

2023

סמינר מסכם

IoT & Cyber Security

מנחה אקדמי: פרופ' רותי גפני

מנחה מקצועי: מר ג'וש בכר

מגישים:

אמרי עוזרי - 204469936

דניאל סולטן - 208611020

גיא ארביב - 208542332

תוכן עניינים

3	תקציר
4	מבוא
5	סקירת ספרות
9	מטרת המחקר
9	שאלת המחקר הראשית :
9	שאלות ממוקדות :
9	הגדרה נומינלית של המשתנים
10	השערות המחקר
11	שיטות מחקר
11	ניתוח מאגרים :
14	Benchmarking :
17	ממצאים
17	ניתוח מאגרים :
17	שאלה ממוקדת 1
19	שאלה ממוקדת 3
20	Benchmarking :
20	שאלה ממוקדת 1 :
20	שאלה ממוקדת 2 :
21	שאלה ממוקדת 4 :
25	דיון ומסקנות
25	שאלה ממוקדת 1
25	שאלה ממוקדת 2
26	שאלה ממוקדת 3
27	שאלה ממוקדת 4
27	מסקנות והמלצות
28	מגבלות המחקר והמלצות להמשך
29	מקורות
32	נספחים
32	נספח א' – מבחן ספירמן (עבור שאלה ממוקדת 1)
32	נספח ב' – ממצאים תיאוריים – סוגי חולשות אל מול רמת חומרה (baseScore)

33.....	נספח ג' – מבחני חי-בריבוע וערכי מתאים קרמר
33.....	1. המשתנה Type לעומת המשתנה confidentialityImpact
33.....	2. המשתנה Type לעומת המשתנה integrityImpact
34.....	3. המשתנה Type לעומת המשתנה availabilityImpact
34.....	4. המשתנה Type לעומת המשתנה attackVector
35.....	5. המשתנה Type לעומת המשתנה attackComplexity
35.....	6. המשתנה Type לעומת המשתנה privilegesRequired
36.....	7. המשתנה Type לעומת המשתנה userInteraction
36.....	8. המשתנה Type לעומת המשתנה scope
37.....	נספח ד' – Benchmarking Scoring
38.....	נספח ה' – הצעת עבודה
45.....	נספח ו' – תכנית העבודה
54.....	נספח ז' – טבלת המשאבים
55.....	נספח ח' – הצהרה על הסכמה לפרסום העבודה
56.....	נספח ט' – הצהרות על הכנה עצמית של העבודה

תקציר

מטרת המחקר	<p>מטרתו של סמינר זה היא לחקור את ההשפעה של שילוב כלי IoT על רמת האבטחה במערכות מידע ארגוניות בחמש השנים האחרונות. המחקר חוקר מהן החולשות הנפוצות בקרב רכיבי IoT בחמש שנים האחרונות, שיטות עבודה מומלצות הקשורות לאבטחת מכשירי IoT, איתור ובחינה של מכנים משותפים בין החולשות הנפוצות והבנה מעמיקה יותר אודות חשיבות ותדירות הורדה של עדכונים ברכיבי IoT.</p>
רקע	<p>האימוץ הנרחב של טכנולוגיית IoT העלה חששות לגבי אבטחת מערכות המידע הארגוניות. ככל שכלי IoT משתלבים יותר ויותר, חיוני להבין את הפגיעויות שהם עשויים להציף ולזהות אמצעי אבטחה יעילים להפחתת סיכונים.</p>
שיטות המחקר	<p>לכל שיטת מחקר בה נעשה שימוש במחקר זה: המערך, השיטה, האוכלוסיה שנדגמה וגודל המדגם (עבור מערך מתאמי) או המניפולציה (עבור מערך ניסויי)</p> <p>המחקר משתמש בשיטות עיקריות, ניתוח מסדי נתונים וניתוח השוואתי (Benchmarking).</p> <ul style="list-style-type: none"> - ניתוח מסד הנתונים, מערך מחקר מתאמי אשר כולל חילוץ מידע ממסד הנתונים VARIOT, אשר מכיל מידע רב אודות תיעוד וניתוח פגיעויות ברכיבי IoT בחינת נקודות תורפה והערכת חומרתן. לאורך המחקר בחרנו להתמקד בנתונים מחמש השנים האחרונות ובשבעת החולשות השכיחות ביותר במאגר. מדגם זה כ- 3452 רשומות. - ניתוח השוואתי, מערך מחקר מתאמי, אשר כלל השוואת 4 מכשירי IoT פופולריים מהיצרניות המובילות: Apple Siri, Amazon Alexa, Google Home, Samsung Bixby על סמך פרמטרים מוגדרים מראש לטובת מדידת רמות האבטחה שלהם וע"פ מגוון מאפיינים.
ממצאים	<p>המחקר חושף את שבעת החולשות הנפוצות ביותר ברכיבי IoT ואת רמת חומרתן, בין חולשות אלו: Buffer Error, XSS, Input Validation Error, Information Disclosure ועוד. לצד חולשות אלו, המחקר מצא כי ישנו מכנה משותף מובהק ע"פ המאפיינים לפיהם מדדנו. מאפיינים אלו, הם אלו שמקנים לחולשות הללו את מעעמדיהם הבולט. כמו כן, המחקר העלה שיטות עבודה מומלצות עבור אבטחת התקני IoT שכוללים הטמעת מנגנוני אימות חזקים, הצפנת שידורי נתונים והקמת מדיניות אבטחה ברורה. בנוסף, המחקר הציף כי עדכוני תוכנה ושמירה על תוכנה מעודכנת חיוניים כדי למזער את הפגיעות של מערכות המידע הארגוניות ובאפשרותן לעלות משמעותית את רמת האבטחה.</p>
מסקנות	<p>שילוב כלי IoT במערכות מידע ארגוניות מצריך התייחסות מדוקדקת של השלכות אבטחה. על ידי יישום נוהלי אבטחה מומלצים, ארגונים יכולים לשפר את רמת האבטחה שלהם ולהפחית סיכונים פוטנציאליים הקשורים באינטגרציה של IoT.</p>
תרומת המחקר	<p>מחקר זה תורם להבנת אתגרי אבטחה הקשורים ל-IoT ומספק המלצות מעשיות לארגונים, חוקרים ובעלי עניין. הממצאים יכולים לסייע לארגונים בשיפור אבטחת מערכות המידע שלהם, שמירה על נתונים רגישים והפחתת הסיכון להתקפות סייבר. יתרה מזאת, המחקר מדגיש את החשיבות של שיתוף פעולה ואמצעים יזומים לטיפול בפגיעויות IoT ביעילות.</p>
מילות מפתח	<p>Internet of Things (IoT), Security, Vulnerabilities, Cyber Security</p>

מבוא

במהלך העשור האחרון, מתרחב מאוד השימוש בחיבור של מוצרי חומרה (מצלמות אבטחה, בקרים, שערים, דלתות, מסכים, מדפסות, מקררים, ועוד) לאינטרנט (Internet of Things) בארגונים בכלל ובחיי היום יום שלנו בפרט (Alfthan et al., 2019). זהו תהליך שגדל במהירות (אנו מאמינים כי הרחבת פריסת רשתות הסלולר מהדור החמישי בשילוב יכולות אינטליגנציה מלאכותית לניהול עצמאי תוביל להגדלה משמעותית בחיבור מוצרי חומרה רבים נוספים לאינטרנט), ומציעה יתרונות רבים כמו הגברת היעילות, הפרודוקטיביות בעזרת תפעול מרוחק וממוחשב של מוצרי חומרה ומאפשרת איסוף נתונים בסדרי גודל וקצבים שלא היו כמותם. כמו כן, היכולת לאסוף ולנתח כמויות אדירות של מידע ממכשירים מחוברים השפיעה באופן משמעותי על מגוון רחב של מודלים עסקיים ויצרה כיווני חשיבה ופעולה שטרם נראו. בסך הכל, IoT אפשר לחברות לשנות את המודלים העסקיים שלהן על ידי מינוף נתונים ואוטומציה ליצירת הצעות ערך חדשות, שיפור היעילות ויצירת מקורות הכנסה חדשים. עם זאת, ריבוי זה של מכשירי IoT רכיבים אשר לרוב בעלי תוכנה/חומרה מוגבלים, המחוברים לאינטרנט, העלה גם חששות לגבי אבטחת הארגונים המשתמשים בהם. וייתכן כי אינטגרציה זו תוביל גם לעלייה בסיכוני האבטחה עקב נקודות התורפה של מכשירי IoT.

ככל שארגונים מרחיבים את השימוש בכלי IoT בפעילותם, חשוב להבין את ההשפעה שיש לשילוב זה על רמת האבטחה בתוך הארגון. ארגונים המשלבים כלי IoT מתמודדים עם איומים מהתקפות סייבר, פרצות מידע ופעילויות זדוניות אחרות שעלולות לסכן את פעילותם (Pan & Yang, 2018). לכן, הצורך באבטחת מכשירי IoT הפך מכריע בהבטחת בטיחות הנכסים הארגוניים ובשמירה על מערכת יחסים אמינה עם הלקוחות.

מחקר זה נועד לחקור את ההשפעה של שילוב כלי IoT על רמת האבטחה והחשיפה של ארגון בחמש השנים האחרונות. באופן ספציפי, במחקר התמקדנו בזיהוי סוגי החולשות הנפוצות ביותר הקיימות ברכיבי IoT, וביקשנו לזהות את השיטות המומלצות לאבטחת מכשירי IoT, וכיצד ארגונים יכולים ליישם שיטות אלו כדי להפחית סיכוני אבטחה.

על מנת להשיג יעדים אלו, לאורך המחקר ניתחנו את הספרות הקיימת בנושא אבטחת מידע בכלל ואבטחת IoT בפרט, לרבות מאמרים אקדמיים, מאמרי מדיניות, דוחות תעשייה ואתרים ממשלתיים של גופי סייבר ומחקר.

כמו כן, לצד המחקר הספרותי המעמיק, **ערכנו ניתוח מקיף של מאגר המידע VaRIoT - פרויקט מחקר במימון האיחוד האירופי שמטרתו לשפר את האבטחה של מכשירי ורשתות IoT** (VaRIoT Vulnerabilities. n.d.) המאגר מכיל כמויות עצומות של מידע אודות חולשות ברכיבי IoT החולשות בהן, עדכוני אבטחה, הסיכונים והפגיעויות הפוטנציאליים הקשורים למכשירי IoT, חומרת התקיפה, ועוד מגוון רחב של פרטים ושדות אותם ננתח לטובת קיום של אנליזות מתקדמות והסקת מסקנות.

בנוסף, **קיימנו ניתוח השוואתי בין כמה רכיבי חומרה אשר להם תכלית זהה, ועמדנו על ההבדלים ביניהם וכיצד השוני ברכיבים משפיע על רמת אבטחת המידע של הרכיב ומכאן כיצד ישפיע על רמת האבטחה בארגון בו ישולב.**

לבסוף, אנו שואפים כי **מחקר זה יתרום להבנה טובה יותר של סיכוני האבטחה** איתם מתמודדים ארגונים בעת שילוב מכשירי IoT ויספק הדרכה כיצד ארגונים יכולים לצמצם סיכונים אלו. על ידי זיהוי החולשות והפגיעויות הקיימות ברכיבי IoT והמלצה על שיטות עבודה מומלצות לאבטחת מכשירים אלו, מחקר זה יסייע לארגונים לקבל החלטות מושכלות לגבי השימוש במכשירי IoT בפעילותם.

סקירת ספרות

השילוב של מכשירי IoT (Internet of Things) הפך נפוץ יותר ויותר בארגונים ונחשב למהפכה טכנולוגית של ממש ומספק יתרונות רבים, כמו הגברת היעילות והפרודוקטיביות, בין אם בארגונים וחברות גדולות ובין אם בהתנהלות היום יומית שלנו כפרטים (Alfrhan, et al., 2019).

IoT מחולל מהפכה באופן שבו אנו מתקשרים עם העולם שסביבנו. והפך להיות חלק אינטגרלי בחיי היומיום שלנו ובאורח החיים שאנו מסגלים לעצמו בסביבה כה מתקדמת, עם מגוון רחב של מכשירים וחיישנים המחוברים לאינטרנט, מבתי חכמים, ציוד לבוש ומכונות אוטונומיות אשר משמים כל אחד ואחד מאיתנו ביום יום, ועד לאוטומציה תעשייתית ושירותי בריאות, טכנולוגיית ה-IoT משנה תעשיות ומשנה את הדרך בה אנו חיים ועובדים (Khalid & Ameen., 2021).

בעוד שטכנולוגיית ה-IoT מציעה יתרונות רבים, כולל שיפור ביעילות ונוחות, היא גם מציבה אתגרי אבטחה משמעותיים. עם השילוב של מכשירי IoT, ארגונים מתמודדים עם סיכוני אבטחה רבים, והבטחת האבטחה של מכשירים אלו הפכה לדאגה מרכזית (Pan & Yang, 2018). סקירת ספרות זו שואפת לשפוך מעט אור אודות ההשפעה של שילוב כלי IoT על רמת האבטחה בארגונים, לרבות הסוגים הנפוצים ביותר של חולשות ברכיבי IoT והשיטות המומלצות לאבטחת מכשירים אלו תוך התמקדות בחמש השנים האחרונות. באמצעות ניתוח מקיף של מחקרים קיימים, מאגרי מידע והשוואה בין רכיבים שונים ע"פ פרמטרים שנקבע, אנו מקווים לספק תובנות לגבי המצב הנוכחי של אבטחת מכשירי ה-IoT ולזהות אזורים למחקר ופיתוח נוספים.

רכיבי IoT הם מכשירים פיזיים המחוברים לאינטרנט ויכולים להחליף נתונים עם מכשירים או יישומים אחרים. מכשירים אלה יכולים לנוע מחיישנים פשוטים ועד למערכות מורכבות כמו בתים חכמים, מכשירי בריאות ומכונות תעשייתיות. רכיבי IoT כוללים בדרך כלל חומרה, תוכנה ופרוטוקולי תקשורת המאפשרים חילופי נתונים בין מכשירים.

Internet of Things (IoT) מתייחס לקונספט של רשת של מכשירים פיזיים, כלי רכב, מכשירי חשמל וחפצים אחרים המוטבעים בחיישנים, תוכנות וקישוריות, המאפשרים להם לאסוף ולהחליף נתונים דרך האינטרנט (Khalid & Ameen., 2021). מכשירי IoT מחוברים בדרך כלל לאינטרנט ולהתקנים אחרים באמצעות רשתות אלחוטיות או קוויות, והם יכולים לתקשר זה עם זה כדי להחליף מידע ולבצע משימות שונות.

רכיבי IoT יכולים להתייחס לאלמנטים הפיזיים והתוכנה השונים המרכיבים מערכת IoT. מכשירים אלה יכולים לנוע מחיישנים פשוטים ועד למערכות מורכבות כמו בתים חכמים, מכשירי בריאות ומכונות תעשייתיות. רכיבי IoT כוללים בדרך כלל חומרה, תוכנה ופרוטוקולי תקשורת המאפשרים חילופי נתונים בין מכשירים. רכיבים אלה כוללים חיישנים, מפעילים, מיקרו-בקרים, פרוטוקולי תקשורת, פלטפורמות ענן ויישומים. חיישנים אלו, מכשירים שמזהים ומודדים שינויים

בסביבה, כגון טמפרטורה, לחץ ותנועה, בעוד שמפעילים הם מכשירים שניתן להשתמש בהם כדי לשלוט במערכות פיזיות, כגון מנועים ושסתומים. מיקרו-בקרים הם מחשבים קטנים המשמשים לשליטה וניהול פעולתם של מכשירי IoT, בעוד פרוטוקולי תקשורת הם הכללים השולטים כיצד מכשירים מתקשרים זה עם זה ברשתות. פלטפורמות ענן מספקות יכולות אחסון ועיבוד של נתוני IoT, ויישומים מאפשרים למשתמשים ליצור אינטראקציה עם מכשירי IoT ולשלוט בהם. יחד, רכיבים אלה פועלים יחד כדי ליצור מערכת מורכבת ומקושרת של התקני IoT שניתן להשתמש בהם כדי לאסוף, לנתח ולפעול על פי נתונים (Farooq et al., 2015).

טרם נעסוק באבטחת המידע בהקשר של שילובם של כלי IoT, עלינו קודם להבין מהי בכלל אבטחת מידע ומדוע מהווה פקטור כל כך משמעותי בחייו של ארגון בכלל או בחיינו כפרטים בפרט. **אבטחה בארגון מתייחסת לאמצעים הננקטים כדי להגן על הסודיות, השלמות והזמינות של נכסיו.** אבטחה בארגון מתייחסת לאמצעים הננקטים כדי להגן על נכסי הארגון, לרבות משאביו הפיזיים והדיגיטליים, מפני גישה לא מורשית, גניבה, נזק או סוגים אחרים של פגיעה. זה כולל הגנה על הקניין הרוחני של הארגון, מידע פיננסי, נתוני לקוחות ומידע רגיש אחר מפני התקפות סייבר, פרצות מידע ואיומי אבטחה אחרים.

אבטחה ארגונית כוללת בדרך כלל שילוב של בקורות פיזיות, מנהליות וטכניות שנועדו להגן על נכסי הארגון. בקורות פיזיות כוללות אמצעים כגון מנעולים, מצלמות אבטחה ובקורות גישה, בעוד שבקורות מנהליות כוללות מדיניות ונהלים לניהול סיכונים אבטחה, כגון הדרכת עובדים ותוכניות מודעות לאבטחה. בקורות טכניות כוללות טכנולוגיות כגון חומות אש, מערכות זיהוי פריצות והצפנה המשמשות להגנה על הנכסים הדיגיטליים של הארגון (Boeckl et al., 2019).

לאחר שהגדרנו מהי אבטחה וכיצד מיישמים אותה, נשאלת השאלה כיצד ניתן למדוד אותה ואת רמת החוזק שלה. **לשאלה זו אין תשובה חד משמעית, והיא מגלמת בתוכה מגוון רחב של שיטות, טכניקות וגישות שתכליתן לתת הערכה או ציון מסויימים לרמת האבטחה בארגון, בין היתר:** הערכת סיכונים שכוללת זיהוי סיכונים פוטנציאליים לאבטחת הארגון והערכת הסבירות וההשפעה של סיכונים אלה, הערכת אבטחה בקרב עובדי הארגון - Capability Maturity Model Integration (CMMI) או תקן ISO/IEC 27001, בדיקות חדירה - כולל הדמיית התקפה אמיתית על מערכות הארגון כדי לזהות נקודות תורפה וחולשות בהגנות האבטחה, ועוד.

בהקשר של אבטחת מידע, **Vulnerabilities & Exploits הם שני מושגים קשורים הקריטיים להבנת האבטחה של מכשירי ורשתות IoT.**

Vulnerability היא חולשה במערכת או ביישום שניתן לנצל כדי לפגוע באבטחת המערכת. Vulnerability יכולות להיגרם ממגוון גורמים, כולל שגיאות תכנות, טעויות תצורה או פגמי עיצוב. סוגים נפוצים של פגיעויות כוללים הצפת מאגר, הזרקת SQL, סקריפטים בין-אתרים (XSS) ותקשורת לא מאובטחת (Naudé et al., 2009).

Exploits הם כלים או טכניקות המשמשות לניצול Vulnerability במערכת. Exploits יכול לשמש כדי לקבל גישה לא מורשית למערכת, לגנוב נתונים רגישים או להפעיל סוגים אחרים של התקפות. Exploit יכול ללבוש צורות רבות, כולל קוד זדוני המנצל Vulnerability, טכניקות הנדסה חברתית שמרמות משתמשים לחשוף מידע רגיש, או התקפות כוח גסות המשתמשות בכלים אוטומטיים כדי לנחש סיסמאות או אישורי אימות אחרים (Nayak et al., 2014).

