CZY IOT GRA W KOŚCI?

PODSTAWY INTERNETU RZECZY

MARCIN SIKORSKI

Ten e-book jest darmowy więc jeśli znasz kogoś z kim chciałbyś się nim podzielić to podrzuć im linka do mojej strony ;) Wielkie dzięki!

Jeżeli spodoba Ci się to co przeczytasz zapraszam na www.smartrzeczy.pl gdzie możesz znaleźć dużo więcej dobroci związanych z Internetem Rzeczy.

Napisane przy niewielkiej pomocy ze strony niewyspanych nocy, zimnych kolacji i kilku galonów zielonej herbaty.

Okładka stworzona przy pomocy canva.com, ikony pochodzą z serwisu flaticon.com/authors/mavadee

SPIS TREŚCI

WPROWADZENIE

Gdy jeszcze będąc dzieckiem po raz pierwszy ujrzałem moc Internetu byłem oczarowany. Magiczny świat pełen ukrytego potencjału, niebywałych korzyści oraz szans na interesujące jutro.

Dzięki swojemu samozaparciu oraz wrodzonej ciekawości zacząłem zgłębiać tę krainę by załapać się na pierwszą falę Internetowego boomu.

Dość szybko stworzyłem pierwsze strony internetowe, które osiągnęły gigantyczną popularność, zainwestowałem w szybko rosnące usługi Internetowe oraz byłem jedną z pierwszych osób, którym zwróciła się inwestycja w Bitcoiny. A wszystko to nim przekroczyłem próg 30. lat.

No dobra, fajnie by było móc tak napisać ale nie tak potoczyła się ta historia.

Mój stymulacyjny próg dociekliwości zatrzymał się na śmiesznych kotach, gołych babach i zmarnowanym czasie spędzonym na YouTubie.

Czyli co – introwertyczna smuta bez krzty polotu?

Niekoniecznie biorąc pod uwagę, i tu piszę już poważnie, że dziwnym trafem, przez zrządzenie losu, stałem się osobą, która w przyszłości miała być mówcą publicznym, członkiem grupy Ministerstwa Cyfryzacji ds. IoT i propagatorem (ambitne słowo) wiedzy na temat Internetu Rzeczy.

Ot, nie chciałem zabawiać się z Panią Internet jak była młoda to postanowiłem przeżyć upojne chwile z córką zwaną Internetem Rzeczy.

Ebook, który czytasz jest więc owocem tej dziwacznej miłości, która zrodziła szereg felietonów, publikacji, wystąpień i innych materiałów

dotyczących IoT. To co dało się upakować w formę pisaną postarałem się zebrać w tej pozycji.

Napisałem całość z perspektywy osoby, która nigdy nie miała do czynienia z samym zagadnieniem, a chciałaby pominąć ten cały korpo-techniczny bełkot. Zobaczyć i spróbować tematu weryfikując czy to zabawa dla niego. Zamoczyć palca, polizać go i stwierdzić „przesolone, ale mi smakuje".

Moim celem nie jest zatem przekabacenie Cię na jedyną, słuszną drogę IoT[1] ale raczej pokazanie Co cię czeka gdy już zdecydujesz się by któregoś dnia rozmawiać ze swoim Smart talerzem o swoim Smart obiedzie, który przyrządził Ci twój Smart piekarnik.

Tak czy owak, bez względu na osobliwą przyszłość, którą przyniosą nam te „smart" rozwiązania liczę, że będziesz już mentalnie gotowy na ich nadejście.

A ja? Będę w tym czasie nadal uskuteczniać swoje cyfrowe kaznodziejstwo.

W każdym razie zaparz kawę, połóż się pod kocykiem i baw się dobrze podczas lektury!

W razie pytań szukaj Mnie na www.smartrzeczy.pl !

Marcin Sikorski

[1] Choć byłoby miło ;)

JAKICH UMIEJĘTNOŚCI POTRZEBUJĘ BY ZROZUMIEĆ IOT?

Zakładam, że dotychczas nie miałeś do czynienia z IoT częściej niż chwile spędzone na zabawie ze swoim smartphonem, smart telewizorem lub asystentem głosowym typu Alexa lub Siri, którym kazałeś odpowiadać na podchwytliwe pytania.

Fajnie było tak wchodzić w interakcje z tymi produktami? Fajnie było jak gadały z sensem i Cię rozumiały?

Pewno, że tak!

Strzelam nawet, że w przypływie natchnienia i ulotnej chwili zapaliła Ci się nad głową żarówka, włączył Ci się tryb Indiany Jonesa i postanowiłeś, że zgłębisz temat mocniej poszukując źródła wiedzy, z którego mógłbyś czerpać.

I już pal licho czy popycha Cię potrzeba zawodowa czy hobbistyczna – grunt, że masz parcie na szkło i chcesz ogarnąć lepiej temat.

Nie będzie Ci przecież maszyna ustawiać życia! Chcesz wiedzieć na czym polega jej intelektualny fenomen!

Ale powiem Ci, że jest co poznawać biorąc pod uwagę przestrzał technologiczny z jakim mamy do czynienia na przestrzeni ostatnich kilkunastu lat. Ta cyfrowa rewolucja, na którą się załapałeś przyjmuje szereg kształtów i wzorów. Stąd brawa dla Ciebie – im wcześniej podjąłeś decyzję o zgłębieniu IoT tym większa szansa, że ominie Cię cyfrowy analfabetyzm.

No dobra – my tu słodkie pitu pitu, a warto by określić jaki rodzaj doświadczenia będzie przydatny na twej drodze. Bo zakładam, że choć częściowo chcesz przekuć zdobyte doświadczenie na pracę, która przyniesie Ci geldy i szekle, co nie?

I tu, bez względu czy marzy Ci się testowanie, developowanie czy zarządzanie projektami IoT mogę Cię częściowo pocieszyć jako, że pewne umiejętności, które będziesz zdobywać są względnie uniwersalne dla wszystkich „klas”:

- znajomość protokołów i zasad elektroniki,
- temat wirtualizacji,
- chęć grzebania w logach i dokumentacji,
- wyrobienie sobie opinii na tematy bezpieczeństwa[2].

Wiem, wiem – już kręcisz głową, że za dużo i skomplikowane ale takie są niestety fakty.

Internet Rzeczy oparty jest o dane, a współczesne dane są oparte o Internet Rzeczy więc prędzej czy później wszystkie aspekty związane z tym przepływem trzeba będzie zrozumieć.

Fakt, protokołów komunikacji jest „troszkę sporawo”, a elektronika może wydawać się przerażająca ale spoko, spoko – wszystko jest do ogarnięcia. Powoli i po kolei.

Na początek wystarczy, że liźniesz co nieco na temat Bluetooth, BLE, WiFi, Zigbee, Z-Wave i Thread[3] i już będzie można z Tobą wypić kawę w pracy.

Inna sprawa, że w przyszłości będziesz spędzał niezdrowe ilości czasu właśnie nad weryfikacją komunikacji lub stopniem zazwyczaj siajowo zmontowanych komponentów i podzespołów danego produktu. Fajnie by zatem było wiedzieć co one robią i za który drucik pociągnąć, żeby nie spalić płytki.

A że sama elektronika z miesiąca na miesiąc tanieje (Aliexpress rządzi), a liczba dostępnych komponentów już dawno zalała rynek ilością i zróżnicowaniem wymówka w postaci “wysokich cen”, braku

[2] No dobra – jest jeszcze sztuczna inteligencja, sieci neuronowe, big data i parę innych pokrętnych zagadnień, które miło by było jeszcze znać.
[3] W razie wątpliwości wszystkie te zagadnienia poruszam na stronie smartrzeczy.pl (w stosownym dziale)

czasu lub niechęci do poświęcenia choćby paru chwil dla lepszego zrozumienia jak działają bebechy inteligentnych produktów będzie dla mnie kompletnie niedorzeczna.

Krótko – chcesz pracować przy IoT i zajmować się na co dzień Internetem Rzeczy? Zacznij już dziś inwestować w wymienione umiejętności!

Kolejną sprawą jest aspekt wirtualizacji.

Brzmi dumnie? Może ale nie ma co się ekscytować – ten kotlet jest do strawienia.

Z własnego doświadczenia[4] powiem Ci, że mnóstwo czasu i w wielu przypadkach pracuję na "gołych płytkach" na których zainstalowany jest Linux lub jemu podobne systemy, które wirtualizują i imitują istniejące Smart produkty.

Świat IT pędzi, terminy gonią, klienci są rozdrażnieni i chcieliby wszystko na wczoraj więc wraz w krótkim okresem developmentu, i chcąc ciąć po kosztach, stawia się wirtualki. Imitacje maszyn, połączeń, ich komunikacji i zachowania. Stąd podstawy wirtualizacji są równie niezbędne co dobra wiedza z obszaru elektroniki.

No dobra, jak już nie masz alternatyw i możliwości to chociaż zapoznaj się z tym co oferują Amazon i konkurencja w kwestii usług dedykowanych w chmurze – AWS IOT, Google IoT, Azure IoT. Podziękujesz mi potem.

Nie mówię, że jest to proste i przychodzi samo, ale twierdzę, że bez tego ciężko jest się odnaleźć podczas stawiania środowiska.

Następny punkt programu to dokumentacja i czytanie logów.

[4] Pracuję jako Tester Internetu Rzeczy. Jak Ci kiedyś słuchawki BT nie zadziałają lub smart głośniki nie odpowiedzą na pytanie – to moja wina.

Zakładam, że lubisz dużo wertować i nagminnie kartkować różne dzieła pisane? Idealnie! Dokładnie do tego sprowadza się w tym momencie praca z IoT.

Bez sprawności czytania logów generowanych przez sprzęt i zrozumienia co oznaczają poszczególne flagi oraz wskaźniki ciężko będzie mówić o jakimkolwiek profesjonalizmie.

Ja wiem - czytanie logów i dokumentacji to obciach, nuda i kojarzy się z mozolną i niewdzięczną pracą (co poniekąd jest prawdą) ale jak „trza" zagwarantować bezpieczeństwo, prostotę oraz efektywność działania produktów to „trza" też wiedzieć z czego ona wynika. To, że urządzenia sobie czule szepczą romantyczne słówka to jedno. Ich zrozumienie to odrębna sprawa.

Znajomość metadanych (czyli danych na temat danych) oraz biegłość w obsłudze logów zapewniają sprawną pracę zarówno Tobie jak i twojemu przyszłemu zespołowi oraz uczynią twoje życie znacząco prostszym.

Następnym razem gdy będziesz zatem na kibelku, zamiast grać w dupograjkę na swym telefonie, zainteresuj się żywo działaniem, a i choćby, Wiresharka. Odpycha to od siebie interfejsem ale da Ci poczucie pewności siebie by bezpiecznie poruszać się po tematyce IoT.

A skoro już poruszyłem temat bezpieczeństwa – warto i tutaj móc wtrącić swoje trzy grosze.

