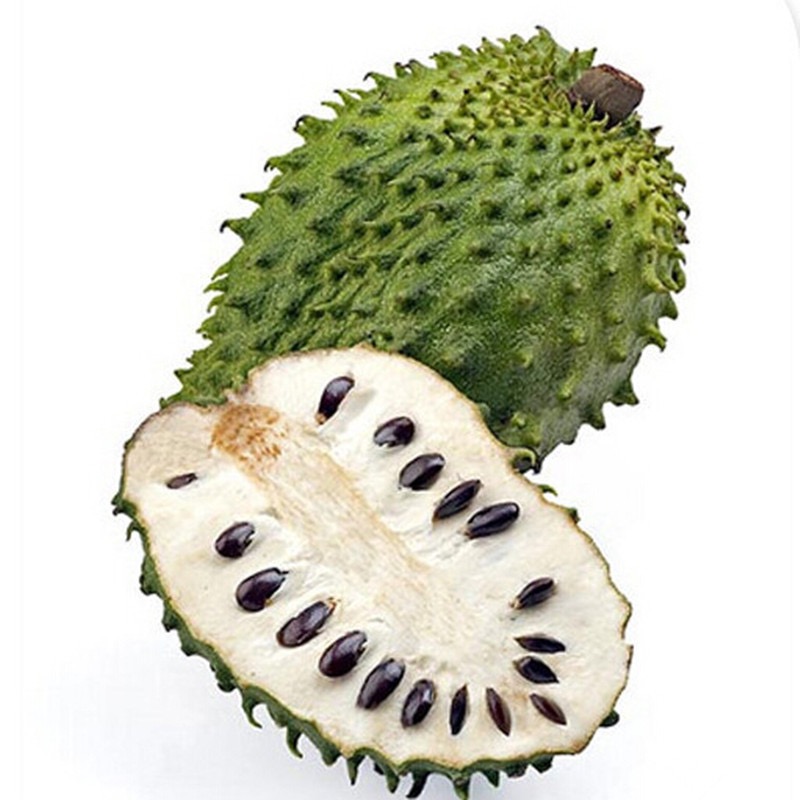
#### ANONA

מסמך עיצוב

גלעד ברק - 209362813

גרסא 1.0

19 ינואר 2017

# הקדמה

### מטרה

מטרתו של מסמך העיצוב היא לסמן את הדרך להצלחת הפרויקט. על המסמך מוטלת האחריות לבטא את מהות הפרויקט והתהליכים המרכזיים שבו לפרטי פרטים. בעזרת מסמך עיצוב מוצלח יוכל המתכנת להביא לידי ביצוע את הפרויקט עם מרווח קטן ככל האפשר מהתכנון המקורי. בנוסף לכך בעזרת יצירת מסמך זה ניתן יהיה למנוע כשלי תכנון שיובילו לבעיות ביצוע עתידיות ותחסוך זמן.

### 1.2 המוצר

שם המוצר: ANONA - Access Naturally Or Neutralize Access

המטרה המרכזית של ANONA היא להגן על עמדת עבודה אישית של משתמש בצורה היעילה ביותר. ANONA מתרכזת ברכיב האנושי של השימוש במערכת, מנתחת את דפוסי ההתנהגות של המשתמש הקבוע של המחשב בתחומים השונים ולומדת אותם. לאחר תקופה מסוימת של למידה תוכל המערכת לזהות כאשר משתמש זר עושה שימוש בעמדת העבודה, ANONA תתריע על כך ובנוסף תנעל את השימוש במחשב.

### מסמך אפיון פרויקט

### 1.3 קישור למסמכים קודמים

* מסמך אפיון

### 1.4 הגדרות

ANONA - - Access Naturally Or Neutralize Access

AI - Artificial Intelligence

עמדת עבודה - תחנת מחשב פרטית של משתמש ממוצע.

משתמש – בעל עמדת עבודה רשום במערכת.

פעילות לא חוקית – פעילות של משתמש זר על עמדת עבודה רשומה במערכת.

# ארכיטקטורת המערכת

### 2.1 מבט על

מודל דגימה – צד לקוח

מודל תקשורת – דו כיווני

מודל בסיס נתונים – צד שרת

מודל למידה – צד שרת

מודל התרעה – צד שרת

### 2.2 פירוט רכיבי המערכת

מודל דגימה – צד לקוח

תפקידו של מודל הדגימה הוא לטפל בלקיחת הדגימות מפעילות המשתמש על עמדת המחשב. האחריות המוטלת על מודל הדגימה היא לבצע הליך דגימה כל פרק זמן מסוים ולגלם את השימוש של המשתמש בעמדת המחשב על כל פרק זמן מסוים כזה בעצם. אותו העצם עתיד להישלח לשרת לצורך למידה ובקרה.

