

טכנולוגיה בשירות ארגונים



האינטרנט של הדברים: כיצד לבנות פתרון מוצלח

חנן מרקוביץ¹

מבוא

דומה כי המושג "האינטרנט של הדברים" או IoT – Internet of Things נהיה שכיח בעת האחרונה. תחזית עדכנית צופה כי גודל שוק ה-IoT יכפיל את עצמו ל-520 מיליארד דולר עד לשנת 2021, עם שיעור צמיחה שנתי מורכב של 50% לרכיבים מסוימים בשוק (מקור: [Bain & Company, August 08, 2018](#)). מאמר זה מתמקד במהפכת האינטרנט של הדברים, הנוגעת לכל אדם ולשיקולים המרכזיים במימוש מוצלח של פתרון, תוך הבאת דוגמאות מעשיות.

כדרכם של מושגים, יש להגדירם לפני השימוש בהם, ולכן מוצעת ההגדרה הבאה עבור האינטרנט של הדברים: חיבור של אנשים, חפצים וסביבות אל האינטרנט, על מנת לייצר ערך. חיבור אנשים אל האינטרנט נעשה לדוגמה על ידי שימוש בטלפון חכם או שימוש במחשב לביש, כגון צמיד שמנטר דופק ותנועה. חיבור חפצים אל האינטרנט מבוצע במקרים של רכב אוטונומי, רחפן, מזגן ביתי או מכונה בקו יצור. סביבות המחוברות לאינטרנט יכולו לרוב גם אנשים ו/או חפצים. דוגמאות נפוצות הן בית חכם בו הרכיבים בבית ניתנים לשליטה מרחוק, או שדה גידולים העושה שימוש בחיישנים לשיפור היבול. כך גם מפעל ייצור ועיר חכמה המאמצת באופן מתמשך טכנולוגיות לשיפור רווחת תושביה ומבקריה. בחיבור "דברים" אל האינטרנט צפונים יתרונות וחסרונות. יתרונות ה-IoT כוללים גישה וניהול מרוחקים של חפצים, איסוף מידע ממגוון מקורות, אוטומציה ואופטימיזציה של תהליכים והפחתת עלויות. מאידך, החסרונות העיקריים של טכנולוגיות אלו נעוצים בבעיות אבטחה ופרטיות מידע, מורכבות פתרונית מולטי-דיסציפלינאריים ועלויות הטמעה בחלק מהמקרים.

עם מגוון כה רחב של שימושים ויישומי אינטרנט של הדברים, נשאלת השאלה כיצד ניתן לבנות פתרון IoT מוצלח? פתרון המניב ערך ומצליח עסקית וטכנולוגית? לצורך כך, אתמקד בדוגמה של העיר החכמה ובשלושה מרכיבים עיקריים לפתרון מוצלח: המודל העסקי, טכנולוגיית "קצה לענן" – Edge to Cloud ותשתית דיגיטלית לפתרון בעית הסיילואים – Silos².

כדי להבין את המרכיבים הנדרשים לפתרון מוצלח, נתבונן בדוגמת פרויקט [LinkNYC](#). עיריית ניו יורק פרסמה מכרז בו ביקשה להחליף 7,500 טלפונים ציבוריים בעמדות דיגיטליות חכמות. קונסורציום בשם City Bridge המורכב מ: CIVIQ Smartscapes, Qualcomm, Google, זכה במכרז. במסגרת הפרויקט מוחלפים הטלפונים הציבוריים בעמדות חכמות, הנקראות גם קיוסקים דיגיטליים או לינק בקיצור.

¹ יזם פנים-ארגוני, יועץ ומרצה hanan@hananmarkovich.com

² תחומים נפרדים ומבודדים הפועלים בתוך מערכת אחת.



