

CCY4303 AI in Cybersecurity**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY2001 and CAI3101	4	8	2	2	--	3

COURSE AIM

To get the students to:

- Learn how to make use of AI techniques to solve cybersecurity problems.
- Know the principles of AI and different neural network architectures
- Understand how to detect spam, phishing, malware threats, and network anomalies through AI
- Understand attacks and defenses for Generative Adversarial networks
- Understand how to use machine learning for fraud detection
- Experiment with detecting patterns and model behavior and identifying anomalous behavior

COURSE WEEKLY CONTENTS

- 1 Course Aim, Course outline, and the principles of artificial intelligence, concentrating on cybersecurity-related applications
- 2 Different cryptographic techniques and some major attacks
- 3 Neural network architectures such as ANN, CNN, and GAN
- 4 Detecting Spams with AI techniques
- 5 Detecting Phishing with AI techniques.
- 6 Detecting Phishing with AI techniques (cont.)
- 7 7th week Assessment
- 8 Malware Threats detection
- 9 Network Anomalies detection
- 10 Machine Learning for fraud detection
- 11 12th week Assessment
- 12 Evaluating AI algorithms
- 13 GANs: Attacks and Defences
- 14 GANs: Attacks and Defences (cont.)
- 15 Projects Presentations

STUDENT GRADING & ASSESSMENT

Weeks	Exams	Assign.	Quizzes	Reports	Present.	Lab.	Total
1 to 7	←		30	MARKS		→	30
8 to 12	←		20	MARKS		→	20
1 to 15	←		10	MARKS		→	10
16 or 17			Final Exam				40

REFERENCES

Textbook Alessandro Parisi, Hands-on Artificial Intelligence for Cybersecurity: Implement Smart AI Systems for Preventing Cyber Attacks and Detecting Threats and Network Anomalies, Packt Publishing