Modulhandbuch

Hochschule für Telekommunikation Leipzig
University of Applied Sciences
Fakultät Informations- und Kommunikationstechnik

für den

weiterbildenden Masterstudiengang

Datenschutz und Sicherheit in den Informationssystemen

Entwurf und Grundlage für das Akkreditierungsverfahren

Fassung vom 27.02.2017

(Gültig für 2017 und später immatrikulierte Studierende)

Allgemeine Informationen und Lesehinweise

Was ist ein Modulhandbuch?

Dieses Modulhandbuch beinhaltet Beschreibungen zu allen Modulen des Studienprogramms. Es dient der Transparenz und versorgt Studierende, Studieninteressierte und andere interne und externe Adressaten mit Informationen über die Inhalte der einzelnen Module, ihre Qualifikationsziele sowie qualitative und quantitative Anforderungen.

Wichtige Lesehinweise:

Aktualität

> Jedes Semester wird der aktuelle Stand des Modulhandbuchs veröffentlicht. Das Generierungsdatum (siehe Deckblatt) gibt Auskunft, an welchem Tag das vorliegende Modulhandbuch generiert wurde.

Rechtsverbindlichkeit

> Modulbeschreibungen dienen der Erhöhung der Transparenz und der besseren Orientierung über das Studienangebot. Einzelne Abweichungen zur Umsetzung der Module im realen Lehrbetrieb sind möglich. Eine rechtsverbindliche Auskunft über alle studien- und prüfungsrelevanten Fragen sind den Prüfungs- und Studienordnungen der Studiengänge gemäß Veröffentlichung im Hochschulinformationssystem zu entnehmen.

Wahlmodule

> Wenn im Rahmen des Studiengangs Wahlmodule aus einem offenen Katalog gewählt werden können, sind diese Wahlmodule in der Regel nicht oder nicht vollständig im Modulhandbuch gelistet.

Impressum

Prorektor für Studium und Forschung
Hochschule für Telekommunikation Leipzig
prorektor@hftl.de
Gustav-Freytag-Str. 43-45
04277 Leipzig
0341/3062 200

Trägerin der Hochschule für Telekommunikation Leipzig ist die HfTL Trägergesellschaft mbH.

Geschäftsführung: Dr. Elke Frank, Dr. Ralph Rentschler
Handelsregister: Amtsgericht Bonn HRB 19361
Sitz der Gesellschaft: Bonn

Status des Studienprogramms

Das Studienprogramm wird gegenwärtig zur Programmakkreditierung vorbereitet. Das Verfahren soll im zweiten Quartal 2017 eröffnet und zur Immatrikulation im März 2018 (Sommersemester) abgeschlossen sein.

Für unsere Masterstudenten (IKT und WIM) sowie für Gasthörer werden die Module im offenen Programm als Profilierungsmodule angeboten.

Es besteht die Möglichkeit die Module als Gasthörer zu belegen und mit einem Zertifikat (Transcript of Records) abzuschließen. Mit dem Abschluss des Verfahrens der Programmakkreditierung können Sie in den weiterbildenden Masterstudiengang immatrikuliert werden. Bestandene Module des Programms werden angerechnet.

Ziele und Qualifikationsprofil des Studienprogramms

Der weiterbildende Masterstudiengang Datenschutz und Sicherheit in Informationsystemen bildet Fachkräfte aus, die selbständig und gemeinsam mit Fachleuten verschiedener Fachdisziplinen komplexe, interdisziplinäre Problemstellungen mit Bezug zur Erhebung, Verarbeitung, Nutzung und Verwaltung personenbezogener Daten lösen können. Die Absolventinnen und Absolventen des weiterbildenden Masterstudiengangs haben insbesondere gelernt, komplexe Fragestellungen mit widersprüchlichen und/oder unvollständigen Vorgaben aus unterschiedlichen Fachdisziplinen allein oder in einem Team zu bearbeiten.

Zu diesem Zweck vermittelt der weiterbildende Masterstudiengang ein tiefes wissenschaftlich-technisches Fachwissen bezüglich Datenschutz und Sicherheit sowie erweiterte Schlüsselqualifikationen für interdisziplinäre berufliche Aufgaben. Die im Studiengang vermittelten Kompetenzen konsolidieren, vertiefen und verbreitern den praxisbezogenen Wissens- und Erfahrungsschatz einer mehrjährigen Berufserfahrung. Der Studiengang erlaubt eine Spezialisierung auf Tätigkeitsfelder mit Datenschutz- und Sicherheitsbezug innerhalb der Informations- und Kommunikationsbranche.

