Azrieli
College of Engineering
Jerusalem
עזריאלי
מכללה אקדמית להנדסה
ירושלים

המחלקה להנדסת תוכנה

פרויקט גמר - תשע"ח

פיתוח מגוון שיטות לזיהוי אנומליות וקבלת החלטות על פי הצבעת הרוב

Developing Variety Of Methods For Identifying Anomalies And Making Decisions According To The Majority Vote

מאת

הדס בן מרדכי 207025412

קארין בנסון 203169792

מנחה אקדמי: דר' גיא לשם	**אישור:**	**תאריך:**
רכז הפרויקטים: מר אסף שפיינר	**אישור:**	**תאריך:**

Ramat Bet Hakerem, P.O.B 3566, Jerusalem 9103501 רמת בית הכרם, ת.ד. 3566, ירושלים מיקוד
Tel. +972-2-6588000 | Fax. +972-2-6588001 | Email: info@jce.ac.il | Web: www.jce.ac.il

מערכות ניהול הפרויקט:

#	מערכת	מיקום
1	מאגר קוד	https://github.com/karinbe/Developing-Variety-Of-Methods-For-Identifying-Anomalies-
2	יומן	https://calendar.google.com/calendar/embed?src=caki4u5vh65nckeb6gos39k8qc%40group.calendar.google.com&ctz=Asia%2FJerusalem
3	ניהול פרויקט (אם בשימוש)	
4	הפצה	

תקציר

"כל המציל נפש אחת, כאילו הציל עולם ומלואו"

במסגרת סגירת התואר של החוג הנדסת תוכנה BS.c ב-"מכללת עזריאלי המכללה להנדסה ירושלים", פרויקט הגמר שלנו יעסוק בפיתוח שיטות לזיהוי אנומליות.

סוגיית האבטחה והניטור, על כל היבטיהם, נהפכו להיות נושא מחקרי חשוב ופופולארי בעולם. זיהוי מצב חריג, בקרב קבוצת נתונים, מעיד כי משהו לא תקין התרחש ויש לעמוד על תיקונו. כמו כן, הרשת הביאה נוחות לעולם בכך שהיא מאפשרת מעבר מהיר של נתונים אך בו במקביל היא חושפת אותנו ומאפשרת לנו להיות פגיעים.

על אף ההתפתחויות הטכנולוגיות והכלים השונים להיענות לבעיה, קשה לקבל כיסוי והגנה מלאה על כל הנתונים שלנו במאה אחוז. בעניין זה, במחקרנו אנחנו מציעות התבוננות עמוקה למודל של גילוי אנומליה, אשר מטרתו למקסם את הפתרון לבעיה תוף מינוף הסיכויים לאיתור מצב חריג, אנומליה, בזמן.

הצהרה

הפרויקט נעשה בהנחיית ד"ר גיא לשם במכללת עזריאלי המכללה להנדסה ירושלים, במחלקה להנדסת תוכנה. החיבור מציג את עבודתנו האישית ומהווה חלק בלתי נפרד מהדרישות לקבלת תואר ראשון בהנדסת תוכנה. העבודה מתבצעת בזוג נוכח היקף העבודה המחקרית הגובלת בנושא וכן מתקיימת חלוקת עבודה.

מילון מונחים, סימונים וקיצורים

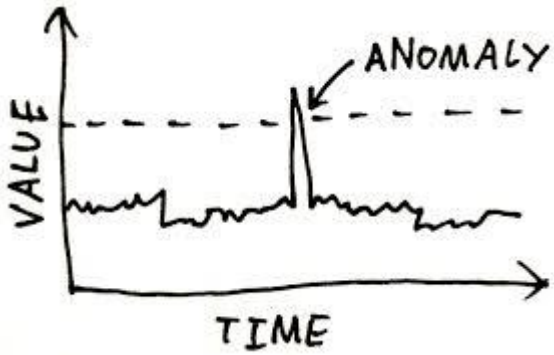
מושגים מעולם אבטחת מידע -

- "מערכות לגילוי פריצות" (Intrusion Detection System) IDS - כאשר המערכת נתקלת בגישה בלתי מורשית, היא יכולה להגיב בסירוב הבקשה. נוסף לכך זה מאפשר "הדלקת נורית אדומה" עבור האדם או הארגון לו שייכת המערכת.
מערכות לאיתור פריצה יכולה להיסוג לשלוש קטגוריות: "מערכות זיהוי חתימה", "מערכות גילוי אנומליות" ו"מערכות היברידיות".

- "מערכות זיהוי חתימה" (Misusebased) - מערכת זו מאתרות התקפות תוך כדי זה שהיא מאמצת לה מסד נתונים משלה אשר מכיל תבניות ספציפיות של אירועים חריגים מוכרים בתעבורה כגון, רצפים ידועים למזימה זדונית. טרמינולוגיה זו מתייחסת לדפוסים אלה כאל חתימות. כאשר מגיעות חבילות, המערכת משווה אותם עם המסד הנתונים הנ"ל ובוחנת האם הוא תקין. היתרון שבשיטה זו הוא שהשיעור החיובי של השגיאות הוא נמוך כאשר מסתמכים על זה שמסד הנתונים הינו אמין. על אף העובדה שמערכת זו יכולה בקלות לזהות התקפות ידועות, הקושי שבה מתבטא בזה שהיא מתקשה לאתר התקפות חדשות.

- "מערכות היברידיות" (Hybrid) - שילוב של "מערכות זיהוי חתימה" ו-"מערכות איתור חדירות המבוססת על אנומליה".

מבוא



אנומליה, או חריגה, פירושה דפוס התנהגות שאינו תואם לאירועים או דפוסים צפויים, כלומר תבנית החורגת מההתנהגות התקינה. קרי, על ידי פעולות ניטור המערכת, על נתונים, ניתן לתאר את המצב כ"נורמלי" ומנגד, בעת חריגה או פגם, כמצב "לא נורמלי" וזוהי למעשה האנומליה.

