KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Biometryczne uwierzytelnianie tożsamości [S1Cybez1>BUT]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
24

Laboratorium
24

Inne
0

Ćwiczenia
0

Projekty/seminaria
16

Liczba punktów ECTS

4,00

Koordynatorzy

dr inż. Sławomir Maćkowiak
slawomir.mackowiak@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student powinien posiadać podstawową wiedzę z zakresu matematyki oraz informatyki, szczególnie w obszarze przetwarzania danych i algorytmów. Wskazana jest znajomość programowania w Pythonie oraz podstawowe umiejętności analizy danych multimedialnych, takich jak obrazy i dźwięk. Mile widziane jest wcześniejsze zapoznanie się z tematyką bezpieczeństwa cyfrowego oraz ochrony danych, które pozwolą na lepsze zrozumienie problematyki uwierzytelniania biometrycznego. Studenci powinni także umieć pracować z narzędziami analitycznymi oraz wykazywać otwartość na stosowanie nowoczesnych technologii w praktycznych zadaniach laboratoryjnych.

Cel przedmiotu

Celem przedmiotu "Biometryczne uwierzytelnianie tożsamości” jest zapoznanie studentów z nowoczesnymi technikami biometrycznymi wykorzystywanymi do weryfikacji i zabezpieczania tożsamości w środowisku cyfrowym. Kurs umożliwia zdobycie wiedzy teoretycznej oraz umiejętności praktycznych w zakresie analizy danych biometrycznych, takich jak obrazy, dźwięki i zachowania użytkowników. Studenci poznają metody implementacji algorytmów uwierzytelniania, techniki ochrony danych biometrycznych przed fałszerstwami oraz zastosowania biometrii w różnych dziedzinach, od zabezpieczania transakcji po zaawansowane systemy identyfikacyjne. Po ukończeniu kursu studenci będą potrafili projektować, testować i oceniać systemy biometryczne w kontekście ich skuteczności i bezpieczeństwa.

Przedmiotowe efekty uczenia się

Wiedza:
• K1_W05 - Ma zaawansowaną wiedzę w zakresie złożonych struktur danych; zna podstawy teorii, zasady administrowania danymi i związane z nimi standardy; zna zasady cyberbezpieczeństwa i prywatności wykorzystywane do zarządzania ryzykiem związanym z wykorzystywaniem, przetwarzaniem, przechowywaniem i przesyłaniem informacji lub danych.
• K1_W12 - Ma pogłębioną wiedzę w zakresie autentykacji, autoryzacji i zasad kontroli dostępu do systemów komputerowych; jest świadom konieczności stosowania polityk kontroli dostępu oraz ich adaptacji do poziomu ryzyka; zna zasady uwierzytelniania biometrycznego.
• K1_W13 - Zna zasady ukrywania danych, tj. kryptografię i steganografię; ma zaawansowaną wiedzę z zakresu kryptografii, algorytmów kryptograficznych, ich ograniczeń i ich udziału w cyberbezpieczeństwie.
• K1_W17 - Ma pogłębioną wiedzę w odniesieniu do przepisów prawa, regulacji, zasad i etyki w zakresie cyberbezpieczeństwa i prywatności; jest świadom skutków operacyjnych naruszeń cyberbezpieczeństwa; ma pogłębioną wiedzę w zakresie zasad cyberbezpieczeństwa i ochrony prywatności oraz wymagań organizacyjnych (odnoszących się do poufności, integralności, dostępności, uwierzytelniania i niezaprzeczalności).
• K1_W16 - Ma podstawową wiedzę na temat systemów maszynowego uczenia się i sztucznych sieci neuronowych; ma usystematyzowaną wiedzę w zakresie zasad oraz metod rozwiązywania problemów decyzyjnych i optymalizacyjnych z zastosowaniem algorytmów heurystycznych i nieheurystycznych przeszukiwania przestrzeni stanów

