Modulhandbuch

Wahlpflichtmodule zum Ba. Studiengang Informatik (B.Sc.)

Hochschule Landshut
gültig ab dem Sommersemester 2023

beschlossen am 31. Januar 2023

Inhaltsverzeichnis

Auflistung aller angebotenen Wahlpflichtmodule

FWP-Modul	SS	WS	Sem.	Ansprechpartner/ Dozent	Nr.	Sprache
Internet of Things	✓		4.	Prof. Dr. Khelil	IB764	Englisch
Innovationslabor IoT Projekt	✓	✓	ab 3.	Prof. Dr. Khelil	IB765	Deutsch (Englisch)[1]
Einführung in die digitale Forensik	✓		4.	Prof. Dr. Scholz	IB772	Deutsch
Operations Research	✓		6.	Prof. Dr. Sagraloff	WIF460	Deutsch
Software Engineering III	✓		6.	Prof. Dr. Scholz	WIF620	Deutsch
Text Mining	✓		4.	Prof. Dr. Busse	WIF725	Deutsch
Module anderer Fakultäten nur nach Genehmigung durch die Prüfungskommission.						
Module der virtuellen Hochschule Bayern nur nach Genehmigung durch die Prüfungskommission[2].						

[1] Wird in Englisch durchgeführt, wenn englischsprachige Studierende die Veranstaltung besuchen.
[2] Siehe: https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp

Internet of Things (IoT) IB764

Modulverantwortlicher:	**Prof. Dr. Abdelmajid Khelil**
Dozent:	Prof. Dr. Abdelmajid Khelil
Studiengang:	Bachelor
Modultyp:	FWPF aus dem Bereich IF
Sprache:	Englisch
Angebot:	im Sommersemester
Dauer:	ein Semester
Vorkenntnisse:	Erster Studienabschnitt oder vergleichbare Kenntnisse
Voraussetzungen:	-
Leistungspunkte:	5
Arbeitsaufwand:	30 Stunden Präsenzzeit im Unterricht 30 Stunden Präsenzzeit im Praktikum 90 Stunden Selbststudium
Lehrformen:	2 SWS seminaristischer Unterricht 2 SWS Praktikum in kleinen Gruppen (14tägig 4 Stunden)
Leistungsnachweise und Prüfung:	schriftliche Prüfung 90 min.

Qualifikationsziele und Inhalte:

Qualifikationsziele:

Lernziel ist die Vermittlung von Kompetenzen im Bereich der vernetzten intelligenten Objekte. Die Studierenden lernen die technologischen Grundlagen des Internet der Dinge (Internet of Things, IoT), z.B. intelligente Objekte, Protokolle, Architekturen, Energieeffiziente SW-Entwicklung, etc.

Lehrinhalte:

Eingebettete Systeme sind heute allgegenwärtig und werden zunehmend mit dem, bzw. über das Internet vernetzt. Der Begriff IoT drückt dabei den Trend der intelligente Vernetzung aller Dinge aus, um den Menschen in seinen Tätigkeiten unmerklich zu unterstützen. In diesem Modul soll den Studierenden die Konzepte und Werkzeuge von IoT vermittelt werden: Die wichtigsten aktuellen Anwendungsgebiete; Elemente der Vernetzung; typische Aktoren und Sensoren; Protokolle (insb. MQTT, CoAP); SW-Plattformen und Interoperabilität. Das Praktikum vertieft das in der Vorlesung erworbene Wissen in ausgewählten Praxisprojekten. Dabei werden verschiedenen IoT Plattformen (z.B. Arduino, Raspberry Pi und Libelium) verwendet um unterschiedliche IoT-Anwendungen (Smart City, Smart Building, eHealth, Smart Agriculture, Industrie 4.0, etc) zu implementieren.

