

Textbooks :

1. “Darkweb Cyber Threat Intelligence Mining”, John Robertson, Ahmad Diab, Ericsson Marin, Eric Nunes, Vivin Paliath, Jana Shakarian, Paulo Shakarian, Cambridge University Press, 2017
2. “Cybercrimes: A Multidisciplinary Analysis”, Sumit Ghosh, Elliot Turrini, Springer, 2010
3. “Big Data Analytics in Cybersecurity”, Onur Savas, Julia Deng, CRC Press, 2017
4. “Data Analytics and Decision Support for Cybersecurity”, Iván Palomares Carrascosa, Harsha Kumara Kalutarage, Yan Huang, Springer, 2017
5. “Data Analysis for Network Cyber-Security”, Niall Adams, Nicholas Heard, Imperial College Press, 2014

CSCS 456 : CLOUD COMPUTING AND SECURITY

Course Objectives :

1. To make the student aware of the trend in the industry to put every service and data on cloud
2. To make student aware of the vocabulary of this new technology and to alert about the security challenges

Course Outcomes :

1. Student gets the skill required to work with various cloud platforms and their pros and cons
2. Student gets the knowledge about the security needs of the cloud technologies

UNIT I

Introduction : Introducing Cloud Computing, Grasping the Fundamentals, Discovering the Value of the Cloud for Business, Getting Inside the Cloud, Developing Your Cloud Strategy.

(12 Hours)

UNIT II

Understanding the Nature of the Cloud : Seeing the Advantages of the Highly Scaled Data Centre, Exploring the Technical Foundation for Scaling Computer Systems, Checking the Cloud’s Workload Strategy, Managing Data, Discovering Private and Hybrid Clouds

(12 Hours)

UNIT III

Cloud Elements & its Security : Seeing Infrastructure as a Service, Exploring Platform as a Service, Using Software as a Service, Understanding Massively Scaled Applications and Business Processes, Setting Some Standards. Web Services Delivered from the Cloud,

Building Cloud Networks, Federation, Presence, Identity, and Privacy in the Cloud, Security in the Cloud.
(12 Hours)
Textbooks : 1. “Cloud Computing for Dummies”, Judith Hurwitz, Robin Bloor, Marcia Kaufman and Dr. Fern Halper, Wiley Publishing, Inc., 2010. 2. “Cloud Computing: A Practical Approach”, Anthony T. Velte, Toby J. Velte, Robert Elsenpeter, McGraw-Hill, 2010. 3. “Cloud Computing - Implementation, Management, and Security”, John Rittinghouse, James Ransome, CRC Press, 2009.
CSCS 458 : INTERNET OF THINGS
Course Objectives : 1. To make the student aware of the new wave of connectivity, of the every “thing” using internet technologies 2. To make the student aware of the security challenges of the new technological trend
Course Outcomes : 1. Student gets the difference between the security needs of an ordinary node and an IoT node 2. Student gets the knowledge of the tradeoffs required in implementing security on an IoT device
 UNIT I
Defining the IoT, Cybersecurity versus IoT security and cyber-physical systems, IoT uses today, The IoT in the enterprise, The IoT of the future and the need to secure. Vulnerabilities, Attacks, and Countermeasures: Primer on threats, vulnerability, and risks (TVR), Primer on attacks and countermeasures, Today's IoT attacks, Lessons learned and systematic approaches. Security Engineering for IoT Development: Building security into design and development, Safety and security design, Processes and agreements, Technology selection – security products and services.
(12 Hours)
UNIT II
The IoT Security Lifecycle: The secure IoT system implementation lifecycle, Operations and maintenance, Dispose. Cryptographic Fundamentals for IoT Security Engineering: Cryptography and its role in securing the IoT, Cryptographic module principles, Cryptographic key management fundamentals, Examining cryptographic controls for IoT protocols, Future directions of the IoT and cryptography. Identity and Access Management Solutions for the IoT: An introduction to identity and access management for the IoT, Authentication credentials, IoT IAM infrastructure, Authorization and access control.