HSNC University,
Mumbai

Ordinances and Regulations With

Respect to

Choice Based Credit
System (CBCS)
For the Programs under

The Faculty of Science and Technology

With effect from the Academic year 2020-2021

Department of M.Sc.
IT Board of Studies

Composition:

(i) The Board of Studies shall consist of the following members, namely: —

(a) One head of the Department from amongst the Schools, Centers and Constituent Colleges, of the University in the relevant subject of the University nominated by the Vice Chancellor in consultation with the Dean concerned; -

Sr. No.	Name	Designation	Contact Details
1.	Dr. Rakhi O. Gupta	Chairperson on HOD Dept. of IT, KC College, HSNC University	9619914191 rakhi.gupta@kccollege.edu.in

(b) Two to five teachers each having minimum five years teaching experience amongst the full time teachers of the Departments, Schools, Centers and Constituent Colleges of the University in the relevant subject nominated by the Vice-Chancellor in consultation with the Dean of the respective faculty; -

r. No.	Name	Designation	Contact Details
1.	Ms. Pragati V.Thawani	Co-chairperson Dept. of IT, KC College, HSNC University	9960782000 pragati.thawani@kccollege.edu.in
2.	Ms. Sandhya Bhavsar	Assistant Professor Dept. of IT, KC College, HSNC University	8446677643 sandhya.bhavsar@kccollege.edu.in

3.	**Ms. Nashrah Gowalker**	**Assistant Professor** **Dept. of IT, KC College, HSNC University**	**9664774108** **nashrah.gowalker@kccollege.edu.in**

(c) one Professor / Associate Professor from other Universities or professor / Associate Professor from colleges managed by Parent Body; nominated by Parent Body; --

r. No.	Name	Designation	Contact Details
1.	Dr. R. Kamatchi	Director, ISME School of Management Studies and Entrepreneurship, Lower Parel.	9224450454 rkamatchiiyer@gmail.com
2.	Dr. Ajay Patil	Professor, School of Computer Sciences, KNMU, Jalgaon.	9423975215 ajaypatil.nmu@gmail.com
3.	Dr. Varsha Turkar	Professor and Head Don Bosco College of Engineering, Margoa, Goa	+91 9920038965 varshaturkar@gmail.com

(d) four external experts from Industry / Research / eminent scholar in the field relevant to the subject nominated by the Parent Body;

r. No.	Name	Designation	Contact Details
1.	Dr. Hiren Dand	Head of Department (IT) Mulund College of Commerce.	9821140717 Hiren.dand@mccmulund.ac.in
2.	Mr. Asif K. Rampurawala	Vice Principal, Vidyalankar School of Information Technology	9820765273 asif.rampurawala@vsit.edu.in
3.	Mr. Kaushal Shah	Senior Manager Reliance Power Ltd.	9869069203 Kaushalshah78@gmail.com

4.	**Mr. Prabhav Daga**	**Proprietor at Curaksha Partner at Gianda Trading Solutions, LLP.**	**8850252861 prabhav@curaksha.com**

(e) top rankers of the Final Year Graduate and Final Year Post Graduate examination of previous year of the concerned subject as invitee members for discussions on framing or revision of syllabus of that subject or group of subjects for one year nominated by Vice Chancellor.

the Board of Studies, at its first meeting, shall elect one of the members as a Chairperson of the Board of Studies from amongst its members, subject that no person shall be Chairperson of the Board of the studies, for a second consecutive term whether as an elected, nominated or co-opted member, as the case may be.

Sr. No.	Name	Contact Details
1.	Ms. Kimberly Moniz	9619147188 kimberlythemoniz@gmail.com

Part –I

Outline of Choice Based Credit System as outlined by University Grants Commission:

R. ** : The Definitions Of The Key TermsUsed In The Choice Based Credit System And Grading System Introduced From TheAcademicYear2020-2021AreAs Under:**

1. **CoreCourse:** A course, which should compulsorily be studied by a candidate as a core requirement is termed as aCore course.

2. **Elective Course:** Generally, a course which can be chosen from a pool of courses and which may be very specific or specialized or advanced or supportive to the discipline/subject of study or which provides an extended scope or which enables an exposure to some other discipline/subject/domain or nurtures the candidate's proficiency/skill is called an Elective Course.

2.1 **Discipline Specific Elective (DSE) Course:** Elective courses may be offered by the main discipline/subject of study is referred to as Discipline Specific Elective. The University/ Institute may also offer discipline related Elective courses of interdisciplinary nature (to be offered by main discipline/subject to study).

2.2 **Dissertation/Project:** An elective course designed to acquire special/advanced knowledge, such as supplement study/support study to a project work, and a candidate studies such a course on his own with an advisory support by a teacher/faculty member is called dissertation/project. A Project/Dissertation work would be of 6 credits. A Project/Dissertation work maybegiveninlieuofadisciplinespecific elective paper.

2.3 **Generic Elective (GE) Course:** An elective course chosen generally from anunrelated discipline/subject,withanintentiontoseekexposure is called a Generic Elective.
P.S.: Acorecourseofferedinadiscipline/subjectmaybetreatedasan electiveby otherdiscipline/subjectandviceversaandsuchelectivesmay also be referred toas Generic Elective.

Choice Base Credit System : CBCS allows students to choose inter- disciplinary, intra-disciplinary courses, skilloriented papers(even from other disciplines according to their learning needs ,interests and aptitude) and more flexibility for students.

3. **Honours Program :** To enhance employability and entrepreneurship abilities among the learners, through aligning Inter Disciplinary / Intra Disciplinary courses with Degree Program. HonoursProgram will have
40 additional credits to be undertaken by the learner across three years essentially in Inter / Intra Disciplinary course.

   A learner who joins Regular Undergraduate Program will have to opt for Honours Program in the first year of the Program. However, the credits for honours, though divided across three years can be completed within three years to become eligible for award of honours Degree.

4. **Program:** A Program is a set of course that are linked together in an academically meaningful way and generally ends with the award of a Degree Certificate depending onthelevelofknowledge attainedandthe totalduration ofstudy,B.Sc.Programs.

5. **Course:** A 'course' is essentially a constituent of a 'program' and may be conceived of as a composite of several learning topics taken from a certain knowledge domain, at a certain level. All the learning topics included in a course must necessarily have academiccoherence,i.e.theremustbeacommonthreadlinkingthevariouscomponents of a course. A number of linked courses considered together are in practice, a 'program'.

6. **Bridge Course:** Bridge course is visualized as Presemester preparation bythe learner beforecommencement ofregularlectures. For eachsemester thetopics, whoseknowledge is considered as essential for effective andseamless learning oftopics of the Semester, willbespecified.TheBridgeCoursecanbeconducted inonlinemode.TheOnlinecontent can be created fortheBridgeCourseTopics.

7. **Module and Unit:** A course which is generally an independent entity having its own separate identity, is also often referred to as a 'Module' in today's parlance, especially when we refer to a 'modular curricular structure'. A module may be studied in conjunction with other learning modules or studied independently. A topic within a course is treated as a Unit. Eachcourse shouldhave exactly3 Units.

8. **Self-Learning: 20% of the topics will be marked for Self-Learning.** Topics for Self-Learning are to be learned independently by the student, in a time- bound manner, using online and offline resources including online lectures, videos, library, discussion forums,fieldwork, internshipsetc.

   Evaluative sessions (physical/online), equivalent to the credit allocation of the Self Learningtopics,shallbeconducted, preferably, everyweekfor each course. Learnersareto beevaluatedrealtimeduringevaluativesessions. Thepurpose of evaluative sessions is toassess thelevelof the students' learning achieved

in the topics earmarked for Self-Learning.

The teacher's role in these evaluative sessions will be that of a Moderator and Mentor, who will guide and navigate the discussions in the sessions, and offer concluding remarks, with proper reasoning on the aspects which may have been missed by the students,inthecourseoftheSelf-Learningprocess.

The modes to evaluate self-learning can be a combination of the various methods such as written reports, handouts with gaps and MCQs, objective tests, case studies and Peer learning. Groups can be formed to present self- learning topics to peer groups, followedby Question and Answer sessions and open discussion. The marking scheme for Self-Learningwill bedefined under Examination andTeaching.

The topics stipulated for self-learning can be increased or reduced as per the recommendations of the Board of Studies and Academic Council from time to time. All decisions regarding evaluation need to be taken and communicated to the stakeholders preferably before the commencement of a semester. Some exceptions maybemadein exigencies, likethecurrentsituationarisingfromthe lockdown,butsuch ad hoc decisionsareto bekept totheminimumpossible.

10 **Credit Point:** Credit Pointreferstothe'Workload' ofa learnerandis an indexof the number of learning hoursdeemedfor acertainsegment oflearning. These learning hours may include a variety of learning activities like reading, reflecting, discussing, attending lectures / counseling sessions, watching especially prepared videos, writing assignments, preparing for examinations, etc. Credits assignedfor a singlecoursealwayspayattentiontohowmanyhours it would take for a learner to complete a single course successfully. A single course should have, byandlargeacoursemaybeassignedanywherebetween 2 to 8 credit points wherein 1 credit is construed as corresponding to approximately 15 learning hours.

11. **Credit Completion and Credit Accumulation:** Credit completion or Credit acquisition shall be considered to take place after the learner has successfully clearedalltheevaluationcriteriawithrespecttoasinglecourse. Thus, alearner who successfully completes a 4 CP (Credit Point) course may be considered to have collected or acquired 4 credits. learner level of performance above the minimum prescribed level (viz. grades / marks obtained) has no bearing on the number of credits collected or acquired. A learner keeps on adding more and more credits as he completes successfully more and more courses. Thus, the learner 'accumulates'coursewise credits.

12. **Credit Bank:** A Credit Bank in simple terms refers to stored and dynamically updated information regarding the number of Credits obtained by any given learner along with details regarding the course/s for which Credit has been given, thecourse-level, nature,etc. In addition,alltheinformationregardingthe number of Credits transferred to different programs or credit exemptions given mayalso be stored with the individual'shistory.

13. **Credit Transfer:** (performancetransfer) Whenalearnersuccessfullycompletes a program, he/she is allowed to transfer his/her past performance to another academic program havingsome common courses andPerformance transfer is said to havetakenplace.

14. **Course Exemption:** Occasionally, when two academic programs offered by a single university or by more than one university, may have some common or equivalent course-content, thelearnerwhohasalreadycompletedoneofthese academicprograms is allowed to skip these 'equivalent' courses while registering forthenew program. TheLearneris'exempted'from 'relearning'the common or equivalent content areaand from re-appearing for the concerned examinations. It is thus taken for granted thatthe learner has already collected in the past the credits corresponding to the exempted courses.

Part-II

O*** The fees for transfer of credits or performance will be based on number of credits that a learner has to complete for award of the degree.**

The Scheme of Teaching and Examination:

The performance of the learners shall be evaluated in two components: Internal Assessment with 40% marks by way of continuous evaluation and by Semester End Examination with 60% marks by conducting the theory examination.

INTERNAL ASSESSMENT:- It is defined as the assessment of the learners on the basis of continuous evaluation as envisaged in the credit based system by way of participation of learners in various academic and correlated activities in the given semester of the programme.

