ದಾವಣಗೆರೆ ವಿಶ್ವವಿದ್ಯಾನಿಲಯ

Davangere University

ಗಣಕ ವಿಜ್ಞಾನ ವಿಭಾಗ

DEPARTMENT OF STUDIES IN COMPUTER SCIENCE

Course Structure and Syllabus(CBCS) of

M.Voc in Cyber Security

(W.E.F 2020-21 and onwards)

Davangere University

Department of Studies in Computer Science

Programme Name: M.Voc in Cyber Security

Course Structure

Semester	Course Component	Subject/Paper Code	Title of the paper	Instruction Hrs/Week	Marks			Credits	Examination duration (Hrs)
					Examination	Internal assessment	Total marks		
Course Structure for SEMESTER-I									
SEMESTER - I	General Component	**MVCS 1.1**	Computer Network and Internet Security	4	70	30	100	4	3
		MVCS 1.2	Programming in C	4	70	30	100	4	3
		MVCS 1.3	Computer Network and Internet Security Lab	4	40	10	50	2	3
		MVCS 1.4	Programming in C Lab	4	40	10	50	2	3
	Skill Component	**MVCS 1.5**	Foundations of Cyber Security and Digital Forensics	4	70	30	100	4	3
		MVCS 1.6	Cyber Law and Indian IT Act	4	70	30	100	4	3
		MVCS 1.7	Python Programming for Cyber Security	4	70	30	100	4	3
		MVCS 1.8	Python Programming for Cyber Security Lab	4	40	10	50	2	3
		MVCS 1.9	Cyber Security and Digital Forensics Lab	4	40	10	50	2	3
Total credits for the Semester - I				36	--	--	700	**28**	--
Course structure for SEMESTER-II									
SEMESTER - II	General Component	**MVCS 2.1**	Ethical Hacking	4	70	30	100	4	3
		MVCS 2.2	Security of Operating System, Database and Infrastructure	4	70	30	100	4	3
		MVCS 2.3	Ethical Hacking Lab	4	40	10	50	2	3
		MVCS 2.4	Security of Operating System, Database and Infrastructure Lab	4	40	10	50	2	3
	Skill Component	**MVCS 2.5**	Cyber Security with Cloud Computing	4	70	30	100	4	3
		MVCS 2.6	Application Threat Detection	4	70	30	100	4	3
		MVCS 2.7	Cyber Threat and Modelling	4	70	30	100	4	3
		MVCS 2.8	Career Paths in Cyber Security and Digital Forensics	4	70	30	100	4	3
		MVCS 2.9	Cyber Security with Cloud Computing Lab	4	40	10	50	2	3
		MVCS 2.10	Cyber Threat and Modelling Lab	4	40	10	50	2	3
Total credits for the Semester - II				40	--	--	800	**32**	--

Semester	Course Component	Subject/Paper Code	Title of the paper	Instruction Hrs/Week	Marks			Credits	Examination duration (Hrs)
					Examination	Internal assessment	Total marks		
Course Structure for SEMESTE-III									
SEMESTER - III	General Component	MVCS 3.1	Data Analysis using R	4	70	30	100	4	3
		MVCS 3.2	Application and System Security	4	70	30	100	4	3
		MVCS 3.3	Data Analysis using R Lab	4	40	10	50	2	3
		MVCS 3.4	Application and System Security Lab	4	40	10	50	2	3
	Skill Component	MVCS 3.5	Cryptography and Information security	4	70	30	100	4	3
		MVCS 3.6	Security Policy and Audit	4	70	30	100	4	3
		MVCS 3.7	IoT and Digital Forensics	4	70	30	100	4	3
		MVCS 3.8	Cryptography and Information Security Lab	4	40	10	50	2	3
		MVCS 3.9	Minor Project	8	80	20	100	4	3
Total credits for the Semester - III				40	--	--	750	**30**	--
Course structure for SEMESTE-IV									
SEMESTER - IV	General Component	MVCS 4.1	Recent Cyber-Security Breaches and Attacks	4	70	30	100	4	3
		MVCS 4.2	Fundamentals of Information Assurance/Security	4	70	30	100	4	3
		MVCS 4.3	Cyber Security Case Studies Lab	4	40	10	50	2	3
		MVCS 4.4	Information Assurance/Security Lab	4	40	10	50	2	3
	Skill Component	MVCS 4.5	Artificial Intelligence for Cyber Security	4	70	30	100	4	3
		MVCS 4.6	Risk Management and Malware Analysis	4	70	30	100	4	3
		MVCS 4.7	Mobile and Wireless Security	4	70	30	100	4	3
		MVCS 4.8	Mobile and Wireless Security Lab	4	40	10	50	2	3
		MVCS 4.9	Major Project	8	80	20	100	4	3
Total credits for the Semester - IV				**40**	--	--	**750**	**30**	--

COURSE OBJECTIVES:

Master of Vocational course(M.Voc) in Cyber Security is a 2-year long postgraduate level degree course inculcating the study of cyber laws and cyber security. It includes the study of communication networks and technologies along with the analysis of legal and ethical issues in cyber security.

- Exhibit knowledge to secure corrupted systems, protect personal data, and secure computer networks in an Organization.
- Practice with an expertise in academics to design and implement security solutions.
- Understand key terms and concepts in Cryptography, Governance and Compliance.
- Develop cyber security strategies and policies
- Understand principles of web security and to guarantee a secure network by monitoring and analyzing the nature of attacks through cyber/computer forensics software/tools.

OUTCOME BASED LEARNING:

After successful completion of M.Voc. in Cyber Security degree, the graduates will be able to:

1. Understand the basic concepts of cyber security and digital forensics.
2. Analyze and evaluate the cyber security needs for current situation.
3. Conduct a cyber security risk assessment.
4. Measure the performance and troubleshoot cyber security systems.
5. Implement cyber security solutions.
6. Identify the key cyber security vendors in the marketplace.
7. Be able to use cyber security, information assurance, and cyber/computer forensics software/tools.
8. Design operational and strategic cyber security strategies and policies.
9. Design and develop security architecture for an institution/industry/organization.
10. Acquire professional and intellectual integrity, professional code of conduct; understand ethical practices and social responsibilities to contribute for the sustainable development of the society.

COURSE OUTCOME:

Upon successful completion of the programme, candidates will be familiar with cyber security landscapes and able to

a) Analyze and evaluate the cyber security needs of an organization.
b) Determine and analyze software vulnerabilities and security solutions to reduce the risk of exploitation.
c) Measure the performance and troubleshoot cyber security systems.

d) Implement cyber security solutions and use of cyber security, information assurance, and cyber/computer forensics software/tools.
e) Comprehend and execute risk management processes, risk treatment methods, and key risk and performance indicators
f) Design and develop a security architecture for an organization.
g) Design operational and strategic cyber security strategies and policies

SPECIFIC OBJECTIVES OF THE PROGRAMME:

1. Acquire in-depth knowledge with an ability to discriminate, evaluate, analyze and synthesize solutions for real time cyber security domain.
2. Apply knowledge to conduct research in a wider theoretical, practical and policy context.
3. Investigate security related issues, design and develop solutions considering public health and safety, societal and environmental factors.
4. Apply appropriate research methodologies and contribute for the improvement of security in science and technology.
5. Assimilate and use appropriate techniques and latest tools to solve complex cyber security problems.
6. Possess knowledge, recognize opportunities and contribute to collaborative and multidisciplinary cyber security research.
7. Recognize the need and engage in life-long learning with enthusiasm and commitment to update knowledge in cyber security domain.

