JYOTI NIVAS COLLEGE AUTONOMOUS
SYLLABUS FOR 2018 BATCH AND THEREAFTER

Programme: B.Sc. **Semester: VI**

COMPUTER SCIENCE – VIII(A)

DATA MINING

Course Code: 18VICS8A **No. of Hours: 45**

COURSE OBJECTIVES:

- Learning data mining principles and techniques
- Learning how to analyze large sets of data
- Describing and demonstrating basic data mining algorithms.

LEARNING OUTCOMES:

- Understanding data mining techniques and functions
- Understanding decision tree algorithm
- Understanding Pattern discovery and Pattern Analysis

UNIT I **(10 HRS)**

Introduction: Basic Data Mining Tasks, Data Mining Versus Knowledge Discovery in Databases, Data Mining Issues, Data Mining Metrics, Social Implications of Data Mining, Data Mining from a Database Perspective, Data Base/OLTP Systems, Decision Support Systems, Dimensional Modeling- Multidimensional Schemas, Indexing, Data WareHousing, OLAP, Machine Learning, Pattern Matching

UNIT II **(08 HRS)**

Data Mining Techniques: Introduction, Statistical Perspective on Data Mining – Point Estimation, Models Based on Summarization, Bayes Theorem, Decision Trees, Neural Networks

UNIT III **(08HRS)**

Classification: Introduction, Statistical Based Algorithms – Bayesian Classification, Distance- Based Algorithms – K Nearest Neighbors, Decision Tree-Based Algorithms

UNIT IV **(09 HRS)**

Clustering : Introduction, Outliers, Partitional Algorithm – Minimum Spaning Tree, Squared Error Clustering Algorithm, K-Means Clustering, Nearest Neighbor Algorithm

Association Rules: Introduction, Large Item Sets, Basic Algorithms – Apriori Algorithm, Sampling Algorithm

UNIT V **(10 HRS)**

Web Mining: Web Content Mining, Crawlers, Web Usage Mining, Preprocessing – Data Structure, Pattern Discovery, Pattern Analysis

Text Mining: Unstructured Text, Episode Rule Discovery for Text, Hierarchy of Categories, Text Clustering

REFERENCES

1. Margaret H. Dunham. Data Mining Introductory and Advanced Topic, LPE , 2003.
2. Arun K Pujari ,Data Mining Techniquesi, Third Edition, 2015
3. Jiawei Han & Micheline KamberData Mining Concepts and Techniques,Third Edition, 2016

JYOTI NIVAS COLLEGE AUTONOMOUS
SYLLABUS FOR 2018 BATCH AND THEREAFTER

Programme: B.Sc. **Semester: VI**

COMPUTER SCIENCE – VIII (B)

INTERNET OF THINGS

Course Code: 18VICS8B **No. of Hours: 45**

COURSE OBJECTIVES:

- To expose students to the world of interconnected devices,
- To understand the communication protocols among these connected devices.
- To transfer the data which is gatheredand further analyze this data to make appropriate decisions.

LEARNING OUTCOMES:

- Analyze the functional blocks involved in Internet of Things.
- Understand the architecture of Internet of Things.
- Demonstrate the application of IoT in real world.

UNIT I **(11 HRS)**

Introduction to Internet of Things

Introduction, Definition and Characteristics**,** Physical Design of IoT, Things in IoT, IoT Protocols, Logical Design of IoT, IoT Functional Blocks, IoT Communication Models, IoT Communication APIs, IoT Enabling Technologies, Wireless Sensor Networks, introduction to Cloud Computing, Introduction Big Data Analytics, Communication Protocols, Embedded Systems, IoT Levels & Deployment Templates.

UNIT II (**09 HRS)**

IoT Physical Devices &Domain Specific IoT

IoT Devices, Boards –Arduino - Raspberry PI-About the Board, Sensors,Actuators, Gateways.

Domain Specific IoT: Home Automation, Cities, Environment, Energy, Retail, Logistics, Agriculture, Industry, Health & Lifestyle.