איתור אנומליה היא סוגיה חשובה בתחומים ומערכות רחבות כללים, ביניהם אבחון רפואי, זיוף זהות ביטוח, חדירה לרשת, פגמים בתכנות ועוד. לדוגמה, זיהוי דפוס תנועה חריג ברשת מחשב עשוי להיות סימן לכך שמחשב פרוץ שולח נתונים רגישים לגורם לא מורשה.
גילוי אנומליה מבוססת לרוב על שיטות של כריית נתונים - הפעלת אלגוריתם או תוכנת מחשב לצורך גילוי מידע הטמון בבסיסי נתונים קיימים, והסקת מסקנות מהצלבתו. בפועל, הדרך הפשוטה לאבחנת חריגות היא להגדיר תחילה התנהגות נורמלית ובעת התקלות בדפוסי נתונים לא צפויים הדבר יצביע על התנהגות בלתי תקינה -חריגה - וזוהי האנומליה.

הדפוסים הלא מתואמים האלה מכונים לעתים קרובות אנומליות, חריגות, חריגים, או הפתעות. טכניקות לזיהוי אנומליה פותחו במספר קהילות מחקר בעולם. חריגות החלו להיחקר כבר החל במאה ה-19 בקהילת הסטטיסטיקה. רבות מהטכניקות שבאו ליישם שיטות לזיהוי אנומליה הללו פותחו במיוחד עבור תחומים מסוימים של יישומים, בעוד שאחרות הן גנריות יותר.

עבור מערכות אבטחה, למשל, שמאמצות שיטות לזיהוי אנומליה, יתרון בולט. בניגוד ל"מערכות מבוססות חתימה", אשר יכולות לזהות רק התקפות שעבורן נוצרה בעבר חתימה, **כאן מתאפשר זיהוי התקפות חדשות.** הסיווג מבוסס על כללים, ולא על דפוסים או על חתימות, ומנסה לאתר כל סוג של שימוש לא נכון הנופל מפעולת המערכת הרגילה.

כמו כן, איתור אנומליות ברשת באמצעות אופי התפלגות התעבורה נעשה יותר ויותר פופולרי על פני חיפוש חריגות בנפח התנועה בתעבורה. הבעיה עם הגישה השנייה נובעת מכך שכיום יש הרבה פעולות חריגות ברשת, כגון סריקה נמוכה של DOS והתפשטות של בוטים כמו תולעת ובהם לא מזהים שינוי של נפח התנועה. כלים אלו מסייעים בעת זיהוי שינויים גדולים ופתאומיים בתעבורה כגון התקפות הצפת רוחב פס, אך עדיין כמות גדולה של אנומליות נותרת בלתי מזוהה.

היבטים שונים של בעיית זיהוי האנומליה

ניסוח ספציפי של הבעיה נקבע על ידי מספר גורמים שונים כגון אופי נתוני הקלט, הזמינות של תוויות והפלט המוחזר.

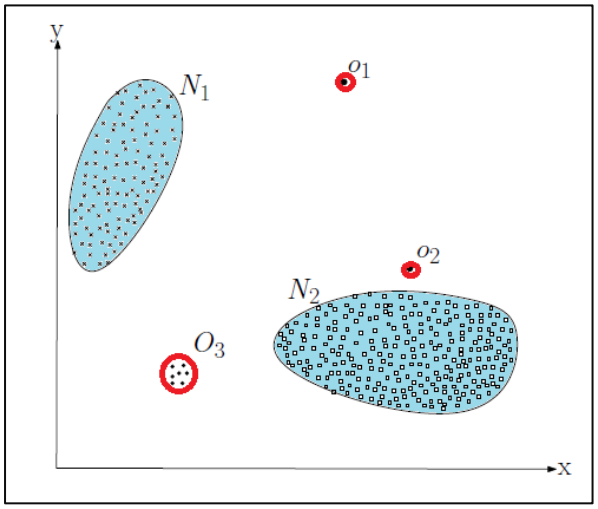
1. <u>נתוני קלט</u>

הקלט הוא בדרך כלל אוסף של מופעי נתונים (אירועים, רשומות, דפוסים , מדגמים, תצפיות, ישויות, אובייקטים). כל מופע יכול להיות מתואר באמצעות קבוצה של תכונות (תכונות, משתנים, מאפיינים). התכונות יכולות להיות מסוגים שונים כגון בינארי, קטגורי או רציף. כל מופע נתונים עשוי לכלול רק תכונה אחת (חד-פעמית) או תכונות מרובות (מרובות משתנים).

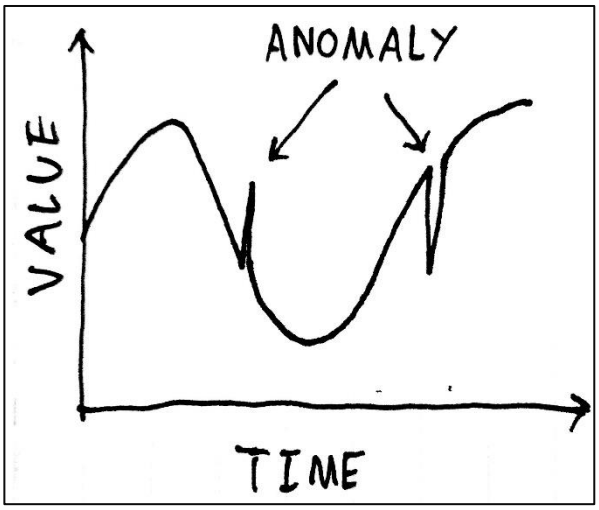
אופי התכונות קובע את הטכניקות לזיהוי האנומליה. לדוגמה, עבור טכניקות סטטיסטיות יש להשתמש במודלים סטטיסטיים לנתונים רציפים וקטגורים.

2. <u>סוג האנומליה</u>

היבט חשוב של טכניקת זיהוי אנומליה היא טבעו של האנומליה הרצויה. אנומליות ניתן לסווג לשלוש קטגוריות הבאות:

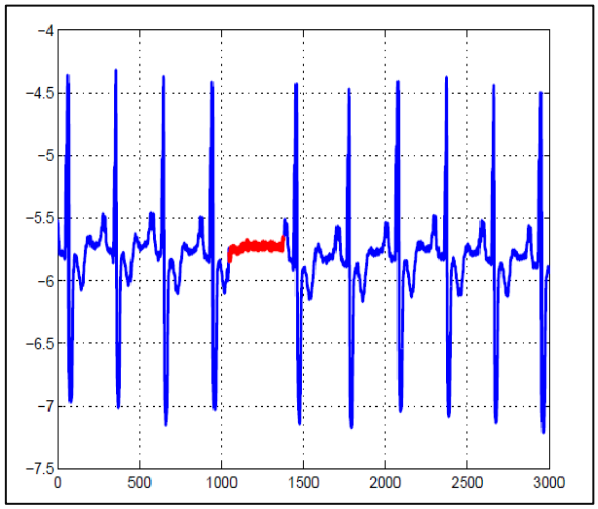


2.2 "נקודות אנומליות" (*POINT ANOMALIES*) - נתונים מבודדים אשר נמצאו כחריגים ביחס לשאר הנתונים, בסביבתם.