הגורמים ל-Vulnerabilities ול-Exploits מגוונים ומורכבים. גורם אחד שיכול לתרום ל Vulnerability הוא השימוש בתוכנה או חומרה מיושנת או לא מאובטחת. מכשירי IoT רבים פועלים על מערכות הפעלה או קושחה מיושנות או לא מעודכנות, שיכולות להכיל Vulnerabilities ידועים שיכולים להיות מנוצלים על ידי תוקפים. בנוסף, המורכבות של מערכות ורשתות IoT עשויה להקשות על אבטחתם, מכיוון שעשויים להיות הרבה מכשירים, פרוטוקולים וממשקים לניהול (Knapp et al., 2009).

גורם נוסף שיכול לתרום להיווצרותה של Vulnerability הוא היעדר הכשרה או מודעות לאבטחה בקרב משתמשים ומפתחים. מכשירי IoT רבים מתוכננים מתוך מחשבה על קלות שימוש, מה שעלול להוביל להתעלמות או התעלמות מהאבטחה. בנוסף, ייתכן שלמפתחים אין את המומחיות האבטחה הדרושה לבניית מכשירי IoT מאובטחים, מה שעלול לגרום להכנסת נקודות תורפה למערכת (פלאח, א., 2018).

ארגונים חייבים לנקוט בגישה פרואקטיבית לאבטחה, תוך הטמעת מגוון אמצעי אבטחה, כולל עדכוני תוכנה שוטפים, בדיקות חדירה וחינוך והכשרת משתמשים, כדי להפחית את הסיכון לניצול פגיעויות.

רמת החומרה של Vulnerability או Exploit נקבעת בדרך כלל על סמך שילוב של גורמים, כולל הסבירות להתרחשות ניצול וההשפעה הפוטנציאלית של ניצול על המערכת או הארגון וההשפעה הפוטנציאלית על הסודיות, השלמות והזמינות של המערכת או הנתונים המושפעים. רמות חומרה יכולות להיות מסווגות כנמוכות, בינוניות, גבוהות או קריטיות, בהתאם לרמת הסיכון הנשקפת מהחולשה. דוגמא למסגרת בשימוש נרחב להערכת חומרת הפגיעות היא מערכת הניקוד הנפוץ של פגיעות (CVSS). ה-CVSS מקצה ציון לפגיעויות על סמך מספר גורמים, כולל מורכבות ההתקפה, רמת ההרשאות הנדרשות לניצול הפגיעות וההשפעה הפוטנציאלית על סודיות, שלמות וזמינות המערכת. הציונים משמשים לאחר מכן להקצאת רמת חומרה, הנעה בין נמוך לקריטי (Holm, Ekstedt, & Andersson, 2005).

בתוך עולם אבטחת המידע שהוא עצום, מוקצה גם תחום ייעודי אשר עוסק ביישום שיטות אבטחה למכשירי IoT ומתי נכון להוריד גרסה ועדכונים (S. H. Li, & Tryfonas, 2016).

ישנן מספר שיטות לאבטחת התקני IoT, כולל אימות, הצפנה, בקרת גישה וניטור. אימות מבטיח שרק משתמשים או מכשירים מורשים יכולים לגשת למערכת. הצפנה עוזרת להגן על נתונים מפני יירוט או שינוי במהלך השידור. בקרת גישה מגבילה את ההרשאות של משתמשים או מכשירים על סמך תפקידם או רמת הסמכות שלהם. ניטור מאפשר זיהוי ותגובה לאירועי אבטחה.

כדי להפחית את סיכוני האבטחה, ארגונים צריכים להבטיח שהם שומרים על מכשירי ה-IoT שלהם מעודכנים עם הגרסאות והתיקונים העדכניים ביותר ומקפידים על תהליכי פיתוח והטמעה מחמירים. מכשירי IoT מועדים לפגיעויות שיכולות להיות מנוצלות על ידי תוקפים, ועדכון הקושחה או התוכנה יכול לעזור לטפל בפרצות אלו (Fagan et al., 2020).

אל מול רמת האבטחה של רכיבי IoT והחולשות הקיימות, נראה כי המכנה המשותף בין רכיבי IoT לחולשות אלו הוא חוסר האבטחה המובנה במכשירים עצמם. מכשירי IoT מתוכננים לעתים קרובות תוך מחשבה על פונקציונליות ועלות, כאשר האבטחה היא מחשבה שלאחר מכן, בדיעבד.

משמעות הדבר היא שלמכשירי IoT רבים יש פגיעויות מובנות שניתן לנצל על ידי תוקפים (Nadir et al., 2022).

בתוך כך, סיכון נוסף הוא אפשרות של פרצות מידע, שעלולות להתרחש כאשר נעשה שימוש במכשירי IoT להעברת מידע רגיש. לדוגמה, מכשיר רפואי מחובר עלול להיפגע, וכתוצאה מכך חשיפה בלתי מורשית של נתוני המטופל. ארגונים המשתמשים במכשירי IoT חייבים להבטיח שהנתונים המועברים על ידי מכשירים אלה מוצפנים ומאובטחים כהלכה (H. L. Damghani et al., 2019).

מכשירי IoT חשופים גם להתקפות פיזיות, כגון גניבה או חבלה. התקפות אלו עלולות לגרום לפגיעה במכשיר עצמו, כמו גם בנתונים המאוחסנים במכשיר. כדי למנוע התקפות פיזיות, ארגונים צריכים ליישם אמצעי אבטחה פיזיים, כגון בקורות גישה ומערכות ניטור.

לבסוף, **ריבוי מכשירי ה-IoT יצר גם נופ אימים חדש**, כאשר תוקפים מכוונים למכשירי IoT כדי להשיק התקפות מניעת שירות מבוזרות (DDoS) בקנה מידה גדול. התקפות אלו עלולות לגרום לזמן השבתה משמעותי לארגון, ולהשפיע על יכולתו לנהל עסקים ולספק שירותים ללקוחות. כדי למנוע התקפות DDoS, ארגונים צריכים ליישם אסטרטגיות הפחתת DDoS ולוודא שמכשירי IoT אינם משמשים כחלק מ-botnet (Panda et al., 2021).

האבטחה היא היבט חיוני בכל התקדמות טכנולוגית, ו-IoT אינו יוצא מן הכלל. ההסתמכות הגוברת על מכשירים וחיישנים מחוברים מעוררת חששות לגבי האבטחה והפרטיות של הנתונים. כאשר לאינטגרציה של רכיבי IoT יכולה להיות השפעה משמעותית על רמת האבטחה בארגון. כאשר מכשירי IoT משולבים בתשתית של ארגון, זה יוצר משטחי התקפה חדשים שהאקרים יכולים לנצל. ניתן להשתמש במכשירים אלה כדי להפעיל התקפות על חלקים אחרים של הרשת, לגנוב נתונים רגישים או לשבש פעולות.

מצד שני, אם רכיבי IoT מאובטחים כראוי, הם יכולים לשפר את עמדת האבטחה הכוללת של הארגון. לדוגמה, חיישני IoT יכולים לשמש כדי לטור את האבטחה הפיזית של בניין, ולהתריע על כל פעילות חשודה. מכשירי IoT יכולים לשמש גם כדי לזהות ולהגיב לאיומי סייבר, ולספק מודיעין איומים בזמן אמת לצוותי אבטחה.

כדי להבטיח שילוב מאובטח של רכיבי IoT בתשתית של ארגון, חשוב לעקוב אחר שיטות אבטחה וסטנדרטים מומלצים. ארגונים צריכים לערוך הערכת סיכונים כדי לזהות נקודות תורפה אפשריות ולפתח אסטרטגיית אבטחה מקיפה המטפלת בסיכונים אלו. כמו כן, עליהם ליישם שיטות פיתוח מאובטחות בעת פיתוח או רכישת רכיבי IoT ולקבוע מדיניות ונהלים לשימוש וניהול מאובטחים של מכשירים אלו (Lee, 2020).

סמינר זה נועד לתרום להבנה מעמיקה יותר של הקשר בין שילוב טכנולוגיית IoT ואבטחת המידע בארגון, לנתח את ההשפעה שבשילוב כלים אלו ולספק המלצות כיצד ארגונים יכולים לנווט בנוף המורכב של אבטחת IoT כדי להגן על הנתונים והמערכות שלהם.

מטרת המחקר

שאלת המחקר הראשית: "מה היא ההשפעה של שילוב כלי IoT על רמת אבטחה של מערכות המידע של הארגון בחמש השנים האחרונות?"

משתנה בלתי תלוי: שילוב כלי IoT, **משתנה תלוי:** רמת האבטחה של מערכות המידע של הארגון.

שאלות ממוקדות:

1. "מהן סוגי החולשות הנפוצות ביותר בחמש השנים האחרונות ברכיבי IoT ומה רמת החומרה שלהן?"

משתנה בלתי תלוי: סוגי חולשות ברכיבי IoT, **משתנה תלוי:** רמת החומרה

2. "מה הן השיטות המומלצות לאבטחת מכשירי IoT, וכיצד ארגונים יכולים ליישם שיטות אלו כדי להפחית סיכוני אבטחה?"

משתנה בלתי תלוי: שיטות מומלצות לאבטחת מכשירי IoT, **משתנה תלוי:** סיכוני אבטחה עבור ארגונים המשתמשים במכשירי IoT

3. "האם ישנו מכנה משותף בין החולשות הקיימות ברכיבי IoT?"

משתנה בלתי תלוי: מכנה משותף (בין חולשות ה-IoT הקיימות), **משתנה תלוי:** חולשות קיימות ברכיבי IoT

4. "באיזו תדירות נדרש לעדכן/להוריד עדכוני גרסה ותיקונים ברכיבי IoT?" **משתנה בלתי תלוי:** רכיבי IoT, **משתנה תלוי:** תדירות ההתקנה וההורדה של עדכונים

הגדרה נומינלית של המשתנים

שם המשתנה	הגדרה נומינלית
שילוב כלי IoT	המשתנה "שילוב כלי IoT" מתייחס לתהליך של שילוב כלי IoT (חפצים ומכשירים פיזיים) בתשתית הטכנולוגית הקיימת של ארגונים, על מנת לאפשר תקשורת וחילופי נתונים בין אותם מכשירי IoT לבין המערכות הארגוניות. בהקשר של אבטחת סייבר, שילוב מכשירי IoT מתייחס לסיכונים ולפגיעויות (vulnerabilities) הפוטנציאליים שעלולים להיווצר ולהתממש בעת שילוב מכשירים אלו ברשת הארגונית. סיכונים אלו יוכלו להשפיע על פרטיות המידע של הארגון, אבטחת הרשת וניהול המכשירים שברשותו (Lee, 2020).
רמת האבטחה של מערכות המידע של הארגון	רמת האבטחה של מערכות המידע של ארגון מתייחסת למידת ההגנה שהארגון יישם כדי להגן ולאבטח את הנכסים הדיגיטליים שלו, לרבות נתונים (data), מכשירים ורשתות מפני איומי סייבר. שילוב מכשירי IoT בתשתית הארגונית יכולה לפגוע ברמת האבטחה שלו ולהכניס פרצות וסיכונים חדשים (Pan & Yang, 2018).
רמת החומרה	"רמת החומרה", בהקשר של חולשות שונות במערכות או מכשירי IoT, מתייחסת לרמת הסיכון וההשפעה הפוטנציאלית שניצול חולשה יכול לגרום למערכת או מכשיר IoT מסויים. זהו מדד לחומרת החולשה והנזק שייגרם אם תוקף ינצל אותה (Holm, Ekstedt, & Andersson, 2005).
סוגי חולשות ברכיבי IoT	סוגי החולשות שניתן למצוא ברכיבי IoT, כגון Buffer Overflow, דליפות זכרון, Stack Overflow, ו-Design Flaws (Nadir et al., 2022).
שיטות מומלצות לאבטחת מכשירי IoT	סט של אסטרטגיות, טכניקות ופרקטיקות שמטרתן היא להגן על סודיות, זמינות ושלמות של הנתונים הזורמים בכשירי IoT שונים. שיטות אלו עשויות לכלול פילוח רשת (network segmentation), בקורות גישה, הצפנות, מנגנוני אימות, עדכוני אבטחה וכו' (Pan & Yang, 2018).

סיכוני אבטחה שיכולים להשפיע על ארגונים הבוחרים להשתמש במכשירי IoT, לרבות סיכונים הקשורים לפרצות נתונים (data breaches), גישה בלתי מורשת, מניפולציה על מכשירים ופגיעה בסודיות, שלמות וזמינות של מידע רגיש (Knapp et al., 2009).	סיכוני אבטחה עבור ארגונים המשתמשים במכשירי IoT
המאפיינים או הגורמים המשותפים שתורמים לקיומן של חולשות של מכשירי IoT שונים (Naudé et al., 2009).	מכנה משותף (בין חולשות IoT קיימות)
חולשות אבטחה נפוצות במכשירי IoT, הכוללות, בין היתר, פגמים בתכנון (Design Flaws), ביישום המכשירים (Implementation) ובשימוש באותם המכשירים, העלויות לחשוף אותם לסוגים שונים של מתקפות סייבר (Farooq et al., 2015).	חולשות קיימות ברכיבי IoT
רכיבי IoT הם אלמנטים של תוכנה וחומרה המרכיבים מערכת IoT שלמה, כגון חיישנים, בקרים, שרתי ענן וכו'. האבטחה של רכיבים אלו חיונית להבטחת האבטחה הכוללת של מערכת IoT, שכן ניצול חולשה באחד מן הרכיבים עלול לסכן את כלל המערכת (S. H. Li, & Tryfonas, 2016).	רכיבי IoT
משתנה זה מתייחס לתדירות בה פאטצ'ים (patches) או עדכונים משוחררים על ידי יצרני מכשירי IoT כדי לטפל בבעיות אבטחה שונות ושיפור האבטחה הכללית של אותו מכשיר (Khalid & Ameen., 2021).	תדירות ההתקנה וההורדה של עדכונים

השערות המחקר

1. "מהן סוגי החולשות הנפוצות ביותר בחמש השנים האחרונות ברכיבי IoT ומה רמת החומרה שלהן?"

השערת המחקר: סוגי החולשות הנפוצות ביותר בחמש השנים האחרונות קשורות לפרצות תוכנה (Software vulnerability), אימות והרשאות וחולשות ברמת הרשת (Network level vulnerability). רמת החומרה של החולשות הללו נעה בין רמה נמוכה לקריטית, כאשר רוב החולשות המוכרות לנו נופלות בטווח החומרה הבינוני עד הגבוה-קריטי (H. L. Damghani et al., 2019).

ביסוס ההשערה: במאמר זה, ערכו המחקרים סקירת ספרות נרחבת על אבטחת מכשירי IoT וניתחו סוגים שונים של מתקפות על מכשירים אלו. הכותבים הצליחו לזהות מגמתיות ואת המתקפות הנפוצות ביותר. בנוסף לכך, נמצא במאמר כי רמות החומרה של החולשות והמתקפות השונות נע בין רמה נמוכה מאוד עד לרמה קריטית, ושרמת החומרה של רבית החולשות והמתקפות הינה בינונית עד גבוהה-קריטית.

2. "מה הן השיטות המומלצות לאבטחת מכשירי IoT, וכיצד ארגונים יכולים ליישם שיטות אלו כדי להפחית סיכוני אבטחה?"

השערת המחקר: השיטות המומלצות ביותר לאבטחת מכשירי IoT הן פילוח רשת (Network Segmentation), הגנה על נקודות קצה (Endpoint Security), קריפטוגרפיה ובקרת גישה (Access Control). ארגונים יכולים ליישם שיטות אלו על ידי ביצוע הערכות סיכונים תכופות ויסודיות (Risk Assessment), פריסה של מכשירי IoT מאובטחים בלבד וביצוע הדרכות תכופות לעובדים על שימוש נכון ובטוח במכשירי IoT (Pan & Yang., 2018).

ביסוס ההשערה: השערת המחקר מתבססת על הניתוח שבוצע במאמר זה, הן באתגרים ובאפשרויות שבעידן החדש שמכשירי ה-IoT מביאים איתם. המאמר מדגיש את החשיבות באבטחת מכשירי IoT ומציע מספר שיטות שונות להשגת מטרה זו.

3. "האם ישנו מכנה משותף בין החולשות הקיימות ברכיבי IoT?"

השערת המחקר: לחולשות הקיימות ברכיבי IoT יש מכנה משותף, בכך שלעיתים במכשירי IoT יש תעדוף לנוחות ולפונקציונליות על פני אבטחה נאותה. מרבית החולשות נובעות מההעדפה זו (Farooq et al., 2015).

ביסוס ההשערה: השערת המחקר מתבססת על מאמר זה הגורס כי מרבית החולשות במכשירי IoT נובעות מההעדפה להתמקד בפונקציונליות ונוחות השימוש במכשירי IoT, אשר לעיתים באה על חשבון אבטחה.

4. "באיזו תדירות נדרש לעדכן/להוריד עדכוני גרסה ותיקונים ברכיבי IoT?"

השערת המחקר: עדכונים ותיקונים הם מרכיב חיוני לאבטחת מכשירי IoT. תדירות העדכונים תקבע על פי סוג המכשיר, רגישותו לפגיעויות וחולשות והקריטיות שהוא מהווה עבור כלל המערכת. ניתן להגיד כי כל מכשיר IoT יצטרך לקבל עדכון לפחות אחת לשלושה חודשים כדי לטפל בפרצות ידועות ולהגן על עצמו מפני מתקפות סייבר (Khalid & Ameen., 2021). ביסוס ההשערה: מאמר זה מבצע סקירת ספרות על אבטחת מכשירי IoT כחלק מחיי היומיום. המאמר גורס כי עדכונים ותיקונים תכופים הינם כלים קריטיים לאבטחת המכשיר. בנוסף לכך, המאמר מראה כי להמון מכשירי IoT אין מנגנון אוטומטי להורדת והתקנת עדכונים. תדירות העדכונים המומלצת תהיה בהתאם לרמת הקריטיות של אותו רכיב לכלל המערכת. מסגרת הזמן של שלושה חדשים שהזכרנו בהשערה מתבססת על הכתוב במאמר ומהווה הערכה הגיונית ומושכלת שמציעה מסגרת זמן סבירה בהתבסס על המלצות מחברי המאמר ושיטות העבודה המומלצות בתעשייה (Industry's best practices).

שיטות מחקר

פרק זה מתאר את שיטות המחקר המשמשות במחקר זה כדי לחקור את ההשפעה של שילוב כלי IoT על רמת האבטחה של ארגון. שיטות המחקר בהן בחרנו, הן ניתוח מסדי נתונים והשוואה מסוג Benchmarking.

ניתוח מאגרים:

א. מערך המחקר: מתאמי.

ב. מטרת השימוש בשיטת המחקר: ניתוח המאגרים שבוצע לאורך המחקר כולל שימוש במסד הנתונים VaRIoT כדי לזהות את סוגי החולשות הנפוצים ביותר ברכיבי IoT בחמשת השנים האחרונות ובחינה ומחקר של הנתונים לטובת מציאה של מכנה משותף בין החולשות הללו. מסד נתונים זה מכיל רשימה מקיפה של חולשות IoT שונות ובוחר פרמטרים שונים עבור כל חולשה שמתועדת בו. המסד מספק תיאור מפורט של כל חולשה, הכולל את רמת החומרה שלה, מה הם מוצרי ה-IoT שנפגעו ממנה, כיצד היא משפיעה על זמינות, שלמות וסודיות המידע וכו'. במהלך המחקר, ניתחנו את הנתונים במסד הנתונים וסיווגנו את סוגי החולשות השונות על פי

רמת החומרה והשכיחות שלהן, מה שעוזר לנו לזהות מה הן החולשות הנפוצות ביותר ברכיבי IoT בחמשת השנים האחרונות.