**הסבר:** נקבע שיוגדר מודל המטפל בלקיחת הדגימות מהסיבה הפשוטה שזוהי משימה אותה ניתן להסתיר משאר הפרויקט, משימת צד בכל עמדת מחשב רשומה. מודל הדגימה יושב בצד הלקוח כיוון שהדגימות נלקחות בצד הלקוח.

**מחלקות:**

מחלקת דגימה – עצם המייצג דגימה לאורך פרק זמן מסוים. עצם זה למעשה מגלם בתוכו את פעילות המשתמש לאורך פרק זמן מסוים בתחומים הנדגמים. את עצם זה ישלח הלקוח לשרת לצורכי למידה וניתוח.

מחלקת דוגם – מחלקת פעולות דגימה מעמדת העבודה. המחלקה תגלם בתוכה את כל פעולות הדגימה מעמדת העבודה, על מנת לבצע את הדגימות כל שיהיה לעשות הוא לגשת לפעולה הנמצאת במחלקה ולהפעילה.

מתחילה דגימה חדשה

דוגם מקלדת

דוגם עכבר

דוגם שימוש ברשת

דוגם אפליקציות פתוחות

...

חותמת זמן של דגימה

הדגימה נשלחת לשרת

הדגימה מגולמת בעצם דגימה

מודל תקשורת – דו כיווני

תפקידו של מודל התקשורת הוא לטפל בהעברת המסרים בין הלקוח לשרת ולהיפך. האחריות המוטלת על מודל התקשורת היא לבצע את מעברת הדגימות וההתראות בין הלקוח לשרת ובין השרת ללקוח.

בנוסף יכיל מודל התקשורת סעיף הצפנה ופיענוח של המידע המועבר הלוך חזור מהשרת ללקוח.

**הסבר:** מודל התקשורת הוא דו כיווני כיוון שהוא מגלם את פרוטוקול התקשורת בין השרת ללקוח, אי לכך ובהתאם לזאת עליו להיות נגיש גם ללקוח וגם לשרת.

**מחלקות:**

מחלקת תקשורת צד שרת – פרוטוקול – מחלקה המכילה בתוכה את כל פעולות התקשורת מצד השרת. מגלמת את פרוטוקול ההתקשרות עבור העושה בה שימוש.

מחלקת תקשורת צד לקוח – פרוטוקול – מחלקה המכילה בתוכה את כל פעולות התקשורת מצד הלקוח. מגלמת את פרוטוקול ההתקשרות עבור העושה בה שימוש.

מחלקת הצפנה ופענוח – מחלקה לשימוש של שתי מחלקות הפרוטוקול הקודמות. בעזרת מחלקת ההצפנה והפענוח התקשורת נשמרת מאובטחת. שמורות בה פעולות ההצפנה והפענוח.

צד לקוח

צד שרת

מעבר המידע יתבצע בעזרת פרוטוקולים.

המידע יוצפן, ויפוענח בעזרת מחלקת הצפנה ופענוח.

מודל בסיס נתונים – צד שרת

תפקידו של מודל בסיס הנתונים הוא לנהל את השימוש והשמירה בבסיס הנתונים של דגימות עמדות המחשב השונות שמחוברות לשרת. האחריות המוטלת על מודל בסיס הנתונים היא לבצע את כל הפעולות הקשורות לשמירה או שליפה של מידע מבסיס הנתונים.

**הסבר:** מודל בסיס הנתונים מאחסן את הדגימות שהתקבלו מכל עמדות המחשב המחוברות לשרת, אי לכך ובהתאם לזאת הוא מאוכסן בשרת. בעזרת אחסון של המידע בשרת, נקשה על הגישה למידע, במיוחד כשמדובר במערכת המזהה שימוש לא חוקי בעמדת המחשב (משתמש זר) לא נרצה שתהיה גישה למידע מעמדת המחשב הפרטית.

**מחלקות:**

מחלקת שימוש בבסיס נתונים – מחלקה המכילה בתוכה את כל הפעולות לשמירה ושליפה מבסיס הנתונים. מטפלת בניהול בסיס הנתונים.

שליפת דגימה

מבסיס נתונים

שמירת דגימה חדשה ממשתמש

בסיס נתונים

מודל למידה – צד שרת

תפקידו של מודל הלמידה הוא לבצע את למידת המכונה המנתחת את פרופיל המשתמש ודפוסי השימוש שלו במחשב. האחריות המוטלת על מודל הלמידה היא לשלוף את המידע בכל הנוגע לדגימות מבסיס הנתונים ולבצע את תהליך הלמידה. בנוסף על מודל הלמידה להתריע בפני המערכת כשהזיהוי מספיק לתחילת אבטחה ובנוסף להתריע כאשר הדגימות לא תואמות את ניתוח דפוסי ההתנהגות.