LinkNYC בניו-יורק. צילום: חנן מרקוביץ

כל עמדה חכמה מציעה להולכים ברחוב את השירותים הבאים בחינם: אינטרנט אלחוטי מהיר מבוסס סיב אופטי, טעינת מכשירים ניידים, קבלת מידע עירוני בזמן אמת, הודעות לתושבים, שיחות ברחבי ארצות הברית וכפתור שירותי חירום – 911. נכון להיום, מותקנות למעלה מ-1,700 מערכות בניו-יורק, והתקנות החלו גם בבריטניה במסגרת פרויקט [InLinkUK](#) (בו מתוכננות כ-1,000 מערכות). בכל חודש מותקנות בניו-יורק כ-35 עמדות חדשות, וכיום כ-5 מיליון משתמשים ו-500,000 שיחות טלפון המבוצעות בכל חודש.

מרכיב ראשון: מודל עסקי

המודל העסקי של פרויקט LinkNYC מבוסס על מתן שירותים דיגיטליים לאנשים ברחוב, מימון העלויות באמצעות הצגת פרסומות על גבי שני מסכי 55" וחלוקת רווחים עם העירייה. למעשה, ההתחייבות היא לשלם תשלום מינימלי שנתי ועוד אחוזים ממכירת הפרסומות. נכון לרגע זה, עומד הקונסורציום בתשלום המינימלי. באשר לתשלום אחוזים ממכירת הפרסומות, נחתם הסכם חדש בו נקבע כי הרווח מהפרסומות ישולם בשנה האחרונה לחוזה (אורכו 15 שנים) עם 10% של ריבית.

אם כן, לפנינו דוגמה למימון פרויקט ומודל עסקי המבוסס על מכירת פרסומות. זאת בניו-יורק, העיר כנראה האידיאלית ביותר למודל עסקי מסוג זה בשל תנועה ערה ומתמשכת של אנשים רבים. אך מה בנוגע לערים ואזורים אחרים שאינם כה פופולריים? האם גם שם ניתן לבסס מודל עסקי המבוסס פרסומות? במקרים כאלה קרוב לוודאי שפרסומות בלבד לא יוכלו לממן את עלות הפרויקט, ויידרש מימון מצד העירייה.

לכן, הלקח הראשון לבניית פתרון IoT מוצלח (ולמעשה, נכון לגבי כל עסק) הוא הגדרת מודל עסקי עובד, מודל בו וידאנו שברור מי משלם, בעבור מה, כמה ואיך. נשמע טריוויאלי ועדיין קיימים מקרים רבים בהם חברות מתמקדות יותר בטכנולוגיה שלהן מאשר במודל העסקי. לדוגמה, סמנכ"ל בכיר בחברה מהגדולות בעולם נאם בכנס ערים חכמות וסיפר על פרויקט פיילוט שביצעה החברה באחת הערים בארצות הברית. בתום הפיילוט המוצלח שאלו נציגי החברה את ראש העירייה, האם היה מרוצה מביצועי המערכת. ראש

העירייה ענה בחיוב ושאל כמה יעלה לעבור משלב הפיילוט להתקנה עירונית, ונענה במספר של עשרות מיליוני דולרים. פה הסתיים הקשר בין החברה לעירייה, סיפר נציג החברה בכנס. הנציג סיים באומרו: "אם אינכם יודעים מראש מאיפה יגיע התשלום, אל תתחילו לעבוד". דוגמה נוספת, בפאנל חברות טכנולוגיות בתחום הערים החכמות, התלוננו נציגי החברות על כך שעיריות אינן מוכנות לשלם בעבור הפתרונות שלהם. האמת הלא נעימה היא, שהפתרונות שהוצעו על ידי החברות לא פותרים בעיות אמיתיות שיש לעיריות, ולכן הן אינן מוכנות לשלם. אם לדוגמה נפער בור מסוכן בכביש, האם תשלם העירייה עבור תיקון הכביש? ומה לגבי סדק מסוכן המתפתח בגשר המשמש הולכי רגל, או תאורה בטיחותית בכביש שהתקלקלה ועלולה לגרום לתאונה? במקרים כאלה העירייה חייבת לשלם בשל היותה ניצבת בפני בעיה המחייבת פתרון. אולם כשחברה טכנולוגית מציעה להטמין חיישנים בקרקע לצורך ניטור חנייה – איזו בעיה מהותית זה פותר לעירייה? לחלופין, כשחברה אחרת מציעה להתקין פחי אשפה חכמים שדוחסים את האשפה ומודיעים מתי הם מלאים ועדיין אין לפרויקט היתכנות כלכלית – מדוע שהעירייה תשלם על כך?