ג. אוכלוסיית המחקר: מגוון החולשות המתועדות במסד הנתונים VaRIoT.

ד. דגימה: בוצעה דגימה לא הסתברותית. בחרנו חולשות שונות ממסד הנתונים VaRIoT בהתאם לצרכים ולמאפיינים שהוחלט עליהם מראש, כגון חולשות אשר התגלו בחמשת השנים האחרונות וחולשות ברמת חומרה מסויימת. יחידת הניתוח היא רשומה בודדה המייצגת חולשה ספציפית ואת תכונותיה, כאשר גודל המדגם חולש על אלפי חולשות שונות מן המאגר.

ה. תקופה: 2017 – 2022 (חולשות אשר התגלו בחמשת השנים האחרונות).

ו. מדידה: להלן המשתנים השונים הנמדדים באמצעות ניתוח המאגר:

שם משתנה	נמדד באמצעות הקטגוריות:	סוג המשתנה של הקטגוריה	סולם המדידה של הקטגוריה	ערכים אפשריים	חישוב המשתנה
סוגי החולשות ברכיבי IoT (שאלה ממוקדת ראשונה)	Index Type (כל ערך מייצג את רמת השכיחות של כל סוג חולשה מהמדגם)	כמותי בדיד	סדר (אורדינאלי)	1-7 : 1 הכי שכיח ו-7, הכי נדיר.	ספרנו את כמות המופעים מכל סוג של חולשה והבאנו לנושא זה את 7 סוגי החולשות הנפוצות ביותר במאגר הנתונים, ולכן משתנה זה מכיל 7 ערכים אפשריים.
רמת החומרה (שאלה ממוקדת ראשונה)	baseScore	כמותי רציף	רווח	1-10	ציון ה- baseScore מורכב משקלול של מספר משתנים ומצביע על רמת החומרה של כל חולשה. ציון ה- baseScore מורכב מהמשתנים exploitability, Scope ו- score, impact Score אשר הם עצמם מורכבים ממשתנים שונים, אשר מקבלים ציונים ומוכנסים למשוואה שהוגדרה ע"י חוקרי המאגר של VaRIoT אשר מחשבת את הציונים של שני המשתנים הללו. כפי שמוגדרים במאגר VaRIoT.
חולשות קיימות ברכיבי IoT (שאלה ממוקדת שלישית)	Type	איכותי	שמי	1. Input Validation Error 2. Lack Of Information 3. Buffer Error (Overflow) 4. XSS 5. Information Disclosure 6. Operating System Command Injection 7. Authorization Issue	מציאת שבעת החולשות השכיחות ביותר במרחב המדגם מן מסד הנתונים של VaRIoT (בחמש שנים האחרונות).
מכנה משותף (שאלה ממוקדת שלישית)	ConfidentialityImpact	איכותי	סדר	• None	נבחן את מדדי המרכז עבור כל סוג חולשה אל מול המאפיינים השונים ונערוך השוואה ביניהם. כל חולשה אשר לה מדדי מרכז דומים לחולשה אחרת, תיחשבה לדומות ובעלי מכנה משותף ע"פ אותו מאפיין אשר נמדד.
	IntegrityImpact	איכותי	סדר	• Low	
	AvailabilityImpact	איכותי	סדר	• High	
	privilegesRequired	איכותי	סדר	מידת העוצמה עבור (כל פרמטר)	
	AttackComplexity	איכותי	סדר	• Low • High	

<ul style="list-style-type: none"> • Adjacent Network • Local • Network • Physical <p>(ערכים אלו מייצגים את מידת הקרבה הנדרשת למכשיר המותקף)</p>	שמי	איכותי	AttackVector
<ul style="list-style-type: none"> • Required • None 	שמי	איכותי	userInteraction
<ul style="list-style-type: none"> • Changed • Unchanged <p>(מייצגים האם החולשה מאפשרת פגיעה ברכיב עצמו בלבד או גם זליגה לרשת)</p>	שמי	איכותי	Scope

מינוח ומושגים:

מתן המשקל המדויק לשלל הפרמטרים המשפיעים על ציון החומרה של החולשות מוסבר בצורה מפורטת בקישור שהוספנו בפרק המקורות.

המשתנה Scope: מראה האם פגיעות ברכיב אשר נגוע בחולשה המדוברת משפיעה על משאבים בסביבת המכשיר.

(1) Changed - פגיעות מנוצלת יכולה להשפיע על משאבים בסביבת הרכיב.

(2) Unchanged - פגיעות מנוצלת יכולה להשפיע רק על משאבי הרכיב.

המשתנה exploitabilityScore: מדדי הניצול משקפים את הקלות והאמצעים הטכניים שבהם ניתן לנצל את הפגיעות. התכונות המרכיבות את המשתנה הזה הן מאפייני החולשה שמובילים להתקפה מוצלחת:

- attackVector: מדד זה משקף את ההקשר שבאמצעותו ניצול פגיעות אפשרי. המשקל יהיה גדול יותר ככל שהתוקף יכול להיות מרוחק יותר (לוגית ופיזית) כדי לנצל את הרכיב הפגיע.

i. Network – חולשה הניתנת לניצול מרוחק, מספר התוקפים הוא גדול יותר משאר האפשרויות.

ii. Adjacent – החולשה חייבת להיות מנוצלת מאותה רשת משותפת, פיזית או לוגית.

iii. Local - הרכיב לא מחובר לרשת כלשהי.

iv. Physical - נדרשת גישה פיזית על מנת לנצל את החולשה.

- attackComplexity: מדד זה מתאר את מורכבות המתקפה.

- הערכים של משתנה זה הם: High, Low בהתאמה לרמת מורכבות המתקפה.

- privilegesRequired: מדד זה מתאר את רמת ההרשאות שהתוקף חייב להחזיק לפני שיצליח לנצל את הפגיעות.

הערכים של משתנה זה הם: None, High, Low בהתאמה לרמת ההרשאות הנדרשת לניצול החולשה.

- **userInteraction** : מדד זה קובע אם ניתן לנצל את החולשה אך ורק בעזרתו של התוקף, או שחייב אינטראקציה עם משתמש מורשה.
 - i. None - לא צריך אינטראקציה עם משתמש.
 - ii. Required – מצריך אינטראקציה.

המשתנה **Impact Score** מודד את ההשפעה הפוטנציאלית שיכולה להיות לפגיעות על הסודיות, השלמות והזמינות של המערכת המושפעת ובנוסף האם סביבתה גם ניזוקה או לא. הניקוד של משתנה זה מושפע מהערכים של המשתנים :

- i. **confidentialityImpact** : מדד זה מודד את ההשפעה על סודיות משאבי המידע המנוהלים על ידי הרכיב עקב פגיעות שניצלה בהצלחה.
- ii. **availabilityImpact** : מדד זה מודד את ההשפעה על הזמינות של הרכיב המושפע כתוצאה מחולשה שנוצלה בהצלחה. מדד זה מתייחס לאובדן הזמינות של הרכיב המושפע עצמו.
- iii. **IntegrityImpact** : מדד זה מודד את ההשפעה על שלמותו ואמינותו של מידע ברכיב שחולשה בו נוצלה בהצלחה.

הערכים של משתנים אלו הם : None ,High ,Low בהתאמה לרמת ההשפעה לאחר ניצול החולשה.

ז. **השערת מחקר עבור שאלה ממוקדת 1** : אנו משערים כי ככל שסוג החולשה נפוצה יותר כך רמת החומרה גבוהה יותר.

מבחן סטטיסטי נבחר : מתאם ספירמן, המאפשר למדוד את עוצמת הקשר בין שני משתנים מסוג סדר ורווח. מבחן זה יבחן את ההשערה בכך שיאמוד את עוצמת הקשר בין המשתנה Index Type (השכיחות במאגר של כל סוג חולשה למשתנה) לבין baseScore (רמת החומרה של כל חולשה).

השערת מחקר עבור שאלה ממוקדת 3 : אנו משערים שהחולשות הנפוצות ביותר חולקות קשר ומאפיינים משותפים אחת עם השניה.

מבחן סטטיסטי נבחר : נערוך מבחן חי בריבוע, אשר מהווה אוסף של מבחנים סטטיסטיים שיסייעו לנו לבדוק האם ישנו קשר בין החולשות הנפוצות ומאפייניהם, בשילוב עם מתאם קרמר שיספק לנו מדד תיאורי על עוצמת הקשר.

Benchmarking

- א. **מערך המחקר** : מתאמי.
- ב. **מטרת השימוש בשיטת המחקר** : ביצוע הניתוח ההשוואתי כולל בדיקה וניתוח של מוצרי IoT בעלי מטרה זהה. ביצוע הניתוח ההשוואתי יאפשר לנו להבין איזה דגשי אבטחה חשובים מיושמים במוצרי IoT שונים, כיצד ניתן לאבטח אותם, מה התכונות המשותפות ביניהם ובאיזו תדירות הם מקבלים עדכוני אבטחה חשובים. נבצע שימוש בגישה סטנדרטית הכוללת זיהוי קריטריונים להשוואה, בחירת מוצרי ה-IoT שייבדקו, עריכת מבחן השוואתי ומתן ציון לכל מוצר בכל קטגוריה בהתאם לביצועים ולתכונות שלו.
- ג. **אוכלוסיית המחקר** : עוזרות קוליות (Voice Assistant) שונות.

- ד. דגימה: הפריטים להשוואה הינם מוצרי עזר קוליים של היצרניות הגדולות ביותר בשוק: Google Home, Amazon Alexa, Apple Siri, Samsung Bixby.
- ה. דרך קביעת הציון: דרך קביעת הציון עבור המדדים השונים התבצעה על ידי כלל החוקרים, תוך ביצוע הערכות משותפות, דיונים והערכות אישיות.
- ו. מדדה:

שם מדד ראשי	משקל מדד ראשי	שם מדד משני	תיאור מדד משני	משקל מדד משני	דרך קביעת משקל למדד
עדכוני תוכנה ופאצ'ים	20%	שחרור פאצ'ים בזמן אמת	שחרור פאצ'ים ועדכוני אבטחה בזמן אמת, באופן המהיר ביותר לאחר גילוי ופרסום של חולשה במוצר IoT או באחת מהטכנולוגיות בהן הוא משתמש, הינו מרכיב קריטי מאוד ברמת האבטחה הכוללת של המוצר. כאשר מתגלה ומתפרסמת חולשה, יש לתקוף חלון הזדמנויות לנצל אותה. ככל שהיצרן יבצע עדכון מהיר יותר למוצר הפגיע שלו, כך חלון ההזדמנויות יקטן וכפועל יוצא הסיכוי שתוקף יצליח לנצל את החולשה בזמן תקטן.	50%	בחירת המשקל לתת קטגוריה זו בוצעה על ידי הערכה אישית של כל אחד מן החוקרים ושקלול משותף.
		תדירות העדכונים	עדכוני תוכנה מהווים גורם משמעותי באבטחה הכוללת של המוצר. מוצר IoT לעולם אינו מאובטח לחלוטין שכן כל הזמן מתגלות פרצות חדשות הקשורות ישירות למוצר או לאחת מהטכנולוגיות בהן הוא עוסק. ביצוע עדכונים תכופים המטפלים בליקויי אבטחה שמתגלים כל הזמן באופן שוטף יבטיח רמת אבטחה נאותה לאותו מוצר IoT.	40%	בחירת המשקל לתת קטגוריה זו מבוססת על המאמר Gupta, & van Oorschot., (2019)
		בהירות המידע	כאשר יצרן משחרר עדכון או פאצ', יש משמעות גדולה להסבר שהוא מספק על העדכון. ככל שההסבר בהיר יותר, מניע לפעולה ומוכן למשתמש הקצה, תעלה הסבירות שהמשתמש יתקין אותו בהקדם. יש חשיבות גדולה למנגנון ברור של שחרור ופרסום עדכונים והתקנה אוטומטית שלהם.	10%	בחירת המשקל לתת קטגוריה זו בוצעה תוך דיון והערכה משותפת של החוקרים.
שיטות לאבטחת מכשירי IoT	20%	אימות	ביצוע בקרת אימות (Authentication) היא קריטית לשימוש בטוח במכשיר IoT. ללא בקרת אימות מהימנות ואיכותיות, מכשירי IoT פגיעים למגוון רחב של איומים, כגון גניבת זהות, גישה בלתי מורשית וכו'. בקרת אימות הינן חלק אינטגרלי מאבטחת מכשירי IoT אשר מונעות סיכונים אבטחה רבים.	25%	בחירת המשקל לתת קטגוריה זו בוצעה תוך דיון והערכה משותפת של החוקרים. במהלך הדיון החוקרים בחנו מכשירי IoT שונים ואת בקרת האימות שלהם.
		בקרת גישה	בקרת גישה הינה גורם קריטי כחלק מאבטוח מוצר IoT. היא מאפשרת להגביל את הגישה לתכונות, פונקציונליות ונתונים מסויימים בהתאם לזהות ורמת ההרשאה של המשתמש או מכשיר המנסים לגשת למכשיר ה-IoT. ללא בקרת גישה נאותות, המכשיר יהיה חשוף למתקפות וליקויי אבטחה רבים.	20%	בחירת המשקל לתת קטגוריה זו מבוססת על המאמר HE) et al., 2018.
		הצפנה והגנה על נתונים	הצפנה והגנה על נתונים הינם תהליכים קריטיים עבור מוצרי IoT והנתונים שהם מייצרים ואוגרים. תהליכים אלו מבטיחים שמירה על	20%	בחירת המשקל לתת קטגוריה זו מבוססת על

המאמר (J. Li et al., 2020).		סודיות ושלמות המידע, מונעים מניפולציות אסורות על מידע ומאפשרות למכשיר ה-IoT לעמוד בתקנות רגולטיביות.			
בחירת המשקל לתת קטגוריה זו מבוססת על המאמר (Arfaoui, 2019).	15%	מכשירי IoT מחוברים לאינטרנט, ולכן כל מכשיר ברמה התאורטית יכול להתחבר אליהם. ישנה חשיבות רבה לבקורות והבדיקות שמכשיר IoT מבצע לפני שהוא מאפשר למכשיר או אדם מרוחק לתקשר איתו או לשלוט בו מרוחק.	גישה מרוחק		
בחירת המשקל לתת קטגוריה זו התבצעה על ידי הערכה אישית ושקלול משותף של כלל החוקרים.	10%	מדיניות הסיסמאות של מכשיר ה-IoT תקבע את סיסמאת ברירת המחדל, תגדיר את מורכבות הסיסמאות הנדרשות, תוקף הסיסמאות וכו'. ככל שהסיסמא תהיה מורכבת יותר, כך רמת האבטחה הכוללת של המכשיר תעלה, אולם היבטי אבטחה אחרים הינם משמעותיים יותר.	מדיניות סיסמאות		
בחירת המשקל לתת קטגוריה זו בוצעה על ידי הערכה משותפת של החוקרים.	5%	ניהול תצורת המוצר (קונפיגורציה) בצורה נכונה יוביל לרמת אבטחה גבוהה יותר. כאשר מוצר IoT מאפשר למשתמש לשנות הגדרות ברירת מחדל להגדרות אחרות (למשל שינוי סיסמאת ברירת מחדל לסיסמא אישית), רמת האבטחה של המוצר תוכל להשתפר במעט. יש לציין כי מתן אפשרויות רחב למדי יוכל גם להוביל את המשתמש ליצור סיכוני אבטחה בעצמו.	ניהול תצורת המוצר		
בחירת המשקל לתת קטגוריה זו בוצעה תוך דיון והערכה משותפת של החוקרים.	5%	ישנה חשיבות לאבטחה הפיזית של מכשיר IoT, שכן פגיעה בו יכולה להרוס את שלמות, סודיות וזמינות המידע שהמכשיר מספק. המכשיר צריך להיות מוגן משינויים פיזיים או נסיונות חילוץ מידע (ברמה הפיזית).	אבטחה פיזית		
בחירת המשקל לתת קטגוריה זו התבצעה על ידי הערכה אישית ושקלול משותף של כלל החוקרים.	50%	היכולת ליידע את המשתמש בנוגע לאירועים חשודים הקשורים למכשיר ה-IoT ולשלוח התראות בזמן אמת הינה קריטית ומהווה היבט חשוב מאוד באבטחה הכוללת של המכשיר.	התראות בזמן אמת		
בחירת המשקל לתת קטגוריה זו בוצעה על ידי הערכה משותפת של החוקרים.	35%	היכולת לשמור ולנתח לוגים היא קריטית לכל מכשיר IoT. לוגים יכולים לספק מידע משמעותי, כמו נסיונות פריצה למכשיר, נסיונות גישה בלתי מורשית ותעבורת רשת חריגה.	ניתוח לוגים	15%	ניטור
בחירת המשקל לתת קטגוריה זו התבצעה על ידי הערכה אישית ושקלול משותף של כלל החוקרים.	15%	צפייה במדדים שונים של המכשיר, כמו ניצול מעבד, ניצול זכרון ותעבורת רשת יכולה לעזור במניעה ומעקב אחר אירועי סייבר. אחוזי ניצול גבוהים במעבד, בזכרון ובשאר משאבים מחשוביים אחרים יכולים להצביע על מתקפה סייבר פעילה.	מדדים (מטריקות)		
בחירת המשקל לתת קטגוריה זו מבוססת על המאמר (Thorburn, 2019).	40%	תאימות לרגולציה (Regulatory Compliance) מבטחה שמכשיר ה-IoT עומד בדרישות מינימליות של אבטחה ושמירה על נתוני המשתמשים. כאשר מכשיר IoT עומד בתקנים הרגולטיביים ניתן לטעון בודאות כי יש לו מידת אבטחה נאותה.	תאימות לרגולציה	15%	עמידה בתקני אבטחה ורגולציה

בחירת המשקל לתת קטגוריה זו מבוססת על המאמר (Bertino, 2016)	40%	מכיוון שמכשירי IoT אוספים, אוגרים ומעבדים כמויות אדירות של מידע על המשתמשים, ישנה חשיבות עצומה לאמצעים בהם מכשירי IoT מגן על המידע הרגיש אותו הוא מחזיק. כמוכן, יש גם תקנות ורגולציות של אבטחת מידע ופרטיות אותן היצרנים חייבים לאכוף.	שמירה על פרטיות המשתמש		
בחירת המשקל לתת קטגוריה זו בוצעה על ידי הערכה משותפת של החוקרים.	20%	עמידה בתקני תעשיה חשובה עבור מכשירי IoT, שכן היא מבטיחה שהמכשיר עומד בסטנדרטים ודרישות מינימליות של אבטחה, שמירה על פרטיות ותפעוליות בינית (Interoperability).	עמידה בתקני תעשיה		
בחירת המשקל לתת קטגוריה זו בוצעה על ידי הערכה משותפת ודיון של החוקרים.	25%	היכולת של מכשירי IoT לבצע אינטגרציה עם מערכות ניהול אבטחה, כגון מערכות SIEM, SOAR וכו', הינה קריטית. ברגע שקיימים מכשירי IoT רבים בארגון, יהיה קשה לנהל אותם ברמה היחידנית ולא תהיה ברירה אלא לנהל אותם דרך מערכת אבטחה רחבה יותר.	אינטגרציה עם פלטפורמות ניהול אבטחה	20%	אינטגרציה עם מערכות אבטחה
בחירת המשקל לתת קטגוריה זו מבוססת על המאמר (Deshmukh, & Sonavane., 2017).	25%	תאימות עם פרוטוקולי אבטחה היא תכונה בסיסית שכל מכשירי IoT מהימן צריך לקיים. כפי שכבר נאמר, מוצרי IoT חשופים למתקפות סייבר רבות ומגוונות, ותאימות עם פרוטוקולי אבטחה תצמצם את הסיכויים שהמכשיר יפרץ. בנוסף לכך, רגולציות מסוימות מחייבות עמידה ותאימות עם פרוטוקולי אבטחה מסוימים.	תאימות עם פרוטוקולי אבטחה		
בחירת המשקל לתת קטגוריה זו התבצעה על ידי הערכה אישית ושקלול משותף של כלל החוקרים.	25%	אינטגרציה עם מוצרי אבטחת חומרה, כגון חומת אש (Firewall), מערכות IDS/IPS (Intrusion Detection System/Intrusion Prevention System) מאפשרת למוצרי IoT להעמיק את רמת האבטחה שלהם מעבר לרמת אבטחת תוכנה, שהיא "רדודה יותר". אינטגרציה זו תשפר את רמת האבטחה הכוללת של המכשיר, אפילו אם נפרץ ברמה האפלקטיבית.	אינטגרציה עם מוצרי אבטחת חומרה		
בחירת המשקל לתת קטגוריה זו בוצעה על ידי הערכה משותפת ודיון של החוקרים.	25%	אינטגרציה מאובטחת עם API הינה קריטית לכל מכשירי IoT, ובאה להבטיח שהתממשקות זו לא תוכל להיות מנוצלת על ידי גורמים זדוניים. API הינו סט של חוקים, פרוטוקולים וכלים אשר מאפשרות לאפליקציות שונות לתקשר אחת עם השנייה.	אינטגרציה מאובטחת עם API (Application Programming Interface)		

ממצאים

כפי שהתייחסנו בפרק שיטות המחקר, במחקר זה בחרנו לענות על שאלות המחקר שלנו בעזרת שתי שיטות מחקר, ניתוח השוואתי (Benchmark) וניתוח מאגרים. בעזרת שתי שיטות אלו, אנו מצפים לאשש או להפריך את השערות המחקר שלנו.

