EKLAVYA UNIVERSITY
ज्ञान प्राप्ये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishwavidyalaya (Sthapna Avam Sanchalana) Adhyadesh, 2020

SCHOOL OF ENGINEERING

SYLLABUS

CYBER SECURITY

Class		**M-Tech.-Cyber Security**	**L**	**T**	**P**	**C**
Semester/Year		**III/II**	**3**	**-**	**-**	**3**
Subject Name		**Biometric Security**				
Subject Code		**MCSCS20S301**				
Paper	**English**					
	Hindi					
Max. Marks		**100**				

Course Objectives:

1. To provide students with understanding of biometrics, biometric equipment and standards applied to security.

Course Outcomes:

After completion of course, students would be:

CO1. Perform R&D on bio-metrics methods and systems.

CO2. A good understanding of the various modules constituting a bio-metric system.

CO3. Familiarity with different bio-metric traits and to appreciate their relative significance.

CO4. A good knowledge of the feature sets used to represent some of the popular bio-metric traits.

CO5. Evaluate and design security systems incorporating bio-metrics.

Unit	Syllabus	Periods
UNIT – I	Introduction and Definitions of bio-metrics, Traditional authenticated methods and technologies. **Introduction to** Image Processing, **Image Enhancement Techniques:** Spatial Domain Methods: Smoothing, sharpening filters, Laplacian filters, Frequency domain filters, Smoothing and sharpening filters.	**10**

UNIT – II	**Image Restoration & Reconstruction:** Model of Image Degradation/restoration process, Noise models, spatial filtering, inverse filtering, Minimum mean square Error filtering. **Introduction to image segmentation: Image edge detection:** Introduction to edge detection, types of edge detectors. Introduction to image feature extraction.	**10**
UNIT – III	**Bio-metric technologies:** Fingerprint, Face, Iris, Hand Geometry, Gait recognition, Ear, Voice, Palm print, On-Line Signature Verification, 3D Face Recognition, Dental Identification and DNA.	**10**
UNIT – IV	The Law and the use of multi bio-metrics systems. Statistical measurement of Bio-metric. Bio-metrics in Government Sector and Commercial Sector. Case Studies of bio-metric system, Bio-metric Transaction. Bio-metric System Vulnerabilities.	**10**
UNIT – V	Recent trends in Bio-metric technologies and applications in various domains. Case study of 3D faces recognition and DNA matching.	**8**

TEXT BOOKS:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi : "Biometrics-Identity verification in a network", 1st Edition, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul : "Implementing Biometric Security", 1st Edition, Wiley Eastern Publication, 2005.

REFERENCE BOOKS:

1. Paul Reid, Biometrics for network security, Hand book of Pearson, 2004.
2. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Finger print Recognition, Springer Verlag, 2003.
3. A. K. Jain, R. Bolle, S. Pankanti (Eds.), BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999.
4. J. Wayman, A.K. Jain, D. Maltoni, and D. Maio (Eds.), Biometric Systems: Technology, Design and Performance Evaluation, Springer, 2004.
5. Anil Jain, Arun A. Ross, Karthik Nanda kumar, Introduction to biometric, Springer, 2011.
6. Biometric Systems: Technology, Design and Performance Evaluation, J. Wayman, A.K. Jain, D. Maltoni, and D. Maio.
7. Gonzalez, R.C. and Woods, R.E., Digital Image Processing. 2nd ed. India: Person Educate.

SYLLABUS

CYBER SECURITY

Class		**M-Tech.- Cyber Security**	**L**	**T**	**P**	**C**
Semester/Year		**III/II**	**3**	**-**	**-**	**3**
Subject Name		**Intelligent System**				
Subject Code		**MCSCS20S302**				
Paper	**English**					
	Hindi					
Max. Marks		**100**				

Course Objectives:

1. Demonstrate good knowledge of basic theoretical foundations of the following common intelligent systems methodologies: Rule-based systems, Fuzzy inference, artificial neural networks, Evolutionary computation, Data Mining, Case-based reasoning, Probabilistic reasoning, and intelligent agents.
2. Determine which type of intelligent system methodology would be suitable for a given type of application problem.
3. Demonstrate, in the form of a major project work, the ability to design and develop an intelligent system for a selected application.

Course Outcomes:

CO1. Gain deep understanding of the basic artificial intelligence techniques.

CO2. Able to Demonstrate knowledge of the fundamental principles of intelligent systems.

CO3. Able to analyses and compare the relative merits of a variety of AI problem solving techniques.