COURSE SYLLABUS

M.Voc in Cyber Security [As per NSQF-UGC Scheme]

SEMESTER –I

Theory: Computer Network and Internet Security

Subject Code	**MVCS1.1**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Understand the principles and concepts on computer networks. Understand general-purpose computer networks.
- Master the computer network applications and Master the knowledge on designing and building a complete system.
- This course provides an in-depth study of various network attacks techniques and methods to defend against them. A number of threats and vulnerabilities of the Internet will be covered, including various vulnerabilities of TCP/IP protocols, denial of service (DOS), attacks on routing, attacks on DNS servers, TCP session hijacking, and so on.
- This course will also cover defending mechanisms, including intrusion detection, firewalls, tracing the source of attacks, anonymous communication, IPsec, virtual private network, and PKI. To make it easy for students to understand these attacks, basics of the TCP/IP protocols will also be covered in the course.

Module -1 15 Hours

Introduction to Data Communication: Components of Data Communication, Networks, Protocols and Standards, Network Models, Review of Reference Models: OSI, TCP/IP and their comparison. Data and signals, Channel Capacity, Inter connecting devices – Repeater, Hub, Switch, Bridge, Router, Gateway. Mobile and Wireless Devices, Simplified Reference Model, Need for Mobile Computing, Wireless Transmission, Multiplexing, Modulation, Spread Spectrum, Cellular Systems, Medium Access Control, Comparisons

Module -2 15 Hours

Mobile Network and Transport Layers: Mobile IP- Goals, Requirements, IP packet delivery, Advertisement and discovery. Registration, Tunneling and Encapsulation, Optimization, Reverse Tunneling, IPv6, Dynamic Host configuring protocol, Ad hoc networks - Routing, DSDV, Dynamic source routing. Traditional TCP, Classical TCP Improvements Indirect TCP, Wireless Application Protocol, World Wide Web. Overview of Wireless sensor networks, VPN, IOT and LiFi.

Module -3 15 Hours

TCP/IP Protocols, Vulnerabilities, Attacks, and Countermeasures

- Physical Layer: jamming attacks
- Data Link Layer: ARP protocol and ARP cache poisoning
- Network Layer: IP protocols, packet sniffering, IP Spoofing, IP fragmentation attacks
- Network Layer: ICMP protocol and ICMP misbehaviors
- Network Layer: IP Routing protocols and Attacks
- Transport Layer: TCP protocol, TCP session hijacking, reset and SYN flooding attacks
- DoS and DDoS attacks
- DNS protocol, attacks, and DNSSEC
- BGP protocol and Attacks

Module -4 15 Hours

- Cryptography Basics and Applications
  - Secret-Key Encryption, DES, AES
  - One-way Hash Functions, MD5, SHA-1, and SHA-2
  - Length extension attacks, Collision attacks
  - Diffie-Hellman Key Exchange
  - Public-Key Encryption, RSA
  - Digital Signatures
  - Public-Key Infrastructure (PKI)
  - Blockchains and Bitcoins
  - Case Studies: common mistakes
- Network Security Mechanisms
  - IP Tunneling and SSH Tunneling
  - Virtual Private Networks
  - Firewalls
  - Bypassing firewalls
  - Transport Layer Security (TLS/SSL)
  - TLS Programming

References:

- Behrouz A Forouzan, Data Communications and Networking, McGraw- Hill, 2006
- Introduction to Cryptography Principles and Applications By Hans Delfs, Helmut Knebl · 2007
- Jochen Schiller, “Mobile Communication”, Pearson Education, Delhi, 2000.•
- Brijendra Singh, Data Communication and Computer Networks, PHI, 2011.•
- Tanenbaum Andrew S., Computer Networks, TMH.

Theory: Programming in C

Subject Code	**MVCS1.2**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- A student will gain a thorough understanding of the fundamentals of C programming
- A student will be able to code, compile and test C programs.
- Be able to take up Systems programming or Advanced C programming course.
- After reading the text, the student is urged to solve the C quizzes

Module -1 15 Hours

Introduction, Compiling a simple C program, Data types and Constants

Module -2 15 Hours

Arithmetic expressions, Control of Flow , Arrays, Functions

Module -3 15 Hours

Structures and Unions, Strings, Pointers, Operation on Bits

Module -4 15 Hours

Input and output, File handling, C Preprocessor

Reference Books:

- The C Programming Language | Second Edition | By Pearson, by Brian W. Kernighan / Dennis Ritchi
- Programming in C, Kochan · 2005
- C Programming: Step By Step Beginner's To Experts Edition by Harry H. Chaudhary

Lab: Computer Network and Internet Security

Subject Code	**MVCS1.3**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- Learn basic concepts of computer networking and acquire practical notions of protocols with the emphasis on TCP/IP. A lab provides a practical approach to Ethernet/Internet networking: networks are assembled, and experiments are made to understand the layered architecture and how do some important protocols work.
- To understand the working principle of various communication protocols. To analyze the various routing algorithms.
- To know the concept of data transfer between nodes.
- analyzing the nature of attacks through cyber/computer forensics software/tools.

List of lab experiments will be as per respective theory's syllabus.

Lab: Programming in C

Subject Code	**MVCS1.4**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- To be familiar with syntax and structure of C-programming.
- To learn problem solving techniques using C
- Students will be able to develop logics which will help them to create programs, applications in C. Also by learning the basic programming constructs they can easily switch over to any other language in future.

List of lab experiments will be as per respective theory's syllabus.

Theory: Foundations of Cyber Security and Digital Forensics

Subject Code	**MVCS1.5**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Learn the cyber threat landscape, both in terms of recent emergent issues and those issues which recur over time.
- Learn the roles and influences of governments, commercial and other organisations, citizens and criminals in cyber security affairs.
- Understand general principles and strategies that can be applied to systems to make them more robust to attack.
- Understand key factors in cyber security from different disciplinary views including computer science, management, law, criminology, and social sciences.
- Notice issues surrounding privacy, anonymity and pervasive passive monitoring.
- To understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices.

Module -1 15 Hours

The cyber security threat landscape; history and evolution: Security surfaces; intelligence, case studies, trend analysis, Actors in cyber security; governments, organisations, citizens, criminals, The multidisciplinary nature of cyber security,ISPs as intermediaries; DPI.

Module -2 15 Hours

Cryptography: Principles of secure communications; digital signatures, PKI, encryption, hashing. Foundations cryptography; crypto-primitives and ciphers.

Privacy and anonymity protocols: Crowds, onion routing, ToR. Data management - anonymisation and de-anonymisation

Module -3 15 Hours

Access control; authentication techniques: Passwords and password analysis. Security assurance and evaluation. Introduction to biometrics.