**הסבר:** מודל הלמידה עושה שימוש בבסיס הנתונים, אי לכך ובהתאם לזאת יהיה מאוכסן יחד עם מודל בסיס הנתונים בשרת.

**מחלקות:**

מחלקת מנגנון למידה

מודל התרעה – צד שרת

תפקידו של מודל ההתרעה הוא לקבל החלטות על בסיס התשובות שיחזיר מודל הלמידה. על מודל ההתרעה מוטלת האחריות להביא את ההחלטות של מודל הלמידה לגבי התאמת הדגימה לכדי החלטה האם נעשה שימוש בלתי חוקי בעמדת המחשב. מודל ההתרעה למעשה מווסת את החלטות מודל הלמידה והוא שיתריע בפני המשתמש הרשום שנעשה שימוש לא חוקי בעמדת המחשב שלו.

**הסבר:** מודל ההתרעה מתקשר עם מודל הלמידה ומודיע לבעל עמדת המחשב על פעילות לא חוקית בה. לכן לא נציב את מודל ההתרעה בעמדת המחשב הפרטית מטעמי אבטחה.

**מחלקות:**

מחלקת התרעה – מקבלת תוצאות ממודל הדגימה, יודעת לגלם אותם לכדי החלטה האם להתריע בפני פעילות לא חוקית על עמדת העבודה או לאפשר המשך עבודה כרגיל. בנוסף במחלקה תופיע פעולה השולחת התראה למשתמש במידה ומתקיימת פעילות לא חוקית על עמדת המחשב שלו.

### 2.3 דיון בנושא העיצוב הנבחר

**יתרונות בחלוקת הרכיבים הנבחרת**

* איבטוח מידע: מידע הדגימות לא נשמר על עמדת המשתמש ונשלח לשרת. פורץ עם כוונות זדון לא יהיה יכול לגשת למידע ולשבש אותו. הצפנת המידע תעשה ברמת בסיס הנתונים שנמצא בשרת ולא ברמת עמדת המחשב.
* הפחתת עומס על עמדת המחשב הפרטית: הפעילות המסיבית מתרחשת ברמת השרת ולמעשה על עמדת המחשב הפרטית מתרחשות רק הדגימות עצמן. אי לכך ובהתאם לזאת התוכנה כמעט ולא מורגשת ברמת המשתמש.
* תחזוקה ברמת השרת ולא ברמת המשתמש: תחזוקה של בסיס המשתמש ועדכון תהליך הלמידה תתבצע על השרת ולא על כל תוכנות המשתמשים הפרטיים.

**חסרונות בחלוקת הרכיבים הנבחרת**

* מצריכה חיבור לאינטרנט: במידה ויתנתק החיבור לאינטרנט, לא יישלחו הדגימות ועמדת המחשב לא תיבדק ותילמד.

חלופה לשיטה הנבחרת הייתה להריץ את תהליך הלמידה על עמדת המשתמש הפרטית ובמידה של חריגה לשלוח הודעה לשרת. הוחלט שלא לבצע חלופה זו כיוון ששמירת הדגימות על עמדת המשתמש תצרוך זיכרון רב ומשאבי מחשוב שלא נרצה לדלות מהמחשב הפרטי.

# עיצוב נתונים ופרוטוקולים

### 3.1 בסיס נתונים

בבסיס הנתונים ייבנה בעזרת MongoDB – מודל לניהול בסיס נתונים פשוט ב-Python.

בסיס הנתונים יכיל את כל עמדות המחשב הרשומות למערכת, פרטי המשתמש הנרשם (שם, מספר טלפון, מייל), רשימת דגימות אמת של שימוש המשתמש בעמדה ויומן המכיל את רישום כל הפעילויות החריגות במערכת.

רשימת דגימות האמת תורכב מאובייקטים המגלמים דגימת אמת אשר נשלחו מן העמדה כשהייתה בשלב למידה התחלתית. אל הרשימה יוספו כל הדגימות התואמות אמת שיגיעו מהעמדה הפרטית בהמשך.

### 3.2 פרוטוקולים

**פרוטוקול שיח בין השרת ללקוח**

הרשמה

לקוח – שולח את פרטי המשתמש שנרשם: שם, מספר טלפון, מייל.

שרת – מחזיר הודעת אימות ולאחריה שולח ID של עמדת מחשב ללקוח.

שליחת דגימת אמת

לקוח – מציין בHeader המתאים שמדובר בדגימת אמת. שולח אובייקט (Pickled) המגלם דגימה.

שרת – מחזיר הודעת אימות.

שליחת דגימה כללית

לקוח – מציין בHeader המתאים שמדובר בדגימה שיש לנתח. שולח אובייקט (Pickled) המגלם דגימה.

שרת – מחזיר הודעת אימות.

**Header:** SIGN, SMPT, SMPN, EXIT

**Data:** Parsed based on header. (User Details, Sample, time stamp of log out)

**פרוטוקול שיח התרעת פעילות בלתי חוקית**

במידה והוחלט להודיע על פעילות בלתי חוקית בעמדת מחשב הרשומה למערכת. נשתמש במודל Email של python. ונשלח מייל המכיל את פרטי המשתמש והשעה בה זוהתה הפעילות הבלתי חוקית.

# ממשק משתמש