ניתוח מאגרים:

שאלה ממוקדת 1

מאפייני הנתונים שנאספו: מתוך כלל החולשות (3432) אשר ניתחנו מן המאגר, הרכבנו רשימה של שבעת סוגי החולשות הנפוצות ביותר (מתוך 42 סוגי חולשות שונים). חישבנו את דרגת החומרה

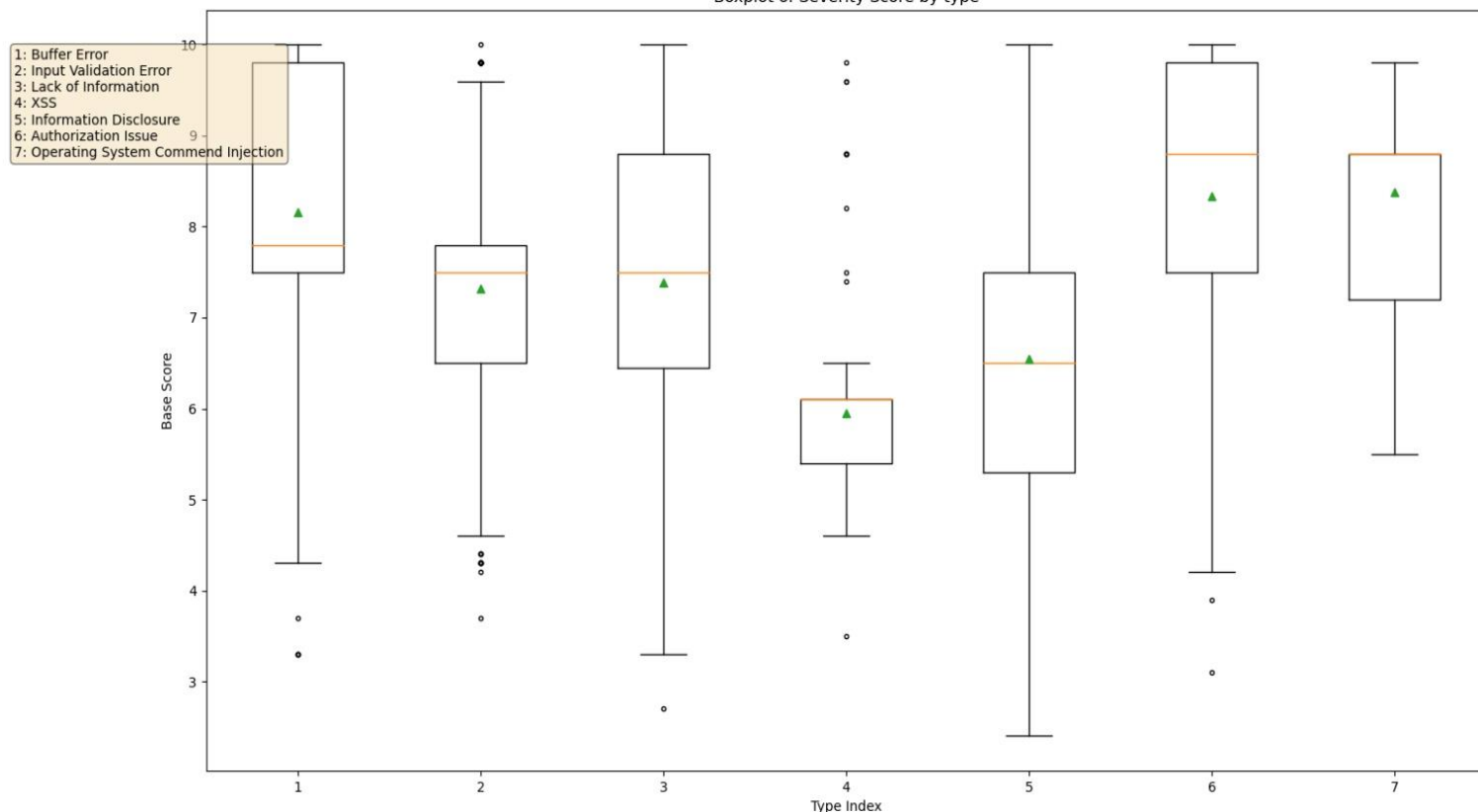
הממוצעת של כל חומרה כדי לבדוק את טיב הקשר בין הפופולריות של סוג החולשה לבין רמת החומרה שלה.

התקופה אליה מתייחסים הנתונים: 2017-2022.

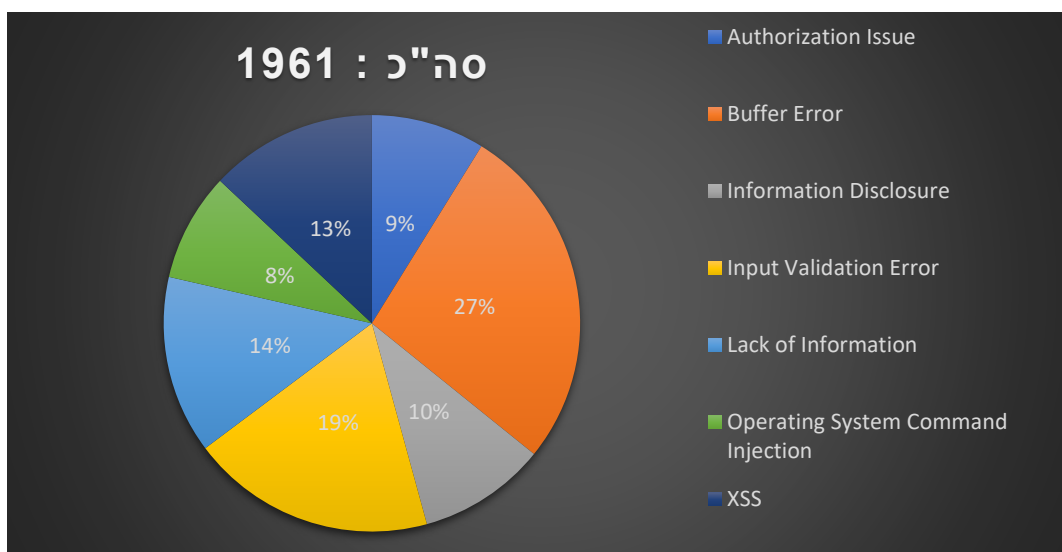
ממצאים תיאוריים: בשאלה זו, המשתנה הבלתי תלוי הוא שכיחות סוג החולשה, והמשתנה הבלתי תלוי הוא רמת החומרה. בכדי לבחון את הקשר בין שני משתנים אלו, ביצענו את מבחן ספירמן הבדוק קשר בין שני משתנים. המבחן בוצע ברמת מובהקות של 0.5 ולאחר ביצוע המבחן בין שני המשתנים קיבלנו ערך מובהקות ששואף לאפס (נספח א') מה שמצביע על קיומו קשר בין שני המשתנים. בנוסף לכך, מקדם ההתאמה (Correlation Coefficient) חיובי, כלומר הקשר בין שני המשתנים הוא חיובי. יש לציין שעל אף שהקשר חיובי, עוצמתו יחסית חלשה. תוצאות המבחן עולות בקנה אחד עם השערת המחקר עבור שאלה זו, אשר גרסה כי **ככל שחולשה נפוצה יותר, כך רמת החומרה שלה גבוהה יותר.**

- תרשים קופסה המציג את מדדי המרכז וממצאים תאוריים שונים עבור כל סוג חולשה ורמת החומרה שלה בהתאם לרמת שכיחותה (נתונים אלו מוצגים בטבלה תיאורית בנספח ב')

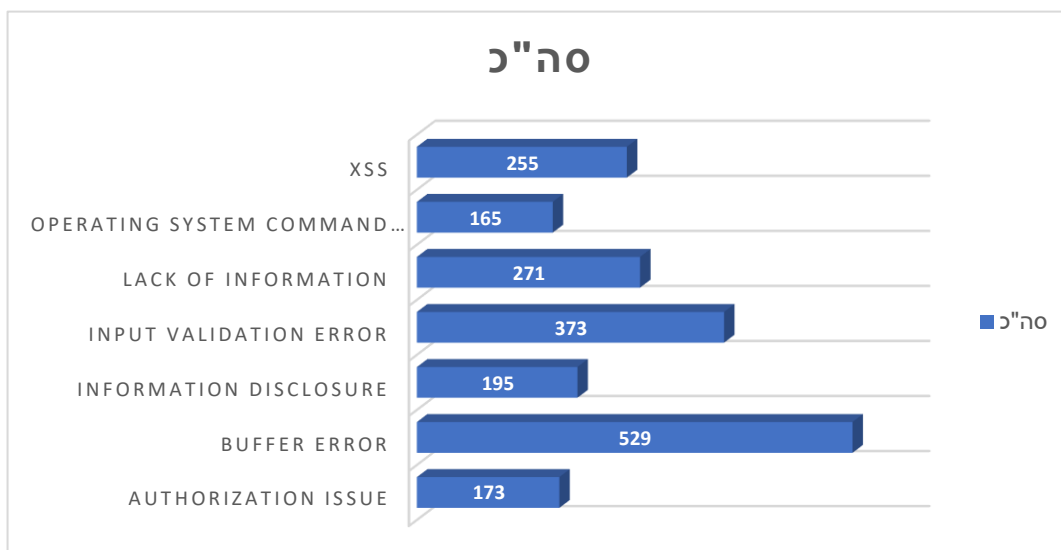
Boxplot of Severity Score by type



שכיחות סוגי החולשות הנפוצות באחוזים, מהחולשות הנפוצות ולא מסך כל החולשות במאגר :



שכיחות על פי ספירת המופעים :



שאלה ממוקדת 3

מאפייני הנתונים שנאספו : גם עבור שאלה זו, בחרנו לבחון את שבע החולשות הנפוצות ביותר ובחנו מדגם זהה למדגם שנבחן עבור שאלה ממוקדת 1. מצאנו את שכיחות הערכים של שמונה פרמטרים שונים עבור כל סוג חולשה כדי לנסות ולמצוא מכנה משותף ביניהן.

התקופה אליה מתייחסים הנתונים : 2017-2022.

ממצאים תיאוריים : בשאלה זו, המשתנה הבלתי תלוי הוא מכנה משותף (בין חולשות IoT קיימות), והמשתנה התלוי הינו חולשות קיימות ברכיבי IoT. בכדי לבדוק האם קיים מכנה משותף בין סוגי החולשות השונות, ביצענו מבחן חי-בריבוע בין סוגי החולשות לפרמטרים השונים כדי לבדוק האם קיים ביניהם קשר, ובנוסף לכך בדקנו את ערכו של מתאם קרמר (נספח ג') כדי לבדוק את עוצמת הקשר בין המשתנים. תוצאות המבחנים הציגו קשרים (ברמות חוזקה שונות) בין המשתנים, ועלו בקנה אחד עם השערת המחקר הגרסה כי קיים מכנה משותף בין החולשות השונות.

תוצאות מבחני חי-בריבוע וערכי מתאם קרמר :

קשר חזק קשר בינוני קשר חלש	תוצאות מבחן חי בריבוע ומתאם קרמר							
	Confidentiality Impact		Integrity Impact		Availability Impact		Privileges Required	
	ציון חי בריבוע		ציון חי בריבוע		ציון חי בריבוע		ציון חי בריבוע	
	0.652		0.686		0.512		0.207	
	שואף ל - 0		שואף ל - 0		שואף ל - 0		שואף ל - 0	
	Attack Complexity		User Interaction		Attack Vector		Scope	
	ציון חי בריבוע		ציון חי בריבוע		ציון חי בריבוע		ציון חי בריבוע	
TYPE	0.185		0.655		0.217		0.775	
	שואף ל - 0		שואף ל - 0		שואף ל - 0		שואף ל - 0	

טבלה המציגה את החולשות השונות והערכים השכיחים של כל אחת מן החולשות עבור כל אחד מן הפרמטרים הנבחרים :

טבלת שכיחים									
Index Type	Vulnerability	Confidentiality Impact	Integrity Impact	Availability Impact	Privileges Required	User Interaction	Attack Vector	Attack Complexity	Scope
1	Buffer Error	High	High	High	None	None	Network	Low	Unchanged
2	Input Validation Error	None	None	High	None	None	Network	Low	Unchanged
3	Lack of Information	High	High	High	None	None	Network	Low	Unchanged
4	XSS	Low	Low	None	None	Required	Network	Low	Unchanged
5	Information Disclosure	High	None	None	None	None	Network	Low	Unchanged
6	Authorization Issue	High	High	High	None	None	Network	Low	Unchanged
7	Operating System Command Injection	High	High	High	Low	None	Network	Low	Unchanged

: Benchmarking

ממצאים תיאוריים: בעזרת הנתונים שנאספו בעת ביצוע הניתוח ההשוואתי, קבענו ציונים עבור המדדים השונים עבור כל אחד מן המכשירים. המדדים חולקו ל-5 קטגוריות ו-20 תתי קטגוריות בסך הכל. הציון נע בין 1-10, כאשר 1 הוא הציון הנמוך ביותר ו-10 הינו הציון הגבוה ביותר.

שאלה ממוקדת 1:

מאפייני הנתונים שנאספו: תוך תהליך הניתוח ההשוואתי, חקרנו היכן הושקעו מירב המאמצים של החברות המובילות בהקשר של התגוננות מפני חולשות אבטחה שונות, ועל אילו אזורים שמם דגש. בעזרת חקירה זו, יכולנו לאתר את החולשות הנפוצות מפניהן החברות מנסות להתגונן.

שאלה ממוקדת 2:

מאפייני הנתונים שנאספו: בעת ביצוע הניתוח ההשוואתי, בדקנו קטגוריות שונות הקשורות לבקורות אבטחה שונות של המכשירים הנבדקים. בעזרת ההשוואה, נוכל לענות על השאלה ולהבין מה השיטות המומלצות ביותר לאבטחת מכשירי IoT וכיצד ארגונים יוכלו ליישם אותן.

שאלה ממוקדת 4:

מאפייני הנתונים שנאספו: כחלק מן הניתוח ההשוואתי, בדקנו מה היא תדירות שחרור העדכונים והפאציים של המכשירים השונים. בעזרת ההשוואה, הצלחנו להגיע להבנה ולאומדן סביר המייצג באיזו תדירות יצרניות מכשירי ה-IoT המובילות בשוק משחררות עדכונים ופאציים לטיפול בבעיות אבטחה.

הסבר לציוני ה-Benchmark (ניתן למצוא את ההשוואה המלאה בנספח ד')

מספר פרמטר	שם המכשיר	הסבר למתן הציון
1	Google Home	לגוגל יש היסטוריה של טיפול מהיר בחולשות ופרצות אבטחה, הכולל שחרור עדכונים תכופים לכלל מוצריה.
	Apple Siri	חברת אפל שמה דגש על אבטחת מוצריה השונים, ביניהם Siri. אפל מוציאה עדכונים בזמנים קבועים ומשתנים בהתאם לאירועי אבטחה שונים.
	Amazon Alexa	קצב העדכונים שהחברה משחררת יכול להשתנות בהתאם לרמת החומרה שמתגלה.
	Samsung Bixby	בהשוואה לתדירות העדכונים של שאר המוצרים, סמסונג משחררת עדכונים בתדירות וקצב איטיים יותר.
2	Google Home	לגוגל יש היסטוריה מוכחת של טיפול יעיל ומהיר בפרצות אבטחה.
	Apple Siri	חברת אפל שמה דגש רחב על היבטי אבטחה ודאגה תמיד לאורך שנות קיומה לשחרר פאציים ועדכונים אבטחה במהירות מיטבית.
	Amazon Alexa	לעיתים מהירות התגובה תהיה איטית יותר לעומת המכשירים האחרים בהשוואה זו, בהתאם לחומרה של החולשה שהתגלתה.
	Samsung Bixby	מכשירי ה-Bixby מבוסס על מערכת הפעלה מסוג אנדרואיד, ומכיוון שהמערכת היא מערכת מסועפת שלא תוכנתה ספציפית למוצר לעיתים יקח זמן משמעותי לחברה לשחרר עדכוני אבטחה רלוונטיים.
3	Google Home	גוגל מספקים הסברים ברורים ורחבים לגבי עדכוני האבטחה שלהם.
	Apple Siri	אפל מספקת הסברים ברורים להבנה לגבי עדכוני האבטחה שלה. לרוב היא גם מסבירה מה העדכון בא לתקן או למנוע.
	Amazon Alexa	אמאזון אף היא דואגת לספק הסברים נרחבים וברורים לעדכוני התוכנה והאבטחה שהיא משחררת.
	Samsung Bixby	מכיוון שמכשיר זה מבוסס על מערכת אנדרואיד מסובכת, לעיתים סמסונג מתקשה לספק הסברים ברורים למשתמש.
4	Google Home	Home Google מציע שיטות אימות חזקות הכוללות בקרת אימות על פי קול, ואימות דו-שלבי.
	Apple Siri	סירי מציעה מגוון רחב של אפשרויות ודרכי אימות, הכוללות אימות ביומטרי ואימות על ידי סיסמא.
	Amazon Alexa	אלכסה מציעה ומבצעת מספר מנגוני אימות, הכוללים אימות ופילוח משתמשים שונים על פי הקול שלהם, אימות על ידי סיסמא ואימות דו שלבי.
	Samsung Bixby	סאמסונג מציעה מספר מנגוני אימות שונים, ביומטריים או על ידי שימוש בסיסמא. אולם, סאמסונג חוותה בעבר אירועים אבטחה שקשורים לשיטות האימות שלה.
5	Google Home	גוגל מציעה מספר בקורות גישה, הכוללות את האפשרות ליצור מספר פרופילים שונים, כאשר לכל פרופיל מותאם אישית למשתמש בו. בנוסף, גוגל מאפשרת למשתמשים להגביל פעולות מסויימות, כמו ביצוע רכישות או גישה לתכנים ואפליקציות מסויימות על ידי שימוש בקוד או זיהוי קול.
	Apple Siri	חברת אפל מציעה בקורות גישה רבות, המאפשרות הגבלה של תכנים, פעולות ואפליקציות מסויימות על ידי אמצעי זיהוי ביומטריים או על ידי סיסמאות. בנוסף לכך, קיימת "בקורת הורים" במכשירי אפל אשר שומרת על קטינים מפני תכנים לא נאותים.

