Module Specification

Data Science for Cyber Security

Version: 2024-25, v1.0, 24 Jan 2024

Contents

Part 1: Information

Module title: Data Science for Cyber Security

Module code: UFCE8B-30-2

Level: Level 5

For implementation from: 2024-25

UWE credit rating: 30

ECTS credit rating: 15

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

Partner institutions: None

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: In our modern technological society, data is gathered and stored for a variety of applications. Many security, and cyber-security, applications are beginning to utilise the large volumes of data that now exist, in order to allow security analysts to make well-informed decisions that relate to the organisations, the assets, and the people, that they are tasked with protecting.

This module is designed to take a modern data-driven approach to security analysis.

With this, large volumes of data can be effectively managed to better support security analysts in their tasks of understanding and reasoning about the current state of their security.

From computer network traffic analysis to user behavioural analytics, we shall consider the variety of different data sources that can be processed, and utilised, in modern security applications.

Features: Not applicable

Educational aims: With practical assignments and coursework that allow students to develop their own tools for conducting such analytics, this course offers would-be analysts the ability to manipulate, visualize, and learn from, ever-growing large datasets.

Outline syllabus: Introduction to data science and programming for data science
Data Science workflows
Statistical analysis
Time series analysis and anomaly detection
Machine Learning methods
Supervised learning and classification
Unsupervised learning and clustering
Autoencoders and self-supervised learning
LSTM and Transformers
NLP methods and LLMs
Image and video based methods
Visualisation methods
Visual Analytics
Interaction methods

Cyber Security Data Science
Data types in Cyber Security
Real time / stream-based learning
Security Information and Event Management
A set of case studies for example,
Malware analysis,

Network traffic and IDS

Social media analysis

Insider threat detection

IoT

CAV

Part 3: Teaching and learning methods

Teaching and learning methods: Teaching will consist of 1 one-hour session each week, where the core module content will be taught via lectures and in-class discussion. In addition, there will be 1 two-hour lab session each week, where students can develop the ideas and concepts that have been discussed in lectures through practical worksheets.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 To demonstrate understanding of programming for the purposes of data science in cyber security

MO2 To demonstrate practical skills of gathering, processing and analysing data to solve cyber security challenges

MO3 To reflect upon techniques and methods used and evaluate their performance

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 228 hours

Lectures = 24 hours

Total = 300

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://rl.talis.com/3/uwe/lists/C37A4F72-0BDF-268A-45CD-DBEB76C7C735.html?lang=en&login=1

Part 4: Assessment

Assessment strategy: The assessment of this module consists of a project portfolio. In the portfolio, students will complete a series of practical lab exercises that cover key topics from the module. Students will be expected to write suitable program code that provides a practical solution to each challenge, and should be able to provide a written narrative of how they solved each task that demonstrates understanding and critical reflection of their work.

Resit strategy.
In the cases where a resit is required, students will be tasked with a set of similar exercises to that of the main run, however, using different data sets. This will enable students to focus on the methodology of solving the tasks programmatically, despite working with different data sets to that of the main run.

Assessment tasks:

Portfolio (First Sit)
Description: A series of practical tasks that form a portfolio of work
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Portfolio (Resit)
Description: A series of practical tasks that form a portfolio of work
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2023-24

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2023-24

Cyber Security and Digital Forensics {Foundation} [Frenchay] BSc (Hons) 2022-23

Computer Security and Forensics {Foundation} [GCET] BSc (Hons) 2022-23