Offensive cyber-attacks; cyber war; hacktivism: Advanced Persistent Threats. Critical infrastructures. Social engineering; phishing. Security aspects of social networks, the web science perspective

Module -4 15 Hours

Computer forensics fundamentals, Benefits of forensics, computer crimes, computer forensics evidence and courts, legal concerns and private issues.
Understanding Computing Investigations – Procedure for corporate High-Tech investigations, understanding data recovery work station and software, conducting and investigations.

References:

- Clarke, R.A., Cyber War (2012). The Next Threat to National Security and What to Do about it.
- The importance of taking a multi-disciplinary approach to cyber security
  By Warren G. Kruse II and Jay G. Heiser, "Computer Forensics: Incident Response Essentials", Addison Wesley, 2002.
- Graham, J.. Howard, R., Olson, R. (2011). Cyber Security Essentials.
- Stallings, W., Brown, L. (2018). Computer Security - Principles and Practice.
- Andress, J., Cyber Warfare (2013). Techniques, Tactics and Tools for Security Practitioners.

Theory: Cyber Laws and Indian IT Act

Subject Code	**MVCS1.6**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Understand and aware Cyber laws which are focusing on protecting the privacy of users from organizations and other users.
- In modern days, BitCoin frauds keep increasing and Cyber Laws have been focused to stop these kinds of frauds happening shortly, study and aware such developments.
- Understand research and development of issues and challenges faced in Cyberspace.
- Cyber Laws strive hard to let people know the cyber threats happening around them and to help them stay secure in the daily use of Cyberspace.

Module -1 15 Hours

Evolution of the IT Act, Genesis and Necessity. Salient features of the IT Act, 2000, various authorities under IT Act and their powers. ; Penalties & Offences, amendments. Impact on other related Acts (Amendments) :Amendments to Indian Penal Code. Amendments to Indian Evidence Act. Amendments to Bankers Book Evidence Act. Amendments to Reserve Bank of India Act.

Module -2 15 Hours

Cyber Space Jurisdiction : Jurisdiction issues under IT Act, 2000. Traditional principals of Jurisdiction, Extra-terrestrial Jurisdiction, Case Laws on Cyber Space Jurisdiction. E – commerce and Laws in India: Digital / Electronic Signature in Indian Laws, E – Commerce; Issues and provisions in Indian Law , E – Governance; concept and practicality in India. E – Taxation issues in Cyberspace, E – Contracts and its validity in India, Cyber Tribunal & Appellate Tribunal, Cyber Regulations Intellectual Property Rights.

Module -3 15 Hours

Domain Names and Trademark Disputes: Concept of Trademarks / in Internet Era, Cyber Squatting, Reverse Hijacking, Jurisdiction in Trademark Disputes Copyright in the Digital Medium , Copyright in Computer Programs , Copyright and WIPO Treaties Concept of Patent Right, Relevant Provisions of Patent Act 1970

Module -4 15 Hours

Sensitive Personal Data or Information (SPDI) in Cyber Law: SPDI Definition and Reasonable Security Practices in India, Reasonable Security Practices – International perspective. Cloud Computing & Law. Cyber Law : International Perspective: EDI: Concept and legal Issues. UNCITRAL Model Law.Electronic Signature Law's of Major Countries, Cryptography Laws, Cyber Law's of Major Countries, EU Convention on Cyber Crime

References:

- Cyber Law & Cyber Crimes By AdvocatPrashant Mali; Snow White publications, Mumbai
- Cyber Law in India by Farooq Ahmad; Pioneer Books
- Information Technology Law and Practice by Vakul Sharma; Universal Law Publishing Co. Pvt. Ltd.
- The Indian Cyber Law by Suresh T. Vishwanathan; Bharat Law House New Delhi
- Guide to Cyber and E – Commerce Laws by P.M. Bukshi and R.K. Suri; Bharat Law House, New Delhi

Theory: Python Programming for Cyber Security

Subject Code	**MVCS1.7**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Create applications using python programming.
- Write clear and effective python code.
- Able to apply the principles python programming.
- Python to write basic programs and high level applications using concepts such as Class, BIF of Python, *functions, variables, if else statements, for loops, while loops*, iterative and recursive programs and algorithms such as the Insertion Sort algorithm.
- This course will be of great interest to all learners who would like to gain a thorough knowledge and understanding of the basic components of computer programming using the Python language

Module -1 15 Hours

Introduction to Python and Computer Programming.Data Types, Variables, Basic Input-Output Operations, Basic Operators. Boolean Values, Conditional Execution, Loops, Lists and List Processing, Logical and Bitwise Operations.

Module -2 15 Hours

Functions, Tuples, Dictionaries, and Data Processing, String functions,

Module -3 15 Hours

File functions. Data Structures, Regular Expressions

Module -4 15 Hours

TCP Server and Client, UDP Server and Client, Retrieving hostname IP and Banner grabbing, Socket Server Framework, Scapy, Syn Flood attack with Scapy

References:

- Dive into Python, by Mike
- Learning Python, 4th Edition by Mark Lutz
- Programming Python, 4th Edition by Mark Lutz
- Wesley J. Chun, “Core Python Programming”, 2nd Edition, Pearson Education.
- Andrew S. Tanenbaum, “Computer Networks”, PHI, Fourth Edition, 2003
- Mark Summerfield, “Programming in Python”, Pearson Education.
- Behrouz A. Forouzan, “Data communication and Networking”, Tata McGraw-Hill, 2004.

Lab: Python Programming for Cyber Security

Subject Code	**MVCS1.8**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- To understand basic programs in Python
- To learn how to design and program Python applications.
- To learn how to use lists, tuples, and dictionaries in Python programs.
- To learn how to identify Python object types.
- To learn how to use indexing and slicing to access data in Python programs.
- To define the structure and components of a Python program.
- To learn how to write loops and decision statements in Python.
- To learn how to write functions and pass arguments in Python.
- To learn how to build and package Python modules for reusability.
- To learn how to read and write files, networking in Python.

List of lab experiments will be as per respective theory's syllabus.

Lab: Cyber Security and Digital Forensics

Subject Code	**MVCS1.9**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- The Cyber Security and Digital Forensics Laboratory simulate the environment of a professional digital forensics and cyber security programs.
- Cybercrime and forensic investigations are simulated in a safe, controlled environment.

List of lab experiments will be as per respective theory's syllabus.

SEMESTER –II

Theory: Ethical Hacking

Subject Code	**MVCS2.1**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Individuals and organizations have to adopt safe practices and usage of their IT infrastructure. Hence understanding the basics of ethical hacking is very much required.
- Starting from the basic topics like networking, network security and cryptography, students will understand various attacks and vulnerabilities and ways to secure them.
- The purpose of ethical hacking is to evaluate the security of and identify vulnerabilities in systems, networks or system infrastructure. It includes finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible.

Module -1 15 Hours

Introduction to ethical hacking. Fundamentals of computer networking. TCP/IP protocol stack. IP addressing and routing. Routing protocols. Introduction to network security. Information gathering: reconnaissance, scanning, etc.

Module -2 15 Hours

Vulnerability assessment: OpenVAS, Nessus, etc. System hacking: password cracking, penetration testing, etc. Social engineering attacks. Malware threats, penetration testing by creating backdoors. Introduction to cryptography, private-key encryption, public-key encryption.

