פרק א - **'goldrive'** - ייזום

**1.** הפרויקט הוא תוכנת שיתוף. לכל משתמש יהיה אזור אישי ואזור שיתופי, באזור האישי הקבצים נגישים רק אל המשתמש ובאזור השיתופי המשתמש יוכל לשתף קבצים וגם הקבצים ששותפו אתו ימצאו שם. קבצים יוכלו להינעל על ידי סיסמא כדי ליצור עוד שכבה של פרטיות לקבצים פרטיים. בחרתי בפרויקט משום שהוא היה נראה מעניין ויכול לתרום לי בכך שישמור לי קבצים במקום שאני סומך עליו ואני יודע שהוא מאובטח. אתגרים שצפויים לי בפרויקט היא אחסון הקבצים בצורה יעילה ושיתוף הקבצים בין משתמשים.

**2.** הפרויקט מיועד לאנשים שמשתמשים בהרבה קבצים ובעיקר לאנשים שמשתפים קבצים עם אנשים אחרים, משום שאפשר בנוחות לאחסן קבצים משותפים ואישיים במקום אחד.

**3.** מטרת הפרויקט היא:

* לאפשר למשתמשים מקום אחסון בטוח ונוח לשימוש לקבצים חשובים או קבצי עבודה ופנאי.
* לאפשר מקום נגיש לכל משתמש רשום מכל מקום ברשת.
* ליצור דרך נוחה ופשוטה לשיתוף קבצים עם משתמשים אחרים.

**4.** הבעיה והתועלות:  
הבעיה העיקרית הינה מציאת פתרון ליכולת מצד אחד לשמור קבצים בצורה מאובטחת ומהצד השני אפשרות לגשת לקבצים האלו מכל מקום ברשת, לשתפם עם אחרים ועוד.  
התועלות של המערכת שלי היא במתן מקום אחסון נוח ומאובטח ברשת עם יכולת לגשת אליו בדרך בטוחה ועם יכולות של שיתוף קבצים עם אחרים ועוד.

סקירת פתרונות הקיימים בשוק:

פתרון ראשון שקיים בשוק הוא הגוגל דרייב, בעזרת חשבון הGmail שלך ניתן לגשת לדרייב ולשמור קבצים שם, הקבצים נשמרים אוטומטית, הבעיה עם הדרייב של גוגל הוא שצריך משתמש מייל ולא מתאפשרת נעילת קבצים.   
הפתרון השני שקיים הוא דרופבוקס, בדומה לדרייב של גוגל התוכנה היא מקום שבו ניתן לשמור קבצים במקום מרוכז אחד, וגם היא לא מאפשרת לנעול קבצים. בנוסף אינה שומרת את הקבצים בצורה אוטומטית לאחר שעורכים אותם.

**5.** הטכנולוגיה אינה חדשה ונמצאת בשוק כבר מעל ל15 שנה אך היא כל הזמן משתנה ומשתפרת, בין אם זה ביעילות השמירה של הקבצים או ההצפנה.

הגבלה שתוכל לנבוע היא הבעיה של שמירת הקבצים משום שייתכן שייגמר המקום במקום שבו אנחנו שומרים את הקבצים.  
בנוסף בגלל הגבלות הרשת של בית הספר, התוכנה תהיה סגורה ותתאפשר גישה אך ורק למשתמשים ברשת הבית ספרית.

**6.** התחומים בהם הפרויקט עוסק הוא רשתות (שרת מרובה לקוחות), משום שהעלאות קבצים והורדת קבצים מהשרת משתמשת ברשת, קבצים, מערכות הפעלה משום שיש הרבה threadים וכמובן גם הצפנה חזקה כדי לשמור על פרטיות הקבצים.

**7.** הפרויקט מתחבר לקיימות בכך ששומר על עבודה ממוחשבת ובכך חוסך כריתת עצים לייצור ניירות משום שהקבצים נמצאים במחשב ולא נכתבים על דף.

פרק ב - **'goldrive'** - אפיון

**1.** הפרויקט יהיה מקום לשמור קבצים בצורה נוחה ויעילה הוא יאפשר למשתמשיו גם נוחות וגם ביטחון משום שקבציי הפרויקט יהיו מוצפנים וכל משתמש יהיה מוגן בעזרת שם משתמש וסיסמא, בנוסף לכך לכל קובץ תהיה אפשרות נעילה שתספק מנגנון הגנה. והכי חשוב ניתן יהיה לגשת לקבצים מכל מחשב ברשת.

**2.** הפרויקט יעניק את היכולות הבאות**:**

* הרשמה כמשתמש חדש במערכת
* התחברות למשתמש קיים במערכת
* העלאת קבצים לאזור הבטוח
* הורדת קבצים מהאזור הבטוח
* שיתוף קבצים עם חברים אחרים
* מחיקת קבצים
* נעילת קבצים
* פעולות שונות על הקבצים כגון שכפול, שינוי שם ועוד
* גישה לאזור הבטוח מכל מקום ברשת
* אבטחה מרבית לקבצים (הצפנה, נעילה, סיסמאות ועוד)

**3. בדיקות קופסא שחורה:**

| **מספר** | **שם הבדיקה (שם שיעיד על תוכן הבדיקה)** | **מה אמורה לבדוק** | **איך מתכננים לבדוק(לתאר בפירוט את שלבי הבדיקה)** |
| --- | --- | --- | --- |
| **1** | **התחברות** | **האם אפשר להתחבר למשתמש כמו שצריך** | **לפתוח את המערכת, להתחבר עם שם משתמש וסיסמא נכונים ולראות שמצליחים להיכנס למערכת.**  **לחזור על הפעולה עם שם משתמש וסיסמא שגויה ולראות שלא מצליחים להיכנס למערכת** |
| 2 | העלאת קבצים | האם אפשר לשמור קבצים למשתמש | לפתוח את המערכת ולהתחבר עם שם סיסמא ומשתמש, לנסות להעלות קובץ ולראות שהוא עלה ומוצג בקבצים שלי, במידה והוא עלה להתנתק מהמשתמש ולהתחבר שוב ולראות שהקובץ עדיין מוצג. |
| 3 | הורדת קבצים | האם אפשר להוריד קבצים | לפתוח את התוכנה, להתחבר למשתמש, לבחור קובץ ולנסות להוריד אותו, לבדוק האם הקובץ מורד כמו שצריך ובמקום הנכון. |
| 4 | איש שלישי | האם אפשר לקרוא מידע שעובר | לפתוח Wireshark ואז לפתוח את התוכנה, להתחבר למשתמש ולנסות להעלות קובץ אחר כך לבדוק Wireshark האם אפשר לקרוא את המידע שעבר או שהוא מוצפן. |
| 5 | שיתוף קבצים | האם אפשר לשתף קובץ עם חבר | לפתוח את התוכנה להתחבר למשתמש, לבחור קובץ ולשתף אותו עם משתמש אחר, להתחבר למשתמש האחר ולראות האם הקובץ ששותף מופיע באזור השיתופים. |
| 6 | מחיקת קבצים | האם אפשר למחוק קבצים | לפתוח את התוכנה, להתחבר למשתמש, לבחור קובץ ולנסות למחוק אותו, לראות שהקובץ נמחק ולא מופיע, להתחבר מחדש למשתמש ולראות שהקובץ עדיין לא מופיע. |
| 7 | שינוי שם | האם אפשר לשנות שם לקובץ | לפתוח את התוכנה, להתחבר למשתמש, לבחור קובץ ולנסות לשנות לו את השם, לראות שהשם משתנה כמו שצריך, להתחבר מחדש ולראות שהשם נותר משונה. |
| 8 | כניסה כפולה | לבדוק האם המערכת מונעת ממשתמש אחד להיכנס בו זמנית ממחשבים שונים | לפתוח את התוכנה, ליצור משתמש, לראות שמתחבר כמו שצריך, ולנסות להתחבר לאותו משתמש ממחשב אחר ולראות שזה **לא** מתחבר. |
| 9 | בדיקת ביצועים | לבדוק האם המערכת מבצעת פעולות במהירות | לפתוח את התוכנה, להתחבר למשתמש ולנסות לבדוק כל פעולה שמתאפשרת לקובץ ולבדוק שהכל נעשה במהירות. |
| 10 | בדיקת יציבות | לבדוק האם המערכת מתפקדת בקביעות למרות שיש מספר משתמשים מחוברים | לפתוח את התוכנה במספר מחשבים, להתחבר מכל מחשב למשתמש ומכל משתמש להריץ איזושהי פעולה על קובץ, לראות שבכל משתמש הפעולה נעשתה כמו שצריך. |
| 11 | זמני תגובה | לבדוק האם יש הבדלים בזמני התגובה של המערכת כאשר מורידים/מעלים קבצים בגדלים שונים | לפתוח את התוכנה, להתחבר למשתמש ולנסות להעלות ולהוריד קבצים שונים בעלי גודל שונה ולבדוק את הזמן שלוקח. |

**4. תכנון לו"ז:**

| **פעילות** | **זמן התחלה מתוכנן** | **זמן סיום מתוכנן** | **זמן התחלה בפועל** | **זמן סיום בפועל** | **הערות** |
| --- | --- | --- | --- | --- | --- |
| יזום | 1.11.23 | 23.11.23 | 6.11.23 | 7.11.23 | הוגש לפני הזמן |
| אפיון | 23.11.23 | 1.12.23 | 14.11.23 | 18.11.23 | הוגש לפני הזמן |
| ניתוח | 1.12.23 | 15.12.23 | 18.11.23 | 30.11.23 | הוגש לפני הזמן |
| עיצוב | 15.12.23 | 15.1.24 | 30.11.23 | 11.1.24 | הוגש לפני הזמן |
| בניית שרת מרובה לקוחות בסיסי | 15.1.24 | 18.1.24 | 11.1.24 | 11.1.24 | סוים לפני הזמן |
| הוספת ממסד נתונים | 18.1.24 | 20.1.24 | 11.1.24 | 11.1.24 | סוים לפני הזמן |
| בניית ממשק לקוח | 20.1.24 | 30.1.24 | 12.1.24 | 22.1.24 | סוים לפני הזמן |
| טיפול בקבצים העלאת קבצים מחיקת קבצים שינוי שם | 30.1.24 | 10.2.24 | 25.1.24 | 26.1.24 | סוים לפני הזמן |
| בניית יכולת לשיתוף קבצים עם משתמשים אחרים | 10.2.24 | 16.2.24 | 28.1.24 | 28.1.24 | סוים לפני הזמן |
| הוספת הצפנות | 16.2.24 | 18.2.24 | 11.1.24 | 12.1.24 | סוים לפני הזמן |
| תיקון באגים | 18.2.24 | 25.2.24 | תוך כדי הפרויקט | תוך כדי הפרויקט | התבצע תוך כדי כתיבת הקוד |
| גרסה ראשונית | 25.2.24 | 1.3.24 | 11.1.24 | 1.3.24 | הוגש בזמן |
| מסמך בדיקות | 1.3.24 | 10.4.24 |  |  |  |
| מדריך למשתמש | 10.4.24 | 1.5.24 |  |  |  |
| גרסה סופית | 10.5.24 | 10.5.24 |  |  |  |
| סגירת תיק פרויקט |  |  |  |  |  |
| מצגת הסבר |  |  |  |  |  |

**5. סיכונים:**

| **הסיכון** | **פירוט הסיכון** | **רמת הסיכון**  **(קל/בינוני/קשה)** | **תיאור דרכים (לפחות 2 ) להתמודדות עם הסיכון ולהקטין אותו** | **מה בוצע בפועל** | **תאריך** |
| --- | --- | --- | --- | --- | --- |
| תכנות מבולגן | ייקח יותר זמן לתכנת כל דבר | קל | * מההתחלה ליצור פעולות ומחלקות נוחות * לכתוב קוד קריא וברור להבנה | הקוד היה כתוב יפה ומסודר | 2.5.24 |
| להתקע על פרטים קטנים | פרויקט יוגש באיחור | בינוני | * גם אם יש באג קטן להמשיך לאבנים הגדולות ולחזור אחר כך * לא קל דבר קטן צריך לעבוד עליו ואפשר לפעמים לוותר על דברים | לא נתקעתי על פרטים קטנים יותר מידי | 2.5.24 |
| תכנות לא יעיל | ירדו נקודות | בינוני | * להיעזר בחברים כדי לקבל עצות * להיעזר באינטרנט כדי למצוא פתרונות יעילים של אנשים לבעיות | התכנות כתוב בצורה יעילה | 2.5.24 |
| אי עמידה בזמנים | פרויקט לא יושלם | קשה | * הקדמת לו"זים משימות * ארגון הזמן בצורה יעילה * להתחיל בדברים היותר קשים | עמידה בזמנים של כתיבת הקוד תוך כדי עמידה בזמנים, בתיק הפרויקט היו קצת עיקובים | 2.5.24 |
| ביצועים גרועים | העלאת והורדת קבצים תיקח זמן רב | קשה | * להיעזר במורה ובחברים מהכיתה כדי למצוא מה מעקב את התוכנית * להריץ כל פעולה בנפרד ולראות האם הבעיה היא כללית או ספציפית | העלאת והורדת קובץ לוקחת זמן קצר | 2.5.24 |
| יציבות | המערכת לא תתפקד עם משתמשים רבים | קשה | * לבדוק האם הבעיה קשורה לכמות המשתמשים או שבכלליות לחיבור של יותר ממשתמש אחד * להריץ פעולות שונות ולראות אם כל הפעולות לא עובדות בחיבור רק של משתמשים או רק פעולות ספציפיות | המערכת מתפקדת היטב גם עם מספר משתמשים רב | 2.5.24 |

