Faculty of Science and Technology

Savitribai Phule Pune University

Maharashtra, India

http://unipune.ac.in

Honours* in Cyber Security

Board of Studies

(Computer Engineering)

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

Savitribai Phule Pune University

Honours* in Cyber Security

With effect from 2020-21

Year & Semester	Course Code	Course Title	Teaching Scheme Hours / Week			Examination Scheme and Marks						Credit Scheme		
			Theory	Tutorial	Practical	Mid-Semester	End-Semester	Term work	Practical	Presentation	Total Marks	Theory / Tutorial	Practical	Total Credit
TE & V	310401	Information and Cyber Security	04	--	--	30	70	--	--	--	100	04	--	04
	310402	Information and Cyber Security Laboratory	--	--	02	--	--	50	--	--	50	--	01	01
		Total	04	-	02	100		50	-	-	150	04	01	05
Total Credits = 05														
TE & VI	310403	Enterprise Architecture and Components	04	--	--	30	70	--	--	--	100	04	--	04
		Total	04	-	-	100		-	-	-	100	04	-	04
Total Credits = 04														
BE & VII	410401	Internet of Things and Embedded Security	04	--	--	30	70	--	--	--	100	04	--	04
	410402	Risk Assessment Laboratory	--	--	02	--	--	50	--	--	50	--	01	01
		Total	04	-	02	100		50	-	-	150	04	01	05
Total Credits = 05														
BE & VIII	410403	Information Systems Management	04	-	--	30	70	--	--	--	100	04	--	04
	410404	Seminar	--	02	--	--	--	-	--	50	50	02	--	02
		Total	04	-	02	100		-	--	50	150	06	-	06
Total Credits = 06														
Total Credit for Semester V+VI+VII+VIII = 20														

*** <u>To be offered as Honours for Major Disciplines as–</u>**

1. Computer Engineering
2. Electronics and Telecommunication Engineering
3. Electronics Engineering
4. Information Technology

<u>For any other Major Disciplines which is not mentioned above, it may be offered as Minor Degree.</u>

Reference: https://www.aicte-india.org/sites/default/files/APH%202020_21.pdf / page 99-100

Savitribai Phule Pune University
Honours* in Cyber Security
Third Year of Engineering (Semester V)
310401: Information and Cyber Security

Teaching Scheme:	Credit:	Examination Scheme:
Theory: 04 Hours/Week	04	**Mid_Semester(TH): 30 Marks** **End_Semester(TH): 70 Marks**

Companion Course, if any: - Information and Cyber Security Laboratory

Course Objectives:

- To understand the basics of computer, network and information security.
- To study operating system security and malwares.
- To acquaint with security issues in internet protocols.
- To analyze the system for vulnerabilities.

Course Outcomes:

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

- Use cryptographic techniques in secure application development.
- Apply methods for authentication, access control, intrusion detection and prevention.
- To apply the scientific method for security assessment
- To develop computer forensics awareness.

Course Contents

Unit I	Security Fundamentals	(06 Hours)

An Overview of Information Security: The Basic Components, Threats, Policy and Mechanism, Assumptions and Trust, Assurance, Operational Issues, Human Issues, Security nomenclature.
Access Control Matrix, Security Policies: Confidentiality, Integrity, Availability Policies and Hybrid Policies, OS Security

Unit II	Modular Arithmetic and Cryptography Basics	(08 Hours)

Modular Arithmetic : Modular Arithmetic Notations, Modular Arithmetic Operations, Euclid's method of finding GCD, The extended Euclid's algorithm.
Cryptography : Classical encryption techniques, Block and Chain ciphers, Data Encryption Standard, Advanced Encryption Standard, RC5

Unit III	Advanced Cryptography	(08 Hours)

Chinese Remainder Theorem and its implication in Cryptography, Diffie-Hellman key exchange algorithm, RSA algorithm, Elgamal Arithmetic, Elliptic Curve Cryptography, Message Digest and Cryptographic Hash Functions, MD5 and SHA-1, Digital Signatures and Authentication.

