Mandsaur University

Master of Technology (Computer Science and Engineering)

Semester-I

L-3 T-1 P-0 C-4

24CSE540 T: Information and network security

Course Objectives

- To give understanding the fundamentals of machine learning, its history, types, and common challenges.
- To learn building and evaluating supervised learning models using techniques like linear regression, SVMs, decision trees, and ensemble methods.
- To explore unsupervised learning techniques to discover patterns, clusters, and associations in data.
- To delve into advanced topics such as ensemble methods, neural networks, deep learning, NLP, and reinforcement learning.
- To learn the principles of genetic algorithms and apply them to solve optimization problems in machine learning.

Course Outcomes (COs): Upon completion of this unit students will be able to:

1. Understand the foundational principles of information security, including cryptographic methods and security policies.
2. Understand various network security protocols and their implementation to protect data over networks.
3. Evaluate risk assessment, and compliance with security standards.
4. Apply network security techniques, including intrusion detection and malware prevention.
5. Understand ethical hacking practices and cyber forensics, preparing them to identify and investigate security breaches.

Articulation Matrix

(Program Articulation Matrix is formed by the strength of correlation of COs with POs and PSOs. The strength of correlation is indicated as 3 for substantial (high), 2 for moderate (medium) correlation, and 1 for slight (low) correlation)

CO/PO/PSO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO1 2	PSO 1	PSO 2	PSO 3
CO1	1	1	-	3	-	-	-	-	-	-	-	-	1	1	-
CO2	2	3	1	-	-	-	-	-	-	-	-	-	2	3	-
CO3	3	1	-	-	3	-	-	-	-	-	-	-	3	2	-
CO4	1	-	2	-	-	-	-	-	-	-	-	-	2	3	2
CO5	2	-	-	-	3	-	-	-	-	-	-	-	3	1	1

High-3 Medium-2 Low-1

UNIT I: Fundamentals of Information Security **12 Hours**

Introduction to Information Security, Security Goals: Confidentiality, Integrity, Availability, Threats, Vulnerabilities, and Risks, Security Policies and Mechanisms, Cryptographic Techniques and Applications.

UNIT II: Network Security Protocols **12 Hours**

Overview of Network Security, IP Security (IPSec), Secure Socket Layer (SSL) and Transport Layer Security (TLS), Virtual Private Networks (VPNs), Wireless Security Protocols (WEP, WPA, WPA2).

UNIT III: Security Management and Risk Assessment **12 Hours**

Security Management Practices, Risk Assessment and Management, Security Auditing and Monitoring, Incident Response and Disaster Recovery, Security Standards and Compliance (ISO 27001, NIST).

UNIT IV: Advanced Topics in Network Security **12 Hours**

Intrusion Detection and Prevention Systems (IDS/IPS), Firewalls and Access Control, Malware Analysis and Prevention, Advanced Persistent Threats (APT), Security in Cloud Computing.

UNIT V: Ethical Hacking and Cyber Forensics **12 Hours**

Ethical Hacking: Tools and Techniques, Penetration Testing Methodologies, Social Engineering Attacks, Cyber Forensics: Data Collection and Analysis, Legal and Ethical Issues in Cyber Security.

Total: 60 Hours

References

1. " Peterson, L. L. and Davie, B. S. (1996) *Computer Networks: A Systems Approach*, Morgan Kaufmann.
2. Principles of Information Security - Michael E. Whitman and Herbert J. Mattord, 2nd
3. Edition, Thompson, 2005.
4. Network Security Essentials Applications and Standards - William Stallings, Person
5. Education, 2000.
6. Cryptography and Network Security - Behrouz A. Forouzan, Tata McGraw-Hill, 2007.
7. " King, T. and Newson, D. (1999) *Data Network Engineering*, Kluwer.
8. " RFC 2401 (1998) *Security Architecture for the Internet Protocol*, Kent, S., Atkinson, R.
9. " Stallings, W (1999) *Cryptography and Network Security*, Prentice Hall.
10. " Stallings, W (2001) *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, 3rd edn, Addison Wesley.
11. " Network Security: The Complete Reference Roberta Bragg, Mark Rhodes-Ousley, Keith Strassberg McGraw-Hill Education, 2004.
12. " Ellis, J. and Speed, T. (2001) *The Internet Security Guidebook*, Academic Press.
13. " SO/IEC 17799 (2000) *Information Technology – Code of Practice for Information Security Management,* International Organization for Standardization.
14. Tanenbaum, A. S. (1996) *Computer Networks*, 3rd edn, Prentice Hall.

