Faculty of Science and Technology
Savitribai Phule Pune University
Maharashtra, India

http://www.unipune.ac.in/

Curriculum
Master of Cyber Security
(Course 2020)

(With effect from 2020-21)

Savitribai Phule Pune University, Pune
Master of Cyber Security (2020 Course)
(with effect from A.Y. 2020-21)

Semester I

Course Code	Course	Teaching Scheme Hours / Week		Examination Scheme and Marks					Credit	
		Theory	Practical	In-Sem	End-Sem	TW	OR/ PRE	Total	TH	PR
510401	Mathematical Foundations for Cyber Security	04	--	50	50	--	--	100	04	--
510402	Modern Cryptography	04	--	50	50	--	--	100	04	--
510403	Secure Software Design, coding practices and Ethics	04	--	50	50	--	--	100	04	--
510101	Research Methodology	04	--	50	50	--	--	100	04	--
510405	Elective I	05	--	50	50	--	--	100	05	-
510406	Laboratory Proficiency I	--	08	--	--	50	50	100	--	04
Total		**21**	**08**	**250**	**250**	**50**	**50**	**600**	**21**	**04**
Total Credit									**25**	
510407	Non-Credit Course I*								Grade	

Elective I

510405A	Data Storage Technologies and Networks	510405B	Information Systems Management
510405C	Ethical Hacking	510405D	High Speed Networks
510405E	**Open Elective**		

Semester II

Course Code	Course	Teaching Scheme Hours / Week		Examination Scheme and Marks					Credit	
		Theory	Practical	In-Sem	End-Sem	TW	OR/ PRE	Total	TH	PR
510408	Network Security	04	--	50	50	--	--	100	04	--
510409	Disaster Recovery and Management	04	--	50	50	--	--	100	04	--
510410	Fundamentals of Block chain	04	--	50	50	--	--	100	04	--
510411	Elective II	05	--	50	50	--	--	100	05	--
510412	Mini Project with Seminar I	--	04	--	--	50	50	100	--	04
510413	Laboratory Proficiency II	--	08	--	--	50	50	100	--	04
Total		**17**	**12**	**200**	**200**	**100**	**100**	**600**	**17**	**08**
Total Credit									**25**	
510414	Non-Credit Course II*								Grade	

Elective II

510411A	Machine Learning for Security	510411B	Digital Forensics
510411C	Identity and Access Management	510411D	IT Acts and Cyber Crime
510411E	Open Elective		

Savitribai Phule Pune University, Pune
Master of Cyber Security(2020 Course)

(with effect from A.Y. 2020-21)

Semester III

Course Code	Course	Teaching Scheme Hours / Week		Examination Scheme and Marks					Credit	
		Theory	Practical	In-Sem	End-Sem	TW	OR/ PRE	Tot.	TH	PR
610401	Cloud Security	04	--	50	50	--	--	100	04	--
610402	Cyber Security and IT infrastructure Protection	04	--	50	50	--	--	100	04	--
610403	Elective III	05	--	50	50	--	--	100	05	--
610404	Industry Internship-I/ In-house Research Project-I	--	04	--	--	50	50	100	--	04
610405	Dissertation Stage I	--	08	--	--	50	50	100	--	08
Total		**13**	**12**	**150**	**150**	**100**	**100**	**500**	**13**	**12**
Total Credit										**25**
610406	Constitution of India	02	--	--	--	--	--	--	02	--
610406	Non-Credit Course III*									Grade

Elective III

610403A	IoT and Embedded Systems Security	610403B	Malware Analysis & Reverse Engineering
610403C	Steganography and Digital Watermarking	610403D	Privacy and Security in Digital World
610403E	Open Elective		

Semester IV

Course Code	Course	Teaching Scheme Hours / Week	Examination Scheme and Marks			Credits
		Practical	TW	OR/PRE	Total	PR
610407	Industry Internship II / In-house Research Project II	05	50	50	100	05
610408	Dissertation Stage II	20	150	50	200	20
Total		**25**	**200**	**100**	**300**	**25**

* : For semester I, II, III, non-credit course is to be selected such that the said non-credit course is not selected in earlier semesters.

Non-Credit Courses

Typically curriculum is constituted by credit, non-credit and audit courses. These courses are offered as compulsory or elective. Non Credit Courses are compulsory. No grade points are associated with non-credit courses and are not accounted in the calculation of the performance indices SGPA & CGPA. However, the award of the degree is subject to obtain a PP grade for non credit courses. Conduction and assessment of performance in said course is to be done at institute level. The mode of the conduction and assessment can be decided by respective course instructor. Recommended but not limited to- (one or combination of) seminar, workshop, MOOC Course certification, mini project, lab assignments, lab/oral/written examination, field visit, field training. Examinee should submit report/journal of the same. Reports and documents of conduction and assessment in appropriate format are to be maintained at institute. Result of assessment will be PP or NP. Set of non-credit courses offered is provided. The Examinee has to select the relevant course from pool of courses offered. Course Instructor may offer beyond this list by seeking recommendation from authority. The selection of 3 distinct non-credit courses, one per semester (Semester I, II & III). The Contents of Non Credit Courses are Provided at the end of the document.

NCC1: English for Research Paper Writing	NCC2: Disaster Management
NCC3:Sanskrit for Technical Knowledge	NCC4: Value Education
NCC5: Stress Management by Yoga	NCC6: Pedagogy Studies
NCC7: Personality Development through Life Enlightenment Skills	NCC8: Game Engineering
NCC9: Advanced Cognitive Computing	NCC10: Virtual Reality
NCC11: Machine Translation	

Savitribai Phule Pune University, Pune
ME Cyber Security (2020 Course)
510401- Mathematical Foundations for Cyber Security

Teaching Scheme:	Credit	Examination Scheme:
TH: 04 hr/week	04	Mid Semester: 50 Marks End Semester: 50 Marks

Prerequisite Courses: Basic knowledge of mathematics

Course Objectives:

1. Build a solid mathematical basis to understand foundations of cryptography
2. Formally understand the notions related to security authentication and privacy.
3. Applications of probability distributions and fuzzy sets.
4. An introduction to algebraic foundations for cryptography and coding theory.

Course Outcomes:

On completion of the course, learner will be able to:

1. To learn the concepts of Integer arithmetic, modular arithmetic, Matrices and Linear Congruence.
2. To understand the concept of Algebraic structure including Groups, Rings, Fields and Classifications.
3. To learn about Number theory including Divisibility, Greatest common divisor and Prime numbers.
4. To understand and apply Euclidean algorithm, Fermat's theorem and Euler's theorem.
5. To apply the knowledge of probabilistic analysis in information security.
6. To apply the concept of Coding and use of Hamming distance

Unit I	Basic Mathematics to start Cryptography	09 hours

Foundation, Integer Arithmetic: Set, Binary operations, Integer division. Modular Arithmetic: Properties, Modular Operator, Set of residue Zn , Congruence, Operations in Zn , Inverses, Addition and Multiplication Tables, Different sets for addition and multiplication Matrices: Definition, Operations and relations, Determinant, Inverses, Residue matrices. Linear Congruence: Single variable linear equation, Set of linear
equations.

Case Studies (if any)	Linear congruence equations for the solutions of the N-Queens problem
Mapping of Course Outcomes for Unit I	**CO 1**

Unit II	Algebraic Structure	08 hours

Groups – Cyclic groups, Cosets, modulo groups, Rings– sub rings, ideals and quotient rings, Inter domains. Field: Finite fields, GF (2n), Classification – Structure of finite fields, Fields: Polynomials, Using a Generator. Lattice as algebraic system, sub lattice, some special lattice

Case Studies (if any)	A case study of completion modulo distributivity and Abelian groups
Mapping of Course Outcomes for Unit II	**CO 2**

Unit III	Number Theory	08 hours
Primes: Definition, Prime numbers, relative prime numbers, Relative prime numbers, Cardinality of Primes, Checking for Primeness, Euler's Phi–Function, Fermat's Theorem, An application of Fermat's Little Theorem and Congruence, Euler's Theorem – General formula to compute Φ(n), Generating Primes. Primality Testing: Deterministic algorithms, AKS (Agrawal, Kayal & Saxena primality test) test Naïve methods, Probabilistic algorithms, Fermat primality test, Miller–Rabin primality test, Recommended primality test		
Case Studies (if any)	Comparative analysis of various methods of testing the primality of number	
Mapping of Course Outcomes for Unit III	**CO 3**	
Unit IV	**Advance Mathematics of Cryptography**	**08 hours**
Primes, Primaility Testing, Factorization: Fundamental theorem of arithmetic, Factorization methods, Fermat method, Pollar p–1 method, Pollard rho method, more efficient methods. Chinese Remainder Theorem (CRT) –its applications. Quadratic congruence: Quadratic congruence modulo a prime, Quadratic congruence modulo a composite. Exponential and logarithm: exponentiation, logarithm		
Case Studies (if any)	Comparative analysis of various factorization methods	
Mapping of Course Outcomes for Unit IV	**CO 4**	
Unit V	**Probability Theory**	**06 hours**
Introduction, Concepts of Probability, Conditional Probability, Baye's Theorem, Monte Carlo algorithms, Random Variables, Expected Value, Pseudorandom number generator, Stochastic Process Markov Chain.		
Case Studies (if any)	Study of the Monty Hall Problem	
Mapping of Course Outcomes for Unit V	**CO 5**	
Unit VI	**Coding Theory**	**06 hours**
Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes - Generator matrices and paritycheck matrices - Syndrome decoding – Hamming codes - Hadamard Code – Goppa codes		
Mapping of Course Outcomes for Unit VI	**CO 6**	

Books & Other Resources:

Textbooks:

1. Cryptography & Network Security, Behrouz A. Forouzan, McGraw Hill
2. An Introduction to Mathematical Cryptography, Hoffstein, Jeffrey, Pipher, Jill, Silverman, J.H.
3. Probability, Statistics, and Stochastic Processes, Peter Olofsson and Mikael Andersson, A Wiley-Interscience Publication
4. Introduction to Coding Theory CMU: Spring 2010, Notes 1: Introduction, linear codes, January 2010. https://www.cs.cmu.edu/~venkatg/teaching/codingtheory/notes/notes1.pdf

Reference Books:

1. Mathematical Cryptology, Keijo Ruohonen (Translation by Jussi Kangas and Paul Coughlan), 2014.
2. Cryptography & Information Security, V. K. Pachghare, PHI
3. Foundation of Mathematical Logic, Haskell B. Curry
4. Math 550, Coding and Cryptography, Workbook, J. Swarts, 0121709 https://www.unf.edu/~wkloster/crypto/gary_notes.pdf

MOOC Courses:

1. https://www.coursera.org/learn/crypto
2. https://www.edx.org/course/more-fun-with-prime-numbers

E-books:

1. https://www.cs.cmu.edu/~venkatg/teaching/codingtheory/notes/notes1.pdf
2. https://www.unf.edu/~wkloster/crypto/gary_notes.pdf
3. http://index-of.es/Varios-2/Modern%20Cryptography.pdf

Important links:

Supplementary Resources:

1. https://crypto.stanford.edu/
2. https://ocw.mit.edu/courses/mathematics/
3. http://homes.soic.indiana.edu/yh33/Teaching/I231-2016/syllabus.html
4. http://nptel.ac.in/syllabus/106105031/
5. https://eliademy.com/catalog/physical-science/elementary-number-theory.html
6. Linear congruence equations for the solutions of the N-Queens problem https://doi.org/10.1016/0020-0190(92)90156-P8.
7. A case study of completion modulo distributivity and Abelian groups DOI :10.1007/978-3-662-21551-7_4

Savitribai Phule Pune University, Pune
ME Cyber Security (2020 Course)
510402- Modern Cryptography

Teaching Scheme:	Credit	Examination Scheme:
TH: 04 hr/week	04	Midsemester: 50 Marks End Semester: 50 Marks

Prerequisite Courses: Discrete structure, algorithms, computer networks

Course Outcomes:

On completion of the course, learner will be able to–

CO1: Understand the difference between cryptography and Modern cryptography.

CO2: Demonstrate an understanding of the mathematical underpinning of Public-Key (Asymmetric) Cryptography.

CO3: Understand the various Security Applications using Public-Key (Asymmetric) Cryptography.

CO4: Acquire background on well known Cryptography Digital Signature and Stenography Techniques.

CO5: Analyze and evaluate the cyber security needs of an organization

CO6: Develop cyber security strategies and policies

Unit I	Cryptography and Modern Cryptography	6 Hrs

Introduction to Cryptography and Modern Cryptography, The Basic Principles of Modern Cryptography , Principle 1 :Formulation of Exact Definitions, Principle 2: Reliance on Precise Assumptions Principle 3 : Rigorous Proofs of Security

The Setting of Private-Key Encryption , Historical Ciphers and Their Cryptanalysis ,

Perfectly-Secret Encryption: Definitions and Basic Properties, The One-Time Pad (Vernam's Cipher), Limitations of Perfect Secrecy, Shannon ciphers and perfect security:Definition of a Shannon cipher ,Perfect security, Computational ciphers and semantic security : Definition of a computational cipher ,Definition of semantic security ,Connections to weaker notions of security ,Consequences of semantic security

Case Studies (if any)	Crypto Forge Encryption Software
Mapping of Course Outcomes for Unit I	CO1

Unit II	Private-Key (Symmetric) Cryptography	7 Hrs

Private-Key Encryption and Pseudo randomness: A Computational Approach to Cryptography, The Basic Idea of Computational Security, efficient Algorithms and Negligible Success, Pseudo randomness,

Constructing Secure Encryption Schemes :A Secure Fixed-Length Encryption Scheme, Handling Variable-Length Messages ,Stream Ciphers and Multiple Encryptions

Security under Chosen-Plaintext Attacks (CPA): Constructing CPA-Secure Encryption Schemes,Pseudorandom Functions ,CPA-Secure Encryption Schemes from Pseudorandom Functions, Pseudorandom Permutations and Block Ciphers, Modes of Operation, Security Against Chosen-Ciphertext Attacks (CCA)2. AES (Advanced Encryption Standard),DES (Data Encryption Standard),IDEA (International Data Encryption Algorithm),Blowfish (Drop-in replacement for DES or IDEA)

Case Studies(if any)	**Demonstration of CertMgr.exe tool**	
Mapping of Course Outcomes for Unit II	**CO2**	
Unit III	**Public-Key (Asymmetric) Cryptography**	**6 Hrs**
Algorithms:RSA,Elliptic curve cryptography,Diffie-Hellman key exchange,DSA,key serialization,Asymmetric Utilities.		
Case Studies(if any)	**Demonstration of Windows BitLocker :** Encrypts your entire drive, which makes it impossible for malicious users stealing your laptop/PC to remove the hard drive and access your file	
Mapping of Course Outcomes for Unit III	**CO3**	
Unit IV	**Cryptography Digital Signature and Stenography Techniques**	**7 Hrs**
Digital signature vs Digital certificate,Models of Digital Signature,Block diagram of digital signature,Importance of Digital Signature,Encryption with digital signature,Digital Signature Algorithm(DSA),Advantages and Disadvantages of DSA. Difference between Stenography and cryptography, clasification of stegnography,Text,Audio,video, ,protocol.Image stegnography, private & public key encryptions, digital signatures, cryptographic hashes and authenticated encryption.		
Case Studies(if any)	**Demo of DocuSign Tool, Demo of Sign on Doc Demo of Steghide tool**	
Mapping of Course Outcomes for Unit IV	**CO4**	
Unit V	**Introduction: Cyber Security**	**7 Hrs**
: Cyber Security – Cyber Security policy – Domain of Cyber Security Policy – Laws and Regulations – Enterprise Policy – Technology Operations – Technology Configuration - Strategy Versus Policy – Cyber Security Evolution – Productivity – Internet – E commerce – Counter Measures Challenges. Botnets.		
Mapping of Course Outcomes for Unit V	**CO5**	
Unit VI	**Cyber security objectives and guidance**	**6 Hrs**
Cyber Security Metrics – Security Management Goals – Counting Vulnerabilities – Security Frameworks – E Commerce Systems – Industrial Control Systems – Personal Mobile Devices – Security Policy Objectives – Guidance for Decision Makers – Tone at the Top – Policy as a Project – Cyber Security Management – Arriving at Goals – Cyber Security Documentation – The Catalog Approach – Catalog Format – Cyber Security Policy Taxonomy.		
Case Studies(if any)	**Demonstration of any free Stenography tool**	
Mapping of Course Outcomes for Unit VI	**CO6**	
Books & Other Resources:		
Jennifer L. Bayuk, J. Healey, P. Rohmeyer, Marcus Sachs , Jeffrey Schmidt, Joseph Weiss “Cyber Security Policy Guidebook” John Wiley & Sons 2012.		
Reference Books: Rick Howard “Cyber Security Essentials” Auerbach Publications 2011. 2. B.G Raggad, “ Information Security Management”, CRC Press, Taylor Francis, 2015		
MOOC Courses: **1.NPTEL course on Cryptography and Network Security**		

Savitribai Phule Pune University, Pune

ME Cyber Security (2020 Course)

510403: Secure Software Design, coding practices and ethics

Teaching Scheme:	Credit	Examination Scheme:
TH: 04 hr/week	04	Midsemester: 50 Marks End Semester: 50 Marks

Prerequisite Courses: Software Engineering and Project Management

Course Objectives:

1. To understand the threats and attacks for the software systems
2. To know the characteristics of a secure software
3. To acquaint with the principles and practices of the secure software development

Course Outcomes:

On completion of the course, learner will be able to–

1. Recognize the threats for software systems
2. Recognize the principles for secure design of the software
3. Apply the SQUARE model for requirement engineering
4. Recognize the coding and testing practices for secure software development
5. Develop an agile threat model for a given software application.

