Azrieli
College of Engineering
Jerusalem

עזריאלי
מכללה אקדמית להנדסה
ירושלים

המחלקה להנדסת תוכנה

פרויקט גמר – תשע"ח

שיתוף מפתחות מבוסס הסתברות עבור IOT

Probability Based Keys Sharing for IOT

מאת

שרה ספרין

רעות נגר

מנחה אקדמי: דר' גיא לשם	אישור:	תאריך:
רכז הפרויקטים: דר' אסף שפנייר	אישור:	תאריך:

מערכות ניהול הפרויקט:

#	מערכת	מיקום
1	מאגר קוד	https://github.com/reutnagar/distributed-RSA-for-IoT
2	יומן	https://trello.com/b/DkjV5sEx/a
3	סרטון	https://drive.google.com/file/d/1yG61mZb-n9U0TWnGObKPunGcjKk5-YSS/view

תוכן הענינים

תקציר

מסמך זה מתאר את פרויקט הגמר שלנו, ומתעסק במציאת פיתרון אבטחה למכשירים קטנים בעלי חיבור אלחוטי לרשת.

מילון מונחים

- מכשיר IoT: מכשיר עם יכולות חישוב קטנות, בעל יכולת שידור אלחוטי
- צומת: מכשיר IoT שנמצא ברשת
- מאסטר/מנהיג: צומת שנבחר לתפקיד יצירת המפתחות והפצתם ברשת

מבוא

אבטחת מידע

אבטחת מידע (באנגלית: Information Security) היא ענף העוסק בהגנה של מידע ומערכות מידע מפני כל גישה למידע שאינה ע"י גורמים מאושרים, לכך עליה לספק את שלושת הבאים: סודיות, שלמות וזמינות של המערכות והמידע בהן. אבטחת מידע היא תחום מתקדם מאוד בימינו. האפשרויות הרבות שעומדות לתוקפים של מערכות ממוחשבות להזיק בתחומים כמו פרטיות, פיננסים וביטחון מניעה את האנושות להגן ככל האפשר על מערכות אלו. מושקעים משאבים רבים בעיצוב המערכות, קידוד ותחזוקה שוטפת כדי לאתר פרצות אבטחה מוקדם ככל האפשר. עם התקדמות היכולות של התוקפים נדרשות לעתים פריצות דרך מצד קהילת המפתחים ולכן אבטחת מידע זהו תחום שמושקעים בו כסף ומשאבים רבים במיוחד על מנת לחקור ולגלות דרכי הגנה חדשות ויעילות יותר להתמודדות מול התוקפים[1].

כוח יישומי חשוב באבטחת המידע היא קריפטוגרפיה. זהו ענף במתמטיקה ומדעי המחשב העוסק במחקר ופיתוח שיטות אבטחת מידע ותקשורת נתונים, ומייצר שיטות למימוש בפועל של מושגי אבטחת המידע. הגנה זו מבוצעת על ידי הצפנת המידע בעזרת פונקציית הצפנה כלשהי, ושימוש במפתח (Key) שהוא רצף תווים סודי שאינו ידוע לתוקף. הצופן (Cipher) הוא כתב הסתר שמתקבל על ידי הפעלת פונקציית ההצפנה על טקסט הקלט. פונקציה הצפנה אדיאלית היא כזו שבהינתן הצופן- הפלט, לא ניתן להסיק ממנו מידע על הקלט.

מכשירי IoT

בעולם הטכנולוגי כיום קיימת מגמה מואצת להפוך כל מכשיר המכיל שבב אלקטרוני לבעל יכולת חיבור לרשת. כבר כיום ניתן לראות מכשירים מכל הסוגים שקיימת בהם אפשרות חיבור לאינטרנט. לדוגמה: מצלמות, מדפסות, שלטי מזגן ועוד. החזון לחבר כל מכשיר חשמלי לרשת נובע מן הרצון שמכשירים כאלו ישדרו למכשירים ומערכות

סביבם את המידע שבידם, ויקבלו מידע מן הרשת לגבי אירועים ותרחישים שונים. הודעות אלו ישדרגו את יכולותיהם ופעילותם והם יוכלו להתנהג בצורה יותר "חכמה", להסיק מסקנות ולפעול אוטומטית על פיהם ללא התערבות אנושית. לדוגמה, כאשר השבב של מערכת החלונות המותקנת ב"בית חכם" קולט שידור ממערכת המיזוג על הפעלת המזגן, הוא יודע לסגור את החלונות המתאימים באופן אוטומטי כדי לייעל את פעולת המיזוג.

