CYBER SECURITY

COURSE CONTENTS:

1- SECURITY CHALLANGES IN AI SYSTMES

a. Challenges of Securing Information in AI
b. Information Security and Controls

- AAA
- PPP

- CIA
- Basic three controls

c. Attacks and Defenses

2- SECURITY THREATS AND VULNERABILITIES

a. **Common Security Threats**

- Overview of Common Threats:
  - Malware (viruses, worms, trojans)
  - Phishing Attacks
  - Denial-of-Service (DoS) Attacks
  - Man-in-the-Middle Attacks

b. Understanding Vulnerabilities

- Definition of Vulnerabilities
- Common Software and System Vulnerabilities:
  - Outdated Software
  - Weak Passwords
  - Lack of Encryption

- Misconfigured Security Settings

c. Real-World Examples

- Briefly discuss recent cybersecurity incidents or breaches
- Highlight the impact of security lapses

d. Protective Measures

Introduction to Protective Measures:

i. Regular Software Updates
ii. Strong Authentication Practices
iii. Encryption Best Practices
iv. Security Awareness Training

e. social engineering psychological attacks
f. physical social engineering attacks
g. different types of server-side web application attacks
h. client-side attacks
i. Types of social media & networking services
j. Risk assessment
k. Safe use of internet/social media - precautions/ practices

3- DIGITAL CERTIFICATES

a. Install a Certificate Authority (CA) Hierarchy
b. Enroll Certificates
c. Secure Network Traffic by Using Certificates
d. Renew Certificates
e. Revoke Certificates
f. Back Up and Restore Certificates and Private keys
g. Restore Certificates and Private keys

4- NETWORK SECURITY

a. Types of network security devices and how they can be used
b. Security enhancement through network Technologies
c. Secure network design elements
d. Network Protocols (ICMP, SNMP, DNS, FTP, TELNET, IPV6)
e. Network Administration Principles

5. MOBILE SECUIRTY

a. Types of Mobile Devices
b. Mobile Device Security
c. Mobile Device App Security
d. BYOD Security

6- **ACCESS CONTROL AND MITIGATION OF AI SYSTEMS**

a. Access control and access control models
b. Authentication Services
c. Authentication credentials
d. Single sign on
e. Account management