ಮಂಗಳೂರು ವಿಶ್ವವಿದ್ಯಾನಿಲಯ

MANGALORE UNIVERSITY

(Accredited by NAAC with 'A' Grade)

ಕ್ರಮಾಂಕ/ No. : MU/ACC/CR 29/2019-20/A2

ಕುಲಸಚಿವರ ಕಛೇರಿ
ಮಂಗಳಗಂಗೋತ್ರಿ – 574 199
Office of the Registrar
Mangalagangothri – 574 199
ದಿನಾಂಕ/Date:15.01.2021

NOTIFICATION

Sub: Syllabus of M.Sc. in Cyber Security programme.
Ref: Academic Council approval vide agenda
No.: ಎ.ಸಿ.ಸಿ:ಶೈ.ಸಾ.ಸ.2:16(2020–21) dtd 23.12.2020.

*****

The Syllabus of M.Sc. in Cyber Security programme (3rd Semester) which is approved by the Academic Council at its meeting held on 23.12.2020 is hereby notified for implementation with effect from the academic year 2020-21.

Copy of the Syllabus shall be downloaded from the University Website (www.mangaloreuniversity.ac.in)

REGISTRAR

To,

1. The Chairman, Dept. of Electronics , Mangalore University, Mangalagangothri
2. The Chairman, Combined BOS in Electronics, Dept. of Electronics, Mangalore University.
3. The Co-ordinator, M.Sc. Cyber Security Programme, Dept. of Electronics , Mangalore University, Mangalagangothri
4. The Registrar (Evaluation), Mangalore University.
5. The Superintendent (ACC), O/o the Registrar, Mangalore University.
6. The Asst. Registrar (ACC), O/o the Registrar, Mangalore University.
7. Guard File.

(16 /12 / 2020)

Preamble

As the internetworked computing devices have become ubiquitous in every sphere of human lives, so are the security threats originating from and to them. Threats are far from simple to be neglected, ranging from confidential information loss to national security. Financial frauds, Identity theft, cyber terrorism, cyber hacktivism, cyber trolls and bullyisms, cyber warfare, Nuclear Plant Cyberattack, are all the manifestations of the different kinds of security threats which are already looming at the corner and if overlooked can endanger the National Security of countries at worst and heckle individuals at minimum. Unfortunately, the law enforcement agencies of the land are battling with the flurry of cybercrimes and due to the lack of trained manpower to handle the cases majority of the cyber criminals are left scottfree. **NITI Aayog** in its report clearly delineates the need for a comprehensive plan to tackle the situation and the urgent need to abridge the severe shortage of skilled manpower between the situation in hand and the process of creation of that manpower. **"Best security starts with the secured hardware"**, is the very well understood wisdom of the recent years and this is where the **M.Sc. Programme in Cyber Security** conducted by the department of Electronics pitches in with a healthy mixture of software and hardware solutions to the problem in hand. There are sufficient future directions shown in the syllabus to the research in the field in terms of Big Data Analysis, IoT, Cloud Computing, Cryptocurrency and Blockchain, Machine Learning, Artificial Intelligence, Physically Unlocatable Functions and Quantum cryptography apart from training the student to become a proficient ethical hacker. This is in line with the very well known philosophy of defense, **"The best defense is a good offense"**.

REGULATION

This programme is designed in line with the regulations governing the choice based credit system for the two years (four semesters) post graduate degree programmes under arts, science, commerce and education discipline (CBCS–PG), as per the mangalore university order MU/ACC/CR.38/CBCS-PG/2015-16/A2 dated 26.05.2017.

Eligibility Criteria for M. Sc. in Cyber Security:

The following candidates are eligible for the M.Sc. in Cyber Security.

(1). Candidates who have passed B.Sc. Degree examination of Mangalore University or any Other University with Electronics or Computer Science or Embedded Systems as optional / major / special subject with 55% (50% for SC / ST / Category–I candidates) marks in aggregate of all the subjects.

(2). Candidates who have passed BCA degree examination of Mangalore University or any Other University with 55% (50% for SC / ST / Category–I candidates) marks in aggregate of all the subjects.

(3). Candidates who have passed B.E or B.Tech degree examination of any University in E&C, E&E, Computer Science, Information Science, Telecommunication are also eligible to apply for M.Sc programme in Cybersecurity provided they have scored 55% (50% for SC / ST / Category-I candidates) marks in aggregate of all the subjects..

Selection of candidates shall be on merit-cum-reservation on the average marks of all the optional subjects and as per the seat matrix prescribed by the Mangalore University from time to time in this effect.

Programme Outcome(PO)s of M.Sc.

PO1 : To evolve a student into a complete professional, ready for the competitive job market.

PO2 : To harness the best potential available among the students and to synergize these human capital with the nation building.

PO3 : To equip the students with the highly essential, critical thinking and analytical skills required for the niche areas of Information age.

PO4 : To instill leadership abilities in the students along with the soft skills and the technical writing skills.

PO5 : To prepare the future leaders of the science and technology space.

PO6 : To evolve the student into a job creator, with ample entrepreneurial aspirations and managerial abilities.

PO7 : To sensitize the students about the value and the need to innovate and to protect these innovative solutions through patents and copyright, adding huge knowledge capital to the country's economy.

Programme Specific Outcome(PSOC) s of M.Sc. in Cyber Security

PSOC1 : Being in line with the National Initiative for Cybersecurity Education(NICE) model of USA, this programme provides a comprehensive and strategic understanding of the cybersecurity education space, against the myopic viewing of the space prevailing among most of the technological institutions, and to find a credible cure for the "Six Blind Men Syndrome", marring the cybersecurity education.

PSOC2 : To understand the nature and origin of cybercrimes & security threats and classify them into different classes on the basis of the degree of damage they can cause.

PSOC3 : To understand the ways to build secured cybersystems for e-commerce, Banking, Financial Services and Insurance sectors.

PSOC4 : To make use of data analytic tools to unearth the patterns leading to the discovery of possible cyberattack and to alarm the concerned and to develop proactive threat Intelligence.

PSOC5 : To learn the ways to hack one's own cybersystems in order to understand the psyche of the cyberattacker and to plug in the security breaches before an outsider attacks, in line with the philosophy in defense, "Best defense is a good offense".

PSOC6 : To understand the software as well as hardware means of securing the cyber systems, in line with the philosophy, "Best cyber defense starts with a secure hardware".

PSOC7 : To understand the potential favorable and unfavorable spinoffs of latest technologies like Big Data, IoT, Cloud, Blockchain, Quantum computers in cybersecurity.

PSOC8 : To understand the ways and means required to trace the cybercrimes and to preserve the crime trails and the evidence required for producing in a court of law to bring the perpetrators of the crime to the book.

PSOC9 : To follow the guidelines set by the National Skill Development Corporation(NSDC) and NASSCOM, in the form of different Qualification Packs(QP) available for the cybersecurity job market.

PSOC10 : To prepare the warriors for cyberwarfare and commandos against cyberterrorism.

M.Sc. in Cyber Security Programme Structure

Semester I		
Sl. No	**Course Name**	**Credits**
Hard Core		
1	CSCH 401 : Strategic Governance of Cybersecurity Risks and Controls	4

2	CSCH 402 : Modern Cryptography	4
3	CSCH 403 : Data Communications in Computer Network	4
Soft Core		
4	CSCS 404 : Mathematical Foundations of Hardware Security	3
5	CSCS 405 : Problem Solving using Python	
6	CSCS 406 : Management of the Digital Value Chain in eBusiness, eCommerce and eGovernance	
7	CSCS 407 : Complexity Analysis of Algorithms	
8	CSCS 408 : Linux Administration & Shell Scripting	
Practicals		
9	CSCP 409 : Implementation and Benchmarking of Cryptographic Algorithms	2
10	CSCP 410 : Linux Administration & Shell Scripting	2
	Total	**22**

Semester II		
Sl. No	**Course Name**	**Credits**
Hard Core		
1	CSCH 451 : Advanced Aspects of Computer Networks	4
2	CSCH 452 : Network Security	4
3	CSCH 453 : Ethical Hacking	4
Soft Core		
4	CSCS 454 : Hardware Design of Cryptographic Algorithms	
5	CSCS 455 : Darkweb Cyber Threat Intelligence Mining : Principled Study of the Industrialization of Cyber Offense	

6	CSCS 456 : Cloud Computing & its Security	3
7	CSCS 457 : Digital System Design using Verilog	
8	CSCS 458 : Internet of Things Security	
Practicals		
9	CSCP 459 : Networking using Python and Network Simulators	2
10	CSCP 460 : Data Analytics of Cybercrimes using Python & R	2
Seminar		
11	CSCS 461: Seminar on latest trends and techniques in Cybersecurity	1
Open Choice		
12	CSCO 462 : Strategic Governance of Cybersecurity Risks and Control Mechanisms I	3
	Total	**26**