מגמה זאת נקראת:"אינטרנט של דברים" (IoT- Internet Of Things). זוהי רשת של חפצים פיזיים, או "דברים" המשובצים באלקטרוניקה, תוכנה וחיישנים המאפשרים תקשורת מתקדמת בין החפצים ויכולות איסוף והחלפת מידע. רשת זו צפויה להוביל לאוטומציה בתחומים רבים. כיום ישנה התפתחות נרחבת בתחום ה IoT, למשל "הבית החכם", שבו כל המכשירים מחוברים לרשת וניתן להפעיל אותם בשלט רחוק ולתאם בין פעולותיהם. תחום הIoT צפוי לגלגל מחזור של כ20 ביליון דולר בשנת 2020, על פי הודעת חברת 'סיסקו' העולמית, ומושקעים בו משאבים רבים לפיתוח מצד החברות בתחום החומרה והתוכנה.

לקראת השינוי הזה יידרש שיפור גם ברמות האבטחה המקובלות כיום בקרב מכשירים כאלו, שעצם חיבורם לרשת חושף אותם להתקפות חיצוניות והם עלולים להוות טרף קל לתוקף. בפרויקט זה נתמקד בחקירת פתרונות אבטחה, בפרט בשימוש בהצפנת RSA, עבור תחום ה"אינטרנט של הדברים" ויצירת פתרונות אבטחה ייעודיים עבורו המתחשבים בחוזקות והחולשות של המוצרים הקיימים בשוק[3].

תיאור הבעיה

בהבנה של הצורך הבסיסי באבטחה ראויה למידע המשתמש והכרה במגבלות המשאבים של מכשירים אלקטרוניים קטנים, ניתן להבחין במספר בעיות ביישום אבטחה במכשירי IoT:

- מכיון שמכשירי הIoT הינם מכשירים זולים וקטנים לרוב, ומאופיינים ביכולות עיבוד חלשות, ומשאבים נוספים דלים כמו: זיכרון, שידור וחישה, לכן להטמיע בהם יכולות אבטחה מתקדמות כמו שקיימות במערכות מחשבים גדולות זוהי משימה קשה וכמעט לא נתמכת מבחינת החומרה של ה IoT.
- מכיוון שהשימוש ב IoT הוא כמכשירים שיש להם בדרך כלל תפקיד עיקרי ייעודי והחיבור לרשת רק מוסיף להם יתרון, הם לא נתפסו עד היום בציבור כבעלי ענין עבור תוקפים. אך עם השימוש הגובר בהם מיום ליום נוצלו פרצות האבטחה שבמכשירים מסוג זה לתקיפת מערכות רגישות, כמו מצלמות אבטחה, מדפסות ועוד. לכן נדרש פיתרון שיספק אבטחה הולמת כנגד נסיונות פריצה אפשריים.

- פתרונות האבטחה שכן מיושמים כיום בתחום ה IoT הים ייעודיים עבור מכשיר מסוג מסוים, ומוטמעים על ידי היצרן. לא נלקחת בחשבון התאמה לשוק המוצרים הכולל של IoT, ולכן פתרונות אלו אינם מתאימים מבחינת תצורה, מגבלות משאבים וייעוד, עבור כל התחום.

על מנת לפתור את הבעיות הנ"ל נדרש פיתוח אבטחתי חדש שיענה על דרישות האבטחה הגבוהות בשוק, יחד עם המגבלות המאפיינות את מכשירי הIoT.

תיאור הפתרון

הפתרון שאנו מציגות הוא שיתוף מפתחות בין ההתקנים ברשת באופן הסתברותי, הנעשה רק ע"י המכשירים ברשת. מפתחות אלו ישמשו להצפנת התקשורת בין המכשירים.