**פרק ג - 'goldrive' - ניתוח**

**1. יכולות בצד לקוח:**

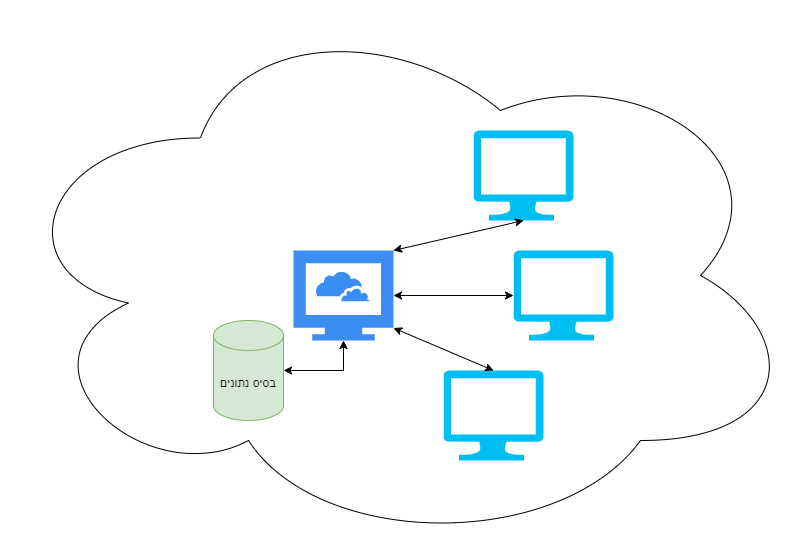
| **שם היכולת** | **מהות היכולת** | **רשימת יכולות** | **רשימת אובייקטים** |
| --- | --- | --- | --- |
| הרשמת משתמש | הרשמת משתמש חדש למערכת | * פתיחת הממשק * קבלת הכנסת פרטי משתמש * הצפנת התוכן * שליחה לשרת * קבלת תשובה מהשרת * פענוח התשובה מהשרת * הצגת התשובה | * תקשורת * הצפנה ופענוח * ממשק משתמש |
| התחברות למשתמש | התחברות למשתמש שקיים במערכת | * פתיחת הממשק * קבלת הכנסת פרטי המשתמש * הצפנת התוכן * שליחה לשרת * קבלת תשובה מהשרת * פענוח התשובה מהשרת * הצגת התשובה | * תקשורת * הצפנה ופענוח * ממשק משתמש |
| העלאת קובץ | העלאת קובץ לענן | * פתיחת ממשק המשתמש * קבלת הקובץ להעלאה * הצפנת הקובץ * שליחה לשרת * קבלת תשובה מהשרת * פענוח התשובה מהשרת * הצגת התשובה | * תקשורת * הצפנה ופענוח * ממשק משתמש * מערכת קבצים |
| הורדת קובץ | הורדת קובץ מהענן | * פתיחת ממשק המשתמש * קבלת הקובץ להורדה * הצפנת שם הקובץ * שליחה לשרת * קבלת תשובה מהשרת * פענוח התשובה מהשרת * הצגת התשובה (הקובץ המורד במידה והצליח) | * תקשורת * הצפנה ופענוח * ממשק משתמש * מערכת קבצים |
| שיתוף קבצים | שיתוף קבצים למשתמשים אחרים | * פתיחת ממשק המשתמש * בחירת קובץ לשיתוף ושם המשתמש אותו רוצה לשתף * הצפנת התוכן * שליחה לשרת * קבלת תשובה מהשרת * פענוח תשובה מהשרת * הצגת התשובה מהשרת | * תקשורת * הצפנה ופענוח * ממשק משתמש * מערכת קבצים |
| מחיקת קובץ | מחיקת קובץ מהענן | * פתיחת ממשק המשתמש * בחירת קובץ למחיקה * הצפנת שם הקובץ * שליחת בקשה למחיקה מהשרת * קבלת תשובה מהשרת * פענוח התשובה מהשרת * הצגת התשובה מהשרת | * תקשורת * הצפנה ופענוח * ממשק משתמש * מערכת קבצים |
| נעילת קבצים | נעילת קבצים באמצעות סיסמא נוספת | * פתיחת ממשק המשתמש * קליטת שם קובץ וסיסמא לנעילה * הצפנת התוכן * שליחה לשרת * קבלת תשובה מהשרת * פענוח תשובה מהשרת * הצגת התשובה מהשרת | * תקשורת * הצפנה ופענוח * ממשק משתמש |
| שכפול קובץ | שכפול קובץ | * פתיחת ממשק המשתמש * קליטת שם קובץ לשכפול * הצפנת שם הקובץ * שליחה לשרת * קבלת תשובה מהשרת * פענוח תשובה מהשרת * הצגת התשובה מהשרת | * תקשורת * הצפנה ופענוח * ממשק משתמש * מערכת קבצים |
| שינוי שם | שינוי שם לקובץ | * פתיחת ממשק המשתמש * קליטת שם הקובץ לשינוי ושם חדש * הצפנת התוכן * שליחה לשרת * קבלת תשובה מהשרת * פענוח תשובה מהשרת * הצגת התשובה מהשרת | * תקשורת * הצפנה ופענוח * ממשק משתמש * מערכת קבצים |

**יכולות בצד שרת:**

| **שם היכולת** | **מהות היכולת** | **רשימת יכולות** | **רשימת אובייקטים** |
| --- | --- | --- | --- |
| הרשמת משתמש | הרשמת משתמש חדש למערכת | * קבלת מידע מהמשתמש * פענוח מידע מהמשתמש * הוספה לבסיס נתונים אם תקין * החזרת תשובה מוצפנת ללקוח | * תקשורת * הצפנה ופענוח * בסיס נתונים |
| התחברות למשתמש | התחברות למשתמש שקיים במערכת | * קבלת מידע מהמשתמש * פענוח מידע מהמשתמש * בדיקת קיימות בבסיס הנתונים * החזרת תשובה מוצפנת ללקוח | * תקשורת * הצפנה ופענוח * בסיס נתונים |
| העלאת קובץ | העלאת קובץ לענן | * קבלת מידע מהמשתמש * פענוח מידע מהמשתמש * בדיקת תקינות הקובץ * הוספת הקובץ לענן במידה ותקין * החזרת תשובה מוצפנת ללקוח | * תקשורת * הצפנה ופענוח * בסיס נתונים * מערכת קבצים |
| הורדת קובץ | הורדת קובץ מהענן | * קבלת מידע מהמשתמש * פענוח המידע מהמשתמש * בדיקת תקינות הקובץ * הצפנת תוכן הקובץ * שליחת תשובה ותוכן הקובץ במידה ותקין | * תקשורת * הצפנה ופענוח * בסיס נתונים * מערכת קבצים |
| שיתוף קבצים | שיתוף קבצים למשתמשים אחרים | * קבלת מידע מהמשתמש * פענוח המידע מהמשתמש * בדיקת תקינות המשתמש לשיתוף בבסיס הנתונים * הוספת הקובץ למשתמש ששותף * החזרת תשובה מוצפנת ללקוח | * תקשורת * הצפנה ופענוח * בסיס נתונים * מערכת קבצים |
| מחיקת קובץ | מחיקת קובץ מהענן | * קבלת מידע מהמשתמש * פענוח המידע מהמשתמש * בדיקת תקינות הקובץ בענן * מחיקת הקובץ במידה ותקין * החזרת תשובה מוצפנת ללקוח | * תקשורת * הצפנה ופענוח * בסיס נתונים * מערכת קבצים |
| נעילת קבצים | נעילת קבצים באמצעות סיסמא נוספת | * קבלת מידע מהמשתמש * פענוח המידע מהמשתמש * בדיקת תקינות קובץ וסיסמא * החזרת תשובה מוצפנת ללקוח | * תקשורת * הצפנה ופענוח * בסיס נתונים |
| שכפול קובץ | שכפול קובץ | * קבלת מידע מהמשתמש * פענוח המידע מהמשתמש * בדיקת תקינות הקובץ * שכפול הקובץ בענן במידה ותקין * החזרת תשובה מוצפנת ללקוח | * תקשורת * הצפנה ופענוח * בסיס נתונים * מערכת קבצים |
| שינוי שם | שינוי שם לקובץ | * קבלת מידע מהמשתמש * פענוח המידע מהמשתמש * בדיקת תקינות הקובץ והשם החדש * שינוי שם הקובץ במידה ותקין * החזרת תשובה מוצפנת ללקוח | * תקשורת * הצפנה ופענוח * בסיס נתונים * מערכת קבצים |

**פרק ד - 'goldrive' - עיצוב**

**1 . תיאור החומרה:**

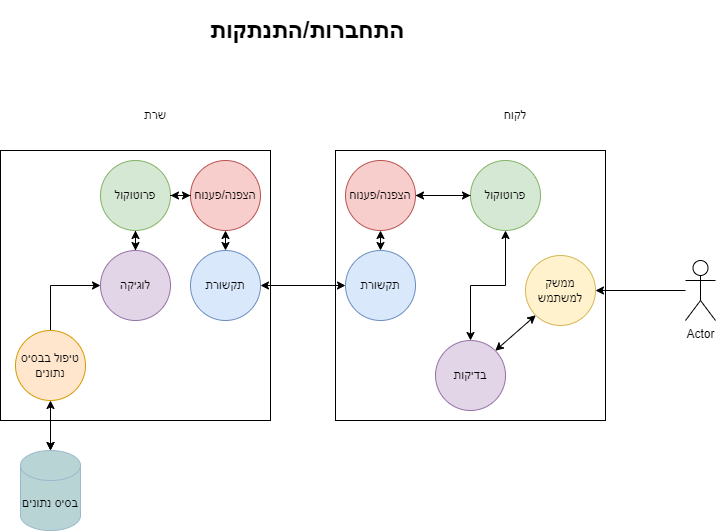
מחשב השרת ומחשבי הלקוחות מבוססי windows ארכיטקטורת התקשורת - שרת מרובה לקוחות, בסיס הנתונים sql מקושר לשרת כל המחשבים נמצאים באותה הרשת.

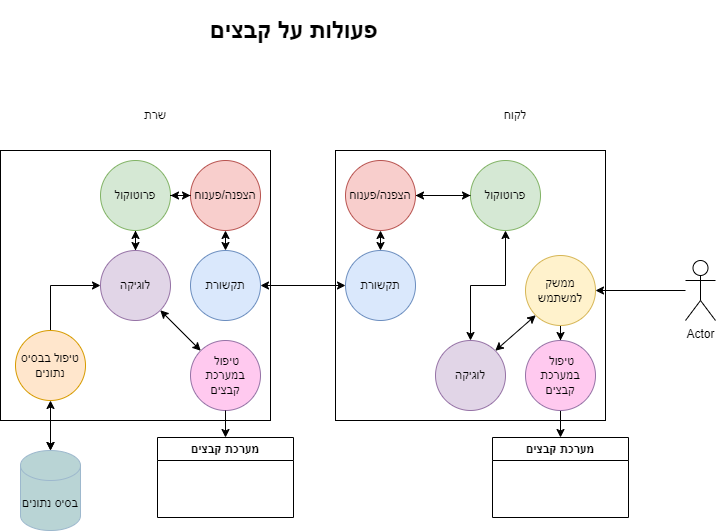
**2. תיאור הטכנולוגיות:**

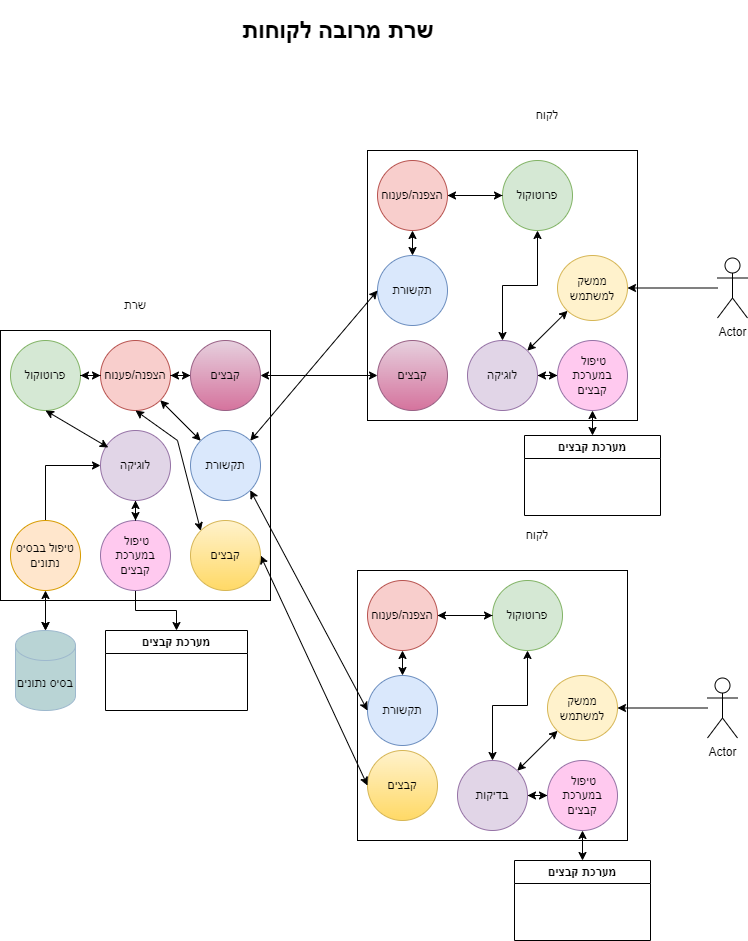
**שפות התכנות-** Python לכתיבת קוד הפרויקט וsql ובעזרת sql אני אממש את בסיס הנתונים.   
**מערכת ההפעלה-** שאני אשתמש בה היא windows.   
תקשורת- שרת מרובה לקוחות מבוסס סוקטים בפרוטוקול TCP.  
**תחומי עניין-**

