Secure Application Design: Secure Development Lifecycle, Application Security Practices, Web Application Security, Client Application Security, Remote Administration Security. Writing Secure Software: Security Vulnerabilities: Causes and Prevention, Buffer Overflows, Integer Overflows, Cross-Site Scripting, SQL Injection, Whitelisting vs. Blacklisting. J2EE Security: Java and J2EE Overview, The J2EE Architecture, Servlets, Authentication and Authorization, Protocols

(12 Hours)

UNIT II

Windows .NET Security: Core Security Features of .NET, Application-Level Security in .NET. Controlling Application Behaviour: Controlling Applications on the Network, Restricting Applications Running on Computers. Security Operations: Communication and Reporting, Change Management, Acceptable Use Enforcement, Administrative Security, Management Practices, Accountability Controls, Keeping Up with Current Events, Incident Response

(12 Hours)

UNIT III

Disaster Recovery, Business Continuity, Backups, and High Availability: Disaster Recovery, Business Continuity Planning, Backups, High Availability, Compliance with Standards. Incident Response and Forensic Analysis: Incident Response, Forensics, Compliance with Laws During Incident Response.

(12 Hours)

Textbooks :

1. Information Security: The Complete Reference by Mark Rhodes-Ousley
2. Web Application Security: Exploitation and Countermeasures for Modern Web Applications 1st Edition by Andrew Hoffman
3. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition by Dafydd Stuttard

CSCS 508 : BIG DATA ANALYTICS

Course Objectives :

1. To make the student aware of the need to analyse the huge volumes of data connected to cyberspace.
2. To make the student aware of the value of the varieties of data in all walks modern life

Course Outcomes :

1. Student gets the right skills required to handle complex data
2. Student gets the knowledge to make right choice of algorithms and technologies for big data analytics

UNIT I

Applying Big data into different Cyber Security aspects: The Power of Big Data in Cybersecurity, Big Data for Network Forensics, Dynamic Analytics-Driven Assessment of Vulnerabilities and Exploitation, Root Cause Analysis for Cybersecurity, Data Visualisation for Cybersecurity, Cybersecurity Training.

(12 Hours)

UNIT II

Machine Unlearning: Repairing Learning Models in Adversarial Environments, Big data in emerging cybersecurity domains : Big Data Analytics for Mobile App Security, Security, Privacy, and Trust in Cloud Computing, Cybersecurity in Internet of Things (IoT), Big Data Analytics for Security in Fog Computing

(12 Hours)

UNIT III

Analysing Deviant Socio-Technical Behaviours Using Social Network Analysis and Cyber Forensics-Based Methodologies, Tools and Datasets for Cybersecurity : Security Tools, Data and Research Initiatives for Cybersecurity Analysis.

(12 Hours)

Textbooks :

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

CSCO 512 : CYBER LAWS

Course Objectives :