Module -3 15 Hours

Key exchange protocols, cryptographic hash functions, applications. Steganography, biometric authentication, lightweight cryptographic algorithms. Sniffing: Wireshark, ARP poisoning, DNS poisoning. Hacking wireless networks, Denial of service attacks.

Module -4 15 Hours

Elements of hardware security: side-channel attacks, physical unclonable functions. Hacking web applications: vulnerability assessment, SQL injection, cross-site scripting. Case studies: various attacks scenarios and their remedies.

References:

- Certified Ethical Hacker (CEH) Version 10 Cert Guide,Third Edition, by Michael Gregg and Omar Santos
- Ethical Hacking-A Comprehensive Beginners Guide to Learn and Understand the Concept of Ethical Hacking By Joe Grant · 2019
- Ethical Hacking-A Beginners Guide to Learning the World of Ethical Hacking By Lakshay Eshan · 2018

Theory: Security of Operating System, Database and Infrastructure

Subject Code	**MVCS2.2**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Understand the roles of OS. The Operating system security is so important is that ultimately all of our software relies on proper behaviour of the underlying hardware.
- Safeguard computer operating systems by demonstrating server support skills and designing and implementing a security system. Identify security threats and monitor network security implementations.
- Database security refers to dedicated means used to protect data stored in databases or database management software from hacker attacks and insider-driven threats.
- It includes a multitude of processes, tools and strategies that ensure security of a database environment.
- Understand goals of Web Security and constraints that affect the confidentiality, integrity, and availability of your data and application.

Module -1 15 Hours

Introduction to OS: Architecture, Applications, types,services, processes, scheduling algorithms.

Module -2 15 Hours

Threading, Memory Management, File System. Authentication, One Time passwords, Program Threats, System Threats, Computer Security Classifications

Module -3 15 Hours

Database Management Systems: Introduction to Relational Data Model, Distributed Databases, Database Security Overview: General security issues, Security policies, Identity management, Integrity and availability,SOA and Cloud data management, Secure stream data management.

Module -4 15 Hours

Web Security Web Security Considerations, User Authentication and Session Management, Cookies, SSL, HTTPS, SSH, Privacy on Web, Web Browser Attacks, Account Harvesting, Web Bugs, Clickjacking, CrossSite Request Forgery, Session Hijacking and Management, Phishing and Pharming Techniques, DNS Attacks, Web Service Security, Secure Electronic Transaction, Email Attacks, Web Server Security as per OWASP, Firewalls, Penetration Testing 12 CO4, CO5

References:

- Guide to Operating Systems Security, Michael Palmer, THOMPSON/Course Technology. ISBN: 0-619-16040-3 © 2004

- T. Ozsu and P. Valduriez, Principles of Distributed Database Systems, Springer; 3rd Edition. edition (March 2, 2011), ISBN-10: 1441988335
- Computer Security Principles and Practice, William Stallings, Sixth Edition, Pearson Education
- Security in Computing, Charles P. Pfleeger, Fifth Edition, Pearson Education
- Network Security and Cryptography, Bernard Menezes, Cengage Learning
- Network Security Bible, Eric Cole, Second Edition, Wiley

Lab: Ethical Hacking

Subject Code	**MVCS2.3**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- Understand the awareness towards increased education and ethics in information security through a series of cyber competitions that encompass forensics, cryptography, reverse-engineering, ethical hacking and defense.
- Develop a professional designation for hackers that perform legitimate services for IT companies/firms.
- Exploit networks like an attacker and discover how protect the system from them. Determine the type of attack used and pinpoint exploit code in network traffic.

List of lab experiments will be as per respective theory's syllabus.

Lab: Security of Operating System, Database and Infrastructure

Subject Code	**MVCS2.4**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- The goal of this course is to have students understand and appreciate the principles in the design and implementation of operating systems software
- To provide necessary skills for developing and debugging programs in OS/DBMS/Web environment.

List of lab experiments will be as per respective theory's syllabus.

Theory: Cyber Security with Cloud Computing

Subject Code	**MVCS2.5**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Fundamentals of cloud computing architectures based on current standards, protocols, and best practices intended for delivering Cloud based enterprise IT services and business applications.
- Identify the known threats, risks, vulnerabilities and privacy issues associated with Cloud based IT services.
- Understand the concepts and guiding principles for designing and implementing appropriate safeguards and countermeasures for Cloud based IT services.
- Approaches to designing cloud services that meets essential Cloud infrastructure characteristics – on-demand computing, shared resources, elasticity and measuring usage.

Module -1 15 Hours

Fundamentals of Cloud Computing and Architectural Characteristics: Understand what is Cloud computing, Architectural and Technological Influences of Cloud Computing, Understand the Cloud deployment models:Public, Private, Community and Hybrid models, Scope of Control, Software as a Service (SaaS),Platform as a Service (PaaS), Infrastructure as a Service (IaaS),Cloud Computing Roles, Risks and Security Concerns. Key Cyber-security Threats to Cloud Computing: Crytopjacking, Data breaches, Denial of service, Insider threats, Hijacking accounts, Insecure applications, Inadequate training.

Module -2 15 Hours

Security Design and Architecture for Cloud Computing: Guiding Security design principles for Cloud Computing, Cloud Security, Secure Isolation, Comprehensive data protection, End-to-end access control, Monitoring and auditing, Quick look at CSA, NIST and ENISA guidelines for Cloud Security, Common attack vectors and threats.

Module -3 15 Hours

Secure Isolation of Physical & Logical Infrastructure: Isolation: Compute, Network and Storage, Common attack vectors and threats, Secure Isolation Strategies. Multitenancy, Virtualization strategies, Inter-tenant network segmentation strategies, Storage isolation strategies.

Module -4 15 Hours

Data Protection for Cloud Infrastructure and Services: Understand the Cloud based Information Life Cycle, Data protection for Confidentiality and Integrity, Common attack vectors and threats, Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key, Management, Assuring data deletion, Data retention, deletion and archiving procedures for tenant data, Data Protection Strategies.

References:

- Securing The Cloud: Cloud Computing Security Techniques and Tactics by Vic (J.R.) Winkler (Syngress/Elsevier) - 978-1-59749-592-9
- Cloud Computing Design Patterns by Thomas Erl (Prentice Hall) - 978-0133858563

Theory: Application Threat Detection

Subject Code	**MVCS2.6**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- To understand about the intruders.
- To know the intrusion detection and prevention policies
- Security Goals, Threat Models

Module -1 15 Hours

INTRODUCTION: Understanding Intrusion Detection – Intrusion detection and prevention basics – IDS and IPS analysis schemes, Attacks, Detection approaches – Misuse detection – anamoly detection – specification based detection – hybrid detection THEORETICAL FOUNDATIONS OF DETECTION: Taxonomy of anomaly detection system – fuzzy logic – Bayes theory – Artificial Neural networks – Support vector machine – Evolutionary computation – Association rules – Clustering

Module -2 15 Hours

ARCHITECTURE AND IMPLEMENTATION: Centralized – Distributed – Cooperative Intrusion Detection – Tiered architecture

Module -3 15 Hours

JUSTIFYING INTRUSION DETECTION: Intrusion detection in security – Threat Briefing –Quantifying risk – Return on Investment (ROI)

Module -4 15 Hours

APPLICATIONS AND TOOLS: Tool Selection and Acquisition Process – Bro Intrusion Detection – Prelude Intrusion Detection – Cisco Security IDS – Snorts Intrusion Detection – NFR security

References:

- Ali A. Ghorbani, Wei Lu, “Network Intrusion Detection and Prevention: Concepts and Techniques”, Springer, 2010.
- Carl Enrolf, Eugene Schultz, Jim Mellander, “Intrusion detection and Prevention”, McGraw Hill, 2004
- Paul E. Proctor, “The Practical Intrusion Detection Handbook “,Prentice Hall , 2001.
- Ankit Fadia and Mnu Zacharia, “Intrusiion Alert”, Vikas Publishing house Pvt., Ltd, 2007.
- Earl Carter, Jonathan Hogue, “Intrusion Prevention Fundamentals”, Pearson Education, 2006.