Die Absolventinnen und Absolventen des weiterbildenden Masterstudiengangs verfügen über aktuelles Fachwissen sowie ein profundes Verständnis über die Prinzipien und den Zweck von Datenschutz und Sicherheit in Informationssystemen. Dieses Wissen hat seinen Ursprung sowohl in den formalen Beschreibungen von Informatik und Recht, als auch im interdisziplinären Überlappungsbereich mit anderen Fachdisziplinen. Die Absolventinnen und Absolventen können mit den Methoden des Fachgebiets sowohl in bestehenden als auch in neu zu entwerfenden Informationssystemen Problemstellungen isolieren, analysieren und dokumentieren und mit konfligierenden Anforderungen umgehen. Darüber hinaus können sie Neuerungen im Fachgebiet frühzeitig antizipieren und in Entscheidungs- und Entwicklungsprozesse einfließen lassen. Die Absolventinnen und Absolventen können Fachwissen aus unterschiedlichen Anwendungsfeldern kombinieren. Sie können dieses Fachwissen auf komplexe, interdisziplinäre Datenschutz-Fragestellungen anwenden, um Informationssysteme unter Berücksichtigung von Datenschutzzielen zu entwerfen und zu realisieren, sowie um bestehende Informationssysteme zu restrukturieren. Dazu verfügen sie über ein fundiertes Verständnis dafür, welche Verfahren auf ein gegebenes Problem sinnvoll anwendbar sind. Die Absolventinnen und Absolventen können innovative Methoden zur Problemlösung entwickeln und anwenden, und sowohl wissenschaftliche als auch praktische Beiträge zur Weiterentwicklung des Datenschutzes leisten. Darüber hinaus können die Absolventinnen und Absolventen neue Ideen, Konzepte, Methoden, Verfahren, Techniken und Technologien im Bereich der Informationssysteme auf ihre Auswirkungen auf die Privatheit der Betroffenen hin kritisch hinterfragen. Sie können in interdisziplinären Teams zusammenarbeiten, solche Teams leiten und die Ergebnisse ihrer Arbeit fachinternen und fachfremden Dritten vermitteln.

Hinweis: Dieser Text ist Grundlage der im Diploma Supplement hinterlegten „Programme Requirements/Qualification Profile of the Graduate“.

Überblick zum Studienablauf

Dieses weiterbildende Masterstudienprogramm ist als Teilzeitstudium für Berufstätige konzipiert.

Studienablauf

.

Einführung in den Datenschutz

Modulniveau	Sprache	Semesterdauer	Häufigkeit
Master	Deutsch	Einsemestrig	Einmal im Studienjahr
Credits:	**Gesamtstunden**	**Präsenzstunden**	**Eigenstudiumsstunden**
5 ECTS	125	36	89
Studien-/Prüfungs-leistung	**Prüfungsart**	**Prüfungsdauer in Minuten**	**Wiederholungs-möglichkeit**
Klausur	Schriftlich	90	Jeweils im Folgesemester

Ziele – Kompetenzen, Lern- und Qualifikationsziele

Das Modul zielt darauf ab, die formalen Grundlagen des Datenschutzes zu vermitteln, eine Abgrenzung des Datenschutzes zu anderen Fachdisziplinen herzustellen und die Herausforderungen des Datenschutzes im Spannungsfeld aus technischen, wirtschaftlichen, organisatorischen, rechtlichen und gesellschaftlichen Aspekten aufzuzeigen. Damit einher geht die Kompetenz zum Antizipieren und Analysieren der Auswirkungen von bestehenden und in der Entwicklung befindlichen Informationssystemen auf die Privatheit der Betroffenen. Die Studierenden können Datenschutzziele definieren und priorisieren. Sie verfügen über ein grundlegendes Verständnis der aktuellen technischen und organisatorischen Mittel des Datenschutzes, um diese Ziele zu erreichen und den Zielerreichungsgrad zu bestimmen.

Modulverantwortliche

- Prof. Dr. Erik Buchmann; buchmann@hftl.de

Inhalt

- Ursprünge des Datenschutzes
- Der gesellschaftliche Diskurs als Brücke zum Datenschutzrecht
- Anonymisierung vs. Datenqualität
- Datenschutz unter Risiko-Gesichtspunkten
- Datenschutzfreundliche Technologien
- Datenschutz vs. Verschlüsselung: kryptographische Verfahren
- Aktuelle Fragen: Datenschutz vs. Terrorismusabwehr, EU-US-Privacy Shield, etc.

