INDIRA GANDHI DELHI TECHNICAL UNIVERSITY FOR WOMEN

(Established by Govt. of Delhi vide Act 9 of 2012)

MTech.- IT (Information Security Management)

First Semester

S. No.	Code	Subject	L-T-P	Credits	Category
1.	MIS-101	Advanced Programming	3-0-2	4	DCC
2.	MIS-103	Secure Coding and Security Engineering	3-0-2	4	DCC
3.	MIS-105	Fundamentals of Information Security	3-0-2	4	DCC
4.	MCS-107	Data Structures and Algorithm Analysis	3-0-2	4	DCC
5	GEC-101	Generic Open Elective	2-0-0 1-1-0 0-0-4 0-2-0	2	GEC
6.	ROC-101	Research Methodology	3-0-0	3	ROC
		Total Credits		21	

Second Semester

S. No.	Code	Subject	L-T-P	Credits	Category
1.	MIS-102	Advances in Machine Learning	3-0-2	4	DCC
2.	MIS-104	Applied Cryptography	3-1-0	4	DCC
3.	MIS-106	Cyber Security and Forensics	3-0-2	4	DCC
4.	DEC-1xx	Departmental Elective Course – 1	3-0-2 3-1-0 2-1-2	4	DEC
5.	DEC-1xx	Departmental Elective Course – 2	3-0-2 3-1-0 2-1-2	4	DEC
6	ROC-102	Research Ethics	3-0-0	3	ROC
		Total credits		23	

Third Semester

S. No.	Code	Subject	L-T-P	Credits	Category
1.	MIS-201	Ethical Hacking	3-0-2	4	DCC
2.	DEC-2xx	Departmental Elective-3	3-0-2 3-1-0 2-1-2	4	DEC
3.	DEC-2xx	Departmental Elective-4	3-0-2 3-1-0 2-1-2	4	DEC
4	GEC-201	General Open Elective	2-0-0 1-1-0 0-0-4	2	GEC
5	MIS-251	Dissertation – I/Project Work	-	8	DCC
6	MIS-253	Industrial Training/Internship	-	1	DCC
		Total credits		23	

Fourth Semester

S. No.	Code	Subject	L-T-P	Credits	Category
1.	MIS-252	Dissertation – II/Project	-	20	DCC
		Total credits		20	

List of Departmental Elective Courses

Category	Course Code	Subject	Credits
Departmental Elective Course-1	MIS-108	Adv. Database Management Systems	3-0-2
	MIS-110	Introduction to Biometrics	3-0-2
	MIS-112	Computer Vision	3-0-2
	MIS-114	Blockchain Fundamentals	3-0-2
Departmental Elective Course-2	MIS-116	Soft Computing	3-0-2
	MIS-118	Semantic Web	3-1-0
	MIS-120	Security Testing and Risk Management	3-0-2
	MIS-122	Natural Language Processing and Information Retrieval	3-0-2
Departmental Elective Course-3	MIS-203	Neural Network and Deep Learning	3-0-2
	MIS-205	Security Patterns	3-0-2
	MIS-207	Cryptographic Protocols and Algorithms	3-0-2
	MIS-209	Advanced Network Technology	3-0-2
Departmental Elective Course-4	MIS-211	Cyber Laws and Rights	3-1-0
	MIS-213	Security and Privacy in Social Networks	3-1-0
	MIS-215	Software Defined Networks	3-1-0
	MIS-217	Cloud Computing Architecture and Security	3-0-2

ETHICAL HACKING	
Course Code: MIS-201 Contact Hours: L-3 T-0 P-2 Course Category: DCC	Credits: 4 Semester: 3

Introduction:
In lieu of the fact that most of the official work (private and public) is done through computer and computer systems, it is important to ensure security in such cases. All the necessary documents, information, and data are stored in a computer these days which should be protected with utmost care. Following this, there is a lot of demand for ethical hacking professionals to keep all the sensitive information protected from the hackers and develop new computer protecting the system. In this course, students will taught how to find loopholes in the security system and how to report these threats to their owners and provide necessary solutions to protect the data and networks.

Course Objectives:
- To acquire knowledge on about various security threats that exist and can be exploited
- To learn how bots, botnets, viruses, worms, Trojans, DOS attacks, DDOS attacks etc. work and are utilized for hacking
- To learn various ethical laws that exist in India and abroad and their significance
- To understand how loopholes and potential risks can be detected and learn wide variety of solutions that can be applied to protect data and networks.