Unit I	Introduction	
System Complexity, software assurance and software security, threats and sources, benefits of early detection of defects, managing secure software development, properties of secure software and perspectives, asserting desired security properties		
Mapping of Course Outcomes for Unit I	**CO1**	
Unit II	**Requirement Engineering and design for secure software**	
Introduction, misuse cases, SQUARE model and output, requirement elicitation methods, requirement prioritization. Architectural risk analysis, security principles, guidelines and attack patterns, Security by design principles		
Mapping of Course Outcomes for Unit II	**CO2, CO3**	
Unit III	**Secure coding and testing**	
Code analysis, coding practices, security testing, security testing throughout software lifecycle. OWASP Security knowledge framework, OWASP Software assurance maturity model, OWASP secure coding practices checklist		
Mapping of Course Outcomes for Unit III	**CO2, CO4**	
Unit IV	**Security Governance**	
Security failures, examples for security analysis, system complexity drivers and deep technical problem complexity. Governance and security, enterprise level security framework adoption, adequacy of security, security and project management, maturity of practice.		

Mapping of Course Outcomes for Unit IV	**CO1, CO2**	
Unit V	**Software testing**	
Software penetration testing, risk based security testing		
Mapping of Course Outcomes for Unit V	**CO4**	
Unit VI	**Secure agile development**	
Agile development process, getting security into requirements, agile vulnerability management, agile threat modeling, code review for security, agile security testing		
Mapping of Course Outcomes for Unit VI	**CO5**	
Books & Other Resources:		
Textbooks: **1. Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw and Nancy R. Mead, "Software Security Engineering: A Guide for project Managers," Addision Wesley** **2. Mark G. Graff, Kenneth R. van Wyk, "Secure Coding: Principles and Practices," O'Reilly Media Inc., ISBN: 9780596002428** **3. Gary R. McGraw, "Software Security: Buildig Security In," Addison-Wesley Professional.** **4. Laura Bell, Michael Brunton-Spall, rich Smith and Jim Bird, "Agile Application security" O'Reilly Media, ISBN: 9781491938843**		
E-books: **1. SEI CERTC Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems, 2016 edition**		
Important links: **1. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=466229** **2. https://www.securityknowledgeframework.org/** **3. https://owasp.org/www-project-samm/** **4. https://wiki.owasp.org/index.php/Security_by_Design_Principles** **5. https://www.oracle.com/java/technologies/javase/seccodeguide.html**		

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 510101: Research Methodology		
Teaching Scheme:	**Credit**	**Examination Scheme:**
TH: 04 hr/week	**04**	**Mid Semester: 50 Marks** **End Semester: 50 Marks**

Prerequisite Courses: -

Companion Course:

1) Mathematical Foundation of Information Security

2) Laboratory Proficiency I

Course Objectives:

1. To understand the philosophy of research in general
2. To understand basic concepts of research and its methodologies
3. To learn the methodology to conduct the Literature Survey
4. To acquaint with the tools, techniques, and processes of doing research
5. To learn the effective report writing skills and allied documentations
6. To become aware of the ethics in research, academic integrity and plagiarism

Course Outcomes:

On completion of the course, learner will be able to–

1. Identify appropriate topics for research work in computer engineering
2. Carry out Literature Survey
3. Select and define appropriate research problem and parameters
4. Design the use of major experimental methods for research
5. Use appropriate tools, techniques, and processes of doing research in Computer science
6. Become aware of the ethics in research, academic integrity and plagiarism
7. Write a research report and thesis

Unit I	**Introduction**	**7 hrs**

Evolution of Research Methodology: Meaning, nature, scope, and significance of research; Research paradigm; The purpose and Products of Research; Reasons for doing research, Objectives of research, Motivation for research; Postulates underlying scientific investigations; Types of research; Research process and work flow.

Engineering Research-Why? Research Questions, Engineering Ethics, conclusive proof-what constitutes A research project-Why take on?

Case Studies (if any)	Code of Ethics, IEEE Code of Ethics, ACM Software Engineering Code of Ethics and Professional Practice, Code of Ethics especially covering Engineering discipline, various aspects- environment, sustainable outcomes, employer, general public, & Nation, Engineering Disasters.
Mapping of Course Outcomes for Unit I	**CO1**

Unit II	**Literature Search & Review, Developing Research Plan**	**7 hrs**

Archival Literature, Why should engineers be ethical? Types of publications- Journal papers, conference papers, books, standards, patents, theses, trade magazine, newspaper article, infomercials, advertisement, Wikipedia & websites, Measures of research impact, Literature review, publication cost.

Developing Research Plan: Research Proposals, Finding a suitable research questions, The elements of research proposals-title, details, budget, Design for outcomes-1D data, 2D data, 3D data, N-D data, The research tools- Experimental measurements, numerical modeling, theoretical derivations & Calculations, curve matching.

Case Studies	Engineering dictionary, Shodhganga, The Library of Congress, Research gate, Google Scholar, Bibliometrics, Citations, Impact Factor, h-index, I-index, plagiarism, copyright infringement. Collect data for overbooking decision for demand and revenue management of flights.	
Mapping of Course Outcomes for Unit II	**CO2**	
Unit III	**Statistical Analysis**	**7 hrs**
Statistical Analysis: Introduction, Sources of error and uncertainty, One-Dimensional Statistics: combining errors and uncertainties, t-test, ANOVA statistics, example, Two-Dimensional Statistics: example, Multi-Dimensional Statistics: partial correlation coefficients, example, Null hypothesis testing.		
Case Studies	GNU PSPP Tool, SOFA, NOST-Dataplot	
Mapping of Course Outcomes for Unit III	**CO3**	
Unit IV	**Optimization Techniques**	**7 hrs**
Optimization Techniques: Introduction, Two-parameter optimization methods: sequential uniform sampling, Monte Carlo optimization, Simplex Optimization method, Gradient Optimization method, Multi-parameter optimization methods, The cost function.		
Case Studies	Google Optimization Tools, OpenMDAO	
Mapping of Course Outcomes for Unit IV	**CO4**	
Unit V	**Survey Research Methods**	**7 hrs**
Survey Research Methods: Why undertake a survey, Ergonomics and human factors, Ethics approval, General survey guidelines, Survey statements, Survey delivery, Respondent selection, Survey timelines, Statistical analysis, Reporting.		
Case Studies(if any)	Qualitative Analysis Tools- AQUAD, CAT. IP related laws in India	
Mapping of Course Outcomes for Unit V	**CO3, CO5**	
Unit VI	**Research Presentation**	**7 hrs**
Research presentation: Introduction, Standard terms, Standard research methods and experimental techniques, Paper title and keywords, Writing an abstract, Paper presentation and review, Conference presentations, Poster presentations, IPR, Copyright, Patents. **Reporting Research:** Thesis, Structure and Style for writing thesis, Dissemination of research findings; Reporting and interpretation of results; cautions in interpretations, Type of reports, Typical report outlines.		

The path forward: Publication trends, Getting started in research, Quality assurance (QA) Occupational health and safety.

Case Studies (if any)	Intellectual Property India- services, InPASS - Indian Patent Advanced Search System, US patent, IEEE / ACM Paper templates Patent act, 1970 and Patent Rules 1972 (with amendments)
Mapping of Course Outcomes for Unit VI	**CO6, CO7**

Books & Other Resources:

Text Books:

1. David V Thiel, "Research Methods- for Engineers", Cambridge University Press, ISBN:978-1-107-61019-4
2. Kothari C.R., "Research Methodology. New Age International, 2004, 2nd Ed; ISBN:13: 978-81-224-1522-3.

Reference Books:

1. Caroline Whitbeck, "Ethics in Engineering Practice and Research", 2nd Ed., Cambridge University Press; ISBN :978-1-107-66847-8
2. Gordana DODIG-CRNKOVIC, "Scientific Methods in Computer Science", Department of Computer Science Malardalen University, Vasteas, Sweden; ISBN: 91-26-97860-1

Important links:

1) WIPO : https://www.wipo.int/portal/en/index.html
2) IP India: http://www.ipindia.nic.in/
3) Cell For IPR Promotion and Management : http://cipam.gov.in/
4) Draft patent rules: http://cipam.gov.in/wp-content/uploads/2018/12/Draft-Patent-Rules-2018.pdf
5) Manual of Patent Office Practice and Procedure: http://www.ipindia.nic.in/writereaddata/Portal/Images/pdf/Manual_for_Patent_Office_Practice_and_Procedure_.pdf
6) WIPO IPR Resources: https://www.wipo.int/reference/en/

Savitribai Phule Pune University, Pune

ME Information Security (2020 Course)

Elective-I: 510405A- Data Storage Technologies and Networks

Teaching Scheme:	Credit	Examination Scheme:
TH: 05 hr/week	05	Midsemester: 50 Marks End Semester: 50 Marks

Unit I	**Storage Primer: Storage Devices and Storage Arrays**	**7 hrs**
The role of storage in IT, Types of storage, Persistent and Non persistent Storage, Disk Storage, Solid-state storage, Tape storage, Storage arrays, architectures, Enterprise-Class arrays, Storage array pros and cons		
Unit II	**Data Integrity and Availability: RAID**	**7 hrs**
RAID, RAID Concepts, RAID Controllers, RAID Levels, Hardware RAID , Software RAID, RAID Array, All-Flash Array		
Unit III	**Network Storage: SAN and NAS**	**7 hrs**
Storage area networks in transition, iSCSI SANS, Virtual SANs, NAS- based Network, Traditional NAS Arrays, Scale-Out NAS Arrays, Object Storage Device(OSD), Network Data Management Protocol(NDMP)		
Unit IV	**Storage Virtualization**	**7 hrs**
Storage Virtualization, Host-based, Network-based, Controller-based storage virtualization, configuration of controller-based virtualization, Software-defined storage		
Unit V	**Cloud Storage**	**7 hrs**
Cloud computing model, Public Cloud, Private Cloud, Hybrid Cloud, Cloud Storage, HPC Clouds, Hybrid Clouds, Data Governance		
Unit VI	**Big data storage**	**7 hrs**
Requirements of consistent and scalable data, defining big data and the type of storage it needs, requirements of big data storage, big data storage infrastructure, Amazon, Google, and Apache: industry standards in providing big data storage solutions.		
Case Studies(if any)	**Industry standards for big data storage for Google**	

Resources:

Textbooks: Network Storage, **by James O'Reilly, Released October 2016**
Publisher(s): Morgan Kaufmann, ISBN: 9780128038659

Data Storage Networking: Real World Skills for the CompTIA Storage+ Certification and Beyond by Nigel Poulton

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) Elective- I: 510405B: Information Systems Management		
Teaching Scheme:	**Credit**	**Examination Scheme:**
TH: 05 hr/week	**05**	**Midsemester: 50 Marks** **End Semester: 50 Marks**
Prerequisite Courses: Information Systems and Engineering Economics		
Course Objectives: 1. To prepare the students to various forms of the Information Systems and its application in organizations. 2. To Prepare engineering students to do economic analyses in the decision making process to justify or reject alternatives / projects on an economic basis for an organization. 3. To learn the skills to make the best use of Business Intelligence 4. To learn the skills in building advanced Information Systems		
Course Outcomes: On completion of the course, learner will be able to–		
1. Understand the activities that are undertaken while managing, designing, planning, implementation, and deployment of computerized information system in an organization. 2. Perform and evaluate present worth, future worth and annual worth analyses on one of more economic alternatives. 3. Evaluate the decisions using What-If Analysis, Sensitivity analysis, Goal-seeking analysis, Optimization analysis techniques of DSS 4. Plan to implement a Business Intelligence Solution		
Selection of Modules: Modules 1 to 3 are compulsory and select any one from modules 4, 5 and 6.		
Module I	**Management Information System (MIS)**	**06 Hours**
Managing Information Systems, Ethical and Social Issues, Information Technology Infrastructure and Choices, Information Systems Security and Control, Managing Data Resources, Business Process Integration and Enterprise Systems, ICT for Development and E-Governance.		
Case Studies (if any)	In-house or cloud based ERP implementation, UIDAI Unique Identification Authority of India.	
Mapping of Course Outcomes for Module I	CO1	
Module II	**Business Intelligence**	**09 Hours**

Business Intelligence an Introduction: Introduction, Definition, History and Evolution, Difference between Information and Intelligence, Factors of Business Intelligence System - Business Intelligence Architecture, Real time Business Intelligence, Business Intelligence Applications Business Intelligence Essentials: Introduction, Creating Business Intelligence Environment, Business Intelligence Landscape, Types of Business Intelligence, Business Intelligence Platform, Dynamic roles in Business Intelligence, Roles of Business Intelligence in Modern Business- Challenges of BI Business Intelligence User Model: Introduction, Evolution of Business Intelligence, Business Intelligence Opportunity Analysis Overview, Content Management System, End User Segmentation, Basic Reporting and Querying, Online Analytical Processing, OLAP Techniques, OLAP Applications, Applying the OLAP to Data Warehousing, Benefits of using OLAP, Dashboard, Advanced/Emerging BI Technologies, Future of Business Intelligence		
Mapping of Course Outcomes for Module II	CO4	
Module III	**Building Advanced Information Systems**	**07 Hours**
Decision Support in Business, Decision Support Trends, Decision Support Systems, Management Information Systems, Online Analytical Processing, Using Decision Support Systems, Executive Information Systems, Enterprise Portals and Decision Support, Knowledge Management Systems		
Case Studies(if any)	Real World Case: Hillman Group, Avnet, and Quaker Chemical: Process Transformation through Business Intelligence Deployments	
Mapping of Course Outcomes for Module III	CO3	
Module IV	**Economics and Management**	**07 Hours**
Engineering Economic Decisions, Time Value of Money, Understanding Money Management, Equivalence Calculations under Inflation, Present-Worth Analysis, Annual-Equivalence Analysis.		
Case Studies(if any)	Economic decisions done in Multi-national companies and comparative analysis of software enterprises from similar domains.	
Mapping of Course Outcomes for Unit IV	CO2	
Module V	**Applications of Business Intelligence**	**07 Hours**
Business Intelligence Strategy and Road Map: Introduction, Planning to implement a Business Intelligence Solution, Understand Limitations of Business Intelligence, Business Intelligence Usage, How to make the best use of Business Intelligence?, Implementing Business Intelligence: Implementation Strategy , Fundamental decisions Business Intelligence Case Studies: Improving Operational Efficiency –Audi AG, Maximizing Profitability-The Frank Russell Company		
Case Studies(if any)	BI and Data mining Applications: ERP and BI, BI applications in CRM,BI in Marketing, Logestics and Productions Finance, Banking ,Telecommunications and fraud detection	
Mapping of Course Outcomes for Module V	C O 4	
Module VI	**Managing Information Systems Projects**	**06 Hours**