Literatur

- Bernhard C. Witt: Datenschutz Kompakt und Verständlich: Eine Praxisorientierte

Einführung, Vieweg+Teubner Verlag, 2010

- Johannes Buchmann: Internet Privacy: Eine multidisziplinäre Bestandsaufnahme. Springer Verlag, 2013
- Michelle Finneran Dennedy, Jonathan Fox, Thomas Finneran: The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value, Apress, 2014
- Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), Zuletzt geändert durch Art. 1 G v. 25.2.2015 I 162

Hinweise

Dieses Modul ist Bestandteil folgender Studienprogramme:

- Weiterbildender Masterstudiengang Datenschutz und Sicherheit in den Informationssystemen (geplant)
- Masterstudiengang Informations- und Kommunikationstechnik (im offenen Programm zur Profilierung)
- Masterstudiengang Wirtschaftsinformatik (im offenen Programm zur Profilierung)

Recht für Datenschutz und Sicherheit

Modulniveau	Sprache	Semesterdauer	Häufigkeit
Master	Deutsch	Einsemestrig	Einmal im Studienjahr
Credits:	**Gesamtstunden**	**Präsenzstunden**	**Eigenstudiumsstunden**
5 ECTS	125	36	89
Studien-/Prüfungs-leistung	**Prüfungsart**	**Prüfungsdauer in Minuten**	**Wiederholungs-möglichkeit**
Klausur	Schriftlich	90	Jeweils im Folgesemester

Ziele – Kompetenzen, Lern- und Qualifikationsziele

In dieser Vorlesung erwerben und vertiefen die Studierenden das theoretische und praktische Rüstzeug zur Auslegung und Anwendung von rechtlichen Normen zu Datenschutz und Sicherheit auf bestehende und neu zu entwickelnde IT-Systeme und Prozesse. Dazu gehört ein umfassendes Verständnis der formaljuristischen Methoden und Prinzipien sowie aktuelles Fachwissen im Bereich Datenschutzrecht. Kenntnisse zum aktuellen Stand der Forschung, zum gesellschaftlichen Diskurs bei Datenschutzthemen sowie zum Ablauf bei der Verabschiedung von Rechtsnormen in Deutschland und der EU ermöglichen es den Studierenden, zu erwartende Entwicklungen frühzeitig zu beurteilen und in Designentscheidungen bei der Entwicklung von IT-Systemen und Prozessen einfließen zu lassen. Die Studierenden können Widersprüche zwischen Normen auflösen und Normen anhand ihrer Stellung im Normengefüge priorisieren. Sie können ihre Erkenntnisse in einem fachübergreifenden Team erarbeiten und vertreten.

Modulverantwortliche

- Prof. Dr. Erik Buchmann; buchmann@hftl.de

Inhalt

- Normenhierarchien, Anwendbarkeit von Normen
- Auslegung von Normen, unbestimmte Rechtsbegriffe
- Abgrenzung von Datenschutznormen zu Persönlicheitsrechten, Urheberrechten etc.
- Betroffenenrechte und Pflichten der verantwortlichen Stelle
- Der Prüfkanon bei der Einführung einer neuen Rechtsvorschrift
- Deutsche Normen mit Bezug zu Datenschutz und Datensicherheit
- EU-Richtlinien zum Datenschutz
- Softwareimplementierte Regeln und Recht

- Ausblicke in Vertragsrecht und weitere Rechtsnormen mit Bezug zur Datenverarbeitung

Literatur

- Jürgen Kühling, Christian Seidel, Anastasios Sivridis: Datenschutzrecht – Start ins Rechtsgebiet, C.F. Müller Verlag, 2015
- EU-Datenschutz-Grundverordnung, Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016
- Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 G v. 25.2.2015 I S. 162
- Telemediengesetz in der Fassung der Bekanntmachung vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Art. 1 G v. 21.6.2016 I S. 1766

Hinweise

Dieses Modul ist Bestandteil folgender Studienprogramme:

- Weiterbildender Masterstudiengang Datenschutz und Sicherheit in den Informationssystemen (geplant)
- Masterstudiengang Informations- und Kommunikationstechnik (im offenen Programm zur Profilierung)
- Masterstudiengang Wirtschaftsinformatik (im offenen Programm zur Profilierung)

IT-Sicherheit

Modulniveau	Sprache	Semesterdauer	Häufigkeit
Master	Deutsch	Einsemestrig	Einmal im Studienjahr
Credits:	**Gesamtstunden**	**Präsenzstunden**	**Eigenstudiumsstunden**
5 ECTS	125	36	89
Studien-/Prüfungs-leistung	**Prüfungsart**	**Prüfungsdauer in Minuten**	**Wiederholungs-möglichkeit**
Klausur	Schriftlich	90	Jeweils im Folgesemester