Pre-requisite: Fundamentals of Information Security

Course Outcome:
On successful completion of this course, students will be able to:
- Learn Ethical hacking tools and techniques
- Learn aspects of security, importance of data gathering, foot printing and system hacking.
- Learn how intruders escalate privileges?
- Learn advanced concepts such as DDoS Attacks, Buffer Overflows, SQL Injection, Cross Site Scripting, Virus Creation
- Develop technical and analytical skills with in-depth knowledge of ethical hacking concepts that will assist them to take certification exam in future

Pedagogy:
The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding of the existing real life cyber security issues and how they are solved. Use of ICT and web based sources by using blended mode will be adopted.

Contents

UNIT-I	10 Hours
Introduction to Ethical Hacking, Hacking Laws, Foot-printing, Reconnaissance, Google hacking, Vulnerable sites, Using Google as a Proxy Server, Directory Listings, Locating Directory Listings, Finding Specific Directories, Finding Specific Files, Server Versioning, Scanning, System hacking Cycle, Enumeration, Cracking Password, Types of password attacks.	
UNIT-II	11 Hours
Trojans and Backdoors, Types of Trojans, Viruses, Worms, Sniffers, Types of Sniffing, Phishing, Methods of Phishing, Types of Phishing Attacks, Process of Phishing, Denial of Service, Classification of DoS attacks, Bots and Botnets, Botnets Life Cycle, System and Network Vulnerability.	
UNIT-III	11 Hours
Ping of Death attack, Session Hijacking, Spoofing vs Hijacking, Session Hijacking Levels, Network Level Hijacking, 3 way handshake, IP Spoofing, RST Hijacking, TCP/IP Hijacking, Hacking web servers, Web Server Defacement, Proxy and Packet filtering, SQL Injection, Cross Site Scripting.	
UNIT-IV	10 Hours
Authentication: HTTP, Basic, Digest, NTLM, Negotiate, Certificate based, Forms-bases, RSA SecurID Token, Biometrics, Hacking Wireless Networks, Bluetooth hacking, Mobile Phone Hacking, Tools for ethical hacking.	
Text Books	
1	S. McClure, J. Scambray and G. Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, Tata Mc Graw Hill Publishers, 3rd ed., 2012.
2	Sean-Philip Oriyano, CEH v9: Certified Ethical Hacker Version 9 Study Guide, 1st Ed., Wiley & Sons, 2016.
Reference Books	
1	M.T. Simpson, N. Antill, "Hands-On Ethical Hacking and Network Defense", 3rd Ed., Cengage Learning , 2016
2	Rafay Baloch, "A Beginners Guide to Ethical Hacking", 1st Ed., CRC Press, 2014

NEURAL NETWORKS AND DEEP LEARNING	
Course Code: MIS-203 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 4 Semester: 3

Introduction:
Deep Learning has received a lot of attention over the past few years to solve a wide range of problems in Computer Vision and Natural Language Processing. Neural networks form the basis of deep learning. This course intends to cover fundamentals of neural networks, deep learning and application areas.

Course Objectives:
- To understand basic Neural Network Models, Learning and applications of Neural Network.
- To learn about the building blocks used in Deep Learning based solutions.
- Introduce major deep learning algorithms, the problem settings, and their applications to solve real world problems

Pre-requisites:
Working knowledge of Linear Algebra, Probability Theory and Machine Learning

Course Outcomes:
On successful completion of the course, students will be able to:
- Identify and describe Artificial Neural Network techniques in building intelligent machines
- Apply Artificial Neural Network to handle uncertainty and solve engineering problems.
- Identify the deep learning algorithms which are more appropriate for various types of learning tasks in various domains.
- Implement deep learning algorithms and solve real-world problems.

Pedagogy:
The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding and implementation of various neural network and deep learning algorithms for real world problems. Use of ICT and web based sources by using blended mode will be adopted.

