IS383 Secure Intelligent Systems

Credit Hours:	2-1-3	**Prerequisites**	Nil

Course Learning Outcomes:

S No	CLO	Domain	Taxonomy Level	PLO
1.	Know various AI search algorithms (tree search, uninformed, informed, and heuristic), understand different types of AI agents, know how to build simple knowledge-based secure intelligent systems	Cognitive	2	1
2.	Apply basic principles of AI in security solutions that require problem solving, inference, perception, knowledge representation, and learning	Cognitive	3	3
3.	Analyze various cyber security applications of AI techniques in intelligent agents, expert systems, artificial neural networks and other machine learning models	Cognitive	4	2
4.	Implement scientific method to models of machine learning in information security	Psychomotor	3	5

Course Content:

An introduction to the basic principles, techniques, and applications of Artificial Intelligence. Coverage includes knowledge representation, logic, inference, problem solving, search algorithms, game theory, perception, learning, planning, and agent design. Students will experience programming in AI language tools. Potential areas of further exploration include expert systems, neural networks, fuzzy logic, robotics, natural language processing, and computer vision. Identify and predict security threats using artificial intelligence, Develop intelligent systems that can detect unusual and suspicious patterns and attacks, Learn how to test the effectiveness of AI cybersecurity algorithms and tools.

Teaching Methodology:

Lectures, Written Assignments, Semester Project, Presentations

Course Assessment:

Midterm Exam, Home Assignments, Quizzes, Project, Presentations, Final Exam

Reference Materials:

1. S. J. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, Prentice-Hall.
2. Koller and Friedman. Probabilistic Graphical Models.
3. Sutton and Barto. Reinforcement Learning: An Introduction.
4. Hastie, Tibshirani, and Friedman. The elements of statistical learning.
5. Parisi Alessandro., Hands-On: Artificial Intelligence for Cyber Security.
6. Kumar, G., Kumar, D: AI Elementary to Advanced Practices, Cyber Defence Mechanisms, Security, Privacy and Challenges

In addition there will be lecture notes and selected articles.