UNIT III (**09 HRS)**

IoT& M2M- Introduction, M2M, Difference between IoT and M2M, SDN and NFV for IoT.

Protocols for IoT: Routing Protocol, IEEE 802.15.4, Bluetooth Low Energy, Z-Wave, Zigbee, MQTT Protocol.

UNIT IV **(08 HRS)**

Arduino Programming

The Arduino ecosystem, Installing the Software, Connecting the Arduino, Opening a Sketch, Sketching in Code, The Structure of Arduino C, Verifying and Uploading, Working with Variables, Making Decisions, Digital Ins and Outs, Analog-In, Analog-Out.

UNIT V **(08 HRS)**

IoT Security & Advanced Topics

IoT Security: Introduction, IoT Security Threats, IoT Security Requirements, IoT Routing Attacks, Security Frameworks for IoT.

Data Analytics in IoT: Introduction to Apache Hadoop.

REFERENCES

1. ArshdeepBahga, Vijay Madisetti, The Internet of Things: A Hands on Approach Universities press, 2015.
2. RajkumarBuyya and Amir VahidDastjerdi, Internet of Things-Principles and Paradigms - 1st Edition, 2016.
3. Brian EvansBeginning Arduino Programming, Apress, 2011
4. Olivier Hersent, David Boswarthick, Omar Elloumi,The Internet of Things: Key Applications and Protocols –Wiley, 2011.
5. Pethuru Raj and AnupamaC.Raman, The Internet of Things: Enabling Technologies, Platforms and Use Cases- CRC Press, 2017.

JYOTI NIVAS COLLEGE AUTONOMOUS
SYLLABUS FOR 2018 BATCH AND THEREAFTER

Programme: B.Sc. **Semester: VI**

COMPUTER SCIENCE – VIII (C)

CYBER SECURITY

Course Code: 18VICS8C **No. of Hours: 45**

COURSE OBJECTIVES:

- Focusing on cyber threats and cyber security.
- To educates how to avoid becoming victims of cybercrime.
- Understand the Importance of Computer Forensics.
- Gain Basic Knowledge about Cyber Laws and to provide adequate orientation on laws in reference to cybercrime and cyber security taking into account the Indian scenario.

LEARNING OUTCOMES:

- Deeper understanding of different threats and Security Issues
- Understand different prevention Techniques to secure the information
- Understands the forensics lifecycle and tools and techniques used
- Basic knowledge on cyber law focusing on offences

UNIT I **(08 HRS)**

Introduction to Cybercrime: Cybercrime: definition and origins of the word - Cybercrime and Information Security - Cybercriminals - **Classification of Cybercrimes**: E-Mail Spoofing, Spamming, Cyberdefamation, Internet Time Theft, Salami Attack/ Salami Technique, Data Diddling, Forgery, Web Jacking, Newsgroup Spam, Industrial Spying/ Industrial Espionage, Hacking, Online Frauds, Pornographic Offenses, Software Piracy, Computer Sabotage, E-mail Bombing / Mail Bombs, Ransomware, Usenet Newsgroup as the source of Cybercrimes, Computer Network Intrusions, Password Sniffing, Credit card frauds, Identity Theft - **Cyber Offenses**: Hackers, Crackers and Phreakers - Categories of Cybercrime.

UNIT II **(10 HRS)**

Types of Attacks: Reconnaissance, Passive Attacks, Active Attacks, Scanning and Scrutinizing Gathered Information, Attack (Gaining and Maintaining the System Access) - **Social Engineering:** Classification of Social Engineering:Human Based, Computer Based. **- Cyber Stalking** – Types of Stalkers, How Stalking Works? – Cybercafé – tips for safety and cybercafé security - **Botnets -** Tips to reduce to be part of Bot **- Attack Vector** - **Mobile and Wireless Devices –** Introduction - Proliferation of Mobile and Wireless Devices **– Credit Card Frauds in Mobile and Wireless Computing Era** -Types and Techniques – Tips to Prevent Credit Card Frauds **– Attacks on Mobile Cell Phones –** Mobile Phone Theft, Mobile Viruses, Mishing, Vishing, Smishing and Bluetooth Hacking. – **Security measures on -** Malware Attacks, Vishing Attacks, Smishing attacks.