A). Internal Assessment–40% 40 marks

Practical's (internal Components of the Practical Course

1. **For Theory Courses**

Sr. No.	Particulars	Marks
1	**ONE** classtest/online examination to be conducted in the given semester	15 Marks
2	One assignment based on curriculum(to be assessed by the teacher Concerned	10 Marks
3	Self-Learning Evaluation	10 Marks
4	Active participation in routine class instructional deliveries	05 Marks

2. For Courses with Practicals

Each practical course can be conducted out of 50 marks with 20 marks for internal and 30 marks for external

Practical's (Internal component of the Practical Course)

Sr. No	Evaluation type	Marks
1	Two Best Practicals /Assignments/Presentation /Preparation of models/ Exhibits **Or** One Assignment/ project with class presentation to be assessed by teacher concerned	10
2	Journal	05
3	Viva	05

The semester end examination (external component) of 60 % for each course will be as follows:

i) **Duration** – **2 Hours** ii) **Theory Question**

Paper Pattern: -

1. There shall be four questions each of 15 marks. On each unit there will be one questionand the fourth one will be based on entire syllabus.
2. All questions shall be compulsory with internal choice within the questions. (Each question will be of 20 to 23 marks with options.)
3. Question may be subdivided into sub-questions a, b, c… and the allocation of marks depend on the weightage of the topic.

The marks will be given for all examinations and they will be converted into grade (quality) points. The semester-end, final grade sheets and transcripts will have only credits, grades, grade points, SGPA and CGPA.

3. Project andAssignment:

- Project or Assignment, which can in the following forms
  - Case Studies
  - Videos
  - Blogs
  - Research paper(Presented in Seminar/Conference)
    Field Visit Report

- Presentations related to the subject(Moot Court,YouthParliament,etc.)
- Internships (Exposition of theory into practice)
- Open Book Test
- Any other innovative methods adopted with the prior approval of Director Board of Examination and Evaluation.

4. Self-Learning Evaluation

- **20% OF THE TOPICS OF CURRICULUM ARE LEARNED BY THE STUDENT THROUGH SELF LEARNING USING ONLINE / OFFLINE ACADEMIC RESOURSE SPECIFIED IN THE CURRICULUM.**
- **HENCE 20% OF THE LECTURES SHALL BE ALLOCATED FOR EVALUATION OF STUDENTS ON SELF LEARNING TOPICS**
- The identified topics in the syllabus shall be learnt independently by the students in a time bound manner preferably from online resources. Evaluative sessions shall be conducted by the teachers and will carry 10 Marks.

CLUB The self-learning topics into 3-4 GROUPS OF TOPICS ONLY FOR EVALUATION.

- PRESCRIBE TIME DURATION (IN DAYS) FOR COMPLETION OF EACH GROUP OF TOPIC AND EARMARK SELF LEARNING EVALUATION LECTURES IN THE TIMETABLE. HENCE EACH GROUP OF TOPIC CAN BE ASSIGNED 3 REGULAR LECTURES FOR THIS EVALUATION FOR ENTIRE CLASS

3 Sub Topics

Each evaluative session shall carry 3 Marks (3 x 3 Units = 9 Marks). Students who participate in all evaluative sessions shall be awarded 1 additional Mark.

4 Sub Topics

Each evaluative session shall carry 2.5 Marks (2.5 x 4 Units = 10 Marks)

- EVALUATION OF SELF LEARNING TOPICS CAN COMMENCE IN REGULAR LECTURES ASSIGNED FOR SELF LEARNING EVALUATION IN THE TIMETABLE

3 Evaluative sessions

Each evaluative session shall carry 3 Marks (3 x 3 = 9 Marks). Students who participate in all evaluative sessions shall be awarded 1 additional Mark.

4 Evaluative sessions

Each evaluative session shall carry 2.5 Marks (2.5 x 4 = 10 Marks). Methods for Evaluation of Self-learning topics:

- Seminars/presentation (PPT or poster), followed by Q&A
- Objective questions /Quiz / Framing of MCQ

questions.

- Debates
- Group discussion
- You-Tubevideos(Marksshallbebasedonthequalityand viewership)
- Improvisation of videos
- Viva Voce

Any other innovative method

TEACHERS CAN FRAME OTHER METHODS OF EVALUATION ALSO PROVIDED THAT THE METHOD, DULY APPROVED BY THE COLLEGE EXAMINATION COMMITTEE, IS NOTIFIED TO THE STUDENTS AT LEAST 7 DAYS BEFORE THE COMMENCEMENT OF THE EVALUATION SESSION AND IS FORWARDED FOR INFORMATION AND NECESSARY ACTION AT LEAT 3 DAYS BEFORE THE COMMENCEMENT OF THE EVALUATION SESSION

SEMESTER END EXAMINATION: - It is defined as the examination of the learners on thebasis of performance in the semester end theory / writtenexaminations.

B.SemesterEndExamination-60% ***60***

Marks

1) Duration – These examinations shall be of 2 Hours duration.
2) Question Paper Pattern: -
   i. Thereshallbefourquestions eachof 15 marks.
   All questions shall be compulsory with internal choice within the questions.
   iii. Questionmaybesubdividedintosubquestionsa, b,c, d&e onlyandthe allocation of marksdepends onthe weightage of thetopic.

THE MARKS OF THE INTERNAL ASSESSMENT SHOULD NOT BE DISCLOSED TOTHE STUDENTSTILLTHE RESULTS OFTHE CORRESPONDINGSEMESTERISDECLARED.

HSNC University
Mumbai

(2020-2021)

Ordinances and Regulations

With Respect to

Choice Based Credit System

(CBCS) For the Programmes

Under

The Faculty of Science and Technology

For the Course

Information Technology

Curriculum – First Year Postgraduate Program

Semester-I and Semester -II

2020-2021

Section D

Preamble

The M.Sc. Information Technology program is started with an aim to make the students employable after Post-Graduation and impart industry oriented training.

1. **Course Objective:** The main objectives of the course are:

- To think analytically, creatively and critically in developing robust, extensible and highly maintainable technological solutions to simple and complex problems related to human, technology and environmental factors.
- To apply their knowledge and skills to be employed and excel in IT professional careers and/or to continue their education in IT and/or related post graduate programs.
- To be capable of managing complex IT projects with consideration of various factors.
- To work effectively as a part of a team to achieve a common stated goal.
- To adhere to the highest standards of ethics, including relevant industry and organizational codes of conduct.
- To develop an aptitude to engage in continuing educational and professional development.
- To build on the basics and the core concepts learnt during relevant undergraduate program.

The new syllabus is aimed to achieve the following objectives. The syllabus spanning two years covers the industry endorsed relevant courses. The students will be ready for the jobs available in different fields like:

- Networking
- Security
- Machine Learning
- Artificial Intelligence
- Big Data
- Image Processing
- Cloud Computing and Applications
- AI Chat Bot (The Department plans to introduce it in Part2)
- And many others

2. **Process adopted for curriculum designing:** The department has conducted multiple meetings with academic partners, industry partners. After discussion with them, the changes in the syllabus were introduced with the view that students need to learn the core concepts in detail.

3. **Salient features, how it has been made more relevant:** After discussion and interaction with the industry partners and understanding the requirement of the industries certain changes in the syllabus are introduced. Upcoming Technologies like AI, Big Data, etc. have been added keeping the upcoming trends in the field of Information Technology.

4. **Learning Outcomes:** It is expected to improvise the soft skill as well as hardware skills for the students.

- **Input from stakeholders (Which sections have been modified) with relevant introduction:** There are modifications suggested by the Industry person to make changes in the syllabus provided by University of Mumbai and add a few more topic to the already developed syllabus.

Part 2 - The Scheme of Teaching and Examination is asunder:

Semester – I

Summary

Sr. No.	Choice Based Credit System			Subject Code	Remarks
1	Core Course (Information Technology)			MS-FIT-101, MS-FIT-102, MS-FIT-103, MS-FIT-104.	
				MS-FIT-1P1, MS-FIT-1P2, MS-FIT-1P3, MS-FIT-1P4.	
2	Elective Course	Discipline Specific Elective (DSE) Course			
		2.1	Interdisciplinary Specific Elective (IDSE) Course		
		2.2	Dissertation/Project		
		2.3	Generic Elective (GE) Course		
3	Ability Enhancement Compulsory Courses (AECC)				
	Skill Enhancement Courses (SEC)				

First Year Semester -I Internal and External Detailed Evaluation Scheme

Sr. No.	Subject Code	Subject Title	Periods Per Week (Period of 45min)					Credit	Internals			Total Marks
			Units	S. L.	L	T	P		S. L. E	CT+ AT= 15+5	PA	
1	MS-FIT-101	Cloud Computing	4	20% *	5	0	0	4	10	20	10	100
2	MS-FIT-102	Applied Artificial Intelligence	4	20% *	5	0	0	4	10	20	10	100
3	MS-FIT-103	Fundamentals of Information Security	4	20% *	5	0	0	4	10	20	10	100
4	MS-FIT-104	Introduction to Data Science and Big Data Analytics	4	20% *	5	0	0	4	10	20	10	100
5	MS-FIT-1P1	Cloud Computing Practical	-	-	0	-	3	2				50
6	MS-FIT-1P2	Applied Artificial Intelligence Practical	-	-	0	-	3	2				50
7	MS-FIT-1P3	Fundamentals of Information Security Practical	-	-	0	-	3	2				50
8	MS-FIT-1P4	Introduction to Data Science and Big Data Analytics Practical	-	-	0	-	3	2				50
	Total Periods/ Credit							24				**600**

***One to two lectures to be taken for CONTINUOUS self -learning evaluation**

First Year Semester I – Units – Topics- Teaching Hours

S. N	Subject Code & Title	Subject Unit Title		Lectures (45 min)	Total Lectures	Credit	Total Marks
1	MS-FIT-101	1	Introduction to Cloud Computing Parallel and Distributed Computing Virtualization	15	60 L	4	100 (60+40)
		2	Cloud Computing Architecture and Fundamental Cloud Security Platforms and New Developments	15			
		3	Specialized Cloud Mechanisms:	15			
		4	Cloud Delivery Model Considerations: Service Quality Metrics and SLAs:	15			
2	MS-FIT-102	1	Review of AI Expert System and Applications	15	60 L	4	100 (60+40)
		2	Probability Theory Fuzzy Sets and Fuzzy Logic	15			
		3	Machine Learning Paradigms Artificial Neural Networks Evolutionary Computation	15			
		4	Intelligent Agents**:** Advanced Knowledge Representation Techniques Natural Language Processing:	15			
3	MS-FIT-103	1	Security and Risk Management Asset Security	15	60 L	4	100 (60+40)
		2	Security Architecture and Engineering, Cyber Law, Rules and Regulations	15			
		3	Identity and Access Management (IAM) Communication and Network Security Software Development Security	15			
		4	Security Operations Security Assessment and Testing	15			
4	MS-FIT-104	1	Introduction to Data science	15	60 L	4	100 (60+40)
		2	Three Management Layers Retrieve Stop, Assess Superstep	15			
		3	Introduction to Big Data	15			
		4	Analytical Theory and Methods	15			

5	MS-FIT-1P1	1	Cloud Computing Practical			2	
6	MS-FIT-1P2	2	Applied Artificial Intelligence Practical			2	
7	MS-FIT-1P3	3	Fundamentals of Information Security Practical			2	
8	MS-FIT-1P4	4	Introduction to Data Science and Big Data Analytics Practical			2	
			TOTAL			**24**	**600**

- Lecture Duration – 48 Minutes
- **One Credit =15 Hours**

L: Lecture: Tutorials P: Practical Ct-Core Theory, Cp-Core Practical, SLE- Self learning evaluation CT-Commutative Test, SEE- Semester End Examination, PA-Project Assessment, AT- Attendance