Contents

UNIT-I	8 Hours
History of Deep Learning, Deep Learning Success Stories, McCulloch Pitts Neuron, Thresholding Logic, Perceptrons, Perceptron Learning Algorithm, Multilayer Perceptrons (MLPs), Representation Power of MLPs, Sigmoid Neurons, Feedforward Neural Network, Backpropagation, Gradient Descent (GD), Momentum Based GD, Nesterov Accelerated GD, Stochastic and Minibatch GD, AdaGrad, RMSProp. Adaptive Learning Rate, Case study: Malware Classification	
UNIT-II	12 Hours
Principal Component Analysis and its interpretations, Singular Value Decomposition . Autoencoders and relation to PCA, SVD, Regularization in autoencoders, Denoising autoencoders, Sparse autoencoders, Contractive autoencoders. Regularization: Bias Variance Tradeo, L2 regularization, Early stopping, Dataset augmentation, Parameter sharing and tying. Greedy Layerwise Pre-training, Better activation functions, Better weight initialization methods, Batch Normalization. Case study: Malware Detection	
UNIT-III	12 Hours
Convolutional Neural Networks, LeNet, AlexNet, ZF-Net, VGGNet, GoogLeNet, ResNet. Learning Vectorial Representations of Words. Recurrent Neural Networks, Backpropagation through time. Encoder Decoder Models, Attention Mechanism, Attention over images. Case study: MNIST dataset	
UNIT-IV	8 Hours
Long Short Term Memory (LSTM), Restricted Boltzmann Machines, Unsupervised Learning, Motivation for Sampling, Markov Chains, Gibbs Sampling for training RBMs, Contrastive Divergence for training RBMs. Case Study: Natural Language Processing/Speech Processing	
Text Books	
1	Deep Learning, An MIT Press book, Ian Goodfellow and Yoshua Bengio and Aaron Courville http://www.deeplearningbook.org, 2016
2	Goodfellow, Yoshua Bengio, Aaron Courville, Francis Bach, Deep Learning (Adaptive Computation and Machine Learning series), MIT Press, 2017
Reference Books	
1	A. Ravindran, K. M. Ragsdell , and G. V. Reklaitis, Engineering Optimization: Methods and Applications, John Wiley & Sons, Inc. , 2016

SECURITY PATTERNS			
Course Code	: MIS-205	Credits	: 4
Contact Hours	: L-3 T-0 P-2	Semester	: 3
Course Category	: DEC		

Introduction:
This course is designed to enable students to recognize the need for building a secure system in which security is an integral part of software lifecycle.

Course Objectives:
- To learn Software Development and Deployment that is reliable, scalable and portable.
- To learn object oriented programming through Security Design Patterns.
- To learn secure integrating web applications developed on varied platform through security patterns.

Pre-requisite:
Basic Knowledge of Object Oriented programming, Design patterns and Database Management

Course Outcome:
On successful completion of this course, students will be able to:
- Acquire Software development skills that are reliable, scalable and portable applications.
- Design and implement software development with Clean Code through use of Security Design patterns.
- Build complex systems with secure and reliable components.

Pedagogy
The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding and implementation of various security patterns. Use of ICT and web based sources by using blended mode will be adopted.

Contents

UNIT-I	10 Hours
Introduction to Security patterns, Nature and need of security patterns, evaluation of secuirty patterns and their effect on security, Anatomy of security patterns, Characteristics of security patterns, uses of security patterns, classification of security patterns	
UNIT-II	**11 Hours**
Security Pattern Landscape, Circle of Trust, Security Needs Identification for Enterprise Assets, Threat Assessment, Vulnerability Assessment, Identification & Authentication (I&A) Requirements and Patterns, Patterns for Access Control: Authorization, Role-Based Access Control, Multilevel Security, Reference Monitor, Role Rights Definition, Implementation of Authentication and Authorisation patterns Using a case study.	
UNIT-III	**10 Hours**
System Access Control Architecture: Access Control Requirements, Single Access Point, Check Point, Security Session, Full Access with Errors, Limited Access, Implementation using web based application.	
UNIT-IV	**11 Hours**
The Implementation-Level Patterns: Secure logger and Auditor, Clear Sensitive Information, Secure Directory, Input Validator, Pathname Canonicalization Implementation of Patterns using web based application.	

Text Books	
1	Eduardo Fernandez, “Security patterns in Practice”, Wiley , First Edition, 2013
2	Markus Schumacher Eduardo Fernandez et al., “Security Patterns Integrating Security and Systems Engineering”, Wiley, 2006
Reference Books	
1	Ben Edmunds, “Securing PHP Apps”, Apress, 2016
2	Chad Dougherty, Kirk Sayre, Robert C. Seacord, David Svoboda, Kazuya Togashi “Secure Design Patterns”, Software Engineering Institute, CERT, First Edition, 2009

CRYPTOGRAPHIC PROTOCOLS AND ALGORITHMS	
Course Code: MIS-207 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 4 Semester: 3