The importance of project management, Selecting projects, Establishing the business value of Information Systems, Managing project risk	
Case Studies(if any)	Hands on mini projects : Management Decision Problems, Improving Decision Making: Using Spreadsheet Software for Capital Budgeting for a New CAD System, Improving Decision Making: Using Web Tools for Buying and Financing a Home
Mapping of Course Outcomes for Module VI	CO1

Books & Other Resources:

Text Books:

1. Rahul De, ―MIS: Management Information Systems in Business, Government and Society‖, Wiley India, ISBN: 13: 978-81-265-2019-0.
2. Chan S. Park , "Fundamentals of Engineering Economics‖, 3rd Edition, Pearson Education, ISBN 13: 978-02-737-7291-0
3. Kenneth C. Laudon, Jane P. Laudon, "Management Information Systems MANAGING THE DIGITAL FIRM", 12th Edition, Prentice Hall
4. James A. O'Brien, George M. Marakas, "INTRODUCTION TO INFORMATION SYSTEMS", 15th Edition, McGraw-Hill

Reference Books:

1. William G. Sullivan, Elin M. Wicks, C. Patrick Koelling, Engineering Economy, Pearson Education, ISBN13: 978-01-334-3927-4

MOOC Couses: "Information Systems Specialization", offered by University of Minnesota https://www.coursera.org/specializations/information-systems

"Enterprise Systems**"** by Jason Chan, Associate Professor, affiliated to University of Minnesota https://www.coursera.org/learn/enterprise-systems

"It Infrastructure and Emerging Trends" by Soumya Sen, Associate Professor, affiliated to **University of Minnesota** https://www.coursera.org/learn/it-infrastructure-and-emerging-trends

"Analysis for business systems" by Ken Reily, Associate Professor, affiliated to **University of Minnesota** https://www.coursera.org/learn/analysis-for-business-systems

"IS/IT Governance" by Gautam Ray, Associate Professor, affiliated to **University of Minnesota** https://www.coursera.org/learn/is-it-governance

Books:

7. Business Intelligence Roadmap: The Complete Project Lifecycle For Decision-Support Applications by Larissa T. Moss & Shaku Atre
8. Data Strategy: How To Profit From A World Of Big Data, Analytics And The Internet Of Things by Bernard Marr
9. Business-Intelligence-by-Michael-Luckevich-Elizabeth-Vitt-Stacia-Misner- Elizabeth-Vitt -Michael-Luc
10. Definitive Guide to DAX, The: Business intelligence for Microsoft Power BI, SQL Server Analysis Services, and Excel, 2nd Edition
11. Oracle Business Intelligence with Machine Learning : Artificial Intelligence Techniques in OBIEE for Actionable BI By Rosendo Abellera and Lakshman Bulusu

6 Business Intelligence Guidebook by Rick Sherman Released November 2014 Publisher(s): Morgan Kaufmann ISBN: 9780124115286

7 Business Intelligence Strategy and Big Data Analytics by Steve Williams Released April 2016 Publisher(s): Morgan Kaufmann ISBN: 9780128094891

Savitribai Phule Pune University, Pune
ME Cyber Security (2020 Course)
Elective- I: 510405C: Ethical Hacking

Teaching Scheme:	Credit	Examination Scheme:
TH: 5 hr/week	05	Midsemester: 50 Marks End Semester: 50 Marks

Prerequisite Courses:

1. Fundamentals for communication,
2. Static and Dynamic website development,
3. Basics of various operating systems.

Course Objectives:

1. Understand how attacker plans for attack through data collection.
2. To evaluate the security and to identify vulnerabilities in systems, networks or system infrastructure.
3. Perform security scan to test the application and network for vulnerability.
4. Understand the threats to web application and mitigation techniques.
5. Simulate the actual hacking attack on test bed.

Course Outcomes:

On completion of the course, learner will be able to–

1. Critically evaluate security techniques used to protect system and user data.
3. Describe the legal and ethical requirements related to ethical hacking.
4. Assess an environment using foot-printing.
5. Plan a vulnerability assessment and penetration test for a network.
6. Install, configure, use and manage hacking software on a closed network environment.
7. Examine the tools for conducting ethical hacking.
8. Demonstrate systematic understanding of the concepts of security at the level of policy and strategy in a computer system by hiding details.

Unit I	Security essentials	8 Hrs

Securing Unstructured Data: Structured Data vs. Unstructured Data; At Rest, in Transit, and in Use; Approaches to Securing Unstructured Data, Approaches to Securing Unstructured Data.

Encryption: A Brief History of Encryption, Symmetric-Key Cryptography, Public Key Cryptography, Public Key Infrastructure

Secure Network Design: Introduction, Performance, Availability, Security.

Case Studies (if any)	Case study on Public Key Infrastructure
Mapping of Course Outcomes for Unit I	2. Critically evaluate security techniques used to protect system and user data.

Unit II	Introduction to Ethical Hacking and Information gathering	8 Hrs

Ethical Hacking definition, difference between hacking and ethical hacking. Vulnerability, Attack Vector. Five stages of hacking: Reconnaissance (Survey), Probing, Actual attack, maintaining presence, Covering attack tracks, Introduction to OWASP top 10 attacks.

Data and Data sources, **Information gathering:** from social media accounts, extraction of photographs exif data, phone number, vehicle registration number, dumpster dumping, google street view and google history. Social Engineering techniques, Google Dork query, Browser extension to collect information. Principles of Ethical hacking (Legality & Ethics)

Case Studies (if any)	Study google dork query usefull for ethical hacking
Mapping of Course Outcomes for Unit II	3. Describe the legal and ethical requirements related to ethical hacking. 4. Assess an environment using foot-printing.

Unit III	Enumeration and System Hacking	8 Hrs
Scanning & Enumeration: Port Scanning, Network Scanning, Vulnerability Scanning, NMAP Scanning tool, OS Fingerprinting, Enumeration. **System Hacking**: Password cracking techniques, Key loggers, Escalating privileges, URL Hiding Files, Sniffers & SQL Injection: Active and passive sniffing, ARP Poisoning, Session Hijacking, DNS Spoofing, Conduct SQL Injection attack, Countermeasures. Study of open source scanning tools.		
Case Studies (if any)	Find all available open source scanning tools and prepare a comparative table on these parameters, operating system support, ability to search, scanning time, ability to detect vulnerabilities and ease of use.	
Mapping of Course Outcomes for Unit III	5. Plan a vulnerability assessment and penetration test for a network and web applications.	
Unit IV	**OWASP Top 10**	**8 Hrs**
1. Injection 2. Broken Authentication 3. Sensitive Data Exposure 4. XML External Entities (XXE) 5. Broken Access Control 6. Security misconfiguration 7. Cross-Site Scripting XSS 8. Insecure Deserialization 9. Using Components with Known Vulnerabilities 10 Insufficient Logging & Monitoring. Benefits to developers and organization.		
Case Studies (if any)	Prepare cheat sheet for all OWASP top 10 attacks	
Mapping of Course Outcomes for Unit IV	4 . Plan a vulnerability assessment and penetration test for a network. 5. Install, configure, use and manage hacking software on a closed network environment.	
Unit V	**Hacking Environment DVWA**	**8 Hrs**
Installation and configuration of DVWA environment. Virtual box installation, Installation of Kali Linux within virtual box. Kali Linux penetration testing and ethical hacking tools. What is TOR? How can you use it to protect your anonymity online? Social Engineering: Phases of an attack, Common targets, Common sources of information. Web Servers and applications: Common attacks and flaws, Current tools.		
Case Studies (if any)	Analysis of SQL Injection Using DVWA Tool	
Mapping of Course Outcomes for Unit V	6 . Examine the tools for conducting ethical hacking.	
Unit VI	**Hiding hacker details**	**8 Hrs**
Proxy chain for using proxy servers, hiding your IP and obtaining access. What is VPN how you can stay anonymous with VPN. Mac-changer, use of mac-changer to change your MAC address. Incident Response and Forensic Analysis.		
Case Studies (if any)	List and compare all available free to use proxy and VPN services.	
Mapping of Course Outcomes for Unit VI	7 . Demonstrate systematic understanding of the concepts of security at the level of policy and strategy in a computer system by hiding details.	

Books & Other Resources:

Textbooks:

1. Mark Rhodes-Ousley, “Information Security: The Complete Reference”, Second Edition, McGraw-Hill, 2013
2. Dafydd Stutarf, Marcus Pinto, “Web Application Hackre’s Handbook”, Wiley
3. Skoudis E. Perlman R. “Counter hack: A step by step Guide to Computer Attacks and effective Defense”, Prentice Hall Professional technical Reference, 2001.

Reference Books:

1. James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing”, Auerbach Publications, CRC Press
2. EC-Council, “Ethical Hacking and Countermeasures Attack Phases”, Cengage Learning
3. Michael Simpson, Kent Backman, James Corley, “Hands-On Ethical Hacking and Network Defense”, engage Learning
4. The Hacker Playbook: Practical Guide To Penetration Testing", by Peter Kim, January 1, 2014

MOOC Courses:

1. "Ethical Hacking" By Indranil Sengupta, IIT Kharagpur, (https://nptel.ac.in/courses/106/105/106105217)
2. https://www.udemy.com/share/101Ws2AEEdeVlaRXUJ/

E- books:

1. http://www.modir-shabake.com/wp-content/uploads/2016/07/CEH-v9-Certified-Ethical-Hacker-Version-9-Study-Guide-3rd-Edition-Technet24.pdf (Certified Ethical Hacker Study Guide v9, Sean-Philip Oriyano, Sybex; Study Guide Edition,2016)

https://ptgmedia.pearsoncmg.com/images/9780789751270/samplepages/0789751275.pdf (Certified Ethical Hacker: Michael Gregg, Pearson Education,1st Edition, 2013)

Important links:

1. https://owasp.org/www-project-top-ten/ (Unit - IV)
2. https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/
3. https://github.com/OWASP/Top10/raw/master/2017/OWASP%20Top%2010-2017%20(en).pdf
4. https://www.guru99.com/ethical-hacking-tutorials.html
5. DVWA: http://www.dvwa.co.uk/ (Unit - V)
6. TOR: https://www.torproject.org/ (Unit - V)
7. Kali Linux: https://www.kali.org/ (Unit -V)
8. Virtual box installation: https://www.virtualbox.org/ (Unit - V)
9. NMAP Security Scanner: https://nmap.org/
10. NMAP Use cases: https://www.redhat.com/sysadmin/use-cases-nmap
11. DVWA tutorial:

https://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson6/index.html

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 510406: Laboratory Proficiency-I		
Teaching Scheme:	**Credit**	**Examination Scheme:**
PR: 08 hr/week	**04**	**Term Work: 50 Marks** **Practical/Oral: 50 Marks**
Prerequisite Courses: Knowledge of programming languages, Basics of Python/R		
Companion Courses: 510301-Mathematical Foundations for Data Science 510302 – Basics of Data Science 510303 – Big Data Analytics 510304 – Research Methodology 510305 – Elective – I		
All assignments are compulsory. Each student should implement the assignment individually. Laboratory teachers should make sure that the dataset/code/writeup is not the same. Laboratory teacher can add more assignments as per requirement.		

510301-Mathematical Foundations for Cyber Security	
1	Write a program to find the Greatest Common Division using Euclidian Algorithm
2	Write a program to find the determinant and the multiplicative inverse
3	Write a program to find the particular and general solution to the linear Diophantine equation
4	Write an algorithm in pseudocode for the Fermat primality test, square root primality test & chinese remainder theorem
5	Write an algorithm to find & store the discrete logarithms for the set Z_p
6	The square & multiply fast exponentiation algorithm allows us to halt the program if the value of the base becomes 1. Modify the algorithm to show this
7	Write a program for Fermat Primility Test
8	Write a program for the square root primility test
9	Write a program for Estimating the value of Pi using Monte Carlo algorithm.
10	Write a program to generate Hamming code

510101 – Research Methodology

1. Use an academic web search to locate a journal paper which describes a design outcome in your field of interest (i.e. your engineering discipline).You must enter several keywords which relate to your topic. Read the paper and, using your own words, demonstrate your understanding of the paper by: Brief Contribution ♣ Performance metric, data set, comparative analysis and outcomes♣ Writing out the major conclusions of the paper;♣ Outlining the verification method(s) used to support these conclusions♣ Describing the author's reflective comments on the quality of the design♣ (positive and negative). The positive and negative environmental impacts;♣ After reading a published research paper, write down the research question you think the author have addressed in undertaking this research. Do you think the paper adequately supports the conclusions reached in addressing the question?

2. Consider a journal article in your discipline that was published approximately five years ago. Note the keywords and type them into one of the web-based academic search engines (e.g. googlescholar.com). Does the original article appear in the search results? How many citations does this article have? Have the same authors published further work in this field? Compare the citations of this paper with those from the most highly cited paper in the search results? How many citations does this highly cited article have? If this paper was published before your original article, is it cited in your article? Do you think this high-cited paper should have been listed as a reference in your original article? Give reasons for your decision. Read a journal paper from your discipline. Following the format of patents, write out one or more important outcomes from the paper in terms of one or more Patent Claims 1, 2…. . These claims must not only be new, they must be not-obvious from previous work
3. a) Literature Review Quality: Using a Journal paper selected in your engineering discipline of interest, write a 400 word evaluation of the quality of Literature Review. In particular, review the quality and relevance of cited papers, the comments made on those papers contribution to the general field, and any omission of papers which are of major importance in the field. b) Develop a new research proposal from a published paper: From selected published Journal paper, read the paper. In particular read the discussion and conclusion section and find Suggestions for further work. Apply one of the question words(How?, Why?, What?, When?) and write one or more research questions arising from this paper. This can be used as guide to help you to develop your own research project proposal
4. a) Download a set of weather data from the Internet covering the temperature and atmospheric pressure over a four day period. Present the data using 2D and 3D plots, and so deduce if the weather conditions are trending either higher or lower over this four day period. (Possible web sites include http://www.bom. gov.au/climate/ data/ and http://www.silkeborg-vejret.dk/english/ regn.php). b) Numerical modeling: Find a paper in which numerical modeling has been used to verify the experimental results. Comment on the differences between the experimental and modeling results. Have the authors commented on the accuracy of the experimental and modeling procedures? What suggestions do you have to improve the quality of the modeling reported in the paper? c) Statistical review: In your engineering discipline review a published paper which includes a statistical analysis. Write a brief report on the statistical methods used. Can you suggest an improved statistical analysis? Suggest some additional parameters that might have been measured during the data acquisition stage and so explain how you would analyze the total data set to deduce the influence (and statistical significance) of these additional measurements.
Elective I
Student should complete one mini project on selected elective

Semester – II

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 510408- Network Security		
Teaching Scheme:	**Credit**	**Examination Scheme:**
TH: 4 hr/week	**04**	**Midsemester: 50 Marks** **End Semester: 50 Marks**

Prerequisite Courses: Mathematical Foundations for Information Security ,
Modern Cryptography

Course Objectives:

1. To understand the concept of security and its applications.
2. To learn various vulnerabilities, threats and attacks
3. To know various detection and prevention techniques in diversified environments
4. To study different algorithms for network security

Course Outcomes:
On completion of the course, learner will be able to–
CO1: Design and choose appropriate security model
CO2: Design and apply the network protocols to web security CO3:
Illustrate the protocols required for email security
CO4: Describe the use of IPSec protocols for network security
CO5: Apply the knowledge of firewall and intrusion detection security for security CO6:
Apply the security protocols to the applications

Unit I	**Introduction**	

Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security, Threats, Vulnerabilities, and Attacks

Mapping of Course Outcomes for Unit I	**CO1**

Unit II	**Transport layer security**	

Web Security Considerations, Secure Socket Layer and Transport Layer Security, Transport Layer Security, HTTPS, Secure Shell (SSH)

Mapping of Course Outcomes for Unit II	**CO2**

Unit III	**Electronic Mail Security**	

Pretty Good Privacy – Notation, Operational Description, Cryptographic Keys and Key Rings Public-Key Management, S/MIME- RFC 5322, Multipurpose Internet Mail Extensions, S/MIME Functionality, S/MIME Messages, S/MIME Certificate Processing, Enhanced Security Services, DomainKeys Identified Mail - Internet Mail Architecture, E-mail Threats, DKIM Strategy, DKIM Functional Flow