Unit IV	Issues in Security Management and Cyber Laws	(08 Hours)

Overview, Risk identification, Risk Assessment, Risk Control Strategies, Quantitative vs. Qualitative Risk Control Practices. Risk Management. Laws and Ethics in Information Security, Codes of Ethics, Protecting programs and data
Cybercrime and Information security, Classification of Cybercrimes, The legal perspectives- Indian perspective, Global perspective, Categories of Cybercrime, Types of Attacks, a Social Engineering, Cyber stalking, Cloud Computing and Cybercrime.

Unit V	Key Management and Secure Communication	(08 Hours)

Public Key Infrastructure(PKI), X.509 Certificate, Needham Schroeder algorithm and Kerberos. IP Security: IPv6 and IPSec, Web Security: SSL, HTTPS, Mail Security: PGP, S/MIME . Firewall : Different Types and Functionalities

Unit VI	Attacks, Malicious Logic and Countermeasures	(08 Hours)

Phishing, Password Cracking, Key-loggers and Spywares, Types of Virus, Worms, DoS and DDoS, SQL injection, Buffer Overflow, Spyware, Adware and Ransomware. Antivirus and other security measures Intrusion Detection System : IDS fundamentals, Different types of IDS. Intrusion Prevention.

Learning Resources

1. William Stallings, Computer Security: Principles and Practices, Pearson 6 Ed, ISBN 978-0-13-335469-0
2. Nina Godbole, Sunit Belapure , Cyber Security- Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiely India Pvt.Ltd, ISBN- 978-81-265-2179-1

1. Bruice Schneier , Applied Cryptography- Protocols, Algorithms and Source code in C, Algorithms, Wiely India Pvt Ltd, 2nd Edition, ISBN 978-81-265-1368-0.
3. CK Shyamala et el., Cryptography and Security, Wiley India Pvt. Ltd, ISBN-978-81-265-2285-9.
4. Berouz Forouzan, Cryptography and Network Security, TMH, 2 edition, ISBN -978-00-707-0208-0.
5. Mark Merkow, Information Security-Principles and Practices, Pearson Ed., ISBN- 978-81-317-1288-7.

Savitribai Phule Pune University
Honours* in Cyber Security
Third Year of Engineering (Semester V)
310402: Information and Cyber Security Laboratory

Teaching Scheme	Credit Scheme	Examination Scheme and Marks
Practical: 02 Hours/Week	01	Term work: 50 Marks

Guidelines for Laboratory Conduction

- **Lab Assignments:** Following is list of suggested laboratory assignments for reference. Laboratory Instructors may design suitable set of assignments for respective course at their level. Beyond curriculum assignments and mini-project may be included as a part of laboratory work. The instructor may set multiple sets of assignments and distribute among batches of students. It is appreciated if the assignments are based on real world problems/applications. The Inclusion of few optional assignments that are intricate and/or beyond the scope of curriculum will surely be the value addition for the students and it will satisfy the intellectuals within the group of the learners and will add to the perspective of the learners. For each laboratory assignment, it is essential for students to draw/write/generate flowchart, algorithm, test cases, mathematical model, Test data set and comparative/complexity analysis (as applicable). Batch size for practical and tutorial may be as per guidelines of authority.
- **Term Work–**Term work is continuous assessment that evaluates a student's progress throughout the semester. Term work assessment criteria specify the standards that must be met and the evidence that will be gathered to demonstrate the achievement of course outcomes. Categorical assessment criteria for the term work should establish unambiguous standards of achievement for each course outcome. They should describe what the learner is expected to perform in the laboratories or on the fields to show that the course outcomes have been achieved. It is recommended to conduct internal monthly practical examination as part of continuous assessment.
- **Assessment:** Students' work will be evaluated typically based on the criteria like attentiveness, proficiency in execution of the task, regularity, punctuality, use of referencing, accuracy of language, use of supporting evidence in drawing conclusions, quality of critical thinking and similar performance measuring criteria.
- **Laboratory Journal-** Program codes with sample output of all performed assignments are to be submitted as softcopy. Use of DVD or similar media containing students programs maintained by Laboratory In-charge is highly encouraged. For reference one or two journals may be maintained with program prints in the Laboratory. As a conscious effort and little contribution towards Green IT and environment awareness, attaching printed papers as part of write-ups and program listing to journal may be avoided. Submission of journal/ term work in the form of softcopy is desirable and appreciated.