Kiedy mowa o Internecie Rzeczy na tak szeroką skalę - pełnym różnorodnych maszyn, sensorów, produktów, beaconów oraz protokołów – nie dziwota, że temat bezpiecznej obsługi i ochrony danych przewinie się to tu, to tam.

Co więcej będziesz musiał wiedzieć jakie istnieją potencjalne zagrożenia wynikające z działania danego urządzenia i starać się im przeciwdziałać na każdym etapie produkcji.

Co prawda nie twierdzę, że z dnia na dzień powinniśmy stać się specjalistami od penetracji (no pun intended) ale już „testops” to i owszem.

Nie będzie innego wyboru skoro ciężko będzie zakwalifikować Cię jako pracownika manualnego, automatycznego, bezpieczeństwa lub obsługi danych. Będziesz człowiekiem od jakości IoT.

Tzn. będziesz jeśli wybierzesz analogiczną ścieżkę związaną z zapewnieniem jakości :)

Z drugiej strony, popatrz na to w ten sposób - przy odrobinie chęci, wraz ze swoją wszechstronną wiedzą, staniesz się kolejnym ogniwem ewolucji branży IoT. Będziesz jedną z osób, które tworzą i pracują przy „tych klawych produktach”, z których korzystają potem tysiące osób na całym świecie.

Ego połechtane? No ja myślę! I oby tak było aż do ostatniej strony!

TECHNOLOGICZNY ANALFABETYZM

INTERNETU RZECZY

Nim to jednak nastąpi – nim staniesz się drugim Stevem Jobsem IoT - chciałbym abyś zapoznał się z manifestem dotyczącym Internetu Rzeczy.

Napisał go pewien znany podróżnik, filozof i kancelrz IoT, który równie mocno ewangelizuje Polskę co zajmuje się budowaniem swej pozycji na piedestale IoT – Paulo Coelo naszych czasów – feldmarszałek Sikorski.

Tak, tak… swego czasu popełniłem osobliwy rodzaj listu otwartego, który uważam za niezbędny przy dalszej lekturze. Pozwoli Ci on uzmysłowić pewne intersujące koncepcje dotyczące właśnie IoT:

Kocham Internet rzeczy.

Odkąd po raz pierwszy raz zetknąłem się z tym zagadnieniem zdałem sobie sprawę jaki kryje w sobie potencjał. Oczyma wyobraźni kreśliłem wizję jak będzie wyglądać przyszłość i dokąd możemy zajść w futurystycznym wyścigu społeczności jutra.

Potem pojawił się Elon Musk i po części zaczął realizować te wszystkie koncepcje.

My, szara masa, zostaliśmy za to ze smutną rzeczywistością.

Niestety ale im dłużej śledzę wiadomości czy wzmianki dot. IoT, czy to na portalach, social mediach czy blogach, tym mocniej dostrzegam, że Internet Rzeczy jest wciąż dziwnym, "niezdefiniowanym bytem", z którym wiele osób albo nie wie co zrobić albo w ogóle nie zdaje sobie sprawy z jego istnienia.

Szczególnie w pewnym nadwiślańskim kraju.

Tak, to prawda, że mamy w Polsce bardzo dobre firmy, które starają wdrażają produkty wpisujące się w standard i formułę Internetu Rzeczy.

Tak, dostrzegam, że mamy potencjał w kwestiach start-upów. Bez wątpienia mamy ekipy, którymi moglibyśmy się śmiało chwalić na świecie.

I tak, dostrzegam sporadycznie pociąg młodszego pokolenia do tego aby zrozumieć i zacząć stosować Internet Rzeczy w swoim życiu. A przynajmniej tak, żeby było im wygodnie.

Niestety ale widzę też że nie robimy kompletnie nic aby aktywizować starsze pokolenia lub edukować zwykłych ludzi o tym jakie korzyści może przynieść im stosowanie Internetu Rzeczy na co dzień..

I przyznam się szczerze że mocno mnie to boli. Boli mnie bo wiem, że takie zmiany technologiczne i rozwój nie trwają i nie zdarzają się z dnia na dzień. Potrzebują czasu – miesięcy, lat, a czasem nawet i dekad – by wrosnąć w mentalność obywateli. Potrzeba czasu by ludzie wiedzieli jakie są dobre praktyki, jak należy działać oraz po co, w pierwszej kolejności, należy korzystać z danej technologii.

Kiedy ostatni raz widziałeś jakąś porządną kampanię na ten temat? No właśnie. Co najwyżej wzmiankę w wiadomościach o tym, że smart auto przejechało jakąś kobietę.

Nie wyobrażam sobie, że Polacy będzie w stanie wiecznego uśpienia podczas gdy Estonia, Niemcy, Czechy, Francja i większość krajów na świecie żyją, oddychają i korzystają z dobroci Internetu Rzeczy. Ciągle zastanawiamy się czy jest u nas potrzeba, czy powinniśmy w ogóle interesować się tematem, czy nie jest to aby jakaś nowinka, która po jakimś czasie umrze nie przynosząc pożytku.

Chryste kochany! Już kilka dekad istnieje IoT. Już kilkadziesiąt miliardów produktów służy na całym świecie. Już dawno zyski i

korzyści przekroczyły zdroworozsądkowe wartości. Stąd odpowiadam – tak! IoT MA potencjał!

Nie ma pieniędzy? Nie ma wiedzy? Nie ma czasu? Nie ma chęci!

Pora zatem obudzić się z tego letargu, przestać gadać o bzdurach i celebrować puste newsy, które nie wnoszą kompletnie nic i zaśmiecają umysły. Zamiast tego trzeba częściej dyskutować o tym jaki potencjał technologiczny kryje się za dwoma słowami Internetu Rzeczy.

Ja wiem, że prawo wciąż nie sprzyja tym działaniom, technologia jest początkowo trudna do zrozumienia, a zmiana wymaga czasu ale jeżeli nie wykonamy pierwszego kroku już teraz i nie będziemy regularnie i często dążyć do tego aby nasze społeczeństwo było obyte technologicznie to na zawsze pozostaniemy technicznymi analfabetami.

Nie róbmy sobie tego. Nie wprowadzajmy siebie w kompleksy.

Zainwestujemy czas i znajdź my w sobie chęć do tego aby codziennie coraz to lepiej poznawać tę technologię.

Bo jeżeli naprawdę nie zaczniemy brać się za siebie to możemy niedługo obudzić się zdziwieni rzeczywistością w której przyszło nam żyć. I to nie dlatego, że sami wybraliśmy sobie jej kształt i wymiar ale dlatego że zostaliśmy do niej wrzuceni.

Nie z powodu własnych umiejętności i przekonań ale dlatego, że nie rozumiejąc ktoś zrobił to za nas.

Nie bądź więc bierny wobec technologicznych zmian.

Zacznijmy działać już dzisiaj.

CZY IOT GRA W KOŚCI?

Jeżeli czujesz się uduchowiony powyższymi słowami i poczułeś głęboko w sercu jak zapłonął Ci ogień potrzeby zgłębiania IoT to jesteś gotów przyjąć kolejne święcenia.

Pora na fragment, w którym zmierzymy się z tematem komunikacji IoT i opowiem Ci co nieco o protokołach. Nieco lepiej objaśnię temat kolaboracji elementów Internetu Rzeczy – przeczesywania, grupowej rekomendacji i ekspertyzy opartej o przewidywanie i dotychczasowe doświadczenie.

Generalnie opowiem Ci co nieco o tych istotnych elementach, o których wspominałem jeszcze parę stron temu.

CHYBA, ŻE… pozwolisz, że wtrącę Ci jeszcze jeden interesujący element do ogródka wiedzy. A co! Bo dlaczego by nie urozmaicić tematu jeszcze bardziej!

Tak się bowiem składa, ze czasami (nie mówię, że często, ale jednak czasami) w ramach dyskusji dotyczącej IoT możesz natknąć się na informację dotyczącą efektu serendipity (PL: rzekomy(?)).

Jak się okazuje jest to swego rodzaju socjologiczny abstrakt (lub koncept jak kto woli), który zakłada, że najlepsze efekty osiąga się nieoczekiwanie.

W przypadku ludzi chodzi zazwyczaj o sytuację gdy inspirację oraz świeże spojrzenie dostarcza nam przypadkowa osoba (znajomy znajomego znajomego), a nie bezpośredni, dobrze znany Nam osobnik. Odizolowany, pozornie nieistotny czynnik, który nakierowuje na nowe tory myślowe.

Co prawda kluczem do istnienia tego „fenomenu” jest pewna doza szczęścia i fakt znalezienie się w odpowiednim czasie i miejscu niemniej skutki tego efektu widoczne są m.in. w nauce jak i sztuce.

Zakładając, że przyjmiemy, że nie jest to socjologiczny bełkot pokroju efektu Mandeli IoT podąża podobnym torem informacyjnego rozwoju opartego na szczęściu.

Nieustanna kooperacja i kolaboracja, synergia urządzeń, ciągła analiza oraz weryfikacja – już same te czynności i zachowanie rozbudzają poniekąd wyobraźnię. Szczególnie jeśli ziściłby się scenariusz zakładający istnienie Internetu Wszystkiego.

Tasowanie nieprzerwanie płynącym źródłem danych, mapowanie urządzeń i jednostek, emocjonalne sensory – ile z tych elementów już dziś potrafi wygenerować interesujące wnioski powstałe wyłącznie w wyniku „suchej" analizy osobnika, a ile z tego jest efektem przypadkowego połączenia kilku pozornie nieistotnych czynników?

Biorąc pod uwagę jak szybko nikną fizyczne granice oraz bariery emocjonalne, cielesne i emocjonalne, biorąc pod uwagę jak wiele urządzeń współdziała ze sobą oraz jaki ocean informacyjnego szumu wylewa się wprost na nas skłonny jestem przyklasnąć tej koncepcji.

Ciągłe dojrzewanie e-biznesu (nowe modele i procesy), kształtowanie się e-zachowania, rozrost cyfrowego ekosystemu czy choćby nacisk na e-geolokalizację (GIS – Geographic Information System) – transformacja dzieje się tuż na naszych oczach, zasady rozpisywane są na nowo, a gra z losem nabiera nowego wymiaru.

Pozornie może to przerażać ale w perspektywie Społeczeństwa Jutra jest to niezbędny czynnik, który może spowodować dalszą transformację w kierunku Internetu Wszystkiego.

Może… ale czy musi? Szczerze powiedziawszy sam chciałbym to wiedzieć.

Bez względu jednak na kierunek i tempo zmian po raz kolejny utwierdzam się w przekonaniu, że niezbadany jest potencjał drzemiący w IoT.

Mam nadzieję, że Ty też zaczniesz to dostrzegać.

OD ZERA DO IOT

No dobra… pora w końcu przejść do konkretów i rozłożyć choć częściowo zagadnienie IoT choć ciężko jest tak naprawdę wybrać najlepszy temat, od którego moglibyśmy zacząć naszą dyskusję dotyczącą Internetu Rzeczy.