Umiejętności:
• K1_U02 - Potrafi posłużyć się właściwie dobranymi metodami i narzędziami, w tym zaawansowanymi technikami informacyjno-komunikacyjnymi, a także opracować proste aplikacje lub skonfigurować proste systemy, w celu przeprowadzenia symulacji, analizy i projektowania systemów lub aplikacji właściwych dla kierunku studiów.
• K1_U03 - Potrafi zaplanować i przeprowadzić testy oprogramowania oraz systemów i sieci komputerowych w celu wykrycia w nich podatności na ataki; potrafi zaproponować rozwiązania poprawiające bezpieczeństwo działania.
• K1_U09 - Potrafi, z wykorzystaniem odpowiednio dobranych metod oraz narzędzi, dokonać krytycznej analizy i oceny funkcjonowania istniejących rozwiązań stosowanych w oprogramowaniu, przetwarzaniu danych oraz systemach i sieciach komputerowych.
• K1_U04 - Potrafi zaplanować i przeprowadzić symulacje komputerowe i pomiary, w tym symulacje i pomiary dotyczące działania systemów teleinformatycznych, potrafi przedstawić otrzymane wyniki w formie liczbowej i graficznej, dokonać ich interpretacji i wyciągnąć właściwe wnioski.
• K1_U07 - Potrafi, przy formułowaniu i rozwiązywaniu zadań dotyczących cyberbezpieczeństwa, dostrzegać ich aspekty systemowe i pozatechniczne, w tym etyczne, ekonomiczne i prawne

Kompetencje społeczne:
• K1_K01 - Rozumie znaczenie podnoszenia kompetencji zawodowych, osobistych i społecznych; ma świadomość, że wiedza i umiejętności w obszarze cyberbezpieczeństwa szybko ewoluują.
• K1_K02 - Rozumie znaczenie wiedzy w rozwiązywaniu problemów z zakresu cyberbezpieczeństwa; jest świadomy konieczności wykorzystania wiedzy ekspertów podczas rozwiązywania zadań inżynierskich w zakresie wykraczającym poza własne kompetencje.
• K1_K03 - Rozumie potrzebę formułowania i przekazywania społeczeństwu informacji i opinii na temat pozytywnych i negatywnych aspektów cyberbezpieczeństwa, a także jest gotowy do działania na rzecz interesu publicznego.
• K1_K05 - Ma świadomość znaczenia pracy własnej i konieczności przestrzegania zasad etyki zawodowej, jest gotowy do podporządkowania się zasadom pracy w zespole i ponoszenia

odpowiedzialności za wspólnie realizowane zadania, a także dbałości o dorobek i tradycje zawodu

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
1. Wykład
Zadanie z rozwiązywania problemów: studium przypadków, które wymagają współpracy w zespołach w celu analizy i rozwiązania problemów. Ocena umiejętności współpracy, ustalania priorytetów i proponowania skutecznych rozwiązań. Ocena krytycznego myślenia, umiejętności rozwiązywania problemów i dynamiki pracy zespołowej. Egzamin pisemy lub ustny.
Próg zaliczeniowy wynosi 50% punktów.
W przypadku zaliczenia pisemnego i ustnego punkty są sumowane.
Skala ocen: <50% - 2,0 (ndst); 50% do 59% - 3,0 (dst); 60% do 69% - 3,5 (dst+) ; 70% do 79% - 4,0 (db); 80% do 89% - 4,5 (db+); 90% do 100% - 5,0 (bdb).
2. Laboratorium
Umiejętności osiągnięte w laboratorium określa się na podstawie raportów (sprawozdań) z przeprowadzonych ćwiczeń laboratoryjnych (OL) oraz zaliczenia końcowego (ZK) w formie samodzielnie realizowanego ćwiczenia lub projektu.
Kompetencje społeczne (KS) ocenia się na podstawie oceny umiejętności aktywnego słuchania, umiejętności współpracy i efektywnego udziału w dyskusjach zespołowych oraz poziomu zaangażowania w procesy rozwiązywania problemów .
Wyznacza się średnią ważoną: OK = 0,5 x OL + 0,3 x ZK + 0,2 x KS i wystawia oceny:
5,0 dla OK > 4,75;
4,5 dla 4,75 > OK > 4,25;
4,0 dla 4,25 > OK > 3,75;
3,5 dla 3,75 > OK > 3,25;
3,0 dla 3,25 > OK > 2,75;
2,0 dla OK < 2,75.
Zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

