | 1. Vulnerability Scanning (OpenVAS \| Nessus)<br>2. System Hacking (Metasploit)<br>3. Malware Threats<br>4. Sniffing Lab (Wireshark \| Ettercap \| Cain & Abel)<br>5. Social Engineering (Phishing attacks \| Open Source Campaign Frameworks) |
| **3** | 1. DoS Tools \| Session Hijacking<br>2. Web App Scanners (Accunetix \| ZAP Proxy)<br>3. Web Interceptor (Burp Suite)<br>4. Web attacks (OWASP Top 10) |
| **4** | 1. Wi-Fi Hacking<br>2. Hacking Mobile Platforms using MSF<br>3. Implementation Of IDS-IPS -SNORT \| Active Directory \| Web Proxy - SQUID \| Firewall _ PF Sense<br>4. Implementation of OpenSSL and exploiting Heartbleed Cryptography |

| | |
|---|---|
| | vulnerability |

**Text Books:**

1. Phillip L. Wylie , The PentesterBluePrint, Wiley Publication, 2021.
2. James Corley, Kent Backman , Michael Simpson , Hands on Ethical Hacking and Network Defense, DelmarCengage Learning.
3. Patrick Engebretso, The Basics of Hacking and Penetration Testing, Second Edition, Syngress Publication.
4. Sean-Philip Oriyano,CEH Certified Ethical Hacker Version 8 Self-study Guide, Wiley / Sybex, 2014

**References:**

1. Peter Kim, The Hacker Playbook 2: Practical Guide to Penetration Testing, Createspace Independent Pub, 2015
2. https://www.ethicalhackx.com/ceh-v10-download/
3. http://egyanagar.osou.ac.in/slmfiles/CSP-016-WHITE-HAT_HACKING-LABORATORY-MANUAL-1516011133.pdf
4. https://repo.zenk-security.com/Magazine%20E-book/EN-Certified%20Ethical%20Hacker%203.0%20Official%20Course.pdf
5. http://www.e-fense.com/helix3pro.php
6. https://santoku-linux.com/download/

## M3020307 IoT EXPERIENCE LAB

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M302307** | **IoT Experience Lab** | **0-1-0-0** | **2021** |

**Prerequisites:** Students should have already taken or are currently taking the following courses : 1. Embedded Systems Course 2. Digital Experience Lab

**Course Objectives:**

1. To train students to use various embedded platforms for designing IoT applications .
2. To train students to develop basic programming skills required for designing IoT applications .
3. To train students to leverage the skills acquired to solve real world problems using IoT technology.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Utilize the Microcontroller and SBC platforms for building components of IoT systems.

**CO2:** Write programs using various platforms for building IoT applications, data acquisition and acquire knowledge on basic protocols for data exchange.

**CO3:** Learn to use lightweight messaging protocols for implementing IoT applications.

**CO4:** Learn interfacing radio and other communication modules for building IoT applications.

**CO5:** Use of web servers, data handling and Cloud interface for storage and analytics.

**Program Learning Outcomes:**

**PLO 1 :** Develop strong fundamental disciplinary knowledge
**PLO 2 :** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3 :** Apply scholarship to conduct independent and innovative research
**PLO 4 :** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** : Practice ethical standards of professional conduct and research;
**PLO6**:Acquire professional skills such as collaborative skills, ability to write grants,entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 1 | 1 | 2 | 3 |
| **CO2** | 2 | 3 | 1 | 2 | 2 | 2 |
| **CO3** | 2 | 2 | 3 | 2 | 2 | 2 |
| **CO4** | 3 | 3 | 2 | 1 | 1 | 2 |
| **CO5** | 2 | 2 | 1 | 2 | 1 | 3 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | IoT HW and SW components<br>1. Building blocks of IoT systems , Sensors, Basic Nodes , IIoT ( Review and exposure to basic building blocks )<br>2. Introduction to IDEs for building IoT Applications ( 8 , 32 Bit microcontrollers )<br>3. Programming and deploying applications on Low power boards. ( JTAG, ICSP etc )<br>4. Optimizing applications for battery powered applications, Efficient BMS |
| **2** | Data Acquisition , Storage and Communication<br>5. Data Acquisition : Signal conditioning and sensor interface experiments ( Review of Sensor interfaces : Light, Motion, Temp, Humidity etc )<br>6. Digital and Analog sensor Interface exercises ( Experiments using SPI, I2C, OneWire Protocols)<br>7. Local storage options for memory constrained edge applications. ( Memory Interface exercises )<br>8. Short range M2M Communication Experiments - Radio interface experiments using Low power transceivers ( Applications with NRF , BLE , Zigbee networks ) |
| **3** | Advanced IoT Platforms, SBCs<br>9. Exposure to Advanced IoT Platforms ( Experiments using SBC , Sensing, Analyzing, |

