TextBooks:

(1). “Hack Proofing your E-commerce Site”, Ryan Russell, Mark S. Merkow, Robin Walshaw, Teri Bidwell, Michael Cross, Oliver Steudler, Kevin Ziese, L. Brent Huston, Syngress, 2001

(2). “The Secure Online Business”, Adam Jolly, Kogan Page, 2003

(3). “The Secure Online Business handbook e-commerce, IT functionality & business continuity”, third edition, jonathan reuvid, Kogan Page, 2003

(4).”Security Fundamentals for E-Commerce”, Vesna Hassler, Artech House, 2001

CSCS 508 : Big Data Analytics in Cybersecurity

CO1 : To understand the enormity of the data which comes and gets accumulated which fall under the purview of cybersecurity specialists.

CO2: To understand the Bigness of the data and appropriately choose the methodologies and tools required for the analysis.

CO3: To be competent in handling the cyber incidents with the aid of Big data analytics.

CO4: To be able to understand the Bigness of the data emanating in an IoT environment and according

UNIT I

Applying Big data into different Cybersecurity 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 Visualization for Cybersecurity, Cybersecurity Training. **(12 hours)**

UNIT II

Machine Unlearning: Repairing Learning Models in Adversarial Environments, B**ig 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

Analyzing Deviant Socio-Technical Behaviors 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 : Strategic Governance of Cybersecurity Risks and Control Mechanisms II

CO1 : To make students aware of the strategic governance of the ICT resources in a business entity or corporate house or government establishment, to thwart the cyberattack and data leakage.

CO2: To make competent in risk assessment and analysis in case of a cyberattack

CO3: To make students aware of the frameworks and policies governing the data privacy in different domains and the need to be compliant with them.

CO4: To make the students aware of the different security control mechanisms available and how they can be implemented and assessed.

UNIT I

Risk Management and Prioritization Using a Control Perspective : Ensuring that Risk Management Process Supports the Organization, Five Elements of the Risk Management Process, **Control Formulation and Implementation Process :** The Control Formulation Process, Creating and Documenting Control Objectives