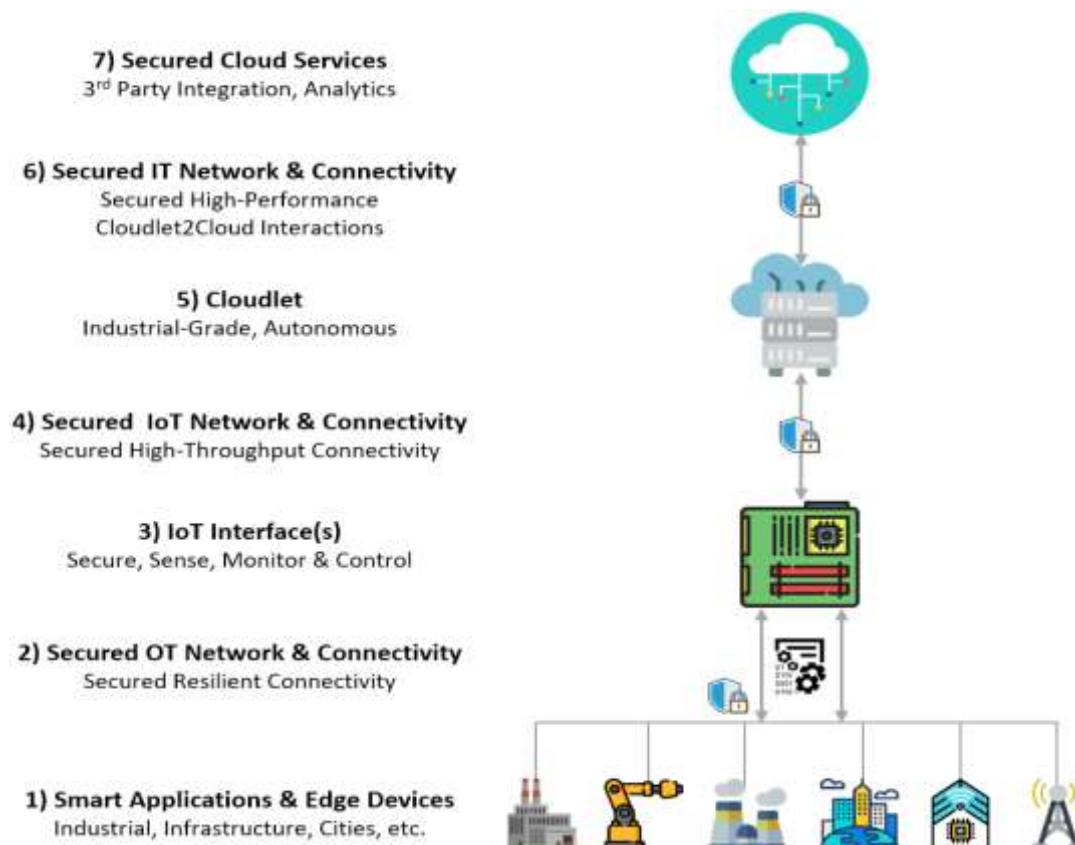
לכן, קריטריון מספר אחד לפתרון IoT מוצלח הוא: מודל עסקי ברור בו לקוחות משלמים עבור הפתרון.

מרכיב שני: הטכנולוגיה

הקריטריון השני לפתרון IoT מוצלח נעוץ כמובן בטכנולוגיה. מכיוון שפתרונות IoT הינם פתרונות מולטי-דיסציפלינאריים, נדרש להתייחס לפתרון לאורך השדרה. מרמת הקצה – Edge – משמע, הרכיבים בעולם הפיזי, ועד לענן – Cloud. לדוגמה, רכיבים או יחידות הקצה – Edge devices – יכולים להיות בני אדם, גוף תאורה, מכונת כביסה, רכב או מכונת ייצור. למעשה, כל רכיב פיזי הצורך או מייצר מידע, מוגדר כיחידת קצה. הענן מתייחס למערכת ניהול מרכזית המאוחסנת בשרתים ובמחשבים מרוחקים ותפקידה לנהל את יחידות הקצה. פתרון משולב ומקיף מרמת יחידות הקצה ועד לענן נקרא בקיצור קצה לענן – Edge to Cloud או E2C.