Semester III		
Sl. No	**Course Name**	**Credits**
Hard Core		
1	CSCH 501 : Digital Forensics	4
2	CSCH 502 : Web Penetration Testing	4
3	CSCH 503 : Cybersecurity with BlockChain	4
Soft Core		
4	CSCS 504 : Cryptanalysis of Hardware Security	3
5	CSCS 505 : Mobile Phone Security and Forensics	
6	CSCS 506 : Cyber Laws	

7	CSCS 507 : eCommerce Site Security	
8	CSCS 508 : Big Data Analytics in Cybersecurity	
Practicals		
9	CSCP 509 : Practical Vulnerability Assessment and Penetration Testing(VAPT) using Kali Linux	2
10	CSCP 510 : Practical Digital Forensics using Python and Kali Linux	2
Seminar		
11	CSCS 511 : Seminar on latest trends and techniques in Cybersecurity	1
Open Choice		
12	CSCO 512 : Strategic Governance of Cybersecurity Risks and Control Mechanisms II	3
	Total	**26**

Semester IV		
Sl No	**Course Name**	**Credits**
1	CSCH 551 : Industry Internship / Project Work	18

Credit Distribution

Semester	Main Course Credits	Open Choice Credits
I	22	0
II	23	03
III	23	03
IV	18	0
Total	86	06

-	**Grand Total**	**92**

Scheme of Examination for M.Sc. in Cyber Security

Semester I

Course Code	Title of the Course	Credits	Hours per week	Duration of the Exam	Marks		
					IA	Exam	Total
Hard Core (All are Compulsory)							
CSCH 401	**Strategic Governance of Cybersecurity Risks and Controls**	**04**	**04**	**3 hours**	**30**	**70**	**100**
CSCH 402	**Modern Cryptography**	**04**	**04**	**3 hours**	**30**	**70**	**100**
CSCH 403	**Data Communications in Computer Network**	**04**	**04**	**3 hours**	**30**	**70**	**100**
Soft Core (two to be chosen by the student)							
CSCS 404	**Mathematical Foundations of Hardware security**	**03**	**03**	**3 hours**	**30**	**70**	**100**
CSCS 405	**Problem solving using Python**	**03**	**03**	**3 hours**	**30**	**70**	**100**
CSCS 406	**Management of the digital Value Chain in eBusiness, eCommerce and eGovernance**	**03**	**03**	**3 hours**	**30**	**70**	**100**
CSCS 407	**Complexity Analysis of Algorithms**	**03**	**03**	**3 hours**	**30**	**70**	**100**
CSCS 408	**Linux Administration & Shell Scripting**	**03**	**03**	**3 hours**	**30**	**70**	**100**
Practicals							

CSCP 409	**Implementation and Benchmarking of cryptographic algorithms**	**02**	**04**	**03 hours**	**30**	**70**	**100**
CSCP 410	**Linux Administration & Shell Scripting**	**02**	**04**	**03 hours**	**30**	**70**	**100**
Total		**-**	**-**	**-**	**210**	**490**	**700**

Semester II

Course Code	Title of the Course	Credits	Hours per week	Duration of the Exam	Marks		
					IA	Exam	Total
Hard Core (All are Compulsory)							
CSCH 451	**Advanced aspects of Computer Networks**	**04**	**04**	**3 hours**	**30**	**70**	**100**
CSCH 452	**Network Security**	**04**	**04**	**3 hours**	**30**	**70**	**100**
CSCH 453	**Ethical Hacking**	**04**	**04**	**3 hours**	**30**	**70**	**100**
Soft Core (two to be chosen by the student)							
CSCS 454	**Hardware Design of Cryptographic Algorithms**	**03**	**03**	**3 hours**	**30**	**70**	**100**
CSCS 455	**Darkweb Cyber Threat Intelligence Mining : Principled Study of the Industrialization of Cyber Offense**	**03**	**03**	**3 hours**	**30**	**70**	**100**
CSCS 456	**Cloud Computing & its Security**	**03**	**03**	**3 hours**	**30**	**70**	**100**

CSCS 457	**Digital System Design using Verilog**	**03**	**03**	**3 hours**	**30**	**70**	**100**
CSCS 458	**Internet of Things Security**	**03**	**03**	**3 hours**	**30**	**70**	**100**
Practicals							
CSCP 459	**Networking using Python and Network Simulators**	**02**	**04**	**03 hours**	**30**	**70**	**100**
CSCP 460	**Data Analytics of Cybercrimes using Python & R**	**02**	**04**	**03 hours**	**30**	**70**	**100**
Seminar							
CSCS 461	**Seminar on latest trends and techniques in Cybersecurity**	**01**	**01**	**-**	**15**	**35**	**50**
Open Choice							
CSCO 462	**Strategic Governance of Cyber Security Risks and Control Mechanisms- I**	**03**	**03**	**3 hours**	**30**	**70**	**100**
Total					**255**	**595**	**850**

Semester III

Course Code	**Title of the Course**	**Credits**	**Hours per week**	**Duration of the Exam**	**Marks**		
					IA	**Exam**	**Total**
Hard Core (All are Compulsory)							
CSCH 501	**Digital Forensics**	**04**	**04**	**3 hours**	**30**	**70**	**100**

CSCH 502	**Web Penetration Testing**	**04**	**04**	**3 hours**	**30**	**70**	**100**
CSCH 503	**Cybersecurity with Blockchain**	**04**	**04**	**3 hours**	**30**	**70**	**100**
Soft core (two to be chosen by the student)							
CSCS 504	**Cryptanalysis of Hardware Security**	**03**	**03**	**3 hours**	**30**	**70**	**100**
CSCS 505	**Mobile Phone Security and Forensics**	**03**	**03**	**3 hours**	**30**	**70**	**100**
CSCS 506	**Cyber Laws**	**03**	**03**	**3 hours**	**30**	**70**	**100**
CSCS 507	**eCommerce Site Security**	**03**	**03**	**3 hours**	**30**	**70**	**100**
CSCS 508	**Big Data Analytics in Cyber Security**	**03**	**03**	**3 hours**	**30**	**70**	**100**
Practicals							
CSCP 509	**Practical Vulnerability Assessment and Penetration Testing(VAPT) using Kali Linux**	**02**	**04**	**03 hours**	**30**	**70**	**100**
CSCP 510	**Practical Digital Forensics using Python and Kali Linux**	**02**	**04**	**03 hours**	**30**	**70**	**100**
Seminar							
CSCS 511	**Seminar on latest trends and techniques in Cybersecurity**	**01**	**01**	**-**	**15**	**35**	**50**
Open Choice							

CSCO 512	**Strategic Governance of Cyber Security Risks and Control Mechanisms II**	**03**	**03**	**3 hours**	**30**	**70**	**100**
Total					**255**	**595**	**850**

Semester IV

Course Code	**Title of the course**	**Credits**	**Marks**		
			IA	**Dissertation / Viva**	**Total**
CSCH 551	**Project Work / Industry internship Dissertation**	**12**	**100**	**300**	**400**
	Literature Review	**03**	**100**	**---**	**100**
	Project Demonstration / Presentation	**03**	**---**	**100**	**100**
Total		**18**	**200**	**400**	**600**

Marks Distribution Semester Wise

Semester	**Credits**	**Marks**
I	22	700
II	26	850
III	26	850
IV	18	600
Total	**92**	**3000**

Semester I

CSCH 401 : Strategic Governance of Cybersecurity Risks and Controls

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

The Importance of Cybersecurity Management: The Growing Pains of an Emerging Discipline, Understanding the Costs and Benefits of cybersecurity management to an Organization, Two Absolute Rules for Cybersecurity Work, Implementing a Strategic Response, **Control-Based Information Governance:** The Value of Formal Control, Organizing Things into a Rational Process, Information Audit and Control, Control Principles, **A Survey of Control Frameworks:** COSO Framework, IT Infrastructure Library Framework, ISO 27001, COBIT 5, IT Security Controls**,** General Structure and Applications. **(16 hours)**

UNIT II

The Importance of Controls: Goal-Based Security Controls, Implementation-Based Security Controls, The Security Control Formulation and Development Process, Control Implementation through Security Architecture Design, **Implementing a Multitiered Governance and Control Framework in a Business :** Constructing Practical Systems of Controls, Building the Security Control System, Initial Setup and Tradeoffs, **Risk Management and Prioritization Using a Control Perspective:** Five Elements of the Risk Management Process, Risk Management Plan, Implementing a Managed Risk Control Process, Planning for Effective Risk Management, Writing the Risk Management Plan, Risk Management Controls, Evaluating the Overall Policy Guidance **(16 hours)**

UNIT III

Control Formulation and Implementation Process: The Control Formulation Process**,** Creating and Documenting Control Objectives, Creating a Management-Level Control Process, Measurement-Based Assurance of Controls, **Security Control Validation and Verification:** Security Control Assessment Fundamentals, NIST Security Control Assessment Process, Common Types of Operational and Technical Security Tests**,** Common Operational and Technical Security Examination Techniques**, Control Framework Sustainment and Security of Operations:** Operational Assurance, Response Management, Operational Oversight and Infrastructure Assurance of Control Set Integrity **(16 hours)**

TextBooks

(1). "The Complete Guide to Cybersecurity Risks and Controls", Anne Kohnke, Dan Shoemaker, Ken Sigleer, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016

(2)."Securing an IT Organization through Governance, Risk Management, and Audit", Ken Sigler, Dr. James L. Rainey, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016

(3). "A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)", Anne Kohnke, Dan Shoemaker, Ken Sigleer, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016

(4). "Cybercrimes: A Multidisciplinary Analysis", Sumit Ghosh, Elliot Turrini, Springer, 2010

CSCH 402 : Modern Cryptography

CO1 : To make students aware of all the modern cryptographic methods which are the backbone of the data privacy in cyberspace.