Suggested list of assignments
(Use suitable programming language/Tool for implementation)

Sr. No	Statement of Assignment
1	Implement Euclid's algorithm to find the GCD of two integers. Further implement extended Euclidean algorithm to find the multiplicative inverse of the given integer.
2	Develop the program to implement DES algorithm for encryption and decryption. Assume suitable key.
3	Develop the program to implement RSA algorithm for encryption and decryption. Assume suitable Private and Public Keys.
4	Write a program to implement SHA1 algorithm using libraries (API)
5	Configure and demonstrate use of vulnerability assessment tool like Wireshark or SNORT

Savitribai Phule Pune University
Honours* in Cyber Security
Third Year of Engineering (Semester VI)
310403- Enterprise Architecture and Components

Teaching Scheme:	Credit	Examination Scheme:
TH: 04 Hours/Week	04	Mid_Semester(TH): 30 Marks End_Semester(TH): 70 Marks

Course Objectives:

- To learn fitting of enterprise information into the broader context of enterprise architecture frameworks
- To learn an architectural foundation that effectively addresses important business and societal challenges.
- To learn a comprehensive architectural guide that includes architectural principles, architectural patterns, and building blocks and their applications for information-centric solutions.
- To provide methodology that is critical for all business leaders and technologist trying to build an enterprise on the internet.

Course Outcomes:

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

- CO1: Explain the concept of the enterprise information architecture.
- CO2: Describe how the domains can be managed within the enterprise though a coherent Information Governance framework.
- CO3: Interpret component model of the EIA Reference Architecture for relevant services with its descriptions and interfaces.
- CO4: Discuss the operational characteristics of the EIA Reference Architecture.
- CO5: Describe the increasing role of enterprise-wide Metadata Management within information-centric use case scenarios.
- CO6: Define enterprise security architecture based on available risk to an enterprise. Discuss various models for enterprise security architecture.

Course Contents

Unit I	Introduction	(08 Hours)

External Forces: A New World of Volume, Variety, and , Internal Information Environment Challenges The Need for a New Enterprise Information, The Business Vision for the Information-Enabled , Building an Enterprise Information Strategy and the Information ,Best Practices in Driving Enterprise Information Planning , Relationship to Other Key Industry and IBM ,The Roles of Business Strategy and Technology, Terminology and Definitions, Methods and Models, Enterprise Information Architecture Reference Architecture in Context

Unit II	Domains and Enterprise information architecture	(08 Hours)

Data domains, Conceptual architecture overview, EIA reference architecture, architecture principals for EIA, Logical view of EIA reference architecture

Unit III	Enterprise information architecture: Component model	(08 Hours)

The component model, component relationship diagram, component description, component interaction diagrams- a deployment scenario

Unit IV	Enterprise information architecture: Operational model	(08 Hours)

Terminology and definitions, Context of operational model design techniques, service qualities, Standards used for operational model relationship diagram framework of operational patterns

Unit V	Metadata and master data management	(08 Hours)

Terminology and definitions, business scenarios, component deep dive, component interaction diagram-deployment scenario, service qualities for metadata management, master data management: Terminology, business scenarios, component deep dive, component interaction diagram, service qualities.