על מנת להבין מדוע פתרון קצה לענן הכרחי בעולם האינטרנט של הדברים ומה קורה אם לא מיישמים פתרון שכזה, נתבונן בדוגמה האמיתית הבאה. חברה המייצרת עבור תחנות כוח ציוד דוגמת מחליפי חום, גנרטורים, ממירי גז ועוד – נקרא לה חברת P (Power). בכיר בחברה זיהה כי יש מקום רב להתייעלות תהליכית בתחום עיסוק החברה, ועל כן פנה לאחת החברות המוכרות בעולם המתמחה בניתוח מידע בענן לצורך שיתוף פעולה – נקרא לה חברת C (Cloud). לאחר שפנה הבכיר לחברת C, התברר כי אנשי החברה לא ידעו כיצד לסייע. בשיחה עם הבכיר בלטו שני פערים מהותיים בין שתי החברות. הראשון, פער בעולמות התוכן של החברות. חברת C עוסקת בניתוח מידע ומציעה כלים שימושיים רבים בענן. אין לחברת C כל הבנה בעולמות התוכן של חברת P, לא לגבי אופן פעולה של חברות חשמל, או ציוד לתחנות כוח, הבעיות או האתגרים המונחים לפתחן של חברות מסוג זה. לכן נדרש חיבור, גשר בין עולמות התוכן השונים. מנהל מוצר מנוסה יכול לאפיין את הבעיות וההזדמנויות שבחברת P, ולהגדיר פתרון עסקי-טכנולוגי שיוכל להתבסס על הטכנולוגיה שמציעה חברת C. מומחיות מסוג זה שמורה לרוב למנהלי שיווק-מוצר – Product Marketing, אנשים קריטיים בכל ארגון. תפקידם לזהות צרכים בשווקים, אתגרים והזדמנויות, ולבנות מודל עסקי מבוסס טכנולוגיות שייצור מנועי צמיחה חדשים לחברה. הפער השני נעוץ בפתרון הטכנולוגי. בעוד לחברת P מערכות קצה הנמצאות בעולם הפיזי, חברת C מציעה פתרונות בענן. אך מה בנוגע לחיבור הקצה אל הענן? מי מטפל בחיבור יחידות הקצה אל האינטרנט? מי מטפל באבטחת המידע? בבחירה ובמיזוג של חיישנים נוספים אל יחידות הקצה? בניהול אוטונומי של יחידות הקצה כשחיבור לענן אינו אפשרי? בניהול תוכנותי

הנתפר במיוחד לצורכי חברה P: התשובה הקצרה היא – לא חברת C. כדי להבין את גודל הבעיה, דמיינו מצב בו אדם נמצא בלב ים ורואה אי נפלא ומרוחק. האנשים שעל האי מבטיחים שלל של יתרונות לאיש הנמצא בלב ים לוא רק יגיע אליהם. "אבל איך אני מגיע אליכם?", שואל האיש בלב ים. "זו כבר הבעיה שלך", עונים האנשים על האי. כך בדיוק בפתרונות IoT רבים היום, חברות מציעות פתרונות חלקיים בלבד שאינם מטפלים בכל צורכי הלקוח והשלבים ההכרחיים - Edge2Cloud. כדי להבין את מורכבות הפתרון והצורך, נתבונן באיור הבא:



פתרון IoT: Edge2Cloud. מקור: Robust E2C

הפתרון מתחיל ביחידות הקצה (רכיב מספר 1 בדיאגרמה) שיכולות להיות קיוסקים דיגיטליים, קווי ייצור במפעל תעשייתי, מצלמות, אביזרים בבית חכם, רובוטים, רחפנים, גופי תאורה וכדומה.