CO2: To make the students aware of the computational complexity point of view of modern cryptography.

CO3: To make competent to perform the cryptanalysis of any cryptography scheme and to assess the security.

CO4: To make the students aware of the implementation hurdles, hassles and tradeoffs about

different cryptographic schemes.

UNIT I

Introduction : Classical Cryptography and Modern Cryptography, The Setting of Private-Key Encryption, Historical Ciphers and Their Cryptanalysis, The Basic Principles of Modern Cryptography, **Perfectly-Secret Encryption :** Definitions and Basic Properties, The One-Time Pad (Vernam's Cipher), Limitations of Perfect Secrecy **Private-Key Cryptography:** Private-Key Encryption and Pseudorandomness, A Computational Approach to Cryptography, Defining Computationally-Secure Encryption, Pseudorandomness, Constructing Secure Encryption Schemes. **(16 hours)**

UNIT II

Message Authentication Codes and Collision-Resistant Hash Functions: Secure Communication and Message Integrity, Encryption vs. Message Authentication, Constructing Secure Message Authentication Codes, Collision-Resistant Hash Functions **Practical Constructions of Pseudorandom Permutations (Block Ciphers):** Substitution-Permutation Networks, Feistel Networks, DES – The Data Encryption Standard, AES – The Advanced Encryption Standard, **Public-Key (Asymmetric) Cryptography:** Number Theory and Cryptographic Hardness Assumptions, Preliminaries and Basic Group Theory. **(16 hours)**

UNIT III

Primes, Factoring, and RSA, Assumptions in Cyclic Groups, Cryptographic Applications of Number-Theoretic Assumptions, **Private-Key Management and the Public-Key Revolution:** Limitations of Private-Key Cryptography, A Partial Solution – Key Distribution Centers, The Public-Key Revolution, Diffie-Hellman Key Exchange, **Public-Key Encryption,** Hybrid Encryption, RSA Encryption, **Digital Signature Schemes:** RSA Signatures, The "Hash-and-Sign" Paradigm, Lamport's One-Time Signature Scheme, Public-Key Cryptosystems in the Random Oracle Model. **(16 hours)**

TextBooks :

(1). **"Introduction to Modern Cryptography"**, Jonathan Katz, Yehuda Lindell, Chapman & Hall/CRC, 2008

(2). **"Foundations of Cryptography - Basic Tools"**, Oded Goldreich, Cambridge University Press, 2004

(3). **"Foundations of Cryptography - Basic Applications"**, Oded Goldreich, Cambridge University Press, 2009

CSCH 403 : Data Communication in Computer Network

CO1 : To make the students aware of how a computer network can be built and to have the knowledge of different protocols which make the computer networks work reliably.

CO2: To make the students aware of the importance of the knowledge of computer networks to secure the data confidentiality, integrity and availability.

CO3: To make the students aware of the different architectures of computer networks.

CO4: To allow students to practically simulate and study all the practical aspects of computer networks.

UNIT I

Foundation: Building a Network, Requirements : Connectivity, Cost-Effective Resource Sharing, Support for Common Services, Network Architecture : Layering and Protocols, OSI Architecture, Internet Architecture, Implementing Network Software : Application Programming Interface (Sockets), Example Application, Protocol Implementation Issues, Performance : Bandwidth and Latency, Delay × Bandwidth Product, High-Speed Networks, Application Performance Needs. **(16 hours)**

UNIT II

Direct Link Networks : Hardware Building Blocks: Nodes, Links, Encoding (NRZ, NRZI, Manchester, 4B/5B), Framing : Byte-Oriented Protocols (BISYNC, PPP, DDCMP), Bit-Oriented Protocols (HDLC), Clock-Based Framing (SONET), Error Detection:Two-Dimensional Parity, Internet Checksum Algorithm, Cyclic Redundancy Check, Reliable Transmission : Stop-and-Wait, Sliding Window, Concurrent Logical Channels, , Ethernet (802.3): Physical Properties, Access Protocol, Experience with Ethernet, Token Rings (802.5, FDDI): Physical Properties, Token Ring Media Access Control, Token Ring Maintenance, Frame Format, Wireless (802.11):Physical Properties, Collision Avoidance, Distribution System, Frame Format, Network Adaptors. **(16 hours)**

UNIT III

Packet Switching : Switching and Forwarding : Datagrams, Virtual Circuit Switching, Source Routing, Bridges and LAN Switches: Learning Bridges, Spanning Tree Algorithm, Broadcast and Multicast, Limitations of Bridges, Cell Switching (ATM): Cells, Segmentation and Reassembly, Virtual Paths, Physical Layers for ATM, ATM in the LAN, Implementation and Performance. **(16 hours)**

TextBooks:

(1). "Computer Networks, A Systems Approach", Larry L. Peterson & Bruce S. Davie, Third Edition, Morgan Kaufmann Publishers, 2003

(2). "Computer Networks" , Andrew S. Tanenbaum David J. Wetherall, Fifth Edition, Pearson Education Limited 2014

(3). "A Professional's Guide to Data Communication in a TCP/IP World", E. Bryan Carne, Artech House Inc, 2004

CSCS 404 : Mathematical Foundations of Hardware security

CO1: To appreciate the mathematical structures which are the foundations of security at the hardware level.

CO2: To appreciate the different digital hardware components required for the realization of security at the hardware level.

CO3: To study the different cryptographic schemes which are suitable for the implementation in the hardware level.

CO4: To understand the tradeoffs required while implementing the security at the hardware level.

UNIT I

Algebra and Number Theory : Modular Arithmetic, Groups, Rings, and Fields, Greatest Common Divisors and Multiplicative Inverse, Subgroups, Subrings, and Extensions, Groups,

Rings, and Field Isomorphisms, Polynomials and Fields, Construction of Galois Field, Extensions of Fields, Cyclic Groups of Group Elements, Efficient Galois Fields, Mapping between Binary and Composite Fields. **(12 hours)**

UNIT II

Block Ciphers: Inner Structures of a Block Cipher, The Advanced Encryption Standard(AES), The AES Round Transformations, Rijndael in Composite Field, Elliptic Curves, Scalar Multiplications: LSB First and MSB First Approaches, Montgomery's Algorithm for Scalar Multiplication. **(12 hours)**

UNIT III

FPGA Architecture, The FPGA Design Flow, Mapping an Algorithm to Hardware: Components of a Hardware Architecture, Case study: Binary gcd Processor, Enhancing the Performance of a Hardware Design, **Modelling of the Computational Elements of the gcd Processor** : Modeling of an Adder, Modeling of a Multiplexer, Total LUT Estimate of the gcd Processor, Delay Estimate of the gcd Processor. **(12 hours)**

TextBooks:

(1). "Hardware Security Design, Threats, and Safeguards", Debdeep Mukhopadhyay Rajat Subhra Chakraborty, CRC Press, 2015

(2). " Hardware IP Security and Trust", Prabhat Mishra, Swarup Bhunia, Mark Tehranipoor, Springer, 2017

(3). "Fault Tolerant Architectures for Cryptography and Hardware Security", Sikhar Patranabis Debdeep Mukhopadhyay, Springer, 2018

(4). "Security of Block Ciphers - From Algorithm Design to Hardware Implementation", Kazuo Sakiyama, Yu Sasaki, Yang Li, Wiley, 2015

(5). "Physically Unclonable Functions From Basic Design Principles to Advanced Hardware Security Applications", Basel Halak, Springer, 2018

(6). "Hardware-Based Computer Security Techniques to Defeat Hackers From Biometrics to Quantum Cryptography", Roger Dube, Wiley, 2008

CSCS 405 : Problem Solving Using Python

CO1 : To make students appreciate the utility of python in the purpose of data analytics.