Mapping of Course Outcomes for Unit III	**CO3**

Unit IV	**IP Security**	

IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange, Cryptographic suites

Mapping of Course Outcomes for Unit IV	**CO4**	
Unit V	**Nework Security, Firewall and Virtual Private Networks**	
Introduction, Brief Introduction to TCP/IP, Firewalls, IP Security, Virtual Private Networks, Intrusion		
Mapping of Course Outcomes for Unit V	**CO5**	
Unit VI	**Case studies on Cryptography and Security**	
Introduction, Cryptographic Solutions, Single Sign on, Secure Inter-branch payment transactions, Denial of service attacks, IP spoofing attacks, Cross Scripting Vulnerability, Contract signing, Secret splitting, Virtual Elections, Secure Multiparty Calculation, Creating VPN, Cookies and Privacy		
Mapping of Course Outcomes for Unit VI	**CO6**	

Books & Other Resources:

Textbooks:

5. William Stallings, “Cryptography and Network Security Principals and Practice”, Fifth edition, Pearson
6. Atul Kahate,”Cryptography and Network Security”, 3e, McGraw Hill Education
7. John E. Canavan,"Fundamentals of Network Security", Artech House

Reference Books:

- ✔ JosephKizza, “Computer Network Security and Cyber Ethics”, *McFarland & Company, Inc., Publishers* , Fourth Edition
- ✔ Prakash C. Gupta, “Cryptography and Network Security”, PHI
- ✔ Cryptography and Network Security – Behrouz A. Forouzan and Mukhopadhay – Mc Graw Hill
- ✔ V.K. Pachghare, “Cryptography and Information Security”, PHI Learning
- ✔ Bernard Menezes, “Network Security and Cryptography”, Cengage Learning India, 2014, ISBN No.: 8131513491
- ✔ K. Jaishankar, “Cyber Criminology”, CRC Press

MOOC Courses

5. Introduction to cyber security, “https://swayam.gov.in/nd2_nou19_cs08/preview” by By Dr. JeetendraPande | Uttarakhand Open University, Haldwani
6. Cyber Security,”https://swayam.gov.in/nd2_cec20_cs15/preview”, By Dr.G.PADMAVATHI | Avinashilingam Institute for Home Science & Higher Education for Women,Coimbatore
7. NPTEL course on Cryptography and network security: https://nptel.ac.in/courses/106/105/106105031/
8. **E-books** Huang, Scott C.-H., MacCallum, David, Du, Ding-Zhu (Eds.) , "Network Security", Springer

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 510410- Fundamentals of Blockchain		
Teaching Scheme:	**Credit**	**Examination Scheme:**
TH: 04 hr/week	**04**	**Midsemester: 50 Marks** **End Semester: 50 Marks**

Prerequisite Courses: Basic Knowledge Of Computer Security, Cryptography, Concurrent Or Parallel Programming

Companion Course: Network Security

Course Objectives:

1. To learn three pillars decentralization, transparency & immutability
2. To familiarise the functional/operational aspects of cryptocurrency
3. To know the development of decentralized applications and data storage.
4. To familarize public blockchain platforms BitCoin, Ethereum and blockchain platforms on the cloud.
5. To familarize with smart contracts and decentralized applications.

Course Outcomes:

On completion of the course, learner will be able to–

1. Apply blockchain in distributed application development.
2. Develop decentralized applications in Blockchain.
3. Work with Etherium, Hyperledger.

Unit I	**Introduction**	

Introduction Need for Distributed Record Keeping,Modeling faults and adversaries, Byzantine Generals problem,
Basic crypto primitives: Hash function, Puzzle friendly Hash, Collison resistant hash, Digital Signature -ECDSA, Memory Hard Algorithm, Zero Knowledge Proof, Technologies Borrowed in Blockchain – hash pointers, consensus, byzantine fault-tolerant distributed computing, digital cash etc.

Mapping of Course Outcomes for Unit I	

Unit II	**Blockchain Basics**	

Basic Distributed Computing, Atomic Broadcast, transactions, formation of blocks, Blockchain Network, Mining Mechanism, consensus algorithms and their scalability problems, Distributed Consensus, Merkle Patricia Tree, Gas Limit, Transactions and Fee, Anonymity, Reward, Chain Policy, Life of Blockchain application, Soft & Hard Fork, Private and Public blockchain.

Mapping of Course Outcomes for Unit II	

Unit III	**Distributed Consensus**	

Verifiable random functions, Zero-knowledge systems, Nakamoto consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy utilization and alternate.

Mapping of Course Outcomes for Unit III	

Unit IV	**Bitcoin Blockchain**	

Bitcoin blockchain, wallet, blocks, Merkley tree, hardness of mining, transaction verifiability, anonymity, forks, double spending, mathematical analysis of properties of Bitcoin, the challenges, and solutions, The Turing Completeness of Smart Contract Languages and verification challenges.

Mapping of Course Outcomes for Unit IV		
Unit V	**Hyperledger and Ethereum**	

Hyperledger architecture, membership,blockchain, transaction, chaincode, Hyperledger fabric, features of hyperledger, the plug and play platform and mechanisms in permissioned blockchain, Ethereum Virtual Machine (EVM), Ethereum subprotocols, Wallets for Ethereum , Solidity, Smart Contracts
, some attacks on smart contracts, Using smart contracts to enforce legal contracts, comparing Bitcoin scripting vs. Ethereum Smart Contracts, Bitcoin vs Ethereum vs Hyperledger.

Mapping of Course Outcomes for Unit V		
Unit VI	**Security in Blockchain and Use Cases**	

Privacy, Security issues in Blockchain : Pseudo-anonymity vs. anonymity, Zcash and Zk-SNARKS for anonymity preservation, attacks on Blockchains –Sybil attacks, selfish mining, Sharding based consensus algorithms to prevent these, blockchain use cases - Financial services, Supply chain management, Government.

Case Studies (if any)	Uses of Blockchain in E-Governance, Land Registration, Medical Information Systems, and others
Mapping of Course Outcomes for Unit VI	

Books & Other Resources:

Reference Books:

1. Draft version of "S. Shukla, M. Dhawan, S. Sharma, S. Venkatesan, 'Blockchain Technology: Cryptocurrency and Applications', Oxford University Press, 2019.
2. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform, 2017.

MOOC Courses https://swayam.gov.in/nd1_noc20_cs01/

Important links:

1. https://github.com/anders94/blockchain-demo
2. https://anders.com/blockchain/
3. https://blockgeeks.com/guides/what-is-blockchain-technology/

Savitribai Phule Pune University, Pune
ME Cyber Security (2020 Course)
510411A - Machine Learning for Security (Elective II)

Teaching Scheme:	Credit	Examination Scheme:
TH: 5 hr/week	05	Mid semester: 50 Marks End Semester: 50 Marks

Prerequisite Courses:

8. Linear Algebra and Calculus
9. Probability Basics
10. Basics of AI and ML

Companion Course: Network Security

Course Objectives:

11. To understand basic concepts of the machine learning
12. To develop problem solving ability using machine learning algorithms
13. To detect, analyse and classify malware using machine learning algorithm
14. To study anomaly detection and analyse network traffic
15. To understand personal and customer web security issues
16. To study adversarial Machine Learning concept for security

Course Outcomes:

On completion of the course, learner will be able to–

CO1: Use of machine learning algorithms for different applications
CO2: Solve the security issues using machine learning techniques
CO3: Provide solution for real time security problems using machine learning algorithms
CO4: Develop awareness of latest trends and advances in security using machine learning
CO5: Protect Consumer Web problems and provide solution using machine learning
CO6: Apply adversarial Machine Learning concept for security

Unit I	Machine learning in security	08

Introduction to Machine Learning: Supervised Machine Learning, Unsupervised Machine Learning, Semi-supervised Machine Learning, Reinforcement Machine Learning, Regression and its types. Applications of machine learning, Real-World Uses of Machine Learning in Security, Spam Fighting: An Iterative Approach, Limitations of Machine Learning in Security

Case Studies	Taxonomy of machine learning algorithms
Mapping of Course Outcomes for Unit I	CO1

Unit II	Clustering and Malware Classification	08

Supervised Classification Algorithms: Naive Bayes Classifier, Support Vector Machines (SVM), Decision Trees, Decision Forest, Nearest Neighbor, Neural Network. Practical Considerations in Classification: Selecting a Model Family, Training Data Construction, Feature Selection, Overfitting and Underfitting, Choosing Thresholds and Comparing Models.

Clustering: K-means, Hierarchical clustering, Fuzzy C-Means Clustering, Density-Based Clustering, State of the Art of Clustering Applications.

Case Studies (if any)	Exploiting XSS Vulnerability in C&C Panels to Detect Malwares	
Mapping of Course Outcomes for Unit II	CO1, CO2	
Unit III	**Anomaly detection and Network Traffic Analysis Using ML**	**08**
Anomaly Detection: Feature Engineering for Anomaly Detection, Anomaly Detection with Data and Algorithms, Challenges of Using Machine Learning in Anomaly Detection Network Traffic Analysis: Theory of Network Defense, Building a Predictive Model to Classify Network Attacks.		
Case Studies (if any)	Network Anomaly Detection Using k-means Stages of a network attack	
Mapping of Course Outcomes for Unit III	CO2, CO3	
Unit IV	**Malware: detection & analysis using SVM**	**08**
Malware Detection using support vector machine: Malware Detection, Maximizing the Margin and Hyper plane Optimization, Lagrange Multiplier, Kernel Methods, Permission-Based Static Android Malware Detection Using SVM. Malware Analysis: Defining Malware Classification, Malware: Behind the Scenes, Feature Generation, Data Collection, Generating Features, Feature Selection, From Features to Classification, How to Get Malware Samples and Labels		
Case Studies (if any)	1.API Call-Based Static Android Malware Detection Using SVM	
Mapping of Course Outcomes for Unit IV	CO3, CO4	
Unit V	**Protecting the Consumer Web**	**06**
Consumer Web: Monetizing the Consumer Web, Types of Abuse and the Data That Can Stop Them - Authentication and Account Takeover, Account Creation, Financial Fraud, Bot Activity, Supervised Learning for Abuse Problems- Labeling Data, Cold Start Versus Warm Start, False Positives and False Negatives, Multiple Responses, Large Attacks, Clustering Abuse- Example: Clustering Spam Domains, Generating Clusters, Scoring Clusters		
Case Studies (if any)	Privacy in e-Shopping Transactions: Exploring and Addressing the Trade-Offs	
Mapping of Course Outcomes for Unit V	CO4, CO5	
Unit VI	**Adversarial Machine Learning for security**	**08**
The Importance of Adversarial ML, Security Vulnerabilities in Machine Learning Algorithms, Attack Transferability, Attack Technique: Model Poisoning, Example: Binary Classifier Poisoning Attack, Attacker Knowledge, Defense Against Poisoning Attacks, Evasion Attack, Example: Binary Classifier Evasion Attack, Defense Against Evasion Attacks		
Case Studies (if any)	Adversarial Attacks on Image Classification and Malware Detection	
Mapping of Course Outcomes for Unit VI	CO5, CO6	
Books & Other Resources:		

Textbooks:

✔ Machine Learning and Security Protecting Systems with Data and Algorithms by Clarence Chio David Freeman, 1st edition, ISBN-978-1-491-97990-7

✔ Machine Learning Approaches In Cyber Security Analytics by Tony Thomas, Athira P Vijayaraghavan, Sabu Emmanuel, Springer, ISBN 978-981-15-1705-1

Reference Books:

1. Hands-On Machine Learning for Cybersecurity Safeguard your system by making your machines intelligent using the Python ecosystem by Soma Halder, Sinan Ozdemir, ISBN 978-1-78899-228-2
2. Introduction to Machine Learning with Applications in Information Security by Mark Stamp, CRC Press, ISBN- 978-1-138-62678-2.
3. Machine learning for computer and cyber security principles, algorithms, and practices by Gupta, Brij Sheng, Quan Z, CRC Press, ISBN - 978-1-138-58730-4.

MOOC Courses

7. https://nptel.ac.in/courses/106/106/106106139/
8. https://nptel.ac.in/courses/106/106/106106202/
9. https://www.classcentral.com/course/independent-machine-learning-security-12651

Important links:

1. https://www.cisco.com/c/en/us/products/security/machine-learning-security.html#:~:text=In%20security%2C%20machine%20learning%20continuously,by%20uncovering%20suspicious%20user%20behavior.
2. https://www.mdsny.com/5-top-machine-learning-use-cases-for-security/

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 510411-B Digital Forensics (Elective-II)		
Teaching Scheme:	**Credit**	**Examination Scheme:**
TH: 5 hr/week	**05**	**Mid semester: 50 Marks End Semester: 50 Marks**

Prerequisite Courses: Computer Network

Companion Course: Network Security

Course Objectives:

3. Understand the basic digital forensics concepts and techniques for conducting the forensic examination on different digital devices.
4. To understand how to examine digital evidences gathered through such as the data acquisition, identification analysis.
5. To understand the basics of Computer forensics and cyber forensics, mobile phone forensics, network forensics, Email forensics and web forensics etc.

Course Outcomes:
On completion of the course, learner will be able to–

- identify the background of various forensic techniques
- to analyze digital crime
- to use different types of tools for various phases of forensics investigation
- prepare report as per standards of digital forensics.
- to select correct tools and techniques for a particular case.
- know how to apply forensic analysis tools to recover important evidence for identifying computer crime

Unit I	**Fundamentals of Digital Forensics**	**7**

Foundations of Digital Forensic: Digital evidence, Awareness, Principles of Digital Forensic, Challenging aspects of digital evidence, Cybertrail. Language of Computer Crime Investigation: Role of Computers in crime, Cybercrime law, offenses, jurisdiction. Traffic analysis, Fraud, IT Act

Case Studies (if any)	17. Discuss about challenges faced in forensics in recent digital crime. 18. Case studies of recent cases of various frauds
Mapping of Course Outcomes for Unit I	**CO1, CO2**

Unit II	**Computer Forensics**	**8**

Digital Evidence : Digital evidence in courtroom: Duty of experts, Admissibility, Locard's exchange principle, Types of Evidence, The Rules of Evidence, Volatile Evidence, Evidence collection and Archiving , Methods of Collection , Collection Steps, Controlling Contamination: The Chain of Custody. **Processing Computer Crime :** Introduction to Crime Scenes, Seizing and storing digital evidence at scene, Documenting the Scene and the Evidence , Dealing with Live Systems and Dead Systems, Using Hashing to Verify the Integrity of Evidence		
Case Studies(if any)	✔ List Challenges faced during live forensics ✔ Discuss Petrol Pump fraud (Computer hardware fraud)	
Mapping of Course Outcomes for Unit II	**CO3, CO4, CO5, CO6**	
Unit III	**Data Acquisition and Data Recovery**	**8**
Data acquisition- Understanding storage formats and digital evidence, determining the best acquisition method, acquisition tools, validating data acquisitions, performing RAID data acquisitions, remote network acquisition tools, other forensics acquisitions tools **Data Recovery :** Data Backup and Recovery, The Role of Backup in Data Recovery, The Data-Recovery Solution Hiding and Recovering Hidden Data , Data Handling tools		
Case Studies(if any)	Role of Forensics Laboratory in Data acquisition and Data recovery report making.	
Mapping of Course Outcomes for Unit III	**CO3, CO4, CO5, CO6**	
Unit IV	**Network Forensics**	**8**
Introduction, Network basics for digital investigators: History, Technical overview, Network Technologies, Connecting networks using Internet Protocols. Applying Forensic Science to Networks: Preparation & Authorization, Identification, Documentation Collection Preservation, Filtering Data reduction, Class / Individual characteristics, evaluation of source, evidence recovery, investigation reconstruction, reporting results. Analyzing network data, Intrusion process, end–to–end forensic investigation. Network addressing scheme: LAN addressing &Internetwork		
Case Studies(if any)	Study of Intrusion prevention and intrusion detection system for network forensics.	
Mapping of Course Outcomes for Unit IV	**CO3, CO4, CO5, CO6**	
Unit V	**Advance Network Forensic**	**9**
Digital evidences gathering at each layer of OSI, Internet gambling investigation, Investing e–mail crimes. Network traffic data sources: Firewalls & Routers, Packet sniffers & Protocol Analyzers, IDS, Security event management software, network forensic analysis tools. Collecting network traffic data: Legal considerations & Technical issues. Examining & Analyzing network traffic data: Identify an event of interest, Examine data sources, Draw conclusions, Attacker identification, Log files as evidence, using multiple logs as evidence, important audit logs.		
Case Studies(if any)	Study of dark web	
Mapping of Course Outcomes for Unit V	**CO3, CO4, CO5, CO6**	