Program przedmiotu obejmuje zarówno teoretyczne, jak i praktyczne aspekty zastosowania biometrii w weryfikacji tożsamości użytkowników. W ramach zajęć omawiane są metody biometryczne oparte na cechach fizycznych, takich jak rozpoznawanie twarzy, analiza tęczówki oka, odcisków palców i głosu, a także techniki wykorzystujące cechy behawioralne, w tym analizę rytmu pisania, sposobu poruszania się myszką oraz innych wzorców zachowań użytkownika. Studenci uczą się podstaw przetwarzania obrazów i dźwięków, stosowania algorytmów do analizy tych danych, a także metod związanych z uczeniem maszynowym. Kurs obejmuje także zagadnienia związane z zabezpieczaniem systemów biometrycznych przed atakami, ochroną danych przed manipulacją oraz technikami ich szyfrowania i przechowywania. W ramach zajęć praktycznych studenci rozwijają umiejętności implementacji i testowania systemów biometrycznych w kontekście ich skuteczności i bezpieczeństwa, a także analizują wyzwania związane z ich wykorzystaniem w rzeczywistych scenariuszach.

Tematyka zajęć

Kurs rozpoczyna się od technik biometrycznych opartych na cechach fizycznych, takich jak analiza twarzy i głosu. Studenci poznają, jak technologia rozpoznawania twarzy, oparta na wzorcach morfologicznych, jest stosowana w celu weryfikacji tożsamości. Kurs obejmuje również biometrię głosu, gdzie analizowane są cechy takie jak ton, melodia i tempo mowy, które są unikalne dla każdego użytkownika. Omówione zostaną algorytmy przetwarzania obrazów oraz sygnałów audio, a także aspekty bezpieczeństwa związane z ich implementacją. Studenci dowiedzą się, jak systemy te mogą być zabezpieczone przed różnymi atakami, takimi jak fałszywe twarze i nagrania głosu.
Kolejny blok kursu skupia się na analizie behawioralnej, która jest nowoczesnym podejściem do uwierzytelniania, opartym na unikalnych wzorcach zachowań użytkownika. Studenci poznają techniki analizy zachowań, takie jak sposób pisania na klawiaturze, nawyki poruszania się myszką oraz analizę rytmu wprowadzania tekstu. Kurs omawia, jak zbierane dane behawioralne mogą być przetwarzane i

porównywane w celu uwierzytelniania użytkownika, a także jak metody te mogą wzbogacać klasyczne techniki biometryczne, zwiększając poziom bezpieczeństwa. Zostaną omówione zagrożenia, takie jak podszywanie się i ataki przechwytywania danych behawioralnych, oraz strategie zabezpieczania takich systemów.
Kurs wprowadza także zagadnienia związane z cyfrowymi podpisami multimedialnymi, które służą jako dodatkowa warstwa zabezpieczająca transakcje. Studenci zapoznają się z technikami cyfrowego podpisywania dokumentów, wideo i audio, co ma na celu potwierdzenie autentyczności i integralności danych. Omówione zostaną algorytmy podpisu cyfrowego, takie jak RSA i ECDSA, oraz techniki hashowania (np. SHA-256), które są kluczowe w procesie uwierzytelniania.
Aby uzupełnić wiedzę o biometryce, kurs obejmuje także inne rodzaje danych multimedialnych, które mogą być wykorzystane w biometrycznym uwierzytelnianiu. Studenci poznają metody rozpoznawania odcisków palców z użyciem obrazów, analizę tęczówki oka oraz technologie rozpoznawania chodu na podstawie nagrań wideo. Zostaną zaprezentowane metody przechowywania i szyfrowania danych biometrycznych, jak również techniki wykrywania i obrony przed spoofingiem, czyli próbami podszycia się pod oryginalnego użytkownika za pomocą fałszywych wzorców biometrycznych.
Zajęcia praktyczne w laboratorium:
- Bezpieczne uwierzytelnianie z wykorzystaniem biometrii głosu i twarzy
- Analiza behawioralna jako metoda uwierzytelniania
- Techniki zabezpieczania transakcji z użyciem cyfrowych podpisów multimedialnych
- Zaawansowane techniki biometryczne z wykorzystaniem danych multimedialnych