2.3 "אנומליית הקשר" (*Contextual Anomalies / Conditional Anomaly*) - מקרה בו מופע נתון נמצא חריג בהקשר ספציפי. כאן, כל תכונה למופע יכולה להיות התנהגותית או הקשרית.

לדוגמה, טמפרטורה של 35 מעלות בחודש אוגוסט הוא מצב שגרתי, אך אם אותה טמפרטורה תהייה גם בחודש חורפי, כגון פברואר, המצב יחשב כחריג.



2.4 "אנומליה קולקטיבית" (*Collective Anomalies*) - חריגה קולקטיבית הינו מצב בו אוסף נתונים מהווה מופע חריג, ביחס לסביבתו. חשוב לציין כי מופעים בודדים בקרב האנומליה הקולקטיבית לא נחשבים חריגים כשלעצמם, אך המופע שלהם יחד הוא חריג.

3. <u>תוויות נתונים</u>

בהתבסס על מידת הזמינות של נתונים, טכניקות זיהוי אנומליה יכולות לפעול בשלושה מצבים: פיקוח, חצי פיקוח וללא פיקוח.

3.1. פיקוח

טכניקות הפועלות במצב מפוקח מניחות את הזמינות של מערך נתוני האימון (training data) שבו המופעים מתויגים כנורמליים או אנומליים. גישה אופיינית במקרים כאלה היא לבנות מודל מנבא עבור מצב נורמלי ומצב של אנומליה, ולאחר מכן משווים כל מופע נתונים שרוצים לבדוק למודל כדי לבדוק האם הוא נורמלי או אנומלי.

ישנן שתי בעיות מרכזיות שעולות בזיהוי אנומליה בפיקוח:

א. בנתוני האימון יש הרבה פחות מופעים אנומליים על פני מופעים נורמליים.

ב. קבלת תווית מדויקת ומייצגת, במיוחד עבור המקרים האנומליים, היא מאתגרת בדרך כלל.

פרט לשני נושאים אלו, בעיית איתור אנומליה במצב מפוקח דומה לבניית מודלים מנבאים.

3.2. חצי פיקוח

טכניקות הפועלות במצב חצי מפוקח מניחות שבמערך נתוני האימון רק המופעים הנורמליים מתויגים כנורמליים ולא מניחות דבר על המופעים האנומליים. מכיוון שמצב זה אינו דורש תוויות עבור מופעים אנומליים, טכניקות כאלה ישימות יותר מאשר טכניקות בפיקוח. לדוגמה, באיתור בעיות בחלל, תאונה הוא תרחיש אנומלי שקשה לבנות לו מודל.

הגישה האופיינית במקרים כאלה היא לבנות מודל לקבוצת ההתנהגות הנורמלית, ולהשתמש במוזל זה כדי לזהות חריגות בנתוני הבדיקה (test data).

קיימת קבוצה מוגבלת של טכניקות זיהוי אנומליה המניחות שבנתוני האימון רק המופעים האנומליים מתויגים כאנומליים; אך טכניקות כאלה אינן נפוצות, בעיקר משום שקשה להשיג מערך נתוני אימון המכסה את כל ההתנהגות החריגה האפשרית בנתונים.

3.3. ללא פיקוח

טכניקות הפועלות במצב ללא פיקוח אינן דורשות נתוני אימון, ולכן הן ישימות ביותר. הטכניקות בקטגוריה זו מתבססות על ההנחה כי מקרים נורמליים שכיחים הרבה יותר מאשר אנומליות בנתוני הבדיקה. אם הנחה זו אינה נכונה, אז טכניקות כאלה סובלות שיעור אזעקות שווא גבוהות.

בענף הרפואה, לרב הנתונים הרפואיים מיוחסים למטופלים בריאים, ולכן רוב הטכניקות המאומצות כאן לצורך ניטור הנתונים יתבצעו בגישת החצי פיקוח.

4. <u>נתוני פלט</u>

היבט חשוב נוסף עבור כל טכניקת זיהוי אנומליה היא האופן שבו התוצאות מדווחות . ככלל, ניתן לסווג את התוצאה של זיהוי האנומליה בשני אופנים :

4.1. ציונים

הקצאת ניקוד בהתאם לרמה בו המופע נחשב אנומליה. לכן התפוקה של טכניקות כאלה היא רשימה מדורגת של אנומליות. אנליסט יכול לבחור לנתח מספר מצומצם של חריגות בולטות או להיעזר במדדי סף לבחינת האנומליה.

4.2. תוויות

הקצאת תווית – נורמלי או אנומליה - לכל מופע מבחן.

במחקרנו, נדון בכלים שניתן להשתמש בהם על-ידי מגיני רשת ומערכי נתונים, לצורך זיהוי אנומליה ברשת. בעניין זה, ניתן התייחסות עמוקה למודל משודרג של גילוי האנומליה עבור לטובת בריאות הציבור.

מבחינת נתונים רפואיים, זיהוי האנומליה נעשה עם רשומות חולה. נתונים יכולים להיות חריגים בשל מספר סיבות כגון מצב חולה חריג, שגיאות מכשור או שגיאות הקלדה. לכן זיהוי אנומליה היא בעיה קריטית מאוד בתחום זה ונדרשת רמה גבוהה של דיוק.

תיאור הבעיה

דרישות ואפיון הבעיה

בעבר, אם נתבונן בהתנהלות ששררה בבתי החולים, כל המסמכים של החולה היו מתויקים תחת מספר דפים עם קליפס צמוד למיטת החולה. הרופא היה מוסיף הערות בכתב יד ובכך היה מסתכם "הדוח של החולה". כיום, בתי החולים עוברים למערכות מיחשוביות, קרי, כל הרשומות הרפואיות של החולה נשמרות ומנוהלות בשרתי המחשוב.