Amazon Alexa	אמאזון, בדומה לסירי מציעה בקרות גישה רבות, ביומטריות ולא ביומטריות וגם "בקרת הורים".	
Samsung Bixby	סאמסונג אף היא מציעה בקרות גישה רבות, אולם יש לה היסטוריה של תקלות וחולשות הקשורות לבקרות הגישה שלה.	
Google Home	משתמשי המוצר יכולים לנהל את תצורת המוצר דרך האפליקציה הייעודית. יש לציין כי גוגל מגבילה את המשתמש ולא ניתן לבצע שינויי הגדרות אשר יכולים לתרום לבעיות אבטחה.	6
Apple Siri	סירי מגבילה מאוד את המשתמש מלבצע שינויי הגדרות אשר יכולים לתרום לבעיות אבטחה.	
Amazon Alexa	אלכסה, בדומה לסירי ול- Google Home, לא מאפשרת לבצע שינויי הגדרות אשר יכולים לתרום לבעיות אבטחה.	
Samsung Bixby	כחלק מכך שמכשיר זה משתמש במערכת ההפעלה אנדרואיד, הוא יותר פתוח ומאפשר לבצע יותר שינויים אשר עלולים לתרום לבעיות אבטחה.	
Google Home	גוגל משתמשת בפרוטוקולי תקשורת מאובטחים, ואוכפת מדיניות נוקשה מאוד בכל הנוגע לאבטחת מידע ושמירה על הפרטיות. אולם, לאורך השנים עלו תהיות ובעיות עם הדרכים בהן גוגל אוספת ושומרת את המידע האישי של משתמשיה.	7
Apple Siri	אפל מגנה על נתוני המשתמשים שלה בעזרת הצפנות ושימוש בפרוטוקולי תקשורת המאובטחים והאמינים ביותר. אפל שמה בראש מעייניה את פרטיות המשתמש ושמירה על נתוניו, וגישה זו מממשת גם במוצר ה-Siri.	
Amazon Alexa	בדומה לגוגל, אלכסה משתמשת בפרוטוקולים הבטוחים והאמינים ביותר לאבטחת תעבורת הנתונים של משתמשיה. אולם, גם אמאזון נמצאת תחת ביקורת תמידית לגבי הדרכים והשיטות בהן היא אוספת ואוגרת את המידע של לקוחותיה.	
Samsung Bixby	סאמסונג משתמשת בפרוטוקולי אבטחה ושיטות אבטחה מתקדמות. אולם יש לציין כי לעומת המוצרים והחברות האחרות בניתוח השוואתי זה, היא חוותה הרבה יותר אירועי אבטחה אשר קשורים לנתונים האישיים של משתמשיה.	
Google Home	גוגל מציעה ואוכפת מדיניות סיסמאות נוקשה, הכוללת ייצור סיסמא חזקה וייחודית במהלך האתחול הראשוני של המוצר. בנוסף לכך, גוגל מעודדת את המשתמש לאפשר אימות דו-שלבי בכל ניסיון גישה למוצר.	8
Apple Siri	בדומה לגוגל, גם סירי של חברת אפל אוכפת מדיניות סיסמאות נוקשה ומעודדת את המשתמשים לאפשר אימות דו-שלבי בכל גישה חדשה למכשיר.	
Amazon Alexa	אמאזון אוכפת מדיניות נוקשה אך לא מבצעת אימות דו-שלבי כברירת מחדל, אלא רק אם המשתמש מבצע זאת באופן ידני, דבר אשר פוגע ברמת האבטחה הכוללת של המכשיר.	
Samsung Bixby	בדומה לאמאזון, סאמסונג אוכפת מדיניות סיסמאות נוקשה אך לא מבצעת אימות דו-שלבי כברירת מחדל.	
Google Home	כלל המכשירים אותם אנו משווים הינם בטוחים מאוד ברמה הפיזית. חילוף מידע מהם ברמה הפיזית כמעט ואינו אפשרי, ולכן כולם קיבלו את הציון 10.	9
Apple Siri		
Amazon Alexa		
Samsung Bixby		
Google Home	גוגל מאפשרת גישה מרוחקת מאובטחת דרך אפליקציית "Google Home App", אשר מאפשרת למשתמשים לגשת למשתמשים לגשת למכשיר מרוחק בצורה מאובטחת ומוצפנת.	10
Apple Siri	אפל מאפשרת גישה מרוחקת למכשיר דרך אפליקציית יעודית אשר מאפשרת גישה מרוחקת מאובטחת למכשיר.	
Amazon Alexa	אמאזון אף היא מאפשרת גישה מרוחקת דרך אפליקציית יעודית אשר מאפשרת גישה מרוחקת מאובטחת. הגישה מאובטחת והתעבורה מוצפנת אולם במכשירי אפל וגוגל יש אמצעי אבטחה רבים ומדויקים יותר.	
Samsung Bixby	סאמסונג אף היא מאפשרת גישה מרוחקת מאובטחת ומוצפנת, אולם היו מספר תקריות אבטחה איתה בעבר ולכן היא זכתה בציון הנמוך ביותר.	
Google Home	המוצר שולח התראות רבות בזמן אמת, ביניהן התראות על קול לא מזוהה שמנסה להפעיל את המכשיר, פתיחת דלת בבית, פעולות חריגות וסטיות שונות שהמכשיר מזהה. בנוסף לכך ניתן להגדיר התראות מסויימות בצורה עצמאית.	11
Apple Siri	אפל שולחת התראות בזמן אמת, ביניהן התראות המתריאות על ניסיונות גישה לא מזוהים, פעילויות חשודות. לעומת גוגל, אפל מציעה פחות גמישות מבחינת האפשרות ליצור התראות מותאמות אישית.	
Amazon Alexa	גם מוצר זה שולח התראות בזמן אמת, אולם בתדירות קטנה יותר לעומת המכשירים של אפל וגוגל.	

מכשיר הסאמסונג שולח התראות בזמן אמת, בתדירות ורמת פירוט נמוכים יותר מאשר שאר המכשירים.	Samsung Bixby	
המכשיר מייצר לוגים שאיתם ניתן לנתח אירועי אבטחה. לוגים אלו יכולו מידע על פעילות המכשיר, היסטוריית פקודות קוליות ואינטרקציות שונות.	Google Home	12
בדומה ל Google home מספק את אותו המידע, אך עם תוספות וכלים לניתוח מעט יותר מעמיק, ועל כן קיבל ציון גבוה יותר.	Apple Siri	
זוהה בפיצ'רים וביכולות ל-Google Home.	Amazon Alexa	
המכשיר קיבל את הציון הנמוך ביותר לאור הדמיון במידע שמספק, אך באופן פחות מעמיק בהשוואה לשאר המכשירים.	Samsung Bixby	
המכשיר מאפשר צפייה במטריקות שונות דרך אפליקציה ייעודית וכלים נוספים בצורה מפורטת וברורה, המספקים תמונת מצב מלאה אודות תקינות המכשיר.	Google Home	13
יכולות דומות ל-Google Home אך תוצאות מעט פחות אינפורמטיביות.	Apple Siri	
מציגים מטריקות בסיסיות בלבד.	Amazon Alexa	
	Samsung Bixby	
גוגל עומדת בצורה מיטבית בתקני התעשייה ומקפידה ליישם אמצעי אבטחה ופרוטוקולי תקשורת ששומרים על פרטיותו של המשתמש. עם זאת, שקלול הציון נפגע, לאור העובדה שגוגל אוספים מידע אודות פעילות המשתמש ללא הפסקה.	Google Home	14
בדומה לגוגל, מפגינה עמידה קפדנית בתקני התעשייה. אך בשונה מגוגל, לא אוספת מידע על המשתמש בצורה אגרסיבית.	Apple Siri	
אופן ההתנהלות הדומה ל-Apple אך משתמשים בשיטות מעט פחות מתקדמות.	Amazon Alexa	
בדומה ל-Amazon משתמשים באותן טכנולוגיות, אך בשונה מהם, הציון בעיות אבטחה רבות בעבר.	Samsung Bixby	
מפגינה עמידה קפדנית לרגולציות העולמיות, אך לאור "הפתיחות" (בהקשר של הורדות והתקנות) של המכשיר, הציון המשקולל נפגע מעט.	Google Home	15
דומה לגוגל, אך בשונה ממנה, המכשיר בעל מע' הפעלה סגורה ובטוחה יותר, ועל כן הציון הגבוה ביותר.	Apple Siri	
זוהה ל-Google Home.	Amazon Alexa	
זוהה ל-Google Home עם היסטוריית כשלים שהובילו לבעיות אבטחה.	Samsung Bixby	
גוגל מיישמת אמצעים וטכנולוגיות רבות לשמירה על פרטיות משתמשיה אולם ישנה ביקורת רבה על אופן ושיטות איסוף המידע שלהם על משתמשיהם.	Google Home	16
בדומה לגוגל, אפל מיישמת שיטות מתקדמות לשמירה על פרטיות המשתמש, תוך כדי, ככל הידוע, המנעות נאותה משימוש מופרז בנתוניו.	Apple Siri	
התנהגות זוהה למוצר של גוגל עם ביקורת פחותה על איסוף ושימוש בנתונים בצורה אגרסיבית.	Amazon Alexa	
משתמשים באמצעים פחות מתקדמים ועם היסטוריה של תקריות אבטחה שונות בהקשר של פרטיות משתמשים.	Samsung Bixby	
מציעה מספר יכולות אינטגרציה עם מגוון רחב של מערכות אבטחה שונות.	Google Home	17
מציעה מספר יכולות אינטגרציה עם המגוון הנמוך ביותר ביחס למערכות הנבחרות.	Apple Siri	
מציעה מספר יכולות אינטגרציה עם מגוון בינוני של מערכות אבטחה שונות.	Amazon Alexa	
מציעה מספר יכולות אינטגרציה עם מגוון רחב של מערכות אבטחה שונות.	Samsung Bixby	
משתמשים בפרוטוקולים הבטוחים והמומלצים ביותר.	Google Home	18
בדומה לגוגל ואמזון, אך לאור הסגירות במערכת ההפעלה שלהם זוכים לציון גבוה יותר.	Apple Siri	

משתמשים בפרוטוקולים הבטוחים והמומלצים ביותר.	Amazon Alexa	
רק לאחרונה התחילו שימוש בפרוטוקולים מתקדמים ובטוחים, אך בעלי היסטוריה בעייתית בשימוש בפרוטוקולים שנחשבו לפחות בטוחים.	Samsung Bixby	
למוצר יכולת אינטגרציה מוגבלת עם מוצרי אבטחת חומרה חיצוניים, כאשר היכולת המרכזית שלו בהקשר של מדד זה, היא עם מוצר אחר של גוגל (Google Nest Secure).	Google Home	19
למוצר יכולת התממשקות עיקרית עם המוצר Ubiquiti UniFi Security Gateway אשר משמש כחומת אש ומכשיר ניהול אבטחה של רשתות קטנות עד בינוניות.	Apple Siri	
למוצר זה יכולת אינטגרציה עם מוצרי Cisco שונים אשר יכולים לנהל רשתות תקשורת גדולות ומורכבות.	Amazon Alexa	
למוצר יכולת התממשקות עם מכשיר ייעודי של סמסונג - SmartThings Wi-Fi אשר מאפשר ניהול של רשת ביתית קטנה.	Samsung Bixby	
גוגל מספקת אינטגרציה מאובטחת עם API ברמה טובה, אך בעבר היו תקריות בהן התגלו חולשות ב-API.	Google Home	20
בדומה לגוגל, אך פחות חשופים לתקיפות מאשר גוגל.	Apple Siri	
זהה לפיצירים וליכולות של Apple.	Amazon Alexa	
Samsung מספקת אינטגרציה מאובטחת עם API ברמה נאותה אך לאור פתיחות המערכת (Android), הייתה חשופה למתקפות בעברה ועל כן הציון המשוכלל של המוצר נפגע.	Samsung Bixby	

ציונים סופיים:

Google Home: 7.77

Apple Siri: 8.61

Amazon Alexa: 7.81

Samsung Bixby: 6.29

סטטיסטיקה תיאורית (ציונים):

ממוצע	חציון	שכיח	סטיית תקן	שונות	טווח	מינימום	מקסימום	מכשיר להשוואה
8.1	8	8	1.1192102	1.2526316	4	6	10	Google Home
8.7	9	9	1.1285762	1.2736842	4	6	10	Apple Siri
7.95	8	8	1.145931	1.3131579	4	6	10	Amazon Alexa
6.75	7	7	1.0195458	1.0394737	5	5	10	Samsung Bixby

דיון ומסקנות:

שאלה ממוקדת 1

שיטות המחקר בהן השתמשנו על מנת לתת מענה לשאלה זו, הן ניתוח מאגרים וניתוח השוואתי. השערת המחקר שלנו עבור שאלה זו הייתה כי סוגי החולשות הנפוצות ביותר בחמש השנים האחרונות קשורות לפרצות תוכנה (software vulnerability), אימות והרשאות וחולשות ברמת הרשת (network level vulnerability) כאשר רמת חומרתן תהיה בטווח הבינוני עד גבוה-קריטי.

אל מול שאלה זו, חקרנו תחילה מהן החולשות הנפוצות ביותר בהן עושים שימוש בחמש השנים האחרונות. לצורך כך, מיפינו את את כלל החולשות במאגר ומנינו אותן ע"פ סוגיהן, תהליך זה העלה כי **שבעת החולשות הנפוצות ביותר (כפי שנמצא במאגר VaRIoT) הן:** Operating System, Information, Input Validation Error, Lack Of Information, Command Injection, Authorization Issues, Buffer Overflow, Disclosure ו-XSS אשר מנצלות פגמים שונים באבטחה של מכשירי IoT בהתאם לאופן המימוש שלהן.

בנוסף, המבחן הסטטיסטי שביצענו, מבחן ספירמן הראה כי ישנו קשר חיובי בין שכיחות החולשה לבין רמת חומרתה, ועל כן ניתן לומר כי בהקשר של שיטת מחקר זו, השערתנו אושרה, **כל שחולשה שכיחה יותר, כך עולה רמת חומרתה**. יש לציין כי אמנם קיים קשר בין המשתנים הללו אך עוצמת הקשר חלשה יחסית.

כמו כן, בנוסף לניתוח המאגר, עבור שאלה זו ביצענו גם ניתוח השוואתי שתכליתו לוודא את הממצאים שעלו מן ניתוח המאגר. בניתוח זה, עלה כי חלק בלתי מבוטל מהממצאים של היצרניות למוצרים המובילים בשוק מתמקדים בהגנה מפני חולשות המנצלות אמצעי אימות, בקורות גישה ופרצות תוכנה או כפי שצוין בניתוח ההשוואתי "שיטות לאבטחת מכשירי IoT". נדגיש כי היסטוריית החולשות של המכשירים אותם ניתחנו עלו בהלימה אחת אל מול החולשות השכיחות שעלו מן ניתוח המאגרים ועל כן גם בשיטת מחקר זו התוצאות עלו בקנה אחד עם השערת המחקר.

בתוך כך, בשילוב של ממצאי ניתוח המאגרים בהם היה קשר בין שכיחות החולשה לרמת חומרתה שהייתה בינונית גבוהה, ניתן היה לראות שבדיוק עבור אותן חולשות נפוצות, מושקעים מירב מאמצי האבטחה והמשאבים של היצרניות המובילות למוצרים שבחנו.

לצד זאת, לפי (Pan & Yang, 2018), **בנוסף** לחולשות השכיחות שמצאנו במאגר שקיבלו משקל רב, ניתן במאמר זה גם משקל משמעותי לחולשות הקשורות לאבטחה פיזית של רכיבי IoT בעוד שבמאגר לא ראינו התייחסות כזאת.

שאלה ממוקדת 2

לאור מאפייניהם של רכיבי IoT אשר להם לרוב מערכת הפעלה "רזה" יחסית, השערתנו הייתה כי **נדרשות מגוון של שיטות לאבטחת אותם הרכיבים**, כאשר שיטות אלו כוללות בין היתר: פילוח רשת, הגנה על נקודות קצה ויישום של בקורות גישה.

על שאלה זו, בחרנו לענות דרך ניתוח השוואתי אשר הראה כי לאור מורכבותו של שילוב רכיבי IoT בארגון אשר מציפים סוגיות אבטחתיות משמעותיות, יש לפעול בטווח רחב של דרכי התמודדות אל מול פערי אבטחה אלו.

בתוך כך, עלה כי המוצרים המובילים של החברות המובילות אשר בהם בחרנו לערוך את הניתוח ההשוואתי שמו דגש דומה למדי בין רוב הקטגוריות על פיהן ביצענו את הניתוח, ברם, ניתן היה לראות כי שתי הקטגוריות המובילות ביותר היו תחת קטגוריית עדכוני תוכנה ושיטות אבטחה שונות, בדגש על בקורות גישה ואימות שכן בטיחות השימוש של ארגון ברכיב IoT מסויים תלויה כמעט באופן גורף ברמת האבטחה איתה הוא מגיע מהיצרן.

לצד ממצאים אלו, ניתן לומר כי השערת המחקר שלנו בהיבט זה אוששה בהחלט שכן ניתן להבחין בצורה שאינה משתמעת לשתי פנים בחלוקה יחסית שווה במגוון רחב של מנגנוני אבטחה ובקורות שתכליתן לשמש כשיטות אבטחה לרכיבי IoT ושילובו בארגון.

נציין כי לאור השינויים הדחופים בעולם אבטחת המידע והדיגיטל, ישנן עוד מגוון של שיטות אבטחה אשר תופסות יותר ויותר מקום. למשל, לפי (Pan & Yang, 2018) אשר מציג כהזדמנות לשלב מנגנון אבטחה אשר מבוסס טכנולוגיית בלוקצ'יין וטכנולוגיית AI לחיזוק בקורות אימות וזיהוי התנהגות חריגה ופיתוח של מנגנוני הגנה פרו אקטיביים מה שמחזק עוד יותר את השערת המחקר שלנו, שכן גם פה, מוצע מגוון רחב של שיטות הגנה עבור רכיבי IoT.

שאלה ממוקדת 3

על שאלה זו בחרנו לענות בעזרת שיטת המחקר של ניתוח מאגרים, אשר אפשר מעבר על מספר רב של חולשות וקיום מבחנים סטטיסטיים שתכליתם לבחון האם ישנו קשר בין סוג החולשה לבין המאפיינים השונים בהם בחרנו להתמקד במאגר.

עם קיום המבחנים הסטטיסטיים, חי בריבוע לטובת בחינה של קיום קשר, ו**מתאם קרמר** לטובת בחינה של עוצמת הקשר, התוצאות היו חד משמעיות וניכר כי קיים קשר מובהק בין כל חולשה וחולשה לבין המאפיינים השונים, אשר מוצגים בטבלת השכיחים בפרק הממצאים, ועל כן ניתן לומר כי איששנו את השערת המחקר שלנו שהייתה כי לחולשות השכיחות ישנו מכנה משותף מובהק.