Ziele – Kompetenzen, Lern- und Qualifikationsziele

Die Studierenden verfügen über ein umfassendes Verständnis über die Zielsetzungen und formalen Grundlagen der IT-Sicherheit, insbesondere in Bezug auf ihre Anwendbarkeit auf Datenschutzprobleme. Sie können bestehende Geschäftsprozesse, Kommunikationsarchitekturen oder Rechnernetze auf ihren Sicherheitsbedarf hin analysieren und entsprechend restrukturieren sowie neue Prozesse und Systeme unter Berücksichtigung von Sicherheitskriterien entwickeln. Die Studierenden sind mit dem aktuellen Stand der Forschung im Bereich der IT-Sicherheit vertraut und kennen die Grenzen der Anwendbarkeit von bestehenden Sicherheitsansätzen auf Datenschutzprobleme. Die Studierenden können Sicherheitskonzepte entwickeln und formale Sicherheitsbeweise für Algorithmen und Kommunikationsprotokolle verstehen.Insbesondere können sie bekannte Ansätze zur IT-Sicherheit kritisch hinterfragen und mit Blick auf zukünftige Anforderungen innovative neue Ansätze und Lösungen entwickeln, präsentieren, implementieren und evaluieren.

Modulverantwortliche

- Prof. Dr. Erik Buchmann; buchmann@hftl.de

Inhalt

- IT-Grundschutz im Überblick
- Firewall-Techniken und Virtual Private Networks
- DRM und Management von Zertifikaten
- Sicherheitsaspekte moderner Betriebssysteme und Anwendungen
- Schichtenübergreifende Datensicherheit
- Datensicherheit auf der Bitübertragungsschicht und der Sicherungsschicht
- Algorithmen und Kommunikationsprotokolle

- Sicherheit im Internet der Dinge
- Praktische Vertiefung in den Computer-Pools/Netz-Laboren

Literatur

- C. Eckert: IT-Sicherheit, 3. Auflage, Oldenbourg Verlag
- S. Garfinkel und G. Spafford: Practical Unix & Internet Security, O'Reilly & Associates
- Schäfer, G.: Netzsicherheit; dpunkt Verlag.
- Swoboda, J. et al.: Kryptographie und IT - Sicherheit: Grundlagen und Anwendungen - eine Einführung; Vieweg+Teubner.
-
- Pohlmann, N. et al.: Der IT-Sicherheitsleitfaden: Das Pflichtenheft zur Implementierung von IT-Sicherheitsstandards im Unternehmen; MiTP.
- Kersten, H. et al.: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Der Weg zur Zertifizierung; Vieweg+Teubner

Hinweise

Dieses Modul ist Bestandteil folgender Studienprogramme:

- Weiterbildender Masterstudiengang Datenschutz und Sicherheit in den Informationssystemen (geplant)
- Masterstudiengang Informations- und Kommunikationstechnik
- Masterstudiengang Wirtschaftsinformatik

Datenschutz und Sicherheit in Prozessen

Modulniveau	Sprache	Semesterdauer	Häufigkeit
Master	Deutsch	Einsemestrig	Einmal im Studienjahr
Credits:	**Gesamtstunden**	**Präsenzstunden**	**Eigenstudiumsstunden**
5 ECTS	125	36	89
Studien-/Prüfungs-leistung	**Prüfungsart**	**Prüfungsdauer in Minuten**	**Wiederholungs-möglichkeit**
Klausur	Schriftlich	90	Jeweils im Folgesemester

Ziele – Kompetenzen, Lern- und Qualifikationsziele

Die Studierenden erwerben in diesem Modul ein fundamentales Verständnis zur Umsetzung von Datenschutz und Sicherheit auf der organisatorischen Ebene der Geschäftsprozesse. Sie verfügen über die nötige Kompetenz und das aktuelle Fachwissen, um neue IT-Systeme und Prozesse unter Datenschutzkriterien zu modellieren und zu gestalten, sowie um bestehende Prozesse zu analysieren und umzustrukturieren. Die Studierenden verfügen über das erforderliche aktuelle Fachwissen, um Anforderungen aus unterschiedlichen Fachgebieten und Anwendungsfeldern zu berücksichtigen sowie konfligierende Anforderungen zu priorisieren und geeignet aufzulösen. Sie besitzen ebenfalls die Kompetenzen zur Konfliktlösung und zur strukturierten interdisziplinären Zusammenarbeit mit den Verantwortlichen aus anderen Fachgebieten und können ihre Ergebnisse gegenüber Fachfremden vertreten.