List of e-Learning Resources:

1. Introduction to network security - Course (nptel.ac.in)
2. https://www.coursera.org/
3. https://alison.com/tag/network-security

Subject Tr. **Academic Coordinator** **HoD** **Sr. Faculty Nominated by DOAA**

Mandsaur University

Master of Technology (Computer Science and Engineering)

Semester-I

L-0T-0P-2C-1

24CSE550 P**:** Advanced Computer Networks

Course Objectives

- Learn about advanced concepts and next generation networks
- Analyze the functionalities of network algorithms, protocols, and TCP/IP variants
- Understand the features of SDN and its application to next generation systems
- Analyze the performance of various server implementations
- Understand the principles of computer networking theory, including the protocols designed for the application layer, transport layer, network layer, and link layer
- Understand the fundamental ideas that underlie the design of large-scale distributed computer networks
- Learn how to do networking systems research and Understand different routing protocols
- Understand the services and network management being offered

Course Outcomes (COs): Upon completion of this unit students will be able to:

1. Understand how to demonstrate working knowledge of key networking technologies and how they interact
2. Apply techniques to collect and analyze the performance of various server implementations.
3. Create ,analyze and design Internet Routing Architectures.
4. Apply how to design simulations and experiments to demonstrate how network technologies and algorithms work.
5. Analyze network algorithms, protocols, and their functionalities, including TCP/IP variants.

Articulation Matrix

(Program Articulation Matrix is formed by the strength of correlation of COs with POs and PSOs. The strength of correlation is indicated as 3 for substantial (high), 2 for moderate (medium) correlation, and 1 for slight (low) correlation)

CO/PO/PSO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	-	1	-	-	1	-	-	-	-	-	1	1	-
CO2	2	3	1	-	2	-	-	-	-	-	-	-	2	1	-
CO3	1	1	-	-	3	-	-	-	-	-	-	-	2	2	-
CO4	2	-	2	-	-	1	-	-	-	-	-	-	2	3	2
CO5	1	-	2	2	3	1	-	-	-	-	-	-	3	1	1

High-3 Medium-2 Low-1

List of Practical's

Experiment 1: Network Simulation with NS-3 **Hour : 6 hours**

Set up a simple network topology using the NS-3 simulator. Implement different routing protocols (e.g., OSPF, BGP) and analyze their performance.

Experiment 2: QoS Configuration in a Network **Hour : 6 hours**

Configure Quality of Service (QoS) settings on a network to prioritize different types of traffic (e.g., VoIP, video streaming). Measure the impact on latency, jitter, and packet loss.

Experiment 3: Implementing SDN with Mininet **Hour : 6 hours**

Use Mininet to create a software-defined network (SDN) and implement a custom OpenFlow controller to manage traffic flows dynamically.

Experiment 4: Securing a Wireless Network **Hour : 6 hours**

Set up a wireless network using WPA2 encryption. Perform penetration testing using tools like Aircrack-ng to identify vulnerabilities and implement security measures to mitigate them.

Experiment 5: Virtual Private Network (VPN) Setup **Hour : 6 hours**

Configure a VPN using OpenVPN. Measure and analyze the performance impact on data transmission in terms of speed and security.

Experiment 6: Intrusion Detection System (IDS) Configuration **Hour : 6 hours**

Install and configure an IDS (e.g., Snort) on a network. Simulate various attack scenarios and analyze the IDS's ability to detect and log these attacks.

Experiment 7: Voice over IP (VoIP) Implementation **Hour : 6 hours**

Set up a basic VoIP system using Asterisk or another VoIP server. Measure call quality and bandwidth usage under different network conditions.

Experiment 8: Multimedia Streaming Protocols **Hour : 6 hours**

Implement a multimedia streaming server using protocols like RTP/RTSP. Analyze the performance in terms of latency and buffering under varying network conditions.

Experiment 9: Network Traffic Analysis with Wireshark **Hour : 6 hours**

Use Wireshark to capture and analyze network traffic. Identify different types of traffic, protocols used, and any potential security issues.

Experiment 10: Implementing IoT Network with MQTT **Hour : 6 hours**

Set up an IoT network using MQTT protocol. Connect multiple IoT devices and measure the performance and reliability of data transmission.

Total: 60 Hours

References:

1. **Rambaugh , Object Oriented Modeling and Design with UML , Pearson Edu.**
2. **Simon Bennett, Steve McRobb and Ray Farmer, Object Oriented system Analysis and Design Using UML, TMH**
3. **Docherty , Object Oriented Analysis & Design with UML , Wiley India**
4. **Ivar Jacobson, Patrik Jonsson: ,Object – Oriented Software Engineering , Pearson.Edu**

List of E-Learning Resources :

1. **Advance Computer Network: nptel.ac.in/noc.**
2. **https://www.coursera.org/**

Subject Tr. **Academic Coordinator** **HoD** **Sr. Faculty Nominated by DOAA**

Mandsaur University

Master of Technology (Computer Science and Engineering)

Semester-I

L-0 T-0 P-6 C-3

24CSE570 P: Web and mobile Application Development Laboratory

Course Objectives

- Develop Proficiency in Front-End Technologies
- Implement Back-End Integration and Data Handling
- Apply Mobile Development Frameworks and Tools.
- Enhance Application Usability and User Experience (UX).
- Implement Security Measures and Best Practices.