* הצפנה היברדית (דיפי הלמן ליצירת מפתח סימטרי והצפנה סימטרית)
* שימוש ב thread-ים למימוש עבודה מקבילית בצד שרת והן בצד לקוח
* מערכת קבצים – לטיפול בקבצים המועלים ומורדים מהמערכת

**בסיס נתונים** - SQL בשרת

**3. תיאור תהליכי המערכת**

****

****

**מודלים שאני מייבא:**

| **שם המודל** | **ייעוד** |
| --- | --- |
| **Os** | **טיפול בקבצים** |
| **Sys** | **לסגור את הלקוח באת שגיאה** |
| **Select** | **משמש לטיפול בsocketים בצד שרת** |
| **wxpython** | **גרפיקה** |
| **Threading** | **Threading ו** **multiprocessing** |
| **Queue** | **לתורים שאני אשתמש בהם במהלך הפרויקט** |
| **Sqlite3** | **לטיפול בבסיס הנתונים** |
| **Socket** | **לתקשורת בין הלקוח והשרת** |
| **Pubsub** | **שליחת וקבלת הודעות דרך מערכת בפעלה בין הקבצים** |
| **Secrets** | **על מנת לקבל מספר בצורה רנדומלית** |
| **Shutil** | **מחיקת קבצים** |
| **Time** | **בדיקת זמן ההתחברות לשרת** |
| **Io** | **קריאת תמונות** |
| **Smtplib** | **שליחת מייל באמצעות פייתון** |
| **Zipfile** | **על מנת לארוז תיקיות לקבצי zip** |
| **Base64** | **הצפנה** |
| **Cryptodome** | **הצפנה** |
| **Hashlib** | **הצפנה** |
| **Chardet** | **הצפנה** |
| **Win32file** | **לנתר את הפעולות על קבצים** |
| **Subprocess** | **ליצור סב פרוסס** |
| **Psutil** | **לעבור על הפרוססים הקיימים** |

**מודלים שאני מייצר:**

| **serverProtocol** |
| --- |
| המחלקה שאחראית על הבנייה והפרוק של הפרוטוקול בצד השרת. |
| **תכונות** |
| |  |  |  | | --- | --- | --- | | **שם הפעולה** | **טענת כניסה** | **טענת יציאה** | | unpack\_message | msg – ההודעה שהתקבלה מהמשתמש | טאפל שכולל בתוכו את קוד הפרוטוקול ואת המשתנים. | | Get\_data\_from\_string | Msg – ההודעה להוציא ממנה מידע leng – האורך של ההודעה | את המידע שהוצא ואת ההודעה ערוכה | | pack\_files\_message | Username – שם המשתמש אליו שולחים את הקבצים | מחרוזת הקבצים של המשתמש לפי הפרוטוקול. | | pack\_register\_response | Response – התגובה לשליחה username – שם המשתמש password – סיסמת המשתמש email – אימייל המשתמש | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_login\_response | Response – התגובה לשליחה email – אימייל המשתמש | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_verify\_ check\_response | Response – התגובה לשליחה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_file\_download\_response | Response – התגובה לשליחה datalen – אורך המידע של הקובץ path – נתיב הקובץ בשרת selected\_path – נתיב הקובץ | מחרוזת הבנויה לפי הפרוטוקול. | | Pack\_upload\_port | port – הפורט להביא למשתמש | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_file\_upload\_response | Response – התגובה לשליחה path – נתיב הקובץ להעלות | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_create\_folder\_response | Response – התגובה לשליחה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_delete\_response | Response – התגובה לשליחה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_rename\_file\_response | Response – התגובה לשליחה new\_name – השם החדש של הקובץ | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_share\_response | Response – התגובה לשליחה | מחרוזת הבנויה לפי הפרוטוקול. | | Pack\_change\_photo\_response | Response – התגובה לשליחה file\_len – אורך מידע הקובץ | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_change\_username\_response | Response – התגובה לשליחה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_change\_password\_response | Response – התגובה לשליחה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_change\_email\_response | Response – התגובה לשליחה email – אימייל המשתמש | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_login\_verify\_response | Status – התגובה לשליחה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_add\_shared\_file | Path – נתיב הקובץ | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_send\_email\_response | Status – התגובה לשליחה email – אימייל המשתמש | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_move\_file\_response | Status – התגובה לשליחה new\_folder – מיקום התיקייה אליו הזיזו את הקובץ | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_paste\_file\_response | Status – התגובה לשליחה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_open\_file\_response | Status – התגובה לשליחה file\_path – נתיב הקובץ data\_len – אורך מידע הקובץ |  | | pack\_get\_details\_response | Status – התגובה לשליחה email – אימייל המשתמש data\_len – אורך מידע הקובץ | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_delete\_profile\_photo\_response | Status – התגובה לשליחה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_register\_verify\_response | Status – התגובה לשליחה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_check\_code\_response | Status – התגובה לשליחה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_forgot\_password\_response | Status – התגובה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_zip\_folder\_response | Status – התגובה לשליחה zipped\_folder\_name – שם הקובץ | מחרוזת הבנויה לפי הפרוטוקול. | |

| **clientProtocol** |
| --- |
| המחלקה שאחראית על הבנייה והפרוק של הפרוטוקול בצד השרת. |
| **תכונות** |
| |  |  |  | | --- | --- | --- | | **שם הפעולה** | **טענת כניסה** | **טענת יציאה** | | unpack\_message | msg – ההודעה שהתקבלה מהשרת | טאפל שכולל בתוכו את קוד הפרוטוקול ואת המשתנים. | | get\_data\_from\_string | Line – ההודעה לפירוק length – אורך ההודעה לפירוק | המידע שפורק וההודעה לפירוק לאחר הפירוק. | | Unpack\_files\_message | Msg – ההודעה שהתקבלה מהשרת | מחרוזת הקבצים של המשתמש לפי הפרוטוקול. | | pack\_register\_request | Username – שם משתמש password – סיסמא email – אימייל | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_login\_request | Username – שם משתמש password – סיסמא | מחרוזת הבנויה לפי הפרוטוקול. | | Pack\_verify\_check\_request | Email – אימייל המשתמש code – הקוד שהמשתמש הכניס | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_send\_verify\_request | Email – אימייל המשתמש | מחרוזת הבנויה לפי הפרוטוקול. | | Pack\_download\_file\_request | Path – נתיב הקובץ בשרת selected\_path – נתיב הקובץ לשמירה | מחרוזת הבנויה לפי הפרוטוקול. | | Pack\_upload\_file\_request | upload\_path – נתיב ההעלאה data\_len – אורך הקובץ | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_create\_folder\_request | upload\_path – נתיב ההעלאה | מחרוזת הבנויה לפי הפרוטוקול. | | Pack\_delete\_request | Path – נתיב הקובץ בשרת למחיקה | מחרוזת הבנויה לפי הפרוטוקול. | | Pack\_rename\_file\_request | Path – נתיב הקובץ בשרת new\_name – השם לשינוי | מחרוזת הבנויה לפי הפרוטוקול. | | Pack\_share\_request | Path – נתיב הקובץ בשרת username – את מי לשתף | מחרוזת הבנויה לפי הפרוטוקול. | | Pack\_change\_photo\_request | Username – שם המשתמש file\_len – אורך מידע התמונה | מחרוזת הבנויה לפי הפרוטוקול. | | Pack\_change\_password\_request | Username – שם המשתמש old\_password – הסיסמא הישנה new\_password – הסיסמא החדשה confirmed\_password – אימות הסיסמא החדשה | מחרוזת הבנויה לפי הפרוטוקול. | | Pack\_change\_email\_request | Username – שם המתמש Email – אימייל לשינוי code – קוד האימות שנשלח למייל | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_send\_email\_request | Username – שם המשתמש | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_move\_file\_folder\_request | Src – נתיב הקובץ להזזה dst – נתיב התיקייה להזיז אליה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_paste\_file\_request | Src – נתיב הקובץ להדפסה dst – נתיב התיקייה להדפיס אליה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_open\_file\_request | Path – נתיב הקובץ לפתיחה | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_get\_details\_request | Username – שם המשתמש | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_delete\_profile\_photo\_request | Username – שם המשתמש | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_verify\_login\_email\_request | Email – אימייל המשתמש code – קוד האימות שנשלח dont\_ask\_again – האם לבקש אימות שוב במחשב זה username – שם המשתמש | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_verify\_register\_email\_request | Username – שם המשתמש password – הסיסמא email – אימייל המשתמש code – קוד האימות שנשלח dont\_ask\_again – האם לבקש אימות שוב במחשב זה |  | | pack\_check\_code\_request | Email – אימייל המשתמש code – קוד האימות שנשלח במייל | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_forgot\_password\_request | Username – שם המשתמש password – סיסמת המשתמש confirmed\_password – אימות הסיסמא | מחרוזת הבנויה לפי הפרוטוקול. | | pack\_zip\_folder\_request | Folder\_path – נתיב התיקייה לדחוס | מחרוזת הבנויה לפי הפרוטוקול. | |

| **serverComm** |
| --- |
| המחלקה שאחראית על יצירת צד שרת בתקשרות עם הלקוחות |
| **תכונות**   |  |  | | --- | --- | | **שם התכונה** | **שימוש** | | Port | הפורט של השרת | | revcQ | תור ההודעות שהתקבלו לטיפול | | Server\_socket | הסוקט של השרת דרכו עוברת התקשורת | | openClients | מילון הסוקטים המחוברים לשרת עם ערך הip שלהם ומפתח ההצפנה שלהם  open\_clients[client\_socket] =[ip, crypto] | | isRunning | האם השרת רץ | | msgLenBytes | אורך כמות הבתים שאליו מדופנת ההודעה | |
| **פעולות**   |  |  |  | | --- | --- | --- | | **שם הפעולה** | **טענת כניסה** | **טענת יציאה** | | \_\_init\_\_ | Port – פורט השרת recvQ – תור ההודעות msgLenBytes – אורך הודעה לשליחה/קבלה | מאתחלת את התכונות ומפעילה את \_main\_loop כ thread | | \_handle\_disconnect | Sock – סוקט לניתוק | מנתק את הלקוח ומוחק אותו מהרשימה open\_clients | | \_find\_socket\_by\_ip | Ip – הכתובת למציאת הסוקט שלו | מחזיר את הסוקט של הלקוח עם הכתובת | | Send | Ip – כתובת הלקוח msg – ההודעה לשליחה | מצפין ושולח את ההודעה ע"פ הפרוטוקול: אורך מדופן ל msgLenBytes ואת ההודעה עצמה | | \_change\_key | client,addr – פרטי הלקוח איתו עושים את ההחלפה | מבצעת החלפת מפתחות עם הלקוח ובסיומה מכניסה את פרטני הלקוח ל open\_clients | | \_close\_server |  | מכבה את isRunning | | \_running\_status |  | מחזיר האם סטטוס השרת | | \_main\_loop |  | מדליק את השרת ומקבל הודעות, מפענח אותן ע"פ מפתח ההצפנה ומכניס tuple ל recvQ הכולל את ה IP של הלקוח ואת ההודעה המפוענחת (ip, msg) | | recv\_file | * **נתיב + שם לשמירה** * **אורך מידע הקובץ (6 בתים)** | תקלוט לתוך הקובץ בנתחים של 1024 בתים את כל הקובץ ותכניס לתור (ip,filenamePath) | | Send\_file | * **Client\_ip – ip המשתמש** * **Params – הנתונים לשליחה** | שולח את הקובץ למשתמש בעזרת הנתונים שהתקבלו | |

| **clientComm** |
| --- |
| **המחלקה שאחראית על יצירת צד לקוח בתקשורת עם השרת** |
| **תכונות**   |  |  | | --- | --- | | **שם התכונה** | **שימוש** | | Port | פורט | | recvQ | תור ההודעות שהתקבלו לטיפול | | my\_socket | הסוקט של הלקוח דרכו עוברת התקשורת | | serverIp | הכתובת של השרת | | Crypt | עצם ההצפנה | | msgLenBytes | אורך כמות הביטים שאליו מדופנת ההודעה | |
| **פעולות**   |  |  |  | | --- | --- | --- | | **שם הפעולה** | **טענת כניסה** | **טענת יציאה** | | \_\_init\_\_ | ServerIP – כתובת השרת Port – פורט השרת recvQ – תור ההודעות | מאתחלת את התכונות ומפעילה את \_main\_loop כ thread | | Send | msg – ההודעה לשליחה | מצפין את ההודעה ושולח את ההודעה ע"פ הפרוטוקול: אורך msgLenBytes בתים וההודעה | | \_change\_key |  | מבצעת החלפת מפתחות עם השרת ויוצרת את עצם ההצפנה | | \_close |  | מכבה את isRunning | | \_main\_loop |  | יוצרת את ההתחברות לשרת, מחליפה מפתחות באמצעות \_change\_key ובלולאה מקבלת הודעות מהשרת , מפענחת ומכניסה אותן לתור recvQ | | \_recv\_file | Params – הנתונים שהתקבלו מהשרת | מקבל את מידע הקובץ לפי הפרוטוקול | | Send\_file | Opcode – מספר הפרוטוקול path – נתיב הקובץ currPath – הנתיב הנוכחי בו נמצא המשתמש | שולח קובץ לשרת לפי הפרוטוקול | | Did\_change\_work |  | מחזיר האם מחלפת המפתחות הסתיימה | |

