MSc Computer Engineering Specialization in Network and Cyber Security (MSNCS)

Institute of Engineering, Pulchowk Campus
Tribhuvan University

Course Curriculum Details

Year: 1st **Part: 2nd**

Semester: I

S. No.	Teaching Schedule			Examination Schedule			Total	Remarks
	Course Code	Course Title	Credit	Assessment Marks	Final			
					Duration Hours	Marks		
1	CT	Next Generation Network Technologies	4	40	3	60	100	
2	CT	Cryptography and Data Security	4	40	3	60	100	
3	CT	Machine Learning and Data Analytics	4	40	3	60	100	
4	CT	Research Methods	4	40	3	60	100	
Total			**16**	**160**		**240**	**400**	

Next Generation Network Technologies (ENCTNS501) Credits: 4

Level : M. Sc. Year : I

Program: MSNCS Part : I

Course Objective:

- Understand the principles and architectures of Next Generation Networking Technologies.
- Gain proficiency in the implementation and deployment of SDN and NFV solutions.
- Explore the role of IoT, 5G, and edge computing in modern networking.
- Analyze challenges and opportunities in securing next-generation networks.
- Evaluate emerging trends and technologies shaping the future of networking.

Learning Outcomes	Chapter Contents	Credit hours	Teaching Methods
• Understand the evolution and drivers of modern networking technologies. • Explain OSI and TCP/IP reference models and their relevance. • Identify key network governance bodies and their roles (IETF, IANA, ITU, ICANN).	**1 Introduction to Latest Networking Technologies** 1.1 Latest networking technology evolution 1.2 Drivers of latest networking technologies 1.3 OSI and TCP/IP reference model 1.4 Network and Internet Governing bodies: IETF, IANA, ITU, ICANN	6	• Lectures: Introduction to networking technologies and their evolution. • Discussions: Analysis of the role of governing bodies in networking. • Case Studies: Examples of real-world implementation of networking models.

• Explain IPv4 challenges and the need for IPv6. • Understand IPv6 addressing types (unicast, anycast, multicast). • Compare IPv4 and IPv6 headers and analyze their benefits. • Learn about ICMPv6, SLAAC, and NDP.	**2 IPv6 Addressing** 2.1 IPv4 addressing overview, challenges, and issues 2.2 Introduction to IPv6 networking 2.3 Features of IPv6 2.4 IPv6 addressing types: unicast, anycast and multicast 2.5 IPv6 address auto-generation, SLAAC 2.6 IPv4 and IPv6 header comparison 2.7 IPv6 extension headers 2.8 NDP, ICMPv6	10	• Lectures: Fundamentals of IPv6 and addressing mechanisms. • Hands-on Labs: IPv6 addressing and routing using GNS3, Packet Tracer, or Mininet. • Group Work: IPv4-to-IPv6 transition scenarios.
• Identify security issues in legacy networks and IPv6-specific threats. • Explain security mechanisms like IPsec, authentication, and encryption. • Understand IPv6 routing protocols (RIP, OSPF, PIM-SM).	**3 Security and Routing in IPv6** 3.1 Security Issues with Legacy Network 3.2 Types of Threats and Vulnerabilities 3.3 Security Techniques 3.4 Tunnel and transport mode of authentication and encryption 3.5 IPSEC Framework 3.6 Introduction to IPv6 Routing 3.7 Unicast Routing in IPv6, RIP and OSPF 3.8 Multicast Routing in IPv6, PIM-SM	10	• Lectures: Security challenges and solutions in IPv6. • Hands-on Labs: Implementing IPsec for IPv6 security. • Demonstrations: Configuring RIP and OSPF for IPv6.
• Understand SDN architecture, components, and protocols like OpenFlow. • Explore SDN APIs and network function virtualization (NFV).	**4 Software-Defined Networking** 4.1 Importance and Application 4.2 SDN architecture and components 4.3 SDN Protocol Standards (OpenFlow) 4.4 SDN APIs (North, South, East and West bound) 4.5 Data and Control Plane overview (NOX, POX, Beacon, floodLight...)	12	• Lectures: SDN fundamentals and applications. • Practical Labs: Mininet simulations and SDN controller programming using Java/Python.

• Learn about SDN applications in telecom/ISP domains.	4.6 SDN in the Telecom/ISP Domain 4.7 SDN Programming (P4, Frenetic) 4.8 Network Function Virtualization concepts and principles 4.9 NFV orchestration and management 4.10 Future smart networking with SDN and IPv6 4.11 Research trends in SDN, NFV and IPv6		• Project Work: Developing small-scale SDN-based networks.
• Describe 5G architecture, applications, and network slicing. • Understand IoT paradigms and technologies like RFID, WSN. • Explore edge computing and industrial IoT applications.	**5 5G Network Technologies and Internet of Things (IoT)** 5.1 Definition, Overview, Applications, Potential & Challenges 5.2 5G Evaluation & Applications 5.3 5G building blocks and Architecture 5.4 5G network slicing 5.5 IoT vision, paradigm, technologies: RFID, WSN 5.6 IoT networking challenges 5.7 Edge computing for IoT applications 5.8 Overview of Industrial IoT 5.9 Cyber physical systems	12	• Lectures: Explain core concepts, network architectures, and emerging IoT technologies. • Laboratory Experiments: Conduct practical tests on wireless protocols and IoT device interactions. • Discussion Sessions: Debate challenges and opportunities in deploying 5G and IoT technologies in real-world scenarios.
• Understand challenges in transitioning to IPv6, SDN, and 5G. • Identify security threats and mitigation strategies in modern networking.	**6 Emerging Trends and Challenges in Networking** 6.1 IPv6, SDN, and 5G network migration approaches and challenges 6.2 Security challenges over latest networking environment	10	• Lectures: Future networking trends and challenges. • Seminars: Research discussions on AI/ML in networking.

• Explore new paradigms like NDN, IBN, QNet, and AI/ML in networking.	6.3 Threats and vulnerabilities in latest networking 6.4 Introduction to Named Data Networking (NDN) 6.5 Introduction to Intent Based Networking (IBN) 6.6 Introduction to Quantum Networking (QNet) 6.7 Research trends on latest networking. 6.8 AI and ML applications in networking		• Case Studies: Security vulnerabilities and solutions in modern networks.

Laboratory Works:

IPv6 addressing and routing implementation using GNS3 or Packet Tracer or Mininet

SDN: Mininet, Controller Programming: Java/Python

IoT: wireless protocol test

SDN, 5G and IPv6: Mininet-WiFi

Network Socket Programming

References:

1. IPv6 Essentials, O’reilly, by *Silvia Hagen*

2. "Software-Defined Networking: Anatomy of OpenFlow," by *David M. Eastlake, et al*.

3. Software Networks: Virtualization, SDN, 5G and Security, by Guy Pujolle, ISBN-13: 978-1848216945, Wiley

4. Getting Started with IoT-1st Edition, O'Reilley Media, by *Cuno Pfister*

5. *e-BOOK*: executive Guide to SDN

Evaluation Scheme:

Chapter	1	2	3	4	5	6
Topics	All	All	All	All	All	All
Marks	6	10	10	12	12	10

*There may be a minor deviation in mark distribution.

Cryptography and Data Security (ENCTNS502) Credits: 4

Level : M. Sc. Year : I

Program : MSNCS Part : I

Course Objective:

- Understand the fundamental principles of cryptography and its role in network and cyber security.
- Design cryptographic algorithms and protocols for ensuring confidentiality, integrity, authentication, and non-repudiation.
- Analyze and mitigate cryptographic attacks and vulnerabilities in real-world scenario.
- Understand cryptographic hash functions, applications, and PKI.
- Identify common cyber threats and vulnerabilities.
- Explore legal and regulatory requirements for data protection
- Understand the basic concepts of cyber security and data privacy.
- Explore emerging trends in cryptography and security

Learning Outcomes	Chapter Contents	Credit Hours	Teaching Methods
• Understand the history and evolution of cryptography. • Identify fundamental cryptographic	**1 Introduction to Cryptography** 1.1 History and evolution of cryptography 1.2 Basic cryptographic terminologies and concepts 1.3 Kerchoff’s law	6	• Lectures and discussions on cryptographic history and principles. • Demonstrations of substitution and transposition ciphers.

terminologies and concepts. • Explain Kerckhoff’s law and zero-knowledge proof. • Comprehend the goals of cryptography: confidentiality, integrity, authentication, and non-repudiation. • Analyze classical cryptographic methods and cryptanalysis techniques.	1.4 Zero knowledge proof 1.5 Goals of cryptography: Confidentiality, integrity, authentication, and non-repudiation 1.6 Classical cryptography: substitution ciphers, transposition ciphers 1.7 Cryptoanalysis techniques		• Hands-on exercises in basic cryptanalysis techniques.
• Explain symmetric key encryption and its properties. • Understand block ciphers (DES, 3DES, AES) and their modes of operation. • Explore stream ciphers and analyze their security aspects. • Discuss the principles and security of public-key cryptography.	**2 Symmetric and Asymmetric Key Cryptography** 2.1 One time pad and perfect secrecy 2.2 Block Ciphers (BC) 2.3 DES, 3DES and AES 2.4 BC Modes of Operation 2.5 Stream Ciphers, RC4 2.6 Attacks on symmetric key cryptosystem and counter measures 2.7 Principles of public-key cryptography 2.8 Deffie-Hellmen key exchange algorithm, security properties and vulnerabilities	12	• Interactive lectures and algorithm breakdown sessions. • Hands-on exercises implementing DES, AES, and RSA. • Group discussions on cryptographic attacks and their mitigation. • Problem-solving sessions on key exchange and encryption models.

• Examine cryptographic algorithms like RSA, Diffie-Hellman, and elliptic curve cryptography. • Identify attacks and countermeasures for both symmetric and asymmetric encryption.	2.9 RSA algorithm, key generation process, key length considerations, applications 2.10 Elliptic curve cryptography, key generation, parameter selection 2.11 Attacks on asymmetric key cryptosystems and counter measures		
• Understand the role and properties of cryptographic hash functions. • Compare different cryptographic hash functions and their applications. • Analyze cryptographic hash function vulnerabilities, including collision and length extension attacks. • Explore hash function applications in password hashing, digital signatures, and blockchain.	**3 Cryptographic Hash Functions** 3.1 Definition and properties of cryptographic hash functions 3.2 Common cryptographic hash functions and comparison 3.3 Cryptoanalysis of hash functions: collision attacks, length extension attacks, time memory trade off attacks 3.4 Applications: password hashing, digital signature, Blockchain and cryptocurrency.	8	• Demonstrations of hash function implementations. • Group exercises on cryptographic attacks and their impact. • Hands-on activities using cryptographic tools to analyze hash outputs.
• Understand the purpose and significance of	4 **Key Management**	8	• Lectures on PKI components and trust models.