Tak się bowiem składa, że IoT jest bardzo specyficznym zagadnieniem – to temat-rzeka i studnia bez dna, z której można czerpać litrami, a i tak nie zabraknie tematów czy wątków wartych omówienia. Wszystkie są równie ciekawe i warte poruszenia.

I choć zdaję sobie sprawę z tego, że IoT ostatnimi laty stał się swego rodzaju chłopcem do bicia, modą i buzzwordem (coś à la Scrum) to nie ma co zbawiać świata na siłę, ani wymyślać koła na nowo – każdy wybór będzie równie wartościowy.

Proponuję zatem rozpocząć od definicji Internetu Rzeczy. A co! Siła tkwi w prostocie, a zrozumienie tego pojęcia pozwoli sprawnie przejść do kolejnych kwestii związanych z istotą tego zagadnienia.

IoT to koncepcja, która zakłada, iż fizyczne urządzenia łączą się za pomocą sieci komputerowej oraz instalacji elektrycznej po to, aby swobodnie gromadzić, wymieniać i przetwarzać między sobą dane.

Tylko tyle, albo aż tyle.

Internet Rzeczy opiera się na założeniu, że kooperacja i kolaboracja są najważniejszymi czynnościami wykonywanymi przez wchodzące w interakcje maszyny.

Głównym celem tego zabiegu jest magazynowanie i analizowanie danych, które wykorzystywane są do optymalizowania procesów i zadań człowieka.

Kluczowe jest takie wykorzystanie IoT, aby usprawnić środowisko pracy jednocześnie uwalniając zasoby ludzkie, czasowe i finansowe,

które można przeznaczyć na inne, bardziej kreatywne zadania. Sprowadza się to do odpowiedzenia sobie na pytanie jak komunikacja i zebrane w jej toku dane mogą przynieść wartość dodaną dla samej firmy i jej klientów.

Samą konstrukcję urządzeń IoT można uprościć do czterech podstawowych komponentów:

- moduł komunikacji, który odpowiada za możliwości porozumiewania się urządzenia w danym "języku",
- sensor, który zajmuje się monitorowaniem zachodzących na określonym terenie zmian,
- bateria pozwalająca na jak najdłuższe działanie produktu,
- procesor, który umożliwia funkcjonowanie i prawidłowe działanie produktu,

a najważniejszym efektem tej działającej maszyny są zebrane i przeanalizowane dane.

Sam proces dostarczania danych opiera się na następujących krokach:

- Po pierwsze – posiadamy urządzenie, które nasłuchuje (sniffuje) otoczenie i monitoruje oznaki fizycznych lub chemicznych zmian typu nacisk, waga, ruch, temperatura itp.
- Następnie – dane te trafiają do bramki IoT (gateway), czyli urządzenia, które pełni funkcję mediatora/pośrednika pomiędzy siecią sensorów, a siecią internetową.
- W następnej kolejności dane są przesyłane do chmury, w której są przechowywane i poddawane procesowi analizy. Ze względu na rozmiar zbieranych danych (czasem wręcz petabajty) stosowane są metody analizy Big Data.
- W ostatnim kroku przetworzone dane przekazywane są do końcowego użytkownika, który może wchodzić z nimi w interakcję (za pomocą np. aplikacji telefonicznej). Użytkownik

sam decyduje o tym, jak bardzo pozyskane dane będą przydatne dla jego codziennych zadań oraz dodatkowo ma możliwość mobilnego kontrolowania i monitorowania produktu.

Istotnym elementem powyższego procesu jest samo pozyskiwanie danych.

Gdzie można je znaleźć i w jaki sposób zdobyć? Pytanie to można by skwitować prostym “wszędzie i w dowolny sposób” i nie będzie to dalekie od prawdy.

Trzymajmy się jednak pewnych granic rozsądku i wykonalności eksponując kilka najpopularniejszych środowisk:

- Home (wliczając w to wszelkiego rodzaju domowe bezpieczeństwo, kontrolery, huby, przełączniki itd.),
- Wearables (wszystko co da się „nosić” czyli zegarki, ubrania, biżuteria),
- Healthcare (szeroko rozumiana branża medyczna – od obszaru definiowanego jako „intymny”, jak choćby pompy insulinowe, tele-medycyna, e-monitoring, po obszar “ogólny” którego przykładem jest zaopatrzenie szpitali),
- Robotics (drony, roboty, automatyka, sztuczna inteligencja etc.),
- Automotive (“smart” auta, bieżniki analizujące podłoże itp.).

Rzecz jasna, powyższa klasyfikacja jest dość umowna. Podział obszarów objętych IoT może przyjmować różne kształty i rozmiary (ot, co książka i specjalista, to inne spojrzenie), przyjmijmy jednak wstępnie, że wymienione wyżej elementy stworzą nam podstawy do dalszej dyskusji.

Równie istotne w aspekcie zbieranie danych jest rozważenie trzech filarów działającego produktu IoT:

- technicznych,
- komercyjnych,
- ekosystemowych,

które to określają skuteczność gromadzenia informacji.

Techniczne aspekty decydują o wymiarze związanym m.in. z pokryciem obszaru. Obejmuje to m.in: informacje o tym, ile urządzeń i z jakim zasięgiem pokryje określony teren działania (inaczej przygotowujemy produkty dla sektora PAN (Personal Area Network), a inaczej WAN (Wide Area Network)), efektywność energii określający czas działania i cyklu życia na jednym ogniwie, “tętno danych”, czyli jak często i jakiego rodzaju dane mają być zbierane, no i, rzecz jasna, same aspekty urządzenia, które będzie spełniać zdefiniowaną rolę.

Komercyjne aspekty decydują m.in o bezpieczeństwie stosowanych technologii (w tym zabezpieczeniu prywatności i przekazywanych danych), koszcie implementacji i utrzymania produktu, skalowalności, która determinuje elastyczność i QoS (Quality of Service) skupiający się głównie na jakości oferowanej usługi w obszarze m.in. opóźnień.

Ekosystem decyduje o globalnym zasięgu i interoperacyjności usług, które mają być jak najprostsze i jak najbardziej efektywne w implementacji. Planowana z wyprzedzeniem jakość ma zapobiegać krótkotrwałym działaniom na rzecz strategicznego inwestowania w ekonomiczny i technologiczny rozwój społeczeństwa.

Wiele osób już dziś zaczyna rozważać temat IoT zastanawiając się czy taka czeka nas przyszłość?

Cóż… od nieuniknionego nie da się uciec – możemy jedynie stawić mu świadomie czoła.

TRENDY IOT

Powoli zdajesz sobie sprawę jak złożonym zagadnieniem jest Internet Rzeczy i jak wiele obszarów obejmuje. Złożoność tę widać na przykładzie samej branży, która nieustannie dostarcza nowatorskich rozwiązań, gdyż zakres możliwości biznesowych i problemów do rozwiązania jest niemalże nieograniczony.

Pora jednak zadać kilka istotnych pytań:

- Jakie trendy przeważają w branży IoT?
- Jakie tematy warto obserwować?
- Czy w Internecie Rzeczy jest coś, co możemy określić mianem "czarnego konia"?
- Na co branża kładzie nacisk?
- Jakimi ścieżkami podąża?

To istotne pytania, a odpowiedź na nie posłuży jako kierunek dalszej dyskusji.

Dzieląc świat na określone segmenty zastosowania IoT, możemy wyróżnić następujące kategorie:

- Smart miasta – wszystko co jest związane z rozwojem, utrzymaniem i kontrolą aglomeracji,
- IIOT – industrialny Internet Rzeczy, który obejmuje swym zasięgiem fabryki i znajdujące się weń maszyny,
- Smart zdrowie – urządzenia do ratowania, poprawy życia i zdrowia,
- Smart domy – a w nich urządzenia użytkowe, monitorujące, wszelkiego rodzaju liczniki itp.,
- Smart pojazdy – od desek rozdzielczych, aż po smart bieżniki oraz semi-inteligentne pojazdy,
- Wearables – inteligentna biżuteria oraz ubrania;

- Smart utilities – dedykowane systemy mierzenia zużycia wody, elektryczności, gazu, zniszczenia dróg, sanitarne etc.,
- Inne – między innymi drony, produkty wojskowe lub kosmiczne,

jak i smart agro-kulturę , smart sklepy oraz sieci dostawy (jako że IoT usprawnia proces logistyczny).

Dziedzina inteligentnych peryferiów domowych (elementy wchodzące w skład smart domów) będzie stanowić nasz początkowy obszar badań.

Skąd taki pomysł?

Otóż stąd, że to tu znajdziemy elementy i urządzenia, które znamy z codziennego użytkowania, a które najłagodniej przechodzą technologiczne dojrzewanie.

Jakie zatem rozwiązania można wyróżnić w dziedzinie peryferii domowych?

Z całą pewnością podstawowym novum są wszelkiego rodzaju “kontrolery“ wykorzystujące moc głosu, gestów oraz wzroku.

IoT w przeważającej liczbie przypadków oferuje możliwości kontrolowania osprzętu za pomocą strun głosowych użytkownika lub symbolicznego ruchu ciałem.

W nowoczesnym IoT do kontrolowania zachowania “rzeczy” nie wystarczą już gesty palcem lub dotyk urządzenia – teraz liczy się głównie głos i mimika!

Szczególny prym wiodą w tych rozwiązaniach takie firmy jak Amazon (Alexa), Google (Google Voice Assistant), Microsoft (Cortana) oraz Apple (Siri), które sprzedają swoje SDK (development kit – „narzędzia” do budowania) zarazem badając ich możliwości w praktycznym zastosowaniu i rozwijając produkty na bazie uzyskanej informacji zwrotnej z rynku.

Coraz częściej spotykamy się z opcją „porozumiewania się" ze sprzętem w taki sposób, aby interakcja przebiegała na bardziej intymnym niż dotychczas poziomie. Przestajemy traktować sprzęt jako odrębny element wyposażenia mieszkania, a zaczynamy postrzegać go niczym "członka rodziny", z którym możemy dyskutować i wchodzić w reakcję.

Gładkie kształty urządzeń, damskie imiona produktów, adaptacja delikatnego głosu wirtualnego asystenta, nieinwazyjny charakter dyskusji i zadawanych pytań – brzmi to cudacznie jednak z psychologicznego punktu widzenia ma to sens – takie zabiegi sprawiają, że ludzie traktują sprzęt bardziej „ludzko", zżywają się z nim i są w stanie wyjawić mu swe prywatne dane.

A przecież – jak już wcześniej wspomniałem – to o dane głównie chodzi firmom zaangażowanym w produkcję IoT.

Od zapewnienia "intymnego" kontaktu konsumenta z urządzeniem jest już tylko krok do kolejnego popularnego rozwiązania świata IoT – subskrypcji.