UNIT III **(09 HRS)**

Tools and Preventive Methods used in Cybercrime: Introduction – Proxy Server and Anonymizers – **Phishing:** Methods of Phishing – Phishing techniques – Spear Phishing – Types of Phishing Scams – Phishing Toolkits and spy Phishing - Phishing Countermeasures – **Password Cracking:** Online Attacks, Offline Attacks, Strong and weak passwords, Random Passwords – **Keyloggers and Spywares**: Software Keyloggers, Hardware Keyloggers, Antikeyloggers - Spywares – **Virus and Worms**: Types of Viruses – **Trojan Horses and Backdoors :** Backdoor, How to protect from Trojan Horse and Backdoors – **Steganography** - Steganalysis – **DoS and DDoS Attacks** – DoS Attacks, Classification of DoS Attacks, Types of Levels of DoS Attacks, Tools used to Launch DoS Attacks, DDoS Attacks, How to protect from DoS/ DDoS Attacks – **SQL Injection** – Steps for SQL Injection Attack, How to Prevent SQL Injection Attacks.

UNIT IV **(09 HRS)**

An Introduction to Computer Forensics Investigations and Electronic Evidence: Computer Forensics: What is it? - **Computer Forensics Investigations**: A Four – Step Process: Acquisition, Identification, Evaluation, Presentation – **Electronic Evidence:** What is it? – Types of Evidence – Authentication of Evidence – Standard of Evidence - The Location of Electronic Evidence – Tools used to search and collect Electronic Evidence – **What should an Investigator Do?:** Conducting an Investigation, Special Consideration for Cybercrime Investigations, Identifying Evidence, Analysis of Evidence, How to Handle Evidence in an Investigation, Evidence Log, Extracting Electronic Evidence.

UNIT V **(09 HRS)**

Cyber Law - Need for Cyber laws – Digital and Electronic Signature, Electronic Governance - The Indian IT ACT for offences: Sections 65, 66A, 66B, 66C, 66D, 66E, 66F 67A, 67B, 67C, 68, 69, 69A, 69B, 70, 70A, 70B, 71, 72, 72A, 73, 74, 75, 76, 77 – Summary of changes to the Indian IT Act of offences – Positive Aspects of the ITA 2000 – Weak areas of the ITA 2000 – Challenges to Indian Law and Cybercrime Scenario in India.

REFERENCES

1. Nina Godbole, Sunit Belapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, First Edition 2011, Reprint: 2019, Wiley India Pvt. Ltd., ISBN:978-81-265-2179-1.
2. Marie – Helen Maras, Computer Forensics: Cybercriminals, laws and Evidence, Second Edition, Library of Congress Cataloging- in- publication Data, ISBN – 978-1-4496-9222-3.
3. Justice Yatindra Singh, Cyber Laws, 6th Edition 2016, Universal Law Publishing Co., New Delhi, ISBN: 978-93-5143-733-8.
4. Nilakshi Jain, Dr. R Dhananjay Kalbande. Wiley, Digital Forensic: The Fascinating World of Digital Evidences, 2017, Wiley India Pvt. Ltd., New Delhi.
5. Chuck Easttom, Computer Security Fundamentals, Second Edition, Pearson, Indianapolis 46240 USA, ISBN- 13: 978-0-7897-4890-4, ISBN -10: 0-7897-4890-8, December 2011.
6. Bhushan Mayank, Rajkumar Singh Rathore, Aatif Jamshed, Fundamentals of Cyber Security, BPB Publications, New Delhi.
7. Vakul Sharma, Information Technology: Law & Practice, 5th Edition, New Delhi: Universal Law Publishing.
8. John R. Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications, 2015, Charles River Media, USA, ISBN: 1-58450-018-2,
9. John Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, 2nd Edition, 2014, Syngress, Elsevier.