Modulverantwortliche

- Prof. Dr. Erik Buchmann; buchmann@hftl.de
- Prof. Dr. Jürgen Anke; anke@hftl.de

Inhalt

- interdisziplinäre Anforderungsanalyse
- Prozessmodellierung, Workflow-Management nach Datenschutzgesichtspunkten
- Enterprise-Architekturen
- Berechtigungskonzepte in Enterprise Software
- Privacy-by-Design, Separation of Concerns, Separation of Duties, Separation of Data
-

Literatur

- Josef L. Staud: Unternehmensmodellierung: Objektorientierte Theorie und Praxis mit UML 2.0, Springer Verlag, 2010
- Michael Gaitanides: Prozessorganisation: Entwicklung, Ansätze und Programme des Managements von Geschäftsprozessen, Vahlen Verlag, 2012
- George O.M. Yee: Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards: Aspects and Standards, IGI Global, 2011
- Primärliteratur aus der Forschung wird in der Vorlesung bekanntgegeben.

Hinweise

Dieses Modul ist Bestandteil folgender Studienprogramme:

- Weiterbildender Masterstudiengang Datenschutz und Sicherheit in den Informationssystemen (geplant)
- Masterstudiengang Informations- und Kommunikationstechnik (im offenen Programm zur Profilierung)
- Masterstudiengang Wirtschaftsinformatik (im offenen Programm zur Profilierung)

Praktischer Datenschutz

Modulniveau	Sprache	Semesterdauer	Häufigkeit
Master	Deutsch	Einsemestrig	Einmal im Studienjahr
Credits:	**Gesamtstunden**	**Präsenzstunden**	**Eigenstudiumsstunden**
5 ECTS	125	36	89
Studien-/Prüfungs-leistung	**Prüfungsart**	**Prüfungsdauer in Minuten**	**Wiederholungs-möglichkeit**
Alternativ	Beleg und Präsentation	ca. 30 min Präsentation	Jeweils im Folgesemester

Ziele – Kompetenzen, Lern- und Qualifikationsziele

Die Studierenden erwerben bzw. vertiefen ihre Kenntnisse und Fähigkeiten zur Analyse konkreter Problemstellungen bei der Umsetzung von Datenschutz- und Sicherheitsaspekten in komplexen IT-Systemen und Prozessen. Dazu zählen insbesondere auch die Fähigkeiten zum wissenschaftlichen Arbeiten, zum eigenständigen Erschließen neuester Entwicklungen sowohl im Fachbereich der zugrundeliegenden Problemstellungen als auch im Bereich Datenschutz und Sicherheit, sowie zum Antizipieren künftiger Entwicklungen in diesen Bereichen. Die Absolventen dieses Moduls können daher sowohl wissenschaftliche als auch praktische Beiträge zu aktuellen und zukünftig zu erwartenden Datenschutzproblemen liefern sowie aktuelle Konzepte, Verfahren und Technologien kritisch hinterfragen, anpassen und weiterentwickeln. Dazu gehört ebenfalls die Kompetenz zur Konfliktlösung und zur strukturierten Zusammenarbeit in einem interdisziplinären Team bzw. mit den Nutzern und Verantwortlichen anderer Fachgebiete sowie zur Darstellung von Erkenntnissen vor einem externen Publikum.

Modulverantwortliche

- Prof. Dr. Erik Buchmann; buchmann@hftl.de

Inhalt

- Wissenschaftliches Arbeiten, z. B. in Form von Literaturstudien, Nutzerbefragungen, Analysen verfügbarer Technologien
- Persönliche und gesellschaftliche Aspekte des Datenschutzes, Durchsetzbarkeit von Datenschutz-Grundrechten
- Teamarbeit mit dem Ziel, ein konkretes Datenschutzproblem zu untersuchen
- Wahrnehmung der Datenschutzthematik in der Öffentlichkeit, Bedeutung für Unternehmen, Politiker, Betroffene

Literatur

- Serge Gutwirth, Ronald Leenes, Paul de Hert: Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges, Springer Science & Business Media, 2013
- Primärliteratur aus der Forschung wird in der Vorlesung bekanntgegeben.