Part 3: Detailed Scheme Theory

F. Y. M.Sc.IT

2020-2021

SEM 1

Course Code: MS-FIT-101 Cloud Computing

Unit	Details	No. of Lectures
1	**1.1 Introduction to Cloud Computing**: Introduction, Historical developments, Building Cloud Computing Environments, Principles of Parallel and Distributed Computing: Eras of Computing, Parallel v/s distributed computing, Elements of Parallel Computing, Elements of distributed computing, Technologies for distributed computing. **1.2 Virtualization:** Introduction, Characteristics of virtualized environments, Taxonomy of virtualization techniques, Virtualization and cloud computing, Pros and cons of virtualization, Technology examples. Logical Network Perimeter, Virtual Server, Cloud Storage Device, Cloud usage monitor, Resource replication, Ready-made environment.	15
2	**2.1 Cloud Computing Architecture:** Introduction, Fundamental concepts and models, Roles and boundaries, Cloud Characteristics, Cloud Delivery models, Cloud Deployment models, Economics of the cloud, Open challenges. **2.2 Fundamental Cloud Security:** Basics, Threat agents, Cloud security threats, additional considerations. Industrial Platforms and New Developments: Amazon Web Services, Google App Engine, Microsoft Azure.	15
3	**3.1 Specialized Cloud Mechanisms:** Automated Scaling listener, Load Balancer, SLA monitor, Pay-per-use monitor, Audit monitor, fail over system, Hypervisor, Resource Centre, Multidevice broker, State Management Database. Cloud Management Mechanisms: Remote administration system, Resource Management System, SLA Management System, Billing Management System, **3.2 Cloud Security Mechanisms**: Encryption, Hashing, Digital Signature, Public Key Infrastructure (PKI), Identity and Access Management (IAM), Single Sign-On (SSO), Cloud-Based Security Groups, Hardened Virtual Server Images	15
4	**4.1 Cloud Delivery Model Considerations**: Cloud Delivery Models: The Cloud Provider Perspective, Cloud Delivery Models: The Cloud Consumer Perspective, Cost Metrics and Pricing Models: Business Cost Metrics, Cloud Usage Cost Metrics, Cost Management Considerations, **4.2 Service Quality Metrics and SLAs:** Service Quality Metrics, SLA Guidelines	15

References:

1. Mastering Cloud Computing Foundations and Applications Programming, Rajkumar Buyya,Elsevier, 2013
2. Cloud Computing Concepts, Technology & Architecture, Thomas Erl, Prentice Hall, 2012.
3. Distributed and Cloud Computing, FromParallel Processing to the Internet of Things, Kai Hwang, MK Publishers, 2013

Course Code: MS-FIT-102 Applied AI

	Details	Lectures
1	**1.1 Review of AI:** History, foundation and Applications **Expert System and Applications:** Phases in Building Expert System, Expert System Architecture, Expert System versus Traditional Systems, Rule based Expert Systems, Blackboard Systems, Truth Maintenance System, Application of Expert Systems, Shells and Tools	**15**
2	**2.1 Probability Theory:** joint probability, conditional probability, Bayes's theorem, probabilities in rules and facts of rule based system, cumulative probabilities, rule based system and Bayesian method **2.2 Fuzzy Sets and Fuzzy Logic:** Fuzzy Sets, Fuzzy set operations, Types of Member ship Functions, Multivalued Logic, Fuzzy Logic, Linguistic variables and Hedges, Fuzzy propositions, inference rules for fuzzy propositions, fuzzy systems, possibility theory and other enhancement to Logic	**15**
3	**3.1 Machine Learning Paradigms:** Machine Learning systems, supervisedand un-supervised learning, inductive learning, deductive learning, clustering, support vector machines, cased based reasoning and learning. **3.2 Artificial Neural Networks:** Artificial Neural Networks, Single-Layer feedforward networks, multi-layer feed- forward networks, radial basis function networks, design issues of artificial neural networks and recurrent networks **3.3 Evolutionary Computation:** Soft computing, genetic algorithms, genetic programming concepts, evolutionary programming, swarm intelligence, ant colony paradigm, particle swarm optimization and applications of evolutionary algorithms.	**15**

4	**4.1 Intelligent Agents:** Agents vs software programs, classification of agents, working of an agent, single agent and multiagent systems, performance evaluation, architecture, agent communication language, applications **4.2 Advanced Knowledge Representation Techniques:** Conceptual dependency theory, script structures, CYC theory, script structure, CYC theory, case grammars, semantic web. Natural Language Processing: Sentence Analysis phases, grammars and parsers, types of parsers, semantic analysis, universal networking language, dictionary	**15**

Reference Books:

1) Artificial Intelligence, Saroj Kaushik, Cengage
2) Artificial Intelligence: A Modern Approach. A. Russel, Peter Norvig
3) Artificial Intelligence, Elaine Rich, Kevin Knight, Shivashankar B Nair, Tata Mc-grawhill.

Course Code: MS-FIT-103 Fundamentals of Information Security

Unit	Details	No. of Lectures
1	**1.1 Security and Risk Management** Understand and apply concepts of confidentiality, integrity and availability Evaluate and apply security governance principles Determine compliance requirements Contractual, legal, industry standards, and regulatory requirements Privacy requirements Understand legal and regulatory issues that pertain to information security in a global context Understand, adhere to, and promote professional ethics Organizational code of ethics Develop, document, and implement security policy, standards, procedures, and guidelines Identify, analyze, and prioritize Business Continuity (BC) requirements Contribute to and enforce personnel security policies and procedures Understand and apply risk management concepts Understand and apply threat modeling concepts and methodologies Apply risk-based management concepts to the supply chain Establish and maintain a security awareness, education, and training program Candidate screening and hiring » Employment agreements and policies Onboarding and termination processes Vendor, consultant, and contractor agreements and controls Compliance policy requirements Privacy policy requirements Identify threats and vulnerabilities Risk assessment/analysis Risk response	15

	Countermeasure selection and implementation Applicable types of controls (e.g., preventive, detective, corrective) Security Control Assessment (SCA) Monitoring and measurement Asset valuation Reporting Continuous improvement Risk frameworks Threat modeling methodology Threat modeling concepts Risks associated with hardware, software and networks **1.2 Asset Security** Identify and classify information and assets Determine and maintain information and asset ownership Protect privacy Ensure appropriate asset retention Determine data security controls Establish information and asset handling requirements Data owners Data processers Data remanence Collection limitation Understand data states Scoping and tailoring Standards selection Data protection methods Data class	
2	**2.1 Security Architecture and Engineering** Implement and manage engineering processes using secure design principles Understand the fundamental concepts of security models Select controls based upon systems security requirements Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption) Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements Assess and mitigate vulnerabilities in web-based systems Assess and mitigate vulnerabilities in mobile systems Assess and mitigate vulnerabilities in embedded devices Apply cryptography Apply security principles to site and facility design Client-based systems Server-based systems Database systems Cryptographic systems Industrial Control Systems (ICS) Cloud-based systems Distributed systems Internet of Things (IoT) Cryptographic life cycle (e.g., key management, algorithm selection) Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves) Public Key Infrastructure (PKI) Key management practices Digital signatures Non-repudiation Integrity (e.g., hashing)	15

	Understand methods of cryptanalytic attacks Digital Rights Management (DRM) Implement site and facility security control **2.2 Cyber Law, Rules and Regulations** Evolution of the IT Act, Genesis and Necessity Salient features of the IT Act, 2000, various authorities under IT Act and their powers. ; Penalties & Offences, amendments. Impact on other related Acts (Amendments) Cyber Space Jurisdiction eCommerce and related Laws in India Intellectual Property Rights, Domain Names and Trademark Disputes Sensitive Personal Data or Information (SPDI) in Cyber Law Cloud Computing & Law Cyber Law : International Perspective Personal Data Protection Law Need for Digital Forensics and Data Recovery	
3	**3.1 Identity and Access Management (IAM)** Control physical and logical access to assets Manage identification and authentication of people, devices, and services Integrate identity as a third-party service Implement and manage authorization mechanisms Manage the identity and access provisioning lifecycle **3.2 Communication and Network Security** Implement secure design principles in network architectures Secure network components Implement secure communication channels according to design Open System Interconnection (OSI) and Transmission **3.3 Software Development Security** Understand and integrate security in the Software Development Life Cycle (SDLC) Identify and apply security controls in development environments Assess the effectiveness of software security Assess security impact of acquired software Define and apply secure coding guidelines and standards	15

4	**4.1 Security Operations** Understand and support investigations Understand requirements for investigation types Conduct logging and monitoring activities Securely provisioning resources Understand and apply foundational security operations concepts Apply resource protection techniques Conduct incident management Operate and maintain detective and preventative measures Implement and support patch and vulnerability management Understand and participate in change management processes Implement recovery strategies Implement Disaster Recovery (DR) processes Test Disaster Recovery Plans (DRP) Participate in Business Continuity (BC) planning and exercises Implement and manage physical security Address personnel safety and security concerns **4.2 Security Assessment and Testing** Design and validate assessment, test, and audit strategies Conduct security control testing Collect security process data (e.g., technical and administrative) Analyze test output and generate report Conduct or facilitate security audits	15

Reference Books:

1. Ross Anderson, Security Engineering. 2nd Edition. John Wiley and Sons. 2008, ISBN-13: 978-0470068526, Required.
2. Charles P. Pfleeger, Security in Computing, 5th Edition, Prentice Hall, 2015, ISBN-10: 0134085043, Recommended.
3. The Official (ISC)² CISSP CBK Reference, 5th Edition by John Warsinske, Mark Graff, Kevin Henry, Christopher Hoover, Ben Malisow, Sean Murphy, C. Paul Oakes, George Pajari, Jeff T. Parker, David Seidl, Mike Vasquez, Publisher: Sybex (2019)
4. (ISC)² Code of Ethics, (2020)
5. Information Security Management Handbook, Sixth Edition by Harold F. Tipton and Micki Krause. Publisher: CRC Press. (2007)
6. Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats, First Edition by Bill Gardner and Valerie Thomas. Publisher: Syngress. (2014)
7. Information Security Handbook: Develop a Threat Model and Incident Response Strategy to Build a Strong Information Security Framework by Darren Death. Publisher: Packt Publishing. (2017)
8. Threat Modeling: Designing for Security by Adam Shostack
9. CISSP All-in-One Exam Guide, Eighth Edition, 8th Edition by Shon Harris, Fernando Maymi, Publisher(s): McGraw-Hill
10. Cyber Law in India by Farooq Ahmad; Pioneer Books
11. Information Technology Law and Practice by Vakul Sharma; Universal Law Publishing Co. Pvt. Ltd.
12. The Indian Cyber Law by Suresh T. Vishwanathan; Bharat Law House New Delhi
13. Guide to Cyber and E – Commerce Laws by P.M. Bukshi and R.K. Suri; Bharat Law House, New Delhi
14. The Information Technology Act, 2000; Bare Act – Professional Book Publishers, New Delhi
15. Guide to Cyber Laws by Rodney D. Ryder; Wadhwa and Company, Nagpur

Course Code: MS-FIT-104 Introduction To Data Science And Big Data Analytics

Unit	Details	No. of Lectures
1	**1.1 Introduction to Data science**: Rapid Information Factory Ecosystem, Data Science Storage Tools, Data Lake, Data Vault, Data Warehouse Bus Matrix, Data Science Processing Tools ,Spark, Mesos, Akka, Cassandra, Kafka, Elastic Search, R, Scala, Python, MQTT, The Future, Definition of Data Science	15