כל הרכיבים הנמצאים מעל ליחידות הקצה (רכיבים 2-7 בדיאגרמה), מהווים את עמוד השדרה של פתרון ה-Edge2Cloud. כדי לתקשר עם יחידות הקצה, יש ראשית, ליצור חיבור מאובטח בין היחידות לשאר המערכת ועד לענן. פתרון תקשורת מאובטחת (רכיב 2 בדיאגרמה) נדרש כדי לאפשר זרימת מידע מיחידות הקצה, ובאותו הזמן לחסום התקפות אפשריות מיחידות קצה מתחזות. חשוב להבין, כי כל מידע הזורם מיחידות הנמצאות בעולם הפיזי מהווה מקור אפשרי לחדירה ולפגיעה במערכת ה-Edge2Cloud. לכן יש להגן על המידע המוזרם מיחידות קצה לגיטימיות, וכמובן חזרה אליהן. סינון המידע, סיווגו כלגיטימי והגנה עליו נעשים בשלושה אופנים: על ידי ניהול זהויות של יחידות הקצה, ניתוח אלגוריתמי של התנהגות יחידות הקצה ושימוש בחומת אש מוגדרת תוכניתית. לאחר שמומשה תקשורת מאובטחת בין יחידות הקצה לתשתית

פתרון ה-Edge2Cloud, נדרש לרוב ממשק אלקטרוני (רכיב 3 בדיאגרמה) בדמות כרטיס(ים) אלקטרוניים ו/או מחשבים מקומיים שתפקידם ניהול מקומי. ניהול זה בלתי תלוי בחיבור לרשת או לענן, של יחידות הקצה וכן שילוב של חיישנים נוספים, חיצוניים ליחידת הקצה המדוברת. לדוגמה, במקרה של הקיוסק הדיגיטלי נמצא כרטיסים אלקטרוניים מבוססי מיקרו-מעבדים המנהלים את פעולת הקיוסקים, לרבות ניהול תרמי של המערכת. במקרה של טמפרטורת סביבה גבוהה, מערכת המחשוב הפנימית תזהה באמצעות חיישנים כי נדרש לקרר את הרכיבים ותגביר את פעולת המאווררים הפנימיים. המערכת אף יודעת להפעיל כל מאוורר במהירות הנדרשת, לזהות במידה וקיימת תקלה במאוורר כלשהו, להתריע ולפצות בעזרת המאווררים האחרים. בנוסף, במידה וטמפרטורת העבודה הפנימית עדיין גבוהה מהרצוי, מערכת הניהול המקומית תדע לעמעם את עצמת המסכים כדי שיפחיתו את כמות החום הנפלטת אל פנים הקיוסק. במקרים מסוימים של טמפרטורות קיצון, אף ייכבו אוטומטית המערכות הלא חיוניות בקיוסק כדי להגן מפני נזק בלתי הפיך. ניהול מתקדם שכזה מצריך ממשק IoT אלקטרוני משולב המבוסס על פיתוח של כרטיסים אלקטרוניים, כתיבה של תוכנה לכרטיסים - קושחה (Firmware), ניהול תוכנת של הכרטיסים ושילוב של חיישנים חיצוניים.

מעל הממשק האלקטרוני נמצאת שכבת הרשת והקישוריות (רכיב 4 בדיאגרמה) שבה רשת מוגדרת תוכנה מאפשרת חיבור מהיר, מאובטח ומופרד של ערוצי תקשורת מרובים. במקרה הקיוסקים הדיגיטליים, החיבור המהיר מתאפשר בשל חיבור לסיב אופטי או כבלי נחושת. האתגר נובע מהצורך לספק על גבי פס התקשורת שירות Wi-Fi פתוח לכל ברחבי העיר. בהיבט של אבטחת מידע, ערוץ כזה של תקשורת הפתוח לכל צופן בחובו סכנות וניסיונות חדירה. על כן, פתרון הרשת מציע מספר ערוצי תקשורת, הנפרדים זה מזה (VPN – Virtual Private Network) ומאפשרים העברת מידע מאובטח. דומה הדבר למערכת כבישים ציבורית בה כל אחד יכול לנוע בנתיביה, וחלק מהנתיבים מוקצה לטובת מנהרות סגורות המאפשרות רק למידע מסוג מסוים לנוע. כך ניתן לייחד "נתיב" לטובת רשת Wi-Fi ציבורית, ו-"נתיבים" אחרים לצורך העברת מידע תפעולי של הקיוסקים, העלאה של תוכן ועוד.