CO4. Apply their knowledge to design solutions to different problems.

CO5. Ability to design and develop an intelligent system for a selected application.

Unit	Syllabus	Periods
UNIT – I	Biological foundations to intelligent systems I: Artificial neural networks, Back- propagation networks, Radial basis function networks, and recurrent networks. Biological foundations to intelligent systems II: Fuzzy logic, knowledge Representation and inference mechanism, genetic algorithm, and fuzzy neural networks.	**12**
UNIT – II	Search Methods Basic concepts of graph and tree search. Three simple search methods: breadth-first search, depth-first search, iterative deepening search. Heuristic search methods: best-first search, admissible evaluation functions, hill- climbing search.Optimisation and search such as stochastic annealing and genetic algorithm.	**10**
UNIT – III	Knowledge representation and logical inference Issues in knowledge representation. Structured representation, such as frames, and scripts, semantic networks and conceptual graphs. Formal logic and logical inference. Knowledge-based systems structures, its basic components. Ideas of Blackboard architectures.	**10**
UNIT – IV	Reasoning under uncertainty and Learning Techniques on uncertainty reasoning such as Bayesian reasoning, Certainty factors and Dempster-Shafer Theory of Evidential reasoning.	**10**
UNIT – V	A study of different learning and evolutionary algorithms, such as statistical learning and induction learning. Recent trends in Fuzzy logic, Knowledge Representation.	**10**

TEXT BOOKS:

1. M.Negnevitsky Artificial Intelligence Addison Wesley.
2. L. Reznik Fuzzy Controllers Butterworth-Heinemann Oxford 1997.
3. Artificial Intelligence: A Modern Approach, Prentice Hall, 2003.

REFERENCE BOOKS:

1. Luger G.F. and Stubblefield W.A. (2008). Artificial Intelligence: Structures and strategies for Complex Problem Solving. Addison Wesley, 6thedition.
2. Russell S. and Norvig P. (2009). Artificial Intelligence: A Modern Approach. Prentice-Hall, 3rd edition.

SCHOOL OF ENGINEERING

SYLLABUS

CYBER SECURITY

Class		M-Tech.-Cyber Security	L	T	P	C
Semester/Year		III/II	3	-	-	3
Subject Name		Mobile Applications & Services				
Subject Code		MCSCS20S303				
Paper	English					
	Hindi					
Max. Marks		100				

Course Objective:

1. Describe those aspects of mobile programming that make it unique from programming for other platforms.
2. Critique mobile applications on their design pros and cons.
3. Utilize rapid prototyping techniques to design and develop sophisticated mobile interfaces.
4. Program mobile applications for the Android operating system that use basic and advanced phone features.
5. Deploy applications to the Android marketplace for distribution.

Course Outcomes:

On completion of the course the student should be able:

CO1. To identify the target platform and users and be able to define and sketch a mobile application.

CO2. Understand the fundamentals, frameworks, and development lifecycle of mobile application platforms including iOS, Android, and Phone Gap.

CO3. Design and develop a mobile application prototype in one of the platform (challenge project).

CO4. Competent with designing and developing mobile applications using one application development framework.

CO5. Competent with understanding enterprise scale requirements of mobile applications.

Unit	Syllabus	Periods
UNIT – I	Introduction: Introduction to Mobile Computing, Introduction to Android Development Environment, Factors in Developing Mobile Applications, Mobile Software Engineering, Frameworks and Tools, Generic UI Development Android User.	**10**
UNIT – II	More on Uis: VUIs and Mobile Apps, Text-to-Speech Techniques, Designing the Right UI, Multichannel and Multimodal Uis,. Storing and Retrieving Data, Synchronization and Replication of Mobile Data, Getting the Model Right, Android Storing and Retrieving Data, Working with a Content Provider.	**10**
UNIT – III	Communications via Network and the Web: State Machine, Correct Communications Model, Android Networking and Web, Telephony Deciding Scope of an App, Wireless Connectivity and Mobile Apps, Android Telephony. Notifications and Alarms: Performance, Performance and Memory Management, Android Notifications and Alarms, Graphics, Performance and Multithreading, Graphics and UI Performance, Android Graphics.	**12**
UNIT – IV	Putting It All Together: Packaging and Deploying, Performance Best Practices, Android Field Service App, Location Mobility and Location Based Services Android Multimedia: Mobile Agents and Peer-to-Peer Architecture, Android Multimedia. Platforms and Additional Issues: Development Process, Architecture, Design, Technology. Selection, Mobile App Development Hurdles, Testing, Security and Hacking, Active Transactions, More on Security, Hacking Android.	**10**
UNIT – V	Recent trends in Communication protocols for IOT nodes, mobile computing techniques in IOT, agents based communications in IOT.	**8**