Public Key Infrastructure (PKI). • Identify key components of PKI, including Certificate Authorities and digital certificates. • Explore certificate generation, revocation, renewal, and trust models.	4.1 Definition, historical context, and importance of PKI 4.2 Key components: Certificate authority, registration authority, certification revocation list, certificate repository 4.3 Digital certificates: structure, contents, formats, certificate chains and hierarchies 4.4 PKI Operations: generation, revocation, renewal 4.5 PKI trust models, standards, and protocols.		• Hands-on exercises on certificate creation and management. • Discussions on real-world PKI implementations and challenges.
• Understand data security concepts, threats, and challenges. • Learn techniques for securing data at rest and in transit. • Explore methods like obfuscation, tokenization, and data loss prevention. • Analyze security considerations for mobile and cloud data.	**5 Data Security** 5.1 Data security concepts, terminology, and principles. 5.2 Data security risks, challenges, and threats 5.3 Securing data at rest and transit 5.4 Data classification and data labelling 5.5 Basic operations: obfuscation and tokenization 5.6 Data loss prevention 5.7 Mobile data security, cloud data security	10	• Case studies on data breaches and security failures. • Hands-on activities on encryption techniques for securing data. • Group discussions on cloud and mobile data security issues.
• Understand fundamental cybersecurity principles and common threats.	**6 Cyber Security and Data Privacy**	12	• Lectures on cybersecurity concepts and real-world case studies.

• Analyze security mechanisms like firewalls and Intrusion Detection Systems (IDS). • Explore data privacy laws, regulations, and compliance frameworks. • Examine privacy concerns in big data and social media. • Understand concepts of user behavior analytics and personal data protection.	6.1 Overview of cybersecurity and data privacy 6.2 Common cyber security and data threats 6.3 Firewalls and intrusion detection systems (IDS) 6.4 General trends in data privacy, information collection, processing, storage, deletion 6.5 Privacy issues in the age of social media and big data 6.6 Overview of data privacy laws, regulations, and compliance 6.7 Consent and right to erasure 6.8 Data governance and privacy impact assessments 6.9 Introduction to Cyber Physical Systems 6.10 User Behavior Analytics 6.11 Personally Identifiable Information and Personal Health Information		• • Hands-on IDS implementation and log data analysis. • • Group discussions on privacy regulations and legal frameworks. • • Problem-solving exercises on cybersecurity threat mitigation.
• Explore advances in cryptographic research, including quantum and post-quantum cryptography. • Understand concepts of homomorphic	**7 Emerging trends in Cryptography and Security** 7.1 Threat intelligence and predictive analytics 7.2 Overview of quantum, post-quantum, and quantum-safe cryptography	6	• Lectures and discussions on emerging trends and future challenges. • Case studies on AI and ML applications in cybersecurity. • Interactive activities exploring quantum cryptography.

encryption and federated learning security. • Analyze the role of AI and ML in cryptography and security. • Examine supply chain security and threat intelligence methodologies.	7.3 Homomorphic encryption 7.4 Overview of supply chain security 7.5 Security aspects in federated learning 7.6 Artificial intelligence and machine learning in cryptography and data security 7.7 Other emerging trends in security		

Laboratory Works:

1. implementation of classical cryptosystem, one-time pad, block ciphers, stream ciphers, DES and RSA.
2. attack on the cryptographic systems
3. IDS implementation
4. Log data analysis

References:

1. “Cryptography and Network Security: Principles and Practice” by *William Stallings*
2. "Introduction to Modern Cryptography" by *Jonathan Katz and Yehuda Lindell*
3. “Computer security, art and science” by *Matt Bishop*

Evaluation Scheme:

Chapter	1	2	3	4	5	6	7
Topics	All	All	All	All	All	All	All
Marks	6	12	8	8	8	12	6

*There may be a minor deviation in mark distribution.

Machine Learning and Data Analytics (ENCTNS551) **Credits: 4**

Level : M. Sc. Year : I

Program : MSNCS Part : I

Course Objectives:

The objective of this course is to provide a fundamental understanding of Machine Learning (ML), Deep Learning, and Data Analytics. This course also explores the understanding of Supervised and unsupervised learning techniques, probability-based learning techniques, performance evaluation of ML algorithms, and applications of ML such as in information /cyber security, etc.

Learning Outcomes	**Chapter Contents**	**Credit Hours**	**Teaching Methods**
• Understand the history, definition, and types of machine learning. • Review basic statistical concepts relevant to machine learning. • Comprehend fundamental machine learning terminology. • Differentiate between training, validation, and test data. • Understand key concepts like generalization tradeoff, bias-variance tradeoff, and learning curves.	1. **Basics of Machine Learning** 1.1 History of machine learning, definition of learning, types of learning, and importance of machine learning 1.2 Review of Statistics: Min., Max., Mean, Mode, Median, Standard deviation, MSE 1.3 Basics of machine learning terminology: class, pattern, feature, training, validation and test data 1.4 Feasibility of learning – error and noise – training versus testing 1.5 Generalization tradeoff – bias and variance – learning curve 1.6 Overfitting and Underfitting	6	• Lectures with real-world examples. • Hands-on exercises using datasets for statistical calculations. • Interactive discussions and case studies. • Visual illustrations of overfitting and underfitting.

• Identify overfitting and underfitting problems.			
• Understand the process of data analytics and its key steps. • Differentiate between various data types and attributes. • Learn data pre-processing techniques for machine learning. • Utilize data visualization methods for exploration. • Understand architectural design patterns for handling Big Data. • Identify different types of analytics (descriptive, diagnostic, predictive, prescriptive).	**2. Data Analytics Process** 2.1 Process of data analytics 2.2 Data types and attributes 2.3 Data pre-processing 2.4 Visualization and exploring data 2.6 Architectural design patterns and stack for handling Big Data 2.5 Descriptive, diagnostic, predictive, prescriptive analytics	9	• Hands-on labs on data pre-processing and visualization. • Group discussions on Big Data handling techniques. • Practical exercises using Python libraries (Pandas, Matplotlib, Seaborn).
• Understand the concept of supervised learning and classification problems. • Learn about classifiers and discriminant functions. • Implement linear supervised learning models such as linear regression and perceptron. • Comprehend neural network structures and decision tree models.	**3. Supervised Learning** 3.1 Definition and classification problem 3.2 Classifiers and discriminant functions 3.3 Linear supervised learning models: linear regression, Perceptron 3.4 Learning neural network structures 3.5 Decision tree representation model, basic decision tree algorithm, and application	9	• Coding exercises using Python and Scikit-Learn. • Hands-on implementation of classifiers. • Comparative analysis of different supervised learning models.

• Explore support vector machines and their applications.	3.6 Support vector machines and applications		
• Understand Bayes' probability theory and conditional probability. • Analyze decision surfaces and classification using Bayes decision theory. • Explore Bayesian belief networks and their applications. • Implement the gradient descent method for optimization. • Understand K-nearest neighbor (KNN) algorithm.	**4. Bayesian Decision based learning** 4.1 Bayes probability theory and conditional probability 4.2 Decision surfaces and classifying with Bayes decision theory 4.3 Bayesian belief network and applications 4.4 Gradient descent method 4.5 K-nearest neighbor	9	• Mathematical derivations and problem-solving sessions. • Algorithmic implementations using Python. • Real-life applications of Bayesian methods.
• Understand the concept of clustering and different clustering algorithms. • Implement K-means, hierarchical, and other clustering techniques. • Comprehend the importance of dimensionality reduction. • Apply Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA).	**5. Un-Supervised learning and dimensionality reduction** 5.1 Introduction to clustering, criterion function for clustering 5.2 Algorithms for clustering; K-means, hierarchical, and other methods 5.3 Dimensionality reduction techniques and need 5.4 Principal component analysis (PCA) 5.5 Linear discriminant analysis (LDA)	9	• Interactive demonstrations of clustering techniques. • Implementation of dimensionality reduction in Python. • Case studies on real-world datasets.
• Evaluate classification accuracy. • Construct and interpret confusion matrices.	**6. Measures for Performance Evaluation** 6.1 Classification accuracy 6.2 Confusion matrix 6.3 Misclassification costs	9	• Practical sessions on evaluating ML models.

• Analyze misclassification costs. • Understand precision, recall, F1-score, and ROC curves. • Conduct cross-validation for performance assessment. •	6.4 Sensitivity and specificity, recall, precision, and F1-score 6.5 ROC curve, box plot, confidence interval 6.6 Cross-validation		• Use of visualization tools like ROC plots. • Case studies on model performance assessment.
• Define deep learning and neural networks. • Understand feed-forward and backpropagation concepts. • Implement activation functions (Sigmoid, Tanh, ReLU, Softmax). • Learn about CNN and RNN architectures. • Explore ML applications in security (anomaly detection, fraud detection, etc.)	**7. Deep Learning Basic** 7.1 Definition of deep networks 7.2 Feed-Forward and backpropagation 7.3 Activation functions sigmoid, Tanh, ReLU and Softmax 7.4 Convolution neural networks: CNN architectures 7.5 Recurrent neural networks: RNN architectures 7.6 ML applications in Security: Anomaly detection /intrusion detection, Malware/phishing / fraud detection	9	• Hands-on coding in TensorFlow and Keras. • Case studies on security-related ML applications. • Interactive discussions on deep learning architectures.

Laboratory Works

Practical work should be done covering all the topics listed above and a small project work should be carried out using the concepts learned in this course using software like Matlab and Python.