Hinweise

Dieses Modul ist Bestandteil folgender Studienprogramme:

- Weiterbildender Masterstudiengang Datenschutz und Sicherheit in den Informationssystemen (geplant)
- Masterstudiengang Informations- und Kommunikationstechnik (im offenen Programm zur Profilierung)
- Masterstudiengang Wirtschaftsinformatik (im offenen Programm zur Profilierung)

Private/Secure Storage

Modulniveau	Sprache	Semesterdauer	Häufigkeit
Master	Deutsch	Einsemestrig	Einmal im Studienjahr
Credits:	**Gesamtstunden**	**Präsenzstunden**	**Eigenstudiumsstunden**
5 ECTS	125	36	89
Studien-/Prüfungs-leistung	**Prüfungsart**	**Prüfungsdauer in Minuten**	**Wiederholungs-möglichkeit**
Alternativ	Kolloquium	30	Jeweils im Folgesemester

Ziele – Kompetenzen, Lern- und Qualifikationsziele

In diesem Praktikum erwerben die Studierenden theoretische und praxisbezogene Kompetenzen zur Analyse und Entwicklung von Techniken zur sicheren Datenorganisation. Sie kennen den Stand der Forschung zu Ansätzen wie der sicheren Portionierung oder Fragmentierung und können den Nachweis erbringen, mit solchen Ansätzen sensible Daten bei Dritten gespeichert und verarbeitet werden können, ohne dass diese Daten offengelegt oder mit den Betroffenen in Zusammenhang gebracht werden können. Die Studierenden können derartige Techniken in bestehende oder neu zu entwickelnde Informationssysteme integrieren, so dass konfligierende Anforderungen aus den Bereichen Datenschutz, Sicherheit und Performanz sinnvoll berücksichtigt werden. Die Studierenden können die Stärken und Schwächen derartiger Verfahren gegenüber Fachfremden präsentieren und auf praktische Probleme zugeschnittene innovative Lösungen entwickeln.

Modulverantwortliche

- Prof. Dr. Erik Buchmann; buchmann@hftl.de
- Prof. Dr. Andreas Thor; thor@hftl.de

Inhalt

- Cloud-basierte Data Stores und Datenbanken
- Bucketization, Partially Order-Preserving Encryption
- Stream-basierte Verfahren, Warenkorb-Verfahren
- Integration in Objekt-Relationales Mapping, Enterprise Java Beans etc.
- Implementieren von Ansätzen aus der Forschung
- Untersuchung der unterstützten Datenoperationen
- Praktische Evaluierung nach Leistungs- und Datenschutzkriterien

- Anwendungsszenarien, z.B. anonyme Duplikatserkennung in Datenbanken

Literatur

- Josep Domingo-Ferrer, David Sánchez, Jordi Soria-Comas: Database Anonymization: Privacy Models, Data Utility, and Microaggregation-based Inter-model Connections, Morgan & Claypool Publishers, 2016
- Sara Foresti: Preserving Privacy in Data Outsourcing, Springer Science & Business Media, 2010
- Raymond Chi-Wing Wong, Ada Fu: Privacy-Preserving Data Publishing: An Overview, Morgan & Claypool Publishers, 2010
- Primärliteratur aus der Forschung wird in der Vorlesung bekanntgegeben.

Hinweise

Dieses Modul ist Bestandteil folgender Studienprogramme:

- Weiterbildender Masterstudiengang Datenschutz und Sicherheit in den Informationssystemen (geplant)
- Masterstudiengang Informations- und Kommunikationstechnik (im offenen Programm zur Profilierung)
- Masterstudiengang Wirtschaftsinformatik (im offenen Programm zur Profilierung)

Verteiltes privates Data-Mining

Modulniveau	Sprache	Semesterdauer	Häufigkeit
Master	Deutsch	Einsemestrig	Einmal im Studienjahr
Credits:	**Gesamtstunden**	**Präsenzstunden**	**Eigenstudiumsstunden**
5 ECTS	125	36	89
Studien-/Prüfungs-leistung	**Prüfungsart**	**Prüfungsdauer in Minuten**	**Wiederholungs-möglichkeit**
Klausur	Schriftlich	90	Jeweils im Folgesemester

Ziele – Kompetenzen, Lern- und Qualifikationsziele

Dieses Vorlesungsmodul vermittelt den Studierenden die Fähigkeiten und Kenntnisse zur Bearbeitung von typischen Data-Mining-Fragestellungen mit einem Fokus auf den Schutz der Privatheit der in den Datensätzen enthaltenen Personen. Die Studierenden verfügen über aktuelles theoretisches und praktisches Fachwissen über datenschutzfreundliche Data-Mining-Verfahren und können dies auf gegebene Fragestellungen sinnvoll anwenden. Sie können neue Data-Mining-Verfahren selbständig auf Datenschutzprobleme analysieren und beurteilen. Die Studierenden können diese zur Vermeidung derartiger Probleme weiterentwickeln und in komplexe IT-Systeme und Prozesse integrieren. Insbesondere verfügen die Studierenden über die erforderlichen Kompetenzen, um mit empirischen und formalen Methoden den Zusammenhang zwischen (a) der Ergebnisqualität von Data-Mining-Verfahren und (b) dem Grad der Bedrohung der Privatsphäre der Betroffenen zu beschreiben.