Literatur:

[1] Jean-Philippe Vasseur, Adam Dunkels, Interconnecting Smart Objects with IP: The next Internet, Morgan Kaufmann, 2010

[2] Adrian McEwen, Hakim Cassimally, Designing the Internet of Things, John Wiley & Sons; November 2013

[3] Fleisch, E.: Das Internet der Dinge, Springer 2005

[4] Charles Bell, Beginning Sensor Networks with Arduino and Raspberry Pi, Apress; Auflage: 2013

Innovationslabor IB765

(IoT-Projekt)

Modulverantwortlicher:	**Prof. Dr. Abdelmajid Khelil**
Dozent:	Prof. Dr. A. Khelil, Prof. Dr. E. Kromer, Prof. Dr. M. Mock, Prof. Dr. J. Uhrmann
Studiengang:	Bachelor
Modultyp:	FWPF aus dem Bereich IF
Sprache:	Deutsch / Englisch
Angebot:	jedes Studiensemester
Dauer:	ein Semester
Vorkenntnisse:	Programmieren I, Software Engineering I
Voraussetzungen:	-
Leistungspunkte:	5
Arbeitsaufwand:	150 Stunden nicht ständig betreute Projektarbeit im Labor
Lehrformen:	4 SWS nicht ständig betreute Projektarbeit. Eigenverantwortliches Arbeiten der Studierenden in Teams von einer kritischen Größe, so dass das Auftreten typischer Schnittstellenprobleme gewährleistet ist, regelmäßige Projekttreffen mit dem Betreuer. Präsentation des Projektergebnisses zum Semesterende in einem Seminar.
Leistungsnachweise und Prüfung:	Benotete individuelle schriftliche Ausarbeitung jedes Teammitglieds zum eigenen Beitrag im Projekt, im Team erstellte Gesamtdokumentation, im Team durchgeführte Präsentation des Projekts. Das Gesamtprojekt wird benotet. Die Note der Teammitglieder wird als Mittelwert aus der individuellen Note und der Projektnote gebildet.

Qualifikationsziele und Inhalte:

Qualifikationsziele:

Die Studierenden identifizieren reale Problemstellungen und erkennen die Problematik der Erstellung komplexer Lösungen mit Hilfe unterschiedlichster IoT-Plattformen. Sie sind in der Lage die Umgebung der Problemstellung zu analysieren und können diese in Zusammenarbeit mit Unternehmen im Vorfeld diskutieren. Kenntnisse über Design Thinking, agiles Projektmanagement und eigenverantwortlicher Durchführung von Projekten erwerben Studierende in der Teamarbeit. Sie sind in der Lage, fachübergreifende Kenntnisse anzuwenden, den Problemsteller in das Projekt agil einzubinden und Arbeitsergebnisse zu präsentieren.

Lehrinhalte:

Die kooperierenden Unternehmen bieten den Studierenden reale Problemstellungen aus den wichtigsten IoT-Domänen, wie etwa Smart Agriculture, Smart Building, Smart Energy, Smart Production, eHealth etc. Die Problemstellung wird anhand definierter Anwendungsfälle detailliert beschrieben. Zusätzlich werden zur Problemstellung die Aspekte IoT Cloud und IoT Security untersucht. Die Studierenden werden vom Dozenten und dem Coach des Innovationslabors fachlich betreut.

Literatur:

Siehe Projektbeschreibung. Weitere Anregungen:

[1] Jean-Philippe Vasseur, Adam Dunkels, Interconnecting Smart Objects with IP: The next Internet, Morgan Kaufmann, 2010.

[2] Charalampos Doukas, Building Internet of Things with the Arduino, CreateSpace Independent Publishing Platform, 2012.

[3] Charles Bell, Beginning Sensor Networks with Arduino and Raspberry Pi, Apress; Auflage: 2013.

[4] E.F. Engelhardt, Sensoren am Raspberry Pi, Franzis Verlag GmbH, 2014.

[5] Vic (J.R.) Winkler, Securing the Cloud, Syngress, 2011.