| **serverLogic** | |
| --- | --- |
| **המחלקה שאחראית על הלוגיקה של השרת** | |
| **תכונות** | |
| main\_server | עצם השרת |
| recv\_commands | מילון המכיל עבור כל מפתח (opcode) את שם הפעולה למימוש לדוגמא:  commands['01'] = \_handle\_registeration וכך הלאה |
| myDB | עצם המייצג את בסיס הנתונים של הפרויקט |
| Used\_port | רשימת פורטים שניתנו להעלאת קבצים |
| **פעולות**   |  |  |  | | --- | --- | --- | | **שם הפעולה** | **טענת כניסה** | **טענת יציאה** | | main\_loop | יוצרת תור להודעות נכנסות  יוצרת עצם שרת | מפעילה את \_handle\_messages כ thread | | \_handle\_messages | main\_server  recv\_q | יוצרת חיבור לבסיס הנתונים - myDB  מוציאה את ההודעה מתור ההודעות: מפענחת באמצעות הפרוטוקול ומפעילה בהתאם את הפעולה הנדרשת(מפורטת בהמשך) | | \_handle\_registration | username  password  mail  myDB  main\_server  clientIP code\_dic | מנסה להוסיף משתמש לבסיס הנתונים באמצעות הפעולה myDB.add\_user – יוצרת תשובה ע"פ הפרוטוקול ושולחת באמצעות main\_server.send(clientIP, msg) | | \_handle\_email\_register | main\_server db client\_ip code\_dic username password email code dont\_ask\_again |  | | \_handle\_login | Username password myDB main\_server clientIP | בודקת האם הערכים תקינים כדי להתחבר למשתמש – יוצרת תשובה ע"פ פרוטוקול ושולחת אימייל | | \_handle\_email\_login | Main\_server db client\_ip users\_by\_ip code\_dic email code dont\_ask\_again username | בודקת האם קוד האימות שנשלח למייל תקין – יוצרת תשובה ע"פ פרוטוקול ושולחת תשובה | | \_create\_files\_thread | Main\_server db client\_ip users\_by\_ip username | מגרילה פורט שלא נמצא ב used\_ports  בונה הודעה ע"פ הפרוטוקול build\_upload\_port\_request  שולחת באמצעות main\_server.send(ip,msg)  יוצרת תור file\_q מפעילה את recv\_file כ thread | | handle\_files | files\_server files\_q db | שולחת ללקוח את רשימת הקבצים והתיקיות שלו ע"פ הפרוטוקול | | \_handle\_open\_file | path main\_server clientIP | שולחת למשתמש את תוכן הקובץ אותו הוא רוצה לפתוח | | \_handle\_change\_email | Username email code  myDB main\_server clientIP | משנה את המייל בבסיס הנתונים ושולחת תשובה ע"פ הפרוטוקול | | \_handle\_change\_password | Username old\_pass new\_pass confirmed\_pass myDB main\_server clientIP | משנה את הסיסמא בבסיס הנתונים ושולחת תשובה ע"פ הפרוטוקול | | \_handle\_forget\_paddword | Username password confirmed\_password myDB main\_server clientIP | משנה את הסיסמא בבסיס הנתונים ושולחת תשובה ע"פ הפרוטוקול | | \_handle\_rename\_file | Path newName db main\_server clientIP | משנה את שם הקובץ בדרייב ומעדכנת את הלקוח ע"פ הפרוטוקול | | \_handle\_share\_file | username  Path users\_by\_ip main\_server clientIP db | משתפת את הקובץ עם המשתמש שהתקבל ומעדכנת את הלקוח ע"פ הפרוטוקול | | \_handle\_delete\_file | db Path main\_server clientIP | מוחקת את הקובץ המבוקש ומעדכנת את הלקוח ע"פ הפרוטוקול | | \_handle\_download\_file | Selected\_path path main\_server clientIP | שולחת ללקוח את הקובץ ע"פ הפרוטוקול | | \_handle\_upload\_file | path data main\_server clientIP | יוצרת את הקובץ אצל השרת ושולחת תגובה ללקוח ע"פ הפרוטוקול | | \_handle\_create\_dir | db path main\_server clientIP | יוצרת תיקייה אצל השרת ושולחת תגובה ללקוח ע"פ הפרוטוקול | | \_handle\_move\_file | Main\_server db client\_ip src dst | מעבירה קובץ אצלי קבצי השרת ושולחת תגובה ללקוח ע"פ הפרוטוקול | | \_handle\_paste\_file | Main\_server db client\_ip src dst | מוסיפה את הקובץ שהודבק לקבצי הלקוח ושולחת תגובה ללקוח ע"פ הפרוטוקול | | \_handle\_get\_details | Main\_server client\_ip db username | שולחת ללקוח את פרטי המשתמש ותוכן התמונת פרופיל | | \_send\_email | Main\_server my\_db client\_ip code\_dic email | מגרילה מספר בין 6 ספרות ושולח למייל של המשתמש שהתקבל | | \_handle\_change\_photo | Files\_server client\_ip username photo\_data | משנה את תמונת הפרופיל של המשתמש אצל השרת ושולחת תגובה ללקוח ע"פ הפרוטוקול | | \_handle\_delete\_profile\_photo | Files\_server client\_ip username | מוחקת את תמונת הפרופיל של המשתמש אצל השרת ושולחת תגובה ללקוח ע"פ הפרוטוקול | | \_handle\_send\_email | Main\_server db client\_ip code\_dic username | מפעילה את שליחת המייל ושולחת תגובה ללקוח ע"פ הפרוטוקול | | \_handle\_check\_email | Main\_server db client\_ip code\_dic email code | בודקת האם הקוד שהוכנס זהה לקוד שנשלח למייל של הלקוח ומחזירה תגובה ע"פ הפרוטוקול | | \_handle\_zip\_folder | Main\_server db client\_ip folder\_path | אורזת את התיקייה שנבחרה ומחזירה תגובה ללקוח ע"פ הפרוטוקול | | |

|  |
| --- |
| **clientLogic** |
| **המחלקה שאחראית על הלוגיקה של הלקוח** |
| **פעולות**   |  |  |  | | --- | --- | --- | | **שם הפעולה** | **טענת כניסה** | **טענת יציאה** | | Main\_loop |  | יוצרת את תור ההודעות ובונה את עצם הלקוח | | \_Handle\_messages | msg\_q | מוציאה את ההודעה מתור ההודעות ומפעילה את הפעולה הנכונה בהתאם | | \_handle\_files | Msg\_q | מוציאה את ההודעה מתור ההודעות ומפעילה את הפעולה הנכונה בהתאם | | \_show\_register\_dialog | Status username password email | מראה תגובה בגרפיקה בהתאם על פי התשובה | | \_handle\_register | status | משנה את הגרפיקה על פי התשובה | | \_show\_login\_dialog | Status email | מראה תגובה בגרפיקה בהתאם על פי התשובה | | \_handle\_login | status | משנה את הגרפיקה על פי התשובה | | \_handle\_change\_email | Status email | משנה את הגרפיקה על פי התשובה | | \_handle\_change\_password | status | משנה את הגרפיקה על פי התשובה | | \_handle\_forget\_paddword | status | משנה את הגרפיקה על פי התשובה | | \_handle\_rename\_file | Status new\_name | משנה את הגרפיקה על פי התשובה | | \_handle\_share\_file | status | משנה את הגרפיקה על פי התשובה | | \_handle\_delete\_file | status | משנה את הגרפיקה על פי התשובה | | \_handle\_download\_file | Status path selected\_path data | משנה את הגרפיקה על פי התשובה | | \_handle\_open\_file | File\_comm status server\_path data | פותחת את הקובץ לעריכה או לצפייה בהתאם לסוג הקובץ | | \_handle\_upload\_file | Status path | משנה את הגרפיקה על פי התשובה | | \_handle\_create\_dir | status | משנה את הגרפיקה על פי התשובה | | Handle\_files\_port\_ | Port | פותחת thread חדש לטיפול בקבצים | | \_handle\_add\_shared\_file | Path | מוסיף את הקובץ לקבציי הלקוח | | \_handle\_move\_file | Status path | משנה את הגרפיקה על פי התשובה | | \_handle\_paste\_file | Status | משנה את הגרפיקה על פי התשובה | | \_handle\_get\_files | Email photo | משנה את הערכים אצל המשתמש | | \_handle\_change\_photo | Data | משנה את ערך תמונת הפרופיל אצל המשתמש | | \_handle\_username\_check | Status email | מראה את דיאלוג האימות אם תקין או שגיאה | | \_handle\_code\_check | Status | מראה את דיאלוג שינוי הסיסמא או שגיאה | | \_handle\_forgot\_password | Status | מראה תגובה ללקוח האם היה תקין או לא | | \_handle\_zip\_file | Status zip\_name | משנה את הגרפיקה ע"פ התשובה | | \_handle\_send\_files | Branches | משנה את קצבי הלקוח | |

| **sFileHandler** |
| --- |
| **המחלקה שאחראית על פעולות הקבצים מצד השרת** |
| **פעולות**   | **שם הפעולה** | **טענת כניסה** | **טענת יציאה** | | --- | --- | --- | | Rename\_file | Path – נתיב הקובץ newname – שם חדש | משנה את שם הקובץ | | Delete\_file | Path – נתיב הקובץ | מוחק את הקובץ | | Generate\_unique\_zip \_name | Path – נתיב הקובץ base\_name – שם הקובץ | בודק את שמות קבצי הזיפ שיש בתיקייה ולפי זה יוצר את שם הזיפ הבא | | create\_zip | Total\_path – נתיב הקובץ | יוצר את קובץ הזיפ מחזיר 1 אם לא עבד 0 אם עבד | |

| **DB** |
| --- |
| **המחלקה שאחראית על טיפול במבנה הנתונים** |
| **תכונות**   |  |  | | --- | --- | | **שם התכונה** | **שימוש** | | Conn | מצביע לבסיס הנתונים | | Cursor | המצביע בתוך בסיס הנתונים על מנת לעשות פעולות | | DBname | שם בסיס הנתונים |   **פעולות**   | **שם הפעולה** | **טענת כניסה** | **טענת יציאה** | | --- | --- | --- | | \_\_init\_\_ |  | יוצרת את עצם בסיס הנתונים וקוראת ל \_create\_table | | \_create\_data\_base |  | מתחברת לבסיס הנתונים ויוצרת את טבלת המשתמשים users אם לא קיימת | | username\_exist | Username – שם המשתמש | בודק האם שם המשתמש קיים בטבלה מחזיר 0/1 לפי אמת או שקר | | add\_user | Username – שם המשתמש password – סיסמא email - מייל | מוסיף משתמש לטבלה אם הוא לא קיים באמצעות \_username\_exists ומחזיר תשובה 1/0 | | Delete\_user | Username – שם משתמש | מסיר משתמש מהטבלה אם הוא קיים ומחזיר תשובה 1/0 | | Change\_password | Username – שם המשתמש password – סיסמא | משנה את הסיסמא של המשתמש אם הוא קיים ומחזיר תשובה 1/0 | | Change\_username | Username – שם המשתמש newname – השם החדש | משנה את שם המשתמש אם הוא קיים  ומחזיר תשובה 1/0 | | Change\_email | Username – שם המשתמש email – אימייל | משנה את האימייל של המשתמש אם הוא קיים  ומחזיר תשובה 1/0 | | Get\_password | Username – שם המשתמש | מחזיר את הסיסמא של המשתמש אם הוא קיים | | Get\_email | Username – שם המשתמש | מחזיר את המייל של המשתמש אם הוא קיים | | get\_ips\_of\_user | Username – שם המשתמש | מחזיר את הכתובות בהם המשתמש היה מחובר מהם | | add\_remembered\_ip | Username – שם המשתמש ip – כתובת המשתמש | מוסיף את הכתובת למשתמש בטבלת הכתובות של המשתמשים | |

| **encryption** |
| --- |
| **המחלקה שאחראית על תהליכי ההצפנה והפענוח בפרויקט** |
| **תכונות**   |  |  | | --- | --- | | **שם התכונה** | **שימוש** | | Key | ממפתח ההצפנה | | Bs | גודל הבלוק | |
| **פעולות**   |  |  |  | | --- | --- | --- | | **שם הפעולה** | **טענת כניסה** | **טענת יציאה** | | \_\_init\_\_ | Key – מפתח ההצפנה | יוצר את האובייקט | | \_pad | message – ההודעה | ריפוד ההודעה | | \_unpad | message – ההודעה | הורדת הריפוד | | Enc\_msg | message – הודעה להצפנה | ההודעה המוצפנת | | Dec\_msg | Encrypt\_Msg – הודעה לפענוח | ההודעה הרגילה | | Hash\_msg | Msg – הודעה לגיבוב | **פעולה חיצונית** – ערך hash של ההודעה | | Get\_DH\_factor |  | **פעולה חיצונית** -מחזירה מספר ראשוני b לטובת החלפת מפתח בשיטת דיפי-הלמן | | Create\_symetry\_key | Private\_key – מפתח ההצפנה הפרטי shared\_key – מפתח ההצפנה המשותף | **פעולה חיצונית** - מייצרת מפתח סימטרי – מחזירה עצם encryption | |