CO2: To make the students understand the versatility of python in the form of huge varieties of packages available for data analysis, artificial intelligence and cryptography.

CO3: To make the students understand the possibility of using python as the language for computer system administration.

CO4: To make the students aware of algorithmic aspects of programming and its need in the study and implementation of cryptography.

UNIT I

Foundation: Computer hardware architecture, Understanding programming, The Way of the Program, The building blocks of programs, Writing a program, Variables, Variable names and keywords, Expressions and Statements, Operators and operands, String operations, Functions, Built-in functions, Type conversion functions, Conditionals and Recursion, Chained conditionals, Catching exceptions using try and except, Iteration, break & continue, Loop patterns. **(12 hours)**

UNIT II

Data Processing : Strings, String slices, String len functions, Looping and counting with strings, string methods, Format operator, Lists, List operations, Lists and functions, Lists and strings, Dictionaries, Dictionaries and files, Looping and dictionaries, Tuples, Tuple assignment, Using tuples as keys in dictionaries, Files, Text files and lines, Using try, except, and open.

(12 hours)

UNIT III

Object Orientation : Managing Larger Programs, Classes as Types, Object Lifecycle, Our First Python Object, Fruitful Functions & void functions, Classes and Functions, Subdividing a Problem-Encapsulation, Many Instances, Classes and Methods, Inheritance, Debugging, Syntax errors, Runtime errors, Semantic errors. **(12 hours)**

Text Books:

(1). “Think Python: How to Think Like a Computer Scientist”, Allen B. Downey, Second Edition, Green Tea Press, 2015.

(2). “Python for Everybody: Exploring Data Using Python 3”, Charles R.Severance, 1st Edition,

CreateSpace Independent Publishing Platform, 2016.

(3). " Learning Python for Forensics - Leverage the power of Python in forensic investigations", Preston Miller, Chapin Bryce, Packt Publishing, Second Edition, 2019

CSCS 406 : Management of the digital Value Chain in eBusiness, eCommerce and eGovernance

CO1 : To make the students aware of digital value in the form of currency, credential information, in eBusiness, eCommerce and eGovernance.

CO2: To make students aware of the importance of digital value and assets in eBusiness, eCommerce and eGovernance

CO3: To make students aware of the different domains of the knowledge economy.

CO4: To make students aware of the data flow paths in eBusiness, eCommerce and eGovernance.

UNIT I

eBusiness Framework: Defining Electronic Business, Case Studies : Electronic Shop (B2C), Electronic Health Market (B2B), Electronic Voting and Elections (A2C), Knowledge Exchange via Electronic Books (C2C), **eProducts and eServices:** Components of a Business Model, Anatomy of an Electronic Marketplace, Classification of Business Webs According to Tapscott, Comparison and Valuation of Networks, The Price Formation Process, **eProcurement:** Strategic and Operational Procurement, Information Support for Procurement, Basic Types of eProcurement Solutions, Catalog Management. **(12 hours)**

UNIT II

eMarketing : The Path to Individual Marketing, Comparison of the Communications Media, The Development Model for Online Customers, Online Promotion**, eContracting:** The Electronic Negotiation Process, Generic Services for the Negotiation Process, The Digital Signature, XML and Electronic Contracts, Legal Rights of the Information Society, **eDistribution:** Components of a Distribution System, Types of Distribution Logistics, Supply Chain Management, Electronic Software Distribution (ESD), Protection Through Digital Watermarks, **ePayment :** Credit Card-Based Procedures, Asset-Based Procedures, Innovative ePayment Solutions, Comparison of ePayment Solutions**.** **(12 hours)**

UNIT III

eCustomer Relationship Management: The Customer Equity Model by Blattberg et al, Analytical Customer Relationship Management, Operational Customer Relationship Management, Use of CRM Systems, **mBusiness :** Mobile Devices, Mobile Communications, Mobile Applications**, eSociety:** Virtual Organizations, Work Organization in eTeams, The Knowledge Worker in a Knowledge Society, Measuring the Success of Intellectual Capita, Ethical Maxims for eTeams**.** **(12 hours)**

TextBooks :

(1). "eBusiness & eCommerce- Managing the digital Value Chain", Andreas Meier, Henrik Stormer, Springer, 2009

(2). "Digital Economy: Impacts, Influences and Challenges", Harbhajan S. Kehal, Varinder P. Singh, IDEA GROUP PUBLISHING, 2005

(3). "The Digital Economy Fact Book", NINTH EDITION, Daniel B. Britton Stephen McGonegal, The Progress & Freedom Foundation, 2007

CSCS 407 - Complexity Analysis of Algorithms

CO1 : To make the students aware of the scarcity of computing resources like time and memory.

CO2: To make the students aware of the computational complexity and hardness of certain problems in various fields of study.

CO3: To understand the notion of security as a spinoff of the computationally hard problems.

CO4: To assimilate in the students, the lingua franca of algorithms, namely Big-Oh notation.

UNIT I

Introduction to algorithms: Big-O notation, **Algorithms with numbers:** Basic arithmetic, Modular arithmetic, Primality testing, Cryptography, Universal hashing, Randomized

algorithms**, Divide-and-conquer algorithms:** Multiplication, Recurrence relations, Mergesort **Decompositions of graphs:** The need of graphs, Depth-first search in undirected graphs, Depth-first search in directed graphs. **(12 hours)**

UNIT II

Paths in graphs: Distances, Breadth-first search, Lengths on edges, Dijkstra's algorithm **Greedy algorithms:** Minimum spanning trees, Huffman encoding **Dynamic programming:** Longest increasing subsequences, Knapsack, Chain matrix multiplication, Shortest paths, Independent sets in trees.
(12 hours)

UNIT III

NP-complete problems: Search problems, Class NP, NP-hard problem, Reduction, NP-complete problems, **Coping with NP-completeness:** Intelligent exhaustive search, Approximation algorithms, Local search heuristics, P vs NP Problem, SAT solvers.
(12 hours)

Textbooks:

(1) Algorithms - Sanjoy Dasgupta, Christos Papadimitriou and Umesh Vazirani, TMH-2008

(2) Introduction to Algorithms – Thomas H.Cormen, Charles E. Leiserson, Ronald L Rivest, Clifford Stein, 3rd edition, The MIT Press, 2009

(3) Combinatorial Optimization : Algorithms and Complexity, Christos H. Papadimitriou, Kenneth Steiglitz

CSCS 408 - Linux Administration & Shell Scripting

CO1 : To make students aware of the robustness of the linux operating system and to train the students to become efficient administrators of it.

CO2: To harness the rich and diverse ecosystem of the open source softwares which can be utilized for cybersecurity.

CO3: To present Linux operating system as credible defense against cyberattacks.

CO4: To understand the linux shell scripting language to be utilized for the automation of

administrative tasks in cybersecurity.

UNIT I

The Linux Command Line : Starting with Linux Shells, Looking into the Linux kernel, Linux Distributions, Getting to the Shell, Terminal Emulation, The Linux Console, The GNOME Terminal, Starting the Shell, Basic bash Shell Commands, Filesystem Navigation, File Handling, More bash Shell Commands, Monitoring Programs, Monitoring Disk Space, Working with Data Files, Using Linux Environment Variables, Setting Environment Variables, Setting the PATH Environment Variable, Understanding Linux File Permissions, Linux Security,Changing Security Settings, Working with Editors-vim, emacs, KDE Family, GNOME. **(12 hours)**

UNIT II

Shell Scripting Basics : Basic Script Building, Creating a Script File, Using Variables, Exiting the Script, Using Structured Commands, The if-then-else Statement, Compound Condition Testing, Advanced if-then Features, The case Command, More Structured Commands, The for, while & until Commands, Looping on File Data, Command Line & Special Parameters, Handling User Input, Presenting Data, Script Control, Handling Signals, Running Scripts in Background Mode, Job Control, Being Nice, Creating Functions, Basic Script Functions, Function Recursion, Creating a Library, Introducing sed and gawk, Regular Expressions, Shell Scripts for Administrators, Monitoring System Statistics, Performing Backups.**(12 hours)**

UNIT III

Linux Administration : Where to Start, Linux's relationship to UNIX, Notation and typographical conventions, Where to go for information, Booting and Shutting Down, Bootstrapping, Using boot loaders: LILO and GRUB, Working with startup scripts, Rebooting and shutting down, Rootly Powers, The superuser, Becoming root, Other pseudo-users, Controlling Processes, Components of a process, The life cycle of a process, The Filesystem, File types, Adding New Users, Adding a Disk, Periodic Processes, Backups, Syslog and Log Files, Software and Configuration Management. **(12 hours)**

Text Books:

(1). "Linux Command Line and Shell Scripting Bible", Richard Blum, Wiley Publishing, Inc, 2008.
(2). "Linux Administration Handbook", Evi Nemeth, Garth Snyder & Trent R. Hein, Second Edition, Prentice Hall, 2006.