Kiedyś sprzęt kupowano z myślą o długich latach użytkowania. Zarówno producenci, jak i konsumenci zakładali, że przy racjonalnym użytkowaniu produktu kolejny zakup nie będzie konieczny przez bardzo długi czas. Obecnie, pomijając samą jakość produktów (co jest tematem na inną, obszerną, dyskusję), ogromną popularnością cieszy się sprzedawanie pakietu usług, które działają w określonych warunkach, czasie i na określonym sprzęcie.

Najczęściej spotykanym podejściem jest model czasowych subskrypcji, które na określony czas odblokowują określone materiały. Wyróżnić tu można wówczas podejście typu:

- Pay per use – płać wówczas gdy korzystasz; np. smart zraszacze mogą aktywować się tylko w określonych warunkach,

- Pay per outcome – płać do osiągnięcia celu; np. maszyna może funkcjonować tak długo, jak nie zostanie osiągnięte przyjęte kryterium wykonania,
- Pay per time period – płać za określony czas; np. usługa kamer jest opłacona na określony przedział czasu.

Warianty usługi zależą od celu, któremu ma służyć Internet Rzeczy oraz od typu klienta, dla którego jest on przeznaczony – sprzedawana jest licencja odnawialna w określonych ramach czasowych.

Stoi to w pewnej sprzeczności z dotychczasowym modelem jednorazowej sprzedaży, do którego wiele firm zdążyło się już przyzwyczaić, ma jednak swoje uzasadnienie – wynika z faktu chęci kontroli (usługa w trybie on demand) przez użytkowników.

Zupełnie innym trendem IoT jest zagadnienie dotyczące sztucznej rzeczywistości (ang. virtual reality, VR).

Ostatnimi laty dał się zauważyć wysyp wszelkiej maści hełmów, okularów i innych urządzeń, których celem jest albo wprowadzenie nas w odmęty wirtualnego świata, albo rozszerzenie naszej rzeczywistości o wirtualne możliwości.

Istnieją tu bowiem dwie szkoły – jedna, która pracuje nad rzeczywistością rozszerzoną (ang. augmented reality, AR), w której “poszerzamy” nasze spektrum wiedzy i interakcji ze światem oraz rzeczywistość wirtualna.

Mając dostęp do nowych technik wizualizacji, możemy korzystać z technologii za pomocą zwyczajnego telefonu lub tabletu, rozwiązania są proste do zintegrowania oraz są naturalnym krokiem w rozwoju IoT (tzn. łatwym do podążania).

Rzeczywistość wirtualna stawia z kolei na nowe doznania wynikające z możliwości korzystania z hełmów przenoszących nas do cyfrowych światów.

Wraz z peryferiami, które symulują ruch, przeciążenia, odepchnięcia i wchodzą w reakcje z innymi zmysłami, użytkownik zaczyna fizycznie doświadczać nowych doznań. Minusem jest jednak wysoki koszt inwestycji, trudność w skutecznej implementacji oraz niechęć lub lęk zwyczajnych użytkowników.

To właśnie VR i AR, moim zdaniem, stanowić będą przykład “czarnego konia” Internetu Rzeczy. To właśnie rozszerzenie rzeczywistości wirtualnej najmocniej wytyczy kierunek rozwoju branży.

O ile bowiem subskrybcje i swoboda wyboru metod interakcji stanowią niepodważalne zalety dla konsumenta, tak prawdziwą rewolucję zaznamy dopiero wtedy, gdy świat IoT poszerzy nasze cyfrowe horyzonty i doznania.

Gdy wyjdziemy poza zwyczajowe ramy integracji i, dosłownie, ujrzymy nowe możliwości interakcji.

Jeszcze dwie dekady temu Internet rozszerzył naszą świadomość o nieograniczone zasoby wiedzy. Internet Rzeczy wprowadza podobną rewolucję oferując nam nieograniczone zasoby zmysłów.

Kwestią czasu pozostaje umiejętne wykorzystanie tych możliwości.

IOT A SIECI

Sprawne funkcjonowanie produktów Internetu Rzeczy opiera się o skuteczne zbieranie, przesyłanie i przetwarzanie danych.

Tego typu czynności wymagają jednak odpowiednich technologii, które będą przystosowane do wysokiego obciążenia transmisją danych.

Pamiętaj, że niejednokrotnie mamy do czynienia z milionami urządzeń działających równocześnie na określonym terenie. Każde z nich zbiera dane, przesyła je do chmury, gdzie poddawane są obróbce, i realizuje dalsze zadania.

Minie jeszcze wiele lat nim rynek przestanie być chaotycznym bytem pełnym wielu podejść, operatorów, metodyk, ekosystemów i standardów, i dojrzeje na tyle, by móc wyłonić technologicznego zwycięzcę.

Jednak już dziś możemy określić trzy typy połączeń, które opanowały rynek:

- traditional cellular – w ramach której funkcjonują sieci GSM (2G), UMTS (3G) oraz LTE (4G),
- proprietary LPWA – w ramach którego działają firmy i standardy Sigfox, Lora, Ingenu,
- cellular LPWA – gdzie funkcjonuje NB-IOT, EC-GSM-IOT oraz eMTC.

Każde z tych rozwiązań zostało opracowane z myślą o zaspokojeniu pięciu podstawowych wymogów sprawnie działającego IoT:

- niskiego zużycia energii*,
- wysokiego współczynnika przesyłu danych,
- obszaru potencjalnego działania,
- dwukierunkowej komunikacji,

- mobilności.

Rozważając IoT najczęściej zetkniesz się jednak z pojęciem LPWA (Low Power Wide Area) – technologią, która została opracowana specjalnie dla celów obsługi IoT.

Dzięki tej technologii został zredukowany koszt implementacji i obsługi rozwiązań (mniej anten, połowiczny duplex, lepsza przepustowość), przygotowano się pod obsługę rzędu miliona użytkowników na kilometr kwadratowy (optymalizacja sygnału, hybrydowe automatyczne odpowiedzi zapytań, adaptacyjna modulacja), zwiększono czas działania baterii (tzw. power saving mode, elastyczne usypianie sprzętu) co wydłuża czas funkcjonowania niektórych produktów do ponad dziesięciu lat i w końcu poprawiono samo pokrycie terenu (za pomocą lepszych technik przesyłu danych pokroju PSD).

Kontynuując powyższe rozważania można stwierdzić, że nastąpił swego rodzaju rozłam na dwa ekosystemy – proprietary LPWA oraz cellular LPWA.

Proprietary LPWA charakteryzuje się możliwością ustanowienia prywatnej sieci bez konieczności certyfikacji, za to z niskim czasem time-to-market – co pozwala na szybką realizację pomysłu i wpuszczenie go na rynek.

Obecnie na rynku funkcjonuje m.in trzech kolosów[5], którzy dyktują warunki:

- LORA – założona przez firmę Semtech, która opatentowała technologię CSS (Chip Spread Spectrum) umożliwiającą sprawne kodowanie i dekodowanie informacji,
- SIGFOX – firma Sigfox promuje własną technologię, która opiera się o sprawną komunikację obiektów, bramek oraz chmury,

[5] No dobra – tych kolosów jest dużo więcej, ale to już przeczytasz na stronie smartzrzeczy.pl :)

- INGENU – konsorcjum, które oparło swe rozwiązania o technologię RPMA (Random Phase Multiple Access), która jest kombinacją stanów pozwalających na lepszą komunikację maszyny z maszyną.

Ryzyko, jakie sprowadza na siebie korzystanie z proprietary LPWA, ogranicza się zasadniczo do braku gwarancji na oferowane usługi, niepewnego czasu ich trwania/dostępności, limitowanego wypuszczenia na określone rynki i braku możliwości migracji mającej na celu wsparcie nowszych standardów.

Po "drugiej stronie barykady" znajduje się cellular LPWA – standardy, które wprowadzane są wolniej i dłużej, ale oferują w zamian globalne pokrycie świata, jakość usługi, są wspierane w czasie rzeczywistym i na wielu systemach oraz pozwalają na migrację (upgrade) do nowszych technologii.

W tym przypadku mowa jest o takich ekosystemach jak:

- eMTC – enhanced machine type communication – zoptymalizowane rozwiązanie dla mobilnych urządzeń,
- NB-IOT – narrowband IoT – zoptymalizowane rozwiązanie z minimalnymi opóźnieniami w przesyle danych. Jest ono tańsze niż eMTC i wspiera do 50 tysięcy urządzeń jednocześnie, stąd chętnie korzysta się z niego m.in. w fabrykach,
- EC-GSM-IOT (znany dotychczas jako EC-EGPRS) – akronim od słów Extended Coverage Global System for Mobile communication Internet of Things, który opracowano z myślą o wydłużeniu działania produktów opartych o technologię GSM. Wzmocniono jakość zabezpieczeń i obniżono koszt implementacji technologii w porównaniu do GPRS.

Czy potrzebujemy tyle różnych standardów?

Okazuje się, że tak.

Niektóre sprawdzają się doskonale na niewielkim obszarze (NB-IOT), zaś inne lepiej poradzą sobie z większymi paczkami danych (eMTC).

Czy możemy jednak wskazać jednego zwycięzcę technologii LPWA?

Wszystko będzie zależeć od rynku i jego potrzeb oraz tego, jak będą rozwijać się same technologie i branża.

Na ten moment jest to wciąż temat mocno dyskusyjny i, w niektórych kręgach, kontrowersyjny.

IOT A ZUŻYCIE ENERGII

Dotychczas wspomniałem Internet Rzeczy jako medium, które zbiera, magazynuje i przetwarza dane celem lepszego zrozumienia użytkownika danego produktu, środowiska oraz ich wzajemnych relacji.

Teraz chciałem opisać inną, równie interesującą właściwość, dzięki której stosowanie Internetu Rzeczy staje się tak popularne – oszczędzanie zużycia energii.

Połączone urządzenia, przetwarzane dane, spersonalizowany sposób użytkowania technologii, nieustanna łączność i potencjał skalowalności – wszystkie te elementy przyczyniają się do redukcji zużycia energii.

Urządzenia śledzą poczynania użytkownika, dostarczają mu odpowiednich danych i tym sposobem poprawiają ogólną efektywność korzystania z zasobów naturalnych.

Jeszcze do niedawna stosowano nierzadko w firmach podejście, w którym rytm zużycia surowców był warunkowany przez koszty, szczegółowo prowadzone komórki księgowe excela i biurowe procedury, a największym sukcesem firm było opłacenie rachunków na czas. Nie zawsze optymalizacja stanowiła nadrzędny cel działania organizacji.

IoT wprowadza perspektywę, w której oszczędzanie energii i kontrola nad zużywanymi zasobami stanowią kluczowe elementy.

Począwszy od optymalizacji pracy klimatyzatorów i żarówek, które uruchamiają się jedynie w określonych warunkach (np. gdy temperatura osiągnie określony pułap), poprzez tryb nocny, w którym redukuje się zużycie oczyszczaczy powietrza, aż po sensory i aktuatory, które precyzyjnie uruchamiają działanie maszyn dopiero wtedy, gdy ktoś zamierza z nich skorzystać.