| **PortsHandler** | |
| --- | --- |
| **המחלקה אשר אחראית על יצירת הפורטים שמשמשים להעלאת והורדת קבצים באמצעות התקשרות** | |
| **תכונות** | |
| **שם התכונה** | **שימוש** |
| **Unused\_ports** | **גנרטור שמחזיר את הפורט הבא שאינו בשימוש בשרת** |
| **פעולות** | |
| **שם הפעולה** | **טענת יציאה** |
| **Get\_next\_port** | **מחזירה את הפורט הבא שאינו בשימוש באמצעות unused\_ports** |

| **monitorFile** | | |
| --- | --- | --- |
| **המחלקה אשר אחראית על יצירת הפורטים שמשמשים להעלאת והורדת קבצים באמצעות התקשרות** | | |
| **פעולות** | | |
| **שם הפעולה** | **טענת כניסה** | **טענת יציאה** |
| **Monitor** | **Path\_to\_watch – נתיב התיקייה אשר אנחנו רוצים לבדוק בה שינויים q – התור בו אנחנו שמים את העדכונים** | **שמה בq האם היה שינוי בקובץ בתיקייה שבה אנחנו מסתכלים עליה** |
| **Get\_all\_pid** | **Process\_name – שם הprocess שאנחנו רוצים לקבל את כל הpids שלו** | **מחזיר את כל הpids עם שם הprocess** |
| **Wait\_until** | **File\_path – נתיב הקובץ q – התור בו אנחנו שמים את העדכונים** | **פותח את הקובץ וכאשר הקובץ נסגר שם בq שהתוכנה נסגרה** |

|  |  |
| --- | --- |
| **ClassSettings** | |
| **המחלקה שבה יש את התכונות המשמשות להרצת הקוד בכיתה** | |
| **תכונות** | |
| **שם התכונה** | **שימוש** |
| **SERVERPORT** | **הפורט להתחברות לשרת בכיתה** |
| **SERVERIP** | **Ip השרת להתחברות בכיתה** |
| **USER\_FILES\_PATH** | **נתיב הקבצים להרצת הגרפיקה של הלקוח בכיתה** |
| **SERVER\_FILES\_PATH** | **נתיב קבצי המשתמשים אצל השרת בכיתה** |
| **USER\_PROFILE\_PHOTOS** | **נתיב תמונות הפרופיל של המשתמשים אצל השרת בכיתה** |

|  |  |
| --- | --- |
| **HomeSettings** | |
| **המחלקה שבה יש את התכונות המשמשות להרצת הקוד בבית** | |
| **תכונות** | |
| **שם התכונה** | **שימוש** |
| **SERVERPORT** | **הפורט להתחברות לשרת בבית** |
| **SERVERIP** | **Ip השרת להתחברות בבית** |
| **USER\_FILES\_PATH** | **נתיב הקבצים להרצת הגרפיקה של הלקוח בבית** |
| **SERVER\_FILES\_PATH** | **נתיב קבצי המשתמשים אצל השרת בבית** |
| **USER\_PROFILE\_PHOTOS** | **נתיב תמונות הפרופיל של המשתמשים אצל השרת בבית** |

|  |
| --- |
| **CurrentSettings** |
| **המחלקה משתמשת בתכונות של HomeSettings ושל ClassSettings ועוזרת לי להחליף בין ההגדרות בבית לבין ההגדרות בכיתה באמצעות שינוי של שורה אחת ולא של כל מופע של התכונות בקוד** |

|  |
| --- |
| **FileMenuFeatures** |
| **תפריט האופציות לפעולות על הקבצים של המשתמש (למחוק קובץ, לשנות שם, לשתף קובץ וכו')** |

|  |
| --- |
| **FolderMenuFeatures** |
| **תפריט האופציות לפעולות על התיקיות של המשתמש (לפתוח את התייקיה, למחוק את התיקייה וכו')** |

|  |
| --- |
| **UserMenuFeatures** |
| **תפריט האופציות לפעולות של המשתמש (העלאת קובץ, יצירת תיקייה וכו')** |

|  |
| --- |
| **ProfileSettingsMenu** |
| **תפריט האופציות להגדרות המשתמש (שינוי תמונת פרופיל ומחיקת תמונת פרופיל)** |

|  |
| --- |
| **ChangePasswordDialog** |
| **דיאלוג אישי לשינוי הסיסמא** |

|  |
| --- |
| **ConfirmMailDialog** |
| **דיאלוג אישי לאימות המייל בעזרת הקוד שנשלח למייל** |

|  |
| --- |
| **ForgotPasswordDialog** |
| **דיאלוג אישי לשכחתי את הסיסמא** |

|  |
| --- |
| **TransparentText** |
| **טקסט ללא רקע** |

|  |
| --- |
| **MyDropTarget** |
| **דרופ טארגט שבעזרתו בודקים גרירה של קבצים** |

|  |
| --- |
| **FilesPanel** |
| **מסך הגרפיקה של קבצי המשתמש שיש בו את כל קבצי ותיקיות המשתמשדד** |

|  |
| --- |
| **LoginPanel** |
| **מסך הגרפיקה של הכנסת פרטי המשתמש על מנת להתחבר למשתמש** |

|  |
| --- |
| **MainFrame** |
| **הפריים הראשי של מסכי הגרפיקה של המשתמש** |

|  |
| --- |
| **MainPanel** |
| **הפאנל הראשי של מסכי הגרפיקה של המשתמש עליו שמים את שאר המסכים** |

|  |
| --- |
| **RegistrationPanel** |
| **מסך הגרפיקה של הכנסת פרטי המשתמש על מנת ליצור למשתמש** |

|  |
| --- |
| **UserPanel** |
| **מסך הגרפיקה שבו המשתמש יכול לראות את פרטי המשתמש שלו, ולשנות שם את תמונת הפרופיל שלו** |

**4. תיאור סביבת הפיתוח:**

**שפות התכנות-** שפות התכנות שאני אשתמש בהם הם **פיתון וsql**, אני אעשה שימוש בsql על מנת לעבוד מול בסיס נתונים של הפרויקט.  
ובפיתון בשביל קבצי הקוד של הפרויקט.  **כלי הפיתוח והכלים** **לבדיקה**- כלי הפיתוח והכלים לבדיקה שאני אשתמש בהם בפרויקט הם **PyCharm**, **Wireshark**, **DB Browser for SQLite** וב**file explorer**. אני אשתמש בPyCharm על מנת לערוך את קבצי הקוד שלי, בWireshark על מנת לבדוק ולעבוד על התקשורת וההצפנה שלי, בDB Browser for SQLite בשביל לבדוק את בסיס הנתונים שלי ובfile explorer על מנת לראות ולבדוק את שינויי הקבצים.

**5. סוגיות מרכזיות בפרויקט:**

**סוגיה** – מימוש התקשורת בפרויקט

| חלופה | תיאור | יתרונות | חסרונות |
| --- | --- | --- | --- |
| 1 | סוקט יחיד דרכו כולם מחוברים לשרת | קל למימוש | לא יעיל, מונע טיפול מקבילי בלקוחות/בקשות שונות |
| 2 | סוקט לתקשורת כללית וסוקט לקבצים | הפרדה ברורה בין קבצים לשאר הדברים ולא נדרש למיין זאת  העלאת/הורדת קבצים לא מעכבת התחברות לקוחות אחרים | קצת יותר מורכב למימוש  ברגע שכמה לקוחות רוצים בו זמנית לעלות/להוריד קבצים נוצר עיכוב |
| 3 | סוקט לתקשורת כללית ולכל לקוח סוקט קבצים משלו | הפרדה מוחלטת בין הלקוחות ולכן מונע עיכובים בין משתמשים  הפרדה ברורה בין קבצים לשאר הדברים ולא נדרש למיין זאת | יותר סוקטים יותר מורכב לניהול |

החלופה שבחרתי בה היא חלופה 3 – בפרויקט שלי, העיסוק העיקרי הוא עם קבצים ולכן חשוב שלא יהיו עיכובים/ תקיעות / ערבוב עם מידע אחר.

**סוגיה** - סוג ההצפנה בפרויקט

| חלופה | תיאור | יתרונות | חסרונות |
| --- | --- | --- | --- |
| 1 | הצפנה סימטרית | מהירה, קלה ליישום | דורש הסכמה על מפתח ההצפנה שצריך לדעת מראש |
| 2 | הצפנה אסימטרית | נוחה לשימוש ובטוחה יותר | איטית יחסית בעיקר בעבודה עם קבצים |
| 3 | הצפנה היברידית (יצירת המפתח הסימטרי בפרוטוקול דיפי הלמן) | פותרת את בעיית העברת המפתח הסימטרי ומהירה | קשה יותר ליישום |

החלופה שבחרתי היא חלופה 3 – בפרויקט שלי, העיסוק הוא עם קבצים והצפנה א-סימטרית יכולה לגרום לעיכובים ולבעיות איטיות, אני אשתמש בפרוטוקול דיפי-הלמן ליצירת מפתח סימטרי וכך אוכל להשתמש בהצפנה הסימטרית שהיא מהירה ונוחה.

**סוגיה** - העברת המידע על הקבצים

| חלופה | תיאור | יתרונות | חסרונות |
| --- | --- | --- | --- |
| 1 | העברת המידע על כל הקבצים של המשתמש בבת אחת | חוסך בתקשורת משום שיש אצל הלקוח את כל המידע | מידע גדול מאוד ועלול לגרום לבעיות של איבוד מידע העברת מידע שברובו עלול להיות מיותר |
| 2 | העברת רק השמות בהתחלה ואחר כך שליחת המידע על הקובץ המתבקש | נוח משום שמעבירה רק את המידע החיוני באמת ויותר קלה לטיפול | יותר תקשורת |

החלופה שבחרתי היא חלופה 2 – משום שאני משתמש בקבצים העברת כל המידע תהיה כבדה מאוד ותעמיס על הרשת ואילו העברת רק הקבצים הנחוצים יותר קלה לטיפול ויותר יעילה

**סוגיה** - אופן שמירת הקבצים **של המשתמשים בשרת**

| חלופה | תיאור | יתרונות | חסרונות |
| --- | --- | --- | --- |
| 1 | כל הקבצים של כל המשתמשים נמצאים במחיצה אחת בצד שרת | קל לשימוש | נדרשת יכולת בצד השרת לדעת אלו קבצים שייכים לאיזה משתמש, פעולה שיכולה לקחת זמן בכל פנייה של משתמש כלשהו לקבצים שלו – יחייב פיתוח אלגוריתם כלשהו בצד שרת |
| 2 | עבור כל משתמש בצד שרת, תהייה מחיצה עם שם המשתמש (שהוא חד ערכי במערכת) שם ישמרו הקבצים שלו | יוצרת סדר וארגון טובים יותר - גישה בצד שרת לקבצי משתמש מהירה ולא מצריכה אלגוריתם כלשהו | בזבוז מקום בצד שרת  במקרים של שינוי שם משתמש במערכת אצרך לשנות גם את שם התיקייה שלו |
| 3 | שמירת הקבצים בבסיס הנתונים | הקבצים הרבה יותר בטוחים, גישה קלה יותר אליהם | מנפחת את בסיס הנתונים ולכן ברוב בסיסי הנתונים גם אצלי שמירת קבצים לא אפשרית בבסיס הנתונים |

החלופה שבחרתי בה היא חלופה 2 –בחלופה זו יש סדר וארגון בצד שרת שמאיצים את הטיפול בבקשות משתמש לקבצים שלו שזה מהות הפרויקט אצלי.

**סוגיה** – אופן שמירת הסיסמא בבסיס הנתונים

| חלופה | תיאור | יתרונות | חסרונות |
| --- | --- | --- | --- |
| 1 | הצפנה | נוח לשימוש משום שמפתח ההצפנה ידוע | איפה שומרים את מפתח ההצפנה ובמידה ומגלים את המפתח מתגלות כל הסיסמאות שבמערכת |
| 2 | פונקציית גיבוב | קלה לבדיקה ובטוחה מאוד | יכולה לגרום להתנגשויות והכנסת סיסמא לא נכונה בכל זאת תכניס את המשתמש למערכת |
| 3 | כמו שהוכנס על ידי המשתמש | קלה מאוד לקריאה ובדיקה | לא בטוחה בעליל |

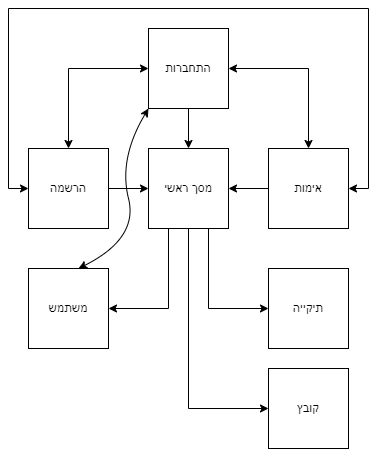
החלופה שבחרתי בה היא חלופה 2 – משום שהסיכויים להתנגשות מאוד נמוכים ובמידה והתקיימה התנגשות אחת היא יותר בטוחה מאשר גילוי מפתח ההצפנה או החוסר בהצפנה.