References Books:

1. Pablo Duboue, *The Art of Feature Engineering: Essentials for Machine Learning*, Cambridge University Press, First Edition, 2020
2. Christopher M. Bishop, *Pattern Recognition and Machine Learning*, Springer, First Edition, 2011
3. Kevin P. Murphy, *Machine Learning: A Probabilistic Perspective*, MIT Press, First Edition, 2012
4. Oliver Theobald, *Machine Learning For Absolute Beginners*, Kindle Edition, 2017

5. Geron Aurelien, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow,* O'Reilly Media, Inc. 2019
7. Ian Goodfellow, Yoshua Bengio, Aaron Courville. Deep Learning, MIT Press. 2016

Evaluation Scheme:

Chapter	1	2	3	4	5	6	7
Topics	All	All	All	All	All	All	All
Marks	7	9	9	9	9	8	9

*There may be a minor deviation in mark distribution.

Research Methods (ENCTNS504) Credits: 4

Level : M. Sc. Year : I

Program : MSNCS Part : I

Course Objectives:

The purpose of research is to discover answers to questions through the application of scientific procedures. The main aim of research is to find out the truth which is hidden and which has not been discovered as yet. Though each research study has its own specific purpose, we may think of research objectives as falling into a number of following broad groupings:

- To generate new knowledge or to gain familiarity or to develop a new insight into some phenomenon.
- To investigate some existing situation or problem.
- To construct or create a new procedure or system.
- To explore and analyze more general issues.
- To investigate some existing situations or problems.
- To test a hypothesis or theory.
- To identify patterns or trends related to the problem

Learning Outcomes	Chapter Contents	Credit Hours	Teaching Methods
• Understand the definition, purpose, and importance of research in engineering. • Identify different types of research methodologies.	**1 Introduction to Research** 1.1 Scientific Methods and Research: Definitions of research; Purpose, importance, steps levels and rigor of research in Engineering discipline	10	• Lectures with real-world examples. • Case studies of engineering research projects.

- Formulate research questions, problems, objectives, and hypotheses. - Design research frameworks based on conceptual and operational principles.	1.2 Basic Types of Researches: Quantitative /Qualitative research, Fundamental/Applied research, Descriptive/Analytical research, Conceptual/Empirical research, Diagnostic/Hypothesis testing research, Conclusion oriented/Decision oriented research, Theoretical /Action research, Longitudinal /Cross sectional research 1.3 Research Question, Research Problem, Research Objective, Research Hypothesis 1.4 Designing of Research work: Principles of designing a research, Conceptual framework and its operationalization, engineering research design		- Group discussions and brainstorming activities. - Interactive presentations on different research designs.
- Recognize different phases of research from desktop research to validation. - Understand theoretical modeling and conceptual frameworks. - Learn ethical considerations in research.	**2 Phases and Methods of Engineering Research** 2.1 Desktop Research 2.2 Literature Study 2.3 Theoretical Modelling and Conceptual Frameworks 2.4 Experimental and Study Design 2.5 Data Collection 2.6 Evaluation, Validation and Verification	8	- Hands-on exercises in literature review and desktop research. - Workshops on research ethics and integrity. - Demonstration of experimental and study design techniques. - Peer review activities for research proposals.

	2.7 Research Ethics		
• Differentiate between primary and secondary data collection methods. • Understand various data collection techniques such as interviews, questionnaires, and observations. • Evaluate the effectiveness of different data collection strategies.	**3 Data Collection** 3.1 Collection of Primary Data 3.2 Observation Method 3.3 Interview Method 3.4 Collection of Data through Questionnaires 3.5 Collection of Data through Schedules 3.6 Difference between Questionnaires and Schedules 3.7 Some Other Methods of Data Collection 3.8 Collection of Secondary Data, 3.9 Selection of Appropriate Method for Data Collection.	5	• Role-playing activities for interview and observation techniques. • Surveys and questionnaire design exercises. • Case studies on effective data collection. • Group discussions on challenges in data collection.
• Understand the steps in data processing and analysis. • Learn statistical methods such as central tendency, dispersion, and regression analysis. • Interpret research data effectively.	**4 Processing and Analysis of Data** 4.1 Processing Operations 4.2 Elements/Types of Analysis 4.3 Statistics in Research 4.4 Measures of Central Tendency 4.5 Measures of Dispersion 4.6 Measures of Asymmetry (Skewness) 4.7 Measures of Relationship 4.8 Simple Regression Analysis	10	• Hands-on practice with statistical tools. • Data analysis exercises using real-world datasets. • Visual presentations of different data processing techniques. • Group discussions on data interpretation challenges.
• Understand hypothesis formulation and testing procedures.	**5 Testing of Hypotheses** 5.1 Definition of Hypothesis	10	• Problem-solving sessions using statistical software.

• Learn different statistical tests such as z-test, t-test, chi-square test, and F-test. • Identify limitations and appropriate applications of hypothesis testing.	5.2 Basic Concepts Concerning Testing of Hypotheses 5.3 Procedure for Hypothesis Testing 5.4 Important Parametric Tests (z-test, t-test, χ2-test, F-test) 5.5 Hypothesis Testing of Means 5.6 Hypothesis Testing for Comparing Two Related Samples 5.7 Hypothesis Testing of Proportions 5.8 Testing the Equality of Variances of Two Normal Populations 5.9 Hypothesis Testing of Correlation Coefficients 5.10 Limitations of the Tests of Hypotheses		• Guided exercises on hypothesis testing. • Group analysis of sample research studies. • Peer review of hypothesis formulation exercises.
• Understand the applications and conditions for chi-square tests. • Learn how to apply one-way and two-way ANOVA techniques in research. • Analyze variance and interpret statistical results.	**6 Chi-Square Test and ANOVA** 6.1 Chi-square as a Test for Comparing Variance 6.2 Chi-square as a Non- parametric Test 6.3 Conditions for the Application of χ2 Test 6.4 Steps Involved in Applying Chi-square Test 6.5 Analysis of Variance (ANOVA) and ANOVA Technique 6.6 Setting up Analysis of Variance Table 6.7 Coding Method	7	• Case studies of research using chi-square and ANOVA. • Hands-on practice with statistical software. • Lecture demonstrations with step-by-step problem-solving. • Interactive quizzes on hypothesis testing methods.

	6.8 Two-way ANOVA		
• Learn the steps of scientific publishing and research reporting. • Understand CPM and PERT for Project Management • Explore open science and continuous scientific research practices. • Develop skills in presenting and writing research findings.	**7 Reporting and Managing Research** 7.1 Reporting Results 7.2 Reporting in Multidisciplinary Fields 7.3 Scientific Publishing 7.4 Steps of continuous scientific research 7.5 Open Science 7.6 Project Management 7.7 Demo Lecture Gantt Charts 7.8 Seminar	10	• Seminar presentations on selected research topics. • Hands-on practice in writing research reports. • Demonstrations of Gantt charts and project management tools. • Interactive peer feedback sessions on research reports.

Laboratory Works:

The laboratory work is designed as a seminar. In Seminar the students are required to choose a topic of their interest, find a high-quality recent journal related to that topic and make a presentation based on that paper.

References:

1. Kothari, C.R., Research Methodology: Methods and Techniques. New Age International. 418p.
2. Practical Research Methods, Dawson, C., UBSPD Pvt. Ltd. 5. Research Methodology, Sharma, N. K., KSK Publishers, NewDelhi.
3. Garg, B. L., Karadia, R., Agarwal, F. and Agarwal, U. K., An introduction to Research Methodology, RBSA Publishers.
4. Sinha, S. C. and Dhiman, A. K., Research Methodology, Ess Publications. 2 volumes.

Evaluation Scheme:

Chapter	1	2	3	4	5	6	7
Topics	All	All	All	All	All	All	All
Marks	10	8	5	10	10	7	10

*There may be a minor deviation in mark distribution.

Year: 1st **Part: 2nd**

Semester: II

S. No.	Teaching Schedule			Examination Schedule			Total	Remarks
	Course Code	Course Title	Credit	Assessment Marks	Final			
					Duration Hours	Marks		
1	CT	Digital Forensics and Incident Response	4	40	3	60	100	
2	CT	Information Systems Audit	4	40	3	60	100	
3	CT	Elective I	4	40	3	60	100	
4	CT	Elective-II	4	40	3	60	100	
Total			**16**	**160**		**240**	**400**	

Digital Forensics and Incident Response (ENCTNS551) Credits: 4

Level : M. Sc.
Year : I

Program : MSNCS
Part : II

Course Objectives

This course provides a comprehensive overview of digital forensics and incident response, focusing on the methodologies, tools, and techniques used to investigate and respond to cybersecurity incidents. Students will learn to systematically gather, analyze, and preserve digital evidence for legal admissibility and effectively manage and mitigate security breaches. The course integrates theoretical concepts with practical exercises to equip students with the skills to conduct thorough forensic investigations and implement robust incident response strategies.

Learning Outcomes	Chapter Contents	Credit Hours	Teaching Methods
● Understand the fundamentals of digital forensics and incident ● Understand the essential legal aspects related to digital forensics ● Grasp a basic understanding of Nepal's legal provisions related to digital forensics ● Build familiarity with the basics of incident response Frameworks. ● Apply NIST and SANS	**1. Introduction** 1.1. Introduction to digital forensics 1.2. Digital evidence and legal admissibility 1.3. Burden of proof 1.4. Chain of custody of digital evidence 1.5. Provisions related to digital evidence in the Evidence Act of Nepal. 1.6. Introduction to Incident Response, phases of incident response.	12	● Lectures: Overview of foundational concepts related to digital forensics and incident response. ● Lectures: Overview of global and Nepal's law associated with Digital Evidence, Chain of custody, and legal admissibility ● Interactive Discussion: Nepal's evidence law and its provisions related to digital evidence