מחד, נפתרה הבעיה של ההתעסקות עם המעמסה ושמירת הרשומות הרפואיות - אין צורך לשמור דברים בארכיונים ולבצע גריסות על מנת להיפטר מדפים מיותרים ובמקרה הגרוע מאמצים שרת נוסף. מאידך, עם המעבר של שמירת המידע על מערכות מחשב נפתח צוהר שלם לעולם אבטחת המידע ובפרט בתחום בריאות הציבור. כלומר, שילוב מכשירים רפואיים, תוכנות, רשתות עם מערכות רפואיות מאתגרות את אופן הניהול וכן את ההגנה הדרושה על מנת לשמור על ביטחון המטופל.

בעת בחינת העדר **מערך אבטחה** ראוי על נתונים רפואיים, המתקיף עשוי לבצע נזק בכמה רמות - החל מחדירה לנתונים אישים, למשל של אישיות מפורסמת אשר מנסה להסתיר את מחלה (אפקט סטרייסנד) ועד לשינוי מינון של תרופה לילד חולה סרטן, או ניסיון פגיעה באדם הצורך תרופות רשומות.

התוקפים הסבירים ביותר לשירותי בריאות ומטרותיהם הינם:

1. אנשים וקבוצות קטנות של האקרים - מונעים בעיקר על ידי רווח ופרסום. לפיכך, הם בדרך כלל בוחרים את מטרותיהם על פי ההזדמנויות.
2. קבוצות פוליטיות ופפראצי - מונעים על ידי אקטיביזם וכן רווח פוליטי ופיננסי. המטרה שלהם בדרך כלל הינה לגרום למבוכה, הכפשה, סחיטה או מכירת מידע על אדם בעל פרופיל גבוה.
3. ארגונים פליליים - מונעים על ידי רווח כספי ופעילות פלילית רחבה יותר כגון סחיטה וכפייה. מטרתם להשיג רשומות רפואיות על האדם הספציפי שהוא המטרה שלהם, לאיים עליהם או לגרום להם נזק פיזי.
4. טרוריסטים - מונעים על ידי השראה של פחד וגורמים נזק. מטרתם היא בדרך כלל לפגוע או לאיים על יחידים.

5. תקיפה מאורגנת מטעם הממשל - האיום הגדול ביותר שעלול להתרחש; מדינות אויב יכולות לכוון לפגוע או לאיים על יחידים.

כמו כן, זיהוי פגמים **בנתונים רפואיים** שלעצמם יכולה לאותת בפני מצב שיש להיערך לקראתו מבחינה רפואית ועל כן חשיבות של זיהוי האנומליה בצורה מדויקת לא פחות חשובה ממערך האבטחה.

הבעיה מבחינת הנדסת תוכנה

הבעיה שלעצמה קיימת וקשה להבטיח פתרון טכנולוגי שיכסה ויתריע מפני כל חריגה אפשרית. **בפועל, כל ארגון או מוסד מאגד לעצמו מערכות לגילוי פריצות המתאפיינות על ידי חוקים ושיטות במטרה להימנע, לזהות ולהגיב בסירוב בקשה בעת היתקלות מצד בקשה של גורם לא מורשה ואף כדי להתמודד עם כשלים בתוך המערכות עצמן.** עם זאת, בעייתי להבטיח כיסוי מלא והענות לכל חריגה בזמן.

מבחינת הנדסת תוכנה, ככל הנראה כעת, הקושי גובל בכתיבת הקוד אשר יבטא את שיטת הפתרון שמחקרנו מעוניין להציג. כמו כן, השאיפה היא להיעזר בתוכנות קיימות, כגון Wireshark , ML in Matlab ועוד.

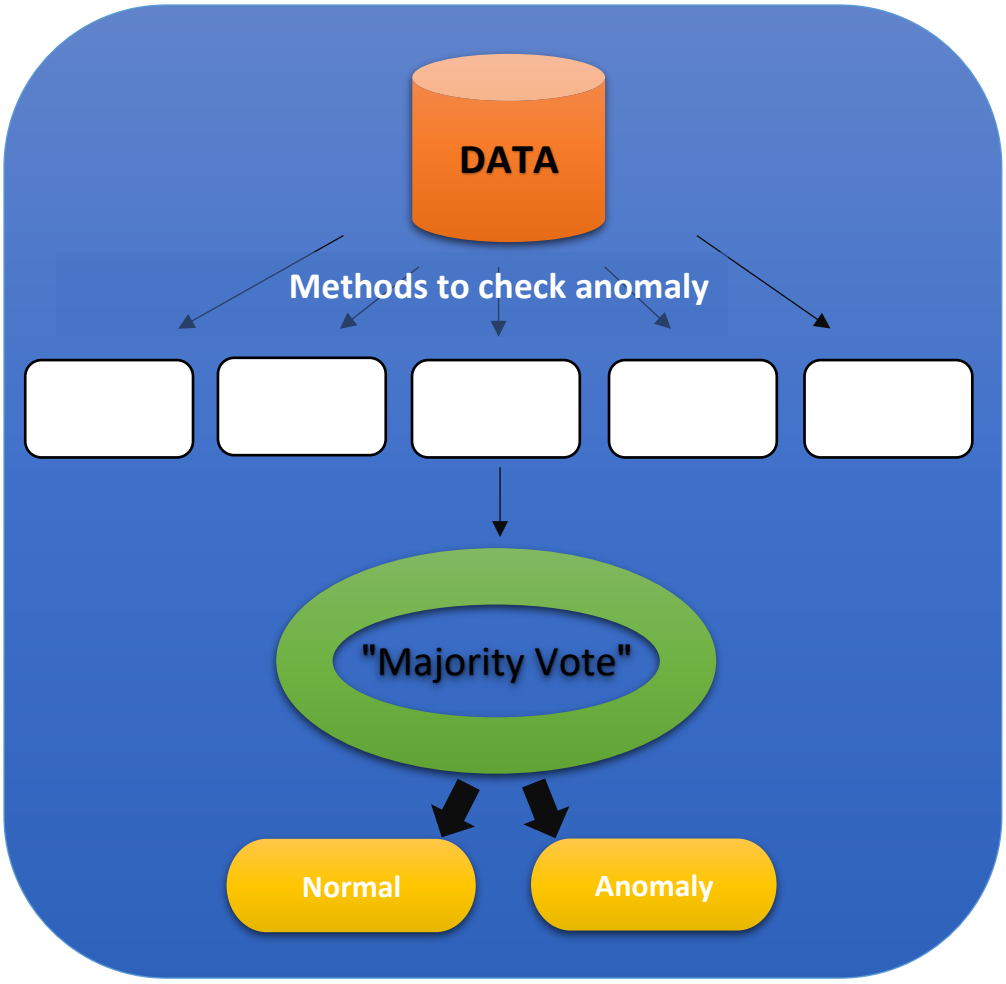
בנוסף לעובדה, שפתרוננו שואף לתת מענה מדויק על וידוא חריגה, עם כריית הנתונים, קושי נוסף עימו אנו עשויים להתמודד הוא מתן המסקנות בזמן מהיר יחסית.

