QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Study plan No.	**2024/2025**		**University Specialization**	**Cybersecurity**	
Course No.	**0133328**		**Course name**	**Artificial Intelligence in Cybersecurity**	
Credit Hours	**3**		**Prerequisite Co-requisite**	**0133325**	
Course type	☐ MANDATORY UNIVERSITY REQUIREMENT	☐ UNIVERSITY ELECTIVE REQUIREMENTS	☐ FACULTY MANDATORY REQUIREMENT	☐ Support course family requirements	☐ **Mandatory requirements** ☐ **✓Elective requirements**
Teaching style	☐ **Full online learning**		☐ Blended learning		☐ ✓Traditional learning
Teaching model	☐ 2Synchronous: 1asynchronous		☐ 2 face to face : 1synchronous		☐ ✓3 Traditional

Faculty member and study divisions information (to be filled in each semester by the subject instructor)

Name	Academic rank	Office No.	Phone No.	E-mail	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

The course aims to explore fundamental techniques of artificial intelligence (AI) and machine learning (ML) and its role in cybersecurity. Students will implement different AI and ML techniques to detect threats, identify anomalies in networks, prevent cyberattacks in order to improve cybersecurity.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber-attacks and detecting threats and network anomalies, Alessandro Parisi, August 2, 2019.			
Supportive learning resources (Books, databases, periodicals, software, applications, others)	1. McKinney, W Brij B. Gupta and Quan Z. Sheng.(2019). Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices. 2. T. Dunning and E. Friedman, Practical Machine Learning - A New Look at Anomaly Detection, O'Reilly, 1st edition, 2014. 3. Ian Goodfellow, Yoshua Bengio, Aaron Courville, Deep Learning, MIT Press, 2016.			
Supporting websites				
The physical environment for teaching	☐ **✓ Class room**	☐ labs	☐ **Virtual educational platform**	☐ Others
Necessary equipment and software				
Supporting people with				

special needs	
For technical support	**E-learning and Open Educational Center. Computer Center**

Course learning outcomes (S= *Skills, C= Competences K= Knowledge,)*

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Understanding varies AI and Machine Learning Techniques	**MK1**
K2	Understand different aspects of Cybersecurity.	**MK2**
	Skills	
S1	Apply different Machine Learning Techniques in Cybersecurity Problems	**MS1**
S2	Analyze various Feature extraction and reduction techniques	**MS2**
S3	Implement various AI based security tools	**MS1**
	Competences	
C1	Develop AI and machine learning techniques for Cybersecurity solutions	**MC1**
C2	Evaluate the performance of various Machine Learning algorithms in Real time network environments	**MC1**

Mechanisms for direct evaluation of learning outcomes

Type of assessment / learning style	Fully electronic learning	Blended learning	Traditional Learning (Theory Learning)	Traditional Learning (Practical Learning)
First exam	0	0	0	**0**
Second / midterm exam	%30	%30	%30	**%30**
Participation / practical applications	0	0	0	**0**
Asynchronous interactive activities	%30	%30	%30	**%30**
final exam	%40	%40	%40	**%40**

Note: Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, work within student groups ... etc, which the student carries out on his own, through the virtual platform without a direct encounter with the subject teacher.

Schedule of simultaneous / face-to-face encounters and their topics

Week	Subject	learning style*	Reference **
1	Introduction to Data Mining and Machine Learning	**Lecture**	**Lecture notes**
2	Cybersecurity attacks and solutions	**Lecture**	**Lecture notes**
3	Fundamentals of Supervised and Unsupervised Machine Learning algorithms	**Lecture**	**Lecture notes**
4	Feature Selection and Feature Extraction	**Lecture**	**Lecture notes**

	Methods		
5	Feature Selection and Feature Extraction Methods	**Lecture**	**Lecture notes**
6	Network Anomaly Detection Methods and Requirements	**Lecture**	**Lecture notes**
7	Anomaly Detection Using Unsupervised Learning	**Lecture**	**Lecture notes**
8	Midterm Exam		
9	Anomaly Detection Using Probabilistic Learning	**Lecture**	**Lecture notes**
10	Anomaly Detection Using Soft Computing	**Lecture**	**Lecture notes**
11	Knowledge base systems in Anomaly Detection. Anomaly Detection Using Combination Learners.	**Lecture**	**Lecture notes**
12	AI based network intrusion detection system evaluation methods	**Lecture**	**Lecture notes**
13	Applications of Machine learning in scan detection and Network traffic analysis	**Lecture**	**Lecture notes**
14	Applications of Machine learning in malware analysis	**Lecture**	**Lecture notes**
15	Tools and Systems	**Lecture**	**Lecture notes**
16	Final Exam		

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**
**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

This activities was designed using the **Project-Based Learning (PBL)**

Project : Evaluation of AI-Based NIDS and ML in Scan Detection

Field / Task / Activity	Reference	Expected Results
1. Dataset Preparation & Feature Engineering: - Source CIC-IDS2017/UNSW-NB15 dataset	Sharafaldin et al. (2018). CIC-IDS2017 dataset paper Scikit-learn preprocessing documentation	1. Cleaned, normalized dataset 2. Feature importance analysis report

Field / Task / Activity	Reference	Expected Results
- Extract flow features (duration, protocol, packet size stats) - Normalize data and apply PCA for dimensionality reduction		3. Reduced dimension feature set
2. Unsupervised Model Implementation: - Build Autoencoder neural network - Train on normal traffic only - Use reconstruction error as anomaly score	TensorFlow/PyTorch Autoencoder tutorials Chandola et al. (2009) anomaly detection survey	1. Trained Autoencoder model 2. Reconstruction error distribution plots 3. Anomaly threshold determination
3. Probabilistic Model Implementation: - Implement Gaussian Mixture Model (GMM) - Fit to normal traffic distribution - Flag low-probability samples as anomalies	Scikit-learn GMM documentation Bishop (2006) Pattern Recognition book	1. Trained GMM with optimal components 2. Probability density function plots 3. Anomaly probability scores
4. Hybrid System Design: - Create knowledge-based rules combining both models - Design decision logic (e.g., "IF Autoencoder error > X AND GMM prob < Y THEN alert")	Rule-based system literature Expert system design principles	1. Rule specification document 2. Hybrid decision algorithm 3. Confidence scoring mechanism

Field / Task / Activity	Reference	Expected Results
5. Evaluation & Comparison: - Test on attack-included dataset - Calculate Precision, Recall, F1, ROC-AUC - Compare model performance across attack types	ML evaluation metrics literature Confusion matrix analysis methods	1. Performance comparison table 2. ROC curves for both models 3. False positive/negative analysis

Week	Task / activity	Reference	Expected results
1			
2			
3			
4			
5			
6			
7			
8			