פרוטוקול "לחיצת יד" חדש עבור רשת התקני IoT

על ידי מערכת חדשה לניהול מפתחות המבוססת על שיתוף מפתחות הסתברותי בין ההתקנים.

להל"ן הפרוטוקול:

1. צור קבוצה של התקני IoT עם תקשורת בינהם.
2. הגדר מנהיג לקבוצה (ההתקן בעל הכוח הרב ביותר).
3. עבור כל התקן בקבוצה, המנהיג נדרש לשלוח תת קבוצה של מפתחות (k) מתוך מאגר מפתחות שהוא נדרש לייצר.

גודל המאגר:

המנהיג צריך לקבוע מה יהיה גודל המאגר, P מתבסס על גודל הזיכרון הפיזי של המכשיר, ואת ההסתברות הנדרשת על ידי המערכת שנועדה להבטיח חפיפה (לפחות מפתח משותף אחד בין 2 התקני IoT).

האלגוריתם למציאת גודל תת הקבוצה:

M - גודל הזיכרון הפיזי (לדוג' 32M).

n - מספר התקני ה-IoT ברשת.

Pc - ההסתברות שלשני התקני IoT יש קישוריות באופן ודאי.

k - גודל הקבוצה של המפתחות מתבסס על M. k מוגדר ע"י הגבול של M.

n' - גודל ה'שכונה' של צומת ברשת האלחוטית.

p' - ההסתברות שלשני צמתים קיים מפתח משותף.

חשב את c, כאשר c קבוע:

$$P_c = e^{e^{-c}} \rightarrow c = -\ln(\ln(P_c))$$

חשב את p: ההסתברות ששני צמתים מחוברים ישירות:

$$p = \frac{\ln(n)}{n} - \frac{c}{n}$$

חשב את d: הערך המצופה של הצומת:

$$d = p(n-1)$$

חשב את p' :

d ניתן מהשלב הראשון ו- n' נתון, מספר הצמתים בשכונה של הצומת:

$$p' = \frac{d}{n'-1}$$

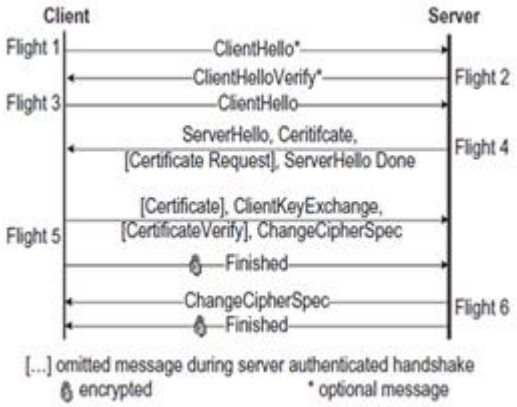
בהתחשב בערך של p', השתמש במשוואה הבאה כדי לחלץ את הערך של P:

$$p' = 1 - \frac{(1-\frac{k}{P})^{2(P-k+1/2)}}{(1-\frac{2k}{P})^{2(P-2k+1/2)}}$$

מ-p' , כעת נוכל לחשב את P (גודל המאגר)[4].

4) בהינתן גודל המאגר, P, כמו שחושב באלגוריתם המוצג בשלב 3, המנהיג צריך לייצר מאגר של מפתחות בגודל P (לפחות 1000), לכל מפתח במאגר יוסף מספר סידורי (index).

5) המנהיג יוצר 'לחיצת יד' מאומתת לחלוטין עם כל הקבוצה.



6) בהתבסס על תקשורת 'לחיצת היד' המאומתת לחלוטין, המנהיג שולח לכל חבר בקבוצה תת קבוצה שונה של מפתחות.

7) בהתבסס על תת קבוצת המפתחות שכל התקן מחזיק, 'לחיצת יד' מאומתת חדשה תהיה קלה.

8) המנהיג ישלח תת קבוצה חדשה של מפתחות לכל התקן שיצטרף לקבוצה.