תיאור הפתרון

המחקר שלנו מכוון לתת מענה לזיהוי אנומליה, תוך שיעור גבוהה של הצלחה באיתור חריגות, בפיתוח של מכשירים רפואיים עתידים.

במסגרת חקר הספרות שעשינו, מצאנו שיטות שונות לזיהוי אנומליות. החל משיטות סטטיסטיות ועד שיטות של לוגריתמים ושימוש במכונה.

לפיכך החלטנו כי הפתרון שיוצג במחקרנו יהיה חקירת ואפיון נתונים עליהם נאמץ ונפתח שיטות שונות של זיהוי אנומליות, ננסה למקסם את שימושן על ידי חישובים במידע, אשר טרם אומצו למערכות זיהוי אנומליות במערכות רפואה. הדרך שלנו להגיע לסבירות גבוהה והכרעה על פי שיטת הצבעת הרוב.



השיטות עמן נפעל על מנת לזהות אנומליה יהיו : למפל זיו, אנטרופיה, מכונת למידה (ML).

1. אלגוריתם למפל-זיו (Lempel-Ziv)

אלגוריתם למפל-זיו הינו אלגוריתם לדחיסת נתונים. הצורך לקודד מסר הוא מפני שאנחנו רוצים להתאים את המסר לצורה שניתן לטפל בה (מסר מעובד), לאחסן אותו ולהעביר אותו דרך ערוצי התקשורת.

במשך השנים התפתחו אלגוריתמים שונים על בסיס אלגוריתם למפל-זיו אשר שיפרו את הביצועים בצורה משמעותית והתגבשה משפחה של אלגוריתמים. הדחיסה היא מסוג דחיסה משמרת מידע, המאפשרת שיחזור המידע הדחוס במלואו (ללא עיוות). האלגוריתם מתבסס על חלוקת המחרוזת המקודדת לתתי-מחרוזות הנקראות פסקאות בתהליך המכונה פיסוק. כל פסקה מותאמת למחרוזת מעל א"ב סופי ונבנה מילון בתהליך דינמי. האלגוריתם הוא אוניברסלי, הדחיסה היא אסימפטוטית אופטימלית ולא נדרש ידע קודם של התוכן הנדחס.

למפל-זיו ידוע כאלגוריתם דחיסה אופטימלי, ולכן כדאי להשתמש בו. בהקשר של זיהוי אנומליה, ניתן להגדיר מודל סטטיסטי להתנהגות רגילה ולאחר מכן להציע מנגנון לבדיקת רצפים חדשים ולא ידועים תוך שימוש במודל זה.

אלגוריתם למפל- זיו ככלל ובגרסה LZ78 בפרט הוא שיטת דחיסה המבוססת על מילון: עבור רצף של סדרת סמלים נתונה, מילון של ביטויים מנותח מתוך רצף זה. הניתוח מצטבר כדלקמן - בהתחלה, המילון ריק. לאחר מכן, במהלך כל שלב של האלגוריתם, הקידומת הקטנה ביותר של סמלי נתונים עוקבים שטרם נראו- כלומר שאינה קיימת במילון, מנותחת ומתווספת למילון; לפיכך, כל ביטוי הוא ביטוי ייחודי במילון, אשר עשוי להרחיב ביטוי שנצפה בעבר (ולכן קיים במילון) בסמל אחד. ייצוג נפוץ של המילון הוא עץ מושרש שבו כל ביטוי במילון מיוצג כנתיב מהשורש לצומת פנימי בעץ על פי קבוצת הסמלים מהן הביטוי מורכב.

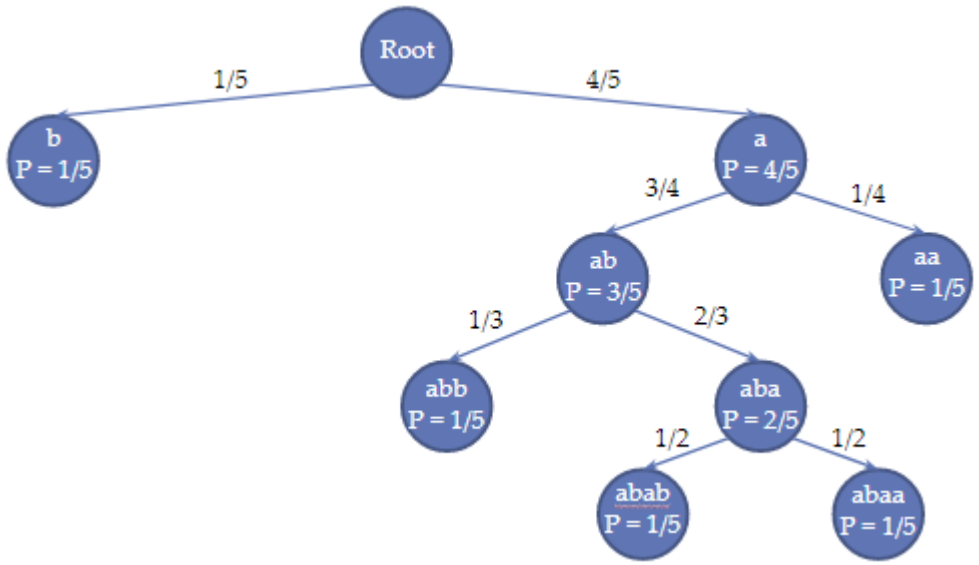
בפרויקט זה, ראשית נמדוד בעזרת התוכנה Wireshark את הזמן שלוקח בין שליחת חבילה לחבילה. לאחר שתהיה לנו רשימת נתונים, נעשה עליהם קוונטיזציה שמטרתה להקטין את טווח הערכים (מתוך כל האלפבית) - נחלק את המספרים לפי תווכים, כאשר כל תווך ייוצג על ידי אות אחרת, ובכך נתרגם את המספרים למחרוזת.