	Framework, Cross- Industry Standard Process for Data Mining (CRISP-DM), Homogeneous Ontology for Recursive Uniform Schema, The Top Layers of a Layered Framework, Layered Framework for High-Level Data Science and Engineering, Business Layer, Engineering a Practical Business Layer, Basic Utility Design, Engineering a Practical Utility Layer What Is Data Science? , Motivating Hypothetical: Data Science, Finding Key Connectors Linear algebra for data science 1. Algebraic view - vectors, matrices, product of matrix & vector, rank, null space, solution of over-determined set of equations and pseudo-inverse)	
2	**2.1 Three Management Layers Retrieve Stop, Assess Superstep:** Operational Management Layer, Processing-Stream Definition and Management, Audit, Balance, and Control Layer, Balance, Control, Yoke Solution, Cause-and-Effect, Analysis System, Functional Layer, Data Science Process Data Lakes, Data Swamps, Training the Trainer Model, Understanding the Business Dynamics of the Data Lake, Actionable Business Knowledge from Data Lakes, Engineering a Practical Retrieve Superstep, Connecting to Other Data Sources, Exploring Your Data, Cleaning and Munging, Manipulating Data, Rescaling, Dimensionality Reduction, Assess Superstep, Errors, Analysis of Data, Practical Actions, Engineering a Practical Assess Superstep,Manual Curation, Recommending What's Popular , User-Based Collaborative Filtering, Item-Based Collaborative Filtering Statistics (descriptive statistics, notion of probability, distributions, mean, variance, covariance, covariance matrix,understanding univariate and multivariate normal distributions, introduction to hypothesis testing, confidence interval for estimates)	15
3	**3.1 Introduction:** Introduction to Big Data, Characteristics of Data, and Big Data Evolution of Big Data, Definition of Big Data, Challenges with big data, Why Big data? Data Warehouse environment, Traditional Business Intelligence versus Big Data. State of Practice in Analytics, Key roles for New Big Data Ecosystems, Examples of big Data Analytics, Big Data Analytics, Introduction to big data analytics, Classification of Analytics, Challenges of Big Data, Importance of Big Data, Big Data Technologies, Data Science, Responsibilities, Soft state eventual consistency. Data Analytics Life Cycle	15
4	**4.1 Analytical Theory and Methods** Statistical & Probabilistic analysis of Data: Multiple hypothesis testing, Parameter Estimation methods, Confidence intervals, Bayesian statistics and Data Distributions, Introduction to machine learning: Supervised & unsupervised learning, classification & clustering Algorithms, Dimensionality reduction: PCA & SVD, Correlation & Regression analysis, Training & testing data: Over-fitting & Under fitting.	15

Reference Books (DataScience):

1) Practical Data Science, Andreas François Vermeulen, APress, 8th Edition, 2018.
2) Principles of Data Science, Sinan Ozdemir, PACKT, 2016
3) Data Science from Scratch first Principle in python, Joel Grus, 2017

Reference Books (BigData):

1) Big Data and Analytics, Seema Acharya, Wiley, First Edition
2) Data Analytics with Hadoop An Introduction for Data Scientists, Benjamin Bengfort and Jenny Kim, O'Reilly, 2016.
3) Big Data and Hadoop, V.K Jain, Khanna Publishing, First, 2018.

Part - 4 Detailed Scheme Practicals

Course Code: MS-FIT-1P1

Practical No	Details
1	Write a program for implementing Client Server communication model using TCP.
2	Write a program for implementing Client Server communication model using UDP.
3	A multicast Socket example
4	Write a program to show the object communication using RMI.
5	Implement Xen virtualization and manage with Xen Center
6.	Implement virtualization using VMWare ESXi Server and managing with vCenter
7	Develop application for Microsoft Azure.
8.	Develop application for Google App Engine
9.	Implement Windows Hyper V virtualization
10.	Show the implementation of web services.

Course Code: MS-FIT-1P2

Practical No	Details
1	Design an Expert system using AIML E.g: An expert system for responding the patient query for identifying the flu.
2	Design a bot using AIML.
3	Implement Bayes Theorem using Python
4	Implement Conditional Probability and joint probability using Python
5	Write a program for to implement Rule based system.
6.	Design a Fuzzy based application using Python / R.
7	Write an application to simulate supervised and un-supervised learning model.
8.	Write an application to implement clustering algorithm.
9.	Write an application to implement support vector machine algorithm.

10.	Simulate artificial neural network model with both feedforward and backpropagation approach. [You can add some functionalities to enhance the model].

Course Code: MS-FIT-1P3

Practical No	Details
1	Checking data integrity using simple parity check
2	Checking data integrity using Two-dimensional parity check
3	Fundamental of Computers a. IP address b. MAC address
4	Information gathering tool
5	Implementing Scanning Tool
6.	Implementing change in Linux policy using commands
7	Implement steganography using tools
8.	Using GNU PGP
9.	Understanding Buffer Overflow and Format String Attack
10.	Implementation of Networking Tools

Course Code: MS-FIT-1P4

Practical No	Details
1	Install, configure and run Hadoop and HDFS ad explore HDFS.
2	Implement word count / frequency programs using MapReduce
3	Implement an MapReduce program that processes a weather dataset.
4	Implement an application that stores big data in Hbase / MongoDB and manipulate it using R / Python
5	Implement the program in practical 4 using Pig.
6.	Prerequisites Data Science Practical. Creating data model using cassandra
7	Conversion from different formats to hours format: a.text delimited CSV format b.XML
8.	Conversion from different formats to hours format: a.Audio b.Video c. Picture
9.	Utilities and auditing
10.	Retrieving Data

Part 5 - The Scheme of Teaching and Examination is asunder:

Semester – II

Summary

Sr. No.	Choice Based Credit System			Subject Code	Remarks
1	Core Course (Information Technology)			MS-FIT-201,. MS-FIT-2P1,.	
2	Elective Course	Discipline Specific Elective (DSE) Course		MS-FIT-202, MS-FIT-203, MS-FIT-204 MS-FIT-205, MS-FIT-206, MS-FIT-207, MS-FIT-208, MS-FIT-209, MS-FIT-210.	
				MS-FIT-2P2, MS-FIT-2P3, MS-FIT-2P4 MS-FIT-2P5, MS-FIT-2P6, MS-FIT-2P7, MS-FIT-2P8 MS-FIT-2P9, MS-FIT-2P10.	
		2.1	Interdisciplinary Specific Elective (IDSE) Course		
		2.2	Dissertation/Project		

		2.3	Generic Elective (GE) Course		
3	Ability Enhancement Compulsory Courses (AECC)				
	Skill Enhancement Courses (SEC)				

First Year Semester –II Internal and External Detailed Evaluation Scheme

Sr. No.	Subject Code	Subject Title	Periods Per Week (Period of 45min)						Internals				Total Marks
			Units	S. L.	L	T	P	Credit	S. L. E	CT+ AT= 15+5	PA	SEE	
1	MS-FIT-201	Microservice Achitecture	4	20%*	5	0	0	4	10	20	10	60	100 (60+40)
2	**Track 1** MS-FIT-202	Aritificial Neural Networks	4	20%*	5	0	0	4	10	20	10	60	100 (60+40)
3	MS-FIT-203	Machine Learning	4	20%*	5	0	0						
4	MS-FIT-204	Robotic Process Automation	4	20%*	5	0	0						
2	**Track 2** MS-FIT-205	Security Assessment, Architecture & Design	4	20%*	5	0	0	4	10	20	10	60	100 (60+40)
3	MS-FIT-206	Digital Forensics & Incident Response	4	20%*	5	0	0						
4	MS-FIT-207	Penetration Testing	4	20%*	5	0	0						
2	**Track 3** MS-FIT-208	Statistical Thinking and Data Analysis	4	20%*	5	0	0	4	10	20	10	60	100 (60+40)
3	MS-FIT-209	Principles of Data Science	4	20%*	5	0	0						
4	MS-FIT-210	Data Science Implementation	4	20%*	5	0	0						
5	MS-FIT-2P1	Microservice Achitecture Practical	-	-	0	-	3	2					50
6	**Track 1** MS-FIT-2P2	Aritificial Neural Networks Practical	-	-	0	-	3	2					50
7	MS-FIT-2P3	Machine Learning Practical	-	-	0	-	3						
8	MS-FIT-2P4	Robotic Process Automation Practical	-	-	0	-	3						
9	**Track 2** MS-FIT-2P5	Security Assessment, Architecture & Design Practical	-	-	0	-	3	2					50
10	MS-FIT-2P6	Digital Forensics & Incident Response Practical	-	-	0	-	3						

11	MS-FIT-2P7	Penetration Testing Practical	-	-	0	-	3						
12	**Track 3** MS-FIT-2P8	Statistical Thinking and Data Analysis Practical	-	-	0	-	3	2					50
13	MS-FIT-2P9	Principles of Data Science Practical	-	-	0	-	3						
14	MS-FIT-2P10	Data Science Implementation Practical	-	-	0	-	3						
	Total Periods/ Credit		(25+45) per week/20						**24**				**600**

***One to two lectures to be taken for CONTINUOUS self -learning evaluation**

First Year Semester II – Units – Topics- Teaching Hours

S. N	Subject Code & Title	Subject Unit Title		Lectures (45 min)	Total Lectures	Credit	Total Marks
1	MS-FIT-201	1	Microservices: Understanding Microservices,	15	60 L	4	100 (60+40)
		2	Building Microservices with ASP.NET Core	15			
		3	Creating Data Service	15			
		4	Configuring Microservice Ecosystems	15			
2	**Track 1** MS-FIT-202	1	The brain metaphor	15	60 L	4	100 (60+40)
		2	Geometry of Binary Threshold Neurons and their Networks	15			
		3	Neural Networks : A Statistical Pattern Recognition Perspective	15			
		4	Dynamic Systems Review	15			
	MS-FIT-203	1	Introduction: Machine learning	15			
		2	Classification: Theory of Generalization: Linear Models	15			
		3	Logic Based and Algebraic Model Distance Based Models Rule Based Models Tree Based Model	15			
		4	Probabilistic Model	15			
	MS-FIT-204	1	Robotic Process Automation: Scope and techniques	15			
		2	Sequence, Flowchart, and Control Flow	15			
		3	Tame that Application with Plugins and Extensions	15			
		4	Managing and Maintaining the code	15			
3	**Track 2** MS-FIT-205	1	Security Assessments Security Architecture Basics Architecture patterns in security	15	60 L	4	100 (60+40)
		2	Cryptography Secure Communications	15			
		3	Middleware Security Web Security Application and OS Security Database Security	15			
		4	Security Components Security and Other Architectural Goals	15			
	MS-FIT-206	1	Incident Response Forensic Fundamentals Network Evidence Collection	15			
		2	Acquiring Host-Based Evidence Understanding Forensic Imaging : Network Evidence Analysis	15			
		3	Analyzing System Memory Analyzing System Storage : Forensic Reporting	15			
		4	Malware Analysis Threat Intelligence	15			
	MS-FIT-207	1	Introduction to Hacking Linux Basics Information Gathering Techniques	15			
		2	Target Enumeration and Port Scanning Technique Vulnerability Assessment Network Sniffing	15			
		3	Remote Exploitation. Client Side Exploitation	15			

			Postexploitation				
		4	Windows Exploit Development Basics Wireless Hacking Web Hacking	15			
4	**Track 3** MS-FIT-208	1	Introduction Introduction to statistical Analysis		60 L	4	100 (60+40)
		2	Random Variables and Probability Distribution Markov chains				
		3	Hypothesis Testing: Linear Regression and Correlation				
		4	Design of Experiments Time series and forecasting	15			
	MS-FIT-209	1	Introduction Statistical Inference	15	60 L		
		2	Exploratory Data Analysis and the Data Science Process Three Basic Machine Learning Algorithms One More Machine Learning Algorithm and Usage in Applications	15			
		3	Feature Generation and Feature Selection Mining Social-Network Graphs	15			
		4	Data Visualization Data Science and Ethical Issues	15			
	MS-FIT-210	1	Data science technology stack	15			
		2	Business Layer	15			
		3	Retrieve Superstep	15			
		4	Transform Superstep	15			
5	MS-FIT-2P1	1			36 L	2	50