Unit VI	Enterprise Security Architecture—A Top-down Approach	(08 Hours)

SABSA, COBIT and TOGAF and Their Relationships, Using the Frameworks to Develop an Enterprise Security Architecture, A Real-Life Example, Using CMMI to Monitor, Measure and Report the Architecture Development Progress

Learning Resources

Text Books:

1. Mario Godinez , EberhardHechler , Klaus Koenig , Steve Lockwood , Martin Oberhofer, Michael Schroeck , Art of Enterprise Information Architecture, The: A Systems-Based Approach for Unlocking Business
2. Rassoul Ghaznavi-Zadeh, Enterprise Security Architecture—A Top-down Approach
3. Daniel Minoli, Enterprise Architecture A to Z, Frameworks, Business Process Modeling, SOA, and Infrastructure Technology, Auerbach Publications, Taylor & Francis Group, ISBN 978-0-8493-8517-9, 2008

Reference Books:

1. Thomas Erl, Service-Oriented Architecture: Concepts, Technology, and Design. ISBN: 0-13-185858-0, Publisher: Prentice Hall PTR, 2005
2. Mathias Weske, Business Process Management, Concepts, Languages, Architectures, ISBN 978-3-540-73521-2 Springer Berlin Heidelberg New York, 2007
3. Eric A. Marks, Michael Bell., Executive's guide to service-oriented architecture, John Wiley & Sons, Inc.ISBN-13: 978-0-471-76894-4, 2006
4. David S. Linthicum, Enterprise Application Integration, Addison-Wesley Professional 2003, ISBN-10: 1402052626

Online Resources:

Prof. Jenamani, IIT Kharagpur, E-business, https://nptel.ac.in/courses/110/105/110105083/

Savitribai Phule Pune University
Honours* in Cyber Security
Fourth Year of Engineering (Semester VII)
410401 -Internet of Things and Embedded Security

Teaching Scheme:	Credit	Examination Scheme:
TH: 04 Hours/Week	04	Mid_Semester(TH): 30 Marks End_Semester(TH): 70 Marks

Prerequisite Courses, if any:

- Fundamentals of Embedded Systems, IoT
- Basic of Network Security

Companion Course, if any:

Course Objectives:

- To understand the main threats and attacks in IoT Environment
- Ability to understand the Security requirements in IoT.
- To learn security aspects in the design of IoT systems
- To learn IoT security life cycle
- To create awareness of IoT security
- To understand cryptographic security for their IoT implementations and deployments
- To learn identity and access management for IoT development
- To understand Identity models for IoT

Course Outcomes:

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

- CO1-Define IoT security issues and concerns
- CO2-Identify the main threats and attacks in IoT Environment
- CO3- Determine secure development methodology for the IoT
- CO4- Describe IoT security lifecycle management processes
- CO5 – Apply cryptography methods in securing the IoT and embedded system
- CO6- Determine IoT IAM infrastructure

Course Contents

Unit I	Introduction: Securing the Internet of Things, Vulnerabilities, attacks and countermeasures	(08 Hours)

Defining the IoT, IoT uses today, The IoT in the enterprise, The IoT of the future and the need to secure, Primer on threats - The classic pillars of information assurance, Threats, Vulnerability, Risks, vulnerability, and risks; Primer on attacks and countermeasures- Common IoT attack types, Attack trees, Fault (failure) trees and CPS; Today's IoT attacks – attacks; Threat modeling an IoT system

Unit II	Security Engineering for IoT Development	(08 Hours)

Building security in to design and development, Secure design - Security in agile developments , Focusing on the IoT device in operation, Safety and security design - Threat modeling , Privacy impact assessment , Safety impact assessment, Compliance, Security system integration, Processes and agreements, Technology selection – security products and services- IoT device hardware, Selecting an MCU, Selecting a real-time operating system (RTOS) , IoT relationship platforms, Cryptographic security APIs , Authentication/authorization