Theory: Cyber Threat and Modelling

Subject Code	**MVCS2.7**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Threat modelling intends to equip defenders and the security team and reporting, which is the overall objective of a threat intelligence program.
- Threat modelling is a method of optimizing network security by locating vulnerabilities, identifying objectives, and developing countermeasures.

Module -1 15 Hours

Dive In and Threat Model, Learning to Threat Model. Strategies for Threat Modelling, Brainstorming Your Threats, Structured Approaches to Threat Modelling, Models of Software.

Module -2 15 Hours

Finding Threats, STRIDE, Spoofing Threats, Tampering Threats, Repudiation Threats, Information Disclosure Threats, Denial-of-Service Threats. Attack Trees, Working with Attack Trees, Representing a Tree, Real Attack Trees. Attack Libraries, Properties of Attack Libraries.

Module -3 15 Hours

Managing and Addressing Threats, Processing and Managing Threats, Starting the Threat Modelling Project, Digging Deeper into Mitigations, Tracking with Tables and Lists, Scenario-Specific Elements of Threat Modelling. Defensive Tactics and Technologies, Tactics and Technologies for Mitigating Threats, Addressing Threats with Patterns, Mitigating Privacy Threats.

Module -4 15 Hours

Threat Modelling Tools, Generally Useful Tools, Open-Source Tools, Commercial Tools. Web and Cloud Threats, Web Threats, Cloud Tenant Threats, Cloud Provider Threats, Mobile Threats.

References:

- Threat Modeling: Designing for Security, Adam Shostack · 2014
- Computer and Cyber Security: Principles, Algorithm,by Brij B. Gupta,2018
- Adam Shostack, "Threat Modelling: Designing for Security Designing for Security" Wiley publication, Edition, 2008.
- Frank Swiderski, Window Snyder "Threat Modelling (Microsoft Professional)" Microsoft Press, Edition, 2008.

Theory: Career Paths in Cyber Security and Digital Forensics

Subject Code	**MVCS2.8**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Understand the career path of cyber security.
- Understand roles and responsibilities of cyber security engineers.
- Future path and trainings and industries.

Module -1 15 Hours

Working in the Cyber security Industry or related companies. Cyber security Job Types, Types of Roles and responsibilities.

Module -2 15 Hours

Cyber Security Engineer Qualifications, Creative ideas for carrier, salary etc

Module -3 15 Hours

How to become a computer forensics investigator: 5 steps to follow when pursue a career in computer forensics: Plan, educate, certify, apply and keep learning. Outlook for computer forensic investigators. What Does a Computer Forensics Analyst Do? Computer Forensics Analyst Main Responsibilities: Securing Devices and/or Systems, Using Specialized Forensics Software, Identifying and Following Data, Writing Reports and Presenting Findings, Analysts need to create written reports of their findings, Upgrading Skills.

Module -4 15 Hours

Forensics Industry/organizations or related companies. Digital Forensics Professional Positions, Duties, and Common Tasks, Forensics. Investigators Training. Forensics Job Types, Types of Roles and responsibilities. Forensics Qualifications, Creative ideas for carrier, salary etc.

References:

- Breaking Into Information Security-Crafting a Custom Career Path to Get the Job You Really Want By Josh More, Anthony J. Stieber, Chris Liu · 2015
- Certified Ethical Hacker (CEH) Foundation Guide By Sagar Ajay Rahalkar · 2016
- Careers in Computer Forensics by Terry Teague Meyer · 2013
- Learn Computer Forensics: A beginner's guide to searching by William Oettinger · 2020

Lab: Cyber Security with Cloud Computing

Subject Code	**MVCS2.9**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- Develop programs under current standards, protocols, and best practices intended for delivering Cloud based enterprise IT services and business applications.
- Pragmatically test threats, risks, vulnerabilities and privacy issues associated with Cloud based IT services.

List of lab experiments will be as per respective theory's syllabus.

Lab: Cyber Threat and Modelling

Subject Code	**MVCS2.10**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- Develop programs for cyber reporting, which is the overall objective of a threat intelligence program.
- Develop optimizing network security programs by locating vulnerabilities, identifying objectives, and developing countermeasures.

List of lab experiments will be as per respective theory's syllabus.

SEMESTER –III

Theory: Data Analysis using R

Subject Code	**MVCS3.1**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Explore and understand how to use the R documentation.
- Read Structured Data into R from various sources. Understand the different data types in R.
- Understand the different data structures in R.
- Learn programs to handle all aspects of data analysis.
- Use R for statistics, security analysis but also for data science.

Module -1 15 Hours

Introduction to R, Features of R, Installation of R. Getting Started, Variables in R, Input of Data, Output in R, In-Built Functions in R, Packages in R.

Module -2 15 Hours

Data Types of R, Vectors, Matrices, Arrays, Lists, Factors, Data Frame.

Module -3 15 Hours

Programming in R, Decision-Making Structures, Loops, User-Defined Functions, User-Defined Package, Reports using R markdown .

Module -4 15 Hours

Data Exploration and Manipulation, Missing Data Management, Data Reshaping through Melting and Casting, Special Functions across Data Elements.

References:

- Willy Publication ,Data analysis with R By Dr. Bharti Motwani.
- Data Analysis with R, Tony Fischetti · 2015

Theory: Application and System Security

Subject Code	**MVCS3.2**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Understand the role of IT Physical Security in transactions
- Describe social networking and evaluate associated risks
- Evaluate web application security vulnerabilities
- Identify IT Physical Security controls and risk mitigation techniques
- Develop a security strategy and solution for securing web based applications
- Assess web application security compliance requirements and objectives.
- Assess Endpoint Device Security

Module -1 15 Hours

Application Security, Authentication & Authorization. Input Validation - Buffer overflow; cross-site scripting; SQL injection; canonicalization, Sensitive information Access sensitive data in storage; network eavesdropping; data tampering. Network eaves dropping; Brute force attack; dictionary attacks; cookie replay; credential theft. Elevation of privilege; disclosure of confidential data; data tampering; luring attacks; Phishing

Module -2 15 Hours

Configuration management & Session management. Unauthorized access to administration interfaces; unauthorized access to configuration. stores; retrieval of clear text configuration data; lack of individual accountability; over privileged process and service accounts. Hijacking; session replay; man in the middle.

Module -3 15 Hours

Auditing and logging, Countermeasures. Auditing and logging User denies performing an operation. Attacker exploits an application without trace; attacker covers his or her tracks, Counter measures.