Framework for Incident Response.	1.7. Reporting 1.8. Common incident response frameworks NIST, SANS 1.9. Incident response plan, Incident response team		● Case Studies: Application of SANS and NIST Framework for Incident Response
● Understanding storage and file system layout ● Learning forensic imaging and acquisition techniques ● Apply tools and techniques to recover deleted data ● Application of standard tools for disk-based forensics analysis	**2. Disk and Filesystem Forensics** 2.1. Understanding storage devices and filesystem layout 2.2. Forensic imaging and acquisition techniques 2.3. Maintaining the integrity of media under analysis 2.4. Locating and recovering deleted data 2.5. Usage of common tools like Autopsy, SleuthKit, FTK	8	● Lectures: Overview of storage layout for filesystem ● Hands-on: Basics of Digital Forensics Image acquisition and analysis ● Interactive discussion: Relevant disk-based forensics cases
● Understanding the importance of memory contents, their acquisition, and analysis in digital forensics ● Apply tools to analyze memory contents and equip to infer the output of the tools used for analysis	**3. Memory Forensics** 3.1. Analyzing memory (RAM) contents 3.2. Importance of analyzing memory contents in digital forensics 3.3. Memory dump analysis with Volatility and Rendell	8	● Lectures: Overview of importance, acquisition, and analysis of memory contents in digital forensics ● Hands-on: Using tools to capture and analyze memory contents in digital forensics
● Understanding the usage of various network data-capturing tools in different scenarios ● Differentiate IPS and IDS and understand their role in forensic analysis	**4. Network Forensics** 4.1. Network traffic capture and analysis with PCAP, Wireshark 4.2. IDS, IPS systems for forensic analysis 4.3. Detecting network attacks and	6	● Lectures: Overview of capturing, collection, and analysis of network forensics artifacts ● Interactive discussion: IPS vs. IDS and their suitability in

● Understand documenting requirements of network forensics regarding legal admissibility	traces and documenting for legal admissibility		forensic analysis ● Hands-on: Using Wireshark to capture and analyze memory forensics-related artifacts
● Understanding the basic concepts and challenges of mobile data acquisition techniques ● Exploring the value mobile forensics adds to forensic investigation ● Evaluate the capability of tools regarding the acquisition, analysis, and usage of data obtained in mobile forensics	**5. Mobile Device Forensics** 5.1. Mobile device acquisition techniques (iOS, Android) 5.2. Recovering SMS, call logs, GPS data, application data 5.3. Usage of tools like Andriller, Cellebrite, Oxygen Forensics suite	8	● Lectures: Overview of the importance of mobile data acquisition, analysis in digital forensics ● Interactive discussion: Usage of mobile devices and usefulness of forensic data acquired from mobile devices ● Lectures and Demonstrations: Mobile forensics tools and analysis of data acquired using these tools
● Understand the changing landscape of data centers to cloud infrastructure ● Understand the challenges in the cloud in the acquisition and analysis of digital artifacts. ● Explore legal constraints in acquiring digital forensics artifacts in a cloud computing environment. ● Understand standard practices and tools for digital forensics in major cloud providers	**6. Cloud Forensics** 6.1. Introduction to digital forensics in the cloud environment. 6.2. Challenges in analyzing digital evidence in the cloud environment 6.3. Common practices and tools for digital forensic analysis in AWS, azure, and GCP.	6	● Lectures: Changing data infrastructure, landscape to cloud, and challenges it poses on digital forensics. ● Presentation: Legal and privacy constraints in collecting digital forensics artifacts in the cloud. ● Group discussions: Common practices and tools for digital forensics for the cloud
● Understand the importance of	**7. Malware analysis**	6	● Lectures: Overview,

malware analysis in digital forensics ● Differentiate various approaches utilized for the analysis ● Explore multiple tools used for dynamic analysis	7.1. Introduction and importance of malware analysis in digital forensics 7.2. Static, dynamic, and hybrid analysis 7.3. Using tools like Cuckoo Sandbox, Ghidra, and Volatility for malware analysis		Importance of malware analysis in digital forensics ● Presentation: Various approaches to malware analysis and ● Group Discussion: usefulness of information obtained from static, dynamic, and hybrid analysis. ● Hands-on: sample analysis of malware using static and dynamic malware analysis tools
● Understand various types of logs ● Evaluate the possibility of a correlation between logs and other system information for forensics analysis ● Understand practices regarding storage and retrieval of logs for legal and admissibility. ● Analyze standard log formats, applications, and tools	**8. Log Analysis** 8.1. Analyzing system, application, and access logs 8.2. Correlating logs with other system information for digital forensics 8.3. Storing and retrieving logs for legal admissibility 8.4. Common log formats, logging applications, and tools	6	● Lectures: Overview of collection, analysis, retrieval, and storing of logs from various log sources ● Hands-on: develop a SIEM system based on open-source tools ● Group discussion: legal aspects of storage and retrieval of log data ● Presentation: Common formats, tools configuration for logging

Laboratory Works:

Students will engage in practical hands-on using open source tools for chapters 2, 3, 4, 7, and 8 and submit their findings as assignments. Practical for Chapter 5 will depend on the availability of tools.

References

1. Johansen, G. (2022). *Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response*. Packt Publishing Ltd.
2. Oettinger, W. (2022). *Learn Computer Forensics–2nd edition: Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence*. Packt Publishing Ltd.
3. Luttgens, J. T., Pepe, M., & Mandia, K. (2014). *Incident response & computer forensics*. McGraw-Hill Education Group.
4. Boddington, R. (2016). *Practical digital forensics*. Packt Publishing Ltd.

Final Examination

The questions will cover all chapters of the syllabus. The evaluation scheme will be as indicated in the table.

Chapter	1	2	3	4	5	6	7	8
Topics	All	All	All	All	All	All	All	All
Marks	12	8	8	6	8	6	6	6

*There may be a minor deviation in mark distribution.

Information Systems Audit (ENCTNS 552) Credits: 4

Level : M. Sc. Year : I

Program : MSNCS Part : II

Course Objectives:

This course offers a comprehensive overview of Information Systems Auditing, focusing on foundational principles, hardware and software security concerns, and the audit process. Students will explore risk-based systems auditing, business continuity, disaster recovery, auditing within the ICT environment, and security testing techniques.

Learning Outcomes	Chapter Contents	Credit Hours	Teaching Methods
▪ Understand the Role and Responsibilities of an Information Systems Auditor. ▪ Analyze Legal and Regulatory Requirements for Information Systems Audits ▪ Evaluate Information Systems Assets and Apply Control Classifications ▪ Apply Global Standards and Frameworks for Information Systems Audits	**1. Introduction to Information Systems Audit** 1.1 Information Systems Audit and Information Systems Auditor 1.2 Legal Requirements of an Information Systems Audit 1.3 Systems Environment and Information Systems Audit 1.4 Information Systems Assets and Classification of Controls 1.5 Information Systems Audit Coverage 1.6 IT Audit Standard and Guidelines, Regulatory Requirements 1.7 ISO 27001, NIST Cyber Security Framework, COBIT, CIS	10	▪ Lecture with visual aids on each topic. ▪ Case Study and Problem-Solving Sessions: Knowledge and Task Statements of an IS Auditor, Information System Assets and Classifications ▪ Group Discussions and Presentations: Assign topics like IT audit coverage based on ISO 27001, NIST Cybersecurity Framework, COBIT and CIS ▪ Seminar on Necessity of IT Governance Framework with COBIT

▪ Evaluate Hardware and Peripheral Security ▪ Assess Hardware Lifecycle Management ▪ Examine Network and Software Security Controls ▪ Verify Compliance in ICT Procurement and Licensing ▪ Understand Audit Problem and Change Management Processes	**2. Hardware and Software Security Issues during Audit** 2.1 Hardware Security Objective 2.2 Peripheral Devices and Storage Media 2.3 Authentication Devices 2.4 Hardware Acquisition, Hardware Maintenance and Management of Obsolescence 2.5 Disposal of Equipment; Problem Management; Change Management 2.6 Network and Communication Issues. 2.7 Overview of Types of Software; Elements of Software Security 2.8 Control Issues during Installation and Maintenance 2.9 Licensing Issues, ICT Procurement Practice	10	▪ Lecture with visual aids on each topic ▪ Case Study: Developing ICT Policy, Procedures and Guidelines ▪ Group Discussion and Presentation: IS Audit Gap Assessment for Hardware and Software Related Issues based on ISO 27001, NIST, CIS ▪ Interactive Discussions: Licensing Issues, ICT Procurement Practices and Guidelines
▪ Understand to Analyze Risk and Threats in Information Systems ▪ Understand Information Systems Control and Audit Objectives ▪ Evaluate Asset Safeguarding and Abuse Prevention ▪ Identify Evidence Collection and Evaluation Techniques	**3. Information Systems Audit Requirements** 3.1 Risk Analysis; Threats, Vulnerability, Exposure, Likelihood, and Attack 3.2 Information Systems Control Objectives; Information Systems Audit Objectives; 3.3 System Effectiveness and Efficiency 3.4 Information Systems Abuse 3.5 Asset Safeguarding Objective and Process 3.6 Evidence Collection and Evaluation 3.7 Logs and Audit Trails as Evidence	10	▪ Lecture with visual aids on each topic ▪ Case Study: Conducting Risk Assessment ▪ Case Study: ISACA Risk Starter Kit ▪ Group Discussions: CCMC, SOC2 Certifications ▪ Group Workshop and Presentation: Building Terms of Reference (TOR) of an IS Audit.
▪ Understand to Develop Audit Programs and Plans ▪ Understand to Apply Audit Procedures, Approaches, and Tools ▪ Understand to Evaluate Risk and Conduct Risk-Based Audits	**4. Conducting an Information System Audit** 4.1 Audit Program and Audit Plan 4.2 Audit Procedures and Approaches 4.3 System Understanding and Review 4.4 Compliance Reviews and Tests 4.5 Substantive Reviews and Tests 4.6 Audit Tools and Techniques 4.7 Sampling Techniques	12	▪ Lecture with visual aids on each topic ▪ Group Workshop and Presentation: Conducting Cybersecurity Maturity Assessment based on NIST Cybersecurity Framework, ISO 27001, CIS or C2M2