הקלט שלנו יהפוך להיות רצפים של ייצוג אלפבית סופי של נתוני התזמון, כאשר הרוב המכריע של הקלט הינם נתונים נקיים. בניית העץ למפל-זיו: נעבור על אות במחרוזת ונראה אם יש אותה כבר בעץ. אם לא נוסיף אותה לעץ (למילון שלנו), אם כן נסתכל על האות הנוכחית עם האות

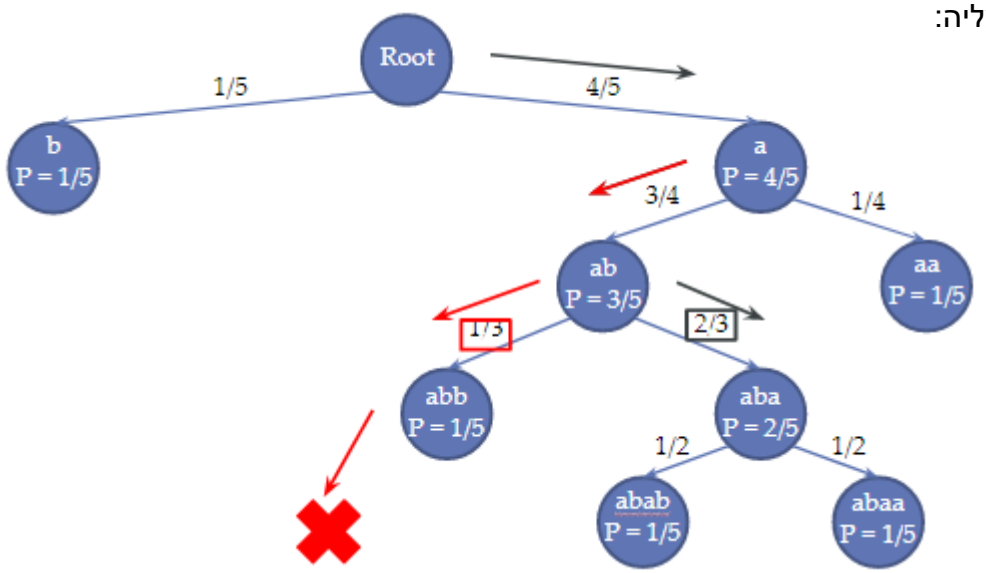
הבאה ונבדוק אם הצמד כבר מופיע בעץ. אם לא נוסיף, אם כן נסתכל על האות הנוכחית עם שתי האותיות העוקבות הבאות אחריה, וכן הלאה. זמן בניית עץ למפל-זיו הינו לינארי, והקצאת ההסתברויות מעט יותר מכך.

הערה: נשים לב כי אלגוריתם הלמידה המבוסס על LZ דורש קלט אלפבית סופי - קיימים שיפורים והצעות כפתרון לבעיה זו, אך אנו לא נעסוק בזה כאן. לאחר בניית העץ, רצפים חדשים (חשודים) ייבדקו על ידי שאילתת ההסתברות שלהם מהעץ בזמן לינארי באורך המחרוזת הנבדקת, וההחלטה תתקבל על בסיס הסתברות זו.

למשל, נניח שלאחר הבנייה קיבלנו את העץ הבא:



בעוד מחרוזות כגון "aab" קיימות בעץ ומוגדרות כנורמליות, המחרוזת "abbb" תאובחן כאנומליה:



2. אנטרופיה (Entropy)

המושג אנטרופיה הינו חלק בלתי נפרד מהחוק השני בתרמודינאמיקה (מונח בעולם הפיזיקה, נקבע כמושג על ידי רודולף קלאוזיוס) העוסק במעברי אנרגיה המניעים את היקום המוכר לנו. הסבר נוסף, המושג אנטרופיה הינו מדד כמותי המייצג את האנרגיה המשתחררת במערכת אשר מורכבת מחלקיקים רבים המייצרים אנרגיה.

החוק השני קובע שבאופן ספונטאני חום זורם מאזור בעל טמפרטורה גבוהה לאזור בעל טמפרטורה נמוכה. על מנת לגרום לחום לזרום בצורה הפוכה יש להשקיע אנרגיה חיצונית. **משמע, אנטרופיה של מערכת לעולם לא תקטן ללא התערבות חיצונית**. בנוסף, היות והחוק השני של התרמודינאמיקה קובע שהאנטרופיה אינה יכולה לקטון באופן ספונטאני, הרי שכל מערכת סגורה (חדר, מדינה, כדוה"א) הולכת ומתפזרת לאורך הזמן. פיזור זה ממשיך עד שהמערכת מגיעה למצב של שיווי משקל-מקסימום אנטרופיה.

דוגמא: החוק השני של התרמודינאמיקה קובע כי בהכנת תה חם, כמות חום מסוימת תעבור מהמים החמים אל שקיק התה ותחמם אותו. נניח שהכוס והשקיק מהווים מערכת סגורה, כלומר לא מושפעים מהעולם החיצוני. בהתאם להגדרת האנטרופיה, אנטרופיית המים תרד (היות וכמות החום המועבר הינה שלילית - חום יוצא מהמים), בעוד אנטרופיית השקיק תעלה מאותה סיבה. אולם, בגלל שטמפרטורת שקיק התה נמוכה מטמפרטורת המים, הרי שהאנטרופיה של השקיק תעלה יותר מאשר ירידת אנטרופיית המים. לכן, באופן כללי אנטרופיית המערכת (המים והשקיק) עלתה. מה שבעצם נוצר הוא שבתהליך ספונטאני (ללא התערבות חיצונית) האנטרופיה של המערכת גדלה.

