שם התלמיד: יובל כוינה שם הפרויקט: ExtremLink

**מאת: יובל כוינה**

**ת.ז: 216825737**

**בית הספר: מקיף ג' אשדוד**

**שם המנחה: מורן טובול**

**שם הפרויקט: ExtremLink**

**שם החלופה: תכנון ותכנות מערכות**

**שנת ההגשה: 2025**



תוכן עניינים:

מבוא:

תיאור תכולת הספר:

ספר הפרויקט שלי כולל מבוא, אשר מתאר את מטרת הפרויקט, תהליך המחקר ואתגרים מרכזיים שאיתם התמודדתי. בנוסף לכך, הספר כולל גם ארכיטקטורה של הפרויקט, מדריך למשתמש, הסבר על בסיסי הנתונים שיצרתי ומדריך למפתח, כאשר על פרק יסביר יותר לעומק על הפרויקט שלי ומרכיביו. בסוף הספר מופיעים רפלקציה אישית וביבליוגרפיה.

רקע על הפרויקט:

הפרויקט שלי נקרא: ExtremLink, והוא מהווה פלטפורמה להשתלטות מרחוק על מחשבים אשר יצרתי. כלומר, תוכנה המבוססת על בסיס מודל שרת-לקוח המתוכנת בשפת #C בסביבת העבודה WPF - Windows Presentation Foundation. בנוסף, השרת כולל גם מאגרי מידע מסוג SQL, כאשר מטרתם הוא לאחסן את נתוני המשתמשים של הלקוחות ואת ההקלטות של ההשתלטויות של אותם המשתמשים.

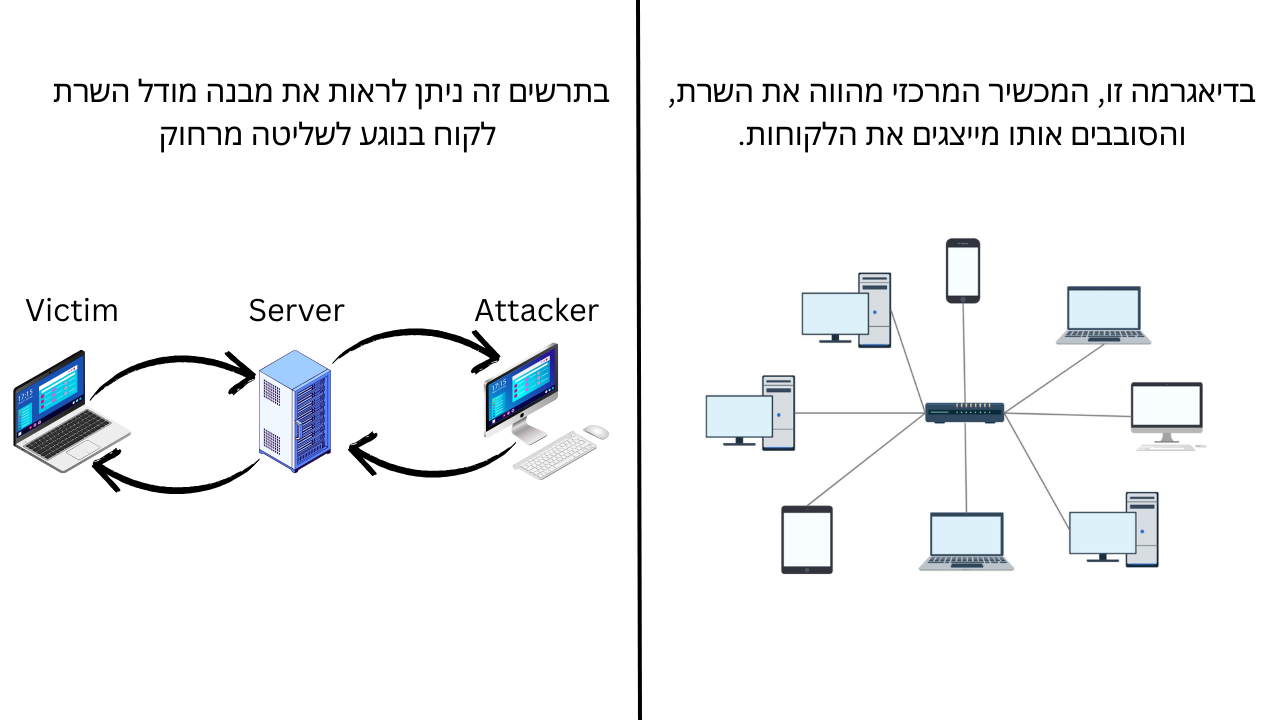
הפרויקט מאפשר תקשורת בין המשתמשים אשר הוזנו במערכת, כאשר התקשורת נעשית על ידי שיתוף מסך המחשב של הלקוח המשתף אל הלקוח השולט. לשם הרשמה למערכת ויצירת חשבון חדש, על הלקוח להזין שם משתמש, סיסמה, את שמו הפרטי, את שם המשפחה שלו, את מקום מגוריו, מספר הטלפון שלו ואת כתובת המייל שלו. לאחר שנתוני הלקוח הוזנו, הם מתאכסנים בתוך מאגר המידע של הלקוחות שנמצא בצד של השרת ובאפשרותם להזדהות במערכת באמצעות שם המשתמש שלהם והסיסמה בלבד. במידה והלקוח שכח את הסיסמה למשתמש שלו באפשרותו לשחזרה באמצעות בקשה לשליחה חוזרת של הסיסמה לכתובת המייל שלו ובכך לשחזר את סיסמתו. לאחר ש 2 לקוחות שונים (משתף ושולט) מתחברים למערכת באותה רשת פנימית, באפשרותם להתחיל את השליטה מרחוק, לעצור אותה באופן זמני, לעצור אותה באופן מוחלט, להמשיך אותה ואף להקליטה במידת הצורך! לאחר מכן במידה ואחד הלקוחות רוצה לצפות בהקלטה שביצע (בתור תוקף) באפשרותו לבחור באחת מבין ההקלטות המשויכות לו ממאגר המידע של ההקלטות ולצפות בה בנגן הוידאו בתוכנה עצמה.