TEXT BOOKS:

1. Mobile Computing Paperback – Illustrated, 14 December 2011 by Raj Kamal.

REFERENCE BOOKS:

1. Wei-Meng Lee, Beginning Android TM 4 Application Development, 2012 by John Wiley & Son.

EKLAVYA UNIVERSITY

ज्ञान प्राप्ये लक्ष्य संधानम्

Estd. by Madhya Pradesh Niji Vishwavidyalaya (Sthapna Avam Sanchalana) Adhyadesh, 2020

SCHOOL OF ENGINEERING

SYLLABUS

CYBER SECURITY

Class	**M-Tech.-Cyber Security**	**L**	**T**	**P**	**C**
Semester/Year	**III/II**	**3**	**-**	**-**	**3**
Subject Name	**Cyber Threat Intelligence**				
Subject Code	**MCSCS20S304**				
Paper — **English**					
Paper — **Hindi**					
Max. Marks	**100**				

Course Objectives:

1. This course will explain what approaches and frameworks are available to implement a Cyber Threat Intelligence unit and how they can be used in it, and at the end you will have the necessary resources to be able to implement a Cyber Threat Intelligence unit.

Course Outcomes:

After completion of course, students would be:

CO1. Define what Cyber Threat Intelligence is and what is not.

CO2. Scope what implementation of Cyber Threat Intelligence is needed for an organization according to its resources and capabilities.

CO3. Understand how Cyber Threat Intelligence interacts with other units.

CO4. Define the type of intelligence that the Cyber Threat Intelligence provides depending on the unit requiring the information.

CO5. Know the basic concepts to build the core of Cyber Threat Intelligence.

Unit	Syllabus	Periods
UNIT – I	**Defining Cyber Threat Intelligence:** The Need for Cyber Threat Intelligence: The menace of targeted attacks, The monitor-and-respond strategy, Why the strategy is failing, Cyber Threat Intelligence defend, Key Characteristics: Adversary based, Risk focused, Process oriented, Tailored for diverse consumers, The Benefits of Cyber Threat Intelligence.	**12**
UNIT – II	**Developing Cyber Threat Intelligence Requirements: Assets** That Must Be Prioritized: Personal information, Intellectual property, Confidential business information, Credentials and IT systems information, Operational systems. Adversaries: Cybercriminals, Competitors and cyber espionage agents, Hacktivists. Intelligence Consumers: Tactical users, Operational users, Strategic users.	**10**
UNIT – III	**Collecting Cyber Threat Information:** Level 1: Threat Indicators, File hashes and reputation data, Technical sources: honeypots and scanners, Industry sources: malware and reputation feeds. Level 2: Threat Data Feeds, Cyber threat statistics, reports, and surveys, Malware analysis. Level 3: Strategic Cyber Threat Intelligence, Monitoring the underground, Motivation and intentions, Tactics, techniques, and procedures.	**12**
UNIT – IV	**Analyzing and Disseminating Cyber Threat Intelligence:** Information versus Intelligence, Validation and Prioritization: Risk scores, Tags for context, Human assessment. Interpretation and Analysis: Reports, Analyst skills, Intelligence platform, Customization. Dissemination: Automated feeds and APIs, Searchable knowledge base, Tailored reports.	**10**
UNIT – V	**Selecting the Right Cyber Threat Intelligence Partner:** Types of Partners: Providers of threat indicators, Providers of threat data feeds, Providers of comprehensive cyber threat intelligence. Important Selection Criteria: Global and cultural reach, Historical data and knowledge, Range of intelligence deliverables, APIs and integrations, Intelligence platform, knowledge base, and portal, Client services, Access to experts. Intelligence-driven Security.	**10**

TEXT BOOKS:

1. Cyber Threat Intelligence: 70 (Advances in Information Security) Hardcover – Import, 14 May 2018 by Ali Dehghantanha (Editor), Mauro Conti (Editor), Tooska Dargahi (Editor).