הפתרון שלנו מאפשר להימנע מניהול האבטחה באמצעים חיצוניים לרשת, ממומש כולו ע"י ההתקנים הנמצאים ברשת, ומספק אבטחה טובה מספיק עבור התקשורת בין המכשירים.

תיאור הכלים המשמשים לפתרון

בפרויקט זה נעבוד עם מכשיר Linkit Smart , מכשיר בעל קלט, פלט אלחוטיים ויכולת עיבוד קטנה על מנת לבדוק וליישם את האלגוריתם.

הכתיבה תיעשה בשפת Python , על מנת שנוכל להעזר בספריות שקיימות בה עבור: תקשורת, הצפנה, ו multi-threading.

ארכיטקטורת המימוש

הארכיטקטורה והמימוש בתוכנה זו הינם מורכבים ביותר, כי אנו כותבות תוכנה זהה עבור שני צמתים בעלי תפקיד אחר לגמרי ברשת: "מאסטר" ו"לקוח", תוך שמירה על קיום מופע אחד בלבד של "מאסטר" ברשת.

"מצבי הרשת" מוגדרים לפי שלבי האלגוריתם:

1. אתחול: חיבור המכשירים הקיימים לרשת, וקביעת מאסטר זמני.

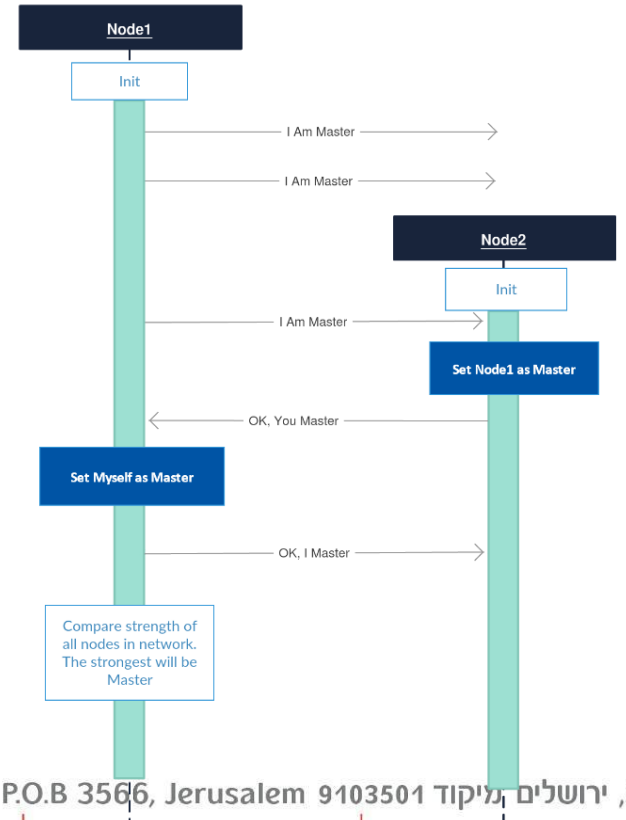
2. קביעת מאסטר: המאסטר הזמני מזהה את הצומת עם היכולות הגבוהות ביותר ומעביר אליו את ההנהגה.
3. יצירת מפתחות: המאסטר יוצר מפתחות לפי האלגוריתם.
4. חלוקת מפתחות: המאסטר שולח תת קבוצה של מפתחות לצמתים ברשת.
5. רשת בטוחה: משלב זה הצמתים יכולים לתקשר בינהם בצורה מאובטחת.

אתחול

לשם הפשטה החלטנו שהראשון שמכריז על עצמו כמנהיג הוא נהיה כזה, ובהמשך הוא מחליט לפי חישוב היכולות של הצמתים ברשת מי הוא החזק ביותר ומכריז עליו כמאסטר.

בהפעלת המכשיר הוא יהיה במצב "לקוח זמני", ויאזין להודעות ברשת המכריזות על מאסטר אחר. תוך כדי הוא ישדר בכל שניה הודעה ברשת שהוא מאסטר.