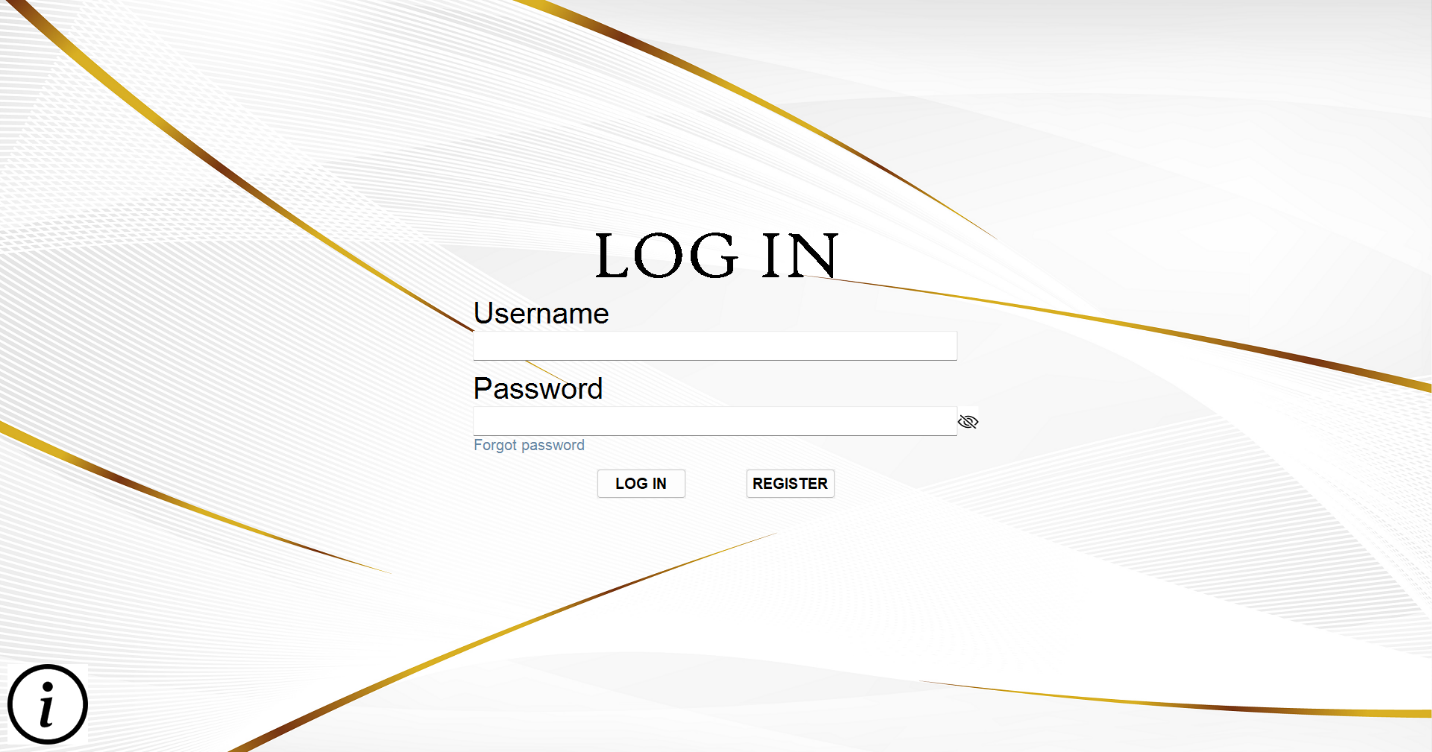
**סוגיה** – אופן העברת תיאור מבנה הקבצים של המשתמש ללקוח (לטובת הצגתם בממשק המשתמש)

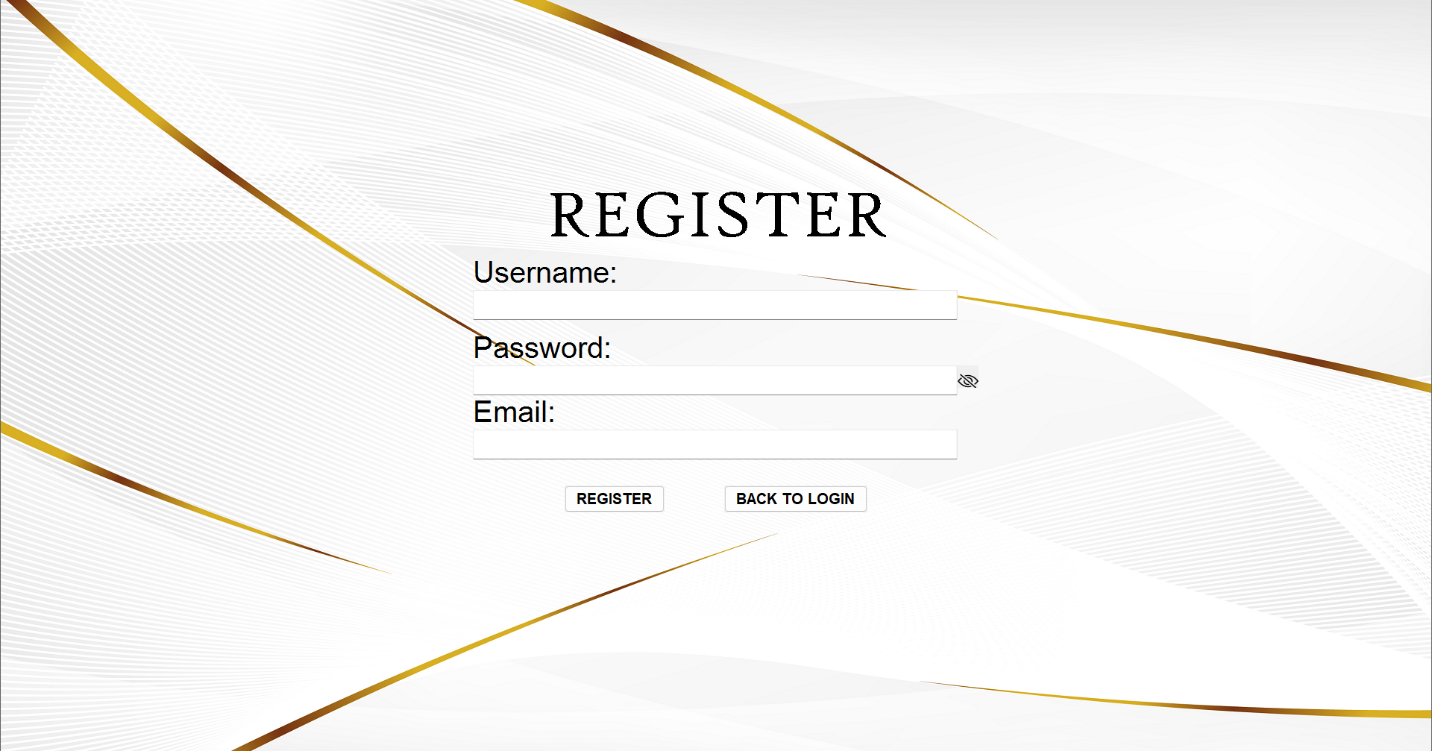
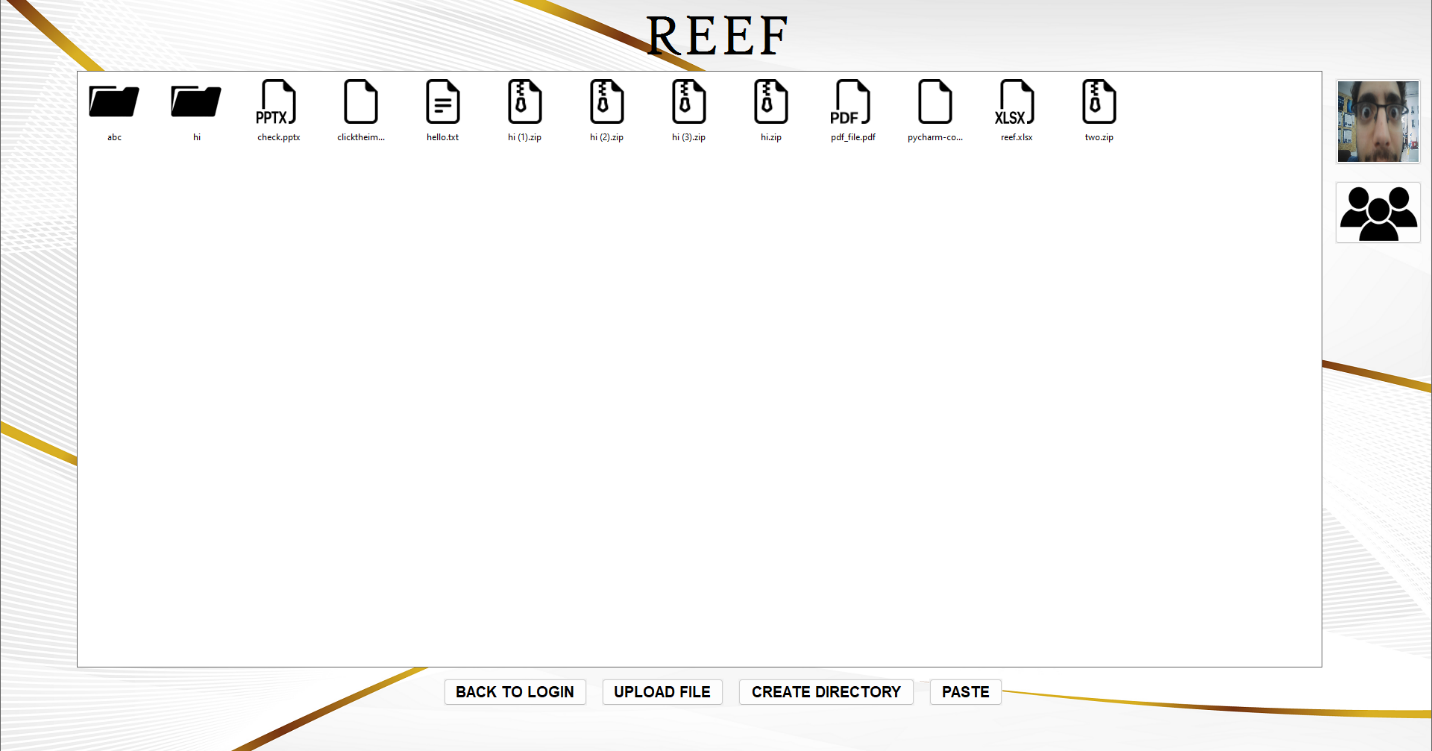
| חלופה | תיאור | יתרונות | חסרונות |
| --- | --- | --- | --- |
| 1 | העברת רק התיקייה הנוכחית (עליה כרגע המשתמש מסתכל) | קל למימוש  מיקום הלקוח בתיקיות נמצא אצל השרת | השרת מנהל את תצוגת הקבצים של הלקוח – עומס על השרת  ישפיע על תגובות התצוגה |
| 2 | העברת מבנה הקבצים הכולל ללקוח | נוחה ומאפשרת רק שליחה אחת  כל ניהול המעבר בין התיקיות בצד לקוח לא מעמיס על השרת | נדרש לממש פרוטוקול לייצוג מבנה הקבצים של המשתמש  בכל שליחה של פעילות במערכת הקבצים תידרש העברת ה מסלול כולו |

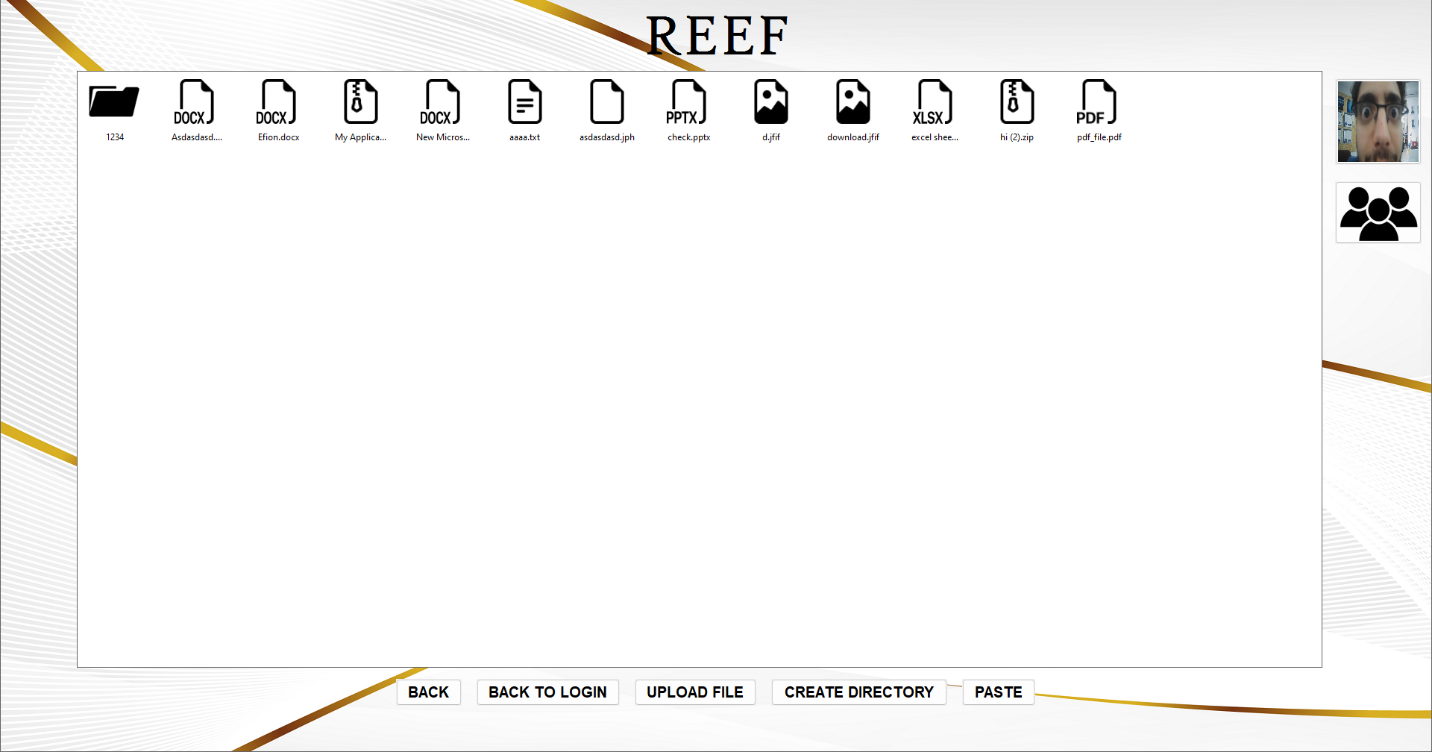
החלופה שבחרתי בה היא חלופה 2 – משום שבפרויקט שלי חשובה מהירות התגובה ואם אני שולח הכל בהתחלה זה מאפשר לתוכנת הלקוח להגיב במהירות לבקשות המשתמש זה הרבה יותר מהיר ומוריד תקשורת ולחץ מהשרת