Semester II

CSCH 451 - Advanced aspects of Computer Networks

CO1 : To make the students aware of the advanced aspects of computer networks and to have the knowledge of different protocols which make the computer networks work reliably.

CO2: To make the students aware of the importance of the knowledge of computer networks to secure the data confidentiality, integrity and availability.

CO3: To make the students aware of the different architectures of computer networks.

CO4: To allow students to practically simulate and study all the practical aspects of computer networks.

UNIT I

Internetworking: Simple Internetworking (IP): Service Model, Global Addresses, Datagram Forwarding in IP, Address Translation (ARP), Host Configuration (DHCP), Error Reporting (ICMP), Virtual Networks and Tunnels , Routing: Network as a Graph, Distance Vector (RIP), Link State (OSPF), Metrics, Routing for Mobile Hosts, Global Internet: Subnetting, Classless Routing (CIDR), Interdomain Routing (BGP), Routing Areas , IP Version 6 (IPv6), Multicast: Link-State Multicast, Distance-Vector Multicast, Protocol Independent Multicast(PIM), Multiprotocol Label Switching (MPLS): Destination-Based Forwarding, **End-to-End Protocols**: Simple Demultiplexer (UDP), Reliable Byte Stream (TCP), Remote Procedure Call.

(16 hours)

UNIT II

Congestion Control and Resource Allocation : Issues in Resource Allocation: Network Model, Taxonomy, Evaluation Criteria, Queuing Disciplines: FIFO, Fair Queuing, , TCP Congestion Control: Additive Increase/Multiplicative Decrease, Slow Start, Fast Retransmit and Fast

Recovery, Congestion-Avoidance Mechanisms: DECbit, Random Early Detection (RED), Source-Based Congestion Avoidance, Quality of Service, **End-to-End Data :** Presentation Formatting, Data Compression. **(16 hours)**

UNIT III

Network Security : Cryptographic Algorithms, Security Mechanisms, Example Systems, Firewalls, **Applications :** Name Service (DNS), Traditional Applications, Multimedia Applications, Overlay Networks. **(16 hours)**

TextBooks:

(1). "COMPUTER NETWORKS, A Systems Approach", Larry L. Peterson & Bruce S. Davie, Third Edition, Morgan Kaufmann Publishers, 2003

(2). "Computer Networks" , Andrew S. Tanenbaum David J. Wetherall, Fifth Edition, Pearson Education Limited 2014

(3). "A Professional's Guide to Data Communication in a TCP/IP World", E. Bryan Carne, Artech House Inc, 2004

CSCH 452 - Network Security

CO1 : To make students aware of the different attacks on the computer networks.

CO2: To make students aware of the different ways to identify and thwart attacks on the computer networks.

CO3: To make students aware of the different network configurations which are vulnerable and the ones which are robust against cyberattacks.

CO4: To make the students aware of the different tools required to attain network security of an organization.

UNIT I

How To Hack Computer Network: Understanding the Current Legal Climate, The Laws of Security: Client-Side Security Doesn't Work : Hacking Firewalls, Evading IDS Can, Insecurity

Secret Cryptographic Algorithms, password to protect password in client side, **Classes of Attack:** Denial of Service, Information Leakage, Symbolic Link Attacks, Attacks against Special Files, Attacks against Databases, Identifying Methods of Testing for Vulnerabilities, Methodology, Diffing, Cryptography, Unexpected Input, Buffer Overflow, Format Strings.

(16 hours)

UNIT II

Sniffing: Obtaining Authentication Information, Popular Sniffing Software, Advanced Sniffing Techniques, Exploring Operating System APIs, Taking Protective Measures, Employing Detection Techniques **Session Hijacking:** Understanding Session Hijacking, Examining the Available Tools, Playing MITM for Encrypted Communications, **Spoofing:** Attacks on Trusted Identity, The Evolution of Trust, Establishing Identity within Computer, Capability Challenges, Desktop Spoofs, Impacts of Spoofs, **Tunneling:** Strategic Constraints of Tunnel Design, Designing End-to-End Tunneling Systems, Port Forwarding: Accessing Resources on Remote Networks, Hardware Hacking, Viruses, Trojan Horses, and Worms. **(16 hours)**

UNIT III

IDS Evasion: Using Packet Level Evasion, Using Application Protocol Level Evasion, **Automated Security Review and Attack Tools** : Exploration of the Commercial automated security Tools, Reporting Security Problems. **(16 hours)**

Text Books

(1). "Hack proofing your network ", Ryan Russell, Syngress, 2002

(2). "Network and System Security", John R. Vacca, Syngress, 2010

(3). "COMPUTER NETWORKS, A Systems Approach", Larry L. Peterson & Bruce S. Davie, Third Edition, Morgan Kaufmann Publishers, 2003

(4). "Computer Networks" , Andrew S. Tanenbaum David J. Wetherall, Fifth Edition, Pearson Education Limited 2014

CSCH 453 - Ethical Hacking

CO1 : To make the students aware of the different ways to assess the vulnerabilities in the ICT

facilities of an organisation or a business entity.

CO2: To hack into the websites and networks of a party, with the consent in a bid to unearth the vulnerabilities and suggest remedies to fix the same.

CO3: To make the students aware of the legal aspects of ethical hacking and to sensitize where the danger line lies.

CO4: To promote ethical hacking as a profession for the students.

UNIT I

Introduction to Ethical Hacking, Footprinting & Reconnaissance, Scanning Networks, Enumeration, Vulnerability Analysis. **(16 hours)**

UNIT II

System Hacking, Malware Threats, Sniffing, Social Engineering, Denial-of-Services, Session Hijacking, Evading IDS, Firewall & Honeypots. **(16 hours)**

UNIT III

Hacking Web Servers, Hacking Web Applications, SQL Injection, Hacking Wireless Networks, Hacking Mobile Platforms, IoT Hacking, Cloud Computing. **(16 hours)**

TextBooks:

(1). "CEH V10 EC-Council Certified Ethical Hacker", Nouman Ahmed Khan, Abubakar Saeed, Muhammad Yousuf

(2). "CEH v10 TM Certified Ethical Hacker Study Guide", Ric Messier, Sybex, 2019

(3). "Hack proofing your network ", Ryan Russell, Syngress, 2002

(4). "Network and System Security", John R. Vacca, Syngress, 2010

CSCS 454 - Hardware Design of Cryptographic Algorithms

CO1 : To make students aware of the different digital hardware options available for implementing security at the hardware level.

CO2: To make students aware of the different FPGA architectures available in the market for hardware security implementation.

CO3: To make aware of the tradeoffs which are necessary while implementing hardware security compared to software security.

CO4: To make the students aware of the Elliptic curve cryptography as faster means of achieving hardware security.

UNIT I

Hardware Design of the Advanced Encryption Standard (AES) : Algorithmic and Architectural Optimizations for AES Design, Circuit for the AES S-Box, Implementation of the MixColumns Transformation, Reconfigurable Design for the Rijndael Cryptosystem, Single Chip Encryptor/Decryptor. **(12 hours)**

UNIT II

Efficient Design of Finite Field Arithmetic on FPGAs : Finite Field Multiplier, Finite Field Multipliers for High Performance Applications, Karatsuba Multiplication, Karatsuba Multipliers for Elliptic Curves, Designing for the FPGA Architecture, Analyzing Karatsuba Multipliers on FPGA Platforms, High-Performance Finite Field Inversion Architecture for FPGAs, Itoh-Tsujii Inversion Algorithm, The Quad ITA Algorithm, Generalization of the ITA for 2^n Circuit, Hardware Architecture for 2^n Circuit Based ITA, Area and Delay Estimations for the 2^n ITA.

(12 hours)

UNIT III

High-Speed Implementation of Elliptic Curve Scalar Multiplication on FPGAs : The Elliptic Curve Cryptoprocessor, Point Arithmetic on the ECCP, The Finite State Machine (FSM), Acceleration Techniques of the ECC Processor, Pipelining Strategies for the Scalar Multiplier, Scheduling of the Montgomery Algorithm, Finding the Right Pipeline, Detailed Architecture of the ECM. **(12 hours)**

TextBooks:

(1). “Hardware Security Design, Threats, and Safeguards”, Debdeep Mukhopadhyay Rajat Subhra Chakraborty, CRC Press, 2015

(2). " Hardware IP Security and Trust " , Prabhat Mishra, Swarup Bhunia, Mark Tehranipoor, Springer, 2017

(3). "Fault Tolerant Architectures for Cryptography and Hardware Security", Sikhar Patranabis Debdeep Mukhopadhyay, Springer, 2018

(4). "Security of Block Ciphers - From Algorithm Design to Hardware Implementation", Kazuo Sakiyama, Yu Sasaki, Yang Li, Wiley, 2015

(5). "Physically Unclonable Functions From Basic Design Principles to Advanced Hardware Security Applications", Basel Halak, Springer, 2018

(6). "Hardware-Based Computer Security Techniques to Defeat Hackers From Biometrics to Quantum Cryptography", Roger Dube, Wiley, 2008

CSCS 455 - Darkweb Cyber Threat Intelligence Mining : Principled Study of the Industrialization of Cyber Offense

CO1 : To make the students aware of the industrialization of cyberattack tools which are available in the most organised in a marketplace called, "darkweb"

CO2: To make the students aware of the ways to use most modern data analytical tools in understanding the organisation of cybercriminals and their ways of functioning.