- לקוח: אם קיבל הודעה ממישהו אחר "אני מאסטר"- יעבור למצב "לקוח", יפסיק להכריז על עצמו כמאסטר ויחזיר הודעת אישור למאסטר. מעתה יאזין להודעות רק מהמאסטר, כדי לקבל את המפתחות ושאר התהליך עד לסיום הקמת רשת מאובטחת.
- מאסטר: אם מכשיר קיבל אישור על היותו מנהיג הוא עובר למצב "מאסטר". הוא מגדיר את מצב הרשת כ:"אתחול", וממשיך לשלוח "אני מאסטר" ברשת במשך זמן אתחול שמוגדר מראש. לאחר מכן הוא קובע את מצב הרשת כ:"קביעת מאסטר".



עד עתה מימשנו את שלב האיתחול בהצלחה. בהמשך הפרויקט נוסיף עדכון לשלבים הבאים.

תוכנית בדיקות

בדיקות מקיפות של כל פונקציות המערכת ע"מ לוודא נכונות, מקרי קצה, מקרים חריגים וכו'.

בדיקות פונקציונליות

- בדיקת הקמת רשת, בה כל הרכיבים מצליחים לתקשר אחד עם השני.
- בדיקה שברשת קיים מנהיג אחד לכולם.
- המנהיג מייצר בריכת מפתחות, בגודל הנדרש לפי האלגוריתם.
- כל אחד מהצמתים ברשת מקבל תת קבוצה של מפתחות לפי האלגוריתם.
- כל שני צמתים ברשת חולקים לפחות מפתח אחד משותף.
- תקשורת מוצפנת בין שני צמתים עוברת בהצלחה (אופציונלי).

בדיקות מערכת

- אינטגרציה בין כל אחד מהשלבים בתהליך הקמת רשת מאובטחת עוברת בהצלחה.
- הרשת יציבה והתקשורת מתבצעת ללא הפרעות.
- האם ניתן להוסיף צומת חדש לאחר הקמת הרשת והפצת המפתחות.
- האם לאחר כיבוי של אחד הצמתים ניתן להקים את הרשת מחדש.

בדיקות תאימות

- בדיקה שהתהליך עובד על מכשירי IoT בעלי חומרה/תוכנה שונה (אופציונלי, תלוי באספקת מכשירים כאלו מן המנחה).

בדיקות תחזוקה (Maintainability)

- האם ניתן לעדכן או לתקן את התכנה אחרי הוצאתה לאור.
- האם הקוד כתוב בצורה פשוטה, ברורה ומתועדת.

מסקנות

במהלך הפרויקט אנו שמות דגש על מחשבה ותכנון לפני כל ביצוע בפועל. במיוחד לפני כתיבת הקוד, שם השקענו רבות בהגדרת מצבים ברשת, בצומת "לקוח" ובצומת

ה"מאסטר". גילינו שהעלאת החלטות על הכתב וניסוחן מקלה על המימוש, מונעת בלבול ומאפשרת התמקדות בפתרון הבעיה.

לאחר התנסות בכתיבת התוכנה נוכל להצביע על שתי בעיות עיקריות הקיימות כרגע במימוש שלנו:

- מבנה הודעות ברשת הוא קבוע, ולא ניתן במתכונת הקוד הנוכחית להוסיף נתונים דינמיים להודעות. נצטרך לשנות זאת כדי לאפשר שליחת מפתחות ברשת וכו'.
- הקוד הקיים אינו משתמש באופן אופטימלי בתכונות של תכנות מונחה עצמים. נצטרך לבצע ניתוח מעמיק כדי לזהות את הבעיות בקוד מבחינה זו ולגבש פיתרון מתאים.

בשלב הבא נמשיך לממש את התוכנה כפי המתוכנן עם דגש על קוד יעיל ונכון, ופתרון הבעיות לעיל.

סקירת עבודות דומות בספרות והשוואה

סקרנו מס' פתרונות אפשריים שהוצעו עבור אבטחה ב- IoT, אולם לכל אחד מן הפתרונות קיימים חסרונות:

- שימוש בענן

ישנו פתרון אבטחה להתקני IoT המסתמך על שימוש בענן על מנת להשיג את האבטחה הרצויה. כל התקן ברשת יתחבר לשירות בענן שיתמוך בניהול האבטחה של כל ההתקנים, ומולו יתבצעו פעולות האימות וההצפנה[5].