REFERENCE BOOKS:

1. Jon Friedman. Mark Bouchard, CISSP. Foreword by John P. Watters, Cyber Threat Intelligence, Definitive Guide TM, 2015.
2. Scott J. Roberts, Rebekah Brown, Intelligence- Driven Incident Response: Outwitting the Adversary, O’Reilly Media, 2017.
3. Henry Dalziel, How to Define and Build an Effective Cyber Threat Intelligence Capability Elsevier Science & Technology, 2014.
4. John Robertson, Ahmad Diab, Ericsson Marin, Eric Nunes, Vivin Paliath, Jana Shakarian, Paulo Shakarian, DarkWeb Cyber Threat Intelligence Mining Cambridge University Press, 2017.
5. Bob Gourley, The Cyber Threat, Create space Independent Pub, 2014.

EKLAVYA UNIVERSITY
ज्ञान प्राप्तये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishwavidyalaya (Sthapna Avam Sanchalana) Adhyadesh, 2020

SCHOOL OF ENGINEERING

SYLLABUS

CYBER SECURITY

Class		**M-Tech.- Cyber Security**	**L**	**T**	**P**	**C**
Semester/Year		**III/II**	**3**	**-**	**-**	**3**
Subject Name		**Cyber Law**				
Subject Code		**MCSCS20S305**				
Paper	**English**					
	Hindi					
Max. Marks		**100**				

Course Objectives:

1. The objectives of this course are to enable learner to understand, explore, and acquire a critical understanding cyber law.
2. Develop competencies for dealing with frauds and deceptions (confidence tricks, scams) and other cyber-crimes for example, child pornography etc. that are taking place via the internet.

Course Outcomes:

By the end of this Course, students should be able to:

CO1. Analyse fundamentals of cyber law.

CO2. Discuss it act & its amendments relate cyber laws with security incidents.

CO3. Develop the understanding of relationship between commerce and cyberspace.

CO4. Give learners in depth knowledge of information technology act and legal frame work of right to privacy, data security and data protection.

CO5. Make study on various case studies on real time crimes.

Unit	Syllabus	Periods
UNIT – I	Concept of Cyberspace, Issues of Jurisdiction in Cyberspace: Jurisdiction Principles under International law, Jurisdiction in different states, Position in India. Conflict of Laws in Cyberspace, International Efforts for harmonization Privacy in Cyberspace.	**10**

UNIT – II	Electronic Commerce, Cyber Contract, Intellectual Property Rights and Cyber Laws UNCITRAL Model Law, Digital Signature and Digital Signature Certificates, E-Governance and Records.	**8**
UNIT – III	Define Crime, Mens Rea, Crime in Context of Internet, Types of Cyber Crime, Computing Damage in Internet Crime.	**8**
UNIT – IV	Obscenity and Pornography, Internet and potential of Obscenity, International and National Instruments on Obscenity & Pornography, Child Pornography, Important Case Studies.	**8**
UNIT – V	Offences under IPC (Indian Panel Code, 1860), Offences & Penalties under IT Act 2000, IT Act Amendments, and Investigation& adjudication issues, Digital Evidence.	**8**

TEXT BOOKS:

1. Kumar," Cyber Laws: Intellectual property & E Commerce, Security", 1st Edition, Dominant Publisher, 2011.
2. Rodney D. Ryder, "Guide to Cyber Laws", Second Edition, Wadhwa And Company, New Delhi, 2007.
3. Information Security policy & implementation Issues, NIIT, PHI.

REFERENCE BOOKS:

1. Dr. Farooq Ahmad, Cyber Law in India, Allahbad Law Agency- Faridabad.
2. J.P. Sharma, Sunaina Kanojia, CyberLaws.
3. Harish Chander , Cyber Laws and IT Protection.
4. Justice Yatindra Singh , Cyber Laws.
5. Prof. R.K. Chaubey, An Introduction to cyber-crime and cyber law.
6. Karnika Seth, Justice Altamas Kabir, Computers Internet and New Technology Laws.

EKLAVYA UNIVERSITY

ज्ञान प्राप्तये लक्ष्य संधानम्

Estd. by Madhya Pradesh Niji Vishwavidyalaya (Sthapna Avam Sanchalana) Adhyadesh, 2020

SCHOOL OF ENGINEERING

SYLLABUS

CYBER SECURITY

Class		**M-Tech.-Cyber Security**	**L**	**T**	**P**	**C**
Semester/Year		**III/II**	**3**	**-**	**-**	**3**
Subject Name		**Operation Research**				
Subject Code		**MCSCS20S306**				
Paper	**English**					
	Hindi					
Max. Marks		**100**				

Course Objectives:

1. To impart knowledge in concepts and tools of Operations Research.
2. To understand mathematical models used in Operations Research.
3. To apply these techniques constructively to make effective business decisions.

Course Outcomes:

At the end of the course, the student should be able to:

CO1. Students should able to apply the dynamic programming to solve problems of discreet and continuous variables.