Introduction:
This advanced course will introduce students to the application of cryptography in real world. The intent of this course is to familiarize students with various classical and modern cryptographic protocols that are widely-used, heavily analysed and accepted as secure. The focus will be on how to design protocols that perform security related function by applying cryptographic methods and primitives and are robust and resistant to attacks

Course Objectives:

- To acquire knowledge on standard cryptographic protocols that are used to provide confidentiality, integrity and authenticity
- To explain and use modern cryptographic methods (hybrid encryption, key management, hybrid digital signatures, mutual authentication)
- To understand wide variety of cryptographic protocols that go beyond the traditional goals of data confidentiality, integrity, and authentication to also secure a variety of other desired characteristics of computer-mediated collaboration

Pre-requisite: Fundamentals of Information Security

Course Outcome:
On successful completion of this course, students will be able to:

- Learn applied cryptographic basics and apply to real world problems
- Students will be able to select the right algorithm, protocol, and systems to develop secure systems to protect digital assets in the cyber world.
- Students will learn advanced security concepts such as secret sharing, how to provide ownership without revealing personal credentials, how to prove data existed at a certain time, auditable voting systems, commitment protocols etc.
- Students will learn interactive protocols that allow the signer to prove a forgery and limit who can verify the signature.

Pedagogy:
The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding of various cryptographic concepts. Course will have a blend of theory and practical for the benefit of students. Use of ICT, web based sources and blended teaching will be adopted.

Contents

UNIT-I	10 Hours
Protocol Building Blocks, Communication Using Symmetric Cryptography, One Way Hash Functions, Communication using Public Key Cryptography , digital signatures, signature with encryption, Random and Pseudo random sequence generation, Basic Protocols: key exchange, Interlock Protocol, Key Exchange with Digital Signatures, Key and Message Broadcast, Basic Protocols: Authentication using hash functions, Authentication using public key cryptography.	
UNIT-II	11 Hours
Mutual Authentication, SKID and SKID 3, Wide Mouth Frog Protocol, Yahalom Protocol, Needham-Schroeder Protocol, Kerberos , DASS, Woo-Lam Protocol, Formal analysis of Authentication and Key exchange protocols, BAN Logic, Multiple Key Public Key Cryptography, Secret Splitting, Secret Sharing, LaGrange Interpolating Polynomial Scheme, Asmuth-Bloom, Secret Sharing with cheaters.	
UNIT-III	11 Hours
Intermediate Protocols: Time stamping services, Arbitrated Protocol, Linking Protocol, subliminal channels, Elgamal Subliminal Channel, Undeniable Digital signatures: Chaum protocol, Proxy signatures, Group signatures, Bit Commitment using symmetric cryptography, Bit Commitment using hash functions, fair coin flips, coin flipping protocol using hash functions and public key cryptography, key escrow.	
UNIT-IV	10 Hours
Advanced Protocols: Zero knowledge proofs, Zero knowledge proof for identity, Interactive ZKP: Graph Isomorphism, Hamiltonian Cycles, Non-interactive Zero knowledge proof, blind signatures, identity based public key cryptography, Oblivious transfer, oblivious signatures, Simultaneous contact signing, Digital certified Mail, Esoteric protocols, secure elections.	
Text Books	
1	W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 7th Ed., 2017.
2	B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley & Sons, 2nd Ed., 2015.
3	Bernard Menezes, Network Security and Cryptography, Cenege Learning, 2nd Ed., 2012.
Reference Books	
1	A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC press, Hardcover Edition, 2018.
2	Dong, Ling, Chen, Kefei, Security Analysis Based on Trusted Freshness, 1st Ed., Springer, 2012.
3	Johannes Buchman, Introduction to Cryptography, 2nd Ed., Springer, 2012.

ADVANCED NETWORK TECHNOLOGY	
Course Code: MIS-209 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 4 Semester: 3

Introduction:
This advanced course develops knowledge about networks to understand their complexity and inform their future design. It seeks to discover and understand common principles and fundamental structures underlying networks and their behaviours. It makes students familiar with the foundations of computer networking, network protocol design and performance evaluation/analysis, and recent advances in network architecture and technology.

Course Objectives:
- To give the students an understanding of the principles behind the latest advances in computer network technology, from IPv6 extending to pervasive and ubiquitous computing
- To develop familiarity with current research problems and research methods in advance computer networks

Pre-requisite: Computer Networks

Course Outcome:
On successful completion of this course, students will be able to:
- Illustrate reference models with layers, protocols and interfaces. Summarize functionalities of different Layers.
- Combine and distinguish functionalities of different Layers and understand principles behind the latest advances in advanced network technology.
- Describe and Analysis of advanced protocols of computer networks, and how they can be used to assist in network design and implementation.