| | |
|---|---|
| | Controlling, Communication / ARM EMBED )<br>10. Gateway Configurations & Implementations ( eg using SBCs : Rpi , Beagle , Custom Boards )<br>11. Data Management and IoT security - implementation and experiments |
| 4 | Stacks, Cloud Platforms & Use Cases<br>12. IoT stacks and protocols. ( Lightweight protocols eg : MQTT implementation experiments )<br>13. Web server applications for IoT and Cloud platforms for IoT Applications ( eg : AWS, Watson, Thingspeak )<br>14. LPWAN (NB-IoT, SigFox, LoRA : Real time implementation and application experiments on various verticals of IoT - Industrial IoT , Smart Cities, Smart Homes )<br>15. Address real world problems using the acquired skills- mini projects. |

**Text Books :**

1. Gary Smart," Practical Python Programming for IoT " ,Packt Publishing.
2. Perry Lea, “IoT and Edge Computing for Architects, 2nd Edition”, Packt Publishing.
3. Simon Monk, “Raspberry Pi Cookbook: Software and Hardware Problems and Solutions “, 3rd Edition, O’Reilly
4. Rolando Herrero, “Fundamentals of IoT Communication Technologies” , Springer.

**References:**

1. Brian Russell & Drew Van Duren, “Practical Internet of Things Security: Beat IoT security threats by strengthening your security strategy and posture against IoT vulnerabilities”, Packt Publishing.
2. Reema Thareja, “Python Programming using Problem Solving Approach”, Oxford Higher Education.
3. Kurose & Ross, “Computer Networking: A Top-Down Approach”, 7th Edition , Pearson.

## M3021116 MACHINE LEARNING LAB – 1

| Course Code | Course Name | Credit Split Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M302116** | **Machine Learning Lab 1** | **0-1-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To provide students with a good understanding of the implementation of major algorithms in Machine Learning
2. To help the students develop the ability to solve problems using the learned concepts.
3. To connect the concepts to other domains and apply in related problems

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Understand the foundations of modern deep learning and reinforcement learning theory, problem and state of the art solutions.

**CO2**: Analyze and evaluate critically the building and integration of deep learning and reinforcement learning algorithms and systems.

**CO3:** Design and demonstrate a working deep learning and reinforcement learning system through team research project, and project report, presentation.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | |
| **CO2** | 3 | 3 | 3 | 2 | | |
| **CO3** | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Exploration of Google AI Experiments platform, Familiarization with NumPy, SciPy, matplotlib and scikit-learn. |
| **2** | Implementation of Perceptron. Implementation of Principal Component Analysis, Experiments with Nave Bayes Classifier, Implementation of Logistic Regression |
| **3** | Implementation of Maximum Likelihood Estimation, Experiments with K-Means Algorithm, Experiments with Hidden Markov Model |
| **4** | Experiments with Support Vector Machine Libraries : SVM, SVC and SVR |

Text Books:

1. Understanding Machine Learning: From Theory to Algorithms, Shai ShalevShwartz, Shai Ben-David, Cambridge University Press, 2014 .

## M3021206 MACHINE LEARNING LAB – 2

| **Course Code** | **Course Name** | **Credit Split<br>Lecture/Lab/Seminar/Project** | **Year of Introduction** |
|---|---|---|---|
| **M302206** | **Machine Learning Lab 2** | **0-1-0-0** | **2021** |
| **Prerequisites:** Nil | | | |

**Course Objectives:**

1. To provide students with a good understanding of the implementation of major algorithms in Deep Learning and Reinforcement Learning
2. To help the students develop the ability to solve problems using the learned concepts.
3. To connect the concepts to other domains and apply in related problems

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Understand the foundations of modern deep learning and reinforcement learning theory, problem and state of the art solutions.