6	**Track 1** MS-FIT-2P2	2	Artificial Neural Networks Practical		36 L	2	50
7	MS-FIT-2P3	3	Machine Learning Practical		36 L		
8	MS-FIT-2P4	4	Robotic Process Automation Practical		36 L		
9	**Track 2** MS-FIT-2P5	5	Security Assessment, Architecture & Design Practical		36 L	2	50
10	MS-FIT-2P6		Digital Forensics & Incident Response Practical		36 L		
11	MS-FIT-2P7		Penetration Testing Practical		36 L		
12	**Track 3** MS-FIT-2P8		Statistical Thinking and Data Analysis Practical		36 L	2	50
13	MS-FIT-2P9		Principles of Data Science Practical		36 L		
14	MS-FIT-2P10		Data Science Implementation Practical		36 L		
			TOTAL			24	**600**

- Lecture Duration – 48 Minutes

- **One Credit =15 Hours**

L: Lecture: Tutorials P: Practical Ct-Core Theory, Cp-Core Practical, SLE- Self learning evaluation CT-Commutative Test, SEE- Semester End Examination, PA-Project Assessment, AT- Attendance

Part 6: Detailed Scheme Theory
SEMESTER 2

Course Code: MS-FIT-201 Microservices Architecture

Unit	Details	No. of Lectures
1	**1.1 Microservices:** Understanding Microservices, Adopting Microservices, The Microservices Way. **1.2Microservices Value Proposition:** Deriving Business Value, defining a Goal-Oriented, Layered Approach, Applying the Goal-Oriented, Layered Approach. **1.3 Designing Microservice Systems:** The Systems Approach to Microservices, A Microservices Design Process, **1.4 Establishing a Foundation:** Goals and Principles, Platforms, Culture Service Design: Microservice Boundaries, API design for Microservices, Data and Microservices, Distributed Transactions and Sagas, Asynchronous Message-Passing and Microservices, dealing with Dependencies System Design and Operations: Independent Deployability, More Servers, Docker and Microservices, Role of Service Discovery, Need for an API Gateway, Monitoring and Alerting **1.5 Adopting Microservices in Practice:** Solution Architecture Guidance, Organizational Guidance, Culture Guidance, Tools and Process Guidance, Services Guidance	15
2	**2.1 Building Microservices with ASP.NET Core:** Introduction, Installing .NET Core, Building a Console App, Building ASP.NET Core App. Delivering Continuously: Introduction to Docker, Continuous integration with Wercker, Continuous Integration with Circle CI, Deploying to Dicker Hub. Building **2.2 Microservice with ASP.NET Core:** Microservice, Team Service, API First Development, Test First Controller, Creating a CI pipeline, Integration Testing, Running the team service Docker Image. **2.3 Backing Services:** Microservices Ecosystems, Building the location Service, Enhancing Team Service	15
3	**3.1 Creating Data Service:** Choosing a Data Store, Building a Postgres Repository, Databases are Backing Services, Integration Testing Real Repositories, Exercise the Data Service. **3.2 Event Sourcing and CQRS:** Event Sourcing,	15

	CQRS pattern, Event Sourcing and CQRS, Running the samples. **3.3 Building an ASP.NET Core Web Application:** ASP.NET Core Basics, Building Cloud-Native Web Applications. **3.4 Service Discovery:** Cloud Native Factors, Netflix Eureka, Discovering and Advertising ASP.NET Core Services. DNS and Platform Supported Discovery	
4	**4.1 Configuring Microservice Ecosystems:** Using Environment Variables with Docker, Using Spring Cloud Config Server, Configuring Microservices with etcd, **4.2 Securing Applications and Microservices:** Security in the Cloud, Securing ASP.NET Core Web Apps, Securing ASP.NET Core Microservices **4.3 Building Real-Time Apps and Services:** Real-Time Applications Defined, Websockets in the Cloud, Using a Cloud Messaging Provider, Building the Proximity Monitor **4.4 Putting It All Together:** Identifying and Fixing Anti-Patterns, Continuing the Debate over Composite Microservices, The Future	15

TRACK 1 Artificial Intelligence

Course Code: MS-FIT-202 Artificial Neural Networks

Unit	Details	No of lectures
UNIT 1	**1.1 The brain metaphor** **1.2 Basics of neuroscience** **1.3 Artificial neurons** **1.4 Neural networks and architectures**	15
Unit 2	**2.1 Geometry of Binary Threshold Neurons and their Networks** **2.2 Supervised Learning 1 : Perceptrons and LMS** **2.3 Supervised Learning 2 : Back Propogation and Beyond**	15
Unit 3	**3.1 Neural Networks : A Statistical Pattern Recognition Perspective** **3.2 Statistical Learning Theory** **3.3 Support Vector Machines** **3.4 Radial Basis Functions** **3.5 Practical based on NLKT**	15
Unit 4	**4.1 Dynamic Systems Review** **4.2 Attractor Neural Networks** **4.3 Adaptive Resonance Theory** **4.4 Toward Self Organizing Feature Map** **4.5 Fuzzy Sets and Fuzzy Systems** **4.6 Evolutionary Algorithms**	15

All practicals can be done using R/Matlab/Python

1. Neural Networks, A Classroom Approach, Satish Kumar, second edition, McGraw Hill
2. Artificial Neural Networks, Robert Schalkoff, Mc Graw Hill
3. Introduction to Neural Networks using MATLAB, S Sivanandam, S Sumathi, McGraw Hill

TRACK 1 Artificial Intelligence

Course Code: MS-FIT-203 Machine Learning

Unit	Details	No of lecture
1	**1.1 Introduction:** Machine learning, Examples of Machine Learning Problems, Structure of Learning, learning versus Designing, Training versus Testing, Characteristics of Machine learning tasks, Predictive and descriptive tasks, **1.2 Machine learning Models:** Geometric Models, Logical Models, Probabilistic Models. **1.3** Features: Feature types, Feature Construction and Transformation, Feature Selection	15
2	**2.1 Classification:** Binary Classification- Assessing Classification performance, Class probability Estimation Assessing class probability Estimates, Multiclass Classification. **2.2 Assessing performance of Regression**- Error measures, Overfitting- Catalysts for Overfitting, Case study of Polynomial Regression. **2.3 Theory of Generalization:** Effective number of hypothesis, Bounding the Growth function, VC Dimensions, Regularization theory. **2.4 Linear Models:** Least Squares method, Multivariate Linear Regression, Regularized Regression, Using Least Square regression for Classification. Perceptron, Support Vector Machines, Soft Margin SVM, Obtaining probabilities from Linear classifiers, Kernel methods for non-Linearity	15
3	**3.1 Logic Based and Algebraic Model:** Neighbours and Examples, Nearest Neighbours Classification, **3.2 Distance Based Models:** Distance based clustering-K means Algorithm, Hierarchical clustering, **3.3 Rule Based Models:** Rule learning for subgroup discovery, Association rule mining. **3.4 Tree Based Model:** Decision Trees, Ranking and Probability estimation Trees, Regression trees, Clustering Trees.	15
4	**4.1 Probabilistic Model:** Normal Distribution and Its Geometric Interpretations, Naïve Bayes Classifier, Discriminative learning with Maximum likelihood, Probabilistic Models with Hidden variables: Estimation-Maximization Methods, Gaussian Mixtures, and Compression based Models **4.2 Trends In Machine Learning:** Model and Symbols Bagging and Boosting, Multitask learning, Online learning and Sequence Prediction, Data Streams and Active Learning, Deep Learning, Reinforcement Learning	15

Reference Books:

1. Machine Learning: The Art and Science of Algorithms that Make Sense of Data, Peter Flach, Cambridge University, 2012
2. Introduction to Statistical Machine Learning with Application in R, Hastie, TIbshirani, Friedman, Springer, second edition, 2012
3. Introduction to Machine Learning, Ethem Alpaydin, PHI, second edition, 2013

TRACK 1 Artificial Intelligence

Course Code: MS-FIT-204 Robotic Process Automation

Unit	Details	No of lectures
UNIT 1	**1.1 Robotic Process Automation:** Scope and techniques of automation, About UiPath **1.2 Record and Play:** UiPath stack, Downloading and installing UiPath Studio, Learning UiPath Studio, Task recorder, Step-by-step examples using the recorder.	15
UNIT 2	**2.1 Sequence, Flowchart, and Control Flow:** Sequencing the workflow, Activities, Control flow, various types of loops, and decision making, Step-by-step example using Sequence and Flowchart, Step-by-step example using Sequence and Control flow **2.2 Data Manipulation:** Variables and scope, Collections, Arguments – Purpose and use, Data table usage with examples, Clipboard management, File operation with step-by-step example, CSV/Excel to data table and vice versa (with a step-by-step example) Taking Control of the Controls: Finding and attaching windows, Finding the control, Techniques for waiting for a control, **2.3 Act on controls** – mouse and keyboard activities, Working with UiExplorer, Handling events, Revisit recorder, Screen Scraping, When to use OCR, Types of OCR available, How to use OCR, Avoiding typical failure points	15

UNIT 3	**3.1 Tame that Application with Plugins and Extensions:** Terminal plugin, SAP automation, Java plugin, Citrix automation, Mail plugin, PDF plugin, Web integration, Excel and Word plugins, Credential management, Extensions – Java, Chrome, Firefox, and Silverlight **3.2 Handling User Events and Assistant Bots:** What are assistant bots?, Monitoring system event triggers, Hotkey trigger, Mouse trigger, System trigger ,Monitoring image and element triggers, An example of 12 CO4 36 monitoring email, Example of monitoring a copying event and blocking it, Launching an assistant bot on a keyboard event **3.3 Exception Handling, Debugging, and Logging:** Exception handling, Common exceptions and ways to handle them, Logging and taking screenshots, Debugging techniques, Collecting crash dumps, Error reporting	15
UNIT 4	**4.1 Managing and Maintaining the Code:** Project organization, Nesting workflows, Reusability of workflows, Commenting techniques, State Machine, When to use Flowcharts, State Machines, or Sequences, Using config files and examples of a config file, Integrating a TFS server **4.2 Deploying and Maintaining the Bot:** Publishing using publish utility, Overview of Orchestration Server, Using Orchestration Server to control bots, Using Orchestration Server to deploy bots, License management, Publishing and managing updates **4.3 Introduction to RPA Tools**.	15

Reference Books:

1. Learning Robotic Process Automation, Alok Mani Tripathi, Packt, first edition, 2018
2. Robotic Process Automation Tools, Process Automation and their benefits: Understanding RPA and Intelligent Automation, Srikanth Merianda, Createspace Independent Publishing, first edition, 2018
3. The Simple Implementation Guide to Robotic Process Automation (Rpa): How to Best Implement Rpa in an Organization, Kelly Wibbenmeyer, iUniverse, first edition, 2018