▪ Understand to Prepare Professional Audit Documentation and Reports	4.8 Audit Questionnaire; Audit Documentation; Audit Report 4.9 Auditing Approaches; Sample Audit Work-Planning Memo 4.10 Sample Audit Work Process Flow 4.11 Conducting a Risk-Based Information Systems Audit 4.12 Risk Assessment and Risk Management Strategy.		▪ Case Study: Risk-Based IS Audit ▪ Group Discussions: Audit Questionnaire, Audit Documentation
▪ Understand the Business Continuity and Disaster Recovery Process ▪ Conduct a Business Impact Analysis (BIA) and Develop an Incident Response Plan ▪ Understand the Emergency Preparedness Audit Checklists	**5. Business Continuity and Disaster Recovery Plan** 5.1 Business Continuity and Disaster Recovery Process 5.2 Business Impact Analysis; Incident Response Plan 5.3 Disaster Recovery Plan 5.4 Types of Disaster Recovery Plans 5.5 Emergency Preparedness Audit Checklist 5.6 Business Continuity Strategies 5.7 Business Resumption Plan Audit Checklist 5.8 Recovery Procedures Testing Checklist; Plan Maintenance Checklist	10	▪ Lecture with visual aids on each topic. ▪ Group Workshop and Presentation: Develop IS Audit Proposal ▪ Group Discussion: Business Impact Analysis ▪ Seminar on: Incident Response and Cyber Incident Reporting for Organizations
▪ Understand the Global Cybersecurity Landscape ▪ Understand VAPT Methods and Techniques. ▪ Understand Security by Design concept ▪ Understand Security Testing Tools and Cloud Audit Approach.	**6. Security Testing and Cloud Computing Audit** 6.1 Cybersecurity, Global Cybersecurity Landscape 6.2 Vulnerability Assessment and Penetration Testing (VAPT) 6.3 Secured Software Development Testing, DevOps and DevSecOps 6.4 Open Web Application Security Project 6.5 Security Testing Tools 6.6 Cloud Audit Considerations	8	▪ Lecture with visual aids on each topic. ▪ Hands on Lab: Working on VAPT tools ▪ Group Workshop and Presentation: Conduct IS and VAPT ▪ Seminar on OWASP ▪ Open Discussions: Conducting Audit on AI Tools ▪ Case Study: AWS Cloud Audit

Laboratory Works

1. Information Security Gap Assessment through ISO 27001
2. Cyber Security Maturity Assessment thorough NIST Cyber Security Framework.
3. IT Governance Audit through Control Objective for Related Technologies.
4. Develop IS Audit Terms of Reference

References

1. Hall, J. A. (2020). *Information Technology Auditing and Assurance* (5th ed.). Cengage Learning
2. Moeller, R. (2022). *IT Audit, Control, and Security* (3rd ed.). Wiley.
3. ISACA. (2023). *CISA Review Manual, 28th Edition*. Information Systems Audit and Control Association. https://books.google.com.np/books?id=3irIzwEACAAJ
4. Hingarh, V., & Ahmed, A. (2013). *Understanding and conducting information systems auditing*. John Wiley & Sons.
5. Champlain, J. J. (2003). *Auditing information systems*. John Wiley & Sons.
6. Cascarino, R. E. (2007). *Auditor's guide to information systems auditing*. John Wiley & Sons.

Evaluation Schemes

Chapter	1	2	3	4	5	6
Topics	All	All	All	All	All	All
Marks	10	10	10	12	10	8

*There may be a minor deviation in mark distribution.

Routing And Switching (ENCTNS561) (Elective-I) **Credits: 4**

Level : M. Sc. Year : I

Program : MSNCS Part : II

Course Objectives:

This course provides an in-depth understanding of networking and associated securities from the perspective of IT governance, focusing on the principles, architecture, and configuration of routing and switching technologies. It covers essential topics such as VLANs, dynamic and static routing, network design, and troubleshooting. Students will gain hands-on experience with configuring routers, switches, and network protocols to build scalable and efficient networks. The course prepares students for real-world networking challenges with recent trends in routing and switching technologies.

Learning Outcomes	**Chapter Contents**	**Credit Hours**	**Teaching Methods**
▪ Understand Digital Transformation and Cybersecurity Challenges ▪ Understand Rubik Cube Model for Information Security ▪ Understand ITSM and Information Security Management Framework ▪ Understand IT Governance	**1. Cyber Security and IT Governance** 1.1. Digital Transformation and Cyber Security Issues 1.2. Information Security with Rubik Cube Model 1.3. Information Technology Service Management (ITSM) 1.4. Information Security Management Framework 1.5. Information Technology Governance	10	▪ Lectures: overview on each topic. ▪ Group Discussion: Defense in Depth Approach of Information Security ▪ Seminar on IT Governance with COBIT

	1.6. Framework of ICT Policy, Procedures and Guidelines		▪ Assignment on development of Standard Operating Procedures (SOP)
▪ Understand the Converged Network Design Guidelines ▪ Review IP Network Concepts with IPv4 and IPv6 ▪ Understand Cross Layer Protocol Engineering ▪ Understand the Importance of Network Documentation and Planning	**2. Converged Network Design Guidelines** 2.1. Converged Network Design Guidelines 2.2. Network Foundation Protection Framework 2.3. Review of IP Networks (IPv4 and IPv6) 2.4. Cross Layer Protocol Engineering 2.5. Network Planning and Documentation 2.6. Building Network Terms of Reference (ToR) and Access Network Design Guidelines	10	▪ Lectures: overview on each topic. ▪ Group Discussion: Network Foundation protection Framework ▪ Case Study: Network Planning, Documentation of an Enterprise ▪ Group Exercise: Develop TOR of Network Projects. ▪ Research Trends: Cross Layer Protocol Engineering
▪ Understand to Design Scalable and Secure Enterprise Network Architectures ▪ Analyze and Apply Enterprise Network Case Studies. ▪ Implement Advanced Routing Techniques ▪ Explore Emerging Trends in Routing and Switching	**3. Enterprise Routing and Packet Forwarding** 3.1. Enterprise Network Architecture with Fault Tolerance, Scalability, QoS and Security 3.2. Enterprise Network Case studies 3.3. Interior and Exterior Routing 3.4. Enterprise Routing Architecture (Homogeneous/Heterogeneous) 3.5. Policy Based Routing 3.6. Routing with IPv6 3.7. Principles of segment routing 3.8. Introduction to routing and switching over SDN and Quantum Networks 3.9. Multi-path routing and load balancing techniques	12	▪ Lectures: overview on each topic. ▪ Hands on Lab: Interior and Exterior Routing Protocols with IPv4 and IPv6. ▪ Seminar: Routing and Switching over SDN and Quantum Networks ▪ Paper Presentations

	3.10. Predictive analytics for proactive routing		
▪ Understand to Design Enterprise Local Area Network Architecture ▪ Configure and Manage VLANs and VLAN Trunking Protocols ▪ Utilize Load Balancing and Link Aggregation Techniques	**4. Enterprise Local Area Network** 4.1. Enterprise Local Area Network Architecture 4.2. Virtual LAN (VLAN), VLAN Trunking Protocol 4.3. Inter VLAN Routing Protocol 4.4. Enterprise LAN Security 4.5. Load Balancing Protocols 4.6. Link Aggregation Technologies and Protocols	10	▪ Lectures: overview on each topic. ▪ Hands on Lab: VLAN, Inter VLAN Routing ▪ Group Discussion: Enterprise LAN Security Best Practices. ▪ Case Study: Link Aggregation for Software Defined Infrastructure.
▪ Understand to Design Enterprise-Wide Area Network Architectures ▪ Develop and Implement VPN Policies ▪ Understand to Monitor Network Performance with Real-time Analytics	**5. Enterprise-Wide Area Networks** 5.1. Enterprise-Wide Area Network Architecture 5.2. Network Address Translation (NAT) 5.3. Introduction to Virtual Private Networks 5.4. Formulation of VPN Policy 5.5. Site to site IPSec VPN 5.6. GRE over IPSec VPN 5.7. Dynamic Multipoint VPN 5.8. Real-time network monitoring and analytics	10	▪ Lectures: overview on each topic. ▪ Hands on Lab: NAT ▪ Group Discussion: Formulation of VPN Policy ▪ Case Study: Dynamic Multipoint VPN deployment in an enterprise.
▪ Explore Hyper-Converged and Software-Defined Infrastructure	**6. Emerging Trends in Switching and Routing** 6.1. Routing and switching in edge networks	8	▪ Lectures: overview on each topic.

▪ Evaluate NFV and SDN Deployment Challenges ▪ Understand to Implement Network Segmentation and Blockchain Security ▪ Analyze the Impact of Emerging Technologies	6.2. Drivers of change: IoT, cloud computing, and edge computing. 6.3. Hyper Converged Infrastructure and Software Defined Infrastructure 6.4. NFV and SDN deployment challenges and benefits 6.5. Network segmentation and micro-segmentation trends 6.6. Blockchain on network routing and security 6.7. Fundamentals of quantum routing and switching		▪ Group Discussions on Emerging Trends in Switching and Routing Industry ▪ Case Study: NFV and SDN Implementations ▪ Paper Presentations ▪ Research Assignments : Explore the opportunities of quantum routing and switching.

Laboratory Activities:

1. Formulate Comprehensive ICT policy of the organization.
2. Develop Terms of Reference for Network Implementation
3. Develop Routing and Switching Architecture for the Enterprise
4. Develop VPN Policy and Framework for the Enterprise
5. IPv4 Routing Protocols
6. IPv6 Routing Protocols
7. VLAN, VTP, Inter VLAN Routing
8. Deployment of VPN (IPSec Site to Site, GRE over IPSec, DMVPN)

References:

1. James F. Kurose, Keith W. Ross (2021), “Computer Networking, A top down approach featuring the Internet “, Pearson Edition, Eight Edition.
2. A S Tanenbaum (2010), “Computer Networks “, Prentice Hall, Fifth Edition, January 9
3. Behrouz A Forouzan (2013), “Data Communications and Networking “, McGraw-Hill, Fourth Edition.
4. Brad Edgeworth. , Kevin Wallace, David Hucaby, Ramiro Rios, Jason Gooley(2019), CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, Cisco Press

Evaluation Schemes:

Chapter	1	2	3	4	5	6
Topics	All	All	All	All	All	All
Marks	10	10	12	10	10	8

*There may be a minor deviation in mark distribution.

Managing Secure Network Systems (ENCTNS562) – (Elective I) Credits: 4

Level : M. Sc. Year : I

Program : MSNCS Part : II

Course Objectives:

This course covers the comprehensive management of secure network systems, including fundamental principles, technologies, and practices. It emphasizes practical applications, solutions, and emerging trends in network security. It makes stay updated with the latest trends and technologies in network security.