כל המבנה שהוסבר עד כה ברכיבים 1 עד 4 מייצג פרישה מקומית, לדוגמה בעיר אחת או מפעל אחד מתוך קבוצה של מפעלים. אך מה בנוגע לפרישה רחבה יותר של מספר ערים, מפעלים או בתי אב? במקרה שכזה נדרש ניהול מקומי של הפרישה, הנעשה באמצעות ענן מקומי/ענן קצה, הנקרא Cloudlet (רכיב 5 בדיאגרמה). ענן הקצה הינו למעשה מרכז מחשוב – Data Center, הנמצא פיזית קרוב ליחידות הקצה. תפקידו לאפשר שרידות בהיעדר קישוריות לענן מרכזי, ניהול יחידות הקצה באופן אוטונומי, אספקת כוח חישובי והפחתה משמעותית בזמן השיהוי (Latency) – הזמן הנדרש מתחילת בקשת מידע מהענן ועד שהמידע מתקבל. בעיר בה מאות אלפי יחידות קצה, ינהל ענן הקצה יחידות אלו וישמש מתווך מידע, תוך חיבור חומרתי ותוכנתי מאובטח (רכיב 6 בדיאגרמה) לפתרון הענן (רכיב 7 בדיאגרמה). לכן, בפרישה של מאות אלפי יחידות IoT נמצא כי פתרון ענן מנהל פרישות של ענני קצה המנהלים בתורם יחידות קצה רבות. חשוב לציין, כי בחינה של פתרון ה-Edge2Cloud מראה כי שילוב אבטחת המידע בפתרון הינו קריטי בכל רובד ועל כן מיושם בכל אחד ממרכיביו.

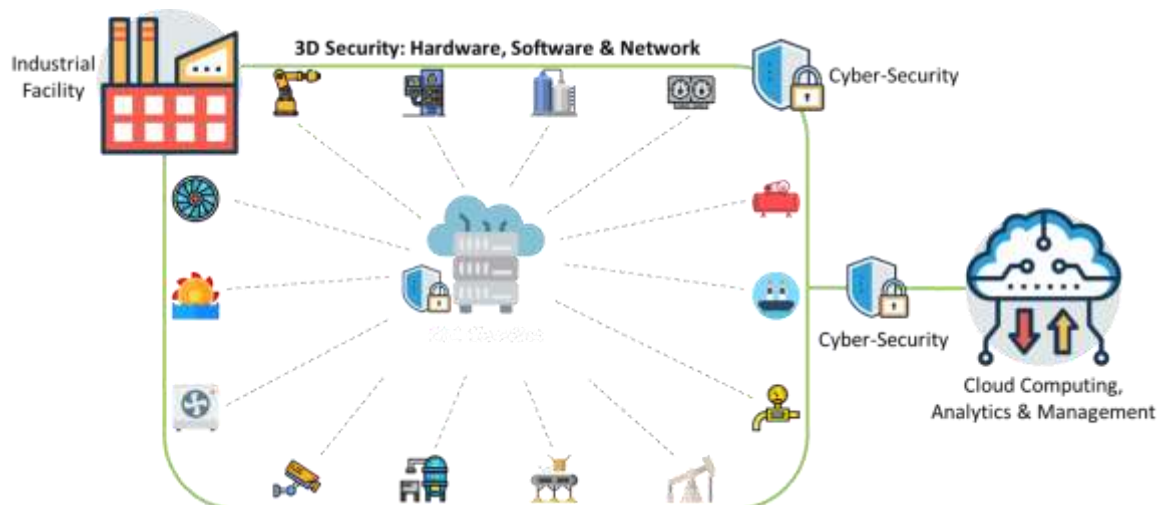
מרכיב שלישי: תשתית דיגיטלית לפתרון בעיות הסיילואים (Silos)

כשבוחנים לעומק שימושי קצה, כגון עיר חכמה או בית חכם, ניתקל באתגר השלישי והחשוב. סיילואים – תחומים נפרדים ומבודדים הפועלים בתוך מערכת אחת. גישור וחיבור בין הסיילואים מניב ערך חדש