Pedagogy:
The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding of advanced networking concepts and their implementation for real world problems. Use of ICT and web based sources by using blended mode will be adopted.

Contents

UNIT- I	10 Hours
TCP/IP Protocol Architecture, OSI Model, Error detection and correction, Medium Access, Flow and Error Control, Noiseless Principles of Internetworking, Internet protocol operation, IPv4:ICMP, ARP, RARP, IPv6, IGMP, Interior Routing protocols, Exterior Routing Protocols, ARQ, TCP, UDP, Congestion control and Flow Control, Overview of QoS, Integrated Services, Differentiated Services	
UNIT-II	10 Hours
IEEE 802.11a/b/n/g/p, 802.15, and 802.16 standards for Wireless PAN, LAN, and MAN, IPv6 – Header, Addressing, Neighbour Discovery, Auto-Configuration, Header Extensions and options, support for QoS, security, etc., DHCPv6, Mobile Ipv6 rationale and operation – intra and inter site IP, Multicasting: Multicast routing protocols, Virtual private network service, Multiprotocol label switching (MPLS)	
UNIT-III	10 Hours
Wireless Sensor Networks, Wireless Body Area Networks, Mobile Ad Hoc Network, Vehicular Adhoc Network, Data Center Networking, Delay Tolerant Networking, Home Networking, Green Networking, Internet of Things, Software Defined Networking, Web-Scale Networking: Distributed Cloud Computing and Virtual Machine Migration.	
UNIT-IV	10 Hours
Content Networks: Video Streaming, Wireless Networking: Wireless Mesh, Geographic Routing, Network Security principles, Security related issues in wireless networks, Public and Private Key Cryptography, Key distribution protocols. Digital Signatures, and digital certificates, Firewall, Next Generation Fire wall, **Radio Networks, Opportunistic Network**	
Reference Books	
1. W. R. Stevens. TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the Unix Domain Protocols, Addison Wesley, 2016.	
2. W. Stallings. Data and Computer Communications , 10th Edition, Pearson, 2013.	
3. J Kurose and KW Ross. Computer Networking: A Top-Down Approach, 7th Edition, Pearson, 2017	
Text Books	
1. W. Stallings. Cryptography and Network Security: Principles and Practice, 7th Edition, Prentice Hall, 2016.	
2. Ibrahiem M. M. El Emary, S. Ramakrishnan, Wireless Sensor Networks: From Theory to Applications, 1st Edition, CRC Press, 2013	

CYBER LAWS AND RIGHTS	
Course Code: MIS-211 Contact Hours: L-3 T-1 P-0 Course Category: DEC	Credits: 4 Semester: 3

Introduction:
The objective of this course is to enable students to understand, explore, and acquire a critical understanding of cyber law. Develop competencies for dealing with frauds and deceptions (confidence tricks, scams) and other cyber crimes. It also covers overview of Intellectual Property Right and Cyber Laws in Indian and global perspectives.

Course Objectives:

- To introduce the cyber world and cyber law in general
- To explain about the various facets of cyber crimes
- To enhance the understanding of problems arising out of online transactions and provoke them to find solutions
- To clarify the Intellectual Property issues in the cyber space and the growth and development of the law in this regard
- To educate about the regulation of cyber space at national and international level

Pre-requisite: Cyber Security Fundamentals

Course Outcome:
On successful completion of this course, students will be able to:

- Understand the cyber world and cyber law in general and various facets of cyber crimes
- Understand regulation of cyber space at national and international level
- Understand the Intellectual Property issues in the cyber space

Pedagogy:
The teaching-learning of the course would be organized through lectures, assignments, projects/presentations and case studies. Students would be encouraged to develop an understanding of cyber laws and cyber rights. Use of ICT and web based sources by using blended mode will be adopted.