Do tego implementowane są “zielone technologie” np. w postaci solarów lub specjalnych spłuczek w toaletach posiadających czujniki korygujące zużycie zbiorników wodnych, które oferują dodatkową oszczędność finansową i energetyczną.

Dzięki holistycznemu podejściu, w którym dane są nieustannie dostarczane, najważniejszy filar działalności Internetu Rzeczy stanowi analiza danych i sposobu życia. W dodatku ciągła nauka i udoskonalanie technologii powodują, że z każdym rokiem taka analiza staje się coraz bardziej skuteczna – my rozumiemy zebrane dane produktów IoT, a i systemy samodoskonalą się i optymalizują.

Dla rozwoju IoT ma również duże znaczenie świadomość społeczeństwa.

Ludzie coraz bardziej przekonują się do wchodzących na rynek technologii, w tym IoT. Chcą zastępować nią stare rozwiązania, dokształcać się w tym obszarze i uczynić krok w stronę zunifikowanego i połączonego świata.

Ekologia, oszczędzanie energii, czyste i odnawialne zasoby – konsumenci coraz częściej chcą żyć wygodnie, bezpiecznie i stabilnie i chcą, aby ich środowisko życia było również higieniczne i bezpieczne.

Chcą mieć świadomość, że ekosystemy IoT działają efektywnie i nie marnotrawią zasobów. IoT pozwala osiągnąć taki stan ze względu na tzw. connectivity czyli poziom połączenia, spójności i świadomości technologicznej.

A ta widoczna jest na każdym kroku SMART świata.

W jaki sposób SMART świat oszczędza środowisko?

Począwszy od tak prostych rozwiązań jak redukcja zbędnych papierowych rachunków (wszystko odbywa się cyfrowo i z minimalnym nakładem pracy ludzi), które pozwalają zaoszczędzić tony celulozy i tuszu, skończywszy na dostępie do portali, które w czasie rzeczywistym przewidują i kalkulują trendy dotyczące zużycia

energii oraz monitorują aktywność poszczególnych elementów otoczenia (żarówek, kanalizacji, zużytej wody etc.).

Kolejnym krokiem jest implementacja HEM (Home Energy Management) czyli systemów do estymowania i kontrolowania konsumpcji zasobów w gospodarstwie domowym.

Możemy śledzić już nie tylko samo środowisko (np. zużycie elektryczności), lecz i poszczególne jego elementy. Kontrolować można jakość komponentów oraz ich stabilność, a implementacja sensorów i aktuatorów pozwala reagować na wszelkie usterki typu pęknięta rura kanalizacyjna lub przepalony bezpiecznik.

Stąd już tylko krok do semi-inteligentnych maszyn i automatyzacji, która świadomie i bez ingerencji człowieka zareaguje na potencjalne zagrożenia i zdecyduje o efektywnym zużyciu zasobów np. samoistnie wyłączy oświetlenie w opustoszałym pomieszczeniu lub uruchomi kontrolę temperatury w zbyt zimnym pokoju.

Implementacja HEM-ów pociągnie za sobą konieczność wdrożenia TOU pricing czyli Time-of-Usage pricing.

Jest to podejście, w którym nie tylko wiemy, co i kiedy robimy z naszą energią, ale jesteśmy na bieżąco informowani jak zaoszczędzić i opłacać rachunki wyłącznie za rzeczywiste zużycie. Nie wykupujemy miesięcznego, przybliżonego pakietu abonamentu, lecz płacimy dokładne, precyzyjnie skalkulowane rachunki.

Wchodzimy zatem na nowy poziom kontroli, która w inteligentny sposób może określać wysokość stawki i częstotliwość wykorzystania materiału.

Nie twierdzę, że takie rozwiązania są proste do zaimplementowania.

Wręcz przeciwnie – należy liczyć się z bardzo wysokim kosztem wejścia na rynek, wynikającym z kosztu implementacji opartej o konieczność wymiany tradycyjnych technologii na cyfrowe.

Pamiętaj też o niepełnej konsumenckiej świadomości i skomplikowanych instalacjach SMART rozwiązań.

Do tego rynek jest “rozwodniony i mglisty” przez szereg mniej lub bardziej uczciwych firm, co czyni ten rynek mocno nieczytelnym w aspekcie “kto zajmuje się czym”.

Na domiar złego dochodzi fakt, iż sami Klienci nie do końca ufają firmom IoT (co jest częściowo uzasadnione, zważywszy na to, jak często słyszymy o wyciekach danych i słabej polityce ochrony systemów i protokołów IoT).

SMART społeczeństwo potrzebuje jeszcze mnóstwo czasu, motywacji i chęci do zmian, by w pełni skorzystać z dobrodziejstw SMART świata.

Ale może nie będzie aż tak źle?

Technologia tanieje, postęp i świadomość napędzają proces zmian, a miraż urządzeń, kontrolerów, aplikacji, sensorów, hubów i sieci staje się rzeczywistością, w której warto żyć.

IOT A BEACONY

Tyle gadamy już o IoT, a w świetle reflektorów nie postawiłem jeszcze jednego z najważniejszych aktorów tego filmu – beaconów.

W przeciwieństwie do sensorów, które analizują i badają środowisko oraz aktuatorów, które reagują na potrzeby sensorów, beacony stanowią nieustanny przekaźnik informacji, która wysyłana jest w powietrze.

To niewielkich rozmiarów urządzenia, których zadaniem jest nieprzerwane emitowanie pasma informacyjnego, które może być odczytane przez znajdujące się w pobliżu smart urządzenia np. telefony komórkowe. Beacony są swego rodzaju latarnią morską, która nadaje w powietrze licząc, że ktoś będzie mógł skorzystać z przekazywanej informacji.

Sens instalowania tych urządzeń sprowadza się do możliwości nieinwazyjnego przekazywania informacji w sposób szybki, łatwy i bezpieczny. Sygnał wykryty przez smart urządzenie przekazuje unikalną wartość ID beacona, którą telefon, przy pomocy Internetu i „chmury”, rozkodowuje na postać polecenia. Każdy beacon ma bowiem unikalną wartość, tak samo jak komputery mają unikalną wartość MAC, co pozwala rozróżnić je bezpośrednio z tłumu i nadać im unikalny charakter.

Co się tyczy kodowanej informacji – jest ona przekazywana w postaci paczki, która, w zależności od standardu, może zawierać:

- ID urządzenia
- Informację na temat zużytej energii
- Typ przekazywanych danych
- Czas życia baterii
- Dane dotyczące telemetrii
- Adres URL

- Ephemeral ID (rodzaj klucza zabezpieczającego)

Część danych służy serwisantom i analitykom, lecz z perspektywy użytkownika najważniejszy jest adres URL, który może aktywować unikalną usługę. Unikalną w kontekście miejsca, czasu i typu klienta.

W przypadku sklepów może to być np. zakodowany portal ze zniżkami na konkretne produkty. W przypadku lotnisk – informacja dotycząca najbliższego baru. W przypadku hotelu – adresy najtańszych taksówek itd.

Wszystko sprowadza się do kreatywności programistów, którzy starają się zaszyć w kodzie i zaoferować klientom unikalną wartość dodaną, która nieinwazyjnie pojawi się z pomocą gdy będą oni tego potrzebować.

O tę „troskę” walczą obecnie trzy standardy:

- iBeacon
- EddyStone
- AltBeacon

Pierwszy został opatentowany przez firmę Apple i prócz unikalnych adresów ID lokalizujących dany beacon (UUID, Major ID, Minor ID) w konkretnym kraju, pozycji i lokalizacji nie oferują w zamian nic więcej.

Eddystone wynaleziony został przez firmę Google, która, w przeciwieństwie do Apple, postawiła na otwarty standard. Open sourcowe rozwiązanie dedykowane na wiele platform oprócz niepowtarzalnych adresów ID oferuje możliwość kodowania danych dotyczących URL, TLM (telemtria) oraz EID (ephemeral ID).

Ostatnim standardem jest AltBeacon – open sourcowe rozwiązanie dostępne na gitHubie, które nie przytłacza swym skomplikowaniem, jest intuicyjne w implementacji i pozwala developerom na szybką realizację projektów (w porównaniu do iBeacon oraz EddyStone formalności wdrażania i certyfikowania wydają się być dużo prostsze).

Rzecz jasna, jak każde rozwiązanie, i to posiada pewne wady i problemy nad którymi trzeba się poważnie zastanowić.

Po pierwsze beacony pozwalają na istnienie czegoś co nazywa się piggybacking, a sprowadza się do doradzania klientowi na nieswoim środowisku. Dla przykładu mógłbym zainstalować beacon Sony w pobliżu sklepu sprzedającego produkty Samsung i doradzać jak złym pomysłem jest kupno produktów koreańskich producentów.

Po drugie istnieje showrooming czyli świadome przechwytywanie klientów i przekierowywanie ich na „konkurencyjną" platformę.

W końcu działa spoofing czyli imitowanie stanu np. klienta celem oszukania danego lokalu, w którym akcja wywoływana jest przez konkretną reakcję.

Stąd beacony nieustannie kojarzone są z tzw. planowanie 10P co odnosi się bezpośrednio do angielskich słów, które mają ułatwiać świadome i racjonalne montowanie beaconów w środowisku:

- Planning (gdzie dokładnie zamontujemy urządzenia, dla kogo, kto będzie z nich mógł skorzystać)
- Placement (dokładna, fizyczna lokalizacja w kontekście terenu i właściwości budynku)
- Propagation (siła sygnału, która musi trafić do określonego konsumenta)
- Procurement (świadomość, że beacon będzie rozgłaszał się wtedy i tylko wtedy gdy będzie to niezbędne; ergo sensowne umiejscowienie)
- Permission (czy lokalizacja wiąże się z dodatkowymi uprawnieniami, zgodami itp.)
- Privacy (umieszczenie widocznej notyfikacji o tym, że lokal znajduje się w obrębie działani beaconów)
- Process (prawidłowe ID i inne aspekty techniczne)
- Power (na jak długo działa jeden cykl baterii)

- Presentation (jak prezentuje się samo urządzenie tzn. walory estetyczne dla klientów i lokalu)
- People (kto się zajmie dodatkowymi działaniami jak utrzymanie etc.)

a co w konsekwencji ma usprawnić wdrażanie beaconów do środowiska.

IOT A BLOCKCHAIN

Poruszając temat Internetu Rzeczy trzeba mieć świadomość istnienia i funkcjonowania technologii blockchain.

Choć pozornie oba zagadnienia nie są ze sobą bezpośrednio powiązane - szczególnie gdy myślimy o blockchain jedynie w wymiarze kryptowalut – to jednak, jak się zaraz okaże, obie technologie wpływają na swój rozwój.