למערכת כולה. לדוגמה, עיר היא מערכת בה פועלים תחומים נפרדים ומבודדים כמו: מערכת התאורה, איסוף האשפה, תחבורה, רמזורים וביטחון. כל תחום כזה פועל בנפרד עד כדי מחלקות נפרדות בעירייה וכוח אדם נפרד, שאינו בהכרח מתואם עם מחלקות אחרות. במצב שכזה, מה קורה אם מצליחים לשלב בין הסיילואים? לצורך כך, נתבונן בדוגמה פשוטה יחסית בה שילוב מידע מסיילו חיישני תנועה ברחוב עם סיילו מערכת ניהול התאורה, יניב ערך חדש לעירייה. למעשה, ניתן להתאים את רמות האור ברחוב לתנועת האנשים, וכך לחסוך כסף ותאורה מיותרת בשעות הלילה. ברחובות רבים אין כל תנועה רוב הלילה, ולכן ניתן לעמעם את תאורת הרחוב. ברגע שתזוהה תנועה על ידי החיישנים, תוגבר רמת ההארה למקסימום כדי לספק תאורה נאותה. כאשר החיישנים מזהים כי שוב אין תנועה ברחוב, יעמעמו גופי התאורה את אורם, יחסכו אנרגיה ועלויות חשמל לעירייה. דוגמה נוספת, היא מעולם הבית חכם. עם מגוון פתרונות ויצרנים, סביר להניח שבית נתון יכלול לדוגמה: רמקול חכם של גוגל, מנעול חכם לדלת של אוגוסט סמארט, מצלמה של לוגיטק, בייבי סנס, וכולם עובדים ללא קשר או תלות אחד בשני. אם הייתה דרך פשוטה לגשר בין כל הסיילואים האלו, ניתן היה לקבל ערך חדש ללקוחות בדמות בית שמנוהל טוב יותר עם רמת אבטחה משופרת. לדוגמה, הבייבי סנס יזהה שהתינוק במיטה, יעביר את המידע למנעול דלת הבית שימנע נעילה של הבית, או לפחות יספק התראה שעומדים לעזוב את הבית ושהתינוק עלול להישאר לבד. בנוסף, הרמקול החכם יתריע קולית לנמצאים בבית על הימצאות התינוק במיטה בזמן שמנסים לצאת מהבית. אתגר הסיילואים רלוונטי כמובן גם בתעשייה ובקווי הייצור, כאשר במקרים רבים מכוונות בקו הייצור עובדות ללא אינטראקציה בין הקווים או בינן לבין עצמן. כך לדוגמה, בטכנולוגיות קיימות חיישנים המזהים תקלה במכונה נתונה יתריעו על כך. אולם מה בנוגע למערכת שתדע להשתמש במידע הזה ולהסיט את הייצור לקו אחר, או לחלופין, לשקלל עדיפויות ייצור של מכוונות אחרות? בביקור שהתקיים באחת מחברות הייצור הגדולות בארץ אמרו המארחים, כי נכון להיום חסרה להם מערכת ניהול ותקשורת מרכזית בין קווי הייצור, מערכות המידע נפרדות, ניהול המלאי מופרד ואתגר אבטחת המידע – בהתאם. אם כך, כיצד מתמודדים עם אתגר הסיילואים, המציע גם הזדמנויות עסקיות משמעותיות לאלו היכולים לו? על ידי הטמעה של תשתית דיגיטלית.