Contents

UNIT-I	10 Hours
Cyber World: An overview, The internet and online resources, Security of information, Digital signature, Cyber Law: An Overview, Introduction about the cyber space, Regulation of cyber space – introducing cyber law, Scope of Cyber laws – e-commerce; online contracts; IPRs (copyright, trademarks and software patenting); e-taxation; e-governance and cyber crimes, Cyber law in India with special reference to Information Technology Act, 2000	
UNIT-II	10 Hours
Computer crime and cyber crimes; Classification of cyber crimes, Distinction between cyber crime and conventional crimes, Reasons for commission of cyber crime, Cyber forensic, Cyber criminals and their objectives, Kinds of cyber crimes – cyber stalking; cyber pornography; forgery and fraud; crime related to IPRs; Cyber terrorism; computer vandalism etc. Regulation of cyber crimes -Issues relating to Investigation, Issues relating to Jurisdiction, Issues relating to Evidence, Relevant provisions under Information Technology Act, 2000, Indian Penal Code, Pornography Act and Evidence Act etc., Plagiarism Issues, Tools to detect Plagiarism, Plagiarism Tools : Turnitin, Viper	
UNIT-III	10 Hours
Online business- Definition of E-commerce, Types of E-commerce, Important Issues in Global E-commerce (Issues relating to Access (to infrastructure; to contents; universal access; Digital Divide and Universal Divide); Trust, Privacy; Security; Consumer Protection; Content Regulation; Uniformity in Legal Standards pertaining to internet), Application of conventional territory based law to E-commerce (Taxation, Intellectual Property Rights, International Trade, Commercial law and standards, Dispute resolution) IPR – An Overview, Copyright Issues in Cyberspace (Linking, Inlining, Framing, Protection of content on web site, International Treaties), Trademark Issues in cyberspace (Domain Name Dispute, Cybersquatting, Uniform Dispute Resolution Policy, Meta-tags and Key words), Computer Software and Related IPR Issues	
UNIT-IV	10 Hours
Indian evidence act, Examiner of Electronic evidence, amendments introduced in Indian evidence act, Indian CERT, Law regarding Electronic Cheques and truncated cheques, IT rules 2000, Ministerial Order on blocking of websites, Cyber laws in Global Prospective	
Text Books	
1. Prashant Mali, Cyber Law & Cyber Crimes Simplified, Fourth Edition, Snow White Publications, 2017.	
2. Vakul Sharma, Information Technology - Law and Practice (Law and Emerging Technology, Cyber Law & E-Commerce), Sixth Edition, Universal Law Publishing Co. (ULPC), 2018.	
3. Pavan Duggal, Textbook on Cyber Law, 2nd Edition, Universal Law Publishing, 2016.	
4. Matthew Richardson, Cyber Crime: Law and Practice, Second Edition, Wildy, Simmonds and Hill Publishing, 2019.	

SECURITY AND PRIVACY IN ONLINE SOCIAL NETWORKS	
Course Code: MIS-213 Contact Hours: L-3 T-1 P-0 Course Category: DEC	Credits: 4 Semester: 3

Introduction

Social Media is playing a significant role and affecting the online user behaviours in many ways. The primary motivations for users to join social media platforms are to share information, connect to their friends and engage with them. On one hand social media offers these advantages, however, on other hand, the issues of privacy and security are also getting manifested in various forms. And, given that we all are using one (or more) social media platforms, it is important for all of us to learn these issues of privacy and security arising out of social media so that we remain safe online.

Course Objectives

- Understand the fundamentals of social media
- Collect social media data as a developer
- Learn challenges in social media related to privacy and security

Pre-requisites

- Knowledge of object oriented programming principles
- Basic understanding of Machine Learning

Course Outcome

On successful completion of the course, students will be able to:

- Understand security and privacy challenges in any social media platform
- Develop automated systems to solve security and privacy problems

Pedagogy

Lectures will be supported with case studies (driven by research papers) of privacy and security problems in social media. Emphasis will be on practical system development by writing programs to collect, analyze and infer insights from social media

Contents

UNIT-I	10 Hours
Social Media - Introduction; Social Media - User vs Developer's Perspective, Data Collection APIs; Social Media Content Analysis - BoW Model, TF-IDF; Network Analysis - Node Centrality Measures, Degree Distribution, Average Path Length, Clustering Coefficient, Power Law; Synthetic Networks - Random Graphs, Preferential Attachment Model.	
UNIT-II	11 Hours
Security Issues in Social Media - Overview; Review of Machine Learning; Identity Theft - Profile Cloning, Social Phishing; Fake, Compromised, Sybil accounts and their behavior; Spamming; Rumour or Misinformation; Cyberbullying; Collective Misbehaviors.	
UNIT-III	11 Hours
Privacy Issues in Social Media - Overview; Privacy Settings; PII Leakage, Identity vs Attribute Disclosure Attacks; Inference Attacks; De-anonymization Attacks; Privacy Metrics - k-anonymity, l-diversity; Personalization vs Privacy, Differential Privacy.	
UNIT-IV	10 Hours
Social Media Case Studies - Facebook, Twitter, Instagram, YouTube, LinkedIn, StackOverflow, GitHub, Quora, SnapChat, Reddit, FourSquare, Yelp.	
Text Books	
1	Zafarani, Reza, Mohammad Ali Abbasi, and Huan Liu. Social media mining: an introduction. Cambridge University Press, 2014.
Reference Books	
1	Bonzanini Marco. Mastering Social Media Mining. Packt Publishing, 2016.
2	Mikhail Klassen, Matthew A. Russell. Mining the Social Web. 3rd Edition. O'Reilly Media, Inc, 2019