Technologia „łańcucha bloków” opiera się o ideę zdecentralizowanej i rozproszonej bazy danych, która przechowuje listę wszystkich transakcji, nieustannie rosnąc z upływem czasu.

Jest to założenie, u którego podstaw leży transparentność, niezależność oraz bezpieczeństwo, które składają się na system funkcjonującego łańcucha.

Każda kolejna, dodatkowa transakcja odnotowywana jest w formie informacji, która trafia do łańcucha wydłużając go i czyniąc coraz to bardziej rozbudowanym i jednocześnie skomplikowanym.

Obecnie niemal cały świat przeżywa swego rodzaju „gorączkę złota blockchain” wynikającą z popularności Bitcoina i Etherium (dwóch najbardziej rozpowszechnionych kryptowalut), które w niedługim czasie osiągnęły zawrotną wartość finansową.

Ich cyfrowa forma (tzn. świadomość, że nie jest to realny, namacalny byt) nie przeszkodziła w rozkwicie popularności, a rynek wirtualnych kopalni oraz walut, których obecnie, jak podaje coinmarketcap, jest już przeszło 1865, zaczął rosnąć i puchnąć z dnia na dzień.

I choć niektórzy nazywają całą tę sytuację spekulacyjną bańką, która pęknie niczym bańka milenijna, tak sam koncept blockchain i ogólnodostępnego wykazu aktualnie wykonywanych „transakcji”

wydaje się być idealnie przemyślanym rozwiązaniem stworzonym dla Internetu Rzeczy.

Zastosowane technologie blockchain rozwijają się coraz szybciej, a ich dojrzałość widoczna jest wraz z kolejnymi proponowanymi rozwiązaniami.

Początkowo chodziło wyłącznie o zdecentralizowaną cyfrową walutę która miałaby służyć przeprowadzanym transakcjom. Dla przykładu algorytmy wykonujące walidację dokonywały weryfikacji stempla z konkretną datą powiązując unikalną transakcję do łańcucha.

Klucze zostawały wymienione pomiędzy zainteresowanymi stronami, podpisy złożone, a matematyczny i kryptograficzny algorytm czyniły całość w pełni anonimową i bezpieczną w użytkowaniu strefą.

Obecnie, w aspekcie makro, blockchain i cyfrowe waluty rozszerzone zostały również o produkty z obszaru IoT.

Postępując z nimi analogicznie co z cyfrowymi pieniędzmi tzn. proponując kontrakt pomiędzy dwiema anonimowymi stronami, które informując się o swoim istnieniu.

Co więcej zastosowanie blockchain posiada zaletę w postaci możliwości rozwiązania dwóch podstawowych problemów dręczących obecny rynek IoT:

- dostępne urządzenia nie są prawidłowo identyfikowalne przez inne maszyny znajdujące się w sieci IoT (co jest kłopotliwe biorąc pod uwagę ich różnorodność oraz stopień skomplikowania jak i dostępność komunikacyjnych formatów oraz protokołów)
- po przeprowadzonej udanej identyfikacji dane powinny pozostać w pełni tajne i poufne

Pozostałymi zaletami przemawiającymi za koniecznością badania blockchain jest możliwość zabezpieczenia adresów RFID (tzn.

unikalny, znany wszystkim kod produktu nie może zostać podmieniony przez nowe urządzenie podszywające się), lepsza weryfikacja i namierzanie lokalizacji produktów, poprawione bezpieczeństwo, zarządzanie i ewaluacja procesami (gdyż znane jest rozmieszczenie i stan przedmiotów – wszystko jest w pełni transparentne).

Dodatkowo wysoki stopień dostępności wiązałby się z prywatnością (pseudo anonimowość osób realizujących usługę), której nie mógłby zmienić ani zmodyfikować żaden rząd.

Następstwem tego jest poprawione zaufanie, zredukowanie do zera manipulacji urządzeń, akceleracja tempa transakcji oraz powstałe oszczędności (uwzględniając brak możliwości wprowadzenia opłat ze stron trzecich – wszystko odbywa się na linii producent – kupujący).

Z tego względu technologia blockchain powinna zostać wykorzystana w obszarze m.in. finansowych transakcji, zarządzania tożsamością, fizycznymi podpisami i innymi danymi, których publiczne składowanie w łańcuchu mogłoby przynieść korzyści w postaci harmonizacji rynku.

Póki co pojawiło się jedynie kilku śmiałków, którzy gotowi byli rozpocząć eksperymentowanie z tymi rozwiązaniami:

- Node Token
- open sourcowy Ruff Chain
- IoT Chain
- SmartMesh
- Modum
- Wabi
- WaltonChain
- VeChain

Gdyby popularyzacja udała się na szeroką skalę można by wówczas mówić o erze blockchain 2.0 (pierwszą są kryptowaluty), która stanowiłaby trzon do kolejnej rewolucji, w której oprócz

identyfikowalnych produktów i walut możliwe byłoby śledzenie placówek (usługi) i toczącego się wokół nich życia (blockchain 3.0).

Jak każde rozwiązanie i to posiada pewne wady (szczególnie niebezpieczne z perspektywy IoT):

- możliwość wystąpienia ataku 51% (w przypadku cyfrowych walut gdyby ktoś teoretycznie posiadał 51% rynku mógłby kontrolować kursem lub poczynaniami rynku)
- wysoki stopień skomplikowania (szczególnie dla osób, które nie są obeznane z technologią)
- możliwość straty prywatnych kluczy (które umożliwiałyby identyfikację użytkownika i weryfikację danych)
- nadużycia wynikające z istniejącego stanu pseudo anonimowości

Suma zysków i strat przemawia jednak na korzyść dalszego propagowania blockchain, a potencjał płynący z redukcji kosztów, optymalizacji tempa pracy oraz lepszej kontroli otoczenia sprawia, że zarówno technologie stojące za IoT oraz blokchcain będą z dnia na dzień dojrzewać.

IOT A SPRAWA ANTYKONSUMENTA

Era Internetu Rzeczy, w której inteligentne produkty kształtują rzeczywistość konsumenta, brzmi bardzo obiecująco.

Smart produkty mają dostosowywać się do naszych potrzeb oraz ułatwiać codzienne życie. Oferować wygodę, optymalizować mozolne czynności, zmieniać byt na lepszy.

Niestety ale szczere chęci zdają się na nic kiedy zamiast rewolucyjnych rozwiązań zaczynamy powoli żyć w czasach „smart śmieci". Produktów, które pod pozorem bycia inteligentnym oferują praktycznie zerową wartość dodaną. Przedmioty, które zalewają rynek nagminnie psując „renomę" i „dobre imię" Internetu Rzeczy.

O ile nie można winić ludzi za chęć posiadania produktów, które ułatwiają wykonywaną pracę i czynią życie prostszym tak obserwując rynek IoT można wyróżnić produkty działające w myśl zasady „rozwiąż problem, o którego istnieniu nie miałeś pojęcia".

Wszystko, rzecz jasna, za odpowiednią cenę.

Jaki potencjał może skrywać się za klapkami Hari Mari X Nokona, których jedyną „smart" usługą jest notyfikacja SMSowa klienta o nowych promocjach?

Czemu ma służyć Nespresso Prodigo, które powiadamia nas mailowo o konieczności wymiany kapsułek kawowych?

Dlaczego mielibyśmy nabyć Egg Mindera – dodatek montowany do lodówki – który, po sprawowaniu z tabletem, wysyła nam notyfikację w momencie gdy wyciągniemy ostatnie jajko z lodówki?

Absurd goni absurd, a urządzenia pokroju Kerastase Hair Comb czyli smart grzebienia, który liczy spalone kalorie podczas przeczesywania głowy mnożą się z dnia na dzień.

Potocznym hasłem i zabiegiem marketingowym są slogany pokroju:

- Przyszłość…
- … XXI wieku
- Rozwiązujemy problem…
- Rewolucja w korzystaniu z …
- Nowa magia ….

podczas gdy, jak na ironię, konsument zamiast kupować „rewolucję technologiczną" w istocie nabywa szereg dotychczas nieposiadanych problemów.

Pomijając ZAWSZE zawyżoną cenę produktu, która nijak ma się do wartości prezentowanej usługi mówimy o produktach o ekstremalnie niskim stopniu bezpieczeństwa (rzadko kiedy mało znani producenci inwestują zasoby finansowe w skuteczne systemy szyfrowania).

Od oferowania pseudo dodatków (aplikacja, system punktów, mini poradnik) poprzez ukryty koszt wymiany baterii i peryferiów.

Od dziwnej polityki prywatności aż po słabą jakość akumulatorów i problemy z połączeniem z innymi produktami.

O tak prozaicznym aspekcie jak brak wsparcia aktualizacjami oraz braku możliwości korzystania w przypadku rozładowanego sprzętu (lub pozbawionego łączności internetowej) nie wspomnę.

Komu mają służyć smart solniczki informujące na głos o poziomie soli (Smalt)?

Dla kogo przeznaczony jest smart kosz na śmieci wyświetlający na ekranie poziom zgnicia (Qube)?

Kto zainwestuje w toster wypiekający wybrane emotki (Toasteroid)?

Czy naprawdę potrzebujemy widelca, który po przekroczeniu poziomu „użycia" podczas obiadu zacznie wibrować uniemożliwiając nam swobodne jedzenie (Hapifork)?

Nie dziwią potem statystyki pokroju 80% ludzi wątpiących w sens IoT lub dane, z których wynika, że tylko 20% posiadaczy smart produktów jest z nich zadowolona i świadomie korzysta z oferowanego przez nie potencjału.

Szkoda tylko, że już dziś 60% użytkowników zgłasza codzienną problematyczność smart produktów, a osoby po 55+. roku życia obawiają się stosowania takich produktów w obszarach medycyny, transportu lub finansach.

Jak już pisałem - społeczeństwo trzeba informować o potencjale IoT, dyskutować i na bieżąco rozwiewać problemy oraz wątpliwości.

Walczyć z fałszywymi przeświadczeniami, cyklicznie organizować szkolenia oraz objaśniać kolejne meandry i zagadnienia. Pokazywać im dobre praktyki, sugerować zachowanie, pomagać w dokonywanych wyborach. Demonstrować, motywować i wskazywać wartość dodaną.

Widmo zmian nie nastąpi jednak póki branża sama nie zacznie stosować inteligentnych rozwiązań ale w obszarze produkcji.

Póki nie skupi się na koncepcjach, które chcemy udoskonalić zamiast produktach i usługach, które chcemy wmusić w rynek.

Wówczas to IoT straci swój anty konsumencki charakter.

LUDZIE BOJĄ SIĘ IOT

Skoro już poruszyłem temat antykonsumenta rozwinę nieco swą myśl podkreślając, że ludzie boją się Internetu Rzeczy. A taki wniosek płynie przynajmniej z raportu[6], w którym zapytano respondentów na temat zaufania do IoT.

I mamy klops!