Unit VI	Mobile device Forensic and Email Forensics	8
Mobile Device Forensics, Types of evidence on mobile device, Handling mobile device as a sources of evidence, Forensic prevention of mobile devices, Forensic examination & analysis of mobile devices, Forensic acquisition & examination of SIM cards(Architecture, Data Storage, Files, Mobile Operating System), Investigative reconstruction using mobile devices, Mobile forensics and its challenges **Email Forensics :** E-Mail Header Analysis, Function & Forensics, Chat and Social Networking Evidence **Web forensics and Antiforensics**		
Case Studies(if any)	5. Investigate hosting obscene profiles crime 6. Official website of Maharashtra Govt. Hacked (website hacking) 7. The 'Piranhas' tragedy with children (misleading information on website) 8. Job racket exposed in Mumbai city cybercrime cell (smishing) 9. Killers take tips from '26/11 Attack' to use VOIP (cyberterrorism using VOIP, e–mail forensic)	
Mapping of Course Outcomes for Unit VI	**CO2, CO3, CO4, CO5, CO6**	

Books & Other Resources:

Textbooks:

1. Digital Evidence & Computer Crime – Forensic science, Computers & The Internet', Eoghan Casey, 3rd edition
2. 'Computer Forensics Computer Crime scene investigation', 2nd edition, Johm R. Vacca
3. Cyber Law Simplified, Vivek Sood
4. Basics of Digital Forensics, Second edition – John Sammons

Reference Books:

4. 'Computer Forensics Investigating Network Intrusions & Cybercrime', EC–Council press, Cengage Learning
5. Guide to Computer Forensics & Investigations, 4th edition, Bill Nelson, Amelia Phillips & Christopher Steuart, Cengage Learning
6. 'Guide to Integrating Forensic Techniques into Incident Response', NIST, Karen Kent, Suzanne Chevalier Tim Grance, Hung Dang

MOOC Courses : MOOC Courses: SWAYAM, Coursera, Palo Alto, CEH

Important links: Web Reference:

Ø MIT Open CourseWare: https://ocw.mit.edu/courses/ Ø
SWAYAM: http://nptel.ac.in
http://www.elsevierdirect.com/companion.jsp?ISBN=9780123742681 Ø
WhatsApp Security policy – Technical White Paper

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 510411C: Identity Access & Management		
Teaching Scheme:	**Credit**	**Examination Scheme:**
TH: 5 hr/week		**Mid_semester: 50 Marks** **End_Semester: 50 Marks**
Prerequisite Courses: Modern cryptographtm Network security,		

Course Objectives:
Students will learn to

- Understand the fundamentals of the Identity and access management.
- Study security techniques that identify and authenticate anything trying to gain access to any systems.
- Design and implement identity/access management to control access to resources.
- Build public key infrastructure to manage trust between identity provider and user.

e Outcomes:
mpletion of the course, learner will be able to–

CO1 - **Describe** the importance of identity management
CO2- **Develop** mechanisms to store identity information
CO3- **Describe** the use of directories to manage identities and explores the methodologies for authentication and access control in depth
CO4- **Design** mechanisms to use identity data for access control
CO5- I**mplement** access rights, provide single sign-on mechanism
CO6- **Describe** the use of public key infrastructure for authenticating users and devices
CO7- **Describe** the effective use of identity access and management

Contents

Unit I	**Introduction to Identity Access & Management (IAM)**	

Introduction to identity, Importance of identity management, Enterprise or Organizational Identities, Electronics and non-electronics Identities, Review of Identity and Access Management: Theory & Practice, Access control, Message authenticity, IAM service, User, Principal or Subject, User credentials, Authentication, Security context, Authorization, IAM Role, Role based access management, Identity trust, IAM Session, Single Sign On, Federation

Mapping of Course Outcomes for Unit I	**CO1**

Unit II	**Identity management and data stores**	

Identity management principles, mechanisms to store identity information, Directories: History of identity data stores, Introduction To Ldap and enterprise directories, Ldap Concepts & Architecture, Ldap Replication

Mapping of Course Outcomes for Unit II	**CO2,CO3**

Unit III	**Authentication and Access control**	

Mechanisms to use identity data for access control – authentication and authorization, Multi Factor authentication (Mfa), Provisioning - Principles for the collection of identity data and establishment of entitlements, Role based access control (RBAC)

Mapping of Course Outcomes for Unit III	**CO3,CO4**	
Unit IV	**Single Sign-On and Federation**	
Authentication mechanisms – the importance of single sign, Single Sign-On Techniques, Access Control, Password Management, Introduction to Single Sign on Methods , Federation Overview, Federation Protocols, Benefits of federated authentication, Governance Risk and Compliance		
Mapping of Course Outcomes for Unit IV	**CO5**	
Unit V	**Public key infrastructure**	
Principles of public key infrastructure (PKI), Capabilities, Design, Methods of certification – certificate authorities, web of trust, decentralized PKI		
Mapping of Course Outcomes for Unit V	**CO6**	
Unit VI	**Identity management and case study**	
Introduction – Identity management, identity portrayal, Different identity management models-Local identity, Network identity, Federated identity, Global web identity, Identity management in Internet of Things – User-centric identity management, Device-centric identity management, Hybrid identity management		
Mapping of Course Outcomes for Unit VI	**CO7**	
Books & Other Resources:		
Textbooks: 1. Identity Management: A Primer, Graham Williamson, David Yip **2.** Identity & Access Management: A Systems Engineering Approach By Omondi Orondo, Ph.D **3.** Identity management for Internet of things by Parikshit Mahalle, River Publishers		
Reference Books: 1. Mastering Identity and Access Management with Microsoft Azure Jochen Nickel by Packt Publishing Ltd		

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 510411D: IT Acts and Cyber Crimes		
Teaching Scheme:	**Credit**	**Examination Scheme:**
TH: 5 hr/week	**05**	**Midsemester: 50 Marks** **End Semester: 50 Marks**

Prerequisite Courses: Network security

Companion Course: Laboratory Proficiency- II

Course Objectives:

1. To understand the IT laws and cyber crime basics
2. To know and make use of Information technology laws
3. To understand cyber crime investigation procedure
4. To investigate a cyber crime
5. To know prevention of Cyber Crimes & Frauds
6. To know International Organizations and Their Roles in IT acts and cyber crime

Course Outcomes:

On completion of the course, learner will be able to–

1. To apply the knowledge of IT laws and cyber crime basics
2. To make use of Information technology laws for appropriate cases
3. To apply cyber crime investigation procedure to investigate a cyber crime
4. To contribute for prevention of Cyber Crimes & Frauds
5. To apply knowledge of international Organizations and their Roles in IT acts and cyber crime

Unit I	**Introduction to IT laws & Cyber Crimes**	**7 Hrs.**

Internet, Hacking, Cracking, Viruses, Virus Attacks, Pornography, Software Piracy, Intellectual property, Legal System of Information Technology, Social Engineering, Mail Bombs, Bug Exploits.

Mapping of Course Outcomes for Unit I	**CO1**

Unit II	**Information Technology Law (Cyber Law)**	**8 Hrs.**

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, e – commerce and Laws in India Intellectual Property Rights, Domain Names and Trademark Disputes, Sensitive Personal Data or Information (SPDI) in Cyber, Cloud Computing & Law, Cyber Law:International Perspective (a) EDI: Concept and legal Issues. (b) UNCITRAL Model Law. (c) Electronic Signature Laws of Major Countries (d) Cryptography Laws (e) Cyber Law's of Major Countries (f) EU Convention on Cyber Crime.

Mapping of Course Outcomes for Unit II	**CO2**

Unit III	**Cyber Crime Investigation**	**7 Hrs.**

Cyber Forensics, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Cyber Forensics Tools and Software, Recovering deleted evidence, Password Cracking

Mapping of Course	**CO3**

Outcomes for Unit III		
Unit IV	**Cybercrime and investigation procedures**	**8 Hrs.**
Cyber Forensic and Computer Crimes and types. Crimes targeting Computers: Definition of Cyber Crime & Computer related Crimes, Classification & Differentiation between traditional crime and cyber crimes. (a) Data Theft (b) Hacking (c) Spreading Virus & Worms (d) Phishing (e) Cyber Stalking / Bullying (f) Identity Theft & Impersonation (g) Credit card & Online Banking Frauds (h) Obscenity, Pornography & Child Pornography (i) Cyber Defamation, Defacement, (j) Illegal online selling & Gambling (k) Denial of Service Attacks (l) Cyber terrorism (m)Software Piracy & illegal downloading, Reasons for Cyber Crimes, Cyber Criminal Mode and Manner of Committing Cyber Crime		
Mapping of Course Outcomes for Unit IV	**CO4**	
Unit V	**Prevention of Cyber Crimes & Frauds**	**8 Hrs.**
Critical analysis & loopholes of The IT Act, 2000, Cyber Crimes: Freedom of speech in cyber space & human right issues, Investigation of Cyber Crimes, Investigation of malicious applications, Agencies for investigation in India, their powers and their constitution as per Indian Laws Procedures followed by First Responders; Search and Seizure Procedures of Digital Evidence, Securing the Scene , Documenting the Scene, Evidence Collection and Transportation (a) Data Acquisition (b) Data Analysis (c) Reporting Digital Forensics (a) Computer Forensics (b) Mobile Forensics (c) Forensic Tools (d) Anti – Forensics, Electronic / Digital Evidence laws & cases Laws		
Mapping of Course Outcomes for Unit V	**CO5**	
Unit VI	**International Organizations and Their Roles**	**8 Hrs.**
(a) ICANN (b) URDP (c) WTO and TRIPS (d) Interpol & Europol (e) Impact of Cyber warfare on Privacy Identity (f) Net Neutrality and EU Electronic communication Regulatory framework (g) WCAG (h) Social Networking sites Vis – a – Vis Human Right, Case Laws : Indian & International Cases		
Mapping of Course Outcomes for Unit VI	**CO5**	

Books & Other Resources:

Textbooks:

1. **Cyber Security: Understanding cyber crimes, computer forensics and legal perspectives, Nina Godbole and Sunit Belapure, ISBN: 9788126521791, Wiley Publication**
2. **Handbook Of Computer Crime Investigation Forensic Tools And Technology, Edited by Eoghan Casey, Academic Press, ISBN 0-12-163103-6**

Reference Books:

1. **Cyber Criminology: Exploring Internet Crimes and Criminal Behavior, Edited by K. Jaishankar, CRC Press, ISBN 978-1-4398-2949-3**
2. **Mark Merkow, "Information Security-Principles and Practices", Pearson Ed., ISBN- 978-81-317-1288-7**

Web resources:

1. **https://www.meity.gov.in/content/cyber-laws**
2. **https://www.meity.gov.in/cyber-security**
3. **https://www.indiacode.nic.in/**

Semester- III

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 510401- Cloud Security		
Teaching Scheme:	**Credit**	**Examination Scheme:**
TH: 4 hr/week	**04**	**Midsemester: 50 Marks** **End Semester: 50 Marks**
Prerequisite Courses: Network Security		
Course Objectives: The course on cloud security introduces the basic concepts of security systems The course will describe the Cloud security architecture and explore the guiding security design principles.		
Course Outcomes: **On completion of the course, learner will be able to–** CO1 : Understand fundamentals of cloud computing architectures based on current standards, protocols, and best practices CO2: Identify the known threats, risks, vulnerabilities and security concerns associated with Cloud CO3: Design the security architecture for Data. CO4: Design security architecture that assures identity and access management. CO5: Explain security management in the cloud CO6: Describe privacy concerns in cloud		
Unit I	**Introduction to Cloud Computing and Security**	
Understanding Cloud Computing, IT Foundation for Cloud, Roots of Cloud Computing, Brief Primer on Security, Brief Primer on Architecture, Cloud Computing Architecture-Cloud Reference Architecture, Control over Security in the Cloud Model, Cloud Deployment., Services Models, How Clouds Are Formed and Key Examples, Real-world Cloud Usage Scenarios		
Mapping of Course Outcomes for Unit I	**CO1**	
Unit II	**Security Concerns and Cloud Security Architecture**	
Cloud Computing: Security Concerns, Assessing Your Risk Tolerance in Cloud Computing, Legal and Regulatory Issues, Security Requirements for the Architecture, Security Patterns and Architectural Elements, Cloud Security Architecture, Planning Key Strategies for Secure Operation .		
Mapping of Course Outcomes for Unit II	**CO2**	
Unit III	**Securing the Cloud: Data Security**	
Overview of Data Security in Cloud Computing, Data Encryption: Applications and Limits, Cloud Data Security: Sensitive Data Categorization, Cloud Data Storage, Cloud Lock-in		
Mapping of Course Outcomes for Unit III	**CO3**	
Unit IV	**Identity and Access Management**	

Trust Boundaries and IAM, IAM Challenges, IAM Definitions, IAM Architecture and Practice, Relevant IAM Standards and Protocols for Cloud Services, IAM Practices in the Cloud, Cloud Authorization Management, Cloud Service Provider IAM Practice		
Mapping of Course Outcomes for Unit IV	**CO4**	
Unit V	**Security Management In The Cloud**	
Security Management Standards, Security Management in the Cloud, Availability Management, SaaS Availability Management, PaaS Availability Management, IaaS Availability Management, Access Control, Security Vulnerability, Patch, and Configuration Management		
Mapping of Course Outcomes for Unit V	**CO5**	
Unit VI	**Privacy and Privacy Tools**	
What Is Privacy?, What Is the Data Life Cycle?, What Are the Key Privacy Concerns in the Cloud?, Who Is Responsible for Protecting Privacy?, Changes to Privacy Risk Management and Compliance in Relation to Cloud Computing, Privacy Tools and Best Practices, 2-factor authentication, secure email for cloud storage, Deletion of private data, security as service, distributed cloud storage, what are best practices, cloud data security and check list, Future of cloud data security		
Mapping of Course Outcomes for Unit VI	**CO6**	
Books & Other Resources:		
Textbooks: Vic (J.R.) Winkler , "Securing the Cloud: Cloud Computer Security Techniques and Tactics", ISBN:159749593X Tim Mather, Shahed Latif, Subra Kumaraswamy, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'Reilly Media, SBN-13: 978-0596802769, ISBN-10: 0596802765		
Reference Books: 5. Ronald L Krutz and Russell Dean Vines , "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", ISBN:0470938943 6. Imad M. Abbadi, "Cloud Management and Security", ISBN: 1118817079 7. Sumner Blount, Rob Zanella, "Cloud Security and Governance: Who's on Your Cloud?", ISBN: 1849280908 8. Ryan Ko, Raymond Choo, "The Cloud Security Ecosystem: Technical, Legal, Business", ISBN: 0128017805		
MOOC Courses **2. Cloud computing,** By Prof. Soumya Kanti Ghosh | IIT Kharagpu **https://swayam.gov.in/nd1_noc20_cs65/preview** **3.** Cloud Computing and Distributed Systems By Prof. Rajiv Misra | IIT Patna **https://swayam.gov.in/nd1_noc20_cs48/preview**		
E-books Cloud Security: Introduction to cloud security and data protection Kindle Edition by Nate Jenne		

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 510402: Cyber Security and IT Infrastructure Protection		
Teaching Scheme:	**Credit**	**Examination Scheme:**
TH: 4 hr/week	**04**	**Midsemester: 50 Marks** **End Semester: 50 Marks**
Prerequisite Courses:		
Companion Course:		
Course Objectives: **1. To understand the basics of cyber security** **2. Get acquainted with the process of securing oneself against the cyber attacks** **3. To know the concepts, issues and applications of infrastructure management**		
Course Outcomes: **On completion of the course, learner will be able to–** **1. Explain the cyber attacks and need of cyber security** **2. Demonstrate a cyber attack on a web application** **3. Recognize the objectives and benefits of infrastructure management** **4. Compare the software used for infrastructure management** **5. Compare security implementations for storage networking**		
Unit I	**Cyber security: Introduction**	
Introduction, Cybercrime, harassment, cyber warfare, cyber surveillance, cyber targets, cyber vulnerabilities and impacts, cyber threats		
Case Studies (if any)	**OWASP threats**	
Mapping of Course Outcomes for Unit I	**CO1**	
Unit II	**Improving cyber security**	
Risk management, business continuity and disaster recovery, basic cyber security steps, cyber security steps, awareness, training, information sharing		
Case Studies (if any)	Attack a web application in controlled environment.	
Mapping of Course Outcomes for Unit II	**CO1, CO2**	
Unit III	**Infrastructure Management**	
What is Infrastructure Management, Basic Framework, Policy Issues, Types of Infrastructure Management: Systems Management, Network Management, Storage Management, Objectives, Benefits of Infrastructure Management system		
Mapping of Course Outcomes for Unit III	**CO3**	
Unit IV	**IT Infrastructure Management**	
Components of IT Infrastructure, Hardware resources, Data storage, Input-output Technologies used in Businesses, Types of Computer Software used for Infrastructure Management in Business, Principle Issues, Foundations of Business Intelligence:Databases and Information Management, Telecommunications, Wireless Technology, Security		