Einführung in die Digitale Forensik IB772

Modulverantwortlicher:	**Prof. Dr. Peter Scholz**
Dozent:	Prof. Dr. Peter Scholz
Studiengang:	Bachelor
Modultyp:	Wahlpflichfach
Sprache:	Folien/Unterlagen in Englisch, Vorlesung in Deutsch oder Englisch
Angebot:	im Sommersemester
Dauer:	ein Semester
Vorkenntnisse:	Kenntnisse in Grundlagen der Informationssicherheit und Kryptografie
Voraussetzungen:	-
Leistungspunkte:	5
Arbeitsaufwand:	45 Stunden Präsenzzeit im seminaristischen Unterricht, 105 Stunden Selbststudium.
Lehrformen:	2 SWS seminaristischer Unterricht 2 SWS Übung, aufgeteilt in Gruppen- Einzel- und Projektarbeit
Leistungsnachweise und Prüfung:	Leistungsnachweis der Übung/Projektarbeit, schriftliche Prüfung 90 Minuten

Qualifikationsziele und Inhalte:

Qualifikationsziele:

Dieses Modul gibt eine Einführung in die digitale Forensik. Es deckt dabei theoretische, praktische und rechtliche Aspekte ab. Der erste Teil konzentriert sich auf die Anforderungen, die nötig sind um ein guter Computerforensiker zu werden. Dieser Personenkreis ist bei Ermittlungsbehörden und Industrieunternehmen gleichermaßen gesucht. Weiterhin werden Methoden, Techniken und Werkzeuge zur forensischen Auswertung von Computern und Smartphones vorgestellt. Dabei werden begleitend stets rechtliche Aspekte, wie beispielsweise der Datenschutz, beleuchtet. Nach erfolgreichem Abschluss dieses Moduls:

- können sie erste forensische Untersuchungen bzw. Auswertungen bei Computern, Smartphones und Tablets auf Basis von Richtlinien durchführen,
- wissen Studierende, wie sie forensische Berichte und Gutachten schreiben,
- können sie die wesentlichen rechtlichen Aspekte und Zusammenhänge verstehen und hieraus ihre Pflichten als Computerforensiker ableiten,
- können sie einschlägige Softwarewerkzeuge anwenden,
- können sie den einschlägigen Stand der Wissenschaft, Technik und Praxis beurteilen.

Lehrinhalte:

- Einführung, Motivation, Geschichte, Anforderungen
- Beschlagnahme und Auswertung von Beweismitteln
- Methoden und Prozesse der digitale Forensik (Analyse von Betriebssystemen, Dateisystemen, Dateien und Datenbanken, Erkennen von Eindringlingen)
- Fallstudien
- Überblick zu forensischen Software Tools (kommerziell, Open Source)
- Erstellung von Berichten und Gutachten
- Digitale Forensik mobiler Endgeräte

Literatur:

Wird zeitnah und aktuell in der ersten Vorlesungsstunde bekannt gegeben.

Operations Research WIF460

Modulverantwortlicher:	**Prof. Dr. Michael Sagraloff**
Dozent:	Prof. Dr. Michael Sagraloff
Studiengang:	Bachelor
Modultyp:	FWP aus dem Bereich WIF
Sprache:	Deutsch
Angebot:	im vierten Studiensemester
Dauer:	ein Semester
Vorkenntnisse:	Mathematik I und II
Voraussetzungen:	Zulassung zum Praktikum erfolgt bei bestandener Prüfung in Mathematik I
Leistungspunkte:	5
Arbeitsaufwand:	60 Stunden Präsenzzeit im Unterricht 90 Stunden Selbststudium
Lehrformen:	2 SWS seminaristischer Unterricht 2 SWS Übungen (14tägig 4 Stunden)
Leistungsnachweise und Prüfung:	Schriftliche Prüfung, 90 Min. Leistungsnachweis im Praktikum.