Modulverantwortliche

- Prof. Dr. Erik Buchmann; buchmann@hftl.de
- Prof. Dr. Benjamin Fabian; fabian@hftl.de

Inhalt

- Wiederholung Data Mining: Ziele, Methoden, Werkzeuge
- Grundlagen: Yaos Millionaire Problem, Secure Sum, Distributed Secure Sum
- Privacy-Aware Data Mining, Distributed Data Mining
- Konkrete Analysealgorithmen: Clustering, Feature Selection, Event Detection
- Information Hiding versus Datenqualität

Literatur

- Pang-Ning Tan, Michael Steinbach, Vipin Kumar: Introduction to Data Mining, Prentice Hall, 2013
- Charu C. Aggarwal, Philip S. Yu: Privacy-Preserving Data Mining: Models and Algorithms, Springer Verlag, 2010
- Jaideep Vaidya, Christopher W. Clifton, Yu Michael Zhu: Privacy Preserving Data Mining, Springer Science & Business Media, 2006
- Raymond Chi-Wing Wong, Ada Fu: Privacy-Preserving Data Publishing: An Overview, Morgan & Claypool Publishers, 2010
- Francesco Bonchi, Elena Ferrari: Privacy-Aware Knowledge Discovery: Novel Applications and New Techniques, CRC Press, 02.12.2010

Hinweise

Dieses Modul ist Bestandteil folgender Studienprogramme:

- Weiterbildender Masterstudiengang Datenschutz und Sicherheit in den Informationssystemen (geplant)
- Masterstudiengang Informations- und Kommunikationstechnik (im offenen Programm zur Profilierung)
- Masterstudiengang Wirtschaftsinformatik (im offenen Programm zur Profilierung)

Datenschutz und Data Science

Modulniveau	Sprache	Semesterdauer	Häufigkeit
Master	Deutsch	Einsemestrig	Einmal im Studienjahr
Credits:	**Gesamtstunden**	**Präsenzstunden**	**Eigenstudiumsstunden**
5 ECTS	125	36	89
Studien-/Prüfungs-leistung	**Prüfungsart**	**Prüfungsdauer in Minuten**	**Wiederholungs-möglichkeit**
Alternativ	Beleg	-	Jeweils im Folgesemester

Ziele – Kompetenzen, Lern- und Qualifikationsziele

Dieses Modul vermittelt und stärkt die Kompetenzen zum kritischen Hinterfragen von aktuellen Data Science-Verfahren und -Anwendungen in Bezug auf die bei deren Einsatz zu erwartenden Datenschutz- und Sicherheitsprobleme. Dabei können die Studierenden komplexe, interdisziplinäre Fragestellungen allein oder in einem Team aufgreifen. Sie können mit Hilfe von Fachwissen aus anderen Modulen auf diese Probleme zugeschnittene, integrierte Lösungen entwerfen und diskutieren, und auf diesem Wege innovative praktische und wissenschaftliche Beiträge entwickeln.

Modulverantwortliche

- Prof. Dr. Erik Buchmann; buchmann@hftl.de

Inhalt

- Verteilte Datenmanagement-Lösungen wie das Hadoop-FS, Key-Value Stores und NoSQL-Datenbanken
- Big Data- und Cloud Computing-Middleware wie Apache Spark und Hadoop
- Knowledge Discovery und Data Mining für Big-Data
- Formale Grundlagen, Statistik und Visualisierung von Big Data
- Innovationen und Geschäftsmodelle für Big Data
- Gesellschaftliche und ethische Implikationen
- Datenschutz und Datensicherheit bei Big Data

Literatur

- Primärliteratur aus der Forschung wird in der Vorlesung bekanntgegeben.