הסבר נוסף למושג מגיע מתחום הסטטיסטיקה. נטען, כי האנטרופיה היא בעצם תופעה סטטיסטית המבטאת את חוסר הסדר של המערכת. עוד הוכח כי האנטרופיה גדלה ככל שלגוף מסוים יש יותר מצבים סטטיסטיים בו הוא יכול להימצא.

נניח שכוס התה שלנו נשפכת בשל תנועת יד לא זהירה, מולקולות המים שעד עתה היו מוגבלות בדפנות הכוס מגלות המגבלה הוסרה (באופן חלקי או מלא). היות והמולקולות נמצאות במצב של תנועה מתמדת, וכן הן נמצאות תחת פעילותו של כוח הכובד, סביר (סטטיסטית)

שהמולקולות שבתוך הכוס תדחפנה את חברותיהן הקרובות החוצה, אז התה יישפך מה שיגרום לכתם על השטיח ולגידול בחוסר הסדר בחדר.

מסקנה, ככל שמערכות מורכבות יותר כך גם האנטרופיה מורכבת וגבוהה יותר.

כעת נציג פירוש נוסף למושג מתוך עולם האינפורמציה.

האנטרופיה של שאנון

מוגדרת לפי הנוסחה הבאה :

$$H_s(X) = \sum_{i=1}^{n} p(x_i) \log_a \frac{1}{p(x_i)}$$

אנטרופיה כמדד לאי וודאות על קבוצת מצבים אפשריים X בהסתברויות p(X1),.....p(Xn)

קלוד שאנון (מתמטיקאי, מהנדס חשמל וקריפטוגרף אמריקאי, נחשב לאבי תורת האינפורמציה) אימץ את הרעיון של האנטרופיה לעולם האינפורמציה, לפיו האנטרופיה היא מדד לאי-הוודאות הקשורה למשתנה אקראי.

ככל שהמשתנה יותר רנדומלי כך האנטרופיה יותר גדולה ואותו דבר הפוך - ככל שיש לנו יותר מודעות באשר למשתנים כך האנטרופיה יותר קטנה.

המטרה שלנו בשימוש בשיטה זו ובפיתוחים שלה, היא לאמץ אותה ולהתאים אותה לעקרונות האנומליה. כאשר חוסר הוודאות יהיה קטן פרוש הדבר שאנטרופיה קטנה. אם נאמץ את הרעיון למערכת מורכבת וסגורה, כאשר שם יש הערכה לסדר גודל המשתנים, בעת זיהוי אנטרופיה נמוכה, סימן שיש התערבות חיצונית - ומכאן נזהה אנומליה.

3. **למידת מכונה** (Machine Learning)

למידת מכונה, הוא תת תחום מחקרי שכיח למימוש בינה מלאכותית (AI – Artifical Intelligence). AI הוא למעשה תחום מחקר העוסק בדרכים אשר יאפשרו למחשב לבצע פעולות אשר כיום בני אדם מטיבים לבצע באופן שקול יותר. הגדרה שכיחה ומופשטת עבור למידת מכונה - למידת מכונה היא יכולת רכיב מכונה לשפר את הביצועים של עצמה וזאת באמצעות שימוש בתוכנה הכוללת בינה מלאכותית אשר מחקות את הדרך שבה בני אדם לומדים, כדוגמת ניסוי ותהייה. כמו כן, למידת מכונה מתייחסת למחקר, תכנון ופיתוח אלגוריתמים המעניקים למחשב יכולת ללמוד וזאת כשהמחשב טרם תוכנת מראש. תחום זה מציג מספר מתודולוגיות המאפשרות למחשב לבצע משימות אינטליגנטיות בדומה לאדם, כגון חיזוי, זיהוי סיווג והכרה. נוסף על הכישרון שלה להתמקצע ולשפר ביצועים, מטרת למידת המכונה היא גם לזהות ולהתמודד עם פגיעויות אבטחת מידע וכשלים פנים מערכתיים הנובעים מכשל אנושי או קוד, לכל הפחות בזמן הקרוב לזמן אמת.

יכולות AI מציעות פתרונות מעניינים לטובת מענה לתרחישי אבטחה. למעשה קיימים אלגוריתמי למידת מכונה אוטומטיים אשר ביכולתם לקבוע דפוסי "התנהגות נורמלית" על בסיס מקורות ידע ללא התערבות אנושית. חריגה מ"ההתנהגות הנורמלית" מאפשרת גילוי מוקדם של דפוסים אשר יכולים להעיד על ניסיון חדירה, דליפה של מידע או כשל פנימי. כמו כן, עבודה נכונה של למידת מכונה עשויה לצמצם את מערך ה- False Positive Errors וגם את ה- False Negative Errors.

סקירת עבודות דומות בספרות והשוואה

מסקירת ספרות שביצענו, נמצא כי סוגיית זיהוי האנומליה הוא תחום שנימצא בבחינה מתמדת בעשורים האחרונים. האנומליה הוא כלי חזק לאיתור חריגות ואכן יש מגוון שיטות ליישומו. ניתן לסווג את השיטות לפי קטגוריות שונות.

בפרט, מאחר ונתמקצע בענף הרפואה, ניתן להיווכח כי גם שם יש שיטות ייחודיות לאיתור חריגות על נתונים רפואיים.

הטבלה הבאה תמחיש את הקטגוריות לשיטות השונות לזיהוי אנומליות שחקרנו בענף הרפואה.

Categories / Technique Used	ML	Algorithm	Statistics
Bayesian Networks			✓
Neural Networks		✓	
Rule-based Systems:	✓		
Nearest Neighbor based Techniques		✓	
Parametric Statistical Modeling			✓

הייחוד במחקרנו הוא שאנו בוחרים לאמץ כלים ושיטות שונות לזיהוי אנומליות (מעולם הסטטיסטיקה, אלגוריתמיקה ולמידת מכונה) המוכרות בענף האנומליה אך שילובן יחד לצורך מענה לעולם הרפואה (עבודה על נתונים רפואיים) טרם נבחן.

כמו כן, מטרתנו למנף את רמת הדיוק של התוצאות לזיהוי חריגה לפי שיטת הצבעת הרוב, מה שטרם נמצא בשימוש. בנוסף, בשלב של כתיבת הקוד המטרה היא לתת הסקה מהירה של בחינת הנתונים.