CO2. Students should able to apply the concept of non-linear programming.

CO3. Students should able to carry out sensitivity analysis.

CO4. Student should able to model the real world problem and simulate it.

CO5. Solve Linear Programming Problems.

Unit	Syllabus	Periods
UNIT – I	Optimization Techniques, Model Formulation, models, General L.R Formulation, Simplex Techniques, Sensitivity Analysis, Inventory Control Models.	**8**
UNIT – II	Formulation of a LPP - Graphical solution revised simplex method - duality theory - dual simplex method - sensitivity analysis - parametric programming.	**10**

UNIT – III	Nonlinear programming problem - Kuhn-Tucker conditions min cost flow problem - max flow problem - CPM/PERT.	**10**
UNIT – IV	Scheduling and sequencing - single server and multiple server models - deterministic inventory models - Probabilistic inventory control models - Geometric Programming.	**10**
UNIT – V	Competitive Models, Single and Multi-channel Problems, Sequencing Models, Dynamic Programming, Flow in Networks, Elementary Graph Theory, Game Theory Simulation.	**10**

TEXT BOOKS:

1. Operations Research—Introduction to Management Science Paperback – 1 January 2019 by A Panel of Authors (Author).
2. Operations Research Paperback – 1 January 2015 by D. S. HIRA, P K GUPTA,(Author).

REFERENCE BOOKS:

1. H.A. Taha, Operations Research, An Introduction, PHI, 2008.
2. H.M. Wagner, Principles of Operations Research, PHI, Delhi, 1982.
3. J.C. Pant, Introduction to Optimisation: Operations Research, Jain Brothers, Delhi, 2008.
4. Hitler Libermann Operations Research: McGraw Hill Pub 2009.
5. Panner selvam, Operations Research: Prentice Hall of India 2010.
6. Harvey M Wagner, Principles of Operations Research: Prentice Hall of India 2010.

SCHOOL OF ENGINEERING

SYLLABUS

CYBER SECURITY

Class		**M-Tech.-Cyber Security**	**L**	**T**	**P**	**C**
Semester/Year		**III/II**	**-**	**-**	**20**	**10**
Subject Name		**Dissertation I**				
Subject Code		**MCSCS20S307**				
Paper	**English**					
	Hindi					
Max. Marks		**250**				

Course Objective:

1. To undertake a substantial in-depth study of a specific topic in Computer Science, Software Engineering, Cyber Security.

Course Outcomes:

At the end of the course, the student should be able to

CO1. Identify Computer Science engineering problems reviewing available literature.

CO2. Identify appropriate techniques to analyze complex Computer Science systems.

CO3. Apply engineering and management principles through efficient handling of project.

Syllabus

- Dissertation-I will have mid semester presentation and end semester presentation. Mid semester presentation will include identification of the problem based on the literature review on the topic referring to latest literature available.
- End semester presentation should be done along with the report on identification of topic for the work and the methodology adopted involving scientific research, collection and analysis of data, determining solutions and must bring out individuals contribution.
- Continuous assessment of Dissertation – I and Dissertation – II at Mid Sem and End Sem will be monitored by the departmental committee.

EKLAVYA UNIVERSITY
ज्ञान प्राप्ये लक्ष्य संधानम्
Estd. by Madhya Pradesh Niji Vishwavidyalaya (Sthapna Avam Sanchalana) Adhyadesh, 2020

SCHOOL OF ENGINEERING

SYLLABUS

CYBER SECURITY

Class		**M-Tech.-Cyber Security**	**L**	**T**	**P**	**C**
Semester/Year		**IV/II**	**-**	**-**	**32**	**16**
Subject Name		**Dissertation II**				
Subject code		**MCSCS20401**				
Paper	**English**					
	Hindi					
Max. Marks		**500**				

Course Objective:

Extension of the work on the topic identified in Dissertation – I.

Course Outcomes:

At the end of the course, the student should be able to

CO1. Solve complex Computer Science problems by applying appropriate techniques and tools.

CO2. Exhibit good communication skill to the engineering community-y and society.

CO3. Demonstrate professional ethics and work culture.

Syllabus

Dissertation – II will be extension of the work on the topic identified in Dissertation – I.

Continuous assessment should be done of the work done by adopting the methodology decided involving numerical analysis/ conduct experiments, collection and analysis of data, etc. There will be pre submission seminar at the end of academic term. After the approval the student has to submit the detail report and external examiner is called for the viva-voce to assess along with guide.