Unit III	The IoT Security Lifecycle	(08 Hours)
The secure IoT system implementation lifecycle, Implementation and integration - IoT security CONOPS document, Network and security integration, System security verification and validation (V&V), Security training, Secure configurations, Operations and maintenance - Managing identities, roles, and attributes, Security monitoring, Penetration testing, Compliance monitoring, Asset and configuration management, Incident management, Forensics, Dispose - Secure device disposal and zeroization, Data purging, Inventory control, Data archiving and records management		
Unit IV	**Cryptographic Fundamentals for IoT Security Engineering**	**(08 Hours)**
Cryptography and its role in securing the IoT, Types and uses of cryptographic primitives in the IoT, Encryption and decryption- Symmetric encryption , Asymmetric encryption, Hashes, Digital signatures- Symmetric (MACs), Random number generation, Ciphersuites, Cryptographic module principles, Cryptographic key management fundamentals - Key generation- Key establishment, Key derivation, Key storage, Key escrow, Key lifetime, Key zeroization, Accounting and management, Examining cryptographic controls for IoT protocols- Cryptographic controls built into IoT communication protocols(ZigBee, Bluetooth, Near field communication (NFC)), Cryptographic controls built into IoT messaging protocols – MQTT,CoAP,DDS, REST, Future directions of the IoT and cryptography		
Unit V	**Identity and Access Management Solutions for the IoT**	**(08 Hours)**
An introduction to identity and access management for the IoT- The identity lifecycle, Establish naming conventions and uniqueness requirements, Secure bootstrap, Credential and attribute provisioning, Account monitoring and control, Account updates, Account suspension, Account/credential deactivation/deletion, Authentication credentials- Passwords, Symmetric keys, Certificates X.509, IEEE 1609.2, Biometrics, New work in authorization for the IoT, IoT IAM infrastructure - 802.1x, PKI for the IoT, Authorization and access control		
Unit VI	**Identity management models**	**(08 Hours)**
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, hybrid identity management		

Learning Resources

Text Books:

4. Practical Internet of Things Security, Brian Russell, Drew Van Duren, PACKT Publishing
5. Parikshit N. Mahalle, Poonam N. Raikar, “Identity management for internet of things”, River publications

Reference Books:

5. Fei Hu, “Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations “, ISBN: 9781498723183, CRC Press, 2016
6. Aditya Gupta, “The IoT Hacker’s Handbook: A Practical Guide to Hacking the Internet of Things”, ISBN: 1484242998, Apress publisher, 2019
7. Fei HU, “Security and Privacy in Internet of Things (IoTs): Models, Algorithms, andImplementations”, CRC Press,2016
8. Orchestrating and Automating Security for the Internet of Things: Delivering Advanced Security Capabilities from Edge to Cloud for IoT, by Anthony Sabella, Rik Irons-Mclean, Marcelo Yannuzzi, Publisher: Cisco Press, Release Date: June 2018,ISBN: 9780134756936
9. Securing the Internet of Things, Shancang Li Li Da Xu, Syngress, 2017, Elsevier, ISBN: 978-0-12-804458-2
10. Ollie Whitehouse, “Security of Things: An Implementers' Guide to Cyber-

Security forInternet of Things Devices and Beyond", NCC Group, 2014

Online Resources:

Introduction to Industry 4.0 and Industrial Internet of Things
By Prof. Sudip Misra | IIT Kharagpur, https://nptel.ac.in/courses/106/105/106105195/

Cryptography and Network Security By Prof. Sourav Mukhopadhyay | IIT Kharagpur
https://onlinecourses.nptel.ac.in/noc21_cs16/preview

Savitribai Phule Pune University
Honours* in Cyber Security
Fourth Year of Engineering (Semester VII)
410402: Risk Assessment Laboratory

Teaching Scheme:	Credit	Examination Scheme:
TH: 02 Hours/Week	01	Term work Marks 50

Prerequisite Courses, if any:

- Embedded Systems and Internet of Things Security

Companion Course, if any:

Course Objectives:

- To understand the importance of protecting IoT devices and sensors
- To safeguard the information IoT devices collect.
- To assess the risks associated with IoT device vulnerabilities.
- To learn IoT device is functioning properly safe from attacks.Course Outcomes:

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

CO1- Understand the vulnerabilities associated with IoT devices and sensors

CO2- Apply the knowledge to secure the data, communication with respect to embedded and IoT device.

CO3- Identify the risks associated in the context of application that uses IoT.

Guidelines for Instructor's Manual

The instructor‘s manual is to be developed as a hands-on resource and reference. The instructor's

manual need to include prologue (about University/program/ institute/ department/foreword/

preface), curriculum of course, conduction and Assessment guidelines, topics under consideration- concept, objectives, outcomes.