Course Outcomes (COs): Upon completion of this unit students will be able to:

1. Create responsive and dynamic web applications using HTML, CSS, and JavaScript.
2. Apply server-side scripting and RESTful API in Node.js and Express.js.
3. Create cross-platform mobile applications using frameworks like React Native and Ionic.
4. Understand integration of cloud services like Firebase and setting up continuous deployment pipelines.
5. Apply performance testing and optimize the user experience for web and mobile applications.

Articulation Matrix

(Program Articulation Matrix is formed by the strength of correlation of COs with POs and PSOs. The strength of correlation is indicated as 3 for substantial (high), 2 for moderate (medium) correlation, and 1 for slight (low) correlation)

CO/PO/PSO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	1	1	-	3	-	-	-	-	-	-	-	-	1	2	-
CO2	3	2	-	-	-	-	-	-	-	1	-	-	3	1	-
CO3	2	1	-	-	3	-	-	-	-	-	-	-	2	2	-
CO4	1	-	2	-	-	-	-	-	-	-	-	-	1	3	2
CO5	3	-	-	-	2	-	-	-	-	-	-	-	3	1	1

High-3 Medium-2 Low-1

1. **Responsive Web Design** **6 Hours**
   Develop a responsive website using HTML, CSS, and Bootstrap that adapts to different screen sizes (desktop, tablet, mobile).
2. **Client-Side Scripting** **6 Hours**
   Create a dynamic web page using JavaScript and jQuery to validate user inputs and manipulate the Document Object Model (DOM).
3. **Server-Side Scripting with Node.js** **6 Hours**
   Build a simple web server using Node.js that serves static content and handles basic HTTP requests and responses.
4. **RESTful API Development** **6 Hours**
   Develop a RESTful API using Express.js and Node.js, allowing clients to perform CRUD (Create, Read, Update, Delete) operations on a database.
5. **Experiment 5 Single Page Application (SPA) with Angular** **6 Hours**
   Create a Single Page Application using Angular. Implement routing, data binding, and form validation.
6. **Mobile App Development with React Native** **6 Hours**
   Develop a cross-platform mobile application using React Native. Implement basic navigation and state management.
7. **Hybrid Mobile App with Ionic** **6 Hours**
   Build a hybrid mobile application using the Ionic framework. Incorporate native device

features like camera and geolocation.

8. **Firebase Integration** **6 Hours**
   Integrate Firebase with a mobile application to handle user authentication and real-time database operations.
9. **Progressive Web App (PWA)** **6 Hours**
   Convert an existing web application into a Progressive Web App by adding service workers and a web app manifest for offline functionality.
10. **Deployment and Continuous Integration** **6 Hours**
    Deploy a web application to a cloud platform like Heroku or AWS. Set up a continuous integration pipeline using tools like Jenkins or GitHub Actions to automate the deployment process.
11. Project Title: **"Smart City Services Hub"** **30 Hours**
    Project Summary - The "Smart City Services Hub" is a web and mobile application designed to provide city residents with a centralized platform for accessing essential services. This includes emergency services, utility bill payments, public transport information, and community announcements. The project focuses on backend and frontend development, data management, and user experience across platforms.

Total: 90 Hours

References

1. Web Development and Design Foundations with HTML5, Terry Felke-Morris
2. Mobile Application Development: Android and iOS, Valentino Lee, Heather Schneider, and Robbie Schell.
3. Powell T. (2010). HTML & CSS: The Complete reference. 5th edition. McGraw Hill Education.
4. Web Technologies: HTML, JavaScript, PHP, Java, JSP, ASP.net, XML and AJAX Black Book. Kogent Learning Solutions Inc., Dreamtech Press.
5. Pollock P. (2013). Web Hosting for Dummies. Wiley Publishing Inc.
6. Ledford J. (2008). SEO: Search Engine Optimization Bible. Wiley Publishing Inc.
7. Learning Web App Development, Semmy Purewal.