נספחים

א. רשימת ספרות \ ביבליוגרפיה

ביבליוגרפיה באנגלית:

- Anomaly Detection : A Survey
https://pdfs.semanticscholar.org/7b5a/c1fb5627addf92ad5804a6569a6cfa9385ac.pdf
- NETWORK ANOMALY DETECTION
https://pdfs.semanticscholar.org/964e/937e50bbcbd97b7d6c7205aa857919faa343.pdf
- Universal Anomaly Detection: Algorithms and Applications
https://arxiv.org/pdf/1508.03687.pdf
- Network Anomaly Detection: Methods, Systems and Tools
http://www.nr2.ufpr.br/~jefferson/pdf/Network_Anomaly_Detection-Methods,_Systems_and_Tools.pdf
http://www.mdpi.com/1099- - An Entropy-Based Network Anomaly Detection Method
4300/17/4/2367/htm
- Compression Algorithms: Huffman and Lempel-Ziv-Welch (LZW)
http://web.mit.edu/6.02/www/s2012/handouts/3.pdf
A Linear Programming Approach to Novelty Detection - http://papers.nips.cc/paper/1822-a-linear-programming-approach-to-novelty-detection.pdf
Cooperative Learning Virtual Reality-Based Visualization for Data Mining -
https://www.researchgate.net/profile/Eric_Paquet2/publication/44052160_Cooperative_Learning_Virtual_Reality-Based_Visualization_for_Data_Mining/links/02e7e5322fea55e8c8000000/Cooperative-Learning-Virtual-Reality-Based-Visualization-for-Data-Mining.pdf
On Abnormality Detection in Spuriously Populated Data Streams -
https://www.researchgate.net/profile/Charu_Aggarwal/publication/220907311_On_Abnormality_Detection_in_Spuriously_Populated_Data_Streams/links/0deec52415b18c0621000000.pdf
HOT SAX: Efficiently Finding the Most Unusual Time Series Subsequence -
http://www.cse.cuhk.edu.hk/~adafu/Pub/icdm05time.pdf
Effect of Outliers and Nonhealthy Individuals on Reference Interval Estimation -
http://clinchem.aaccjnls.org/content/47/12/2137.full
Detection of Outliers in Reference Distributions: Performance of Horn's Algorithm -
http://clinchem.aaccjnls.org/content/51/12/2326.full
DAMAGE DETECTION IN MECHANICAL STRUCTURES USING EXTREME VALUE STATISTICS -
http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-02-1891
Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem - https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/pdf/mder-8-305.pdf
STATE OF CYBERSECURITY & CYBER THREATS IN HEALTHCARE ORGANIZATIONS -
http://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf
Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications -
https://link.springer.com/article/10.1007/s10916-010-9449-4
Contextual anomaly detection framework for big sensor data -
https://journalofbigdata.springeropen.com/articles/10.1186/s40537-014-0011-y

ביבליוגרפיה בעברית:
- למידת מכונה - http://www.digitalwhisper.co.il/files/Zines/0x3B/DW59-1-ML-Security.pdf
- אנטרופיה - מתוך ספר של האוניברסיטה העברית "תורת האינפורמציה"
- אלגוריתם למפל זיו -
https://he.wikipedia.org/wiki/%D7%90%D7%9C%D7%92%D7%95%D7%A8%D7%99%D7%AA%D7%9D_%D7%9C%D7%9E%D7%A4%D7%9C-%D7%96%D7%99%D7%95

ב. תכנון הפרויקט

17.9.17	פגישת היכרות עם המנחה והגעת רעיונות למחקר
16.10.17	מציאת תחום מחקר - אנומליה בתחום הסייבר
9.11.17	מציאת בעיה מחקרית - סייבר במערכות רפואה
-	מציאת מאגר נתונים בענף הרפואה – סכרת
-	הגהת דרך לפתרון הבעיה המוצגת
-	חקירת השיטות המוצעות לזיהוי אנומליה
-	אימוץ השיטות והתאמתן למאגר הנתונים שברשותנו
-	קוד למימוש השיטות שחקרנו

-	הצלבת נתונים אל מול השיטות
-	הסקת מסקנות
-	הגשת מצע מחקרי

ג. טבלת סיכונים

#	הסיכון	חומרה	מענה אפשרי
1	קושי במציאת שיטות לזיהוי אנומליה	High	התייעצות עם גורם בקיא בנושא, שינוי שיטות מוכרות לצרכי המחקר
2	למידה של שימוש בכלי Wireshark	High	למידה עצמית
3	קושי בהצלבת הנתונים אל מול השיטות המוצעות לזיהוי אנומליה	High	בחינת השיטות והתאמתן למאגר הנתונים שברשותנו, ייעוץ עם איש מקצוע
4	העדר ידע של סביבת ניהול מאגרי נתונים בענף הרפואה	Medium	ייעוץ עם המנחה ושימוש במנוע החיפוש של האינטרנט והספרות
5	קושי במציאת מאגרי נתונים גולמיים לפרויקט	Medium	ייעוץ עם המנחה ושימוש במנוע החיפוש של האינטרנט והספרות

6	כתיבת קוד בשפת תכנות לא מוכרת	Medium	למידה עצמית
7	קושי במציאת ידע אודות שיטות לזיהוי פריצות במערכות הרפואה	Medium	שינוי ההתמקדות של האנומליה במחקרנו
8	הערכה שגוייה של פריסת היקף המחקר	Low	בקרה מתמדת והגדרת דרישות ולוח זמנים ראלי
9	תחרות - מחקר דומה שנערך בו זמנית	Low	התייעצות עם המנחה וכן מעקב אחר ההתקדמות של המתחרה הפוטנציאלי וזירוז ניהול הפרויקט בבית

ד. רשימת דרישות

בפרויקט זה אנו שואפות לפתח שיטות שונות לזיהוי אנומליה לצרכי אבטחה ותקינות נתונים אשר מיועדות לשרת בעיקר את מערכת בריאות הציבור. השיטה המוצעת אצלנו שואפת למקסם יכולות מוכרות ולהגיע להיסקים מדויקים על פי הצבעת הרוב.