פתרון זה דורש ניהול של שירות בענן, וזו תקורה שדורשת משאבים נוספים, בנוסף, יהיה צורך בהגדרת ספקים אמינים לכזה שירות, ופתרון במקרה של התחזות. במחקר שלנו אנו מנסים להביא את השליטה באבטחה להיות בבלעדיות אצל רשת ההתקנים המקומית, ללא קישור לשירות חיצוני.

- שימוש בTPM:

פתרון זה מסתמך על מכשיר הTPM לביצוע פעולות קריפטוגרפיות ונתינת שירותי הצפנה למכשירים ברשת[6]. זה נראה אמנם רעיון ישים, אך החיסרון בו שדרוש מכשיר TPM כזה עבור כל רשת IoT, וזה גובה עלות נוספת. בפרויקט שלנו אנו ממשים פתרון אבטחה שמתבסס אך ורק על מכשירים הקיימים ברשת, ללא עלות נוספת.

- ארכיטקטורת IoT מאובטחת לערים חכמות המטפלת בפגיעויות במערכות IoT:

הארכיטקטורה כוללת רשתות שחורות ומערכת ניהול מרכזית (KMS) המספקות סודיות, שלמות, פרטיות והפצה מרכזית יעילה. המטרה הייתה לספק שירותי אבטחה הממתנים את הפגיעות של רשתות IoT בשכבות הקישור והרשת, במיוחד עבור נתונים קריטיים.
החסרונות של גישה זו כוללים היעדר פתרון פרטיות להגדרת מיקום המכשיר ואיתור ניתוב חדש עבור צמתים, מה שמוביל לאובדן נתונים.

- ארכיטקטורת SDN לפיתוח יישומי IoT:

ארכיטקטורת SDN אומצה על מנת לספק בסיס לפיתוח מערכת מאובטחת שמאפשרת למנהלי מערכות להציג את העולם באופן גלוי של איומים אפשריים להתקפות ברשת ה- IoT ולספק להם את הזכות לשלוט ברשת מפני האיומים.
עם זאת, אבטחה, מדרגיות ואמינות הן חלק מהחסרונות של רשתות SDN. ההפרדה בין מטוסי הבקרה והנתונים של ה- SDN גורמת לביצועים ירודים בעיבוד חבילות, אשר מובילה לבעיות משמעותיות, כגון עיכוב או אובדן של חבילות והתקפות DoS (DDoS).

- ארכיטקטורת אבטחה חדשה המבוססת על SDN עבור ה- IoT, הידועה גם בשם תחום ה- SDN באמצעות בקרי הגבול:

המחברים תיארו כיצד ניתן להשתמש ב- SDN כדי לחבר בין התקני IoT הטרוגניים, כיצד ניתן לשפר את האבטחה של כל דומיין, וכיצד ניתן לחלק את כללי האבטחה מבלי לפגוע בביטחון של כל תחום.
עם זאת, המחברים לא היו מסוגלים להתמודד עם האתגר של הבטחת תעבורה רצויה ולא רצויה והגנה על הארגון, אשר הם החסרונות העיקריים של שימוש בבקרי הגבול.

- פרוטוקול לניהול מפתחות בצורה קלה:

הפרוטוקול תלוי בהתאמות של רכיבי אבטחה שונים ב- IoT כדי להגדיר ערוצי תקשורת מאובטחים ומוגנים עבור IoT. במהלך העברת הנתונים לאורך הערוץ, הפרוטוקול מבטיח סודיות נתונים ואימות צומת מוגבל.
עם זאת, פרוטוקול האבטחה מוגבל, ואינו מפרט את ההתאמה הנדרשת בין תקורה לתקשורת לבין מספר צדדים שלישיים[7].