Mapping of Course Outcomes for Unit IV	**CO4**	
Unit V	**Key system applications**	
Achieving Operational Excellence and Customer Intimacy:Enterprise Applications, E-Commerce: Digital Markets, Digital Goods, Improving Decision Making and Managing Knowledge,Building Information Systems, Ethical and Social Issues in Information Systems		
Mapping of Course Outcomes for Unit V	**CO4**	
Unit VI	**Securing & Managing the Storage Infrastructure**	
Storage Security Framework, Risk Triad, Storage Security Domains, Security Implementations in Storage Networking, Monitoring the Storage Infrastructure, Storage Management Activities, Storage Infrastructure Management Challenges		
Books & Other Resources:		
Textbooks: **1. David Sutton, "Cyber Security: A Practitioner's guide", O'Reilly (BCS Learning & Development Limited). ISBN: 9781780173405** **2. 'Essentials of Business Information Systems', by Jane P. Laudon,Azimuth Information Systems, Pearson, ISBN-10: 0132277816 • ISBN-13: 97801322778152.** **3. Introduction to IMS, An: Your Complete Guide to IBM Information Management System", by Barbara Klein, Richard Alan Long, Kenneth Ray Blackman, IBM Press, ISBN-10: 0132886871, ISBN-13: 97801328868713** **3. Managing Information Systems: Strategy and Organisation', by David Boddy, Albert Boonstra, Financial Times Press,ISBN-10: 0273716816, ISBN-13: 9780273716815** **4. EMC Educational Services, "Information Storage and Management", Wiley India**		

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 510403A: IoT and Embedded Systems Security (Elective-III)		
Teaching Scheme:	**Credit**	**Examination Scheme:**
TH: 05 hr/week	**05**	**Mid semester: 50 Marks** **End Semester: 50 Marks**

Prerequisite Courses: IOT and Embedded Systems

Companion Course: Cloud Security

Course Objectives:

- Understand the basics of security in IOT and Embedded systems
- Identify and analyze security problems .
- Explore the various Technologies of IOT and Embedded systems security.
- Effectively apply their knowledge to the construction of secure systems development

Course Outcomes:

On completion of the course, learner will be able to–

- Analyze security requirements of system development.
- Develop secure systems and the software.
- Inter-relate security and software development.

Unit I	**Introduction to Embedded System and Internet of Things**	7

▪ Application Domain and Characteristic of Embedded System, ▪ Real time systems and Real-time scheduling, ▪ Processor basics and System-On-Chip, ▪ Introduction to ARM processor and its architecture. IoT: ▪ Definition and characteristics of IoT, ▪ Internet of Things: Vision, Emerging Trends, Economic Significance, ▪ Technical Building Blocks, Physical design of IoT, Things of IoT, , IoT functional blocks, ▪ IoT communication models, IoT Issues and Challenges, Applications

Case Studies (if any)	**In a typical factory environment significance of Energy Management System(EMS). It will help monitor the energy consumption of entire factory and individual equipment especially energy guzzlers. Predictive alerts can be generated and to be sent based on the hierarchy.**

Unit II	**IoT Protocols and Security**	8

Protocol Standardization for IoT, ▪ M2M and WSN Protocols, ▪ SCADA and RFID Protocols, ▪ Issues with IoT Standardization, ▪ Unified Data Standards, ▪ Protocols – IEEE 802.15.4, ▪ BACNet Protocol, Modbus, KNX, Zigbee Architecture, ▪ Network layer, APS layer. ▪IoT Security: • Vulnerabilities of IoT, Security Requirements, • Challenges for Secure IoT, Threat Modeling, • Key elements of IoT Security: Identity establishment, Access control, Data and message security, Non-repudiation and availability, • Security model for IoT Security framework for IOT, Light weight cryptography, Asymmetric LWC Algorithms, Key agreement, Distribution, and Bootstrapping

Case Studies (if any)	**Define security architecture for EMS mentioned above for the end to end factory setup for the remote access of EMS data.**

Unit III	**Embedded Security :**	8

Introduction, Types of Security Features – Physical, Cryptographic, Platform. Kinds of Devices – CDC, CLDC. Embedded Security Design, Keep It Simple and Stupid Principle, Modularity Is Key, Important Rules in Protocol Design, Miniaturization of security, Wireless Security, Security in WSN.

Case Studies (if any)	**Define MODBUS TCP / MODBUS RTU security in a factory to collect data in EMS from Smart meters or PLCs**

Unit IV	**Choosing and optimizing cryptographic**	8

	algorithms for resource constrained systems	
Do e need cryptography, Hashing,to optimize or not to otimize,choosing cryptographic algorithms,Tailoring security for your application.		
Case Studies (if any)	**Management of Sensor Based Bridges.**	
Unit V	**IoT Application Development**	
Application Protocols MQTT, REST/HTTP, CoAP, MySQL Back-end Application Design Apache for handling HTTP Requests, PHP & MySQL for data processing, MongoDB Object type Database, HTML, CSS & jQuery for UI Designing, JSON lib for data processing, Security & Privacy during development, Application Development for mobile Platforms: Overview of Android / IOS		
Case Studies (if any)	Create a small dashboard application to be deployed on cloud. Different publisher devices can publish their information and interested application can subscribe You can explore the same Energy Management System example	
Unit VI		8
Embedded IoT Platform Design Methodology , Purpose and requirement specification, Process specification, Domain model specification, information model specification, Service specifications, IoT level specification, Functional view specification, Operational view specification, o Device and component integration, Application development		
Case Studies (if any)	Develop a Real-time application like a smart home with following requirements: If anyone comes at door the camera module automatically captures his image send it to the email account of user or send notification to the user. Door will open only after user's approval.	

Books & Other Resources:

Textbooks:

- Practical Embedded Security: Building Secure Resource Constrained Systems - Timothy Stapko, Publisher Newnes.
- Honbo Zhou, "The Internet of Things in the Cloud: A Middleware Perspective", CRC Press, 2012. ISBN : 9781439892992
- Internet of Things Principles and Paradigms Rajkumar Buyya, Amir Vahid Dastjerdi, ISBN : 978-0-12-805395-9, Morgan Kaufmann
- Olivier Hersent, Omar Elloumi and David Boswarthick, "The Internet of Things: Applications to the Smart Grid and Building Automation", Wiley, 2012, 9781119958345

Practical Embedded Security Building Secure Resource-Constrained Systems Author: Timothy Stapko

Reference Books:

1. Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, Dr. Ovidiu Vermesan, Dr. Peter Friess, River Publishers
Interconnecting Smart Objects with IP: The Next Internet, Jean-Philippe Vasseur, Adam Dunkels, Morgan Kuffmann
2. The Internet of Things: From RFID to the Next-Generation Pervasive Networked Lu Yan, Yan Zhang, Laurence T. Yang, Huansheng Ning
3. Internet of Things (A Hands-on-Approach) , Vijay Madisetti , Arshdeep Bahga
4. Designing the Internet of Things , Adrian McEwen (Author), Hakim Cassimally
5. Asoke K and Roopa R Yavagal, "Mobile Computing," Tata McGraw Hill, 2010.

Savitribai Phule Pune University, Pune
ME Cyber Security (2020 Course)
510403B: Malware Analysis and Reverse Engineering (Elective-III)

Teaching Scheme:	Credit	Examination Scheme:
TH: 5 hr/week	05	Midsemester: 50 Marks End Semester: 50 Marks

Prerequisite Courses: Software Engineering

Companion Course:

Course Objectives:

1. To learn reverse engineering and malware detection conceptually
2. To learn static analysis and dynamic analysis
3. To acquire knowledge of malware functionalities and persistence
4. To learn advanced techniques for malware detection and reverse engineering

Course Outcomes:
On completion of the course, learner will be able to–
-understand need of malware analysis
-understand employability reverse engineering
-understand use of advanced techniques of malware detection

Unit I	Introduction to Malware Analysis and Reverse Engineering	08 hrs

Introduction to Malware Analysis: What Is Malware? What Is Malware Analysis? Why Malware nalysis? Types of Malware Analysis, Setting Up the Lab Environment, Malware Sources

What Is Reverse Engineering? Software Reverse Engineering: Reversing, Reversing pplications, Security-Related Reversing, Reversing in Software Development, Low-Level Software, The Reversing Process, The Tools, Is Reversing Legal?, Code Samples & Tools

Reversing Tools: Different Reversing Approaches, Disassemblers, Debuggers, Decompilers, System-Monitoring Tools, Patching Tools, Miscellaneous Reversing Tools, Executable-Dumping Tools

Reversing Malware: Malware Vulnerability, Polymorphism, Metamorphism, Establishing a Secure Environment, The Backdoor. Hacarmy.

Unit II	Static Analysis and Dynamic Analysis	08 hrs

Static Analysis: Determining the File Type, Fingerprinting the Malware, Multiple Anti-Virus Scanning, Extracting Strings, Determining File Obfuscation, Inspecting PE Header Information, Comparing And Classifying The Malware

Dynamic Analysis: Lab Environment Overview, System And Network Monitoring, Dynamic nalysis (Monitoring) Tools, Dynamic Analysis Steps , Putting it All Together: Analyzing a Malware Executable, Dynamic-Link Library (DLL) Analysis

Unit III	Malware Functionalities and Code Injection	08 hrs

Malware Functionalities and Persistence: Malware Functionalities, Downloader , Dropper, Keylogger, Malware Replication Via Removable Media, Malware Command and Control (C2), PowerShell-Based Execution, Malware Persistence Methods, Running the Registry Key, Scheduled Tasks, Startup Folder , Winlogon Registry Entries, Image File Execution Options, Accessibility Programs, AppInit_DLLs, DLL Search Order Hijacking, COM hijacking, Service

Code Injection and Hooking : Virtual Memory, User Mode And Kernel Mode, Code Injection Techniques, Remote DLL Injection, DLL Injection Using APC (APC Injection), DLL Injection Using SetWindowsHookEx(), DLL Injection Using The Application Compatibility Shim, Remote Executable/Shellcode Injection, Hollow Process Injection (Process Hollowing), Hooking Techniques

Unit IV	Malware Techniques and Hunting Malware	08 hrs

Malware Obfuscation Techniques: Simple Encoding , Caesar Cipher, Base64, Encoding, XOR Encoding, Malware Encryption, Identifying Crypto Signatures Using Signsrch, Detecting Crypto Constants Using FindCrypt, Decrypting In Python, Custom Encoding/Encryption, Malware Unpacking, Automated Unpacking

Hunting Malware Using Memory Forensics: Memory Forensics Steps, Memory Acquisition, Volatility Overview , Enumerating Processes, Listing Process Handles , Listing DLLs , Dumping an Executable and DLL, Listing Network Connections and Sockets, Inspecting Registry, Investigating Service, Extracting Command History

Unit V	Advanced Malware Detection and Antireversing Techniques	08 hrs

Detecting Advanced Malware Using Memory Forensics: Detecting Code Injection, Investigating Hollow Process Injection, Detecting API Hooks, Kernel Mode Rootkits, Listing Kernel Modules, I/O Processing, Displaying Device Trees, Detecting Kernel Space Hooking, Kernel Callbacks And Timers

Antireversing Techniques
Why Antireversing?, Basic Approaches to Antireversing,, Eliminating Symbolic Information , Code Encryption, Active Antidebugger Techniques, Confusing Disassemblers, Code Obfuscation , Control Flow Transformations, Data Transformations

Unit VI	Languages and Techniques	08 hrs

Reversing Bytecode Languages: .NET, Java
Scripts and Macros: Reversing, Deobfuscation, and Debugging: VBScript, JavaScript
Analyzing Android Malware Samples: Malware behavior patterns, Attack stages, advanced techniques, Static and dynamic analysis of threats

Books & Other Resources:

1. **Textbooks:** "Learning Malware Analysis ",Monnappa K A, Publisher: Packt Publishing, 2018, ISBN 978-1-78839-250-1
2. "Mastering Malware Analysis ",Alexey Kleymenov, Amr Thabet, Publisher: Packt Publishing, 2019, ISBN 978-1-78961-078-9
3. "Reversing: Secrets of Reverse Engineering ",Eldad Eilam, Publisher: Wiley Publishing, Inc., 2005, ISBN -13: 978-0-7645-7481-8

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 510403C- Steganography and Digital Watermarking (Elective-III)		
Teaching Scheme:	**Credit**	**Examination Scheme:**
TH: 5 hr/week	**05**	**Midsemester: 50 Marks** **End Semester: 50 Marks**
Prerequisite Courses: Mathematical Foundations for Information Security		

Course Objectives:

1. To learn about the watermarking models, message coding, watermark security and authentication.
2. To learn about stegnography, hiding techniques and tools, steganalysis,
3. To Demonstrate how to develop and implement methods to guarantee the authenticity of digital media
4. Explains the categorization of digital watermarking techniques based on characteristics as well as applications

Course Outcomes:
On completion of the course, learner will be able to–

1. Know the History, importance and Applications of steganography and watermarking and properties of steganography and watermarking
2. Demonstrate Models and algorithms of steganography and watermarking
3. Identify potential in various media for hiding the secret information and preserving authentication of Information
4. Analyze the potential of different steganography, steganalysis and watermarking techniques

Unit I	**Introduction to Steganography and Watermarking**	

Information hiding, Steganography and watermarking, History and Importance of Steganography and watermarking, Steganography communication – Notation and terminology – Information theoretic foundations of steganography, Basic concepts of watermarking, Watermark creation, insertion and Extraction, Applications of Steganography and watermarking, Desired Properties of Steganography and watermarking, Evaluating steganography systems, Evaluating watermarking systems

Case Studies (if any)	Tutorial 1 - Understanding digital image formats Tutorial 2 - Working with JPEG images in MATLAB/Python
Mapping of Course Outcomes for Unit I	**CO1**

Unit II	**Steganography Models and Techniques**	

Steganography by cover selection and synthrsis, LSB Embedding, Steganography in palette Images Practical steganographic methods- Model preserving steganography, Steganography by mimicking natural processing, Steganalysis-aware steganography, Minimal impact steganography, Minimizing the embedding impact – Steganalysis		
Case Studies(if any)	Tutorial 3 - LSB Embedding Tutorial 4 - Steganography in palette images	
Mapping of Course	**CO2**	
Outcomes for Unit II		
Unit III	**Steganographic Security and Tools**	
Information theoretic definition: KL Divergence as a measure of security, KL Divergence for Benchmarking, Perfectly Secure Steganography: Perfect security and compression, Perfect security with respect to model, Secure stegosystems with limited embedding distortion: Spread spectrum steganography, Stochastic quantization index modulation, Complexity theoretic approaches, Steganography Tools, Steganalysis Tools		
Case Studies(if any)	Tutorial 5 - Spread spectrum image steganography Tutorial 6 - Steganography Tools / Steganalysis Tools	
Mapping of Course Outcomes for Unit III	**CO2,CO3,CO4**	
Unit IV	**Models and Techniques of Watermarking**	
Desired Characteristics of Watermarks, triangle of robustness, transparency and capacity, General Framework and Life cycle Stages for Digital Watermarking, Technical Challenges of watermarking Types/Classification of Digital Watermarking (visible, invisible, robust, fragile, Semi fragile, Invisible-Robust, Invisible-Fragile, Communication based models of watermarking, Geometric models of watermarking, Watermarking Approaches: Spatial Domain (Additive, LSB, Texture mapping coding Technique, Patchwork Algorithm, Correlation-Based Technique, Watermarking Approaches: Frequency Domain (DCT, DWT, DFT), Detecting multi-symbol watermarks, Evaluation and benchmarking		
Case Studies(if any)	Tutorial 7- Visible Image Watermark: creation, insertion and Extraction and Tools Tutorial 8 - Invisible Image Watermark: creation, insertion and Extraction and Tools	
Mapping of Course Outcomes for Unit IV	**CO2**	
Unit V	**Watermarking of Digital Images**	
A formal generic watermarking model, Visible and In-Visible watermarking Techniques in spatial domain, Visible and In-Visible watermarking Techniques in frequency domain Spread spectrum watermarking Techniques for Digital images, Medical Image Watermarking Photo Watermarking Softwares, Audio watermarking: Requirements, Algorithms and Benchmarking, Video watermarking: Requirements, Algorithms and Benchmarking		
Case Studies(if any)	Tutorial 9 - Audio Watermark: creation, insertion and Extraction and Tools Tutorial 10 - Video Watermark: creation, insertion and Extraction and Tools	
Mapping of Course Outcomes for Unit V	**CO3**	
Unit VI	**Attacks, Security and Tools of Watermarking**	

Security requirements – Watermark security and cryptography, Watermark detection and extraction Techniques, Types of Attacks – Noise like signal processing, Geometric Distortions, Mosaic Attacks, Stir Mark Attacks, Geometric Attacks, Forgery Attacks, Robustness, Presentation and Counterfeiting Attacks, Countermeasures against various attacks, Benchmarking: Stirmark, CERTIMARK	
Case Studies(if any)	Tutorial 11 - Detecting multi-symbol watermarks Tutorial 12 - Case study of Tools of Watermarking
Mapping of Course Outcomes for Unit VI	**CO2, CO3, CO4**

Books & Other Resources:

Textbooks:

1. Steganography in Digital Media: Principles, Algorithms and Applications, 1st Edition, Fridrich, Jessica (For Unit No. 1,2,3) Publisher: Cambridge University Press; 1 edition (December 21, 2009)

2. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, “Digital Watermarking and Steganography”, Margan Kaufmann Publishers, New York, 2008.

3. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, “Digital Watermarking”, Margan Kaufmann Publishers, New York, 2003. L T P C 3 0 0 3 Page 35 of 44

4. Michael Arnold, Martin Schmucker, Stephen D. Wolthusen, “Techniques and Applications of Digital Watermarking and Contest Protection”, Artech House, London, 2003.

5. Juergen Seits, “Digital Watermarking for Digital Media”, IDEA Group Publisher, New York, 2005.

Reference Books:

1. Ruchira Naskar, Rajat Subhra Chakraborty, "Reversible Digital Watermarking: Theory and Practices", Morgan & Claypool Publishers
2. Frank Y. Shih,"Digital Watermarking and Steganography: Fundamentals and Techniques", Taylor & Francis

MOOC Courses

Ethical Hacking By Prof. Indranil Sen Gupta | IIT Kharagpur

E-books

Wang, Feng-Hsing, "Innovations in Digital Watermarking Techniques", Springer publications

Savitribai Phule Pune University, Pune
ME Cyber Security (2020 Course)
510403D - Privacy and Security in Digital World (Elective-III)

Teaching Scheme:	Credit	Examination Scheme:
TH: 05 hr/week	05	Midsemester: 50 Marks End Semester: 50 Marks

Prerequisite Courses: Basics of Cyber Security

Course Objectives:

1. To understand security threats for Digital World.
2. To analyze all the different ways how malware infects a computer.
3. To provide understanding of security issues in online world and social networking.
4. To understand privacy spanning in Big data and Mobile Devices.
5. To understand privacy spanning in Biometric and Social networks.
6. To understand privacy spanning in HealthCare and Location based Privacy.

Course Outcomes:
On completion of the course, learner will be able to–

CO1- Discuss security threats for Digital World.
CO2- Illustrate all the different ways how malware infects a computer.
CO3- Discuss security issues in online world and social networking.
CO4- Discuss technical, legal, and ethical privacy issues in Big data and Mobile Devices.
CO5- Discuss technical, legal, and ethical privacy issues in Biometric and Social networks.
CO6- Discuss technical, legal, and ethical privacy issues in HealthCare and Location based Privacy.

Unit I	Security in Digital world: Password & Email Security	6 Hrs

Introduction: Difference between Privacy and Security, Threat Model
Passwords Under Attack: Authentication process, Password threats, Strong passwords, Password management
Email Security: Email systems, Email security and privacy

Case Studies (if any)	Securely handling suspicious email attachments.
Mapping of Course Outcomes for Unit I	CO1

Unit II	Malware Defence & Secure WWW	6 Hrs

Malware-The Dark Side of Software: Malware, How do I get malware, What does malware do?

Malware-Defense in Depth: Data backup, Firewalls, Software patches, Antivirus software, User education **Securely Surfing the World Wide Web:** Web browser, “Http Secure”, Web browser history

Case Studies (if any)	Recovery of hacked email account.	
Mapping of Course Outcomes for Unit II	**CO2**	
Unit III	**Secure Online Shopping & Social Networking**	**8 Hrs**
Online Shopping: Consumer decisions, Spyware and key-loggers, Wireless sniffing, Scams and phishing websites, Misuse and exposure of information **Wireless Internet Security:** How wireless networks work, Wireless security Threats, Public wi-fi security, Wireless network administration **Social Networking: C**hoose your friends wisely, Information sharing, malware and phishing **Social Engineering**: **Phishing for Suckers: S**ocial engineering: malware distribution, Phishing, Detecting a phishing url, Staying safe online: the human threat		
Case Studies (if any)	Detection of threat in Wireless Internet Security	
Mapping of Course Outcomes for Unit III	**CO3**	
Unit IV	**Privacy in Big data & Mobile Devices**	**7 Hrs**
Privacy Model, Privacy and Big Data: Introduction, Curse of Dimensionality, Scale & Technology, Privacy Issues, Ethics and Law, Privacy Protection and Big Data, Challenges **Privacy in Mobile Devices:** Background, Privacy Issues, Privacy Solutions, Challenges and Opportunities		
Case Studies (if any)	Smart phones and malware.	
Mapping of Course Outcomes for Unit IV	**CO4**	
Unit V	**Privacy in Biometric systems & Social Networking**	**7 Hrs**
Privacy in Biometric Systems: Background on Biometrics, Challenges in Biometric Systems, Privacy Concerns with Biometrics, Privacy-Aware Biometric Solutions, Challenges and Solutions, Current Trends **Privacy in Social Networks:** Social Media, Privacy Issues in Social Networks, Privacy Solutions for Social Networks, Challenges and Opportunities in Social Networks Privacy		
Case Studies (if any)	Online Marketplace (i.e., eBay, Amazon Marketplace)	
Mapping of Course Outcomes for Unit V	**CO5**	
Unit VI	**Privacy in HealthCare & Location-Based Privacy**	**8 Hrs**
Privacy in HealthCare: Background, Privacy concerns in modern Healthcare, Ensuring Privacy in modern Healthcare, Future challenges & opportunities **Location-Based Privacy, Protection, Safety, and Security**: Background, Privacy and Security Issues, Solutions, Challenges		

Case Studies (if any)	An Internet of Things Healthcare Intervention Through Human Robot Interaction and Ubiquitous Computing.
Mapping of Course Outcomes for Unit VI	**CO6**

Books & Other Resources:

Textbooks:

1. Douglas Jacobson and Joseph Idziorek, "Computer Security Literacy Staying Safe in a Digital World", International Standard Book Number-13: 978-1-4398-5619-2 (eBook - PDF), Publisher: CRC Press, 2013
2. Sherali Zeadally and Mohamad Badra, "Privacy in a Digital, Networked World Technologies, Implications and Solutions", ISBN 978-3-319-08469-5 ISBN 978-3-319-08470-1 (eBook), Publisher: Springer, 2016
3. Graham Day, "Security In the Digital World", ISBN 978-1-84928-962-7, Publisher: IT Governance Publishing, 2017

Reference Books:

1. Anthony Sabella, Rik Irons-Mclean, Marcelo Yannuzzi, "Orchestrating and Automating Security for the Internet of Things: Delivering Advanced Security Capabilities from Edge to Cloud for IoT, Publisher: CiscoPress, 2018

MOOC Courses

https://swayam.gov.in/nd2_cec20_cs15/preview
https://nptel.ac.in/noc/courses/noc19/SEM1/noc19-cs25/

E-books

1. "The Keys to Data Protection , A Guide for Policy Engagement on Data Protection Web Security , Security for users, Administrators & ISPs, Privacy & Commerce", August 2018, https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf

Important links:

Computer Emergency Response Team

https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 510404: Industry Internship-I/ In house Research Project - I		
Teaching Scheme:	**Credit**	**Examination Scheme:**
PR: 04 Hr/Week	**04**	**TW: 50 Marks** **OR/PRE : 50 Marks**
Prerequisite Courses:		

Course Objectives:

- To identify the domain of research
- To learn to communicate in a scientific language through collaboration with a guide.
- To categorize the research material confined to the domain of choice

Course Outcomes:
On completion of the course, learner will be able to–

CO1:Conduct thorough literature survey confined to the domain of choice
CO2:Develop presentation skills to deliver the technical contents
CO3:Furnish the report of the technical research domain

CO4:Analyze the findings and work of various authors confined to the chosen domain

Conduction guidelines

The preferences/choices of the domain will be taken from the students. The guide needs to be allocated based on the preference/choices. The research project should be assigned to students. In case of Industry Internship-I, the assigned guide from college has to monitor and evaluate the progress of the student. The student has to exhibit the continuous progress through regular reporting and presentations and proper documentation. The continuous assessment of the progress needs to be documented unambiguously.

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 510405- Dissertation Stage I		
Teaching Scheme:	**Credit**	**Examination Scheme:**
TH: 08 hr/week	**08**	**Mid Semester: 50 Marks** **End Semester: 50 Marks**
Companion Course:		

Course Objectives:

1. To identify the domain of research
2. To learn to communicate in a scientific language through collaboration with a guide.
3. To understand the various means of technical publications and terminologies associated with publications
4. To categorize the research material confined to the domain of choice
5. To formulate research problems with the help of the guide/mentor elaborating the research.
6. To acquire information independently and assess its relevance for answering the research questions.

Course Outcomes:

On completion of the course, learner will be able to–

CO1: Conduct thorough literature survey confined to the domain of choice
CO2:Develop presentation skills to deliver the technical contents
CO3: Furnish the report of the technical research domain
CO4:Analyze the findings and work of various authors confined to the chosen domain

Dissertation Stage–I is an integral part of the Dissertation work. In this, the student shall complete the partial work of the Dissertation which will consist of problem statement, literature review, design, scheme of implementation (Mathematical Model/SRS/UML/ERD/block diagram/ PERT chart,) and Layout & Design of the Set-up.

The student is expected to complete the dissertation at least up to the design phase. As a part of the progress report of Dissertation work Stage-I, the candidate shall deliver a presentation on the advancement in Technology pertaining to the selected dissertation topic. The student shall submit the duly approved and certified progress report of Dissertation Stage-I in standard format for satisfactory completion of the work by the concerned guide and head of the Department/Institute.

The examiner will be assessed by a panel of examiners of which one is necessarily an external examiner. The assessment will be broadly based on literature study, work undergone, content delivery, presentation skills, documentation and report.

The students are expected to validate their study undertaken by publishing it at standard platforms.

The investigations and findings need to be validated appropriately at standard platforms – conference and/or peer reviewed journal.

The student has to exhibit the continuous progress through regular reporting and presentations and proper documentation of the frequency of the activities at the sole discretion of the PG coordination.

The continuous assessment of the progress needs to be documented unambiguously. For standardization and documentation, it is recommended to follow the formats and guidelines circulated / as in the dissertation workbook approved by the Board of Studies. Follow guidelines and formats as mentioned in Dissertation Workbook.

Savitribai Phule Pune University, Pune
ME Cyber Security (2020 Course)
610406: Constitution of India

Teaching Scheme:	**Credit**
01 hr/week	**02**

Course Objectives:
Students will be able to:

1. Understand the premises informing the twin themes of liberty and freedom from a civil rights perspective.
2. To address the growth of Indian opinion regarding modern Indian intellectuals' constitutional role and entitlement to civil and economic rights as well as the emergence of nationhood in the early years of Indian nationalism.
3. To address the role of socialism in India after the commencement of the Bolshevik Revolution in 1917 and its impact on the initial drafting of the Indian Constitution.

Course Outcomes:

On completion of the course, Students will be able to:
CO1: Discuss the growth of the demand for civil rights in India for the bulk of Indians before the arrival of Gandhi in Indian politics.
CO2: Discuss the intellectual origins of the framework of argument that informed the conceptualization of social reforms leading to revolution in India.
CO3: Discuss the circumstances surrounding the foundation of the Congress Socialist Party [CSP] under the leadership of Jawaharlal Nehru and the eventual failure of the proposal of direct elections through adult suffrage in the Indian Constitution.
CO4: Discuss the passage of the Hindu Code Bill of 1956.

Course Contents

Unit I	**History of Making of the Indian Constitution**	**02 Hours**
History Drafting Committee, Composition & Working		
Unit II	**Philosophy of the Indian Constitution**	**02 Hours**
Preamble, Salient Features		
Unit III	**Contours of Constitutional Rights & Duties**	**03 Hours**
Fundamental Rights, Right to Equality, Right to Freedom, Right against Exploitation, Right to Freedom of Religion, Cultural and Educational Rights, Right to Constitutional Remedies, Directive Principles of State Policy, Fundamental Duties.		
Unit IV	**Local Administration**	**03 Hours**
District's Administration head: Role and Importance, Municipalities: Introduction, Mayor and role of Elected Representative, CEO of Municipal Corporation. Pachayati raj: Introduction, PRI: ZilaPachayat, Elected officials and their roles, CEO ZilaPachayat: Position and role. Block level: Organizational Hierarchy (Different departments), Village level: Role of Elected and Appointed officials, Importance of grass root democracy.		
Unit V	**Organs of Governance**	**3 Hours**

Parliament, Composition, Qualifications and Disqualifications, Powers and Functions, Executive, President, Governor, Council of Ministers, Judiciary, Appointment and Transfer of Judges, Qualifications, Powers and Functions		
Unit VI	**Election Commission**	**3 Hours**
Election Commission: Role and Functioning, Chief Election Commissioner and Election Commissioners, State Election Commission: Role and Functioning., Institute and Bodies for the welfare of SC/ST/OBC and women.		

Textbooks:

1. The Constitution of India, 1950 (Bare Act), Government Publication.
2. Dr. S. N. Busi, Dr. B. R. Ambedkar framing of Indian Constitution, 1st Edition, 2015.
3. M. P. Jain, Indian Constitution Law, 7th Edn., Lexis Nexis, 2014.
4. D.D. Basu, Introduction to the Constitution of India, Lexis Nexis, 2015.

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 610407: Industry Internship-II/ In house Research Project – II		
Teaching Scheme:	**Credit**	**Examination Scheme:**
TH: 05 hr/week	**05**	**TW: 50 Marks** **OR/PRE : 50 Marks**

Course Objectives:

1. To identify the domain of research
2. To learn to communicate in a scientific language through collaboration with a guide.
3. To categorize the research material confined to the domain of choice
4. To work in professional environment

Course Outcomes:

On completion of the course, learner will be able to–

CO1: Conduct thorough literature survey confined to the domain of choice
CO2: Develop presentation skills to deliver the technical contents
CO3: Furnish the report of the technical research domain
CO4: Analyze the findings and work of various authors confined to the chosen domain

Conduction guidelines

Industry or research internship should include partial/complete project implementation. Student should be allocated to the research guide in first semester itself and same guide should be continued for the**:** Industry Internship-I/ In house Research Project –I. Otherwise the preferences/choices of the domain should be taken from the students. The guide needs to be allocated based on the preference/choices. The research project should be assigned to students. In case of Industry Internship-I, the assigned guide from college has to monitor and evaluate the progress of the student. The student has to exhibit the continuous progress through regular reporting and presentations and proper documentation. The continuous assessment of the progress needs to be documented unambiguously.