Learning Outcomes	Chapter Contents	Credit Hours	Teaching Methods
• Understand the fundamental principles of network security. • Analyze the TCP/IP protocol suite and its security challenges. • Evaluate secure network protocols like HTTPS, SSH, and TLS/SSL. • Explain the importance of SSL certificates in security. • Identify key security goals: Confidentiality, Integrity, Availability (CIA).	**1. Introduction to Network Security & Protocols** 1.1. Overview of Network Security 1.2. TCP/IP Protocol Suite and Security 1.3. Secure Network Protocols: HTTPS, SSH, TLS/SSL 1.4. SSL Certificates 1.5. Security Goals: Confidentiality, Integrity, Availability, 1.6. Access Control, Authentication, Authorization, 1.7. Threat Landscape and Risk Management	10	• **Lectures**: Basics of network security and secure protocols. • **Case Studies**: Real-world network attacks and defenses. • **Hands-on Labs**: Configuring SSL/TLS, HTTPS, and SSH security. • **Group Discussions**: Risk management in modern networks.

• Assess threat landscapes and risk management techniques.			
• Understand VPN concepts and their role in secure communication. • Differentiate between tunnel mode and transparent mode. • Implement and manage Site-to-Site and Remote Access VPNs. • Configure IPSec, SSL, and MPLS VPNs. • Utilize tunneling protocols like GRE for secure connections.	**2. Design, Implement & Mange VPNs** 2.1. Virtual Private Network (VPN) Concepts and Technologies 2.2. Tunnel Mode, Transparent mode 2.3. Site-to-Site (IPSec) and Remote Access VPNs 2.4. IPsec, SSL, and MPLS VPNs 2.5. Tunnelling with Generic Routing Encapsulation (GRE) 2.6. Interesting traffic and Split Tunnelling	10	• Demonstrations: Configuring Site-to-Site VPN using IPSec. • Lab Exercises: VPN setup and split tunneling implementation. • Case Studies: Enterprise use cases for VPNs. • Hands-on Practice: Configuring VPNs on Cisco and OpenVPN.
• Classify different types of firewalls and their functionalities. • Understand firewall architectures and policies. • Implement DMZ, core, and perimeter firewall strategies. • Configure firewall objects, policies, and rule directions (ingress/egress). • Explore Next-Generation Firewalls (UTM, AV & IoT).	**3. Firewalls and Perimeter Security** 7.7 Types of Firewalls: Packet Filtering, Stateful Inspection, Application Layer 7.8 Web Application Firewall, Email Security Gateways 7.9 Firewall Architectures and Policies 7.10 Concept of Core, Edge or Perimeter and DMZ firewalls 7.11 Objects, policies and directions, egress, ingress policy rules 7.12 NAT and Virtual IP, concepts and use cases 7.13 Next Generation Firewalls (UTM, AV & IoT)	10	• Interactive Lectures: Firewall concepts and architectures. • Hands-on Labs: Configuring packet filtering and stateful firewalls. • Case Studies: Real-world firewall security breaches. • Practical Demonstrations: Implementing NAT and virtual IP use cases.

• Differentiate between IDS and IPS technologies. • Compare signature-based and anomaly-based detection techniques. • Analyze IDS/IPS deployment strategies in network security. • Understand inline and promiscuous models of IDS/IPS.	**4. Intrusion Detection and Prevention Systems (IDS/IPS)** 4.1 Introduction to IDS and IPS 4.2 Types of IDS/IPS, Inline and Promiscuous model of deployment 4.3 Signature-Based vs. Anomaly-Based Detection 4.4 IDS/IPS Deployment Strategies	**8**	• Lab Exercises: IDS/IPS deployment using SNORT. • Lectures: Understanding attack detection methodologies. • Simulation-Based Learning: Simulating real-time network attacks. • Practical Demonstrations: IDS vs IPS in real-time attack scenarios.
• Learn principles of secure network design. • Configure VLANs and DMZ for enhanced security. • Analyze secure wireless networking protocols (WPA, WPA2, WPA3). • Implement network segmentation strategies. • Understand zero-trust network architectures.	**5. Secured Wired and Wireless Network Systems and Architecture** 5.1 Principles of Secure Network Design 5.2 DMZ, VLANs, and Network Segmentation 5.3 Secure Network Topologies 5.4 WPA, WPA2, and WPA3 Security Protocols 5.5 Securing Wireless Networks 5.6 Two-Tiered and Three-Tiered Architecture 5.7 Zero Trust Networks	4	• Hands-on Labs: VLAN segmentation and DMZ configurations. • Workshops: Implementing WPA3 security on wireless networks. • Case Studies: Wireless security breaches and mitigation. • Group Discussions: The future of zero-trust security models.
• Understand best practices for network infrastructure hardening. • Apply configuration management for secure network systems.	**6. Hardening Network Infrastructure** 6.1 Applications of Hardening 6.2 Configuration of Hardening 6.3 Logging and Reporting 6.4 Best Practices and Industry Standards	4	• Demonstrations: Configuring logging and reporting tools. • Lab Exercises: Hardening network devices and access controls. • Case Studies: Real-world infrastructure attacks and defenses.

• Implement logging and reporting for security monitoring. • Follow industry standards and compliance guidelines.			• Practical Exercises: Implementing security baselines on network devices.
• Learn cloud security principles and risk-sharing models. • Implement virtualization security, audits, and compliance. • Secure cloud environments (AWS, Azure, GCP). • Understand network security groups and cloud security objects. • Analyze data center security technologies and planning.	**7. Concepts on Cloud Security and Virtualization** 7.1 Introduction to Cloud Technology, Cloud Security, Risk Sharing Modality 7.2 Virtualization Security, Audits and Compliance 7.3 Securing Cloud Environments (e.g. AWS, Azure, GCP) 7.4 Security Objects, Network Security Groups 7.5 Datacenter Technologies, Design and Planning	8	• Lectures: Cloud security concepts and compliance standards. • Hands-on Labs: Configuring security policies in AWS/Azure. • Case Studies: Cloud security incidents and mitigation. • Practical Demonstrations: Implementing network security groups in cloud environments.

Laboratory Works:

Network Design and Simulation, VLAN Configuration and Security, DHCP Security, DMZ segregation, IPsec configuration, IPS Configuration using NMAP, SNORT Applications, Firewall Objects and Policy Creations, Syslog Server Configurations for log management, Device access, control & Hardening.

References

1. Stallings, W. (2016). *Network security essentials: applications and standards*. Pearson.
4. Adkins, H., Beyer, B., Blankinship, P., Lewandowski, P., Oprea, A., & Stubblefield, A. (2020). *Building secure and reliable*

systems: best practices for designing, implementing, and maintaining systems. O'Reilly Media.

5. Coleman, D. D., Westcott, D. A., & Harkins, B. E. (2016). *CWSP Certified Wireless Security Professional Study Guide: Exam CWSP-205*. John Wiley & Sons.
6. Mather, T. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance.

Evaluation Schemes:

Chapter	1	2	3	4	5	6	7
Topics	All	All	All	All	All	All	All
Marks	10	10	10	8	10	4	8

*There may be a minor deviation in mark distribution.

Intelligent Networking (ENCTNS565) – (Elective I) Credits: 4

Level : M. Sc. Year : I

Program : MSNCS Part : II

Course Objectives

This course provides an in-depth exploration of intelligence in advanced and programmable networking technologies and protocols shaping the future of intelligent communication networks using machine learning. Topics include Intelligent network fundamentals, Intelligence in software-defined networking (SDN), Intelligence in Data Centric Networking/Intent Based Networking and Quantum networking through the application of artificial intelligence and machine learning in such latest networking technologies. The purpose of this course is to provide new knowledge on the latest generation networking technologies making it intelligent through the use of Artificial Intelligence and Machine Learning.

Learning Outcomes	**Chapter Contents**	**Credit hours**	**Teaching Methods**
□ Understand the evolution and fundamentals of intelligent networking. □ Differentiate between traditional and advanced networking technologies (SDN, IPv6, IBN, DCN, CDN). □ Grasp the basics of quantum and self-organizing networks. □ Apply cognitive networking concepts and recognize its applications. □ Analyze machine learning methods in networking contexts.	**1. Foundations of Intelligent Networking** 1.1. Evolution of intelligent networking 1.2. Overview of latest networking technologies: SDN, IPv6, IBN, DCN, CDN. 1.3. Overview of Quantum and Self Organization Networks 1.4. Fundamental of cognitive networking and its applications. 1.5. Basics of Machine Learning and AI in Networking 1.6. Supervised, Unsupervised, and Reinforcement Learning in Networking	8	□ Lectures: Overview of foundational concepts. □ Case Studies: Examples of advancements in intelligent networking. □ Interactive Discussions: Topics like cognitive networking and machine learning. □ Hands-On Tutorials: Basic implementation of machine

			learning techniques in networking scenarios. □ Paper presentations.
□ Analyze the architecture and advantages of SDN. □ Evaluate AI applications like QoS/QoE management and traffic prediction. □ Design AI-powered SDN controllers for data-driven decision-making. □ Explore AI-driven network security, anomaly detection, and cloud-edge integration.	**2. Intelligence in SDN** 2.1 Overview of SDN Architecture 2.2 Advantages of Integrating Intelligence in SDN 2.3 Adaptive QoS and QoE Management in SDN 2.4 Deep Learning Applications in SDN for Traffic Prediction and Classification 2.5 Intelligent NFV & Virtual Network Function (VNF) Placement 2.6 Design and Architecture of AI-Powered SDN Controllers 2.7 Data-Driven Decision Making in SDN Environments 2.8 Integration of SDN with Cloud and Edge Computing Architectures 2.9 AI-Driven Network Security in SDN 2.10 Anomaly Detection and Behavioral Analysis in SDN Environments	12	□ Lecture overview on each topic. □ Hands-On Labs: Working with SDN controllers and simulating traffic prediction. □ Problem-Solving Sessions: AI-driven SDN security scenarios. □ Group Projects: Design and architecture of AI-powered SDN controllers. □ Research Assignments: Exploring adaptive QoS and NFV placement. □ Paper presentations.
□ Workshops: Implementing AI-based cache placement techniques. □ Discussion Panels: Host-centric vs data-centric paradigms. □ Simulation Exercises: Dynamic caching and name-based routing. □ Mini-Projects: AI in secure content access and distribution.	**3. Data Centric Networking** 3.1 Overview and Concepts of DCN 3.2 Host-Centric vs Data-Centric Networking 3.3 Architectural concepts of Named Data Networking (NDN) 3.4 Benefits and Challenges of DCN 3.5 Applications of AI in DCN 3.6 AI-Based Cache Placement and Replacement Techniques 3.7 AI-Based Content Naming and Discovery Techniques	10	□ Lecture overview on each topic. □ Understand the shift from host-centric to data-centric networking. □ Identify AI-based techniques for cache management, content discovery, and secure distribution. □ Apply reinforcement learning for dynamic content caching. □ Paper presentations.