SOFTWARE DEFINED NETWORKS	
Course Code: MIS-215 Contact Hours: L-3 T-1 P-0 Course Category: DEC	Credits: 4 Semester: 3

Introduction:
This course introduces software defined networking, an emerging paradigm in computer networking that allows a logically centralized software program to control the behaviour of an entire network.

Course Objectives:

- Differentiate between traditional networks and software defined networks
- Understand advanced and emerging networking technologies
- Obtain skills to do advanced networking research and programming
- Learn how to use software programs to perform varying and complex networking tasks
- Expand upon the knowledge learned and apply it to solve real world problems

Pre-requisites:

Basic understanding of data communication and computer networks

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

- Understand the functionalities of core SDN and its applications
- Get an exposure of SDN programming frameworks

Pedagogy:
The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding of SDN and related technologies. Use of ICT and web based sources by using blended mode will be adopted.

Contents

UNIT-I	10 Hours
Introduction: Evolution of networking technology, Forerunners of SDN, SDN origins and evolution – Why SDN? Evolution of switches and control planes Centralised and Distributed control and data planes, The genesis of SDN, Software Defined Network software stack	
UNIT-II	10 Hours
SDN architecture: How SDN works? ForCES and Open Flow control. SDN controllers: Introduction-general concepts. **Network virtualization:** Network programmability-NetApp development, Network slicing.	
UNIT-III	8 Hours
SDN applications: SDN solutions for data centre networks-use cases and applications, Open network operating system SDN applications in wireless networks and IoT-case studies and applications.	
UNIT-IV	12 Hours
Implementing SDN: Juniper SDN Framework-IETF SDN Framework- Open Daylight Controller-Floodlight Controller-Bandwidth-Calendaring-Data Center Orchestration **SDN future and challenges:** Control and data plane scalability, Security, Fault tolerance, Enhancing the data plane: OpenFlow++	

Text Books	
1	SDN - Software Defined Networks by Thomas D. Nadeau & Ken Gray, O'Reilly, 2013
2	Software Defined Networking with OpenFlow By Siamak Azodolmolky, Packt Publishing, 2013

References	
1	Software Defined Networks: A Comprehensive Approach by Paul Goransson and Chuck Black, Morgan Kaufmann Publications, 2014
2	Feamster, Nick, Jennifer Rexford, and Ellen Zegura. "The road to SDN: an intellectual history of programmable networks." ACM SIGCOMM Computer Communication Review 44.2 (2014): 87-98.
3.	Kreutz, Diego, et al. "Software-defined networking: A comprehensive survey." Proceedings of the IEEE 103.1 (2015): 14-76.
4.	Nunes, Bruno AA, et al. "A survey of software-defined networking: Past, present, and future of programmable networks." Communications Surveys & Tutorials, IEEE 16.3 (2014): 1617-1634.

CLOUD COMPUTING ARCHITECTURE AND SECURITY	
Course Code: MIS-217 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 3 Semester: 3

Introduction:
The course aims to familiarize the students with the advanced concepts of Cloud Computing Architecture and its Security Life Cycle. The prominent attributes of a secure cloud platform are data security, scalability, easy accessibility and sharing of data, zero maintenance, and easy data recovery. The course is designed for inculcating the research aptitude in graduate students, keeping the needs of Enterprise Cloud Computing in Industry 4.0 and the academic research.

Course Objectives:
- To comprehend importance of Enterprise Cloud Computing in Industry 4.0 and research
- To learn Cloud Computing architecture, its Security Requirements and Virtualization
- To understand Cloud Computing Life Cycle Management and Provisioning
- To identify current Security Challenges in Enterprise Cloud Computing

Pre-requisites:
Basic understanding of Operating System, Network Security, Parallel and Distributed Computing, Computer Organization and Architecture

Course Outcome:
On successful completion of the course, students will be able to:
- Conceptualize the Grid and Cloud Computing architecture in real life system
- Implementation of Virtualization at different levels
- Implement the security primitives in Cloud Computing

Pedagogy:
Subject lectures would be delivered via class discussions, tutorials, slide-shows, white board and online quizzes. Students would be encouraged to take an individual case study from Industry 4.0. Students would be guided to survey the state-of-the-art and undertake a research project.