**CO2**: Analyze and evaluate critically the building and integration of deep learning and reinforcement learning algorithms and systems.

**CO3:** Design and demonstrate a working deep learning and reinforcement learning system through team research project, and project report, presentation.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 2 | 3 | 2 | | |
| **CO2** | 3 | 3 | 3 | 2 | | |
| **CO3** | 2 | 3 | 3 | 2 | | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|
| **1** | Familiarisation with Deep Learning Frameworks : Keras and Tensorflow (Introduction to Caffe and Torch is optional)<br>Exploration of any three popular data sets used in Deep Learning/Reinforcement Learning Research |
| **2** | Experiments with Recurrent Neural Networks for sequence modelling problems - sequence prediction, sequence labelling,<br>Experiments with any pre-trained transformer model<br>Experiments with Convolutional Neural Networks - Image classification and object detection |
| **3** | Demonstration of the application of an MDP. Implementation of Q-Learning, Experiments with DQN |

| | |
|---|---|
| 4 | Experiments with DDPG, Implementation of any solution to Bandit Problem discussed in recent research literature. |

**Text Books:**

1. Mastering Machine Learning Algorithms, Giuseppe Bonaccorso, Ingram short title, 2018

## M1020107 PYTHON PROGRAMMING LAB

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| M102107 | Python Programming Lab | 0-1-0-0 | 2021 |

**Prerequisites:** Should have already taken or is currently taking the 'Problem Solving with Python' course

**Course Objectives:**

1. To train students to write algorithms and flowcharts to solve computational problems.
2. To train students to develop basic programming skills.
3. To train students to solve simple computational problems using the Python programming language
4. To train students to use object-oriented concepts and data handling.

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Analyze computational problems and solve them systematically.
**CO2:** Write algorithms and flowcharts to solve computational problems.
**CO3:** Solve computational problems by writing their own computer programs.
**CO4:** Use the Python programming language for solving computational problems.
**CO5:** Use the data handling features of the Python for data analysis.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge
**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature
**PLO 3** Apply scholarship to conduct independent and innovative research
**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;
**PLO 5** Practice ethical standards of professional conduct and research;
**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | PLO1 | PLO2 | PLO3 | PLO4 | PLO5 | PLO6 |
|---|---|---|---|---|---|---|
| CO1 | 3 | 1 | | | | |

| | |
|---|---|
| **CO2** | 3 |
| **CO3** | 3 |
| **CO4** | 3 |
| **CO5** | 3 |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus: List of exercises/Lab programs:**

| **Module** | **Content** |
|---|---|
| **1** | 1. Problems on number systems and data encoding.<br>2. Writing simple algorithms and flowcharts.<br>3. Writing advanced algorithms and flowcharts, installing and running Python. 4. Writing simple programs (e.g. Drake equation) to familiarize with variables, keywords, operators, expressions, data types andoperator precedence. The print() function, type conversion, formatting numbers and strings. |
| **2** | 5. Conditional statements, writing simple scripts, using comments for program readability.<br>6. Loops, nested loops, break and continue statements (e.g. Prime number, Fibonacci series, Factorial, Armstrong number, Palindrome)<br>7. Built-in data structures and their applications - Lists, Tuples, Sets and Dictionaries, Range function, Functions such as zip() and enumerate().<br>8. More coding exercises using lists (e.g. Merging sorted lists), tuples, sets, dictionaries. |
| **3** | 9. Defining and calling functions: Passing arguments and returning values (e.g. Pascal’s triangle.), scope, local functions, Lambda functions, function redefinition, standard library modules.<br>10. File and exception handling.<br>11. Coding exercises to practice Object Oriented Programming. |
| **4** | 12. Data Handling using NumPy and Pandas.<br>13. Python and SQL<br>14. Data Visualization in Python |