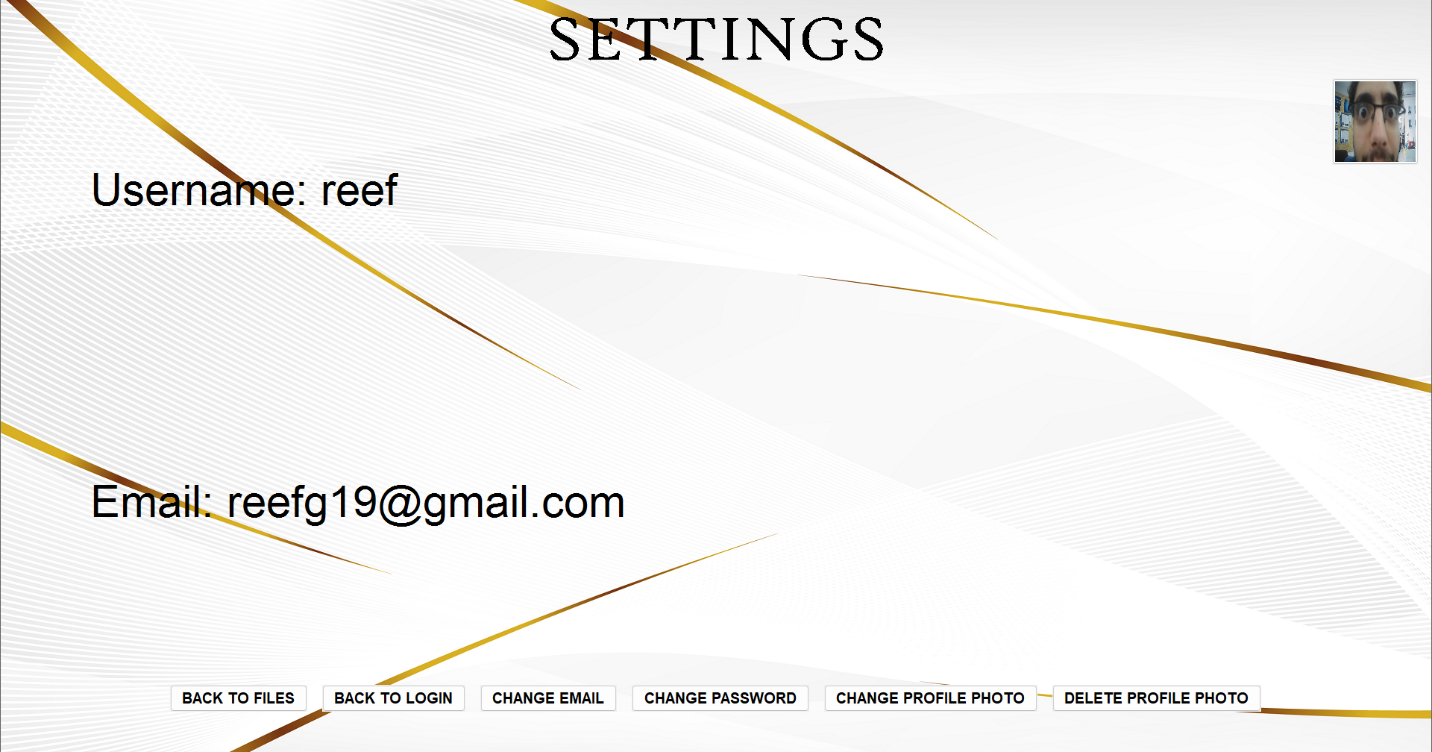
**6. תרשים מסכי הפרויקט**

א. תרשים עץ המסכים:  


**מסך התחברות**: ****

**מסך יצירת משתמש:מסך הקבצים הראשי:** 

**מסך של תיקייה: **

**מסך פרטי המשתמש: **

**7. פרוטוקול תקשורת**

**בסוקט הודעות כלליות** שליחת הודעה:  
תמיד: אורך הודעה מוצפנת – 2 בתים, הודעה עצמה מוצפנת

**בסוקט הקבצים** שליחת הודעה:  
תמיד: אורך הודעה מוצפנת – 10 בתים, הודעה עצמה מוצפנת

| **שם הפרוטוקול** | **שולח** | **נמען** | **opcode** | **שדות ההודעה** | **דוגמא** |
| --- | --- | --- | --- | --- | --- |
| **הרשמה** | **לקוח** | **שרת** | **01** | * **אורך שם משתמש (2 בתים)** * **שם המשתמש** * **אורך סיסמא (2 בתים)** * **סיסמא** * **אורך מייל (2 בתים)** * **מייל** | **0104reef06reef1114 reef@gmail.com** |
| **הרשמה** | **שרת** | **לקוח** | **01** | **0/1 הצליח/נכשל** | **010** |
| **התחברות** | **לקוח** | **שרת** | **02** | * **אורך שם משתמש (2 בתים)** * **שם המשתמש** * **אורך סיסמא (2 בתים)** * **סיסמא** | **0204reef07reef981** |
| **התחברות** | **שרת** | **לקוח** | **02** | **0/1 הצליח/נכשל** | **021** |
| **שליחת שמות הקבצים במחיצה** | **שרת** | **לקוח** | **03** | * **אורך שם התיקייה (2 בתים)** * **שם התיקייה** * **אורך שמות התיקיות שבתיקייה (4 בתים)** * **שמות התיקיות שבתיקייה מופרד על ידי !** * **אורך שמות הקבצים שבתיקייה (4 בתים)** * **שמות הקצבים שבתיקייה מופרד על ידי @** | **01b0003a!c0019file2.txt@03 hello.txt** |
| **שינוי תמונת פרופיל** | **לקוח** | **שרת** | **04** | * **אורך שם משתמש חדש (2 בתים)** * **שם משתמש חדש** | **0408Reef6213** |
| **שינוי תמונת פרופיל** | **שרת** | **לקוח** | **04** | **0/1 הצליח/נכשל** | **040** |
| **שינוי אימייל** | **לקוח** | **שרת** | **05** | * **אורך אימייל חדש (2 בתים)** * **אימייל חדש** | **0518Reef6213@gmail.com** |
| **שינוי אימייל** | **שרת** | **לקוח** | **05** | **0/1 הצליח/נכשל** | **051** |
| **שינוי סיסמא** | **לקוח** | **שרת** | **06** | * **אורך סיסמא חדשה (2 בתים)** * **סיסמא חדשה** | **0608Reef@41!** |
| **שינוי סיסמא** | **שרת** | **לקוח** | **06** | **0/1 הצליח/נכשל** | **060** |
| **שליחת אימייל לאימות** | **לקוח** | **שרת** | **07** | * **אורך המייל (2 בתים)** * **מייל** | **0717reefg19@gmail.com** |
| **שליחת אימייל לאימות** | **שרת** | **לקוח** | **07** | **0/1 הודעה נשלחה כן/לא** | **071** |
| **שינוי שם קובץ** | **לקוח** | **שרת** | **08** | * **אורך שם ישן + הנתיב (2 בתים)** * **שם ישן + הנתיב** * **אורך שם חדש (2 בתים)** * **שם חדש** | **0816folder/text1.txt12fold er12.txt** |
| **שנוי שם קובץ** | **שרת** | **לקוח** | **08** | **0/1 הצליח/נכשל** | **081** |
| **שיתוף קובץ** | **לקוח** | **שרת** | **09** | * **אורך שם + נתיב (2 בתים)** * **שם + נתיב** * **אורך שם אליו משתפים (2 בתים)** * **שם אליו משתפים** | **0915reef/myText.txt06 friend** |
| **שיתוף קובץ** | **שרת** | **לקוח** | **09** | **0/1 הצליח/נכשל** | **090** |
| **מחיקת קובץ** | **לקוח** | **שרת** | **10** | * **אורך שם + נתיב (2 בתים)** * **שם + נתיב** | **1016files/text1.docx** |
| **מחיקת קובץ** | **שרת** | **לקוח** | **10** | **0/1 הצליח/נכשל** | **100** |
| **הורדת קובץ** | **לקוח** | **שרת** | **11** | * **אורך שם + נתיב (2 בתים)** * **שם + נתיב** | **1108text.txt** |
| **הורדת קובץ** | **שרת** | **לקוח** | **11** | * **אורך מידע הקובץ (6 בתים)** * **מידע הקובץ** | **110000131001011011101** |
| **העלאת קובץ** | **לקוח** | **שרת** | **12** | * **אורך נתיב + שם לשמירה (2 בתים)** * **נתיב + שם לשמירה** * **אורך מידע הקובץ (6 בתים)** * **מידע הקובץ** | **1216random/file1.txt000012 101101011010** |
| **העלאת קובץ** | **שרת** | **לקוח** | **12** | **0/1/2 הצליח/קובץ כבר קיים/נכשל** | **121** |
| **יצירת מחיצה** | **לקוח** | **שרת** | **13** | * **אורך נתיב + שם לשמירה (2 בתים)** * **נתיב + שם לשמירה** | **1314folders/reefs** |
| **יצירת מחיצה** | **שרת** | **לקוח** | **13** | **0/1/2 הצליח/שם תיקייה קיים/נכשל** | **130** |
| **עידכון הוספת קובץ** | **שרת** | **לקוח** | **14** | * **אורך נתיב + שם (2 בתים)** * **נתיב + שם** | **1410reefs/page** |
| **אימות במייל** | **לקוח** | **שרת** | **15** | * **אורך קוד (2 בתים)** * **קוד** | **1513reefg19@gmail0512345** |
| **אימות במייל** | **שרת** | **לקוח** | **15** | **/01 הצליח/נכשל** | **150** |
| **פורט להעלאת קובץ** | **שרת** | **לקוח** | **16** | **מספר פורט** | **161200** |
| **בקשה לאימות** | **לקוח** | **שרת** | **17** | * **אורך שם משתמש (2 בתים)**   **שם משתמש** | **1704reef** |

**8. תיאור מבני הנתונים של הפרויקט:**

* **Queue – ישמשו להעברת ההודעות הנכנסות מהתקשורת ללוגיקה**
* **Dictionary – ישמשו לאחזקת פרטי הלקוחות המחוברים, פעולות לטיפול בהודעות נכנסות ועוד.**
* **List – ישמשו להחזקת פרטי משתמשים**
* **Tuple – המידע שיוכנס לתורים יכלול תמיד גם מידע מזהה על הלקוחות לדוגמא (ip, msg)**

מאגר המידע שאשתמש בו הוא מערכת הקבצים של windows. **במחשב השרת** לכל משתמש תהיה תיקייה בשם המשתמש שלו שתכיל את כל הקבצים והתיקיות שלו.