תהליך המחקר:

תהליך המחקר המקדים לפרויקט שאותו ביצעתי, מהווה חקירה לעומק על מודל שרת-לקוח. מודל זה הינו ארכיטקטורת תוכנה לחישוב מבוזר, אשר מגדירה את היחס בין תוכנות משתפות פעולה על בסיס רשת דיגיטלית. כלומר, המודל מורכב משני חלקים, כאשר הוא מחלק את המשימות או את עומס העבודה ביניהם. יישום השרת הינו אחד מהחלקים המרכיבים את המודל, ותפקידו לספק את השירותים/משאבים אל מבקשי השירות. אלו נקראים הלקוחות אשר מהווים את החלק השני של המודל.

**השרת** הינו תוכנה פסיבית המאזינה לרשת באופן תמידי, ומחכה לקבל בקשות. לעומת זאת, **הלקוח**, שהוא לרוב מהווה את ממשק המשתמש, מופעל על ידי המשתמש והוא פונה לשרת כאשר הוא זקוק למידע או לשירותים ממנו. אופן התקשורת בין שני חלקי היישום נעשית על ידי העברת הודעות כפי שנקבע בפרוטוקול התקשורת. כלומר, כאשר לקוח מעוניין לקבל שירות מהשרת, הוא שולח לשרת בקשה ליצירת קשר. לאחר מכן, השרת אשר מאזין ומחכה לקבל בקשות, מקבל את הבקשה ומשיב עליה. מכאן, שניתן להגדיר את הלקוח כיוזם קשר, ואת השרת כמאזין ליצירת קשר. הלקוח בדרך כלל נדרש לדעת את שמו של השירות אותו הוא מעוניין לקבל, ובנוסף את שמו או שמותיהם של השרת או השרתים הזמינים על מנת להגיע אליהם. בניגוד לכך, השרת אינו צריך לדעת מי הם לקוחותיו ואת מספר הלקוחות שיש.