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) 610408: Dissertation Stage II		
Teaching Scheme:	**Credit**	**Examination Scheme:**
PR: 20hr/week	**20**	**TW: 150 Marks** **OR/PRE: 50 Marks**

Course Objectives:

1. To follow SDLC meticulously and meet the objectives of proposed work
2. To test rigorously before deployment of system
3. To validate the work undertaken
4. To consolidate the work as furnished report

Course Outcomes:

On completion of the course, learner will be able to–

CO1: Show evidence of independent investigation

CO2: Critically analyze the results and their interpretation; infer findings

CO3: Report and present the original results in an orderly way and placing the open questions in the right perspective.

CO4: Link techniques and results from literature as well as actual research and future research lines with the research.

CO5: Appreciate practical implications and constraints of the specialist subject

Guidelines:

In Dissertation Work Stage–II, the student shall consolidate and complete the remaining part of the dissertation which will consist of Selection of Technology, Installations, UML implementations, testing, Results, measuring performance, discussions using data tables per parameter considered for the improvement with existing/known algorithms/systems, comparative analysis, validation of results and conclusions. The student shall prepare the duly certified final report of Dissertation in standard format for satisfactory completion of the work by the concerned guide and head of the Department/Institute.

The students are expected to validate their study undertaken by publishing it at standard platforms.

The investigations and findings need to be validated appropriately at standard platforms – conference and/or peer reviewed journal.

The student has to exhibit continuous progress through regular reporting and presentations and proper documentation of the frequency of the activities in the sole discretion of the PG coordination. The continuous assessment of the progress needs to be documented unambiguously.

It is recommended to continue with guidelines and formats as mentioned in the DissertationWorkbook approved by the Board of Studies.

Savitribai Phule Pune University, Pune
ME Cyber Security (2020 Course)
Non Credit Course1: English For Research Paper Writing

Units	CONTENTS
1	Planning and Preparation, Word Order, Breaking up long sentences, Structuring Paragraphs and Sentences, Being Concise and Removing Redundancy, Avoiding Ambiguity and Vagueness
2	Clarifying Who Did What, Highlighting Your Findings, Hedging and Criticising, Paraphrasing and Plagiarism, Sections of a Paper, Abstracts. Introduction
3	Review of the Literature, Methods, Results, Discussion, Conclusions, The Final Check.
4	key skills are needed when writing a Title, key skills are needed when writing an Abstract, key skills are needed when writing an Introduction, skills needed when writing a Review of the Literature,
5	skills are needed when writing the Methods, skills needed when writing the Results, skills are needed when writing the Discussion, skills are needed when writing the Conclusions
6	useful phrases, how to ensure paper is as good as it could possibly be the first- time submission

Suggested Studies

1. Goldbort R (2006) Writing for Science, Yale University Press (available on Google Books)
2. Day R (2006) How to Write and Publish a Scientific Paper, Cambridge University Press
3. Highman N (1998), Handbook of Writing for the Mathematical Sciences, SIAM. Highman'sbook.
4. Adrian Wallwork, English for Writing Research Papers, Springer New York Dordrecht Heidelberg London, 2011

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) Non Credit Course2: Disaster Management	
Units	**CONTENTS**
1	**Introduction** Disaster: Definition, Factors And Significance; Difference Between Hazard And Disaster; Natural And Manmade Disasters: Difference, Nature, Types And Magnitude.
2	**Repercussions Of Disasters And Hazards**: Economic Damage, Loss Of Human And Animal Life, Destruction Of Ecosystem. Natural Disasters: Earthquakes, Volcanisms, Cyclones, Tsunamis, Floods, Droughts And Famines, Landslides And Avalanches, Man-made disaster: Nuclear Reactor Meltdown, Industrial Accidents, Oil Slicks And Spills, Outbreaks Of Disease And Epidemics, War And Conflicts.
3	**Disaster Prone Areas In India** Study Of Seismic Zones; Areas Prone To Floods And Droughts, Landslides And Avalanches; Areas Prone To Cyclonic And Coastal Hazards With Special Reference To Tsunami; Post-Disaster Diseases And Epidemics
4	**Disaster Preparedness And Management** Preparedness: Monitoring Of Phenomena Triggering A Disaster Or Hazard; Evaluation Of Risk: Application Of Remote Sensing, Data From Meteorological And Other Agencies, Media Reports: Governmental And Community Preparedness.
5	**Risk Assessment** Disaster Risk: Concept And Elements, Disaster Risk Reduction, Global And National Disaster Risk Situation. Techniques Of Risk Assessment, Global Co-Operation In Risk Assessment And Warning, People's Participation In Risk Assessment. Strategies for Survival.
6	**Disaster Mitigation** Meaning, Concept And Strategies Of Disaster Mitigation, Emerging Trends In Mitigation. Structural Mitigation And Non-Structural Mitigation, Programs of Disaster Mitigation In India.

Suggested Studies

SUGGESTED READINGS:

1. R. Nishith, Singh AK, "Disaster Management in India: Perspectives, issues and strategies "'New Royal book Company.
2. Sahni, PardeepEt.Al. (Eds.)," Disaster Mitigation Experiences And Reflections", Prentice Hall Of India, New Delhi.
3. Goel S. L., Disaster Administration And Management Text And Case Studies", Deep & Deep Publication Pvt. Ltd., New Delhi.

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) Non Credit Course3: Sanskrit For Technical Knowledge	
Unit	***Content***
1	• Alphabets in Sanskrit, • Past/Present/Future Tense, • Simple Sentences
2	• Order • Introduction of roots • Technical information about Sanskrit Literature
3	• Technical concepts of Engineering-Electrical, Mechanical, Architecture, Mathematics

Suggested reading

1. "Abhyaspustakam" – Dr.Vishwas, Samskrita-Bharti Publication, New Delhi
2. "Teach Yourself Sanskrit" Prathama Deeksha-VempatiKutumbshastri, Rashtriya Sanskrit Sansthanam, New Delhi Publication
3. "India's Glorious Scientific Tradition" Suresh Soni, Ocean books (P) Ltd., New Delhi.

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) Non Credit Course4: Value Education	
Unit	***Content***
1	Values and self-development –Social values and individual attitudes. Work ethics, Indian vision of humanism.
	• Moral and non- moral valuation. Standards and principles. • Value judgements
2	• Importance of cultivation of values. • Sense of duty. Devotion, Self-reliance. Confidence, Concentration. Truthfulness, Cleanliness. • Honesty, Humanity. Power of faith, National Unity. • Patriotism.Love for nature,Discipline
3	• Personality and Behavior Development - Soul and Scientific attitude. Positive Thinking. Integrity and discipline. • Punctuality, Love and Kindness. • Avoid fault Thinking. • Free from anger, Dignity of labour. • Universal brotherhood and religious tolerance. • True friendship. • Happiness Vs suffering, love for truth. • Aware of self-destructive habits. • Association and Cooperation. • Doing best for saving nature
4	• Character and Competence –Holy books vs Blind faith. • Self-management and Good health. • Science of reincarnation. • Equality, Nonviolence,Humility, Role of Women. • All religions and same message. • Mind your Mind, Self-control. • Honesty, Studying effectively
1. Chakroborty, S.K. “Values and Ethics for organizations Theory and practice”, Oxford University Press, New Delhi 2. AICTE **Universal Human Value** course material	

Savitribai Phule Pune University, Pune
ME Cyber Security (2020 Course)

Non Credit Course 5: Stress Management By Yoga

Unit	*Content*
1	• Definitions of Eight parts of yog. (Ashtanga)
2	• Yam and Niyam. Do`s and Don't's in life. Ahinsa, satya, astheya, bramhacharya and aparigraha Shaucha, santosh, tapa, swadhyay, ishwarpranidhan
3	• Asan and Pranayam i. Various yog poses and their benefits for mind & body ii. Regularization of breathing techniques and its effects-Types of pranayam

Suggested reading

1. 'Yogic Asanas for Group Tarining-Part-I" :Janardan Swami Yogabhyasi Mandal, Nagpur
2. "Rajayoga or conquering the Internal Nature" by Swami Vivekananda, AdvaitaAshrama (Publication Department), Kolkata

Savitribai Phule Pune University, Pune ME Cyber Security (2020 Course) Non Credit Course 6: Pedagogy Studies	
Units	**Content**
1	• **Introduction and Methodology:** • Aims and rationale, Policy background, Conceptual framework and terminology • Theories of learning, Curriculum, Teacher education. • Conceptual framework, Research questions**.** • Overview of methodology and Searching.
2	• Thematic overview: Pedagogical practices are being used by teachers in formal and informal classrooms in developing countries. • Curriculum, Teacher education.
3	• Evidence on the effectiveness of pedagogical practices • Methodology for the in depth stage: quality assessment of included studies. • How can teacher education (curriculum and practicum) and the school curriculum and guidance materials best support effective pedagogy? • Theory of change. • Strength and nature of the body of evidence for effective pedagogical practices. • Pedagogic theory and pedagogical approaches. • Teachers' attitudes and beliefs and Pedagogic strategies.
4	• Professional development: alignment with classroom practices and follow-up support • Peer support • Support from the head teacher and the community. • Curriculum and assessment • Barriers to learning: limited resources and large class sizes
5	• **Research gaps and future directions** • Research design • Contexts
	• Pedagogy • Teacher education • Curriculum and assessment • Dissemination and research impact.

Suggested reading

1. Ackers J, Hardman F (2001) Classroom interaction in Kenyan primary schools, Compare, 31 (2): 245-261.
2. Agrawal M (2004) Curricular reform in schools: The importance of evaluation, Journal of Curriculum Studies, 36 (3): 361-379.
3. Akyeampong K (2003) Teacher training in Ghana - does it count? Multi-site teacher education research project (MUSTER) country report 1. London: DFID.
4. Akyeampong K, Lussier K, Pryor J, Westbrook J (2013) Improving teaching and learning of basic maths and reading in Africa: Does teacher preparation count? International Journal Educational Development, 33 (3): 272–282.
5. Alexander RJ (2001) Culture and pedagogy: International comparisons in primary education. Oxford and Boston: Blackwell.
6. Chavan M (2003) Read India: A mass scale, rapid, 'learning to read' campaign.
7. www.pratham.org/images/resource%20working%20paper%202.pdf.

Savitribai Phule Pune University, Pune
ME Cyber Security (2020 Course)
Non Credit Course 7:Personality Development Through Life Enlightenment Skills

Unit	Content
1	Neetisatakam-Holistic development of personality • Verses- 19,20,21,22 (wisdom) • Verses- 29,31,32 (pride & heroism) • Verses- 26,28,63,65 (virtue) • Verses- 52,53,59 (dont's) • Verses- 71,73,75,78 (do's)
2	• Approach to day to day work and duties. • Shrimad BhagwadGeeta : Chapter 2-Verses 41, 47,48, • Chapter 3-Verses 13, 21, 27, 35, Chapter 6-Verses 5,13,17, 23, 35, • Chapter 18-Verses 45, 46, 48.
3	• Statements of basic knowledge. • Shrimad BhagwadGeeta: Chapter2-Verses 56, 62, 68 • Chapter 12 -Verses 13, 14, 15, 16,17, 18 • Personality of Role model. Shrimad BhagwadGeeta: Chapter2-Verses 17, Chapter 3-Verses 36,37,42, • Chapter 4-Verses 18, 38,39 • Chapter18 – Verses 37,38,63

Suggested reading

1. "Srimad Bhagavad Gita" by Swami SwarupanandaAdvaita Ashram (Publication Department), Kolkata
2. Bhartrihari's Three Satakam (Niti-sringar-vairagya) by P.Gopinath,
3. Rashtriya Sanskrit Sansthanam, New Delhi.

Savitribai Phule Pune University
ME Cyber Security (2020 Course)
Non Credit Course 8: Game Engineering

Unit	Course Contents
1.	**Introduction to Unity 3D Game Engines** Introduction to game industry Unity Basic (Interface Intro), Intro to tools & navigation, The Main Windows, Game Objects , Scenes ,Cameras and Types, The assets store, Intro to Asset Work flow
2.	**Basic Photoshop** File types, size and resolution, Cropping and Editing sprite sheet
3.	**C# programming in unity**
4.	**4D Game Development Using Unity 3D** Intro to 2D Game system in unity, Sprite Editor in Unity, Sprite Animation in Unity 2D Physics in Unity
5.	**5. 3D Game Development Using Unity 3D** • UI system in Unity, Artificial Intelligence for 3D Game • Object Oriented Design & Programming for 3D Games • Multiplayer Game in unity, Creating 3D Game For PC
	Books
	1. Fabian Birzele, "The Java Game Development Tutorial **2.** Sean M. Tracey, "Make Games with Python on Raspberry Pi"

Savitribai Phule Pune University
ME Cyber Security (2020 Course)
Non Credit Course 9: Advanced Cognitive Computing

Unit	Course Contents
1.	**The Foundation of Cognitive Computing** Interdisciplinary Nature of Cognitive Science, Cognitive Computing Systems, Representations for Information and Knowledge, Principal Technology Enablers of Cognitive Computing, Cognitive Computing Architectures and Approaches, Cognitive Computing Resources
2.	**Cognitive Computing and Neural Networks: Reverse Engineering the Brain** Brain Scalability, Neocortical Brain Organization, The Concept of a Basic Circuit, Abstractions of Cortical Basic Circuits, Large-Scale Cortical Simulations, Hardware Support for Brain Simulation, Deep Learning Networks
3.	**The Relationship Between Big Data Analytics and Cognitive Computing** Evolution of Analytics and Core Themes, Types of Learning, Machine Learning Algorithms, Cognitive Analytics: A Coveted Goal, Cognitive Analytics Applications
4.	**Applications of Cognitive Computing** Applications in expert systems, Natural language programming, neural networks, robotics, virtual reality, Future applications
	Books
	1. **'Cognitive Computing and Big Data Analytics', by** Judith Hurwitz, Marcia Kaufman, Adrian Bowles, Wiley publications, ISBN: 978-1-118-89662-4 2. '**Cognitive Computing: Theory and Applications**', by Vijay Raghvan, Venu Govindaraju, C.R. Rao, Elsevier publications, eBook ISBN: 9780444637512, Hardcover ISBN: 9780444637444 3.**https://www.research.ibm.com/software/IBMResearch/multimedia/Computing_Cognition_WhitePaper.pdf**

Savitribai Phule Pune University
ME Cyber Security (2020 Course)
Non Credit Course 10:Virtual Reality

Unit	Course Contents
1.	**Introduction and Background** What VR is and why it is so different from other mediums. Its history and different forms of reality, ranging from the real world to fully immersive VR. Its various hardware and components, which composes those realities.
2.	**Perception** Understanding the human brain and how we perceive real and virtual worlds, real-world examples that prove reality is not always what we think it is, explanations of perceptual models and processes, the physiology of the different sensory modalities, theories of how we perceive space and time, and a discussion of how perception relates to action.
3.	**Designing in VR** Fundamentals of VR design including ergonomics, user testing, interface design, scale and scene setting, graphical user interfaces, and motion mechanics for mobile VR, simulator sickness, its causes.
4.	**VR Platforms and Applications** Understand what is happening in the VR industry, surveying current trends and technology in VR, the hardware: Mobile Performance & 360 Media, High-Immersion Unity, or High-Immersion Unreal.
	Books
	1. Jason Jerald, The VR Book: Human-Centered Design for Virtual Reality, Association for Computing Machinery and Morgan & Claypool New York, NY, USA©2016, ISBN: 978-1-97000-112-9 2. John Vince, Virtual Reality Systems, Pearson Prentice Hall, ISBN 10: 0201876876 or ISBN 13: 9780201876871 3. Grigore C. Burdea, Philippe Coiffet, Virtual Reality Technology, 2nd Edition, ISBN: 978-0-471-36089-6

Savitribai Phule Pune University ME Cyber Security (2020 Course) Non Credit Course 11: Machine Translation	
Unit	**Course Contents**
1.	**Introduction:** Concept and translation process. Approaches viz rule based, statistical, example based, hybrid and neural MT.
2.	**Learning and inference for translation models:** Maximum likelihood, Expectation maximization, Discriminative learning, Stochastic methods, Dynamic programming, Approximate search.
3.	**Linguistic phenomena and their associated modeling problems:** Morphology, syntax and semantics.
4.	**Applications & Evaluation:** Scaling, approximation and efficient data structures
	Books
	1.Statistical Machine Translation, P. Koehn, Cambridge University Press 2. Machine Translation by Pushpak Bhatacharyya (2015) 3. Milestone in Machine Translation by John Hutchines