Module -4 15 Hours

Implement and Operate Endpoint Device Security: Module Topics: Host-Based Intrusion Detection Systems (HIDS), Host-Based Firewalls, Application White listing, Endpoint Encryption, Trusted Platform Module (TPM), Mobile Device Management (MDM), Secure Browsing. In Host-Based Intrusion Detection Systems (HIDS), you will learn about Advantages and Disadvantages of HIDS. In Application White listing, you will learn about software Restriction Policies (SRP), Trusted Platform Module (TPM). In Mobile Device Management (MDM), you will learn about Bring your Own Device (BYOD), Security, BYOD Policy Considerations, BYOD Policy Considerations, Corporate Owned, Personally Enabled (COPE), and Secure Browsing.

References:

- IT Application security (IBM ICE Publication)

Lab: Data Analysis using R

Subject Code	**MVCS3.3**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- Open RStudio. Identify the Console, Script, Environment, and Plots pane.
- Load a script file, run lines from it, edit and save the script file. Set a working directory.
- Load a Workspace containing an R data frame, edit the dataset, and save the Workspace.
- Install an R 'package'; import data from .csv (comma separated value) file format and .xlsx
- (Excel) file format.
- Type your own R code to use the API (application programming interface)
- Create a 'GapMinder' style plot.
- Create univariate visualizations with two different R packages.
- Identify books, websites, and additional sources for further learning and help.

List of lab experiments will be as per respective theory's syllabus.

Lab: Application and System Security

Subject Code	**MVCS3.4**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- Become familiar with how to operate the user account. Different types of user accounts and their options. How to protect your system with password.
- Generate secure passwords. Apply password manager to generate secure password. Point out various features of different password managers
- Know how to hack a simple or a strong password. Know the different types of hacking process and type of applications.

List of lab experiments will be as per respective theory's syllabus.

Theory: Cryptography and Information Security

Subject Code	**MVCS3.5**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- The objective of the course is to provide a basic understanding of the various issues related to information systems security (E-security).
- The course will present an overview of the risks encountered in information systems security, and the tools used for resolving these risks.

Module -1 15 Hours

Overview of e-security: Threats, risks, consequences. Sources of threats. Attacks classification. Preventive measures, remedial measures. Cryptography for e-security: Historical perspective, Confusion vs. diffusion, Stream ciphers vs. block ciphers, Keys and key management, Key exchange (peer to peer, peer – key server - peer), Diffie Helman key sharing scheme, Symmetric key cryptography vs asymmetric key cryptography, Trapdoor functions.

Module -2 15 Hours

Hash digests: Properties of cryptographic hash functions, Merkle Damgard construction, md family, sha family, Digital signatures,sha3. GPG: Overview of GPG, Commands and CLI,GPG trust model, GUI – KGPG, Seahorse, Frontends – Kleopatra, enigmail.

Module -3 15 Hours

Block ciphers: Block cipher principles, Feistel networks boxes and P boxes, Block cipher modes of operation, DES,3DES, AES. Elementary number thoery: Prime numbers, Factoring. Modular arithmetic, Fermat's & Euler's theorems, gcd, Euclid's algorithm, Discrete logarithm problem.

Module -4 15 Hours

Public key encryption: Public key crypto systems, RSA algorithm, Elliptic Curve cryptography.

References:

- William Stallings, Cryptography and network security, Pearson Education.
- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone , Handbook of Applied Cryptography, CRC Press.
- Margaret Cozzens, Steven J Miller, The mathematics of encryption,American Mathematical Society
- Bruce Schneier Applied Cryptography, John Wiley and Sons
- Mark Stamp, Information Security: Principles and Practice, John Wiley and Sons
- Matt Bishop, Computer Security, Art and Science, Pearson Education

Theory: Security Policy and Audit

Subject Code	**MVCS3.6**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- The Security Policy is intended to define what is expected from an organization with respect to security of Information Systems.
- Understand information security policies underpin the security and well being of information resources.
- The overall objective is to control or guide human behaviour in an attempt to reduce the risk to information assets by accidental or deliberate actions.

Module -1 15 Hours

Introduction to Information Security: History and evaluation of Information security CIA triangle Components of IS, Control in IT environment, Information security Management system, components of ISMS and conceptual framework Steps for developing ISMS.

Module -2 15 Hours

Need of Information security: Threats to information security, Risk to Information systems Information security in organization, Introduction to cybercrimes and attacks Information security policy, policy definition and security life cycle.

Module -3 15 Hours

Domains of IT security- User/accepted usage/ access, data access, physical access Internet access, e-mail, digital signature, outsourcing, software development and acquisition, hardware acquisition Network and telecom, BCP and DRP, security organization structure. Domains related security based case studies.

Module -4 15 Hours

Auditing: Auditing concepts ISA need, concept, standards, performance, steps, Techniques, methodologies, around and through computer, Controls – Concept objectives, types, risk

References:

- Information Security And Audit By Prof. Yogesh Ghorpade Prof. Rajesh More, Self Publication

Theory: IoT and Digital Forensics

Subject Code	**MVCS3.7**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Understand the impact of IoT technologies , Be able to draw the big picture of IoT ecosystem , Be able to identify the architecture of IoT systems
- Be able to describe the essential components of IoT, Have the knowledge of the emerging technologies of IoT, Be able to examine the security and privacy challenges of IoT , Be able to find appropriate security/privacy solutions for IoT , Have hands-on experience on IoT and security projects.

Module -1 15 Hours

IoT definition, advantages, and impact (Introduction of IoT devices and discussion on the difference among IoT devices, computers, and embedded devices. How will IoT possibly change our lives?).Sensors and actuators in IoT (accelerometer, photoresistor, buttons, motor, LED, vibrator, analog signal vs. digital signal).

Module -2 15 Hours

Iot forensics curriculum: is it a myth or reality? Iot forensics tools in the market and priv a'ie sector's opinions. Iot forensics ecosys'iem. Iot forensics challenges and activities of the research lab.

Module -3 15 Hours

IoT Ignorance is Digital Forensics Research Bliss: A Survey to Understand IoT Forensics Definitions, Challenges and Future Research Directions. IoT Forensic Frameworks, IoT Forensic Challenges. IoT Forensic Investigations. Evidence on IoT Devices. Responses from participants' interpretation of IoT forensics

Module -4 15 Hours

IoT Forensics: Challenges For The IoA Era: forensic evidence handling. The changing landscape of crime. Internet of anything (ioa)

References:

- IoT Ignorance is Digital Forensics Research Bliss: A Survey to Understand IoT Forensics Definitions, Challenges and Future Research Directions by Tina Wu, et al, University of New Haven Digital Commons @ New Haven Electrical & Computer Engineering and Computer Science Faculty Publications Electrical & Computer Engineering and Computer Science, 8-2019.
- Computer Security: Principles and Practice, ISBN 0-13-377392-2.
- Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, by FrancisdaCosta, ISBN: 978-1-4302-5740-0, 2013
- Architecting the Internet of Things, by Dieter Uckelmann, Mark Harrison and Florian Michahelles,ISBN: 978-3-642-19157-2, 2011
- Internet of Things: Privacy & Security in a Connected World, Federal Trade Comission, 2015
- Security and the IoT ecosystem, KPMG International, 2015
- "Internet of Things: IoT Governance, Privacy and Security Issues" by European Research Cluster Network Security Essentials, Prentice Hall, 5th Ed., ISBN-10:013337043, ISBN-13:8-0133370430.
- Bulletproof Android: Practical Advice for Building Secure Apps, ISBN-10:0133993329
- Relevant recent research journal articles and conference papers.