בתוך כך, ובהסתכלות רחבה יותר, עלה כי החולשות המובילות במדדי הפגיעה ב – CIA (Confidentiality, Integrity, Availability) הן **Authorization Issues**, **Buffer Error**, **Operating System Command Injection** ו-**Lack Of Information**. מדובר ביותר ממחצית מסוגי החולשות הנבדקות.

בנוסף לכך, במאפיין **AttackVector**, הבודק את הקרבה הנדרשת לטובת ביצוע התקיפה, נמצא כי כלל החולשות הנבדקות דורשות, ברוב המוחץ של התקיפות השונות להיות באותה הרשת של המכשיר הנתקף.

כמו כן, בניתוח מאפיין **PrivilegesRequired** אשר מצביע על רמת ההרשאות הנדרשות לטובת ביצוע התקיפה, בכל החולשות הערך השכיח ביותר הינו **None** (לא נדרשות הרשאות מיוחדות) למעט חולשות מסוג **Operating System Command Injection**, בה הערך השכיח הוא **Low**, כלומר נדרשת רמה מסויימת של הרשאות בכדי לבצע את התקיפה.

דומה למאפיין **PrivilegesRequired**, גם במאפיין **UserInteraction** אשר מציין את רמת המעורבות הנדרשת מהמשתמש במערכת המותקפת, בכל החולשות הערך השכיח ביותר הינו **None** (לא נדרשת מעורבות) למעט חולשות מסוג **XSS** בהן השכיח הוא **Required**.

במאפיין **Scope** כל החולשות חולקות את אותו ערך שכיח שהינו **Unchanged**, כלומר מימוש החולשה תשפיע לרוב רק על הרכיב המותקף ולא על סביבתו.

שאלה ממוקדת 4

על שאלה ממוקדת זו, בחרנו לענות בעזרת ניתוח השוואתי שמטרתו הייתה לבחון את תדירות העדכונים במכשירים הנבדקים. בשאלה זו, שיערנו כי תדירות העדכונים תהיה לערך כל שלושה חודשים אך תשתנה בין מכשיר למכשיר בהתאם לרגישותו לפגיעויות והקריטיות שהוא מהווה עבור כלל המערכת.

בניתוח ההשוואתי, עלה כי החברות המובילות משחררות עדכונים שוטפים בהתאם לאירועי סייבר והתרחשויות בעולם הדיגיטלי. כמו כן, ניכר כי החברות המובילות משקיעות משאבים רבים לאיתור חולשות והוצאת עדכונים באופן שוטף ולכן **בניתוח ההשוואתי ניתן לקטגוריה משקל רב יחסית.**

בנוסף, מצאנו כי מכשירי IoT של יצרניות מובילות אשר שמות דגש על אבטחה, משחררות עדכון לפחות אחת לחודש.

אל מול כל אלה, ואל מול מדגם יחסית מצומצם, קשה לומר כי השערתינו אוששה באופן מלא, אמנם מצאנו כי משוחררים במכשירים הנבדקים עדכונים באופן תדיר, לפחות אחת לחודש, אולם קשה לספק אמירה רחבה יותר אל מול מדגם זה שכן מדובר ברכיבים אשר מיוצרים על החברות המובילות והחזקות בשוק, שלהן משאבים רבים ודגש מהותי על אבטחה ולכן הן לא בהכרח מהוות מדגם מייצר של כלל תעשיית ה-IoT. מעבר לכך, לאורך ביצוע המחקר נתקלנו ברכיבי IoT רבים אשר יצרניהם זונחים לאחר שחרורם הראשוני וכפועל יוצא אינם מקבלים עדכוני אבטחה לטיפול בבעיות שונות.

מסקנות והמלצות

במחקר זה, שאפנו לחקור את ההשפעה של שילוב כלי IoT על רמת האבטחה במערכות מידע ארגוניות בחמש השנים האחרונות. לאורך המחקר, התייחסנו לארבע שאלות ממוקדות שהנחו את החקירה שלנו. בפרק זה, נסכם את הממצאים ונספק המלצות מעשיות לארגונים המבקשים לשפר את האבטחה של מערכות המידע שלהם לאור האינטגרציה ההולכת וגוברת של כלי IoT.

בתור התחלה, ניתן לומר באופן חד משמעי וברור, כי כל שילוב של רכיב דיגיטלי כזה או אחר, מגדיל את שטח הפנים של הרשת עם העולם החיצון ועל כן מגדיל את סיכוני האבטחה בארגון, עד כמה וכמה שמדובר בכלי IoT שנחשבים לכלים בעלי מערכת הפעלה רזה שלה יכולות הגנה מוגבלות.

הממצאים שלנו חשפו כי שבעת החולשות הנפוצות ביותר בחמש השנים האחרונות הן: XSS, Operation System Command Injection, Lack of Information, Input Validation Error, Authorization Issue ו-Information Disclosure, Buffer Error. כאשר ניתן לומר כי נפוצות, נובעת ממגוון רחב של **מאפיינים משותפים** אשר מקנים להן מעמד של חולשות מועדפות לניצול.

בין מאפיינים אלו, נגענו בעוצמת הפגיעה של החולשות הללו ע"פ מאפייני ה-CIA שקיבלו ציונים גבוהים יוצאים מגדר הרגיל, וכלי בוקטור התקיפה, מעורבות המשתמש הנתקף, וההרשאות הנדרשות אשר חלקו מדדים נמוכים מאוד שמצביעים על קלות מימוש החולשה לביצוע התקיפה. בכלל זה חומרת החולשות הללו נע בין בינוני לגבוהה, כאשר חלקן מהוות סיכון גבוה יותר לאבטחת

מערכות המידע הארגוניות. כדי לטפל בחולשות אלו, אנו ממליצים לארגונים לבצע הערכות אבטחה יסודיות, ליישם שיטות קידוד מאובטחות ולעדכן באופן קבוע את מערכות הארגון כדי לצמצם את החשיפה לחולשות אלו.

באבטחת מכשירי IoT, אנו ממליצים לארגונים לפעול לפי שיטות עבודה מומלצות כגון הטמעת מנגנוני אימות חזקים, הצפנת שידורי נתונים וקביעת מדיניות אבטחה ופרוטוקולים ברורים ומחמירים. ניטור קבוע של פעילות המכשיר ותגובה בזמן לאירועי אבטחה פוטנציאליים הם חיוניים לשמירה על סביבת IoT מאובטחת.

לגבי תדירות העדכון עבור רכיבי IoT, אנו מדגישים את החשיבות של עדכוני תוכנה ותיקונים בזמן. ארגונים צריכים לקבוע לוח זמנים לעדכונים, לעקוב מקרוב אחר מהדורות של ספקים ולהבטיח תאימות למערכות קיימות. עדכון יזום ממזער את החשיפה לפגיעויות ידועות ומחזק את עמדת האבטחה הכוללת של מערכות המידע של הארגון.

מגבלות המחקר והמלצות להמשך

למרות שהמחקר שלנו מספק תובנות חשובות, חשוב להכיר במגבלותיו. המחקר התמקד בטווח זמן מסוים וייתכן שלא יתפוס את כל סיכוני האבטחה המתעוררים בנוף ה-IoT המתפתח במהירות או שייתכן שהממצאים לא יהיו ישימים לתקופות קודמות. כמו כן, ניתוח מסד הנתונים מסתמך על הדיוק והשלמות של מסד הנתונים VaRIoT. לצד זה, הניתוח ההשוואתי לא לוכד את כל הניואנסים של הביצועים של מכשירי IoT בתרחישים בעולם האמיתי.

לבסוף, המחקר מוגבל לקבוצה ספציפית של מכשירים ותכונות של מכשירי IoT שונים, וייתכן שלא ניתן יהיה להכליל את הממצאים למכשירים אחרים.

למרות מגבלות אלו, שיטות המחקר בהן נעשה שימוש במחקר זה מספקות תובנות חשובות לגבי ההשפעה של שילוב כלי IoT על רמת האבטחה של מערכות המידע של ארגון. אנו מעודדים מחקר נוסף כדי לחקור גורמים נוספים ואסטרטגיות הפחתה אפשריות.

לסיכום, המחקר שלנו מדגיש את הצורך של ארגונים לתעדף אבטחת IoT במערכות המידע שלהם. על ידי יישום ההמלצות המעשיות שפורטו לעיל, ארגונים יכולים לצמצם חולשות נפוצות, לשפר את עמדת האבטחה שלהם ולהגן על נתונים ומשאבים יקרי ערך מפני איומים מתעוררים הקשורים ל-IoT.

מקורות:

- Alfrhan, A. A., Alhusain, R. H., Alassaf, M. A., Alalwi, H. M., & Elkhediri, S. (2019). CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques. Journal of Physics: Conference Series.
<https://doi.org/10.1109/CAIS.2019.8769560>
- Arfaoui, A., Cherkaoui, S. Kribeche A., & S. M. Senouci, (2019). Context-Aware Adaptive Remote Access for IoT Applications, in IEEE Internet of Things Journal, 7(1), 786-799.
<https://doi.org/10.1109/JIOT.2019.2953144>
- Bertino, E. (2016). Data privacy for IoT systems: Concepts, approaches, and research directions. Journal of Information Security and Applications.
<https://doi.org/10.1109/BigData.2016.7841030>
- Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., Nadeau, E., O'Rourke, D. G., Piccarreta, B., & Scarfone, K. (2019). Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (NISTIR 8228). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.IR.8228>
- Common Vulnerability Scoring System v3.1: Specification Document (n.d.) Retrieved from: <https://www.first.org/cvss/v3.1/specification-document#7-1-Base-Metrics-Equations>
- Damghani, H., Damghani, L., Hosseinian, H., & Sharifi, R. (2021). Classification of Attacks on IoT. Journal of Electrical and Computer Engineering Innovations, 6(2), 245-252.
- Deshmukh S., & Sonavane, S. S. (2017) Security protocols for Internet of Things: A survey. International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), Chennai.
<https://doi.org/10.1109/ICNETS2.2017.8067900>
- Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8259A>
- Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on Internet of Things (IoT). International Journal of Computer Applications, 113(1), 1-7.
[A review on internet of things \(IoT\)](#)
- Gupta, H., & van Oorschot, P. C. (2019). Onboarding and software update architecture for IoT devices. In Proceedings of the 15th ACM International Conference on

Computing Frontiers. ACM.

<https://doi.org/10.1109/PST47121.2019.8949023>

He, W., Golla, M., Padhi, R., Ofek, J., Durmuth, M., Fernandes, E., & Ur, B. (2018). Rethinking Access Control and Authentication for the Home Internet of Things (IoT). 27th USENIX Security Symposium, 255 – 272.

<https://www.usenix.org/conference/usenixsecurity18/presentation/he>

Holm, H., Ekstedt, M., & Andersson, D. (2005). Empirical analysis of system-level vulnerability metrics through actual attacks. IEEE Transactions on Dependable and Secure Computing, 9(6), 824-836.

<https://doi.org/10.1109/TDSC.2012.66>

Khalid, L. F., & Ameen, S. Y., (2021). Secure IoT integration in daily lives: A review. Journal of Information Technology and Informatics, 1(1), 6-12.

<https://qabasjournals.com/index.php/jiti/article/view/23>

Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. Computers & Security, 28(7), 493-508.

<https://doi.org/10.1016/j.cose.2009.07.001>

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet, 12(9), 157.

<https://doi.org/10.3390/fi12090157>

Li, J., Zhang, Y., Ning, J., Huang, X., Poh, G. S., & Wang, D. (2020). Attribute Based Encryption with Privacy Protection and Accountability for CloudIoT. IEEE Internet of Things Journal, 10(2), 762 - 773.

<https://doi.org/10.1109/TCC.2020.2975184>

Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: A security point of view. Internet Research, 26(2), 337-359.

<https://doi.org/10.1108/IntR-07-2014-0173>

Nadir, I., Mahmood, H., & Asadullah, G. (2022). A taxonomy of IoT firmware security and principal firmware analysis techniques. Journal of Internet Services and Applications, 38, 100552.

<https://doi.org/10.1016/j.ijcip.2022.100552>

Naudé, W., Santos-Paulino, A. U., & McGillivray, M., (2009). Measuring vulnerability: An overview and introduction. Oxford Development Studies, 37(3), 183-191.

<https://doi.org/10.1080/13600810903085792>

Nayak, K., Marino, D., Efstathopoulos, P., & Dumitraş, T., (2014). Some vulnerabilities are different than others: Studying vulnerabilities and attack surfaces in the wild. Springer International Publishing Switzerland, 426–446.

https://doi.org/DOI: 10.1007/978-3-319-11379-1_21

Pan, J., & Yang, Z. (2018). Cybersecurity challenges and opportunities in the new "Edge Computing + IoT" world. In SDN-NFV Sec'18: 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, 29 - 32.

<https://doi.org/10.1145/3180465.3180470>

Panda, M., Mousa, A. A., & Hassanein, A. E. (2021). Developing an Efficient Feature Engineering and Machine Learning Model for Detecting IoT-Botnet Cyber Attacks. IEEE Access, 9, 91038-91049.

<https://doi.org/10.1109/ACCESS.2021.3092054>

Thorburn, R., Margheri, A., & Paci, F. (2019). Towards an integrated privacy protection framework for IoT: contextualising regulatory requirements with industry best practices. Personal and Ubiquitous Computing.

<https://doi.org/10.1049/cp.2019.0170>

VARIOT. Vulnerabilities (n.d.). Retrieved from <https://www.VaRIoTdb.pl/vulns/>

פלאח, א. (2018). תהליך הפיתוח כקו הגנה מרכזי מפני תקיפות סייבר. האוניברסיטה הפתוחה, מחקרים ומסמכי עבודה במדעי המחשב, (2).

נספחים

נספח א' – מבחן ספירמן (עבור שאלה ממוקדת 1)

		baseScore	IndexType
baseScore	Correlation Coefficient	1.000	.150**
	Sig. (2-tailed)	.	.000
	N	1961	1961
IndexType	Correlation Coefficient	.150**	1.000
	Sig. (2-tailed)	.000	.
	N	1961	1961

נספח ב' – ממצאים תיאוריים – סוגי חולשות אל מול רמת חומרה (baseScore)

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Max
					Lower Bound	Upper Bound		
Authorization Issue	173	8.335	1.5649	.1190	8.100	8.570	3.1	10
Buffer Error	529	8.160	1.3235	.0575	8.047	8.273	3.3	10
Information Disclosure	195	6.543	1.7373	.1244	6.298	6.788	2.4	10
Input Validation Error	373	7.320	1.3533	.0701	7.182	7.458	3.7	10
Lack of Information	271	7.389	1.6634	.1010	7.190	7.588	2.7	10
Operating System Command Injection	165	8.381	1.0325	.0804	8.222	8.539	5.5	10
XSS	255	5.945	.7441	.0466	5.854	6.037	3.5	9.8
Total	1961	7.479	1.5914	.0359	7.409	7.549	2.4	9.8

נספח ג' – מבחני חי-בריבוע וערכי מתאים קרמר

1. המשתנה Type לעומת המשתנה confidentialityImpact

תוצאות מבחן חי-בריבוע:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1668.416 ^a	12	.000
Likelihood Ratio	1442.114	12	.000
N of Valid Cases	1961		

חישוב מתאם קרמר:

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	.922	.000
	Cramer's V	.652	.000
N of Valid Cases		1961	

2. המשתנה Type לעומת המשתנה integrityImpact

תוצאות מבחן חי-בריבוע:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1846.422 ^a	12	.000
Likelihood Ratio	1537.498	12	.000
N of Valid Cases	1961		

חישוב מתאם קרמר:

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	.970	.000
	Cramer's V	.686	.000
N of Valid Cases		1961	

3. המשתנה Type לעומת המשתנה availabilityImpact

תוצאות מבחן חי-בריבוע:

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1029.785 ^a	12	.000
Likelihood Ratio	1102.616	12	.000
N of Valid Cases	1961		

חישוב מתאם קרמר:

Symmetric Measures

	Value	Approximate Significance
Nominal by Nominal	Phi	.725
	Cramer's V	.512
N of Valid Cases	1961	

4. המשתנה Type לעומת המשתנה attackVector

תוצאות מבחן חי-בריבוע:

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	277.999 ^a	18	.000
Likelihood Ratio	312.603	18	.000
N of Valid Cases	1961		

חישוב מתאם קרמר:

Symmetric Measures

	Value	Approximate Significance
Nominal by Nominal	Phi	.377
	Cramer's V	.217
N of Valid Cases	1961	

5. המשתנה Type לעומת המשתנה attackComplexity
תוצאות מבחן חי-בריבוע:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	67.232 ^a	6	.000
Likelihood Ratio	69.321	6	.000
N of Valid Cases	1961		

חישוב מתאם קרמר:

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	.185	.000
	Cramer's V	.185	.000
N of Valid Cases		1961	

6. המשתנה Type לעומת המשתנה privilegesRequired
תוצאות מבחן חי-בריבוע:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	167.259 ^a	12	.000
Likelihood Ratio	150.920	12	.000
N of Valid Cases	1961		

חישוב מתאם קרמר:

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	.292	.000
	Cramer's V	.207	.000
N of Valid Cases		1961	

7. המשתנה Type לעומת המשתנה userInteraction
תוצאות מבחן חי-בריבוע:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	841.121 ^a	6	.000
Likelihood Ratio	869.161	6	.000
N of Valid Cases	1961		

חישוב מתאם קרמר:

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	.655	.000
	Cramer's V	.655	.000
N of Valid Cases		1961	

8. המשתנה Type לעומת המשתנה scope
תוצאות מבחן חי-בריבוע:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1178.404 ^a	6	.000
Likelihood Ratio	975.558	6	.000
N of Valid Cases	1961		

חישוב מתאם קרמר:

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	.775	.000
	Cramer's V	.775	.000
N of Valid Cases		1961	

נספח ד' – Benchmarking Scoring

Bixby		alexa		Apple		Google HOME		משקל	מדד
ציון משוקלל	ציון	ציון משוקלל	ציון	ציון משוקלל	ציון	ציון משוקלל	ציון		
6	1.2	7.6	1.52	9.9	1.98	8.5	1.7	20%	עדכוני תוכנה ופאצ'ים
2.8	7	3.2	8	4	10	3.6	9	40%	תדירות העדכונים
2.5	5	3.5	7	5	10	4	8	50%	שחרור פאצ'ים בזמן אמת
0.7	7	0.9	9	0.9	9	0.9	9	10%	בהירות המידע
5.45	1.09	8.65	1.73	9.5	1.9	8.9	1.78	20%	שיטות לאבטחת מכשירי IoT
0.25	7	2.5	10	2.5	10	2.5	10	25%	אימות
1.2	6	1.8	9	1.8	9	1.6	8	20%	בקורות גישה
0.35	7	0.45	9	0.45	9	0.45	9	5%	ניהול תצורת המוצר (קונפיגורציה)
1.4	7	1.6	8	2	10	1.6	8	20%	הצפנה והגנה על נתונים
0.7	7	0.6	6	0.9	9	0.9	9	10%	מדיניות ססמאות
0.5	10	0.5	10	0.5	10	0.5	10	5%	אבטחה פיזית
1.05	7	1.2	8	1.35	9	1.35	9	15%	גישה מרחוק
7.1	1.06	6.85	1.02	7.35	1.1	7.65	1.14	15%	ביטור
3.5	7	3.5	7	3.5	7	4	8	50%	התראות בזמן אמת
2.7	6	2.45	7	2.8	8	2.45	7	35%	ניתוח לגים
0.9	6	0.9	6	1.05	7	1.2	8	15%	מודים (מטריקות)
6.6	0.99	8	1.2	9.2	1.38	7.6	1.14	15%	עמידה בתקני אבטחה ורגולציה
1.4	7	1.6	8	1.8	9	1.6	8	20%	עמידה בתקני תעשייה
2.8	7	3.2	8	3.6	9	3.2	8	40%	תאימות לרגולציה (Regulatory Compliance)
2.4	6	3.2	8	3.8	9	2.8	7	40%	שמירה על פרטיות המשתמש
6.5	1.95	7.8	2.34	7.5	2.25	6.7	2.01	30%	אינטגרציה עם מערכות אבטחה
2	8	1.75	7	1.5	6	2	8	25%	אינטגרציה עם פלטפורמות ניהול אבטחה
1.5	6	1.75	7	2	8	1.5	6	25%	תאימות עם פרוטוקולי אבטחה
1.8	6	2.7	9	2.4	8	1.8	6	30%	אינטגרציה עם מוצרי אבטחת חומרה
1.2	6	1.6	8	1.6	8	1.4	7	20%	אינטגרציה מאובטחת עם API
6.29		7.81		8.61		7.77		100%	ציון סופי משוקלל

הצעת עבודה לסמינר בלמידה מעשית

חלק א' (למילוי על ידי הסטודנטים)

1. הגשת ההצעה לסמסטר : למשל תשפ"ג ב'
2. קוד עבודה: 20232033
3. פרטים מזהים:

שם סטודנט:י	אמר עוזרי	ת"ז:	204469936
שם סטודנט:י	גיא ארביב	ת"ז:	208542332
שם סטודנט:י	דניאל סולטן	ת"ז:	208611020

4. תחום הידע : נושא אבטחת המידע בעולם ה-IOT.