מסד הנתונים שאשתמש בו הוא מסד נתונים מסוג SQL בעל טבלה אחת

שם מסד הנתונים: **GolDrive**

הטבלה: טבלת המשתמשים

שם הטבלה: users  
מפתח הטבלה: שם המשתמש username  
שדת הטבלה:

* **username – שם המשתמש מטיפוס String**
* **password – סיסמת המשתמש מוצפנת באמצעות hash מטיפוס String**
* **email – מייל המשתמש מטיפוס String**

**דוגמא:**

|  |  |  |
| --- | --- | --- |
| **email** | **password** | **username** |
| **עד 50 תווים** | **עד 10 תווים** | **עד 10 תווים** |
| **reefg19@gmail.com** | **av123ffas151** | **1Reef** |
| **Imrih2006@gmail.com** | **ta12mam61** | **Imri24** |

**9. היבטי אבטחה בפרויקט – חולשות והדרך לטפל בהן**

| **שם החולשה** | **תיאור החולשה** | **פתרון** |
| --- | --- | --- |
| **Sql injection** | בעזרת הכנסות קלט מסוימות המשתמש עלול להשתמש בהם על מנת לקבל פרטים חשאיים ולחדור למערכת | במימוש שאילתות ה SQL אדאג לשימוש בקוד שלא יאפשר הכנסת מידע מזיד לשאילתא |
| **MITM** | מישהו עלול להאזין לתקשורת ולגלות פרטיים חשאיים | הצפנת כלל המידע שעובר ברשת ובנוסף מתקבלת הודעת אישור על כל בקשה מהשרת או מהלקוח מהצד השני |
| **DOS/DDOS** | הצפת השרת בהודעות התחברות | המערכת לא תאפשר הרבה ניסיונות של התחברות מכתובת אחת בפרק זמן קצר ולאחר מספיק ניסיונות תחסום את הכתובת |
| **התחזות** | משתמש עלול לגלות פרטים של משתמש ולפרוץ לחשבון שלו | התוכנה תשתמש באימות דו שלבי ותשלח מייל למשתמש אליו ניסו להתחבר ורק לאחר הכנסת הקוד הסודי שנשלח למייל יוכל להתחבר לחשבון |

פרק ה - **'goldrive'** – הקוד

**1 .**מימוש הסוקטים בפרויקט

**class** PortsHandler:  
 unused\_ports = (port **for** port **in** range(1235, 2235))  
  
 @staticmethod  
 **def** get\_next\_port():  
 *"""* **:return***: returns the next port in the generator  
 """* **return** next(PortsHandler.unused\_ports)

סוג ההצפנה בפרויקט

**import** base64  
**from** Cryptodome.Cipher **import** AES  
**from** Cryptodome **import** Random  
**import** hashlib  
**import** random  
**import** chardet  
  
  
**class** Encryption(object):  
 **def** \_\_init\_\_(self, key):  
 *"""* **:param** *key: the encryption key  
 """* self.bs = AES.block\_size  
 self.key = hashlib.sha256(str(key).encode()).digest()  
  
 **def** enc\_msg(self, message):  
 *"""* **:param** *message: the message to encrypt* **:return***: the encrypted message  
 """* **if** type(message) == str:  
 message = message.encode()  
 raw = self.\_pad(message)  
 iv = Random.new().read(AES.block\_size)  
 cipher = AES.new(self.key, AES.MODE\_CBC, iv)  
 **return** base64.b64encode(iv + cipher.encrypt(raw))  
  
 **def** dec\_msg(self, encrypt\_message):  
 *"""* **:param** *encrypt\_message: the encrypted message to decrypt* **:return***: the decrypted message  
 """* enc = base64.b64decode(encrypt\_message)  
 iv = enc[:AES.block\_size]  
 cipher = AES.new(self.key, AES.MODE\_CBC,iv)  
 a = self.\_unpad(cipher.decrypt(enc[AES.block\_size:]))  
 encoding = chardet.detect(a)  
 **if** encoding[**'encoding'**] == **"ascii"**:  
 a = a.decode()  
 **return** a  
  
 **def** \_pad(self, message):  
 *"""* **:param** *message: message* **:return***: the message with the padding  
 """* **return** message + (self.bs - len(message) % self.bs) \* chr(self.bs - len(message) % self.bs).encode()  
  
 @staticmethod  
 **def** \_unpad(message):  
 *"""* **:param** *message: encrypted message* **:return***: the encrypted message without the padding  
 """* **return** message[:-ord(message[len(message) - 1:])]  
  
  
**def** hash\_msg(msg):  
 *"""* **:param** *msg: the msg to hash* **:return***: the hash of the msg  
 """* **return** hashlib.sha3\_256(msg.encode()).hexdigest()  
  
  
**def** get\_dh\_factor():  
 *"""* **:return***: creates the dh factor  
 """* private\_key = random.randint(1, p)  
  
 **return** private\_key, (g \*\* private\_key) % p  
  
  
**def** create\_symmetry\_key(private\_key, shared\_key):  
 *"""* **:param** *private\_key: the personal key* **:param** *shared\_key: the key i got from the server* **:return***: returns the symmetrical encryption object from the dh key change  
 """* **return** Encryption((shared\_key \*\* private\_key) % p)  
  
  
p = 7723  
g = 1229

העברת המידע על הקבצים

**def** pack\_files\_message(username):  
 *"""* **:param** *username: username of user* **:return***: string with all files and directories of user in the drive  
 """* files\_of\_user = **"03"**path = **f"{**Settings.SERVER\_FILES\_PATH**}/{**username**}"  
  
 for** (dirname, dirs, files) **in** os.walk(path):  
 *# removing the path so that it's only the directories in the system and not from the server* dirname = dirname[len(path) + 1::].replace(**'\\'**, **'/'**)  
  
 *# adding the length of the name and the name* files\_of\_user += str(len(dirname)).zfill(2) + dirname  
  
 *# adding the length of the directories and the directories list* dirs = **'!'**.join(dirs)  
 files\_of\_user += str(len(dirs)).zfill(4) + dirs  
  
 *# adding the length of the files and the files list* files = **'@'**.join(files)  
 files\_of\_user += str(len(files)).zfill(4) + files  
  
 files\_of\_user += **'\n'  
  
 return** files\_of\_user

אופן שמירת הקבצים **של המשתמשים בשרת**

**def** \_handle\_email\_register(main\_server, db, client\_ip, code\_dic, username, password, email, code, dont\_ask\_again):  
 *"""* **:param** *main\_server: the server object* **:param** *db: the database* **:param** *client\_ip: the clients ip* **:param** *code\_dic: dictionary containing the code sent to an email* **:param** *username: the username of the client* **:param** *password: the password of the client* **:param** *email: the email of the client* **:param** *code: the code entered* **:param** *dont\_ask\_again: does the user want to verify his email in his computer* **:return***: try's adding the user to the database and sends response to the client  
 """* ans = 2  
  
 **if** email **in** code\_dic:  
 **if** code\_dic[email] == code:  
 **if** 4 <= len(username) <= 10 **and** len(password) >= 4:  
 ans = db.add\_user(username, password, email)  
  
 **if** ans == 0 **and** dont\_ask\_again == **"True"**:  
 db.add\_remembered\_ip(username, client\_ip)  
  
 msg = serverProtocol.pack\_register\_verify\_response(ans)  
 main\_server.send(client\_ip, msg)  
  
 **if** ans == 0:  
 **if not** os.path.isdir(**f"{**Settings.SERVER\_FILES\_PATH**}/{**username**}"**):  
 os.mkdir(**f"{**Settings.SERVER\_FILES\_PATH**}/{**username**}"**)  
 os.mkdir(**f"{**Settings.SERVER\_FILES\_PATH**}/{**username**}/@#$SHAREDFILES$#@"**)

אופן שמירת הסיסמא של המשתמש בבסיס הנתונים

**def** add\_user(self, username, password, email):  
 *"""* **:param** *username: username* **:param** *password: password* **:param** *email: email* **:return***: adds user to table  
 """* flag = 1  
 **if not** self.username\_exist(username):  
 sql = **"INSERT INTO users VALUES (?,?,?)"** self.curr.execute(sql, (username, encryption.hash\_msg(password), email))  
 self.conn.commit()  
  
 flag = 0  
 **return** flag

אופן העברת תיאור מבנה הקבצים של המשתמש ללקוח (לטובת הצגתם בממשק המשתמש)

**def** pack\_files\_message(username):  
 *"""* **:param** *username: username of user* **:return***: string with all files and directories of user in the drive  
 """* files\_of\_user = **"03"** path = **f"{**Settings.SERVER\_FILES\_PATH**}/{**username**}"  
  
 for** (dirname, dirs, files) **in** os.walk(path):  
 *# removing the path so that it's only the directories in the system and not from the server* dirname = dirname[len(path) + 1::].replace(**'\\'**, **'/'**)  
  
 *# adding the length of the name and the name* files\_of\_user += str(len(dirname)).zfill(2) + dirname  
  
 *# adding the length of the directories and the directories list* dirs = **'!'**.join(dirs)  
 files\_of\_user += str(len(dirs)).zfill(4) + dirs  
  
 *# adding the length of the files and the files list* files = **'@'**.join(files)  
 files\_of\_user += str(len(files)).zfill(4) + files  
  
 files\_of\_user += **'\n'  
  
 return** files\_of\_user

בדיקה מתי הלקוח סוגר את הקובץ שהוא רצה לפתוח מתוך האפליקציה

def get\_all\_pid(process\_name):  
 current = []  
 for p in psutil.process\_iter():  
 if p.name() == process\_name:  
 current.append(p.pid)  
  
 return current  
  
  
def wait\_until(file\_path, q):  
 file\_extension = file\_path[file\_path.rfind('.') + 1:]  
  
 if file\_extension in default\_for\_type:  
 process\_name = default\_for\_type[file\_extension]  
 else:  
 process\_name = 'Notepad.exe'  
  
 ls1 = get\_all\_pid(process\_name)  
 subprocess.Popen(['start', file\_path], shell=True)  
  
 while True:  
 ls2 = get\_all\_pid(process\_name)  
 if ls2 != ls1:  
 break  
  
 new\_pid = set(ls2) - set(ls1)  
 pid = list(new\_pid)[0]  
  
 while psutil.pid\_exists(pid):  
 pass  
  
 q.put("Finished")

פרק ו - **'goldrive'** – בדיקות('קופסא לבנה')

| **מספר** | **שם הבדיקה** | **מטרת הבדיקה** | **מה נרדש לבצע** | **מתי** | **מה בוצע בפועל** |
| --- | --- | --- | --- | --- | --- |
| **1** | **התחברות** | **האם אפשר להתחבר למשתמש כמו שצריך** | **לפתוח את המערכת, להתחבר עם שם משתמש וסיסמא נכונים ולראות שמצליחים להיכנס למערכת.**  **לחזור על הפעולה עם שם משתמש וסיסמא שגויה ולראות שלא מצליחים להיכנס למערכת** | **7.5.24** | **הכניסה למשתמש מתאפשרת רק בהכנסת פרטי משתמש תקינים** |
| 2 | העלאת קבצים | האם אפשר לשמור קבצים למשתמש | לפתוח את המערכת ולהתחבר עם שם סיסמא ומשתמש, לנסות להעלות קובץ ולראות שהוא עלה ומוצג בקבצים שלי, במידה והוא עלה להתנתק מהמשתמש ולהתחבר שוב ולראות שהקובץ עדיין מוצג. | 7.5.24 | העלאת קבצים מתאפשרת ונשמרת גם להתחברות הבאה |
| 3 | הורדת קבצים | האם אפשר להוריד קבצים | לפתוח את התוכנה, להתחבר למשתמש, לבחור קובץ ולנסות להוריד אותו, לבדוק האם הקובץ מורד כמו שצריך ובמקום הנכון. | 7.5.24 | הקובץ מורד להכין שהמשתמש בחר ומכיל את התוכן |
| 4 | איש שלישי | האם אפשר לקרוא מידע שעובר | לפתוח Wireshark ואז לפתוח את התוכנה, להתחבר למשתמש ולנסות להעלות קובץ אחר כך לבדוק Wireshark האם אפשר לקרוא את המידע שעבר או שהוא מוצפן. | 12.5.24 | המידע שעובר בתקשורת מוצפן היטב ואינו ניתן לקריאה. |
| 5 | שיתוף קבצים | האם אפשר לשתף קובץ עם חבר | לפתוח את התוכנה להתחבר למשתמש, לבחור קובץ ולשתף אותו עם משתמש אחר, להתחבר למשתמש האחר ולראות האם הקובץ ששותף מופיע באזור השיתופים. | 7.5.24 | ניתן לשתף קבצים עם משתמשים אחרים. מופיע בזמן אמת. |
| 6 | מחיקת קבצים | האם אפשר למחוק קבצים | לפתוח את התוכנה, להתחבר למשתמש, לבחור קובץ ולנסות למחוק אותו, לראות שהקובץ נמחק ולא מופיע, להתחבר מחדש למשתמש ולראות שהקובץ עדיין לא מופיע. | 7.5.24 | ניתן למחוק קבצים ולא מופיע גם לאחר התנתקות והתחברות מחדש. |
| 7 | שינוי שם | האם אפשר לשנות שם לקובץ | לפתוח את התוכנה, להתחבר למשתמש, לבחור קובץ ולנסות לשנות לו את השם, לראות שהשם משתנה כמו שצריך, להתחבר מחדש ולראות שהשם נותר משונה. | 7.5.24 | ניתן לשנות לקובץ השינוי מופיע גם לאחר התנתקות והתחברות מחדש. |
| 8 | כניסה כפולה | לבדוק האם המערכת מונעת ממשתמש אחד להיכנס בו זמנית ממחשבים שונים | לפתוח את התוכנה, ליצור משתמש, לראות שמתחבר כמו שצריך, ולנסות להתחבר לאותו משתמש ממחשב אחר ולראות שזה **לא** מתחבר. | 12.5.24 | אי אפשר להתחבר מ2 מחשבים לאותו משתמש באותו הזמן. |
| 9 | בדיקת ביצועים | לבדוק האם המערכת מבצעת פעולות במהירות | לפתוח את התוכנה, להתחבר למשתמש ולנסות לבדוק כל פעולה שמתאפשרת לקובץ ולבדוק שהכל נעשה במהירות. | 7.5.24 | כל הפעולות נעשות בצורה מהירה. |
| 10 | בדיקת יציבות | לבדוק האם המערכת מתפקדת בקביעות למרות שיש מספר משתמשים מחוברים | לפתוח את התוכנה במספר מחשבים, להתחבר מכל מחשב למשתמש ומכל משתמש להריץ איזושהי פעולה על קובץ, לראות שבכל משתמש הפעולה נעשתה כמו שצריך. | 7.5.24 | המערכת מתפקדת בקביעות גם כשיש מספר משתמשים מחוברים |
| 11 | זמני תגובה | לבדוק האם יש הבדלים בזמני התגובה של המערכת כאשר מורידים/מעלים קבצים בגדלים שונים | לפתוח את התוכנה, להתחבר למשתמש ולנסות להעלות ולהוריד קבצים שונים בעלי גודל שונה ולבדוק את הזמן שלוקח. | 7.5.24 | יש הבדל בזמני התגובה רק כאשר מדובר בקובץ גדול מאוד, אחרת העבודה עם הקבצים היא מהירה מאוד. |