אוניברסיטת תל אביב
TEL AVIV UNIVERSITY

סילבוס מפורט

שם הקורס

פרטיות מידע

מרצה

אורי שטמר

סמסטר

2021/2 - ב' תשפ"ב

קורסי קדם נדרשים

מבוא להסתברות + אלגוריתמים

הרכב הציון הסופי

תרגילי בית ובחינה סופית

מבנה הקורס

דמיינו ארגון המחזיק מאגר מידע גדול עם נתונים אישיים של אנשים, כמו למשל בית חולים או הלשכה המרכזית לסטטיסטיקה. מצד אחד, הארגון רוצה לאפשר גישה מסויימת למידע הזה (למשל לחוקרים, על מנת ללמוד על מחלות חדשות). מצד שני, הארגון רוצה להבטיח שהגישה הזאת לנתונים לא מסכנת את הפרטיות של האנשים שהמידע שלהם נמצא במאגר. השאלה הראשונה כאן היא איך נוכל להגדיר מהי פגיעה בפרטיות בהקשר הזה. למרות שהשאלה אולי נראית פשוטה במבט ראשון, מתברר שזאת שאלה מאוד טעונה. לאחר שמסכימים על ההגדרה, השאלה הבאה היא תחת אילו תנאים ניתן לבנות וואריאנטים פרטיים לאלגוריתמי ניתוח מידע קיימים, ומהו המחיר לכך? בקורס זה נבחן את השאלות האלו מנקודת מבט תיאורטית. אנו נתמקד בהגדרת פרטיות הנקראת פרטיות דפרנציאלית, שהיא הגדרה מתמטית מחמירה של פרטיות. בפרט, נדבר על הנושאים הבאים:

מתקפת שחזור נתונים והפרת פרטיות בוטה

פרטיות דפרנציאלית (הגדרות ותכונות)

אלגוריתמים בסיסיים המשמרים פרטיות

אלגוריתמים למענה על שאילתות

אלגוריתמי למידה

המודל הלוקלי של פרטיות דפרנציאלית

מודל ה shuffle

נושאים נוספים בהתאם לשיקול המרצה

קריאת חובה

קריאת רשות

הערות