5. הגדרת הבעיה או המוטיבציה למחקר – בעולם בו אנו חיים כיום, האינטרנט מקבל מקום נרחב ומשמעותי אפילו בפעולות יום יומיות ותופס יותר ויותר מקום ככל שעובר הזמן. זה בא לידי ביטוי בקישורים של רכבים ומכשירים רבים לרשת האינטרנט לסובת שיפור ביצועים והעלאת פונקציונליות.
כל אלה, מציבים אתגרים חדשים בהיקשרם של אבטחת מידע, ומציפים שאלות ותהיות שלא היו בעבר, שלהן השפעות רחבות על הביטחון האישי ופרטיות המשתמש, בכלל זה, העלאת הסיכון למתקפות סייבר, לאור רגישות כלי IOT בין היתר:
- חשיפה למידע רגיש: מכשירי IOT לעיתים אוספים נתונים רגשים כמו מיקום, מידע בריאותי, מידע פיננסי, "מקשיבים" לסביבתם, וכו'.
- פגיעה בתשתיות קריטיות (משולבים בתשתיות ציבוריות נרחבות: חשמל, תחב"צ, מים וכד') וייתכן אפילו פגיעה פיזית

- לאור אופיים של רכיבי IOT אשר להם מערכת הפעלה רזה יחסית, פוטנציאל האבטחה שלהם מוגבל, למשל: מנגנוני אימות חלשים, ופרוטוקלי הצפנה מיושנים.

- מורכבות המערכת – בד"כ מערכות IOT מורכבות ממספר רב של רכיבים אשר תלויים אחד בשני ומציבים בפנינו מורכבות ביכולת שלנו לזהות פרצות אבטחה פוטנציאליות.

מונחי חיפוש אפשריים: IoT Security Best, IoT Security Risks, Cyber Security, IoT Security Standards, IoT Cybersecurity Practices, IoT groups devices.

6. מאמרים :

6.1. מאמר ראשון :

- הפניה למאמר לפי APA :

Lee, I. (2020, September 1). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet; MDPI.
<https://doi.org/10.3390/fi12090157>

- מהי שאלת המחקר במאמר?
- How can effective IoT cyber risk management be achieved for organizations and users through the use of cybersecurity technologies and tools?
- מהו המשתנה התלוי/מסביר והמשתנה הבלתי תלוי/מסביר במאמר?

Independent variable: cybersecurity technologies and tools

Dependent variable: reduction of cybersecurity risk for organizations

- אילו שיטות מחקר בוצעו במחקר המתואר?
- מאמר זה מציג סקירה טכנולוגית אבטחת סייבר של IoT ומסגרות לניהול סיכונים סייבר ומציג מסגרת ארבע שכבות לניהול סיכונים סייבר של IoT. המאמר מיישם גם שיטות תכנות ליניארית להקצאת משאבים פיננסיים למספר פרויקטים של אבטחת סייבר של IoT. שיטות המחקר בהן נעשה שימוש במחקר זה כוללות סקירת ספרות וניתוח כמותי בשיטות תכנות ליניארית.

6.2. מאמר שני :

- הפניה למאמר לפי APA :

Jia, Y., Yang, K., Chen, J., & Li, X. (2020). IoT Security Risk Assessment Model Based on Fuzzy Analytic Hierarchy Process. *Journal of Computer Research and Development*, 57(7), 1409-1417.

- מהי שאלת המחקר במאמר?

Research question: How can a security risk assessment model be developed to evaluate the security of IoT systems?

- מהו המשתנה התלוי/מוסבר והמשתנה הבלתי תלוי/מסביר במאמר?

Independent variable - Security risk assessment model; Dependent variable - Security risks associated with IoT systems.

- אילו שיטות מחקר בוצעו במחקר המתואר?

במאמר 2, הוצג מודל הערכת סיכונים אבטחה עבור מערכות IoT המבוסס על תהליך היררכיה אנליטית מסוּשטשת (FAHP). FAHP היא שיטת קבלת החלטות המשתמשת במבנה היררכי לפירוק בעיה מורכבת למרכיבים קטנים יותר ומעריכה כל רכיב על סמך חשיבותו והרלוונטיות שלו לבעיה הכוללת. הוא משלב בין המושגים של לוגיקה מסוּשטשת, המאפשרת מידע לא ודאי ולא מדויק, לבין תהליך ההיררכיה האנליטית (AHP), שמתעדף חלופות על סמך חשיבותן היחסית.

6.3. מאמר שלישי:

- הפניה למאמר לפי APA:

Li, S., Tryfonas, T., Li, H., Faculty of Engineering, University of Bristol, Bristol, UK, & Department of Mathematics and Information Sciences, Northumbria University, Newcastle upon Tyne, UK. (2016). The Internet of Things: a security point of view. *Internet Research*, 26(2), 337-359.
<https://doi.org/10.1108/intr-07-2014-0173>

- מהי שאלת המחקר במאמר?

What are the security challenges and issues associated with the Internet of Things, and what solutions can be proposed to address them?

- מהו המשתנה התלוי/מוסבר והמשתנה הבלתי תלוי/מסביר במאמר?

Dependent variable: Proposed solutions to address security challenges and issues associated with the Internet of Things

Independent variable: Security challenges and issues associated with the Internet of Things

- אילו שיטות מחקר בוצעו במחקר המתואר?

המאמר אינו מתאר מחקר או ניסוי ספציפי, אלא מספק סקירה וניתוח מקיפים של מחקרים וספרות קיימים הקשורים לאבטחת IoT. המחבר מסנתז מידע ממגוון מקורות, כולל מאמרים אקדמיים, דוחות בתעשייה ופרסומים ממשלתיים, כדי לזהות אתגרי אבטחה נפוצים ובעיות הקשורות למכשירי ומערכות IoT. כמו כן, המאמר מציע פתרונות אפשריים להתמודדות עם אתגרים וסוגיות אלו, תוך הסתמכות על תובנות מהספרות הקיימת ומהמומחיות של המחבר עצמו בתחום. שיטות המחקר בהן נעשה שימוש במאמר הן אפוא בעיקר סקירת ספרות וניתוח.

7. **שאלת המחקר:** מהי ההשפעה של שילוב כלי IoT (משתנה בלתי תלוי) על רמת האבטחה של ארגון (משתנה תלוי)?

8. **שיטות המחקר:** סממני כיוון שיטות תבצעו את המחקר. בחירה בשיטות מחקר מסוימות מחייבת איסוף היקף מינימלי של משתתפים – בעבודה תוכלו לממש מעבר לכך, אם תרצו. השיטות והגדלים משפיעים גם על רמת המורכבות של הסמינר ולכן גם על העיון. יש לעיין לפחות שתי שיטות מחקר ארבע השיטות הראשונות. ראיונות עומק, יכולים להתבצע בנוסף לשתי השיטות האחרות – ראיונות מהווים תמיכה לשיטות האחרות ולא שיטת מחקר העומדת בפני עצמה, מבחינת הדרישות של קורס זה.

ניתוח מאגרים: לאורך אופי שאלת המחקר שלנו, נרצה לבצע אנליזה מעמיק על מאגרי נתונים



אשר מכילים מידע אודות רכיבי IOT ושלל תכונותיהם, הפונקציונליות שלהם וכמובן יכולות ומגבלות האבטחה שלהם.

מסד הנתונים של VARIOt:

הינו מאגר המכיל מידע על חולשות ידועות ובעיות אבטחה המשפיעות על התקני IoT ומערכות תומכות. הוא משמש כמקור מידע על ידי חוקרים, מפתחים ובעלי עניין אחרים בקהילת ה-IoT כדי לזהות ולטפל בסיכוני אבטחה במכשיר ומערכות IoT.

מסד הנתונים כולל מגוון של מידע על פגיעויות IoT, כולל פרטים טכניים על הפגיעויות, חומרתן וההשלכות הפוטנציאליות במקרה של ניצול. מסד הנתונים מספק גם מידע על המכשירים והמערכות המושפעים, ומציע הדרכה כיצד להפחית או לטפל בפגיעויות ובחולשות.

בסיס הנתונים נקרא VARIOt והוקם על ידי צוות חוקרים ממספר אוניברסיטאות אירופיות, כולל האוניברסיטה הטכנית של מינכן ואוניברסיטת טרנטו. המטרה העיקרית של מסד הנתונים היא לתמוך בפיתוח של מערכות IoT מאובטחות וגמישות יותר, על ידי אספקת משאב מקיף ועדכני על פגיעויות ידועות וסיכוני אבטחה פוטנציאליים.

בעזרת מסד זה, נוכל לבחון את חומרת/נכמות ואיכות החולשות והפגיעויות הנלוות לשילוב של רכיבי IOT במערכות גדולות וההשלכות לכך.

Benchmarking:

נרצה לערוך השוואה בין רכיבי IOT אשר מוסמעים ברכיבים/תהליכים ומערכות גדולות בעלי פונקציונליות מסוימת ונבחן את רמת האבטחה שלהם.

כאמור, לצורך כך, נבחר כלי IOT בעלי פונקציונליות דומה, ומשווה את רמת האבטחה שלהם בהתאם לקריטריונים מוגדרים מראש שנבחר, כמו: רמת פונקציונליות (כמה תהליכים ממומשים בעזרת הרכיב?), מס' חולשות קיימות, סוגי החולשות: sql injection, didos, buffer overflow, ... תדירות הורדות גרסא ועדכונים, תדירות הוצאת פאטצ'ים, האם הותקף בעבר, באיזו מע' הפעלה ניתן להסמיע?

9. שאלות מחקר ממוקדות:

9.1. שאלה ממוקדת ראשונה

האם ישנו מכנה משותף בין החולשות הקיימות ברכיבי IOT?

9.2. שאלה ממוקדת שניה

כל כמה זמן נדרש לעדכן/להוריד גרסה ופאטצ'ים ברכיבי IOT?

9.3. שאלה ממוקדת שלישית


מהן סוגי החולשות הנפוצות ביותר ברכיבי IOT ומה רמת החומרה שלהן?

9.4. שאלה ממוקדת רביעית

מהן השיטות המומלצות לאבטחת מכשירי IoT, וכיצד ארגונים יכולים ליישם שיטות אלו כדי להפחית סיכוני אבטחה?

חלק ב' (למילוי על ידי המנחה האקדמי)

1. נושא הסמינר מאושר / לא מאושר

2. שם המנחה האקדמי: פרופ' חתי גפני חתימה:  תאריך: 10/3/23

הערות:

מחקתי (בקו על המלל) קטעים שהייתם צריכים למחוק בכלל. להבא תקראו היטב את ההוראות ותפעלו בדיוק על פיהן.

אם המנחה האקדמי אישר תוך מתן הערות, הסטודנטים מחויבים ליישם את ההערות בתוכנית העבודה ובסמינר עצמו, והמנחה המקצועי מתבקש לשים לכך לב.



מערך למידה מעשית

תוכנית עבודה – סמנר
גירסת מרץ 2023

תוכנית עבודה לסמינר

חלק א' (למילוי על ידי הסטודנט)

1. פרטים מזהים

שם סטודנט/ית:	אמרי עוזרי	ת"ז:	204469936
שם סטודנט/ית:	גיא ארביב	ת"ז:	208542332
שם סטודנט/ית:	דניאל סולטן	ת"ז:	208611020

2. סמסטר הגשה: תשפ"ג ב'

3. קוד עבודה : c3320231

4. שם המנחה המקצועי : מר ג'וש בכר

5. **שאלת המחקר -** מהי ההשפעה של שילוב כלי IoT (משתנה בלתי תלוי) על רמת האבטחה של ארגון (משתנה תלוי) בחמש השנים האחרונות?

6. **שאלות ממוקדות**

6.1 מהן סוגי החולשות הנפוצות ביותר בחמש השנים האחרונות ברכיבי IoT ומה רמת החומרה שלהן?

6.2 מהן השיטות המומלצות לאבטחת מכשירי IoT, וכיצד ארגונים יכולים ליישם שיטות אלו כדי להפחית סיכוני אבטחה?

6.3 האם ישנו מכנה משותף בין החולשות הקיימות (ידועות?) ברכיבי IoT?

6.4 באיזו תדירות נדרש לעדכן/להוריד גרסה ותיקונים ברכיבי IoT?

7. **משתנים שיבדקו במחקר**

שם משתנה	משמש כמשתנה תלוי / מוסבר, בלתי תלוי / מסביר	בשאלה/ות ממוקדות/ות מס'
רמת החומרה	משתנה תלוי המושפע מסוג החולשה	6.1
סוגי חולשות ברכיבי IoT	משתנה בלתי תלוי - סוגי החולשות הם משתנה מסביר, שכן הם משמשים כדי להסביר את רמת החומרה.	6.1
סיכוני אבטחה עבור ארגונים המשתמשים במכשירי IoT	משתנה תלוי	6.2
שיטות מומלצות לאבטחת מכשירי IoT	משתנה בלתי תלוי - השיטות המומלצות לאבטחת מכשירי IoT הן משתני מסביר, מכיוון שהם משמשים כדי להסביר כיצד ארגונים יכולים להפחית סיכוני אבטחה.	6.2
חולשות קיימות (ידועות?) ברכיבי IoT	משתנה תלוי	6.3

מכנה משותף	משתנה בלתי תלוי - המכנה המשותף הוא משתנה מסביר, שכן הוא משמש כדי להסביר את החולשות הקיימות ברכיבי IoT.	6.3
תדירות העדכונים/תיקונים	משתנה תלוי	6.4
רכיבי IoT	משתנה בלתי תלוי - רכיבי ה-IoT הם משתנה מסביר, שכן הם מאסברים על ידי תדירות העדכונים/תיקונים.	6.4

כאמור, שאלת המחקר הכוללת היא: "מהי ההשפעה של שילוב כלי IoT (משתנה בלתי תלוי) על רמת האבטחה של ארגון (משתנה תלוי)?"
כל אחת מהשאלות הממוקדות מתייחסת להיבט ספציפי של שאלת המחקר, והתשובות לשאלות אלו יכולות לעזור לשפוך אור על ההשפעה הכוללת של שילוב כלי IoT על אבטחה ארגונית.

"האם יש מכנה משותף בין החולשות הקיימות ברכיבי IoT?"
על ידי זיהוי מכנה משותף בין החולשות, הארגון יכול לפעול לטיפול בגורמים השורשיים של פגיעויות אלו ולשפר את האבטחה הכוללת.

"באיזו תדירות נדרש לעדכן/להוריד גרסה ותיקונים ברכיבי IoT?"
עדכונים ותיקונים קבועים יכולים לסייע בהפחתת סיכוני אבטחה על ידי טיפול בפרצות ידועות, ולהפחית את הסבירות להתקפות מוצלחות.

"מהם סוגי החולשות הנפוצים ביותר ברכיבי IoT ומה רמת החומרה שלהם?"
הבנת סוגי וחומרת הפגיעות ברכיבי IoT יכולה לעזור לארגונים לתעדף מאמצי אבטחה ולהקצות משאבים בצורה יעילה יותר.

"מהן השיטות המומלצות לאבטחת מכשירי IoT ואיך ארגונים יכולים ליישם את השיטות הללו כדי להפחית סיכוני אבטחה?"
על ידי הטמעת שיטות אבטחה מומלצות עבור מכשירי IoT, ארגונים יכולים להפחית את הסיכון הכולל שלהם לפרצות אבטחה ולשפר את אבטחת הפעילות שלהם.

ביחד, התשובות לשאלות ממוקדות אלו יכולות לספק הבנה מקיפה של ההשפעה של שילוב כלי IoT על אבטחה ארגונית, על ידי התייחסות הן לנקודות התורפה והן לאמצעי האבטחה המומלצים להפחתת סיכונים.

8. רשימת מקורות

8.1 מאמר ראשון :

- Lee, I. (2020, September 1). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet; MDPI. <https://doi.org/10.3390/fi12090157>
- מאמר זה מספק סקירת ספרות של המצב המוכי של אבטחת סייבר וניהול סיכונים של IoT, תוך הדגשת האתגרים וההזדמנויות לאבטחת מערכות IoT. המחבר מזהה תחומים מרכזיים לשיפור אבטחת ה-IoT, כגון בקרת גישה ומנגנוני אימות טובים יותר, פרוטוקולי הצפנה חזקים יותר ואסטרטגיות משופרות לניהול סיכונים.
- מאמר זה יכול לעזור לענות על כמה משאלות המחקר, כולל זיהוי חולשות נפוצות ברכיבי IoT, הבנת שיטות מומלצות לאבטחת מכשירי IoT והערכת ההשפעה הכוללת של שילוב IoT על האבטחה הארגונית.

8.2 מאמר שני :

- Jia, Y., Yang, K., Chen, J., & Li, X. (2020). IoT Security Risk Assessment Model Based on Fuzzy Analytic Hierarchy Process. Journal of Computer Research and Development, 57(7), 1409-1417
- מאמר זה מציע מודל של תהליך היררכיה אנליטית מטושטשת (FAHP) להערכת סיכונים האבטחה הקשורים למערכות IoT. המחברים מעריכים את האפקטיביות של המודל שלהם באמצעות מחקר מקרה ומגלים שהוא יכול לזהות ולתעדף ביעילות סיכונים אבטחה במערכות IoT.
- מאמר זה יכול לעזור לענות על שאלת המחקר על סוגי החולשות הנפוצות ביותר ברכיבי IoT וחומרתן על ידי מתן מודל להערכת ותעדוף סיכונים אבטחה.

8.3 מאמר שלישי :

- Li, S., Tryfonas, T., Li, H., Faculty of Engineering, University of Bristol, Bristol, UK, & Department of Mathematics and Information Sciences, Northumbria University, Newcastle upon Tyne, UK. (2016). The Internet of Things: a security point of view. *Internet Research*, 26(2), 337-359. <https://doi.org/10.1108/intr-07-2014-0173>

- מאמר זה מספק סקירה חקירה של אתגרי אבטחת IoT ומציג טקסנומיה לניתוח בעיות אבטחת IoT. המחקרים חוקרים אינטי אבטחה ופגיעות שונות במערכות IoT ודנים במתרחות פוטנציאלים להתמודדות עם אתגרים אלו.
- מאמר זה יכול לעזור לענות על שאלת המחקר על השיטות המופלגות לאבטחת מכשירי IoT והמתחת סיכוי אבטחה על ידי מתן ניתוח מעמיק של אתגרי אבטחה ומתרחות פוטנציאלים. במספר, הוא יכול לספק תובנות לגבי המבנה המשותף בין התולדות הקיימות ברובי IoT.