CO3: To make cyber threat intelligence as a credible way to tackle cyber warfare and cyber terrrorism.

CO4: To use game theoretic concepts in thwarting the cyberattacks.

UNIT I

Moving to Proactive Cyber Threat Intelligence: Proactive Intelligence beyond the Deepweb and Darkweb, **Understanding Darkweb Malicious Hacker Forums:** Forum Structure and Community Social Organization. **(12 hours)**

UNIT II

Automatic Mining of Cyber Intelligence from the Darkweb, Analyzing Products and Vendors in Malicious Hacking Markets: Marketplace Data Characteristics, Users Having Presence in Markets/Forums, Discovery of Zero-Day Exploits, Exploits Targeting Known Vulnerabilities.

(12 hours)

UNIT III

Using Game Theory for Threat Intelligence: Security Game Framework, Computational Complexity, Algorithms, **Application:** Protecting Industrial Control Systems, **Challenges and Environmental Characteristics.** **(12 hours)**

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 & its Security

CO1 : To make the students aware of the different cloud architectures which are available for services.

CO2: To make the students aware of the security of data in a cloud environment.

CO3: To make the students aware of the misconfiguration of the cloud settings as the biggest source of vulnerabilities.

CO4: To make robust cloud services with all the security aspects put in place.

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 Center, 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)

Text Books:

(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 457 - Digital System Design using Verilog

CO1 : To make the student ready with the skills of digital hardware design.

CO2: To understand the different language constructs of Verilog HDL which are utmost essential.

CO3: To make the students aware of the tradeoffs between different language constructs in achieving the best performance.

CO4: To make the master of designing computational elements of cryptography over a hardware.

UNIT I

Introduction to logic design using Verilog HDL: Logic Elements, Expressions, Modules and Ports, Built-In Primitives , User-Defined Primitives, Dataflow Modeling, Behavioral Modeling, Structural Modeling, Tasks and Functions, Problems. **(12 hours)**

UNIT II

Combinational Logic Design Using Verilog HDL: Number Systems, Boolean Algebra, Logic Equations, Multiplexers, Comparators, Programmable Logic Devices, Additional Design Examples, Problems. **(12 hours)**

UNIT III

Sequential Logic Design using Verilog HDL : Definition of a Sequential Machine, Synchronous Sequential Machines, Asynchronous Sequential Machines, Pulse-Mode Asynchronous Sequential Machines, Problems. Introduction to Computer Arithmetic design using Verilog HDL: Introduction, Fixed point arithmetic operations (basic), ALU, Decimal arithmetic operations, Floating point operations, Problems. **(12 hours)**

Textbooks:

(1). “Verilog HDL Design Examples”, Joseph Cavanagh, CRC Press, 2018

(2). “Verilog HDL: A Guide to Digital Design and Synthesis”, Samir Palnitkar, Pearson Education, 2003.

(3). “Digital Design : With an Introduction to the Verilog HDL”, M. Morris Mano, Michael D. Ciletti, Prentice Hall, 2012

(4). “Verilog HDL Synthesis A Practical Primer”, J. Bhasker, Star Galaxy Publishers, 1998.

CSCS 458 - Internet of Things Security

CO1 : To make the students aware of the IoT as the new wave in the computing arena, wherein anything and everything is being connected to the internet.

CO2: To make the students aware of the security of data on IoT.

CO3: To make the students aware of the certain specific security issues which are impotent to IoT.

CO4: To make the students aware of the cost and tradeoffs in achieving security and balancing the performance in an IoT.

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. **(12 hours)**

UNIT III

Mitigating IoT Privacy Concerns: Privacy challenges introduced by the IoT, Guide to performing an IoT PIA, PbD principles, Privacy engineering recommendations. **Setting Up a Compliance Monitoring Program for the IoT**: IoT compliance, A complex compliance environment. **Cloud Security for the IoT:** Cloud services and the IoT, Exploring cloud service provider IoT offerings, Cloud IoT security controls, Tailoring an enterprise IoT cloud security

architecture, New directions in cloud-enabled IOT computing. **IoT Incident Response**: Threats both to safety and security, Planning and executing an IoT incident response **(12 hours)**

Text Books:

1. Brian Russell and Drew Duren, "Practical Internet of Things Security", Packt Publishing, 2016

2. Giancarlo Fortino and Carlos E. Palau "Interoperability, Safety and Security in IoT" Springer Publications 2017.

3. Zaigham Mahmood, Shijiazhuang, "Security, Privacy and Trust in the IoT Environment" Springer Publications, 2019.

CSCO 462 - Strategic Governance of Cybersecurity Risks and Control Mechanisms I (OPEN CHOICE)

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 the students competent in risk assessment and analysis in case of a cyber incidence.

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

The Importance of Cybersecurity Management: The Growing Pains of an Emerging Discipline, Understanding the Costs and Benefits of cybersecurity management to an Organization, Two Absolute Rules for Cybersecurity Work, Implementing a Strategic Response.

(12 hours)

UNIT II

Control-Based Information Governance: The Value of Formal Control, Organizing Things into a Rational Process, Information Audit and Control, Control Principles, **A Survey of Control**

Frameworks: COSO Framework, IT Infrastructure Library Framework, ISO 27001, COBIT 5, IT Security Controls**,** General Structure and Applications. **(12 hours)**

UNIT III

The Importance of Controls: Goal-Based Security Controls, Implementation-Based Security Controls, The Security Control Formulation and Development Process, Control Implementation through Security Architecture Design, **Implementing a Multitiered Governance and Control Framework in a Business :** Constructing Practical Systems of Controls, Building the Security Control System, Initial Setup and Tradeoffs. **(12 hours)**

TextBooks:

(1). "The Complete Guide to Cybersecurity Risks and Controls", Anne Kohnke, Dan Shoemaker, Ken Sigleer, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016

(2)."Securing an IT Organization through Governance, Risk Management, and Audit", Ken Sigler, Dr. James L. Rainey, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016

(3). "A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)", Anne Kohnke, Dan Shoemaker, Ken Sigleer, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016

(4). "Cybercrimes: A Multidisciplinary Analysis", Sumit Ghosh, Elliot Turrini, Springer, 2010

Semester III

CSCH 501 : Digital Forensics

CO1 : To train the students to become digital forensics professionals who are required for the law enforcement in the case of cyber incidents.

CO2 : To give the students all possible practical scenarios for the students to perform the digital forensics tasks, with both the technological and legal aspects of the case.

CO3 : To provide the students with the adequate skills required in the form of technical writing skills for the digital forensics.

CO4 : To cultivate the habit of reporting any cyber incidents at the earliest to the law

enforcement agencies.

UNIT I

Introduction To Digital Forensics : Introduction, Evolution Of Computer Forensics, Stages Of Computer Forensics Process, Benefits Of Computer Forensics, Uses Of Computer Forensics, Objectives Of Computer Forensics, Role Of Forensics Investigator, Forensics Readiness, **Computer Forensics Investigation Process** : Introduction To Computer Crime Investigation, Assess The Situation, Acquire The Data, Analyze The Data, Report The Investigation, Digital Evidence And First Responder Procedure, Digital Evidence, First Responder Toolkit, Issues Facing Computer Forensics, Types Of Investigation, Techniques Of Digital Forensics

(16 hours)

UNIT II

Understanding Storage Media And File System : Hard Disk Drive, Details Of Internal Structure Of Hdd, The Booting Process, File System, **Windows Forensics** : Introduction, Recovering Deleted Files And Partitions, More About Recovering Lost Files/Data, **Logs & Event Analysis And Password Cracking** : Introduction, Windows Registry, Windows Event Log File, Windows Password Storage, Application Passwords Crackers, **Network Forensics** : Introduction, Network Components And Their Forensics Importance, Osi, Forensics Information From Network, Log Analysis, Forensics Tools, **Wireless Attacks** : Introduction, 4.3wireless Fidelity (Wi-fi)(802.11), Wireless Security, Wireless Attacks Detection Techniques, Wireless Intrusion Detection Systems

(16 hours)

UNIT III

Investigating Web Attacks : Introduction, Types Of Web Attacks, Web Attack Forensics, Web Application Forensics Tools, **Investigating Email Attacks** : Introduction, Email Attacks And Crimes, Privacy In Emails, Email Forensics, Email Forensic Tools, **Mobile Device Forensics** : Introduction, Challenges In Mobile Forensics, Mobile Communication, Evidences In A Mobile Device, Mobile Forensic Process, Forensic Acquisition Tools, Investigative Reports, **Expert Witness And Cyber Regulations** : Introduction, Report Preparation, Legal Aspects Of Computing

(16 hours)

Text Books:

(1). “Digital Forensics”- Dr.Jeetendra Pande, Dr. Ajay Prasad, Uttarakhand Open University, Haldwani - 2016

(2). “Computer Forensics and Cyber Crime An Introduction”- Marjie T. Britz, Pearson, Third Edition, 2013

(3). “ Learning Python for Forensics - Leverage the power of Python in forensic investigations”, Preston Miller, Chapin Bryce, Packt Publishing, Second Edition, 2019

(4). “ A Practical Guide to Computer Forensics Investigations”, Dr. Darren R. Hayes, Pearson Education, 2015

CSCH 502 : Web Penetration Testing

CO1 : To assess the vulnerabilities available in a website, with a written consent from the owner of the website.