Metody dydaktyczne

1. Techniki aktywnego uczenia się: Strategie aktywnego uczenia się, takie jak dyskusje w grupach, rozwiązywanie problemów i studia przypadków, aby aktywnie zaangażować studentów w proces uczenia się. Zachęcanie do wspólnego uczenia się i interakcji, aby wspierać krytyczne myślenie i stosowanie wiedzy.
2. Integracja technologii: Wykorzystanie narzędzi i platformy technologicznej, aby poprawić jakość nauki. Korzystanie z narzędzi do współpracy online podczas sesji burzy mózgów, wirtualnych symulacji do rozwiązywania problemów oraz prezentacji multimedialnych, aby dostarczać wciągające treści. Ponadto wykorzystanie internetowych forów dyskusyjnych lub systemów zarządzania nauczaniem do asynchronicznego uczenia się i udostępniania zasobów.
3. Uczenie się oparte na przypadkach: włączenie rzeczywistych studiów przypadków do wykładów i laboratoriów, aby zademonstrować praktyczne zastosowanie kreatywnego myślenia w rozwiązywaniu problemów technicznych. Zachęci to do analizowania i omawiania przypadków, identyfikowania kreatywnych rozwiązań i refleksji nad procesem podejmowania decyzji.
4. Informacja zwrotna i nauczanie od studentów: Wprowadzenie mechanizmów informacji zwrotnej od studentów, w ramach których uczniowie przekazują konstruktywne informacje zwrotne na temat podejść do rozwiązywania problemów lub rozwiązań projektowych swoich rówieśników. Zachęcanie do sesji nauczania studenckiego, podczas których studenci mogą dzielić się swoją wiedzą i kreatywnymi technikami z kolegami.
5. Nauka oparta na projektach: Włączenie nauki opartej na projektach do programu nauczania, w której studenci pracują nad rzeczywistymi problemami lub projektują wyzwania wymagające kreatywnego myślenia. Takie podejście pozwala zastosować swoje umiejętności, przeprowadzić dogłębne badania i opracować innowacyjne rozwiązania poprzez praktyczne, empiryczne uczenie się.
6. Wykłady online

Literatura

Podstawowa:
• Anil K. Jain, Patrick Flynn, Arun A. Ross, Handbook of Biometrics, Springer, 2007.
• David D. Zhang, Automated Biometrics: Technologies and Systems, Kluwer Academic Publishers, 2000.
• James Wayman, Anil K. Jain, Davide Maltoni, Dario Maio, Biometric Systems: Technology, Design and Performance Evaluation, Springer, 2005.

Uzupełniająca:
Uzupełniająca
• Anil K. Jain, Ruud M. Bolle, Sharath Pankanti, Biometrics: Personal Identification in Networked Society, Springer, 1999.

• Julian Ashbourn, Practical Biometrics: From Aspiration to Implementation, Springer, 2004.
• John Chirillo, Scott Blaul, Implementing Biometric Security, Wiley, 2003.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	119	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	64	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	55	2,00