Lab: Cryptography and Information Security

Subject Code	**MVCS3.8**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- Creation of key pairs using GPG
- Encryption, decryption, signing, verification using GPG
- Key signing party. Creation of a web of trust
- Computation of hash digests (md5, sha1)
- Building a fortress
- Encryption of a whole drive/partition

List of lab experiments will be as per respective theory's syllabus.

Lab: Minor Project

Subject Code	**MVCS3.9**	IA Marks :	20
Number of Lecture Hours/Week	04	Exam Marks :	80
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- EVALUATION PROCEDURE:
- Preliminary stage of the Project work must be carried out by each student individually.
- Project proposals submitted and presentation made by the candidate are evaluated by a committee consisting of project advisors or at least two senior faculty members.
- i. Synopsys must be submitted immediately after the1st week of the semester.
- ii. Periodically Project Progress report must be submitted to Advisor/Guide.
- iii. Critically looks into the relevance of problem area, coverage, Depth of understanding, clarity of the basic principles involved, and the presentation style.
- iv. Critically look into the completion/achievements made, clarity of the underlying principles, depth of understanding, presentation style and quality of the draft project report (organization, content grammar).
- v. Before the commencement of final examination the draft report must be submitted, followed by the presentation.

  FINAL EVALUATION

- The examination is conducted as per University Norms.

List of lab experiments will be as per respective theory's syllabus.

SEMESTER –IV

Theory: Recent Cyber-Security Breaches and Attacks

Subject Code	**MVCS4.1**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Understand Major breaches
- Understand Major attacks
- Technical tools and side effects.

Module -1 15 Hours

Cyber-Security Breaches in latest news: Major breaches across globe/India.

Module -2 15 Hours

Cyber-Security attacks in latest news: Major attacks across globe/India.

Module -3 15 Hours

Understanding recent Cyber-Security tools/techniques/coding used for attacks.

Module -4 15 Hours

Side effects of recent Cyber-Security Breaches and Attacks: Financial losses, Service Interruption, national security threats, theft, sensitive data leak, political triggers, legal issues, etc. Best practices to avoid Cyber-Security Breaches and Attacks.

References:

- The New Era of Cybersecurity Breaches: A Case Study by Graeme Payne · 2019
- Data Security Breaches and Privacy in Europe by Rebecca Wong · 2013
- Investigating the Cyber Breach: The Digital Forensics Guide by Joseph Muniz, Aamir Lakhani · 2018
- Managing Information Security Breaches: Studies from real life by Michael Krausz · 2015
- Cybersecurity Attacks – Red Team Strategies by Johann Rehberger · 2020

Theory: Fundamentals of Information Assurance/Security

Subject Code	**MVCS4.2**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Develop a fundamental understanding of the information security profession, enterprise physical security, cryptography, application development security, enterprise incidence response, enterprise business continuity, disaster recovery planning, cyber resiliency, enterprise risk management and governance.
- Understand new trends that are transforming enterprise information security and assurance related to cloud computing and mobile applications, Bring Your Own Device (BYOD) strategies, and current, increasingly rigorous security and information assurance compliance requirements.

Module -1 15 Hours

Introduction: Why Study Information Security? Information Security Principles of Success, Certification Programs and the Common Body of Knowledge, Governance and Risk Management.

Module -2 15 Hours

Security Architecture and Design, Business Continuity Planning and Disaster Recovery, Planning, Law and Investigations and Ethics.

Module -3 15 Hours

Physical Security Control, Operations Security, Access Control Systems and Methodology, Cryptography.

Module -4 15 Hours

Telecommunications, Network, and Internet Security. Software Development Security. Securing the Future.

References:

- Information Security: Principles and Practices, 2nd Edition, Mark S. Merkow, Jim Breithaupt, June 2014, Paperback: 324 pages; Publisher Pearson Education ISBN-13: 978-0-7897-5325-0
- Certified Ethical Hacker (CEH), Cert Guide, Michael Gregg, May 2014, Hardcover 677 pages; Publisher Pearson Education ISBN-13: 978-0-7897-5127-0
- Information Assurance by Yi Qian David Tipper Prashant Krishnamurthy James Joshi, Elsevier 1st Edition.

Lab: Cyber Security Case Studies

Subject Code	**MVCS4.3**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- Research and analyze cyber security incidents.
- Conduct search of high profile cyberattacks. Using search engine conduct a search for each of the major cyberattacks.
- Note: You can use the web browser in virtual machine installed in a previous lab to research the hack. By using the virtual machine, you may prevent malware from being installed on your computer.
- Read the articles found from your search-in and be prepared to discuss and share your research on the who, what, when, where, and why of each attack.
- Write an analysis of a cyberattack.
- Select one of the high-profile cyberattacks from above exercises and write an analysis of the attack that includes answers to the questions below.

  a. Who were the victims of the attacks? Answers will vary based on the cyberattack chosen.

  b. What technologies and tools were used in the attack? The answers will vary based on the cyberattack chosen.

  c. When did the attack happen within the network? The answers will vary based on the cyberattack chosen.

  d. What systems were targeted? The answers will vary based on the cyberattack chosen.

  e. What was the motivation of the attackers in this case? What did they hope to achieve? The answers will vary based on the cyberattack chosen.

  f. What was the outcome of the attack? (stolen data, ransom, system damage, etc.) The answers will vary based on the cyberattack chosen.

List of lab experiments will be as per respective theory's syllabus.

Lab: Information Assurance/Security

Subject Code	**MVCS4.4**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- Experiments programs can include leading practices for information security and assurance governance and risk management; network architecture and design of systems to maximize assurance; business continuity, disaster recovery planning, resiliency; data privacy risks and laws; understanding legal, investigation, information-security incident response and management processes; and developing secure application software.

List of lab experiments will be as per respective theory's syllabus.

Theory: Artificial Intelligence for Cyber Security

Subject Code	**MVCS4.5**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- In the face of this changing landscape, there is significant concern and interest among policymakers, security practitioners, technologists, researchers, and the public about the potential implications of AI and ML for cybersecurity.
- The course will address key AI technologies including machine learning and natural language processing in an attempt to help in understanding their role in cyber security and the implications of these new technologies to the world of politics. AI deficiently will complement and strengthen the cyber security practices and will improve their applications in enhancing our security.

Module -1 15 Hours

How is AI transforming cyber-security for good? How is AI transforming cyber-security for bad? Deployment of ML/AI to detect specific cyber-security problems. Deployment of engineered attacks on machine learning models.

Module -2 15 Hours

Cyber-attacks on water treatment facilities. Engineered attacks on water distribution systems. Engineered attacks on image recognition capability of autonomous vehicles.

Module -3 15 Hours

Engineered attacks on driving operational parameters (via manipulation of datasets). Currently Deployed Artificial Intelligence and Machine Learning Tools for Cyber Defense Operations.