CO2: To master various tools available for the web penetration testing.

CO3: To understand all the strategic steps necessary to perform the web penetration testing professionally and to be legally compliant.

CO4: To encourage the students to take up web penetration testing as a profession and make a living out of it.

UNIT I

Introduction to Penetration Testing and Web Applications : Proactive security testing, Considerations when performing penetration testing, Kali Linux, A web application overview for penetration testers, **Setting Up Your Lab with Kali Linux** : Kali Linux, Important tools in Kali Linux, Vulnerable applications and servers to practice on, **Reconnaissance and Profiling the Web Server** : Reconnaissance, Information gathering, Scanning – probing the target, **Authentication and Session Management Flaws :** Authentication schemes in web applications, Session management mechanisms, Common authentication flaws in web applications, Detecting and exploiting improper session management, Preventing authentication and session attacks

(16 hours)

UNIT II

Detecting and Exploiting Injection-Based Flaws : Command injection, SQL injection, XML injection, NoSQL injection, Mitigation and prevention of injection vulnerabilities, **Finding and Exploiting Cross-Site Scripting (XSS)Vulnerabilities :** An overview of Cross-Site Scripting,

Exploiting Cross-Site Scripting, Scanning for XSS flaws, Preventing and mitigating Cross-Site Scripting, **Cross-Site Request Forgery, Identification, and Exploitation :** Testing for CSRF flaws, Exploiting a CSRF flaw, Preventing CSRF, **Attacking Flaws in Cryptographic Implementations :** A cryptography primer, Secure communication over SSL/TLS, Identifying weak implementations of SSL/TLS, Custom encryption protocols, Common flaws in sensitive data storage and transmission, Preventing flaws in cryptographic implementations

(16 hours)

UNIT III

AJAX, HTML5, and Client-Side Attacks : Crawling AJAX applications, Analyzing the client-side code and storage, HTML5 for penetration testers, Bypassing client-side controls, Mitigating AJAX, HTML5, and client-side vulnerabilities, **Other Common Security Flaws in Web Applications :** Insecure direct object references, File inclusion vulnerabilities, HTTP parameter pollution, Information disclosure, Mitigation, **Using Automated Scanners on Web Applications :** Considerations before using an automated scanner, Web application vulnerability scanners in Kali Linux, Content Management Systems scanners, Fuzzing web applications, Post-scanning actions

(16 hours)

Text Books :

(1). "Web Penetration Testing with Kali Linux", Gilberto Najera-Gutierrez, Juned Ahmed Ansari, Packt Publishing, Third Edition, 2018

(2). "Kali Linux Revealed", Mastering the Penetration Testing Distribution, Raphaël Hertzog, Offsec Press, 2017

(3). " Learn Kali Linux 2019", Glen D. Singh, Packt Publishing, 2019

(4). " Quick Start Guide to Penetration Testing", Sagar Rahalkar, Apress, 2019

CSCH 503: Cybersecurity with Blockchain

CO1 : To understand the new form of disruptive technology which is coming up in the world wide economy, as a way to assure data security.

CO2: To offer an alternative form of DNS servers, based on blockchain with better security aspects.

CO3: To consider blockchain as a means to thwart cyberattacks like DDoS.

CO4: To look into the future perspective available for cybersecurity and blockchain.

UNIT I

Cyber Threat Landscape and Security Challenges : Current threat landscape, Defender perspectives, Live attack execution, Emerging security challenges, **Evolution of Security:** The security ecosystem, The zero-trust approach, The assume breach approach, Evolution at the foundation layer, **Introducing Blockchain and Ethereum :** Introduction to blockchain, Internet versus blockchain, How blockchain works, The building blocks of blockchain, Ethereum, Private vs Public Blockchain, Business adaptation

(16 hours)

UNIT II

Hyperledger, the Blockchain for Businesses : Technical requirements, Hyperledger overview, Blockchain-as-a-service (BaaS), Architecture and core components, Hyperledger Fabric model, Bitcoin versus Ethereum versus Hyperledger, Hyperledger Fabric capabilities, **Blockchain on the CIA Security Triad :** Understanding blockchain on confidentiality, Blockchain on integrity, Understanding blockchain on availability, **Deploying PKI-Based Identity with Blockchain :** PKI, Challenges of the existing PKI model, How blockchain can help, **Two-Factor Authentication with Blockchain:** Introduction to 2FA, Blockchain for 2FA

(16 hours)

UNIT III

Blockchain-Based DNS Security Platform : Understanding DNS components, DNS structure and hierarchy, DNS topology for large enterprises, Challenges with current DNS, Blockchain-based DNS solution, **Deploying Blockchain-Based DDoS Protection :** DDoS attacks, Types of DDoS attacks, Challenges with current DDoS solutions, How blockchain can transform DDoS protection, **Facts about Blockchain and Cyber Security:** Decision path for blockchain, Leader's checklist, Challenges with blockchain, The future of cybersecurity with blockchain

(16 hours)

TextBooks:

(1). "Hands-On Cybersecurity with Blockchain", Rajneesh Gupta, Packt Publishing, 2018

(2). “Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions”, Joseph J. Bambara Paul R. Allen, McGraw-Hill Education, 2018

(3). “Blockchain Enabled Applications”, Vikram Dhillon, David Metcalf, Max Hooper, Apress, 2017

(4). “Blockchain Blueprint for a New Economy”, Melanie Swan, O’Reilly Media, 2015

(5). “Blockchain Basics: A Non-Technical Introduction in 25 Steps”, Daniel Drescher, Apress, 2017

CSCS 504 : Cryptanalysis of Hardware Security

CO1 : To perform the cryptanalysis at the hardware level, which requires special kind skills, tools and methods which are different from software level cryptanalysis.

CO2: To understand the different means of breaking the hardware security like side channel attack.

CO3: To understand the different means of breaking hardware security like power analysis attack.

CO4: To understand the different means of breaking hardware security like timing attack.

UNIT I

Side Channel Analysis : Difference of Side Channel Analysis and Conventional Cryptanalysis, Types of Side Channel Attacks, Kocher’s Seminal Works, Power Attacks, Fault Attacks, Cache Attacks, Scan Chain Based Attacks, **Differential Fault Analysis of Ciphers :** General Principle of DFA of Block Ciphers, DFA and Associated Fault Models, Principle of Differential Fault Attacks on AES. **(12 hours)**

UNIT II

State-of-the-art DFAs on AES, Multiple-Byte DFA of AES-128, Extension of the DFA to Other Variants of AES, DFA of AES Targeting the Key Schedule, DFA countermeasures **Cache Attacks on Ciphers :** Memory Hierarchy and Cache Memory, Timing Attacks Due to CPU Architecture, Trace-Driven Cache Attacks, Access-Driven Cache Attacks, Time-Driven Cache

Attacks, Countermeasures for Timing Attacks. **(12 hours)**

UNIT III

Power Analysis of Cipher Implementations, Testability of Cryptographic Hardware, Hardware Intellectual Property Protection through Obfuscation, Hardware Trojans, Logic Testing based Hardware Trojan Detection, Side-channel Analysis Techniques for Hardware Trojans Detection, Design Techniques for Hardware Trojan Threat Mitigation, Physically Unclonable Functions: a Root-of-Trust for Hardware Security, Genetic Programming-based Model-building Attack on PUFs. **(12 hours)**

TextBooks:

(1). "Hardware Security Design, Threats, and Safeguards", Debdeep Mukhopadhyay Rajat Subhra Chakraborty, CRC Press, 2015

(2). " Hardware IP Security and Trust " , Prabhat Mishra, Swarup Bhunia, Mark Tehranipoor, Springer, 2017

(3). "Fault Tolerant Architectures for Cryptography and Hardware Security", Sikhar Patranabis Debdeep Mukhopadhyay, Springer, 2018

(4). "Security of Block Ciphers - From Algorithm Design to Hardware Implementation", Kazuo Sakiyama, Yu Sasaki, Yang Li, Wiley, 2015

(5). "Physically Unclonable Functions From Basic Design Principles to Advanced Hardware Security Applications", Basel Halak, Springer, 2018

(6). "Hardware-Based Computer Security Techniques to Defeat Hackers From Biometrics to Quantum Cryptography", Roger Dube, Wiley, 2008

CSCS 505 : Mobile Phone Security and Forensics

CO1 : To make the students aware of the forensics of mobile phones, which would aid the police investigation of a cybercrime.