Bo oto okazuje się, że tanie hasła, planowana sprzedaż oraz obroty i niespotykana skala wdrażania tracą na znaczeniu gdy zapytamy zwyczajnych ludzi o opinię.

O to co sądzą na temat Internetu Rzeczy.

Czego oczekują.

Jakie mają doświadczenia.

A to, niestety, nie należy do najprzyjemniejszych.

Już dzisiejszy poziom rozwoju technologii sprawia ludziom umiarkowane trudności w zrozumieniu i prawidłowym działaniu. Już teraz zgłaszane są liczne usterki i kłopotliwe sytuacje. A przecież IoT nie jest jeszcze w pełni dojrzałe!

Smart zegarki, wirtualni asystenci, mierniki, lodówki, termostaty, piekarniki – już teraz ich codzienna problematyczność oscyluje na poziomie ~60%, mimo, że produkty są używanie umiarkowanie często.

Co się stanie gdy zwiększymy częstość obcowania z produktami?

Co gdy dodamy więcej funkcjonalności?

A co się stanie gdy skalą rozwoju obejmiemy autonomiczne pojazdy?

[6] https://assets.dynatrace.com/en/docs/report/2824-iot-consumer-confidence-report-dynatrace.pdf?_ga=2.188215136.916262675.1534940675-863453299.1534940675

Szereg problemów, na które już dziś wskazują klienci, obejmuje m.in. nieufność wobec decyzyjności pojazdu na drodze. Aż 85% osób wyczekuje zagrożenia w postaci usterki, która spowoduje przekroczenie prędkości i kolizję.

Ponad 70% klientów wierzy, że błąd oprogramowania zakończy się wypadkiem, uszczerbkiem na zdrowiu lub śmiercią pasażerów! Ludzie są przerażeni wizją braku kontroli. Boją się podporządkować maszynie, która „świadomie" podejmować będzie decyzje.

Do tego niemal 85% respondentów obawia się, że smart zamki w autach uniemożliwią im dostanie lub wydostanie się z pojazdu, a powyżej 60% osób uważa, że na drogach zapanuje chaos z chwilą wprowadzenia autonomicznych pojazdów i inteligentnych sygnalizacji świetlnych.

Płynie z tego smutny wniosek – prawie 90% zapytanych waha się lub niechętnie planuje inwestowanie w smart pojazdy.

A przecież IoT to nie tylko pojedyncze produkty i pojazdy lecz także ekosystemy świetlne, wodociągowe, energetyczne, bezpieczeństwa, które instalowane i montowane są w określonych budynkach, strefach, lokalizacjach. To przecież również wszelkie kontrolery i systemy optymalizujące zużycie surowców!

Obawy okazują się podstawne skoro obecnie ~40% konsumentów wskazuje na dysfunkcję tych rozwiązań, a liczba niezadowolonych w niektórych krajach waha się niemal do 60%.

Stąd podstawny strach przed utratą kontroli nad własnym domem i jego zasobami.

Aż 80% pytanych wątpi w skuteczność stosowania inteligentnych pomiarów i czujników uważając, że mogą one przynieść więcej problemów niż korzyści.

Spory odsetek twierdzi, że „wadliwe IoT" oznacza brak możliwości dostania się do własnego domu, niemożność kontrolowania świateł, temperatury lub dostępu do innych zasobów/pomieszczeń.

Nieszczególnie nastraja to przyszłe pokolenie konsumentów.

Konsumentów, którzy mieliby dodatkowo powierzyć wysokość swoich opłat systemowi, który autonomicznie wylicza i dostarcza rachunki. Rachunki, które mogą być zawyżone przez błędy w systemie.

To jednak nie dom ani pojazdy stanowią największą bolączkę przekonania IoT. Jest nią medycyna i leczenie za pomocą smart produktów i urządzeń.

Raport wskazuje na gigantyczne obawy pacjentów co do sensu korzystania z autonomicznego systemu wydawania leków, który miałby wyliczać kiedy i ile tabletek wydzielić.

Szczególny lęk wykazuje pokolenie powyżej 55 roku życia, które w żadnym wypadku nie powierzyłoby życia automatowi samoistnie wydającemu leki. Wierzą oni, że IoT przyniesie problemy z medycznymi danymi (przekłamania, pomyłki, nieprawidłowości) i doprowadzi do nieodwracalnych błędów medycznych.

Takie raporty są potrzebne aby uświadomić jak ważna jest edukacja społeczeństwa. Jak niezbędne jest upewnianie ich w słuszności wdrażania IoT. Rozwiewanie ich lęków oraz edukowanie na elementarnym poziomie. Powolna adaptacja do zmian.

Obecna skala konsumenckich doświadczeń świadczy na niekorzyść Internetu Rzeczy, media chłoną historię o nieudanych eksperymentach, a póki organizacje/firmy nie przygotują odpowiednich kampanii i nie przekonają ludzi do swoich racji IoT może być pięknym produktem, z którego konsumenci nie będą chcieli korzystać.

IOT A SPRAWA AMBIENT INTELLIGENCE

Powiało grozą, smutkiem i rozgoryczeniem. Nic tylko położyć się i przykryć telewizorem. A przecież nie oto chodzi, prawda? Chciałem jedynie pokazać Ci różne oblicza IoT – te dobre jak i te mniej.

Żeby lekko rozchmurzyć podkopane morale opowiem Ci co nieco na temat Ambient Intelligence. Co ty na to?

Ambient Intelligence to bardzo ważne pojęcie jako, że jest to kolejny krok występujący podczas technologicznej rewolucji jaka dzieje się tuż na naszych oczach. To następne stadium rozwoju świata IoT, w którym egzystencja opiera się na kooperacji maszyn, urządzeń, sensorów i proptech (Property Technology – smart budowle) komunikujących i kolaborujących ze sobą w sposób inteligentny i autonomiczny.

Mówimy tu o świecie, w którym IoT, mgła oraz wszechobecne komputery są codziennością, a w którym to sprzęt działa w myśl zasad:

- Jestem świadom istnienia jednostki.
- Rozpoznaję i identyfikuję jednostkę.
- Jestem świadom kontekstu (pogoda, wiadomości, ruch, stan).
- Jestem świadom aktywności.
- Jestem adaptowalny do zmiennych potrzeb jednostki.

Ambient Intelligence (AmI) to krok w futurystyczną przyszłość w pełni zautomatyzowanego społeczeństwa, w którym maszyny potrafią myśleć i działać niezależnie od kontroli ludzkiej.

Aby jednak mogło dojść do tego przeskoku musi nań złożyć się kilka istotnych czynników, których suma umożliwią rozwój tej fantastycznej gałęzi technologii.

Po pierwsze musi nastąpić metamorfoza otoczenia jakie znamy na co dzień. Mowa tu zarówno o:

- inteligentnych materiałach (które same się naprawiają, informują o defektach i wchodzą w interakcję ze środowiskiem),
- MEMach (Microelectromechanical Systems; technicznie jest to już obszar biotechnologii i nanotechnologii),
- systemach embedded,
- urządzeniach wejścia i wyjścia
- oraz adaptacyjnym oprogramowaniu.

To świat przyszłości, w którym mówimy o połączeniu na skalę, o której nawet twórcy Internetu i futuryści nie śnili.

Drugim filarem, który musi zostać postawiony jest rozwój inteligencji w szeroko rozumianym tego słowa znaczeniu co oznacza, że wzmożona musi zostać praca nad m.in.:

- naturalną interakcją (mowa, gesty, mimika, feromony etc.),
- zwiększona moc inteligencji obliczeniowej,
- lepsze zarządzanie i kontrola ogólnie pojętymi mediami,
- oraz świadomość kontekstualna.

Dopiero ten inteligentny sznyt, dalsza miniaturyzacja i odchudzanie sprzętu oraz „uczłowieczenie” technologii pozwolą wkroczyć w obszar inteligencji środowiskowej.

Najprostsza analogia może odnieść się do wychowywania dziecka.

Jak i my przekazujemy im wiedzę, wchodzimy z nimi w interakcję i próbujemy nauczyć dobrego zachowania, które czasem przerywane jest przez „świat zewnętrzny” tak i tu trzeba jasno określić, że AmI zadziała wyłącznie w przypadku gdy suma pojedynczych jednostek osiągnie masę krytyczną.

Dopiero gdy pojedynczy klient będzie wchodzić w interakcję z maszyną, a ona będzie przyglądać się jemu i dopiero gdy do głosu dojdą czynniki zewnętrzne, autonomiczne nasłuchiwanie sensorami i reagowanie na zebrane dane to wówczas to będziemy mogli mówić o efekcie inteligencji środowiskowej.

To i fakt, że większość świata zgodzi się na tego typu interakcję i życie.

Będzie to bowiem wymagać ogromnego pokładu zaufania (do maszyn, tego co dzieje się z danymi i w jaki sposób chcemy kształtować nasze życie jako króliki doświadczalne), zrozumienia potencjału i możliwości stojących za tymi działaniami (w tym celności, przepustowości, bezpieczności), zaakceptowaniu użyteczności (maksymalnie user friendly interfejs i pragmatyzm) oraz socjologicznego i ekonomicznego wpływu („Co ja z tego będę mieć?”) pozwolą tej branży rozkwitnąć w należyty sposób.

Rzecz jasna, jak zawsze pojawia się pytanie na co to wszystko.

Jaki jest sens poddawania się woli maszyn, uczeniu ich, dawaniu im wolnej woli kosztem człowieka?

Ano stąd, że społeczeństwa się starzeją, a dzieci nie przybywa. Zmieniająca się demografia wymusza zwiększenie nakładów czasowych i finansowych w rozwój technologii obszaru służby zdrowia lub opieki nad chorymi. Do tego społeczeństwo chce żyć coraz wygodniej (stąd nakłady na e-commerce i możliwość kupowania wszystkiego i zawsze) nie przejmując się potencjalnymi niebezpieczeństwami.

Stąd zatem i bezpieczeństwo ulega zmianie na lepsze obejmując swym kształtem i obszarem coraz większe terytorium.

Stąd coraz większa popularność AmI.

Szczególnie kiedy uwzględnimy w jak krótkim czasie IoT „rozlał” się na cały świat zaś użytkownicy z dnia na dzień pozwolili zaprosić smart produkty do swych domostw.

Nie zdziw się zatem, że idea środowiskowej inteligencji jest abstrakcyjna i nierealna. Wręcz przeciwnie! Jesteśmy coraz bliżej tej sytuacji.

I choć nie wydarzy się to ani za miesiąc, ani za rok, ani za dekadę to wizja ta jest namacalna bardziej niż kiedykolwiek.

MGŁA IOT

A właśnie - tam gdzie kończą się zasoby i możliwości lokalnych maszyn zaczyna się atlas chmur. Tam gdzie kończą się możliwości chmur zaczyna się ulotny świat mgieł.

Wyjaśniliśmy już sobie znaczenie tej frazy w kontekście lokalnym i globalnym?

Najwyższa pora naprawić swój błąd!