TRACK 2 Security

Course Code: MS-FIT-205 Security Architecture And Design

Unit	Details	No of lectures
1	**1.1 Security Assessments** What Is a Security Assessment? The Organizational Viewpoint The Five-Level Compliance Model The System Viewpoint Pre-Assessment Preparation The Security Assessment Meeting Security Assessment Balance Sheet Model Describe the Application Security Process Identify Assets Identify Vulnerabilities and Threats Identify Potential Risks Examples of Threats and Countermeasures Why Are Assessments So Hard? Matching Cost Against Value Why Assessments Are Like the Knapsack Problem Why Assessments Are Not Like the Knapsack Problem Enterprise Security and Low Amortized Cost Security Controls **1.2 Security Architecture Basics** Security As an Architectural Goal Corporate Security Policy and Architecture Vendor Bashing for Fun and Profit Security and Software Architecture System Security Architecture Definitions Security and Software Process Security Design Forces against Other Goals1Security Principles Additional Security-Related Properties Other Abstract or Hard-to-Provide Properties Inference Aggregation Least Privilege Self-Promotion Graceful Failure Safety Authentication User IDs and Passwords Tokens Biometric Schemes Authentication Infrastructures Authorization Models for Access Control Mandatory Access Control Discretionary Access Control Role-Based Access Control Access Control Rules Understanding the Application's Access Needs Other Core Security Properties Analyzing a Generic System **1.3 Architecture patterns in Security** Pattern Goals Common Terminology Architecture Principles and Patterns The Security Pattern Catalog Entity Principal Context Holders Session Objects and Cookies Ticket/Token Sentinel Roles Service Providers Directory Trusted Third Party Validator Channel Elements Wrapper Filter Interceptor Proxy Platforms Transport Tunnel Distributor Concentrator Layer Elevator Sandbox Magic Conclusion	15
2	LOW LEVEL ARCHITECTURE **2.1 Code Review** Why Code Review Is Important, **2.2 Cryptography** The History of Cryptography Cryptographic Toolkits One-Way Functions Encryption Symmetric Encryption Encryption Modes Asymmetric Encryption Number Generation Cryptographic Hash Functions Keyed Hash Functions Authentication and Digital Certificates	15

	Digital Signatures Signed Messages Digital Envelopes Key Management Cryptanalysis Differential Cryptanalysis Linear Cryptanalysis Cryptography and Systems Architecture Innovation and Acceptance Cryptographic Flaws Algorithmic Flaws Protocol Misconstruction Implementation Errors Wired Equivalent Privacy Performance Comparing Cryptographic Protocols **2.3 Secure Communications** The OSI and TCP/IP Protocol Stacks The Structure of Secure Communication The Secure Sockets Layer Protocol SSL Properties The SSL Record Protocol The SSL Handshake Protocol SSL Issues The IPSec Standard IPSec Architecture Layers IPSec Overview Policy Management IPSec Transport and Tunnel Mod IPSec Implementation Authentication Header ProtocolEncapsulating Security Payload Internet Key Exchange Some Examples of Secure IPSec Datagrams IPSec Host Architecture IPSec Issues	
3	MID LEVEL ARCHITECTURE **3.1 Middleware Security** Middleware and Security Service Access Service Configuration Event Management Distributed Data Management Concurrency and SynchronizationReusable Services The Assumption of Infallibility The Common Object Request Broker Architecture The OMG CORBA Security Standard The CORBA Security Service Specification Packages and Modules in the Specification Vendor Implementations of CORBA Security CORBA Security Levels Secure Interoperability The Secure Inter-ORB Protocol Secure Communications through SSL Why Is SSL Popular? Application-Unaware Security Application-Aware Security Application Implications Conclusion Adversarial Simulation **3.2 Web Security** Web Security Issues Questions for the Review of Web Security Web Application Architecture Web Application Security OptionsSecuring Web Clients Active Content Scripting Languages Browser Plug-Ins and Helper Applications Browser Configuration Connection Security Web Server Placement Securing Web Server Hosts Securing the Web Server Authentication Options Web Application Configuration Document Access Control CGI Scripts JavaScript Web Server Architecture Extensions Enterprise Web Server Architectures The Java 2 Enterprise Edition StandardServer-Side JavaJava Servlets Servlets and Declarative Access Control Enterprise Java Beans Conclusion **3.3 Application and OS Security** Structure of an Operating System Structure of an Application Application Delivery Application and Operating System Security Hardware Security Issues Process Security Issues Software Bus Security Issues Data Security Issues Network Security Issues	15

	Configuration Security Issues Operations, Administration, and Maintenance Security Issues Securing Network Services UNIX Pluggable Authentication Modules UNIX Access Control Lists Solaris Access Control Lists HP-UX Access Control Lists **3.4 Database Security** Database Security EvolutionMulti-Level Security in DatabasesArchitectural Components and Security Secure Connectivity to the Database Role-Based Access Control The Data Dictionary Database Object Privileges Issues Surrounding Role-Based Access Control Database Views Security Based on Object-Oriented Encapsulation Procedural Extensions to SQL Wrapper Sentinel Security through Restrictive Clauses Virtual Private Database Oracle Label Security ad and Write Semantics	
4	HIGH LEVEL Architecture **4.1 Security Components** Secure Single Sign-On Scripting Solutions Strong, Shared Authentication Network Authentication Secure SSO Issues Public-Key Infrastructures Certificate Authority Registration Authority Repository Certificate Holders Certificate Verifiers PKI Usage and Administration PKI Operational Issues Firewalls Firewall Configurations Firewall Limitations Intrusion Detection Systems LDAP and X.500 Directories Lightweight Directory Access Protocol Architectural Issues Kerberos Kerberos Components in Windows 2000 Distributed Computing Environment The Secure Shell, or SSH The Distributed Sandbox Conclusion **4.2 Security and Other Architectural Goals** Metrics for Non-Functional Goals Force Diagrams around Security Normal Architectural Design Good Architectural Design 3High Availability Security Issues Robustness Binary Patches Security Issues Reconstruction of Events Security Issues Ease of Use Security Issues Maintainability, Adaptability, and Evolution Security Issues Scalability Security Issues Interoperability Security Issues Performance Security Issues Portability Security Issues **4.3 Enterprise Security Architecture** Security as a Process Applying Security Policy Security Data Databases of Record Enterprise Security as a Data Management Problem The Security Policy Repository The User Repository The Security Configuration Repository The Application Asset Repository The Threat Repository The Vulnerability Repository Tools for Data Management Automation of Security Expertise Directions for Security Data Management David Isenberg and the “Stupid Network” Extensible Markup Language XML and Data Security The XML Security Services Signaling Layer XML and Security Standards J2EE Servlet Security Specification XML Signatures XML Encryption S2ML SAML XML Key Management Service XML and Other Cryptographic Primitives 368 The Security Pattern Catalog Revisited XML-Enabled Security Data HGP: A Case Study in Data Management 371 Building a Single Framework for Managing Security	15

Reference Books:

1. Ross Anderson, Security Engineering 2nd 3rd Edition.
2. Charles P. Pfleeger, Security in Computing, 5th Edition, Prentice Hall, 2015, ISBN-10: 0134085043, Recommended.
3. The Official (ISC)² CISSP CBK Reference, 5th Edition by John Warsinske, Mark Graff, Kevin Henry, Christopher Hoover, Ben Malisow, Sean Murphy, C. Paul Oakes, George Pajari, Jeff T. Parker, David Seidl, Mike Vasquez, Publisher: Sybex (2019)
4. Enterprise Security Architecture: A Business-Driven Approach by Nicholas A Sherwood
5. Enterprise Information Security Architecture A Complete Guide by Gerardus Blokdyk
6. Designing Security Architecture Solutions by Jay Ramachandran
7. https://security-and-privacy-reference-architecture.readthedocs.io/en/latest/index.html

TRACK 2 Security

Course Code: MS-FIT-206 Digital Forensics, Incident Response & Malware Analysis

1	**1.1 An Introduction to Digital Forensics** Forensics Fundamentals ; Computer Forensics and Law Enforcement- Indian Cyber Forensic - Forensics Services, Professional Forensics Methodology- Types of Forensics Technology Forensics system and Services : Forensics on - Internet Usage – Intrusion - Firewall and Storage Area Network; Occurrence of Cyber-crimes- Cyber Detectives- Fighting Cyber Crimes- Forensic Process, Legal aspects Laws and regulations Rules of evidence Digital forensic fundamentals A brief history The digital forensic process Identification Preservation Collection Proper evidence handling Chain of custody Examination Analysis Presentation Digital forensic lab Physical security Tools Hardware, Data Backup and Recovery - Test Disk Suite, Data-Recovery Solution, Hiding and Recovering Hidden data, Evidence Collection and Data Seizure **1.2 An Introduction to Incident Response** The incident response process the role of digital forensics The incident response framework The incident response charter CSIRT CSIRT core team Technical support personnel Organizational support personnel External resources The incident response plan Incident classification The incident response playbook Escalation procedures Maintaining the incident response capability,
2	**THE FORENSICS PROCESS** **2.1 Network Evidence Collection** Preparation Network diagram Configuration Logs and log management Network device evidence Security information and event management system Security onion Packet capture tcpdump WinPcap and RawCap Wireshark Evidence collection **2.2 Acquiring Host-Based Evidence** Digital Repositories - Evidence Collection – Data Preservation Approaches – Meta Data and Historic records – Legal aspects , Preparation Evidence volatility Evidence acquisition Evidence collection procedures Memory acquisition Local acquisition FTK Imager Winpmem Remote acquisition Winpmem F-Response Virtual machinesNon-volatile data **2.3 Understanding Forensic Imagin**g Overview of forensic imaging Preparing a stage drive Imaging Dead imaging Live imaging Imaging with Linux **2.4 Network Evidence Analysis** Analyzing packet captures Command-line tools Wireshark Xplico and CapAnalysis Xplico CapAnalysis Analyzing network log files DNS blacklists SIEM ELK Stack **2.5 Analyzing System Memory** Memory evidence overview Memory analysis Memory analysis methodology SANS six-part methodology Network connections methodology Tools Redline Volatility Installing Volatility Identifying the image pslist psscan pstree DLLlist Handles svcscan netscan and sockets LDR modules psxview Dlldumpmemdump procdump Rekall imageinfo pslist Event logs Sockets Malfind **2.6 Analyzing System Storage** Forensic platformsAutopsy Installing Autopsy Opening a case Navigating Autopsy Examining a Case Web Artifacts Email Attached Devices Deleted Files Keyword Searches timeline Analysis Registry analysis

	Basic Steps of Forensic Analysis in Windows and Linux – Forensic Scenario – Email Analysis – File Signature Analysis – Hash Analysis – Forensic Examination of log files **2.7 Forensic Reporting** Documentation overview What to document Types of documentation Sources Audience Incident trackingFast incident response Written reports Executive summaryIncident report Forensic report Overview of different software packages – Encase-Autopsy-Magnet – Wireshark - Mobile Forensic Tools – SQLite Case study Report Preparation A real Forensic case study – Processing a complete Forensic case – Preparing Forensic Report Working with cloud vendors, obtaining evidence, reviewing logs and APIs, Introduction to Mobile Forensic – Android Device – Analysis- Android Malware – iOS Forensic Analysis – SIM Forensic Analysis – Case study
3	**3.1 Cyber security Incident Management** The Cyber security Incident Chain, Stakeholders, Cyber security Incident Checklist. Five Phases of Cyber security Incident Management: Plan and Prepare, Detect and Report, Assess and Decide, Respond and Post-Incident Activity. Handling an Incident: Preparation: Preparing to Handle Incidents, Preventing Incidents. Detection and Analysis: Attack Vectors, Signs of an Incident, Sources of Precursors and Indicators, Incident Analysis, Incident Documentation, Incident Prioritization& Incident Notification. Coordination and Information Sharing: Coordination: Coordination Relationships, Sharing Agreements and Reporting Requirements. Information Sharing Techniques: Ad Hoc, Partially Automated, Security Considerations. Granular Information Sharing: Business Impact Information, Technical Information. Containment, Eradication, and Recovery: Choosing a Containment Strategy, Evidence Gathering and Handling, Identifying the Attacking Hosts, Eradication and Recovery. Post-Incident Activity: Lessons Learned, Using Collected Incident Data, Evidence Retention. **3.2 Threat Modeling** Threat modelling process and its benefits: Identifying the Threats by Using Attack Trees and rating threats using DREAD, Risk Mitigation Techniques and Security Best Practices. Security techniques, authentication, authorization. Defence in Depth and Principle of Least Privilege. **3.3 Data Backup and Recovery** Test Disk Suite, Data-Recovery Solution, Hiding and Recovering Hidden data, Evidence Collection and Data Seizure. Digital Repositories - Evidence Collection – Data Preservation Approaches – Meta Data and Historic records – Legal aspects Containment, Eradication, and Recovery: Choosing a Containment Strategy, Evidence Gathering and Handling, Identifying the Attacking Hosts, Eradication and Recovery. Post-Incident Activity: Lessons Learned, Using Collected Incident Data, Evidence Retention.
4	**4.1 Malware Analysis** Malware Analysis: Introduction, What is Malware Analysis? The Goals of Malware Analysis. Malware Analysis Techniques. Basic Static Analysis, Basic Dynamic Analysis, Advanced Static Analysis, Advanced Dynamic Analysis, Malware taxonomy - Malware threats - Malware analysis methodologies - Legal considerations - Identifying and protecting against malware - Malware hiding places - Collecting malware from live system - Identifying malware in dead system Malware Analysis Environment : Virtual machine - Real systems, Types of Malware, General Rules for Malware Analysis, Malware