Module -4 15 Hours

Adversarial Artificial Intelligence for Cybersecurity: Research and Development and Emerging Areas. Security Risks of Artificial Intelligence-Enabled Systems. Deep Fakes. The Future of AI in Advancing Cyber Security. Tools/Software used: Python, Jupyter Notebook, Scikit-Learn, Keras, TensorFlow.

References:

- National Academies of Sciences, Engineering, and Medicine. 2019. Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop. Washington, DC: The National Academies Press. https://doi.org/10.17226/25488.
- Cyber Security Intelligence and Analytics by Zheng Xu, Reza M. Parizi, Mohammad Hammoudeh · 2020.
- Malware Data Science: Attack Detection and Attribution, Joshua Saxe, Hillary Sanders · 2018
- Machine Learning and Data Mining for Computer Security Methods and Applications, ISBN:9781846282539, 1846282535, by Marcus A. Maloof

Theory: Risk Management and Malware Analysis

Subject Code	**MVCS4.6**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- To understand and development of concepts required for risk-based planning and risk management of computer and information systems.
- Know how to safely handle malware and potentially malicious files encountered during an engagement.

Module -1 15 Hours

An Introduction to Risk Management: Introduction to the Theories of Risk Management; The Changing Environment; The Art of Managing Risks. The Threat Assessment Process: Threat Assessment and its Input to Risk Assessment; Threat Assessment Method; Example Threat Assessment;

Module -2 15 Hours

The Risk Process: What is Risk Assessment? Risk Analysis; Who is Responsible? Tools and Types of Risk Assessment: Qualitative and Quantitative risk Assessment; Policies, Procedures, Plans, and Processes of Risk Management; Tools and Techniques; Integrated Risk Management; Future Directions: The Future of the Risk Management.

Module -3 15 Hours

Malware Introduction: The cyber kill chain, Definition of malware and its role in the kill chain, Different types of malware, The goal of malware analysis, Types of malware analysis, Setting up a safe environment for malware analysis. Analyzing malicious Windows programs:The Portable Executable file format, PE header and sections, The Windows loader, Windows API, Import Address Table, Import functions, Export functions. System architecture, processes, threads, memory management, registry. PE files on disk and in memory.

Module -4 15 Hours

Analysis of malicious documents:mFile formats: OLE2, OOXML, RTF and PDF. Malicious macro. Document exploits, e.g. exploit example for Equation editor vulnerability (CVE-2017-11882). Introduction to oletools. Defeat malware: Examples of how to use the information we got during malware analysis to defend against malware attacks. Threat Intelligence, IOCs. Security solutions. Open source tools: Yara, Snort/Suricata.

References:

- Malcolm Harkins, Managing Risk and Information Security, Apress, 2012.
- Daniel Minoli, Information Technology Risk Management in Enterprise Environments, Wiley, 2009.
- Michael Sikorski and Andrew Honig: Practical Malware Analysis, The Hands-On Guide to Dissecting Malicious Software. No Starch Press. ISBN: 978-1-593-27290-6

- Monnappa K A: Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware. Packt Publishing. ISBN: 978-1788392501
- Michael Hale Ligh, Steven Adair, Blake Hartstein and Matthew Richard: Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Wiley. ISBN: 978-0-470-61303-0

Theory: Mobile and Wireless Security

Subject Code	**MVCS4.7**	IA Marks :	30
Number of Lecture Hours/Week	04	Exam Marks :	70
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

- Mobile devices today have outnumbered computers worldwide. Since mobile devices, such as smart phones provide convenient anytime anywhere access to the Internet and the ability to make phone calls, run apps centered around our lives, they have become enticing targets for cyber criminals. This course is designed to address this growing threat to mobile devices, networks and services delivered over the mobile infrastructure.
- This course covers methods and techniques to secure wireless networks against threats and attacks.

Module -1 15 Hours

Introduction to Mobile Security. Building Blocks – Basic security and cryptographic techniques. Security of GSM Networks. Security of UMTS Networks. LTE Security. SIM/UICC Security. Mobile Malware and App Security.

Module -2 15 Hours

Android Security Model. IOS Security Model. SMS/MMS, Mobile Geolocation and Mobile Web Security. Security of Mobile VoIP Communications. Emerging Trends in Mobile Security.

Module -3 15 Hours

Review of Network Security: from Crypto to Security Protocols. Fundamentals of Wireless & Mobile Systems: key features and mechanisms of wireless and mobile systems. Security Standards in current Wireless & Mobile Systems: WiFi Security (WEP, WPA, WPA-Enterprise); Cellular Security (GSM, 3G, LTE); Internet of Things / Wireless Sensor Networks / RFID. Emerging Privacy concerns: location, tracking, traffic analysis, mobile and the cloud.

Module -4 15 Hours

Wireless and Mobile as a Cyber Physical Infrastructure (CPS). Denial of Service Attacks Cellular, WiFi, GPS Implications to CPS: e.g., Electricity grid, Internet of Things. WiFi and Bluetooth Security.

References:

- Mobile Application Security, Himanshu Dviwedi, Chris Clark and David
- Security of Mobile Communications, Noureddine Boudriga, 2009
- Mobile Security For Dummies, Palo Alto Networks Edition
- Wireless Network Security, Yang Xiao, Xuemin Shen, Ding-Zhu Du · 2007
- Wireless Security and Cryptography by Nicolas Sklavos, Xinmiao Zhang · 2017
- Wireless and Mobile Network Security Security Basics, Security in On-the-shelf and Emerging Technologies Edited by Hakima Chaouchi Maryline Laurent-Maknavicius

Lab: Mobile and Wireless Security

Subject Code	**MVCS4.8**	IA Marks :	10
Number of Lecture Hours/Week	04	Exam Marks :	40
Total Number of Lecture Hours	30	Exam Hours :	03

Objectives:

- Conduct relevant lab exercises and carry out related programs/project work.
- To support research activity in the area of mobile/wireless communications.
- To develop killer-applications of interest to the organizations/industry or academia.

List of lab experiments will be as per respective theory's syllabus.

Lab: Major Project

Subject Code	**MVCS4.9**	IA Marks :	20
Number of Lecture Hours/Week	04	Exam Marks :	80
Total Number of Lecture Hours	60	Exam Hours :	03

Objectives:

EVALUATION PROCEDURE:

- Preliminary stage of the Project work must be carried out by each student individually in the previous semester.
- Project proposals submitted and presentation made by the candidate are evaluated by a committee consisting of project advisors or at least two senior faculty members, it has to be approved in the previous semester.

i. Synopsys must be submitted immediately after the 1st week of the previous semester and should be approved.

ii. Periodically Project Progress report must be submitted to Advisor/Guide.

iii. Critically looks into the relevance of problem area, coverage, Depth of understanding, clarity of the basic principles involved, and the presentation style.

iv. Critically look into the completion/achievements made, clarity of the underlying principles, depth of understanding, presentation style and quality of the draft project report (organization, content grammar).

v. Before the commencement of final examination the draft report must be submitted, followed by the presentation.

FINAL EVALUATION

- The examination is conducted as per University Norms.

List of lab experiments will be as per respective theory's syllabus.