Guidelines for Student's Laboratory Journal

The laboratory assignments are to be submitted by student in the form of journal. Journal consists

of prologue, Certificate, table of contents, and handwritten write-up of each assignment (Title,

Objectives, Problem Statement, Outcomes, software and Hardware requirements, Date of

Completion, Assessment grade/marks and assessor's sign.

As a conscious effort and little contribution towards Green IT and environment awareness,

attaching printed papers as part of write-ups and program listing to journal may be avoided.

Guidelines for Laboratory Conduction

The instructor may set multiple sets of assignments and distribute among batches of students. It is

appreciated if the assignments are based on real world problems/applications. Student should

perform at least three experiments from group A, four experiments from group B and, two experiments from C and any one assignment from group D.

Suggested List of Laboratory Experiments/Assignments

Sr. No.	**Group A**
1	Study of Raspberry-Pi, Beagle (History & Elevation) board, Arduino and other micro controller
2	Study of different operating systems for Raspberry-Pi /Beagle board. Understanding the process of OS installation on Raspberry-Pi /Beagle board
3	Study of different sensors:- temperature sensor, bio-sensor, IR sensor, chemical sensor(PH), gauge sensor, ultrasonic sensor etc.
4	Understand the connection and configuration of GPIO and its use in programming. Write an application of the use of LEDs.
Group B	
5	Design and implement program to detect and report invalid login attempts and malicious activities to embedded device.
6	Design and implement the program to secure the communication between the IoT devices.
7	Design and implement the program to protect the data stored at IoT device.
8	Design and implement the program for detecting tampering of data at storage at IoT
9	Write a program identifying operating system, version and IP address assigned to the device.
10	Design and implement the code to authenticate the communication with IoT device.
Group C	
11	Install and use open source tools to Identifying various types of attacks on IoT device. Analyze the risks associated with the attacks. Write a C++/Java/Python program to identify at least one such attack.
12	Design and implement program/ use open source tool to analyze the packets in IoT environment.
13	Develop a Real time application like a smart home security. **Description**: When anyone comes at door the camera module automatically captures his image and send a notification to the owner of the house on his mobile phone using GSM modem.

Group D	
14	Design Real time application like smart home with following requirements: When user enters into house the required appliances like fan, light should be switched ON. Appliances should also get controlled remotely by a suitable web interface. The objective of this application is student should design complete Smart application in group and analyze the risks associated with it. Perform following five steps to risk assessment a. Identify hazards, i.e. anything that may cause harm. b. Decide what it may be harmed, and how? c. Assess the risks and take action. d. Make a record of the findings. e. Review the risk assessment
15	Design 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. The objective of this application is student should design smart home application in group and analyze the risks associated with it. a. Identify the various types of risk like Technical IoT risk, Security and privacy IoT risk, Ethical IoT risk b. Identify Vulnerabilities of IoT devices c. Identify threats and do the threat analysis.

Savitribai Phule Pune University
Honours* in Cyber Security
Fourth Year of Engineering (Semester VIII)
410403: Information System Management

Teaching Scheme	Credit Scheme	Examination Scheme and Marks
Lecture: 04 Hours/Week	**04**	**Mid_Semester (TH): 30 Marks** **End_Semester (TH): 70 Marks**

Prerequisites: Basic knowledge of Operating System and Data bases

Companion Course : ---

Course Objectives:

1. The course is blend of Management and Technical field.
2. Discuss the roles played by information technology in today's business and define various technology architectures on which information systems are built.
3. Define and analyze typical functional information systems and identify how they meet. the needs of the firm to deliver efficiency and competitive advantage.
4. Identify the basic steps in systems development.