	Functionality, Downloaders and Launchers, Backdoors, Reverse Shell, RATs, Botnets, RATs and Botnets Compared, Credential Stealers, INA Interception, Hash Dumping, Keystroke Logging, Persistence Mechanisms, Trojanized System, Binaries, DLL Load-Order Hijacking, Privilege Escalation Using SeDebugPrivilege, Covering Its Tracks-User-Mode Rootkits, IAT Hooking, Inline Hooking, Tools for malware analysis, ApateDNS, Autoruns, BinDiff, BinNavi, Deep Freeze, Pestudio, Volatility, Remnux Dynamic analysis Process Explorer, Cuckoo sandbox, IDA Pro, ProcMon, CFF Explorer, ProcExplore, BinText, FileAlyzer, OllyDbg **4.2 Threat Intelligence** Open Source and Competitive Intelligence, Privacy, Snooping on People Through Open Sources, Web Browsing, Privacy Regulations, Piracy, Copyright Infringement, Trademark Infringement, Dark Web, Deep Web, Web Scraping to gather Hidden Data, Correlating OSINT, Threat intelligence overview Threat intelligence types Threat intelligence methodology Threat intelligence direction Cyber kill chain Diamond model Threat intelligence sources Internally developed sources Commercial sourcing Open source Threat intelligence platforms MISP threat sharing 280 Using threat intelligence Proactive threat intelligence 2 Reactive threat intelligence Autopsy Redline Yara and Loki Insight VM

Reference books:

1. Digital forensics and incident response by Gerard Johansen
2. Enterprise Security Architecture: A Business-Driven Approach by John Sherwood, Andrew Clark, David Lynas
3. Practical Packet Analysis by Chris Sanders
4. The Art of Memory Forensics by Michael Hale Ligh, Andrew Case, Jamie Levy and Aaron Walters
5. Open Source Intelligence Techniques (2019) by Michael Bazzell
6. Investigating Windows Systems by Harlan Carvey
7. Practical Malware Analysis by Michael Sikorski & Andrew Honig
8. Intelligence Driven Incident Response by Scott Roberts & Rebekah Brown
9. Blue Team Field Manual by Alan White & Ben Clark
10. File System Forensic Analysis by Brian Carrier
11. Real Digital Forensics: Computer Security and Incident Response by Keith Jones, Richard Bejtlich, Curtis Rose
12. Digital Forensics with Open Source Tools by Cory Altheide, Harlan Carvey
13. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics by John Sammons
14. Warren G. Kruse II and Jay G. Heiser, "Computer Forensics: Incident Response Essentials", Addison Wesley, 2002.
15. The Practice of Network Security Monitoring – Understanding Incident Detection and Response by by Richard Bejtlich
16. Malware Analyst's Cookbook: Tools and Techniques for Fighting Malicious Code by Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard
17. K. Dunham and S. Abu-Nimeh, Mobile Malware Attacks and Defense. Washington, DC, United States: Syngress Media

TRACK 2 Security

Course Code: MS-FIT-207 Penetration Testing

Unit	Details	No of lectures
1	**Basics of Vulnerability Assessment & Penetration Testing** **1.1 Vulnerability Assessment and Penetration Testing (VPAT):** Introduction, Benefits, Methodology, Vulnerability Assessment, Reasons for Vulnerability Existence, Steps for Vulnerability Analysis, Web Application Vulnerabilities, Types: SQL-Injection, Blind Injection Detection, Cross-Site Scripting, Broken Authentication & Session Management, Insecure Direct Object References, Failure to Restrict URL, Remote Code Execution. Vulnerability Assessment Using Acunetix, Working of Vulnerability Assessment Tool, OWASP, OWASP Top10 **1.2 Penetration Testing Overview:** What is Penetration Testing? When to Perform Penetration Testing? How is Penetration Testing Beneficial? Penetration Testing Method: Steps of Penetration Testing Method, Planning & Preparation, Reconnaissance, Discovery, Analyzing Information and Risks, Active Intrusion Attempts, Final Analysis, Report Preparation. Penetration Testing Vs. Vulnerability Assessment, Penetration Testing, Vulnerability Assessment, and Which Option is Ideal to Practice? Types of Penetration Testing: Types of Pen Testing, Black Box Penetration Testing. White Box Penetration Testing, Grey Box Penetration Testing, Areas of Penetration Testing. Penetration Testing Tools, Limitations of Penetration Testing, Conclusion	15
2	**Methodologies** **2.1 Project Management Body of Knowledge** **2.2 Information System Security Assessment Framework** **2.3 Open Source Security Testing Methodology Manual**	15
3	**Penetration Testing Process** **3.1 Pre-Engagement Interactions** Passive Information Gathering (Web Presence, Corporate Data, WHOIS and DNS Enumeration, Additional Internet Resources), Active Information Gathering (DNS Interrogation, E-mail Accounts, Perimeter Network Identification, Network Surveying) **3.2 Reconnaisance** Vulnerability Discovery Methodologies, What is Fuzzing, Fuzzing Methods and Fuzzer Types, Data Representation and Analysis, Requirements for Effective Fuzzing. Automation and Data Generation, Environment Variable and Argument Fuzzing, Environment Variable and Argument Fuzzing: Automation, Web Application and Server Fuzzing, Web Application and Server Fuzzing: Automation, File Format Fuzzing, File Format Fuzzing: Automation on UNIX, File Format Fuzzing: Automation on Windows, Network Protocol Fuzzing, Network Protocol Fuzzing: Automation on UNIX, Network Protocol Fuzzing: Automation on Windows, Web Browser Fuzzing, Web Browser Fuzzing: Automation, In-Memory Fuzzing, In-Memory Fuzzing: Automation. - Fuzzing Frameworks, Automated Protocol Dissection, Fuzzer Tracking, Intelligent Fault Detection. **3.3 Vulnerability Identification** Port Scanning, Target Verification, UDP Scanning, TCP Scanning, Perimeter Avoidance Scanning, System Identification, Active OS Fingerprinting, Passive OS	15

	Fingerprinting, Services Identification, Banner Grabbing, Enumerating Unknown Services, Vulnerability Analysis **3.4 Vulnerability Verification** Exploit Codes – Finding and Running (Internet Sites & Automated Tools), Exploit Codes – Creating Your Own (Fuzzing, Code Review & Reverse Engineering), Web Hacking (SQL Injection, Cross-Site Scripting & Web Application Vulnerabilities). Project Management -- Executing Process Phase, Monitoring and Control Process **3.5 Exploitation** System Enumeration (Internal Vulnerabilities, Sensitive Data), Network Packet Sniffing, Social Engineering (Baiting, Phishing, Pretexting), Wireless Attacks (Wi-Fi Protected Access Attack, WEP Attack & similar) **3.6 Post-Exploitation** Maintaining Access (Shells and Reverse Shells, Encrypted Tunnels, Other Encryption and Tunnel Methods), Covering Your Tracks (Manipulating Log Data, Hiding Files) **3.7 Reporting** What Should You Report? (Out of Scope Issues, Findings, Solutions, Manuscript Preparation), Initial Report (Peer Reviews, Fact Checking, Metrics), Final Report (Peer Reviews, Documentation) **3.8 Archiving** Should You Keep Data from a Pentest? (Legal Issues, E-mail, Findings and Reports), Securing Documentation (Access Controls, Archival Methods, Archival Locations, Destruction Policies), Archiving Lab Data, Creating and Using System Images (VMs), Creating a "Clean Shop", Creating a Risk Management Register, Prioritization of Risks and Responses, Creating a Knowledge Database, Sanitization of Findings, Project Management Knowledge Database, Project Assessments, Team Assessments, Training Proposals	
4	**ADVANCED CONCEPTS** **4.1 Social Engineering** Social Engineering: Social Engineering, Overview, Definition(s) of Social Engineering. The Social Engineering Life Cycle: Foot printing, Establishing Trust, Psychological Manipulation, The Exit. Social Engineering Attack Cycle: Research, Developing Rapport and Trust, Exploiting Trust Factor, Exploiting Trust Factor, Recruit & Cloak, Evolve/Regress. The Weapons of a Social Engineer: Shoulder Surfing, Dumpster Diving, Role playing, Trojan horses, Phishing, Surfing Organization Websites & Online forums, Reverse Social Engineering. Different Types of Social Engineering: Physical Social Engineering, Remote Social Engineering, Computer-based Social Engineering, Social Engineering by Email, Phishing, Nigerian 419 or advance-fee fraud scam, Popup windows **4.2 SCADA & DCS Security** Scada Basics- Scada and ICS Architecture, PLC and HMI Basics, RTOS - real time operating systems Scada Related Protocols- Modbus RTU, Modbus TCP/IP, DNP3, DNP3 TCP/IP, OPC DA/HAD, SCADA protocol fuzzing Finding Vulnerabilities in HMI software- Buffer Overflows, Shellcode Previous attacks Analysis- Stuxnet, Duqu. Hardware Testing- Jtag, GNU/Radio for Exploiting Radio Frequencies, SCADA RTOS firmware reversing	15

	4.3 Advanced Linux Exploitation Linux heap management, constructs, and environment, Navigating the heap, Abusing macros such as unlink() and frontlink(), Function pointer overwrites, Format string exploitation, Abusing custom doubly-linked lists, Defeating Linux exploit mitigation controls, Using IDA for Linux application exploitation, Patch Diffing, one day Exploits and Return Oriented Shellcode, The Microsoft patch management process and Patch Tuesday, Obtaining patches and patch extraction, Binary diffing with BinDiff, patchdiff2, turbodiff, and darungrim, Visualizing code changes and identifying fixes, Reversing 32-bit and 64-bit applications and modules, Triggering patched vulnerabilities, Writing one-day exploits, Handling modern exploit mitigation controls. **4.4 Windows Kernel Debugging and Exploitation** Understanding the Windows Kernel, Navigating the Windows Kernel, Modern Kernel protections, Debugging the Windows Kernel, WinDbg, Analysing Kernel vulnerabilities and Kernel vulnerability types, Kernel exploitation techniques. **4.5 Windows Heap Overflows and Client-Side Exploitation** Windows heap management, constructs, and environment, Browser-based and client-side exploitation, Remedial heap spraying, Understanding C++, vftable/vtable behavior, Modern heap spraying to determine address predictability, Use-After-Free attacks and dangling pointers, Determining exploitability, Defeating ASLR, DEP, and other common exploit mitigation controls **4.6 Android Exploitation** Android Basics, Android Security Model, Introduction to ARM, Android Development Tools, Engage with Application Security, Android Security Assessment Tools, Exploiting Applications, Protecting Applications, Secure Networking, Native Exploitation and Analysis. **4.7 iOS exploitation** Introduction to iOS hacking, iOS User Space Exploitation, iOS Kernel Debugging and Exploitation	