היותו של מודל שרת לקוח ארכיטקטורה מבוזרת, מהווה יתרון חשוב ביותר, כאשר הוא יכול לנצל ביעילות מספר רב של משימות. בנוסף, ניתן לשלב שרת או לקוח חדשים לתוך המערכת ולשדרג קיימים, מבלי להשפיע על חלקים אחרים במערכת ובצורה קלה ביותר.

ישנם שני צורות שלפיהם מודל שרת לקוח יכול לפעול, כאשר בדרך כלל תוכנות השרת והלקוח רצות על גבי מחשבים שונים והתקשורת ביניהם מתבצעת על גבי רשת מחשבים. אולם, ישנם מקרים שבהם המודל פועל לפי צורת הפעולה השנייה, כאשר היא מתבססת על כך שהתוכנות רצות על גבי אותו המחשב. מודל השרת לקוח הפך לאחד מהרעיונות המרכזיים ברשתות מחשבים, כאשר מספר רב של יישומים אשר נכתבים היום משתמשים ומבוססים על מודל זה. שירותים כגון: גישה לאתרי אינטרנט, גישה לבסיסי נתונים, וכמו כן גם הפרויקט שלי אשר מהווה שירות המאפשר תקשורת בין מחשבים תוך שימוש בשרת המיועד לקבל ולשלוח נתונים ללקוחות המחוברים אליו כמו לדוגמה בעת ההשתלטות שהלקוח המשתף שולח את הפריימים מהמסך שלו אל השרת והשרת בתגובה מעביר אותם למחשב התוקף.

טופולוגית רשת מתארת את הסידור הממשי או הווירטואלי של הרכיבים השונים ברשת מחשבים. דוגמא לטופולוגית רשת הינה טופולוגית כוכב, המכונה גם רשת כוכבים, והיא אחת מהתקנות הרשת הנפוצות ביותר. בתצורה זו, כל הצמתים (nodes) מתחברים לרכיב תקשורת אחד הנמצא במרכז באמצעות כבלים, כאשר רכיב התקשורת המרכזי יכול להיות: מרכזת, מתג, נתב, מחשב וכדומה. רכיב תקשורת זה מהווה ופועל כשרת, כאשר המכשירים הסובבים אותו פועלים כלקוחות. נוצרת כאן תצורה בצורת כוכב, וכך טופולוגית רשת זו קיבלה את שמה. תמונה שמכילה שרטוט, תרשים, עיצוב

תוכן שנוצר על-ידי בינה מלאכותית עשוי להיות שגוי.

היתרונות של הרשת כוללים את זה שרשת כזו הינה קלה לתחזוקה, וניתן להסיר ולהוסיף אליה קצוות בקלות. בנוסף, אם אחד מן המכשירים ההיקפיים הנמצאים ברשת מפסיק לפעול, זה אינו משפיע על המכשירים האחרים והרשת ממשיכה לפעול כרגיל.

עם זאת, לטופולוגית כוכב ישנם חסרונות הכוללים את זה שהיא בזבזנית במקצת באורכי הכבלים שהיא דורשת. בנוסף, הצומת המרכזי מהווה נקודת חולשה בטופולוגית כוכב, מכיוון שבמידה וצומת זו אינו פעיל, כל הרשת אינה יכולה לתפקד. יתר על כן, מכשיר הרשת המרכזי קובע את הביצועים ואת מספר הצמתים שהרשת יכולה להתמודד איתם.

אתגרים מרכזיים:

הבעיה שאיתה התמודדתי ופתרונותיה -

הייתי צריך להתמודד עם מספר אתגרים במהלך עבודתי על הפרויקט, כאשר הבעיה העיקרית שהייתי צריך להתמודד עימה הייתה העברת הפריימים של השידור החי של שיתוף המסך בפרויקט בין המחשבים. כדי להתמודד עם בעיה זו, היה עלי לבצע תהליך חקירה לעומק על הנושא. החקירה כללה חיפוש על תקשורת נתונים, פרוטוקולי תקשורת המאפשרים לבצעה העברה מהירה של נתונים גדולים ושיטות להמרת הנתונים. מושגים אלו המגיעים מעולמות מדעי המחשב והתקשורת מתעסקים בתקשורת בין מחשבים הכוללת העברת נתונים גרפיים כגון תמונות וודיאו בזמן אמת תוך מימוש מספר עקרונות המאפשרים ייעול מירבי של כלל התהליכים המעורבים בתקשורת הזאת. בפרוייקט שלי העוסק בהעברת קבצי תמונות וודיאו בזמן אמת היה עליי לערוך מחקר בנוגע לפרוטוקולי התקשורת המותאמים ביותר למשימה מה שהוביל אותי בסופו של דבר להשתמש בפרוטוקול UDP. פרוטוקול זה שנמצא בשכבת התעבורה (כחלק ממודל השכבות שעליו מבוססת התקשורת האינטרנטית) נמצא כיעיל ביותר להעברת נתונים רחבי היקף בזמן קצר על חשבון אמינות המידע שהתקבל (בחלקו או בשלמותו) מכיוון שהוא אינו בודק את אמינות המידע על מנת לצמצם זמן חשוב. לכן השימוש המושכל בפרוטוקול היה אבן דרך משמעותית בפתרון הבעיה שאיתה התמודדתי. בנוסף לכך, בנוגע להמרת הנתונים היה עליי לחקור על שיטות המרה של נתונים בפורמט וויזואלי לידי פורמט בינארי (שפה המבוססת על בסיס 2 המכיל את הספרות 0 ו 1) הידוע ככזה המשמש לתקשורת בין מחשבים. לכן הבנתי שהפתרון הטוב ביותר שאיפשר לי המרה של תמונות ווידאו לפורמט בינארי הוא יצירה של קבצים זמניים שיאחסנו באופן זמני את האמצעים הוויזואלים ולאחר מכן שליחה של התוכן הבינארי של הקבצים עצמם. ובכך פתרתי את הבעיה המרכזית שלי בפרויקט!

הסיבות לבחירת הפרויקט ומוטיבציה לעבודה -

אני בחרתי בפרויקט ExtremLink, מכיוון שהיה לי רצון וכמיהה ליצור פרויקט המיישם עקרונות מעולמות תקשורת הנתונים והסייבר שאני מאוד מתחבר אליהם ואף חוקר עליהם בשעות הפנאי. בנוסף לכך, גם ברצוני היה ליצור פרויקט גדול ומסודר שאוכל להוסיפו לתיק הפרויקטים שלי ולהשתמש בו בתור אסמכתא לשימוש עתידי בתעשיית היי-טק.

מה גם, הפרויקט איפשר לי לצבור ניסיון מעמיק ורב בתכנות ככלל ובשפת סי-שארפ בפרט. ניסיון זה כמובן יקנה לי יתרון בשוק העבודה וגם ייאפשר לי ליצור פרויקטים נוספים בתחום ואף להגיע לתוצרים שלא חלמתי שאוכל ליצור!