Contents

UNIT- I	10 Hours
Introduction: Introduction of Cloud Computing (CC), NIST definition of CC, Peer-to-Peer Approach, Parallel-Distributed Computing, Cluster and Grid Computing, Evolution of CC from Grid Computing, Autonomic and Utility Computing, Platform Virtualization, Service Oriented Architecture, Significance of CC Paradigm in Industry 4.0, Advantages, Disadvantages and Limitations of CC, Green CC, Elastic Computing, Enterprise CC, CloudStack. **Cloud Architecture and Service Models:** Cloud Dynamic Infrastructure and Architecture, Cloud Life Cycle Management, Service Models of CC: SaaS, IaaS, PaaS, CaaS, CC Sub-Service Models, Deployment Models of Cloud: Public, Private, Community Clouds, Linthicum Cloud Deployment Model, Jericho Cloud Cube Model, CC Sub-Service Models, Cloud Deployment Models: Public, Private, Community Clouds, Linthicum and Jericho Cloud Cube Deployment Model.	
UNIT - II	10 Hours
Basics of Virtualization: Introduction of Virtualization & its need, Types of Virtualization, Virtual Clusters, Virtualization Reference Model, Advantages and Limitations of Virtualization, Techniques used for computing Virtualization, Logical Partitioning, Hypervisor Taxonomy, Concept of Virtual Machine, Hardware Virtual machine, Virtualization at Server End, Virtualization at Desktop End, Network Virtualization and Data Center Virtualization. **Concepts in Virtualization:** Virtualization Reference Model, Server/Compute Virtualization (at Server) and its Components, Techniques and Components for Desktop Virtualization, Features of Desktop Virtualization Drivers, Components of Network Virtualization: Virtual Switches and Virtual LAN, Traffic Management and its Techniques, Virtual Machine Migration Services, Virtual Machine Provisioning and Migration Services Management.	
UNIT - III	10 Hours
Cloud Data Center: Core elements of Cloud Data Center, Storage Network Technologies and Virtualization, Object-based Storage Technologies, Unified Storage, RAID Technology and its Advantages, Technologies of Backup and Disaster Recovery, Replication Technologies, Cloud Data Center Management, Information Life Cycle Management, Cloud Analytics, Computing on Demand. **Introduction to Secure CC:** Overview of Data Security and Privacy, Security Concerns of CC, Security requirements for CC Architecture, Security Patterns and Architectural Elements, Cloud Security Design Principles, Cloud Security Architecture, Planning Strategies for Secure Operations, Data Encryption, Cloud Data Storage, Cloud Lock-in.	
UNIT – IV	10 Hours
Advanced Security Issues: Security Concerns-Threats to Infrastructure, Data and Access Control, Cloud Information Security Objectives: Confidentiality, Accessibility, Organizational Security and Privacy Requirements, Client-Side Computing Environment Requirements, Integrity, Cloud Security Design Principles, Secure Cloud Software Testing, Vulnerability Assessment Tools, Input Validation and Content Injection, Database Integrity Issues, Network Intrusion and Session Hijacking Attacks, Fragmentation Attacks, Secure Cloud Software Testing, Identity Management and Access Control, VM Security Techniques, Information Privacy, Laws and Legal Matters in Cloud Computing, Mobile Cloud Computing, Cloud Computing Environment Open-Stack, Cloud Usage for Big Data Analytics and Internet of Things.	
Text Books	

1. Ronald L. Krutz, Russell Dean Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley-India 1st edition, 2010
2. Barrie Sosinsky, "Cloud Computing Bible", Wiley-India 1st Edition, 2011
3. Austin Young, Cloud Computing: A Comprehensive Guide to Cloud Computing, Independently Published, July-2019
Reference Books
1. Gautam Shroff, "Enterprise Cloud Computing Technology Architecture Applications" Cambridge University Press 1st edition, 2010
2. Rajkumar Buyya, James Broberg, Andrzej M. Goscinski, "Cloud Computing: Principles and Paradigms", Wiley-India , 2011
3. Miller Michael, "Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online", Pearson Education India ,1st edition, 2008