	3.8 Dynamic Content Caching Using Reinforcement Learning 3.9 AI-Driven Name-Based Routing Protocols 3.10 Secure Content Distribution and Access Control with AI		
□ Differentiate traditional networking from IBN. □ Apply machine learning for intent recognition and translation. □ Understand NLP's role in processing user-defined intents. □ Design network slicing strategies for 5G/6G integration.	**4. Intent-Based Networking (IBN)** 4.1 Overview of IBN Concepts and Architecture 4.2 Traditional Networking vs IBN 4.3 Benefits and Challenges of IBN 4.4 Machine Learning for Intent Recognition and Translation 4.5 Role of NLP in Intent Translation and Parsing 4.6 Understanding and Processing User-Defined Intents 4.7 Automated Threat Detection and Mitigation in IBN 4.8 Integration of SDN and NFV with Intelligent IBN 4.9 Concept of Network Slicing in 5G/6G with IBN	10	□ Lecture overview on each topic. □ Tutorials: NLP techniques for intent parsing. □ Collaborative Projects: IBN integration with SDN and NFV. □ Case Studies: Automated threat detection in IBN. □ Lectures and Demonstrations: Network slicing concepts. □ Paper presentations.
□ Explore quantum networking principles, including Qubits and entanglement. □ Analyze protocols like QKD and quantum teleportation. □ Evaluate security vulnerabilities in quantum networks. □ Understand quantum AI applications in traffic analysis.	**5. Quantum Networking** 5.1 Evolution from Classical to Quantum Networking 5.2 Classical vs Quantum Networks 5.3 Applications and Benefits of Quantum Networking 5.4 Overview of Quantum Bits (Qubits), Superposition and Entanglement 5.5 Quantum Communication Protocols: QKD protocol – BB84, Entanglement-Based QKD 5.6 Quantum Teleportation Protocols	10	□ Lecture overview on each topic. □ Interactive Lectures: Quantum protocols and their comparison with classical networks. □ Practical Sessions: Quantum communication protocol simulations. □ Group Discussions: Future applications of quantum AI.

	5.7 Quantum Link/Network/Transport Layer Protocol 5.8 Quantum Repeater Chains and Entanglement Distribution 5.9 Security Threats and Vulnerabilities in Quantum Networks 5.10 Quantum AI for Network Traffic Analysis and Anomaly Detection		□Research-Based Assignments: Study of quantum repeater chains. □ Paper presentations.
□ Predict trends in intelligent network automation and management. □ Develop strategies for self-optimizing and self-healing networks. □ Examine resource optimization techniques using ML. □ Analyze the role of blockchain in secure networking.	**6. Future Directions and Research Challenges in Network Intelligence** 6.1 Intelligent Network Monitoring, Automation and Management 6.2 Self-Configuring, Self-Optimizing and Self-Healing Networks 6.3 Resource Optimization and Scaling with ML Algorithms 6.4 AI-Based Load Balancing Algorithms in SDN 6.5 Dynamic Traffic Engineering and Load Balancing Using AI 6.6 Quantum Networking with SDN, NDN and IBN 6.7 Blockchain for Secure and Decentralized Networking 6.8 Emerging Trends and Open Research Challenges in Latest networking	10	□ Lecture overview on each topic. □ Hackathons: Resource optimization using AI. □ Seminars: Exploring blockchain and decentralized networking. □ Debates: Emerging trends vs established practices. □ Capstone Projects: Innovative solutions for intelligent network challenges.

Laboratory Works:

Students will engage in research based experimental activities in each chapter from 2 to 5.

References

1. Kaur, M., Jain, V., Nand, P., & Rakesh, N. (Eds.). (2024). *Software-Defined Network Frameworks: Security Issues and Use Cases*. CRC Press.
2. Ahmed, S. H., Bouk, S. H., & Kim, D. (2016). Content-centric networks: an overview, applications and research challenges.
3. Bassoli, R., Boche, H., Deppe, C., Ferrara, R., Fitzek, F. H., Janssen, G., & Saeedinaeeni, S. (2021). *Quantum communication networks* (Vol. 23, pp. 1-213). Berlin/Heidelberg, Germany: Springer.

Evaluation Schemes:

Chapter	1	2	3	4	5	6
Topics	All	All	All	All	All	All
Marks	8	12	10	10	10	10

*There may be a minor deviation in mark distribution.

Security and Privacy in Cloud Computing (ENCTNS 571) – (Elective II) Credits: 4

Level : M. Sc. Year : I

Program : MSNCS Part : II

Course Objectives

This course presents comprehensive introduction to cloud computing, cloud computing architecture, Cloud management, Security Management in the Cloud, Monitoring, Auditing and Management, Cloud security. It Focus on the Real-world goals for services provided by security and privacy in cloud Computing, the constrains on cloud computing infrastructure security and addresses regulatory compliance requirements critical to design, implement, deliver and manage secure cloud-based services.

Learning Outcomes	Chapter Contents	Credit Hours	Teaching Methods
• Understand the history and evolution of cloud computing. • Identify key features and service requirements of cloud computing. • Analyze cloud and dynamic infrastructure. • Evaluate the challenges of cloud computing.	**1 Introduction to cloud computing** 1.1. History of Cloud Computing 1.2. Features of cloud computing 1.3. Cloud services requirements 1.4. Cloud and dynamic infrastructure 1.5. Challenges of cloud computing	8	• Lectures: Introduction to cloud computing concepts and trends. • Case Studies: Real-world examples of cloud adoption. • Hands-on Labs: Exploring cloud platforms (AWS, Azure, GCP). • Group Discussions: Challenges and benefits of cloud adoption.
• Understand cloud computing characteristics and models (PaaS, SaaS, IaaS). • Compare different cloud deployment models (Public, Private, Hybrid, Community).	**2 Cloud Computing Architecture** Cloud computing Characteristics 2.1 Cloud reference model -platform as service 2.2 Software as a service, infrastructure as service 2.3 Cloud deployment models	12	• Lectures: Explanation of cloud models and architectures. • Lab Sessions: Implementing cloud environments in AWS or Azure. • Case Studies: Cloud adoption strategies for businesses.

• Design and implement cloud architecture using SOA principles. • Evaluate security, trust, and privacy in cloud environments.	2.3.1 Public clouds 2.3.2 Private clouds 2.3.3 Community cloud, hybrid clouds 2.4 Cloud design and implementation using SOA 2.5 Security, trust and privacy		• Hands-on Projects: Deploying applications on different cloud models.
• Understand security management standards for cloud computing. • Implement availability management for SaaS, PaaS, and IaaS. • Analyze access control mechanisms and security vulnerabilities. • Apply patch management and configuration best practices.	**3 Security Management in the Cloud** 3.1 Security Management Standards, 3.2 Security Management in the Cloud Availability Management, 3.3 SaaS Availability Management 3.4 PaaS Availability Management, 3.5 IaaS Availability Management, 3.6 Access Control, 3.7 Security Vulnerability 3.8 Patch, and Configuration Management	10	• Lectures: Security management frameworks (ISO 27001, NIST). • Workshops: Implementing access control in cloud environments. • Practical Demonstrations: Patch management in AWS/Azure. • Case Studies: Cloud security incidents and mitigation strategies.
• Understand the cloud-based information life cycle. • Apply data protection techniques for confidentiality and integrity. • Identify common attack vectors and threats in cloud environments. • Implement encryption, tokenization, PKI, and key management strategies. • Develop data retention, deletion, and archiving procedures.	**4 Data Privacy for Cloud Infrastructure and Services** 4.1 Cloud based Information Life Cycle 4.2 Data protection for Confidentiality and Integrity 4.3 Common attack vectors and threats 4.4 Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key 4.5 Management, Assuring data deletion 4.6 Data retention, deletion and archiving procedures for tenant data 4.7 Data Protection plan and Strategies.	12	• Hands-on Labs: Implementing encryption and data protection techniques. • Lectures: Cloud data privacy regulations and compliance. • Case Studies: Real-world breaches and data privacy failures. • Group Activities: Designing secure cloud storage strategies.
• erform proactive monitoring and incident response in cloud environments.	**5 Monitoring, Auditing and Management** 5.1 Proactive activity monitoring 5.2 Incident Response	12	• Lab Exercises: Implementing SIEM (Security Information and Event Management).

• Detect unauthorized access, malicious traffic, and privilege abuse. • Implement intrusion detection and security event management. • Audit logs and ensure tamper-proof security compliance. • Evaluate Quality of Service (QoS) and secure user management.	5.3 Monitoring for unauthorized access, malicious traffic, abuse of system privileges, intrusion 5.4 Detection, events and alerts auditing 5.5 Tamper-proofing audit logs 5.6 Quality of Services 5.7 Secure Management 5.8 User management 5.9 Identity management 5.10 Security Information and Event Management		• Lectures: Incident response planning and auditing best practices. • Simulations: Security breach and forensic investigation scenarios. • Hands-on Labs: Analyzing cloud security events in real-time.
• Identify security challenges and risks in cloud computing. • Implement security monitoring techniques for cloud-based applications. • Design security architecture for cloud deployments. • Apply data security and application security principles. • Implement identity management and access control for virtual environments.	**6 Cloud Security** Cloud Security challenges and Risks 6.1 Software-as-a-Service Security 6.2 Security Monitoring 6.3 Security Architecture Design 6.4 Data Security 6.5 Application Security 6.6 Virtual Machine Security 6.7 Identity Management and Access Control	6	• Lectures: Cloud security threats and risk management. • Workshops: Implementing identity management in cloud environments. • Practical Demonstrations: Configuring virtual machine security. • Case Studies: Cloud security failures and lessons learned.