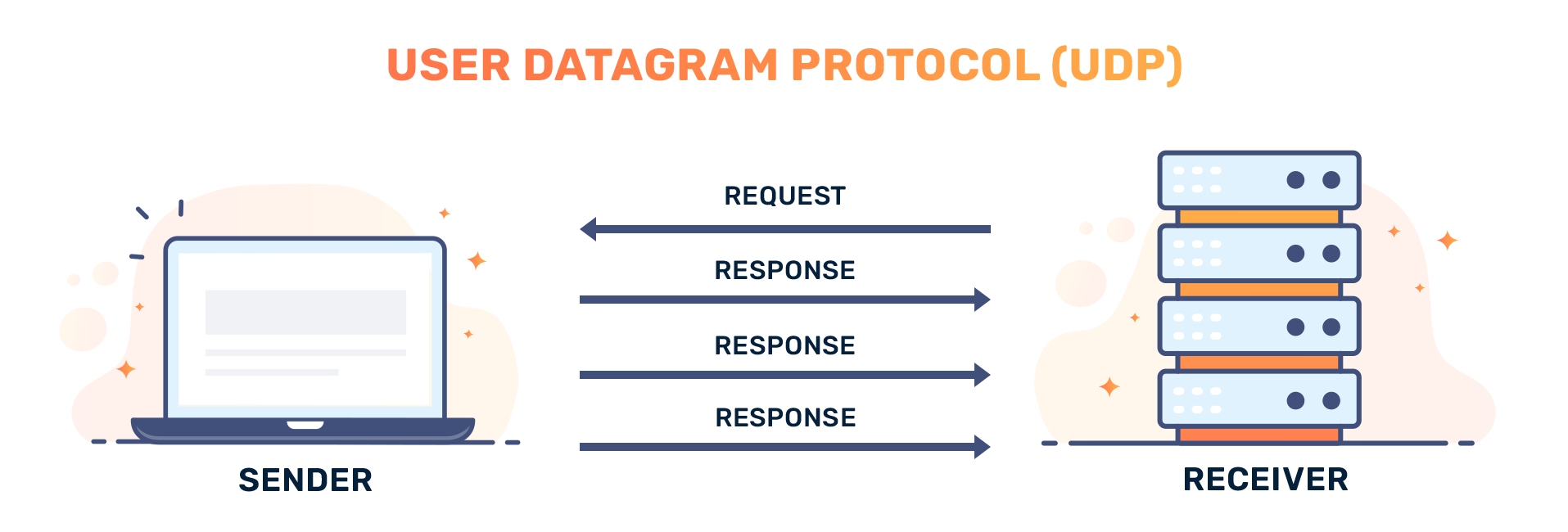
הצורך שעליו עונה הפרויקט -

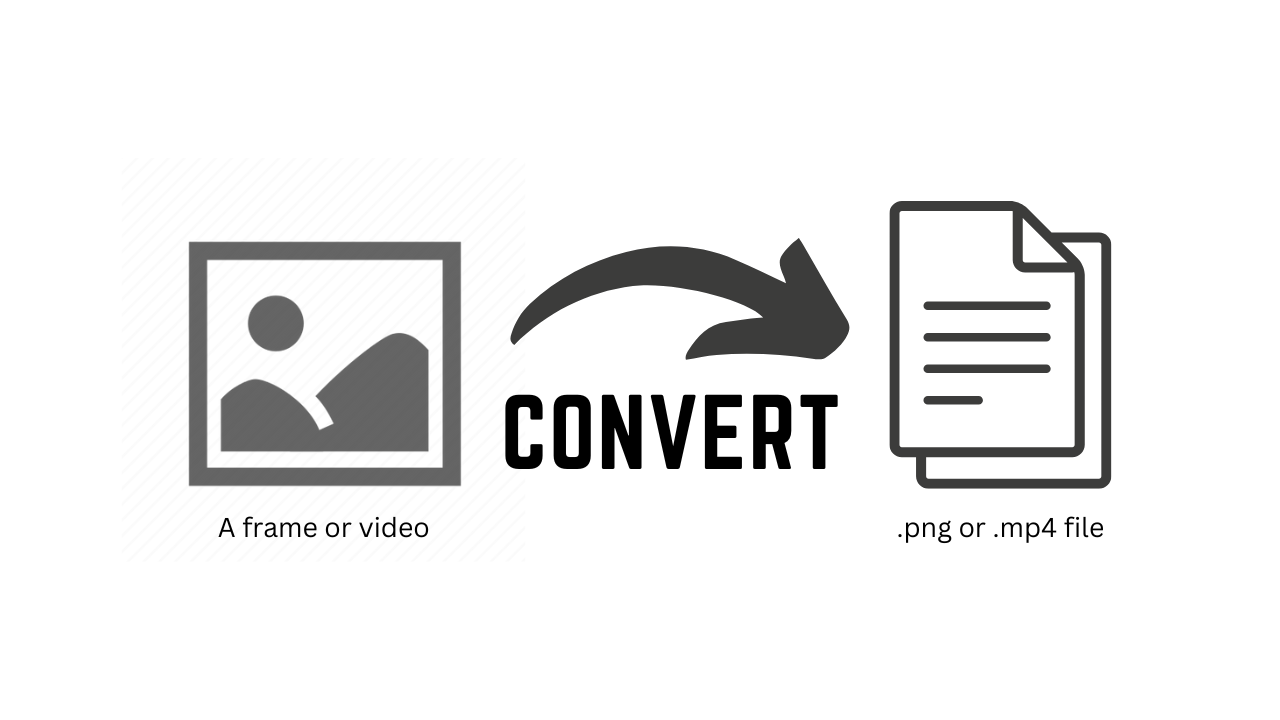
הפרויקט שלי עונה על הצורך לאמצעי תקשורת זמין ומהיר, כאשר לקוח מסוים נתקל בבעיה כלשהי במחשבו האישי וברצונו שמפעיל מרחוק כגון טכנאי או כמגיש שירות לקוחות יתקן את התקלה מרחוק ללא צורך בהגעה פיזית. פתרון זה יפתח צוהר לשירותים חדשים בעולמות טכנאות המחשבים ויקל על הלקוחות.