=

Reference Books:

1. Penetration Testing A hands on Introduction to hacking by Georgia Weidman
2. ETHICAL HACKING AND PENETRATION TESTING GUIDE by RAFAY BALOCH
3. Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Thomas Wilhelm
4. “Linux Basics for Hackers” by OccupyTheWeb
5. Professional Penetration Testing Creating and Operating a Formal Hacking Lab by Thomas Wilhelm
6. “The Basics of Hacking & Penetration Testing” by Patrick Engebreston
7. “The Hacker PlayBook 2” and “The Hacker PlayBook 3” by Peter Kim
8. “Red Team Field Manual” by Ben Clark
9. “Metasploit: The Penetration Tester’s Guide” by David Kennedy, Devon Kearns, Jim O’Gorman and Mati Aharoni
10. “Black Hat Python” by Justin Seitz
11. “The Web Application Hacker’s Handbook” by Dafydd Stuttard and Marcus Pinto
12. Gray Hat Hacking: The Ethical Hacker's Handbook, Latest Edition by Allen Harper, Daniel Regalado, et al.
13. Hacking: The Art of Exploitation, 2nd Edition by Jon Erickson
14. The Database Hacker's Handbook: Defending Database Servers by David Litchfield , Chris Anley, et al.
15. The Browser Hacker's Handbook by Wade Alcorn , Christian Frichot , et al.
16. The Mobile Application Hacker's Handbook by Dominic Chell , Tyrone Erasmus , et al

17. iOS Hacker's Handbook by Charlie Miller , Dion Blazakis , et al.
18. The Mobile Application Hacker's Handbook by Dominic Chell , Tyrone Erasmus , et al.
19. The Mac Hacker′s Handbook by Charlie Miller and Dino Dai Zovi
20. The Antivirus Hacker's Handbook by Joxean Koret and Elias Bachaalany

TRACK 3 Data Science And Big Data

Course Code: MS-FIT-208 Statistical Thinking and Data Analysis

Unit	Details	No of lectures
1	**1.1 Introduction:** Nature and objectives of research, Study and formulation of research problem, Scope and formulation of hypothesis, Preparation and presentation of research and project proposals, Selection of thrust research.	15
	1.2 Introduction to Statistical Analysis: Measures of central tendency and dispersion, Mean, Median,Mode, Range, Mean deviation, Standard deviation.	
2	**2.1 Random Variables and Probability Distribution**: Definition, Distributions, Functions, Mathematical Expectation, Binomial, Poisson, Geometric, Negative binomial, Exponential, Normal and log-normal	15
	distributions.	
	2.2 Markov chains: Basics of markov chains, Finite state space, Markov chains, transition and stationary	
	markov chains, Continuous time markov process: Pure birth, Pure death, Birth and death process.	
3	**3.1 Hypothesis Testing**: Tests of significance based on normal, Analysis of variance technique,Anova	15
	3.2 Linear Regression and Correlation: Linear regression, Least square principle and fitted models, Karl Pearson's correlation coefficient, Rank correlation, Lines of regression.	
4	**4.1 Design of Experiments:** Completely randomized design, Random block design, Latin square design, Statistical analysis.	15
	4.2 Time series and forecasting: Components of time series, Analysis of time series, Measurement of trend, Measurement of seasonal variations	

Reference Book:

1. Introduction to Statistics and Data Analysis : With Exercises, Solutions and Applications in R by Christian Heumann, Michael Schomaker, Shalabh (auth.)

TRACK 3 Data Science And Big Data

Course Code: MS-FIT-209 Principles Of Data Science

Unit	Details	No of lectures
1	**1.1 Introduction:** What is Data Science? - Big Data and Data Science hype – and getting past the hype - Why now? – Datafication - Current landscape of perspectives - Skill sets needed	15
	1.2 Statistical Inference - Populations and samples - Statistical modeling, probability distributions, fitting a model - Intro to R	
2	**2.1 Exploratory Data Analysis and the Data Science Process** - Basic tools (plots, graphs and summary statistics) of EDA - Philosophy of EDA - The Data Science Process - Case Study: RealDirect (online real estate firm)	15
	2.2 Three Basic Machine Learning Algorithms - Linear Regression - k-Nearest Neighbors (k-NN) - k-means	
	2.3 One More Machine Learning Algorithm and Usage in Applications - Motivating application: Filtering Spam - Why Linear Regression and k-NN are poor choices for Filtering Spam - Naive Bayes and why it works for Filtering Spam - Data Wrangling: APIs and other tools for scrapping the Web	
3	**3.1 Feature Generation and Feature Selection (Extracting Meaning From Data)** - Motivating application: user (customer) retention - Feature Generation (brainstorming, role of domain expertise, and place for imagination) - Feature Selection algorithms – Filters; Wrappers; Decision Trees; Random Forests Recommendation Systems: Building a User-Facing Data Product - Algorithmic ingredients of a Recommendation Engine - Dimensionality Reduction - Singular Value Decomposition - Principal Component Analysis - Exercise: build your own recommendation system	15
	3.2 Mining Social-Network Graphs - Social networks as graphs - Clustering of graphs - Direct discovery of communities in graphs - Partitioning of graphs - Neighborhood properties in graphs	
4	**4.1 Data Visualization** - Basic principles, ideas and tools for data visualization Examples of inspiring (industry) projects - Exercise: create your own visualization of a complex dataset	15
	4.2 Data Science and Ethical Issues - Discussions on privacy, security, ethics - A look back at Data Science - Next-generation data scientists	

Reference Book:

1. Principles of Data Science, ZIman Osdemir
2. Data Science from Scratch, Book by Joel Grus

TRACK 3 Data Science And Big Data

Course Code: MS-FIT-210 Data Science Implementation

Unit	Details	No of lectures
1	**1.1 Data Science Technology Stack:** Rapid Information Factory Ecosystem Data Science Storage Tools, Schema-on-Write and Schema-on-Read , Data Lake, Data Vault, Hubs , Links, Satellites, Data Warehouse Bus Matrix, Data Science Processing Tools **1.2 Spark :** Spark Core, Spark SQL, Spark Streaming, MLlib Machine Learning Library, GraphX, Mesos, Akka, Cassandra **1.3 Kafka :** Kafka Core , Kafka Streams , Kafka Connect, Elastic Search , R, Scala , Python, MQTT (MQ Telemetry Transport)	15

	1.4 Layered Framwork: Definition of Data Science Framework, CrossIndustry Standard Process for Data Mining (CRISP-DM), Homogeneous Ontology for Recursive Uniform Schema, The Top Layers of a Layered Framework, Layered Framework for High-Level Data Science and Engineering	
2	**2.1 Business Layer:** Business Layer, Engineering a Practical Business Layer **2.2 Utility Layer:** Basic Utility Design, Engineering a Practical Utility Layer **2.3 Three Management Layers:** Operational Management Layer, Processing-Stream Definition and Management, Audit, Balance, and Control Layer, Balance, Control, Yoke Solution, Cause-and-Effect, Analysis System, Functional Layer, Data Science Process	15
3	**3.1 Retrieve Superstep:** Data Lakes, Data Swamps, Training the Trainer Model, Understanding the Business Dynamics of the Data Lake, Actionable Business Knowledge from Data Lakes, Engineering a Practical Retrieve Superstep, Connecting to Other Data Sources, **3.2 Assess Superstep:** Assess Superstep, Erroros, Analysis of Data, Practical Actions, Engineering a Practical Assess Superstep Process Superstep: Data Vault, Time-Person-Object-Location-Event Data Vault, **3.3 Data Science Process:** Transform Superstep, Building a Data Warehouse, Transforming with Data Science, Hypothesis Testing, Overfitting and Underfitting, Precision-Recall, Cross-Validation Test.Univariate Analysis, Bivariate Analysis, Multivariate Analysis, Linear Regression, Logistic Regression, Clustering Techniques,	15
4	**4.1 Transform Superstep:** ANOVA, Principal Component Analysis (PCA), Decision Trees, Support Vector Machines, Networks, Clusters, and Grids, Data Mining, Pattern Recognition, Machine Learning, Bagging Data, Random Forests, Computer Vision (CV) , Natural Language Processing (NLP), Neural Networks, TensorFlow. **4.2 Organize and Report Supersteps:** Organize Superstep, Report Superstep, Graphics, Pictures, Showing the Difference	15

Reference book:

1. Practical Data Science Andreas François Vermeulen APress

a. For Tableau Practicals
Practical Tableau by Ryan Sleeper.
https://www.pdfdrive.com/practical-tableau-100-tips-tutorials-and-strategies-from-a-tableau-zen-master-d188034960.html

Part 7- Detailed Scheme Practicals

FIT- 2P1 Microservices Architecture

Practical No	Details
1	Building APT.NET Core MVC Application.
2	Building ASP.NET Core REST API.
3	Working with Docker, Docker Commands, Docker Images and Containers
4	Installing software packages on Docker, Working with Docker Volumes and Networks.
5	Working with Docker Swarm.
6	Working with Circle CI for continuous integration.
7	Creating Microservice with ASP.NET Core.
8	Working with Kubernetes.
9	Creating Backing Service with ASP.NET Core.
10	Building real-time Microservice with ASP.NET Core.

TRACK 1 : ARTIFICIAL INTELLIGENCE

Sr. No		Title
1		Create a data model using Cassandra
2		Conversion from different formats to HORUS
	A	CSV to HORUS
	B	XML to HORUS
	C	JSON to HORUS
	D	MySQL Database to HORUS
	E	Picture to HORUS
	F	Video to HORUS
	G	Audio to HORUS
3		Utilities and Auditing
	A	Fixer Utilities
	B	Data Binning or Bucketing
	C	Aggregating of Data
	D	Outlier Detection
	E	Audit
4		Retrieving Data
	A	Data Processing
	B	Retrieve different attributes of data
	C	Data Pattern
	D	Loading IP_DATA_ALL.csv
	E	Building a diagram for scheduling of jobs
	F	Connecting other Data Sources
5		Assessing Data
6		Processing Data
7		Transforming Data
8		Organizing Data
	A	Horizontal Style
	B	Vertical Style
	C	Island Style
	D	Secure Vault Style

9		Reporting Data
	A	Create a network routing diagram
	B	Directed Acyclic Graph
	C	Graphics
10		Working with Power BI
	A	Importing data from Excel
	B	Importing data from OData Feed
	C	Data Visualization with Power BI

TRACK 3 Data Science And Big Data

MS-FIT-20 Data Science Implementation

Sr. No		Title
1		Create a data model using Cassandra
2		Conversion from different formats to HORUS
	A	CSV to HORUS
	B	XML to HORUS
	C	JSON to HORUS
	D	MySQL Database to HORUS
	E	Picture to HORUS
	F	Video to HORUS
	G	Audio to HORUS
3		Utilities and Auditing
	A	Fixer Utilities
	B	Data Binning or Bucketing
	C	Aggregating of Data
	D	Outlier Detection
	E	Audit
4		Retrieving Data
	A	Data Processing
	B	Retrieve different attributes of data
	C	Data Pattern
	D	Loading IP_DATA_ALL.csv
	E	Building a diagram for scheduling of jobs
	F	Connecting other Data Sources
5		Assessing Data
6		Processing Data
7		Transforming Data
8		Organizing Data
	A	Horizontal Style
	B	Vertical Style
	C	Island Style
	D	Secure Vault Style
9		Reporting Data
	A	Create a network routing diagram
	B	Directed Acyclic Graph
	C	Graphics
10		Working with Power BI
	A	Importing data from Excel
	B	Importing data from OData Feed
	C	Data Visualization with Power BI