Laboratory Activities:

1. Information Security Gap Assessment through ISO 27001
2. Cyber Security Maturity Assessment thorough NIST Cyber Security Framework.
3. IT Governance Audit through Control Objective for Related Technologies.
4. Develop IS Audit Terms of Reference
5. IS Audit Case Studies and Practical Exercises

References:

1. Vacca, J. R. (Ed.). (2013). *Network and system security*. Elsevier.
2. Subramanian, M., Gonsalves, T. A., & Rani, N. U. (2010). *Network management: principles and practice*. Pearson Education India.
3. Buyya, R., Vecchiola, C., & Selvi, S. T. (2013). *Mastering cloud computing: foundations and applications programming*. Newnes.
4. Mather, T. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance.
5. Mather, T. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance.

Evaluation Schemes:

Chapter	1	2	3	4	5	6
Topics	All	All	All	All	All	All
Marks	8	12	10	12	12	6

*There may be a minor deviation in mark distribution.

Year: 2nd **Part: 1st**

Semester III

S. No.	Teaching Schedule			Examination Schedule			Total	Remarks
	Course Code	Course Title	Credit	Assessment Marks	Final			
					Duration Hours	Marks		
1	CT	Project	4	40	3	60	100	
2	CT	Elective-III	4	40	3	60	100	
3	CT	Elective-IV	4	40	3	60	100	
Total			**12**	**120**		**180**	**300**	

Project:

It is an individual project to be developed by each student under the rules defined at academic guidelines of IOE

Generative AI and Security (ENCTNS 615) – (Elective III) Credits: 4

Level : M. Sc. Year : I

Program : MSNCS Part : II

Course Objectives

This course combines the principles of Generative AI with cybersecurity practices such as penetration testing, vulnerability analysis, threat intelligence, digital foot printing, and attack prevention. Students will explore how generative models enhance cybersecurity operations while mitigating their misuse in cyberattacks. Real-world scenarios and hands-on labs will prepare students to design both offensive and defensive cybersecurity strategies.

Learning Outcomes	Chapter Contents	Credit Hours	Teaching Methods
• Understand the fundamentals and historical evolution of Generative AI. • Differentiate between discriminative and generative models. • Explore deep learning basics such as neural networks and backpropagation. • Analyze generative learning techniques, including Bayesian learning and likelihood estimation. • Examine popular Generative AI models like GANs, VAEs, and Transformers (GPT, BERT). • Assess the impact of Generative AI on cybersecurity (both beneficial and harmful).	**1 Introduction to Generative AI [10 hours]** 1.1. Generative AI Overview and importance in technology. 1.2. Historical evolution of machine learning to generative models. 1.3. Key differences between discriminative and generative models. 1.4. Overview of deep learning basics (neural networks, backpropagation). 1.5. Generative learning: Probabilistic foundations (Bayesian learning, likelihood estimation). 1.6. Popular GenAI Models: Generative Adversarial Networks (GANs, Variational Autoencoders (VAEs) 1.7. Transformers: Self-attention mechanism, architecture, and their dominance (GPT). 1.8. Generative AI Model Developments: The evolution of transformer models (GPT, BERT, DALL-E), Diffusion models,	10	• Lectures: Overview of Generative AI and deep learning principles. • Case Studies: Evolution of GPT, BERT, and other AI models. • Hands-on Labs: Implementing a basic GAN for data synthesis. • Group Discussions: Ethical concerns and security risks of Generative AI.

	Hybrid models: Combining GANs and VAEs for cybersecurity tasks. 1.9. Interplay of AI and cybersecurity: Benefits and risks.		
• Understand how AI automates reconnaissance and target identification. • Explore OSINT tools powered by AI for digital footprint analysis. • Implement security measures to reduce attack surfaces and prevent AI-driven reconnaissance.	**2 Generative AI for Reconnaissance and Digital Foot printing** 2.1 AI-powered reconnaissance: Identifying targets using AI-driven OSINT tools. 2.2 Digital foot printing automation with generative models. 2.3 Preventive measures: Reducing attack surfaces and implementing secure configurations.	8	• Hands-on Labs: Using AI for reconnaissance and countermeasures. • Practical Demonstrations: Digital footprint automation with Generative AI. • Discussion Panels: Defensive measures against AI-powered attacks.
• Use Generative AI for automated exploit development and testing. • Enhance vulnerability scanning with AI-driven prioritization techniques. • Integrate AI tools in penetration testing workflows. • Implement defensive strategies, including system hardening and real-time monitoring.	**3 Penetration Testing and Vulnerability Analysis with AI** 3.1 Generative AI in automated exploit development and testing. 3.2 Vulnerability scanning and AI-driven prioritization. 3.3 AI tools for enhancing penetration testing workflows. 3.4 Defensive strategies: Patching, monitoring, and system hardening.	8	• Lab Exercises: AI-assisted penetration testing and vulnerability analysis. • Lectures: AI in ethical hacking and exploit generation. • Group Activities: Developing secure countermeasures against AI-driven attacks.
• Apply AI techniques for threat intelligence gathering. • Use Generative AI to predict adversarial behavior. • Detect anomalies in network traffic using ML models. • Counter AI-generated attacks with real-time monitoring solutions.	**4 Threat Intelligence and Anomaly Detection** 4.1 Using AI for threat intelligence gathering and analysis. 1.1. Generative models for adversarial behavior prediction. 1.2. Detecting anomalies using machine learning techniques. 1.3. Countering generative AI-based attacks with real-time monitoring tools	8	• Hands-on Labs: Implementing AI-based anomaly detection systems. • Case Studies: AI-powered threat intelligence in modern cybersecurity. • Simulation-Based Learning: Attack detection using machine learning models.
• Understand how Generative AI can craft phishing content and spear-phishing attacks.	**5 Social Engineering and Phishing Attacks** 5.1 Generative AI for phishing content generation and spear-phishing attacks.	6	• Lab Exercises: Simulating phishing attacks and countermeasures.

• Explore AI-driven social engineering tactics. • Implement defensive measures like email filtering, sandboxing, and user awareness training.	5.2 Crafting social engineering strategies with AI. 5.3 Defensive measures: Awareness training, email filtering, and sandboxing.		• Case Studies: Real-world AI-driven phishing incidents. • Role-Playing Scenarios: Understanding social engineering techniques.
• Understand AI-driven malware creation techniques, such as obfuscation and polymorphic malware. • Analyze Generative AI's role in wireless attacks (e.g., WPA cracking, spoofing). • Implement security measures like IDS, endpoint protection, and secure Wi-Fi configurations.	**6 Malware Development and Wireless Attacks** 6.1 AI in malware creation: Obfuscation, polymorphic malware, and evasion techniques. 6.2 Generative AI in wireless attacks (e.g., WPA cracking and spoofing). 6.3 Defense strategies: Secure Wi-Fi configurations, intrusion detection systems (IDS), and endpoint protection	8	• Hands-on Labs: AI-generated malware analysis and wireless security. • Practical Demonstrations: AI-driven evasion techniques. • Case Studies: Defense strategies against AI-assisted cyber threats.
• Learn how AI enhances security operations, SIEM systems, and SOC workflows. • Develop resilient AI security systems with adversarial robustness and secure coding practices. • Apply AI techniques in incident response and forensic investigations. • Understand risk management frameworks for AI security (NIST, ISO 27001).	**7 Advanced Security Operations and AI Risk Management** 7.1 Security operations and monitoring with AI: SIEM systems and SOC workflows. 7.2 Building resilient AI systems: Adversarial robustness and secure coding practices. 7.3 AI in incident response and forensics. 7.4 Frameworks for managing AI risks in cybersecurity (e.g., NIST, ISO 27001)**.**	8	• Workshops: Implementing AI-based security monitoring. • Lab Exercises: Adversarial robustness testing. • Group Discussions: AI in digital forensics and incident response.
• Predict the future of autonomous AI-driven cyberattacks. • Evaluate the ethical concerns and dual-use risks of Generative AI. • Understand legal and compliance considerations for AI in cybersecurity.	**8 Emerging Trends and Ethical Consideration** 8.1 Future attack scenarios: Autonomous AI-driven cyberattacks. 8.2 Ethical concerns: Dual-use AI and societal risks. 8.3 Legal and compliance considerations for generative AI in cybersecurity. 8.4 Preparing for quantum AI and post-quantum security challenges.	8	• Panel Discussions: Future cyber threats and ethical AI usage. • Lectures: Legal frameworks and compliance in AI security. • Debates: Balancing innovation with security and ethics.

• Prepare for quantum AI and post-quantum security challenges.			

Laboratory Works

1. Hands-on Labs: Building a simple GAN for data synthesis
2. Hands-on Lab: Using AI for reconnaissance and countermeasures.
3. Hands-on Lab: Conducting AI-assisted penetration tests.
4. Case Study: AI-powered threat detection systems.
5. Hands-on Lab: Simulating phishing and counter-phishing defenses.
6. Hands-on Lab: Analyzing AI-generated malware and securing wireless networks.
7. Project work: Design an AI-enabled system for cybersecurity (offensive or defensive). E.g. AI-driven threat detection tools, Generative phishing simulators for awareness training, A generative malware analyzer and defensive toolkit)

References

1. Foster, D. (2022). Generative Deep Learning. United States: O'Reilly Media.
2. Meeuwisse, R. (2017). Cybersecurity for Beginners. United Kingdom: Cyber Simplicity Limited.
3. Bengio, Y., Goodfellow, I., & Courville, A. (2017). *Deep learning* (Vol. 1). Cambridge, MA, USA: MIT press.
4. Soma, H., & Sinan, O. (2018). Hands-On Machine Learning for Cybersecurity. *Birmingham–Mumbai: Packt Publishing*.

Evaluation Schemes:

Chapter	1	2	3	4	5	6	7	8
Topics	All	All	All	All	All	All	All	All
Marks	10	8	8	8	8	8	8	4

*There may be a minor deviation in mark distribution.

***Elective IV: Detail course will be designed based on students' choice in the next semester.**

Year: II **Part: II**

Semester IV

S. No.	Teaching Schedule			Examination Schedule			Total	Remarks
	Course Code	Course Title	Credit	Internal Evaluation	Final			
					Duration Hours	Marks		
1	CT	Thesis	16	100			100	
Total			**16**					

*Thesis will be conducted as per the rules defined in academic guideline of IOE