Hinweise

Dieses Modul ist Bestandteil folgender Studienprogramme:

- Weiterbildender Masterstudiengang Datenschutz und Sicherheit in den Informationssystemen (geplant)
- Masterstudiengang Informations- und Kommunikationstechnik (im offenen Programm zur Profilierung)
- Masterstudiengang Wirtschaftsinformatik (im offenen Programm zur Profilierung)

Interdisziplinäres Datenschutz-Seminar

Modulniveau	Sprache	Semesterdauer	Häufigkeit
Master	Deutsch	Einsemestrig	Einmal im Studienjahr
Credits:	**Gesamtstunden**	**Präsenzstunden**	**Eigenstudiumsstunden**
5 ECTS	125	36	89
Studien-/Prüfungs-leistung	**Prüfungsart**	**Prüfungsdauer in Minuten**	**Wiederholungs-möglichkeit**
Alternativ	Beleg	-	Jeweils im Folgesemester

Ziele – Kompetenzen, Lern- und Qualifikationsziele

Eine wesentliche Eigenschaft von Datenschutz-Problemen besteht darin, dass dabei Aspekte aus vielen unterschiedlichen Fachrichtungen eine Rolle spielen, z. B. rechtliche Fragestellungen, ökonomische und strategische Ziele des Unternehmens, Nutzerwünsche und technische Gegebenheiten. Dieses Seminar zielt darauf ab, die interdisziplinäre Kompetenz der Studenten zu stärken. Zu diesem Zweck sollen sich die Seminarteilnehmer in eine für sie fachfremde Thematik einarbeiten und diese vor Komilitonen und Fachfremden verständlich präsentieren und vertreten.

Modulverantwortliche

- Prof. Dr. Erik Buchmann; buchmann@hftl.de

Inhalt

- Kommunikation von Informatik-Inhalten für Fachfremde
- Aufgreifen von fachfremden Themen
- Interdisziplinäre Teamarbeit

Literatur

- Primärliteratur aus der Forschung wird in der Vorlesung bekanntgegeben.

Hinweise

Dieses Modul ist Bestandteil folgender Studienprogramme:

- Weiterbildender Masterstudiengang Datenschutz und Sicherheit in den Informationssystemen (geplant)

- Masterstudiengang Informations- und Kommunikationstechnik (im offenen Programm zur Profilierung)
- Masterstudiengang Wirtschaftsinformatik (im offenen Programm zur Profilierung)

Datenschutz und Sicherheit

Modulniveau	Sprache	Semesterdauer	Häufigkeit
Master	Deutsch	Einsemestrig	Einmal im Studienjahr
Credits:	**Gesamtstunden**	**Präsenzstunden**	**Eigenstudiumsstunden**
5 ECTS	125	36	89
Studien-/Prüfungs-leistung	**Prüfungsart**	**Prüfungsdauer in Minuten**	**Wiederholungs-möglichkeit**
Alternativ	Beleg und Kolloquium	30 min	Jeweils im Folgesemester

Ziele – Kompetenzen, Lern- und Qualifikationsziele

In diesem Praktikum erwerben die Studierenden die erforderlichen Kompetenzen zum Analysieren, Entwickeln, Restrukturieren, Integrieren und Realisieren von komplexen Unternehmensstrukturen und Geschäftsprozessen nach Datenschutz- und Sicherheitskriterien. Dazu zählt insbesondere die Fähigkeit, Fachwissen über aktuelle Verfahren und Methoden aus den bereits absolvierten Modulen zu Lösungen zu kombinieren, die komplexen sowie ggf. widersprüchlichen Anforderungen aus allen betrieblichen Fachgebieten genügen. Die Studierenden können aktuelle Konzepten und Methoden zur Umsetzung von Datenschutz- und Sicherheitszielen in Informationssystemen gemeinsam mit den Beteiligten aus unterschiedlichen Fachgebieten einer kritschen Evaluation zu unterziehen. Sie sind damit in der Lage, sowohl wissenschaftliche als auch praktische Beiträge in diesem Bereich zu leisten.

Modulverantwortliche

- Prof. Dr. Erik Buchmann; buchmann@hftl.de
- Prof. Dr. Andreas Hartmann; hartmann@hftl.de

Inhalt

- Praktische Anwendung des Erlernten aus den in im Regelstudienablauf vorgelagerten Modulen
- Modellierung eines integrierten Geschäftsvorgangs nach Datenschutz- und Sicherheitskriterien
- Analyse und Evaluation einer vorgegebenen IT-Komponente
- Praktischer Umgang mit widersprüchlichen Anforderungen aus unterschiedlichen Fächern
- Evaluierung des eigenen Modells nach Leistungs-, Datensicherheits- und Datenschutzkriterien

Literatur

- Primärliteratur aus der Forschung wird in der Vorlesung bekanntgegeben.

Hinweise

Dieses Modul ist Bestandteil folgender Studienprogramme:

- Weiterbildender Masterstudiengang Datenschutz und Sicherheit in den Informationssystemen (geplant)
- Masterstudiengang Informations- und Kommunikationstechnik (im offenen Programm zur Profilierung)
- Masterstudiengang Wirtschaftsinformatik (im offenen Programm zur Profilierung)