CO2: To sensitize the students about the process of the mobile phone forensics and the legal aspects of the same.

CO3: To make students use the different tools required for the mobile phone forensics.

CO4: To make the students aware of the ways and means to acquire different data from mobile phones.

UNIT I

Mobile Phone Security : Confidentiality, Integrity, and Availability Threats in Mobile Phones, A Multinational Survey on Users' Practices, Perceptions, and Awareness Regarding Mobile Phone Security, Voice, SMS, and Identification Data Interception in GSM, Software and Hardware Mobile Phone Tricks, SMS Security Issues, Mobile Phone Forensics.

(12 hours)

UNIT II

Introduction to Mobile Forensics : The need for mobile forensics, Understanding mobile forensics, Challenges in mobile forensics, The mobile phone evidence extraction process, Practical mobile forensic approaches, Potential evidence stored on mobile phones, Examination and analysis, Rules of evidence, Good forensic practices, **Android Forensics** : Understanding Android, The evolution of Android, The Android architecture, Android security, The Android file hierarchy, The Android filesystem, Android Forensic Setup and Pre-Data Extraction Techniques, Setting up a forensic environment for Android, Connecting an Android device to a workstation, Screen lock bypassing techniques, Gaining root access

(12 hours)

UNIT III

Android Data Extraction Techniques : Understanding data extraction techniques, Manual data extraction, Logical data extraction, Physical data extraction, Android Data Analysis and Recovery, Analyzing and extracting data from Android image files using the Autopsy tool, Understanding techniques to recover deleted files from the SD card and the internal memory, Android App Analysis, Malware, and Reverse Engineering, Analyzing widely used Android apps to retrieve valuable data, Techniques to reverse engineer an Android application, Android malware.

(12 hours)

Text Books:

(1). "Mobile Phone Security and Forensics - A Practical Approach", Iosif I. Androulidakis, Springer International Publishing Switzerland, 2016

(2). "Practical Mobile Forensics - Forensically investigate and analyze iOS, Android, and

Windows 10 devices", Rohit Tamma. et al, Packt Publishing, Fourth Edition, 2020

(3). "Why Should I Care? to Protect Yourself and Your Organization from Today's Mobile Computing Threats, 10 Simple Things You Can Do, Mobile Security For The Rest Of Us", Veracode,

(4). "iPhone and iOS Forensics - Investigation, Analysis and Mobile Security for Apple iPhone, iPad, and iOS Devices", Andrew Hoog, Katie Strzempka, Elsevier, 2011

CSCS 506 : Cyber Laws

CO1 : To make the students aware of the different data privacy acts existing in India and worldwide.

CO2: To sensitize the students about the need to be compliant with the data privacy acts, as an Information governor.

CO3: To make the students aware of the penalty provisions available in the data privacy acts for any deviation.

CO4: To make students aware of the job opportunities in the field of cybersecurity due to the mandatory needs of officers like Data Protection Officers.

UNIT I

The Information Technology Act (IT Act), 2000 : Preliminary, Digital Signature And Electronic Signature, Electronic Governance, Attribution, Acknowledgement And Despatch Of Electronic Records, Secure Electronic Records And Secure Electronic Signature, Regulation Of Certifying Authorities, Electronic Signature Certificates, Duties Of Subscribers, Penalties, Compensation And Adjudication, The Appellate Tribunal, Offences, Intermediaries Not To Be Liable In Certain Cases, Examiner Of Electronic Evidence, Miscellaneous, Amendments As Introduced By The IT Amendment Act, 2008 **(12 hours)**

UNIT III

Personal Data Protection Bill(PDPB), 2019: Preliminary, Obligations Of Data Fiduciary, Grounds For Processing Of Personal Data Without Consent, Personal Data And Sensitive Personal Data Of Children, Rights Of Data Principal, Transparency And Accountability Measures, Restriction On Transfer Of Personal Data Outside India, Exemptions, Data Protection

Authority Of India, Penalties And Compensation, Appellate Tribunal, Finance, Accounts And Audit, Offences, Miscellaneous **(12 hours)**

UNIT III

General Data Protection Regulation(GDPR), 2018 of European Union : General provisions, Principles, Rights of the data subject, Controller and processor, Transfers of personal data to third countries or international organisations, Independent supervisory authorities, Cooperation and consistency, Remedies, liability and penalties, Provisions relating to specific processing situations, Delegated acts and implementing acts, Final provisions. **(12 hours)**

Text Books:

(1). "The Information Technology Act", 2000

(2). "The Personal Data Protection Bill", 2019

(3). "General Data Protection Regulation(GDPR)"- Official Journal of the European Union, 2016, https://gdpr-info.eu/

(4). "The Information Technology ACT", 2008

(5). "A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians"- Expert Committee Report under the Chairmanship of Justice B.N. Srikrishna, 2018

(6). "Computer Forensics and Cyber Crime An Introduction"- Marjie T. Britz, Pearson, Third Edition, 2013

CSCS 507 : eCommerce Site Security

CO1 : To assess the vulnerabilities available in a eCommerce website, with a written consent from the owner of the website.

CO2: To master various tools available for the eCommerce web penetration testing and to make sure that the reports are generated as per the legal requirements.

CO3: To understand all the strategic steps necessary to perform the web penetration testing

professionally and to be legally compliant, and in turn feed back the site design team with the necessary inputs for updation.

CO4: To encourage the students to take up eCommerce site design as a profession and make a living out of it.

UNIT I

Applying Security Principles to E-Business: Security as a Foundation**,** Applying Principles to Existing Sites, How to Justify a Security Budget, **DDoS Attacks:** Intent, Tools, and Defense, DDoS Attack, Reasons for E-Commerce Sites becoming the Prime Targets for DDoS, Motivations for an an Attacker to damage ecommerce sites, Some of the Tools used by attackers to Perform DDoS Attacks, **Secure Web Site Design:** Choosing a Web Server, The Basics of Secure Site Design, Guidelines for Java, JavaScript, and Active X**,** Designing and Implementing Security Policies.

(12 hours)

UNIT II

Implementing a Secure E-Commerce Web Site: Implementing Security Zones, Understanding Firewalls, Implementing Intrusion Detection, Managing and Monitoring the Systems, Pros and Cons of Outsourcing Your Site, **Securing Financial Transactions:** Understanding Internet-Based Payment Card Systems, Options in Commercial Payment Solutions, Examining E-Commerce Cryptography, **Hacking Your Own Site :** Anticipating Various Types of Attacks, Performing a Risk Analysis on Your Site, Testing Your Own Site for Vulnerabilities, **Disaster Recovery Planning:** The Best Defense.

(12 hours)

UNIT III

Handling Large Volumes of Network Traffic : Determining the Load on Your Site, Managing Bandwidth Needs, Introduction to Load Balancing, **Incident Response, Forensics and the Law:** Importance of Incident Response Policy, Establishing an Incident Response Team, Establishing an Incident Response Process, Introduction to Forensic Computing, Tracking Incidents

(12 hours)

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

(12 hours)

UNIT II

Creating a Management-Level Control Process, Assessing Control Performance, Developing a Comprehensive ICT Security Control Program **Security Control Validation and Verification:** Security Control Assessment Fundamentals, NIST Security Control Assessment Process, Control Testing and Examination Application.

(12 hours)

UNIT III

Control Framework Sustainment and Security of Operations : Operational Control Assurance: Aligning Purpose with Practice, Operational Assurance (Sensing), Analysis, Response Management (Responding), Operational Oversight and Infrastructure Assurance of Control Set Integrity. **(12 hours)**

TextBooks

(1). "The Complete Guide to Cybersecurity Risks and Controls", Anne Kohnke, Dan Shoemaker, Ken Sigleer, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016

(2)."Securing an IT Organization through Governance, Risk Management, and Audit", Ken Sigler , Dr. James L. Rainey, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016

(3). "A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)", Anne Kohnke, Dan Shoemaker, Ken Sigleer, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016

(4). "Cybercrimes: A Multidisciplinary Analysis", Sumit Ghosh, Elliot Turrini, Springer, 2010