מבנה / ארכיטקטורה של הפרויקט:

הצגת הפתרון המוצע והסיבות לבחירתו -

הביעה שאיתה התמודדתי הייתה העברת נתונים וויזואלים בין מחשבים, לצורך יצירת האפשרות לשיתוף מסך בין לקוחות. הדרך שאיתה התמודדתי הייתה חיפוש מעמיק ברחבי האינטרנט, באתרים העוסקים במדעי המחשב, בפורמים ואף לשאול מומחים העוסקים בתחום. הפתרונות כאמור מבוססים על מודל שרת-לקוח הם **שימוש בפרוטוקול UDP** ו**המרת נתונים לקבצים ושליחתם.**





מחלקות הפרויקט

צד שרת -

|  |  |  |
| --- | --- | --- |
| **קלט ופלט** | **תפקיד המחלקה** | **שם המחלקה** |
| **המחלקה לא מקבלת כלום והפלטים שלה כוללים מערכי בתים (byte arrays) המייצגים פריימים של וידאו או קבצי סשן מוקלטים, מחרוזות בפורמט JSON המכילות מידע על סשנים, רשימות של אובייקטים מסוג סשן, ערכים לוגיים (true/false) המצביעים על הצלחה או כישלון בפעולות מול מסד הנתונים, אובייקטים של חיבור למסד נתונים, וכן פלטים שאינם מוחשיים כמו שליחת נתונים דרך רשת, עדכון מידע אצל הלקוחות, או רישום פעולות ביומן לוגים – מבלי להחזיר ערך ישיר.** | **מחלקת Server אחראית על ניהול התקשורת בין לקוחות השולט והנשלט בתכונה. היא מטפלת בהתחברות ויצירת הלקוחות, בהעברת פקודות וידאו, מקלדת ועכבר, ובניהול משתמשים והקלטות מול מסד הנתונים, תוך התבססות על תבנית העיצוב Singleton.** | **Server** |
| **המחלקה מקבלת בעת יצירתה מחרוזת שמייצגת כתובת IP של שרת, וסוג של לקוח (תוקף או קורבן). הפלטים שלה כוללים הודעות בפורמט מפורק כמבני נתונים מתוך תקשורת TCP ו־UDP, אובייקטים של שקעי רשת (Sockets) שמייצגים ערוצי תקשורת שונים, כתובות IP ומידע מזהה של הלקוח. בנוסף, מתקיימות פעולות שלא מחזירות ערך ישיר אך גורמות לחיבור לרשת, שליחת הודעות, קבלת נתונים מהלקוח, וקביעת נקודת הקצה של תקשורת UDP בהתאם לסוג הלקוח.** | **מחלקת Client מייצגת לקוח (שולט או נשלט) בצד השרת. היא אחראית על ניהול החיבורים מסוג TCP ו-UDP מול השרת, קבלת ושליחת הודעות, שמירת פרטי המשתמש וה-IP של הלקוח, ותמיכה בתקשורת עבור זרמי וידאו וסשנים מוקלטים. המחלקה מהווה את נקודת הקצה בתקשורת מצד השרת מול הלקוח הרלוונטי.** | **Client** |
| **המחלקה מקבלת בעת יצירתה תאריך הקלטה, שם משתמש ולעיתים גם מזהה ייחודי של סשן. הפלטים שלה כוללים מערכי בתים (byte arrays) שמייצגים תוכן וידאו מוקלט, מחרוזות עם שמות משתמשים, מזהים מספריים ותאריכים. בנוסף, מתבצעות פעולות שלא מחזירות ערך ישיר אך מבצעות שמירה של נתוני הסשן למסד נתונים, פתיחת חיבורים למסד וכתיבת הודעות ליומן לוגים לצורך תיעוד הפעולות.** | **מחלקת Session מייצגת סשן של שליטה מרחוק הכולל הקלטת וידאו של פעילות המשתמש. היא שומרת את תוכן הווידאו כ־byte array, את זמן ההקלטה, את שם המשתמש ואת מזהה הסשן (ID). בנוסף, היא מאפשרת להעלות את הסשן למסד הנתונים לצורכי אחסון ושימוש מאוחר יותר.** | **Session** |
| **המחלקה אינה מקבלת כלום בעת יצירתה והפלט היחיד שלה הוא שם המשתמש בפורמט string.** | **מחלקת User מייצגת משתמש של לקוח במערכת. היא שומרת את שם המשתמש ומספקת ממשק פשוט לגישה למידע זה. המחלקה משמשת כתשתית בסיסית לזיהוי וניהול משתמשים בצד השרת.** | **User** |
| **המחלקה לא מקבלת קלט בעת יצירתה, והפלטים שלה כוללים מחרוזות המייצגות הודעות לוג, וכן פעולות שאינן מחזירות ערך ישיר אך גורמות לעדכון פנימי של יומן הרישום. בנוסף, מתבצעת גישה למופע יחיד של המחלקה המנוהל באופן עצמאי, תוך שמירה על עקביות של המידע לאורך חיי היישום.** | **המחלקה Log מנהלת יומן רישום (Log) של הודעות בצד השרת, באמצעות שמירה של רשימת הודעות תוך שימוש בתבנית העיצוב Singleton, המחלקה מאפשרת הוספה של הודעות ליומן ואיחסונם.** | **Log** |