Course Outcomes:

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

1. Understand the concepts of Information systems and design the strategies for dealing with competitive forces.
2. Apply Ethical and Social Issues to Information Systems.
3. Design and analyse of IT Infrastructure. Understand the concepts of Operating System Platforms, Enterprise Software Applications, Data Management and Storage
4. Identify and evaluate the knowledge. Apply it to the Decision-Making Process.
5. Outline the range of solutions for Systems Development and Organizational Change.
6. Demonstrate the use of The Information Security Triad: Confidentiality, Integrity, Availability (CIA) Confidentiality, Manage the Tools for Information Security

Course Contents

Unit I	Information Systems, Organizations, and Strategy	(06 Hours)

Organizations and Information Systems, What Is an Organization? , Features of Organizations, How Information Systems Impact Organizations and Business Firms, Economic Impacts, Organizational and Behavioural Impacts, The Internet and Organizations, Implications for the Design and Understanding of Information Systems, Using Information Systems to Achieve Competitive Advantage, Porter's Competitive Forces Model, Information System Strategies for Dealing with Competitive Forces, The Internet's Impact on Competitive Advantage

#Exemplar/Case Studies	ERP

Unit II	Ethical and Social Issues in Information Systems	(09 Hours)

Understanding Ethical and Social Issues Related to Systems, A Model for Thinking About Ethical, Social, and Political Issues, Five Moral Dimensions of the Information Age, Key Technology Trends That Raise Ethical Issues, Ethics in an Information Society, Basic Concepts: Responsibility, Accountability, and Liability, Ethical Analysis, Candidate Ethical Principles, Professional Codes of Conduct, Some Real-World Ethical Dilemmas, The Moral Dimensions of Information Systems, Information Rights, Privacy and Freedom in the Internet Age, Property Rights: Intellectual Property

#Exemplar/Case Studies	Kiuwan Code Security (SAST), Nmap, Netsparker

Unit III	IT Infrastructure and	(09 Hours)

	Emerging Technologies	
IT Infrastructure, Defining IT Infrastructure, Evolution of IT Infrastructure, Technology Drivers of Infrastructure Evolution, Infrastructure Components, Computer Hardware Platforms, Operating System Platforms, Enterprise Software Applications, Data Management and Storage, Networking/Telecommunications Platforms, Internet Platforms, Consulting and System Integration Services, Contemporary Hardware Platform Trends, The Mobile Digital Platform, Consumerization of IT and BYOD, Grid Computing, Virtualization		
#Exemplar/Case Studies	Windows, Android, iOS, MacOS	
Unit IV	Managing Knowledge and Enhancing Decision Making	(08 Hours)
The Knowledge Management Landscape, Important Dimensions of Knowledge, The Knowledge Management Value Chain, Types of Knowledge Management Systems, Enterprise-Wide Knowledge Management Systems, Enterprise Content Management Systems, Knowledge Network Systems, Collaboration And Social Tools and Learning Management Systems, Knowledge Work Systems, Knowledge Workers and Knowledge Work, Requirements of Knowledge Work Systems, Examples of Knowledge Work Systems, Decision Making and Information Systems, Business Value of Improved Decision Making, Types of Decisions, The Decision-Making Process, Managers and Decision Making in the Real World, High-Velocity Automated Decision Making, Business Intelligence in the Enterprise, What Is Business Intelligence?, The Business Intelligence Environment		
#Exemplar/Case Studies	AsinSeed, AVDecision, Expert Choice	
Unit V	Building and Managing Systems	(08 Hours)
Systems as Planned Organizational Change, Systems Development and Organizational Change, Business Process Redesign, Overview of Systems Development, The Importance of Project Management, Runaway Projects and System Failure, Project Management Objectives, Selecting Projects, Management Structure for Information Systems Projects, Linking Systems Projects to the Business Plan, Information Requirements and Key Performance Indicators, Portfolio Analysis, Scoring Models, Establishing the Business Value of Information Systems, Information System Costs and Benefits, Real Options Pricing Models, Limitations of Financial Models, Managing Project Risk, Dimensions of Project Risk, Change Management and the Concept of Implementation, Controlling Risk Factors		
#Exemplar/Case Studies	ASANA, Basecamp, JIRA, Teamwork PM, Microsoft Team	
Unit VI	Information Systems Security	(08 Hours)
The Information Security Triad: Confidentiality, Integrity, Availability (CIA) Confidentiality, Tools for Information Security, Password Security, Blockchain & Bitcoin Blockchain, Backups, Physical Security, Security Policies, Mobile Security, Personal Information Security		
#Exemplar/Case Studies	Norton, Life Lock, Zone Alarm.	
Learning Resources		