List of e-Learning Resources:

4. Android Mobile Application Development (nptel.ac.in)
5. https://www.coursera.org/

Subject Tr. **Academic Coordinator** **HoD** **Sr. Faculty Nominated by DOAA**

Mandsaur University

Master of Technology (Computer Science and Engineering)

Semester-I

L-3 T-1 P-0 C-4

24CSE540 T: Information and network security

Course Objectives

- To give understanding the fundamentals of machine learning, its history, types, and common challenges.
- To learn building and evaluating supervised learning models using techniques like linear regression, SVMs, decision trees, and ensemble methods.
- To explore unsupervised learning techniques to discover patterns, clusters, and associations in data.
- To delve into advanced topics such as ensemble methods, neural networks, deep learning, NLP, and reinforcement learning.
- To learn the principles of genetic algorithms and apply them to solve optimization problems in machine learning.

Course Outcomes (COs): Upon completion of this unit students will be able to:

6. Understand the foundational principles of information security, including cryptographic methods and security policies.
7. Understand various network security protocols and their implementation to protect data over networks.
8. Evaluate risk assessment, and compliance with security standards.
9. Apply network security techniques, including intrusion detection and malware prevention.
10. Understand ethical hacking practices and cyber forensics, preparing them to identify and investigate security breaches.

Articulation Matrix

(Program Articulation Matrix is formed by the strength of correlation of COs with POs and PSOs. The strength of correlation is indicated as 3 for substantial (high), 2 for moderate (medium) correlation, and 1 for slight (low) correlation)

CO/PO/PSO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	1	1	-	3	-	-	-	-	-	-	-	-	1	1	-
CO2	2	3	1	-	-	-	-	-	-	-	-	-	2	3	-
CO3	3	1	-	-	3	-	-	-	-	-	-	-	3	2	-
CO4	1	-	2	-	-	-	-	-	-	-	-	-	2	3	2
CO5	2	-	-	-	3	-	-	-	-	-	-	-	3	1	1

High-3 Medium-2 Low-1

UNIT I: Fundamentals of Information Security **12 Hours**

Introduction to Information Security, Security Goals: Confidentiality, Integrity, Availability, Threats, Vulnerabilities, and Risks, Security Policies and Mechanisms, Cryptographic Techniques and Applications.

UNIT II: Network Security Protocols **12 Hours**

Overview of Network Security, IP Security (IPSec), Secure Socket Layer (SSL) and Transport Layer Security (TLS), Virtual Private Networks (VPNs), Wireless Security Protocols (WEP, WPA, WPA2).

UNIT III: Security Management and Risk Assessment **12 Hours**

Security Management Practices, Risk Assessment and Management, Security Auditing and Monitoring, Incident Response and Disaster Recovery, Security Standards and Compliance (ISO 27001, NIST).

UNIT IV: Advanced Topics in Network Security **12 Hours**

Intrusion Detection and Prevention Systems (IDS/IPS), Firewalls and Access Control, Malware Analysis and Prevention, Advanced Persistent Threats (APT), Security in Cloud Computing.

UNIT V: Ethical Hacking and Cyber Forensics **12 Hours**

Ethical Hacking: Tools and Techniques, Penetration Testing Methodologies, Social Engineering Attacks, Cyber Forensics: Data Collection and Analysis, Legal and Ethical Issues in Cyber Security.

Total: 60 Hours

References

15. " Peterson, L. L. and Davie, B. S. (1996) *Computer Networks: A Systems Approach*, Morgan Kaufmann.
16. Principles of Information Security - Michael E. Whitman and Herbert J. Mattord, 2nd
17. Edition, Thompson, 2005.
18. Network Security Essentials Applications and Standards - William Stallings, Person
19. Education, 2000.
20. Cryptography and Network Security - Behrouz A. Forouzan, Tata McGraw-Hill, 2007.
21. " King, T. and Newson, D. (1999) *Data Network Engineering*, Kluwer.
22. " RFC 2401 (1998) *Security Architecture for the Internet Protocol*, Kent, S., Atkinson, R.
23. " Stallings, W (1999) *Cryptography and Network Security*, Prentice Hall.
24. " Stallings, W (2001) *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, 3rd edn, Addison Wesley.
25. " Network Security: The Complete Reference Roberta Bragg, Mark Rhodes-Ousley, Keith Strassberg McGraw-Hill Education, 2004.
26. " Ellis, J. and Speed, T. (2001) *The Internet Security Guidebook*, Academic Press.
27. " SO/IEC 17799 (2000) *Information Technology – Code of Practice for Information Security Management,* International Organization for Standardization.
28. Tanenbaum, A. S. (1996) *Computer Networks*, 3rd edn, Prentice Hall.

List of e-Learning Resources:

6. Introduction to network security - Course (nptel.ac.in)
7. https://www.coursera.org/
8. https://alison.com/tag/network-security

Subject Tr. **Academic Coordinator** **HoD** **Sr. Faculty Nominated by DOAA**