מערכת אחודה של תוכנה, חומרה, ותקשורת המאגדת, מאבטחת, מוליכה ומתפעלת מידע. בדומה לתשתיות החשמל, מים ותחבורה המשמשות צרכנים שונים, כך התשתית הדיגיטלית משמשת את הצרכנים ויצרני המידע שבא או עובר ליחידות הקצה. אם נתבונן בשכונה של בתים פרטיים, לכל בית כביש גישה שמתחבר לכבישי השכונה ומשם למערכת כבישים עירונית ובינעירונית. לא היינו מעלים על הדעת שכל נהג המתגורר בבית פרטי יסלול לעצמו כביש עד העיר, אלא מובן מאליו שכל הנהגים חולקים תשתית כבישים משותפת. כך גם בתשתיות משותפות אחרות בהם התושבים חולקים, למשל איסוף אשפה או תאורה. שימוש בתשתית שיתופית נראה טבעי, אך לא כך הוא הדבר עם פתרונות IoT המותקנים היום. לדוגמה, בפתרונות עיר חכמה כל יצרן פורש לעצמו תשתית מקומית. כך לדוגמה, ספק גופי תאורה יציע את יחידות הקצה עם פתרון תקשורת ייחודי, חומרה ייעודית, אבטחת מידע ופתרון ענן בהתאם. ספק חיישני חנייה יציע אף הוא פתרון תקשורת משלו, חומרה ייעודית, אבטחת מידע ופתרון ענן אחר. והנה לאט, אבל בטוח, כל ספק טכנולוגיה מטמיע סיילו משלו, כאשר העירייה אינה יכולה לנהל את כל הפתרונות בצורה אחודה. הבעיה מחמירה לנוכח העובדה, כי פריסת תשתית באשר היא דורשת מומחיות. ישנם היבטי שרידות, שירותיות, אבטחת מידע וניהול, שאינם בתחום המומחיות של ספקי פתרונות הקצה. זאת ועוד, פרישה של מספר תשתיות יוצרת כפילות מיותרת, המסתכמת בעלויות גבוהות יותר ללקוח. לכן, מימוש ארכיטקטורת

Edge2Cloud מהווה למעשה תשתית דיגיטלית, בה ניתן ורצוי להשתמש לכלל צורכי ה-IoT בעיר החכמה, בבית החכם או במפעל חכם, כפי שמוצג בדיאגרמה.



תשתית IoT דיגיטלית: מימוש במפעל תעשייתי. מקור: Robust E2C.

כאשר מוטמעת תשתית אחודה, ניתן לנהל את יחידות הקצה ללא תלות במיקומן ואופיין, לפתור את בעית הסיילואים ולהפיק ערך חדש. חשבו על חזון בו עיר או מפעל מטמיעים תשתית מידע שכזו ומחייבים את כל חברות הפתרונות המעוניינות לשלב את הטכנולוגיות שלהן, להתאים עצמן ולהשתמש בתשתית הקיימת של העיר או המפעל. למעשה, ספקיות פתרונות קצה צפויות לקבל בברכה תשתית שכזו שתקל על שלב האינטגרציה, תקצר את משך זמן ההטמעה ותעלה את האמינות הכוללת של המערכת המשולבת. זאת ועוד, תשתית דיגיטלית שכזו צפויה לחסוך עלויות רבות, הן ללקוח והן לספקי הפתרונות, בשל השימוש בתשתית האחודה.

סיכום

פתרון IoT מוצלח דורש, בראש ובראשונה, מודל עסקי ברור ובדוק, בו הפתרון עונה על צורך אמיתי של לקוחות וכאשר ברור מי ישלם, על מה וכמה. הפתרון הטכנולוגי דורש התייחסות גורפת מהקצה לענן – Edge2Cloud, אחרת מדובר בפתרון חסר, וגלגול בעיות רבות לפתחם של הלקוחות. בעת מימוש הפתרון הטכנולוגי, אבטחת המידע היא נדבך קריטי לאורך השדרה מהקצה לענן, ודורשת מומחיות, בדומה לשאר רכיבי הפתרון. לבסוף, אתגר הסיילואים מהווה, כאמור, בעיה אמיתית שהולכת וגדלה עם התקנתם של פתרונות IoT מקומיים שאינם מתוכננים כראוי. התשובה לבעית הסיילואים טמונה בתכנון ובפריסה של תשתית דיגיטלית: תוכנה, חומרה ותקשורת המנהלים באופן אחוד, מידע הנוצר מרכיבי IoT באשר הם.

בראייה ניהולית, כמנהל מפעל או כמנהל טכנולוגיות בעיר, חשוב להכיר את אתגרי פתרונות ה-IoT ולהתמקד בפתרון בעיית הסיילואים. למידת לקחים מפתרונות שהוטמעו ובוצעו בהצלחה והבנת הנדרש ברמה התשתיתית, הינם צעד ראשון בדרך להצלחה.