Text Books:

1. Management Information Systems: Managing the Digital Firm, 13th Edition, Kenneth C. Laudon, New York University, Jane P. Laudon, New York University, 2014, Pearson
2. James A O'Brien, George M Marakas and Ramesh Behl. (2009). Management Information Systems, 9th Edition, Tata McGraw Hill Education, New Delhi.
3. Michael Hammer and James Champy, (2003). Reengineering the Corporation: A Manifesto for Business Revolution,1st Edition, HarperCollins

Reference Books:

1. Turban, E., McLean, E. and Wetherbe, J. (2000). Information Technology for Management: Making Connections for Strategic Advantage. , 2nd Edition, John Wiley and Sons.

2. D.P.Goyal. (2006). Management Information Systems-Managerial Perspectives, 2nd

Edition, Macmillan, New Delhi.

3. S.A.Kelkar. (2009).Management Information Systems-A concise Study, 2nd Edition, Prentice Hall of India.

4. NirmalyaBagchi, (2010). Management Information Systems, 1st Edition, Vikas Publishing House, New Delhi

e-Books:

Information Systems for Business and Beyond, David T. Bourgeois Biola University, James L. Smith Shouhong Wang, Joseph Mortati

MOOC/ Video Lectures available at: Prof. Kunal Ghosh, Prof. Surojit Mookherjee, Prof. Saini Das, IIT Kharagpur, Management Information System, https://nptel.ac.in/courses/110/105/110105148/

Savitribai Phule Pune University
Honours* in Cyber Security
Fourth Year of Engineering (Semester VIII)
410404: Seminar

Teaching Scheme	Credit Scheme	Examination Scheme and Marks
Practical: 02 Hours/Week	**02**	**Presentation: 50 Marks**

Course Objectives:

- To train the student to independently search, identify and study important topics in computer science.
- To develop skills among students to study and keep themselves up to date of the technological developments taking place in computer science
- To expose students to the world of research, technology and innovation.

Course Outcomes:

On completion of the course, student will be able to

- To train the student to independently search, identify and study important topics in computer science.
- To develop skills among students to study and keep themselves up to date of the technological developments taking place in computer science.
- To expose students to the world of research, technology and innovation

Guidelines for Seminar:

- The department will assign an internal guide under which students shall carry out Hons. seminar work
- In order to select a topic for Hons. Seminar, the student shall refer to various resources like books, magazines, scientific papers, journals, the Internet and experts from industries and research institutes
- The topic selected for Hons. Seminar by the students will be scrutinized and if found suitable, shall be approved by the internal guide
- Student should also explore the tools and technologies available for implementation of selected topic. Student should implement/ simulate the seminar work partially/ fully for enhancing the practical skill set on topic.
- Student shall submit the progress of his/her Hons. Seminar work to the internal guide.
- The student shall prepare a REPORT on the work done on Hons. Seminar and submit it at the time of presentation.

Evaluation of IT Seminar Work

- During the seminar work, its progress will be monitored, by the internal guide.
- At the end of seminar work, copy of Hons. Seminar Report should be prepared and submitted to department.
- End Examination shall be based on the Report, technical content and Presentation.
- **Guidelines for Assessment**: Panel of staff members along with a guide would be assessing the seminar work based on these parameters-Topic, Contents and Presentation, implementation, regularity, Punctuality and Timely Completion, Question and Answers, Report, Paper presentation/Publication, Attendance and Active Participation.

References:

1. Rebecca Stott, Cordelia Bryan, Tory Young, “Speaking Your Mind: Oral Presentation and Seminar Skills (Speak-Write Series)”, Longman, ISBN-13: 978-0582382435
2. Johnson-Sheehan, Richard, “Technical Communication”, Longman. ISBN 0-321-11764-6
3. Vikas Shirodka, “Fundamental skills for building Professionals”, SPD, ISBN 978-93-5213- 146-5