Qualifikationsziele und Inhalte:

Qualifikationsziele:

Die Studierenden sind mit den wichtigsten Themengebieten des Operations Research wie (nicht) lineare (ganzzahlige) Optimierung, Optimierung in Graphen, Netzplantechnik, sowie heuristische und probabilistische Verfahren vertraut. Sie sind nach der Vorlesung in der Lage, neue Algorithmen leicht zu verstehen, an eingeführten Verfahren Modifikationen vorzunehmen oder und auch selbst Verfahren zu entwickeln. Zudem können sie für Standardprobleme der industriellen Praxis das richtige OR-Verfahren auswählen und anwenden.

Lehrinhalte:

- Einführung und Grundbegriffe des Operations Research
- Lineare Optimierung (Simplex Algorithmus, Dualität, Sensitivitätsanalyse)
- Ganzzahlige lineare Optimierung (Branch and Bound-Algorithmus, Gomory Verfahren)
- Nichtlineare Optimierung (Newton Verfahren, Lagrange Verfahren, Gradientenverfahren, Simulated Annealing)
- Optimierung in Graphen (Algorithmen von Dijkstra, Kruskal, und Prim)
- Netzplantechnik (Modellierung, Berechnung kritischer Pfade, Pufferzeiten)
- Transport- und Tourenplanung als Beispiel für Standard-Probleme der industriellen Praxis

Literatur:

Domschke W., Drexl A.: „Einführung in Operations Research“, 7. Auflage, Springer, Berlin, 2007 Hillier F.S., Liebermann G.J.: „Introduction to Operations Research“, 9. Auflage, McGraw Hill, 2012 Heinrich G., Grass J.: „Operations Research in der Praxis“, Oldenbourg Verlag, 2006
Neumann K., Morlock M.: „Operations Research“, 2. Auflage, Hanser Verlag, 2004
Zimmermann H.-J.: „Methoden und Modelle des Operations Research für Ingenieure, Ökonomen und Informatiker“, 2. Auflage, Vieweg Verlag, 2008
Zimmermann W.: „Operations Research - Quantitative Methoden zur Entscheidungsvorbereitung“, Oldenbourg Verlag, 1999
Ulrich Kathöfer und Ulrich Müller-Funk: “Operations Research”, 2017, 3. Auflage, 256 Seiten, UVK Verlagsgesellschaft mbH

Software Engineering III WIF620

(Secure Software Engineering)

Modulverantwortlicher:	**Prof. Dr. Peter Scholz**
Dozent:	Prof. Dr. Peter Scholz
Studiengang:	Bachelor
Modultyp:	FWP aus dem Bereich WIF
Sprache:	Folien/Unterlagen in Englisch, Vorlesung in Deutsch oder Englisch
Angebot:	im sechsten Studiensemester
Dauer:	ein Semester
Vorkenntnisse:	Software Engineering I (Überblick über alle Phasen der Softwareentwicklung und die dort eingesetzten Methoden und Verfahren); Software Engineering II (Objektorientierte Analyse und Design von Software, UML), Informationssicherheit
Voraussetzungen:	Zulassung erfolgt bei bestandener Prüfung in Programmieren I oder Programmieren II
Leistungspunkte:	5
Arbeitsaufwand:	45 Stunden Präsenzzeit im Unterricht 105 Stunden Selbststudium
Lehrformen:	2 SWS seminaristischer Unterricht 1 SWS Übung zur Erstellung einer Hausarbeit oder Projekt(gruppen)arbeit 1 SWS Erstellung einer Hausarbeit oder Projekt(gruppen)arbeit
Leistungsnachweise und Prüfung:	Leistungsnachweis, schriftliche Prüfung 90 Minuten

Qualifikationsziele und Inhalte:

Qualifikationsziele:

Aufbauend auf den Grundlagen des Software Engineerings in den Modulen WIF210 und WIF310 haben die Studierenden vertieften Einblick in ausgewählte spezielle Themengebiete des Software Engineering. Insbesondere haben sie verstanden und eingeübt, wie sichere Software entwickelt werden kann. Sichere Software ist gegen absichtliche Angriffe geschützt. Die Studierenden lernen, wie Sicherheit im Entwicklungsprozess verankert wird.