**Text Books:**

1. Charles Dierbach, “Introduction to Computer Science Using Python: A Computational Problem-Solving Focus”, Wiley.
2. Ashok NamdevKamthane, Amit Ashok Kamthane, “Programming and Problem Solving with Python”, McGraw Hill Education.
3. Steven F. Lott, “Object Oriented Python”, Packt Publishing.
4. Fabio Nelli, Python Data Analytics: With Pandas, NumPy, and Matplotlib 2nd Edition, Kindle Edition

**References:**

1. Reema Thareja, “Python Programming using Problem Solving Approach”, Oxford Higher Education.
2. Bradley N. Miller, David L. Ranum Problem Solving with Algorithms and Data Structures Using Python, Franklin, Beedle& Associates.
3. Steven F. Lott, “Object Oriented Python”, Packt Publishing.

## M2022206 SECURITY AUDITING LAB

| Course Code | Course Name | Credit Split<br>Lecture/Lab/Seminar/Project | Year of Introduction |
|---|---|---|---|
| **M202206** | **Security Auditing Lab** | **0-1-0-0** | **2021** |

**Prerequisites:** Nil

**Course Objectives:**

1. To help the students to apply tools and techniques to detect security vulnerabilities in systems, software and networks.
2. To enable the students to perform security audits of the systems, network infrastructure and software/applications

**Course Outcomes:** After completion of this course, the students would be able to:

**CO1:** Apply tools and techniques to evaluate whether computer systems, and networks are vulnerable to cyber attacks.

**CO2**: Understand the need for protecting network and computer systems from cyber attacks.

**CO3:** Perform incident management and security auditing of software, systems and networks.

**Program Learning Outcomes:**

**PLO 1** Develop strong fundamental disciplinary knowledge

**PLO 2** Demonstrate research skills that are of experimental, computational, or theoretical nature

**PLO 3** Apply scholarship to conduct independent and innovative research

**PLO 4** Show communication skills in a variety of formats (oral, written) and to expert and non-expert audiences;

**PLO 5** Practice ethical standards of professional conduct and research;

**PLO 6** Acquire professional skills such as collaborative skills, ability to write grants, entrepreneurial skills, and write articles for scholarly journals if it is taught by faculty in the department.

**Mapping of course outcomes with program learning outcomes:**

| | **PLO1** | **PLO2** | **PLO3** | **PLO4** | **PLO5** | **PLO6** |
|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 2 | | 3 | 2 |
| **CO2** | 3 | 3 | 2 | | 3 | |
| **CO3** | 3 | 3 | 2 | | 3 | |

(Correlation: 1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High))

**Syllabus:**

| **Module** | **Content** |
|---|---|

| | |
|---|---|
| **1** | Familiarize with tools such as Burp Suite, Kali / Parrot OS, SQLMap, WPScan (for Wordpress Vulnerability Scanner), Nmap, Metasploit, Wireshark, Android Debug Bridge, Drozer, and MobSF, etc.<br>Perform penetration testing with the following tools<br>1. Wireshark<br>2. John the Ripper Tool<br>3. Hydra<br>4. Burp Suite |
| **2** | Perform network security auditing with the following tools<br>1. Nessus<br>2. Nmap<br>3. OpenVAS<br>4. Metasploit |
| **3** | Perform web application security testing using<br>1. Wapiti<br>2. W3af<br>3. Nogotofail<br>4. Netsparker<br>5. SonarQube |
| **4** | Perform forensics with the following tools<br>1. Sleuth Kit<br>2. Autopsy<br>3. FTK Imager<br>4. Linux 'dd'<br>Perform incident management audit with the following tools<br>1. ProcDump<br>2. Cyphon<br>3. TheHive Project<br>4. Volatility |

**Text Books:**

1. IT Auditing: Using Controls to Protect Information Assets, Third Edition Book by Chris Davis and Mike Schiller
2. https://www.elsevier.com/books/the-basics-of-it-audit/gantz/978-0-12-417159-6

**References:**

1. https://www.wireshark.org/docs/wsug_html_chunked/
2. https://www.openvas.org/
3. https://nmap.org/
4. https://www.metasploit.com/
5. https://www.geeksforgeeks.org/what-is-burp-suite/
6. https://www.tenable.com/products/nessus
7. https://wapiti.sourceforge.io/
8. https://github.com/AndroBugs/