9. שיטות מחקר

9.1 שיטה ראשונה – ניתוח מאגרים

מסד הנתונים של VARIO:

היום מאגר המכיל מידע על תולדות דיווח בעיות אבטחה המסופקות על התקני IoT ומערכות תומכות. הוא משמש כמקור מידע על ידי חוקרים, מפתחים ובעלי ערך אחרים בקהילת ה-IoT - כדי לזהות ולטפל בסיכוי אבטחה במכשירי ומערכות IoT. מסד הנתונים כולל מגוון של מידע על פגיעות IoT, כולל פרטים טכניים על הפגיעות, תומכות והשלכות הפוטנציאליות במקרה של בעול. מסד הנתונים מספק גם מידע על המכשירים והמערכות המושפעים, ומציע הדרכה כיצד להפחית או לטפל בפגיעות ובתולדות.

בסיס הנתונים וקרא VARIO הוקם על ידי צוות חוקרים ממספר אוניברסיטאות אירופיות, כולל האוניברסיטה הטכנית של מינכן ואוניברסיטת טרונט. המטרה העיקרית של מסד הנתונים היא לתמוך בפיתוח של מערכות IoT מאובטחות וביטחון יעיל, על ידי אספקת משאב מקיף ועדכני על פגיעות ידועות וסיכוי אבטחה פוטנציאלים. בעזרת מסד זה, ככל לבחון את חומרת/גומות ואיכות התולדות והפגיעות הנליות לשילוב של רכיבי IoT במערכות גדולות והשלכות לנך. הקישור למסד זה אינו דרוש אישור.

9.2 שיטה שניה – Benchmarking

נרצה לערוך השוואה בין רכיבי IOT אשר מוטמעים ברכיבים/תהליכים ומערכות גדולות בעלי פונקציונליות מסויימת ונבחן את רמת האבטחה שלהם. כאמור, לצורך כך, נבחר כלי IOT בעלי פונקציונליות דומה, ונשווה את רמת האבטחה שלהם בהתאם לקריטריונים מוגדרים מראש שנבחר, כמו: רמת פונקציונליות (כמה תהליכים ממומשים בעזרת הרכיב), מס' חולשות קיימות, סוגי החולשות - buffer overflow, sql injection, didos, תדירות הודעות גרסא ועדכונים, תדירות הוצאת פאטצ'ים, האם הותקף בעבר, באיזו מע' הפעלה ניתן להטמיע ועוד.

10. מיפוי חקירת שאלות ממוקדות

שאלה ממוקדת שמספרה	9.1 ניתוח מאגרים	9.2 Benchmarking
6.1	האם ישנו מכנה משותף בין החולשות הקיימות ברכיבי IOT?	
6.2		באיזו תדירות נדרש לעדכן/להוריד גרסה ותיקונים ברכיבי IoT?
6.3	מהם סוגי החולשות הנפוצים ביותר ברכיבי IoT ומה רמת החומרה שלהם?	מהם סוגי החולשות הנפוצים ביותר ברכיבי IoT ומה רמת החומרה שלהם?

6.4	מהן השיטות המומלצות לאבטחת מכשירי IOT, וכיצד ארגונים יכולים ליישם שיטות אלו כדי להפחית סיכויי אבטחה?
-----	--

Benchmarking יכול לעזור לענות על שאלות אלה על ידי מתן דרך להשוות את ביצועי האבטחה של ארגונים או מערכות שונות. על ידי ניתוח החוזקות והחולשות של ארגונים או מערכות עם ביצועים מובילים, ארגונים יכולים לזהות שיטות עבודה ואסטרטגיות מומלצות לשיפור עמדת האבטחה שלהם.

11. הערכת סיכונים

סיכון ספציפי	התמודדות אם יתמש
חוסר תקשורת בין חברי הצוות	אם חברי הצוות אינם מתקשרים באופן קבוע או יעיל, זה יכול להוביל לאי הבנות, החמצת מועדים ובעיות אחרות. כדי להפחית את הסיכון הזה, נקבע פגישות צוות קבועות כדי לדון בהתקדמות, לשתף עדכונים ולטפל בכל בעיה או דאגה. ונשתמש בכלי תקשורת כמו דואר אלקטרוני, אפליקציות הודעות או תוכנות לניהול פרויקטים כדי לשמור על קשר בין פגישות
גישה מוגבלת לחומרי מחקר	בהתאם לנושא המחקר, ייתכן שיהיה קשה לגשת למידע או נתונים רלוונטיים. כדי להתגבר על סיכון זה, פתח תוכנית מחקר מקיפה הכוללת מגוון משאבים ואסטרטגיות חיפוש. השתמש במאגרי מידע מקוונים, בכתבי עת אקדמיים ובמשאבים אחרים כדי לאסוף מידע, ושקול לפנות למומחים במשאבים לקבלת עצות או תובנות.
קשיים טכניים	אחת משיטות המחקר שלנו היא חקר מאגרים, שיטה זו מציפה לא מעט אתגרים טכנולוגיים בעיבוד המאגר והפיכת כל המידע שהוא מכיל לכדי ידע רלוונטי עבור המחקר. על מנת לגשר על הסיכון הזה, נוכל להעזר באנשי מקצוע שבקיאיים בעבודה עם מידע מובנה באופן הזה, פניה לשירות לקוחות של בעלי המאגר עצמו ואפילו חיפוש של מאגר חליפי.
קונפליקטים אישיים או מגבלות זמן	לחברי הצוות עשויים להיות סדרי עדיפויות מתחרים או קונפליקטים אישיים שעלולים להשפיע על יכולתם לתרום לפרויקט. כדי לנהל את הסיכון הזה, נערוך תיאום ציפיות ותאריכים ברורים לכל חבר צוות, ונעבוד יחד כדי לתעדף משימות ואחריות. נעודד תקשורת פתוחה ונעניק תמיכה וגמישות בעת הצורך.

ניהול משאבים - ינוהל בקובץ נפרד.

את טבלת ניהול המשאבים יש לנהל **בקובץ אקסל נפרד** (ניתן להורידו במאמא).
יש למלא את הטבלה במשימות ובמשאבים הנדרשים לצורך הכנת הסמינר.
באקסל המשאבים מופיעה דוגמה חלקית וקצרה לדרך שבה יש למלא את המשימות בטבלה.
הקפידו לאגד מספר משימות תחת חבילת עבודה אחת וספרו את המשימות בהיררכיה
המתאימה של חבילת העבודה, כמודגם בטבלה.

לתשומת הלב: המשימות שתכללנה בתוכנית הן אך ורק משימות שתבצעו **לאחר אישור**

התוכנית, ולא קודם.

לפי אורכו הקלנדרי של הסמסטר, הוסיפו או מחקו עמודות של שבועות עבודה בטבלה.
כמו-כן, הוסיפו שורות הנחוצות לכם לפי פירוט חבילות עבודה ומשימות. בכל מקרה אין
לשבש את העמודות שאינן שבועות העבודה.
חשוב! על מנת לודא התקדמות סבירה בהכנת העבודה, הקפידו לבנות תוכנית כך שעד
למועד מפגש **ניצוצות** (אם יש שניים אז המוקדם יותר), תשלימו לפחות את סקירת הספרות
המלאה כולל רשימת המקורות שמוזכרים בה, ותשלחו למנחה המקצועי שלכם להערותיו.
כמו-כן להיות במצב של לקראת סיום תכנון 2 שיטות המחקר כך שאם אתם משתמשים
בשאלון, אז שלחתם לפחות גרסה ראשונה למנחה המקצועי לאישורו.
ובאופן דומה, לקראת מפגש **עמיתים** (אם יש שניים אז המוקדם יותר) תהיו במצב של לאחר
סיום איסוף המידע של שתי השיטות, וכן אחרי ששלחתם למנחה המקצועי את שני הפרקים:
מטרת המחקר ושיטת המחקר.

את אקסל המשאבים יש להגיש במאמא **לצד** תוכנית העבודה המאושרת, לאחר שקובץ
טופס תוכנית העבודה, הכולל חתימת המנחה המקצועי הומר לקובץ PDF.
כמו-כן, יש להדפיס את תוכנית העבודה המאושרת במלואה, כולל חתימת המנחה המקצועי
וטבלת המשאבים המאושרת כנספח של התוצר הסופי של הסמינר.

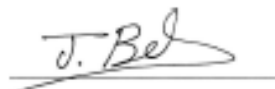
חלק ב' (למילוי על ידי המנחה המקצועי/ת)

הערה למנחה המקצועי/ת:

נא למלא, להוסיף חתימה דיגיטלית (עדיף כ"צירוף"), להוסיף הערות אם יש, ולשמור כקובץ PDF. כנ"ל נדרש גם באקסל של טבלת המשאבים. את שני קבצי ה-PDF נא לשלוח באימייל לסטודנטים.

תוכנית העבודה מאושרת על ידי.

שם המנחה: גוש בכר



חתימה:

תאריך: 1 יוני 2023

הערות:

נספח ז' – טבלת המשאבים

טבלת ניהול המשאבים - פיצור השעות לכל המשימות בפירוט שבועי (חשוב! רק משימות שאחרי אישור התוכנית הזאת)																			
#	תאור	#	תאור	מטרת קדם	סדר	שם	סדר	שם	סדר	שם	סדר	שם	סדר	שם	סדר	שם	סדר	שם	סדר
1	קריאת מאמרים וכתובת סקירת ספרות	1.1	סקירת ספרות	11	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
1.2	רשימת מקורות	1.1	רשימת מקורות	13	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
1.3	ניסוח מונח המחקר	1.1	ניסוח מונח המחקר	6	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
2	תכנון שיטת המחקר	2	תכנון שיטת המחקר	19.5	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
2.1	חקירה מעמיקה של המאגר	56	חקירה מעמיקה של המאגר	56	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
2.2	ביצוע Benchmarking	37	ביצוע Benchmarking	37	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
2.3	ייצוג נתונים סיכומיים	2.2/1	ייצוג נתונים סיכומיים	20	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
2.4	ניתוח הנתונים	2.3	ניתוח הנתונים	17	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
3	ממצאים	3	דיווח הממצאים	9.5	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
3.1	ניתוח הממצאים או מור שאלות המחקר	2.4	ניתוח הממצאים או מור שאלות המחקר	15	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
3.2	ניתוח הממצאים או מור שאלות קודמת	2.4/1.1	ניתוח הממצאים או מור שאלות קודמת	15	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
3.3	כתובת מודל דיון ומסקנות	21	כתובת מודל דיון ומסקנות	21	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
4	התבוננות להמשך	4	כתובת חקירה	13	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
4.1	מסקנות	10	מסקנות	10	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
4.2	שער	4	שער	4	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
4.3	איושקס	5	איושקס	5	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
	סקירת העבודה	12	סקירת העבודה	12	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
0	107.5	אביר	אביר	107.5	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
0	104	אביר	אביר	104	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר
0	105.5	אביר	אביר	105.5	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר	אביר

טבלת ניהול המשאבים מאושרת על ידי:	
שם המנחה:	מר ג'וש בכר
תאריך:	March 20 2023
חתימה:	

נספח ח' – הצהרה על הסכמה לפרסום העבודה

הסכמה לפרסום עבודה

שם העבודה:	20232C33
סוג העבודה:	סמינר
שם המנחה המקצועי:	גיוש בכר

האם תהיו מוכנים שנשלח את עבודתכם לתחרות או ליחסי ציבור?

בכדי למנוע אי הבנה בנדון, אנו מבקשים מכם לחתום על הסכמתכם לכך.
מכיון שעבודה היא משותפת לצוות של סטודנטים, הרי שרק אם כל אחד מצוות הכותבים יסכים, אזי העבודה תחשב ככזאת שניתנה הסכמה לפרסומה.
לפיכך, על כל אחד מהסטודנטים השותפים לציין אם הוא מסכים או לא מסכים לפרסום העבודה ולחתום.

שם סטודנט	ת.ז.	הסכמה לפרסום ?	תאריך	חתימה
גיא ארביב	208542332	כן	31/05/2023	
דניאל סולטן	208611020	כן	31/05/2023	
אמרי עוזרי	204469936	כן	31/05/2023	

נספח ט' – הצהרות על הכנה עצמית של העבודה

טופס הצהרה על הכנה עצמית של עבודה

סמינר / פרויקט / סדנה

עבודה זו נדרשה לאפשר לסטודנטים בשלב לימודים מתקדם זה ליישם את הידע והמיומנות שרכשו במהלך לימודיהם. בעבודה זו צריכים לבוא לכדי ביטוי הכישורים האקדמיים, כגון: יכולת קריאה, הבנה וניתוח של טקסטים מדעיים, אינטגרציה של סוגי ידע שונים, חשיבה ביקורתית, כושר תכנון מחקר וביצועו (במקרים מסוימים) ולבסוף, כתיבה מדעית רהוטה.

העבודה חייבת להיות ברובה המכריע **יצירה עצמית** של הסטודנטים. כדי להבחין בין תרומתם לבין תרומותיהם של אחרים, וכדי למנוע פגיעה ב"קניין הרוחני" של כותבים שעליהם מסתמכת העבודה, חייבים הכותבים להקפיד על ציון המקורות שעליהם הסתמכו. במילים אחרות, יש להצהיר מה המקור של כל אמירה או ידע שנלקח מאחרים. בכלל זה: ציטוטים ישירים של אמירות או ממצאים, רעיונות, דעות ופרשנות של אנשים אחרים. סטייה מכללי הציטוט והפנייה, לא כל שכן נטילה ללא ציון ראוי של חלקי עבודה או עבודה שלמה של כותבים אחרים, מתפרשת לחומרה כניסיון להציג דברי אחרים כדברי הכותבים עצמם והיא בבחינת עבירה חמורה על כללי האתיקה המדעית.

כדי למנוע אי הבנה בנדון אנו מבקשים ממך לחתום על ההצהרה הבאה:

אני _____ אמרי עוזרי ת.ז. _____ 204469936 מצהיר/ה בזאת כי העבודה הסמינריונית / הפרויקט / הסדנה (לסמן את הרלוונטי) המצורפת בזאת היא פרי יצירתי **העצמית** ונכתבה על פי כללי ציטוט והפנייה המקובלים באקדמיה. כמו כן, אני מצהיר/ה כי ידוע לי שהגשת עבודה אשר חלקים רבים ו/או משמעותיים ו/או מהותיים בה הועתקו מעבודה אחרת היא עבירה, וכי אם יתגלה כי עברתי עבירה זו, תוגש נגדי תלונה על כך לועדת המשמעת של מכללת תל אביב יפו.

תאריך 31.05.2023 חתימה _____ - 

טופס הצהרה על הכנה עצמית של עבודה

סמינר / פרויקט / סדנה

עבודה זו נדרשה לאפשר לסטודנטים בשלב לימודים מתקדם זה ליישם את הידע והמיומנות שרכשו במהלך לימודיהם. בעבודה זו צריכים לבוא לכדי ביטוי הכישורים

האקדמיים, כגון : יכולת קריאה, הבנה וניתוח של טקסטים מדעיים, אינטגרציה של סוגי ידע שונים, חשיבה ביקורתית, כושר תכנון מחקר וביצועו (במקרים מסוימים) ולבסוף, כתיבה מדעית רהוטה.

העבודה חייבת להיות ברובה המכריע **יצירה עצמית** של הסטודנטים. כדי להבחין בין תרומתם לבין תרומותיהם של אחרים, וכדי למנוע פגיעה ב"קניין הרוחני" של כותבים שעליהם מסתמכת העבודה, חייבים הכותבים להקפיד על ציון המקורות שעליהם הסתמכו. במילים אחרות, יש להצהיר מה המקור של כל אמירה או ידע שנלקח מאחרים. בכלל זה : ציטוטים ישירים של אמירות או ממצאים, רעיונות, דעות ופרשנות של אנשים אחרים. סטייה מכללי הציטוט והפנייה, לא כל שכן נטילה ללא ציון ראוי של חלקי עבודה או עבודה שלמה של כותבים אחרים, מתפרשת לחומרה כניסיון להציג דברי אחרים כדברי הכותבים עצמם והיא בבחינת עבירה חמורה על כללי האתיקה המדעית.

כדי למנוע אי הבנה בנדון אנו מבקשים ממך לחתום על ההצהרה הבאה :

אני גיא ארביב ת.ז. 208542332 מצהיר/ה בזאת כי העבודה הסמינריונית / הפרויקט / הסדנה (לסמן את הרלוונטי) המצורפת בזאת היא פרי יצירתי **העצמית** ונכתבה על פי כללי ציטוט והפנייה המקובלים באקדמיה. כמו כן, אני מצהיר/ה כי ידוע לי שהגשת עבודה אשר חלקים רבים ו/או משמעותיים ו/או מהותיים בה הועתקו מעבודה אחרת היא עבירה, וכי אם יתגלה כי עברתי עבירה זו, תוגש נגדי תלונה על כך לועדת המשמעת של מכללת תל אביב יפו.



חתימה

תאריך 31.05.2023

טופס הצהרה על הכנה עצמית של עבודה

סמינר / פרויקט / סדנה

עבודה זו נדרשה לאפשר לסטודנטים בשלב לימודים מתקדם זה ליישם את הידע והמיומנות שרכשו במהלך לימודיהם. בעבודה זו צריכים לבוא לכדי ביטוי הכישורים האקדמיים, כגון : יכולת קריאה, הבנה וניתוח של טקסטים מדעיים, אינטגרציה של סוגי ידע שונים, חשיבה ביקורתית, כושר תכנון מחקר וביצועו (במקרים מסוימים) ולבסוף, כתיבה מדעית רהוטה.

העבודה חייבת להיות ברובה המכריע **יצירה עצמית** של הסטודנטים. כדי להבחין בין תרומתם לבין תרומותיהם של אחרים, וכדי למנוע פגיעה ב"קניין הרוחני" של כותבים שעליהם מסתמכת העבודה, חייבים הכותבים להקפיד על ציון המקורות שעליהם הסתמכו.

במילים אחרות, יש להצהיר מה המקור של כל אמירה או ידע שנלקח מאחרים. בכלל זה: ציטוטים ישירים של אמירות או ממצאים, רעיונות, דעות ופרשנות של אנשים אחרים. סטייה מכללי הציטוט והפנייה, לא כל שכן נטילה ללא ציון ראוי של חלקי עבודה או עבודה שלמה של כותבים אחרים, מתפרשת לחומרה כניסיון להציג דברי אחרים כדברי הכותבים עצמם והיא בבחינת עבירה חמורה על כללי האתיקה המדעית.

כדי למנוע אי הבנה בנדון אנו מבקשים ממך לחתום על ההצהרה הבאה:

אני _____ דניאל סולטן _____ ת.ז. _____ 208611020 _____ מצהיר/ה בזאת כי העבודה הסמינריונית / הפרויקט / הסדנה (לסמן את הרלוונטי) המצורפת בזאת היא פרי יצירתי **העצמית** ונכתבה על פי כללי ציטוט והפנייה המקובלים באקדמיה. כמו כן, אני מצהיר/ה כי ידוע לי שהגשת עבודה אשר חלקים רבים ו/או משמעותיים ו/או מהותיים בה הועתקו מעבודה אחרת היא עבירה, וכי אם יתגלה כי עברתי עבירה זו, תוגש נגדי תלונה על כך לועדת המשמעת של מכללת תל אביב יפו.



חתימה

תאריך 31.05.2023