צד לקוח -

|  |  |  |
| --- | --- | --- |
| קלט ופלט | תפקיד המחלקה | שם המחלקה |
| הפונקציות במחלקה **Client** פועלות על הנתונים הפנימיים שלה, כגון חיבורי הרשת וכתובות השרת, ללא צורך בקלט חיצוני. הפלטים המוחזרים משתנים בהתאם להקשר הפעולה - החל מנתונים בינאריים של פריימי וידאו וקבצי סשן, דרך מידע מובנה בפורמט JSON על מצב החיבורים, ועד רשימות אובייקטים המייצגות סשנים פעילים. הפונקציות מחזירות ערכים בוליאניים המעידים על הצלחה או כישלון בביצוע פעולות קריטיות כמו עדכון מסד נתונים, או לחילופין לבצע פעולות רקע כגון העברת נתונים, סנכרון בין לקוחות ורישום אירועים במערכת הלוגים - כל זאת ללא החזרת ערך ישיר. | מחלקת **Client** מייצגת לקוח שמתחבר לשרת מרחוק. היא אחראית על יצירת והגדרת החיבורים בין המחשב של המשתמש לשרת, כולל חיבורים רגילים וחיבורים מיוחדים לפעולות ספציפיות. המחלקה מאפשרת קבלת פרטים מהשרת כמו כתובתו והודעות וכמו כן אחראית לשלוח אליו הודעות ספציפיות לשרת וללקוחות אחרים דרך השרת. | Client |
| המחלקה לא מקבלת כלום והפלטים שלה כוללים מערכי בתים **המייצגים פריימים של וידאו או קבצי סשן מוקלטים, מחרוזת** | מחלקת **Attacker** מייצגת תוקף המחובר לשרת מרחוק ומנהל תקשורת עם קורבן. היא יורשת ממחלקת Client ומתמקדת בשליטה ובקרה על הקורבן - כולל קבלת תמונות מסך בזמן אמת, ניהול הקלטות, וטיפול בפקודות מקלדת ועכבר. המחלקה משתמשת בתבנית העיצוב **Singleton** ומטפלת בשליחה וקבלה של הודעות דרך חיבורי רשת ייעודיים, תוך פיצול הנתונים לחבילות והרכבתם מחדש. | Attacker |
|  | מחלקת **Victim** מייצגת קורבן המחובר לשרת מרחוק ומאפשר שליטה בו על ידי תוקף. היא יורשת ממחלקת Client ומתמקדת בטיפול בפקודות מהתוקף - כולל שליחת תמונות מסך, הקלטות, וקבלת פקודות מקלדת ועכבר. המחלקה משתמשת בתבנית העיצוב **Singleton** ומטפלת בחלוקת הנתונים לחבילות לפני שליחתם דרך הרשת. בנוסף, היא מספקת יכולת תגובה לשרת עם סטטוס פעולות כמו אישור קבלת פקודות או עדכון מצב ההקלטה. | Victim |
|  | מחלקת **User** מייצגת את המשתמש במערכת, בין אם הוא תוקף או קורבן. היא כוללת את שם המשתמש, סוג הלקוח (תוקף/קורבן) ורשימת ההקלטות שלו. המחלקה מאפשרת גישה ועדכון לפרטי המשתמש בצורה מבוקרת. | User |
|  | מחלקת Session מייצגת הקלטת מסך (session) במערכת. היא כוללת את תאריך ההקלטה, תוכן הווידאו (כמערך בתים) ומזהה ייחודי. המחלקה מספקת פונקציונליות לשליחת בקשות לשרת - הן לקבלת רשימת ההקלטות של משתמש מסוים והן לקבלת תוכן הקלטה ספציפית לפי ID. | Session |
|  | מחלקת **AttackerSession** אחראית על הקלטת וניהול סרטוני המסך מהצד התוקף. היא מספקת יכולת להתחיל ולהפסיק הקלטות, להוסיף פריימים לסרטון בזמן אמת, ולשלוח את ההקלטות לשרת. | AttackerSession |
|  | מחלקת **CustomMouseAttacker** מייצגת את ממשק העכבר של התוקף ומאפשרת שליטה מרחוק בעכבר הקורבן. היא בנויה כמופע יחיד Singleton ומנהלת את מיקום הסמן ופעולות העכבר. המחלקה יוצרת פקודות JSON הכוללות את סוג הפעולה (תזוזה/לחיצה) ומיקום הסמן, ושולחת אותן דרך השרת לקורבן. | CustomMouseAttacker |
|  | מחלקת **CustomMouseVictim** אחראית על ביצוע פעולות העכבר בפועל במחשב הקורבן. היא מקבלת פקודות מהתוקף (כמו תזוזה או לחיצות) ומתרגמת אותן לפעולות ממשיות על מערכת ההפעלה של הקורבן באמצעות קריאות ל **WIN API.** | CustomMouseVictim |
|  | מחלקת **CustomKeyboardAttacker** מייצגת את ממשק המקלדת בצד התוקף ומאפשרת שליטה מרחוק במקלדת הקורבן. המחלקה בנויה על פי תבנית העיצוב **Singleton.** | CustomKeyboardAttacker |
|  | מחלקת **CustomKeyboardVictim** מייצגת את ממשק המקלדת בצד הקורבן ומבצעת בפועל את פקודות המקלדת שמתקבלות מהתוקף. המחלקה בנויה על פי תבנית העיצוב **Singleton.** | CustomKeyboardVictim |
|  | מחלקת **SoundManager** אחראית על ניהול ושליטה בקבצי האודיו בתוכנה. היא בנויה על פי תבנית העיצוב **Singleton** ומספקת ממשק פשוט להפעלת מוזיקה בתוכנה. | SoundManager |
|  | מחלקת **EmailsManager** אחראית על ניהול ושליחת הודעות אימייל למתשמשים. המחלקה פועלת כמחלקה סטטית המשמשת לארגון פונקציות המאשרות שליחת הודעות מייל. | EmailsManager |