Lehrinhalte:

- Angriffe auf Software
- Softwaresicherheit aus Nutzer- und Angreifersicht
- Formulierung von Sicherheitsanforderungen
- Modellierung von Bedrohungen
- Sicherer Softwareentwurf
- Sicheres Programmieren
- Qualitätssicherung von sicherer Software

Literatur:

Wird zeitnah und aktuell in der ersten Vorlesungsstunde bekannt gegeben. Darüber hinaus:
Sachar Paulus: „Basiswissen Sichere Software“, dpunkt.verlag, Heidelberg, 2011.
Walter Kriha, Roland Schmitz: „Sichere Systeme“, Springer-Verlag, Berlin, Heidelberg, 2009.

Text Mining WIF725

Modulverantwortlicher:	**Prof. Dr. Johannes Busse**
Dozent:	Prof. Dr. Johannes Busse
Studiengang:	Bachelor
Modultyp:	FWP aus dem Bereich WIF
Sprache:	Deutsch
Angebot:	im Sommersemester
Dauer:	ein Semester
Vorkenntnisse:	-
Voraussetzungen:	-
Leistungspunkte:	5
Arbeitsaufwand:	30 Stunden Präsenzzeit im Unterricht 30 Stunden Präsenzzeit im Praktikum 90 Stunden Selbststudium
Lehrformen:	4 SWS seminaristischer Unterricht
Leistungsnachweise und Prüfung:	Studienarbeit;

Qualifikationsziele und Inhalte:

Qualifikationsziele:

Die TN können unter Linux in Python mit einschlägigen Bibliotheken (wie z.B. scikit-learn, SpaCy, Gensim, NLTK) schwach strukturierte Texte sowie Tabellendaten aus dem Bereich der Wirtschaftsinformatik mit Verfahren des Machine Learning analysieren, Textähnlichkeit feststellen, klassifizieren, korrelierte Daten vorhersagen.
Praktisch beschäftigen wir uns mit der Bepreisung von Immobilien (Boston Housing Dataset), der Text-Klassifikation (20 Newsgroups Dataset) oder der Sentiment Analysis aufgrund von Produktbewertungen. An weiteren Anwendungsfällen diskutieren wir exemplarisch (Weiss 2015): 8.1 Market Intelligence from the Web — 8.3 Generating Model Cases for Help Desk Applications — 8.8 Mining Social Media — 8.9 Customized Newspapers
Die hier vermittelte Technologie bildet eine Grundlage für weiterführende KI-Anwendungen in der Wirtschaftsinformatik.

Lehrinhalte:

- Grundlagen des dsc-lab: Linux, bash, Jupyter Notebook, Publizieren mit Jupyterbook etc.
- Grundlagen des Machine Learning : Klassifikation, Regression, Modellevalution, Confusion Matrix etc.
- Grundlagen der Informationsextraktion aus Text: Regex, NLP mit Spacy etc.
- Theorie des Information Retrieval (IR) from text

Die Veranstaltung beruht auf einem virtuellen Data Science Laboratory http://jbusse.de/dsci-lab/, das den Studierenden unter VirtualBox als virtuelle Xubuntu-Maschine zur Verfügung gestellt wird.

Literatur:

Bücher:

- Tobias Roelen-Blasberg: Automatisierte Präferenzmessung: Extraktion und Evaluation von Produktattributen auf Basis von Online-Rezensionen. Springer 2019.
- Winfried Gödert, Jessica Hubrich und Matthias Nagelschmidt: Semantic Knowledge Representation for Information Retrieval. De Gruyter Saur 2014.
- Weiss, Sholom M.: Fundamentals of Predictive Text Mining. Springer 2nd ed. 2015
- Aggarwal, Charu C.: Machine learning for text (2018)

Online:

- ausgewählte Einführungs-Lectures aus https://www.kaggle.com/learn/overview
- SpaCy https://spacy.io/usage/spacy-101
- Beautiful Soup https://www.crummy.com/software/BeautifulSoup/bs4/doc/
- RegEx online zum Üben: https://regex101.com/ > Python flavor