נספחים

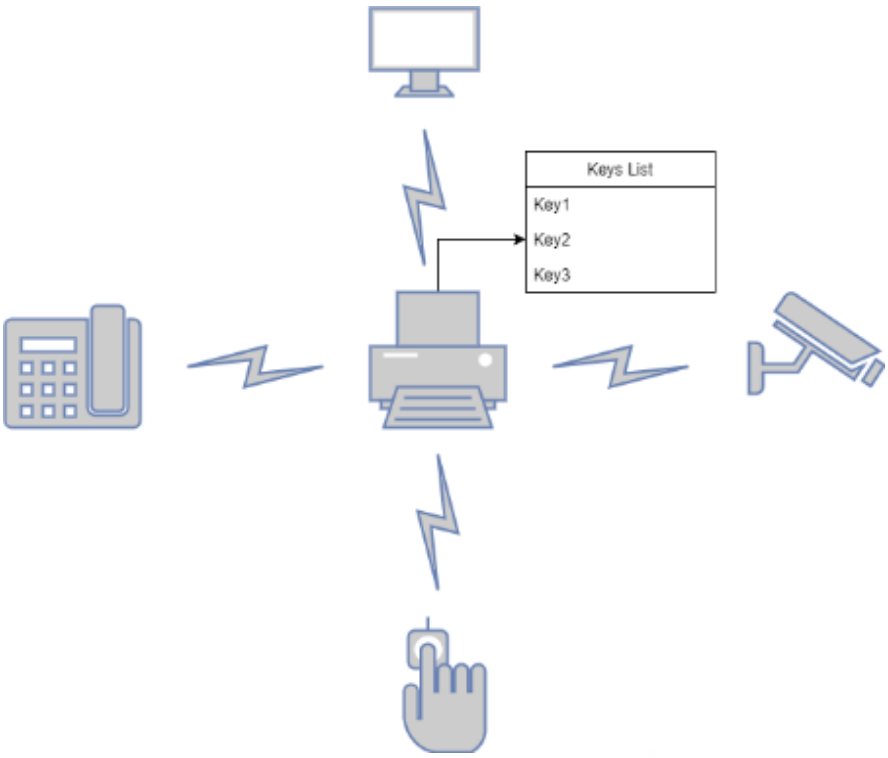
א. רשימת ספרות \ ביבליוגרפיה

[1] "אבטחת מידע – ויקיפדיה [Online]. Available: ."

https://he.wikipedia.org/wiki/אבטחת_מידע.[Accessed: 19-Nov-2017] .
[2] "RSA – ויקיפדיה." [Online]. Available: https://he.wikipedia.org/wiki/RSA. [Accessed: 19-Nov-2017].
[3] "האינטרנט של הדברים – ויקיפדיה." [Online]. Available: https://he.wikipedia.org/wiki/האינטרנט_של_הדברים.[Accessed: 19-Nov-2017] .
[4] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," *Proc. 9th ACM Conf. Comput. Commun. Secur.*, pp. 41–47, 2002.
[5] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 1040–1051, 2018.
[6] H. Hamadeh, S. Chaudhuri, and A. Tyagi, "Area, energy, and time assessment for a distributed TPM for distributed trust in IoT clusters," *Integr. VLSI J.*, vol. 58, no. December 2016, pp. 267–273, 2017.
[7] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, no. March, pp. 10–28, 2017.

ב. תרשימים וטבלאות

מראה רשת בעלת RSA מבוזר ב"בית חכם". בדוגמה זו המכשיר המנהיג הוא המדפסת. בידיו נמצאת רשימת המפתחות, אותה הוא יחלק לשאר המכשירים בבית באמצעות תקשורת אלחוטית.



ג. תכנון הפרויקט

19.1.2018	יצירת קבוצת התקני IoT עם תקשורת בינהם
5.5.2018	הגדרת מנהיג לקבוצה
26.5.2018	שליחת K מפתחות ע"י המנהיג לכל התקן בקבוצה

ד. טבלת סיכונים

#	הסיכון	חומרה	מענה אפשרי
	השערת המחקר אינה נכונה	5	ניתוח ספרות מעמיק
	אי עמידה בזמני מימוש האלגוריתם	4	הערכת יכולות והערכות בהתאם
	דרישות השוק משתנות	3	גמישות בשינוי המחקר והאלגוריתם
	מתפרסם מחקר דומה	4	שמירה על סודיות