Wszyscy twierdzą, że praca w lokalnym środowisku niesie ze sobą szereg korzyści – od błyskawicznego dostępu do zasobów i programów, poprzez zwiększone bezpieczeństwo wynikające z hermetycznego środowiska, aż po możliwość pracy offline w przypadku gdy żadne źródło połączenia do sieci nie jest możliwe. Jak wieść niesie „lokalne = dobre”.

Problemy zaczynają się z chwilą gdy nasze zasoby pamięci, twardego dysku lub mocy przerobowych, z których korzystamy, powoli, acz nieubłaganie, kurczą się. Wówczas to jedynym i skutecznym rozwiązaniem jest skorzystanie z zasobów chmury.

Nieograniczone zasoby, bezproblemowa skalowalność, dostępność do zasobów z każdego krańca świata – to zdecydowanie przemawia na korzyść Cloud. Podobnie jak malejące koszty jakie trzeba zapłacić aby stać się posiadaczem tego środowiska.

IT zauważyło jednak, że oba te światy działają niezależenie od siebie uniemożliwiając tym samym pełne wykorzystanie potencjału maszyn i cyfryzacji.

W związku z tym zadano sobie pytanie – co by się stało gdyby można było połączyć te dwa rozwiązania?

Tak narodziła się mgła czyli architektura, która czerpie pełnymi garściami z obu tych światów skupiając się przy tym na lepszym koordynowaniu pracy z dostępnymi danymi.

Idea opiera się o założenie interakcji środowiska fizycznego (takiego jak Internet Rzeczy lub Embedded) oraz wirtualnego (m.in. chmura) przy uwzględnieniu „stacji pośrednich", które służą jako bufor komunikacyjny, kalkulacyjny oraz kontrolnym (więcej na ten temat poruszyłem w osobnym artykule poświęconym stricte fog nodom).

Mamy zatem dwa podstawowe światy – cloud (służący do kalkulacji) i edge („brudny" świat urządzeń oraz IoT). Pomiędzy nie ulokowany jest fog (ze swymi nodami) , który rozgranicza warstwy Big Data i Business Logic oraz Micro Data Storage i Petabajtów danych.

Brr… poniosło mnie z ambitnymi frazesami stąd wiedz, że wszystko co dotyczy mgły można zamknąć i opisać pięcioma słowami:

- Mierzenie
- Monitorowanie
- Proces
- Analiza
- Reakcja

Każde z tych słów opiera się o jak najszybsze rozpoznawanie zadania, efektywne reagowanie, elastyczne dostosowywanie się do potrzeb oraz jak najmniejsze opóźnienia, które, jak twierdzą włodarze blue chipów, jedynie mgła może sprawnie realizować w szalonym świecie wszechogarniającej cyfryzacji i wzmożonej mobilności.

Podstawowymi zaletami przemawiającymi za korzystaniem z mgły (pomijając rosnące tempo potrzeb dotyczących magazynowania i obróbki danych w czasie rzeczywistym) są m.in. bezpieczeństwo, skalowalność oraz otwartość oferowanych usług.

Mgła pozwala na lepszą kontrolę zaufania oraz prywatności pomiędzy urządzeniami co wynika poniekąd z ulokowania urządzeń w tej architekturze.

Do tego , ze względu na lepszy podział ról urządzeń, widoczny jest wzrost jakości i tempa analizy danych, skuteczniejsze przeciwdziałanie wąskim gardłom oraz doskonalsza wizualizacja i interoperatywność wykorzystywanych zasobów.

Mgła działa również na zasadzie elastycznego, autonomicznego bytu, który, podobnie jak samą chmurą, można swobodnie rozbudowywać, migrować oraz zastępować kolejnymi nodami/serwerami.

A wszystko przy uwzględnieniu zasady RAS tzn. Reliability (niezawodność), Availability (dostępność) oraz Serviceability (serwisowalność).

Mgła działa również przy założeniu łatwo dostępnej i zrozumiałej hierarchii zadań oraz priorytetów i niezwykle przejrzystej programowalności umożliwiającej szybką adaptację infrastruktury, efektywne nią zarządzanie, prostsze w implementacji operacje oraz wzmocnione bezpieczeństwo kierowanych do (i z niej) poleceń.

Nie da się ukryć, że możliwości i skala mgły jest niewyobrażalna. Jej potencjał jest niebywały biorąc pod uwagę jej skalowalność.

Ta może być mierzona przy uwzględnieniu wydajności i rozmiaru (inne nody mogą szybko się podłączać i przejmować kolejne role) oraz zaufania i bezpieczeństwa (mgła dobrze radzi sobie z przeciążeniami oraz klasycznymi problemami Big Data).

Szczególnie mocno da się to zauważyć i docenić w momencie uwzględnienia miliardów urządzeń IoT oraz przeróżnych sensorów, które wysyłają dziesięciokrotnie więcej poleceń wymagających natychmiastowej interpretacji lub reakcji ze strony systemu.

Co ciekawe w tym całym świecie chmur, mgieł oraz granic istnieje miejsce na jeszcze jedno środowisko, które co po niektórzy nazywają Mist (mgiełką?).

Chodzi o takie zestawienie maszyn i zachodzącej pomiędzy nimi komunikacji aby uwzględnić swego rodzaju „mini-komputerki” (low powered computers), które będą ulokowane jeszcze bliżej urządzeń i sensorów wykonując jeszcze bardziej odseparowane zadania.

Uwzględniając skłonność do odseparowywania kolejnych warstw istnieje pewne pole do popisu i uzasadnienie dla tych maszyn jednak ich moc i zalety poznamy zapewne dopiero w niedalekiej przyszłości.

Podstawowe pytanie, które mnie nurtuje to fakt na ile jest to rozwiązanie, które podyktowane zostało potrzebami, a na ile metoda, która ma zasilić portfele najbardziej uznanych graczy rynku IT?

Na ile jest to świadome i skuteczne izolowanie i wykorzystywanie mocy przerobowych, a na ile meteorologiczna zabawa wariacją na temat?

FOG NODE

Zabawa w pogodynkę trwa nadal – wyjaśnię jeszcze idee stojącą za fog nodami.

Podczas gdy przyzwyczajeni zostaliśmy do używania jednostek rzędu mega, giga, terabajtów, a niektórzy byliby nawet skłonni powiedzieć, że wiedzą czym jest petabajt tak w przypadku IoT musimy dokonać kolejnego przeskoku do poziomu exabajtów lub wręcz zettabajtów.

Ale czym jest ten exabajt?

Przecież stwierdzenie, że to miliard gigabajtów lub milion terabajtów nic nam nie powie!

Jeśli jednak powiem, że typowa, roponośna platforma wiertnicza tygodniowo generuje 0,5TB informacji, pół godzinny przelot samolot wypluwa 10TB danych, a Facebook generuje ruch z ponad 500+TB na dzień to powoli zacznie na naszych oczach rysować się rozmiar.

Jednak nadal nie przeskoczyliśmy jeszcze o dwa kolejne poziomy!

I z tym będzie problem jako, że exabajty stanowią nadal abstrakcyjne pojęcie!

Dla przykładu rocznie użytkownicy telefonów komórkowych generują 8EB danych, użytkownicy komputerów szerzą w tym samym czasie 100EB, a 5EB to wszystkie wypowiedziane przez ludzkość słowa.

Jak to się jednak ma do fog nodów?

Fog nody są to niewielkie rozmiarowo urządzenia, które mogą być rozmieszczone w dowolnym miejscu w obszarze transmisji oraz przechwytywania danych, a które to, w ramach swego działania, oferują dostęp do sieci, przechowywania oraz kalkulacji danych.

Mogą zatem być to wszelkiej maści routery, switche, serwery embedded lub kamery monitoringu, które będą stały na pierwszym froncie obsługi danych.

Widzisz, źródłem wszelkiego „zła” w świecie IoT jest fakt, że dane spływają obecnie zewsząd. Generują je zarówno urządzenia wysyłające nieprzerwane pasmo informacji (tzw. Streaming Data Source – samoloty, pojazdy, telewizory, odbiorniki etc.), typowe smart przedmioty (tzw. IoT Data Source – żarówki, krany, kamerki, odbiorniki, sensory, beacony etc.) oraz produkty działające z klasycznymi danymi wygenerowanymi przez ruch w sieci (tzw. Web Data Source – smartphony, smart telewizory, komputery etc.).

Na domiar złego współczesny użytkownik oczekuje, że takie dane:

- Będą miały jak najmniejsze opóźnienie – nawet milisekundy mogą zadecydować o tym jak skutecznie działa system radzący sobie z przekazywanie i przetwarzaniem informacji
- Będą bezpieczne – będą zabezpieczone i monitorowane przed, w trakcie i po przekazaniu
- Będą możliwe do zebrania na całym globie –tzn. zasięg obsługi danych powinien zezwalać na komunikację z produktami na całym globie
- Będą efektywnie zarządzane – zarówno w wymiarze kalkulacji, przetwarzania jak i konserwacji przepustowości sieci

Stąd potrzeba zastosowania fog nodów, które, w przeciwieństwie do klasycznej chmury, radzą sobie z powyższymi problemami nad wyraz dobrze. Ba! Są w stanie analizować dane na bieżąco, działają w czasie poniżej paru milisekund oraz mają dostęp od ręki do historycznych analiz.

A jak bardzo są gotowe na obsługę „dużej ilości zapytań”?

Wystarczy rzec, że domyślnie mają ustawioną przepustowość na, mniej więcej, 2EB danych na dzień.

Efekt skali jest w tym przypadku przytłaczający.

Przyjmując, że niedługo przekroczymy próg 50 miliardów urządzeń IoT, żyjący w erze informacji konsumenci oczekują, że wszystko będzie działać „w locie", problemy będą rozwiązywane przy niskim koszcie napraw (oraz przestoju), zaś komunikacja na linii wszystkich produktów Internetu Rzeczy zadziała niezauważalnie w tle.

Dzisiejsze urządzenia IoT nie są przystosowane ani zaprojektowane z myślą o takiej ilości, różnorodności i prędkości danych oraz nie istnieją dla celu zunifikowanego świata do którego dążymy.

Przy takim tempie generowania kolejnych (pół)produktów oraz kolejnych kanałów komunikacji nie wyrobimy się z wymaganiami, które narzucono za sprawą wygodnictwa, konsumpcjonizmu oraz lenistwa.

Stąd idea fog nodów, które, będąc najbliżej potencjalnego źródła generującego dane, obrabiają informację szybko (zredukowany jest koszt przesłania pasma) oraz bezpiecznie (bo informacja nie musi wypływać poza zamknięty obieg).

A, że dodatkowo mogą oferować działanie w ramach komunikacji maszyna z maszyną lub maszyną z człowiekiem to tym bardziej doceniane są w branży IoT. Szczególnie w obszarze produkcji, logistyki, sektorze publicznym oraz wydobywczym (oleje, gazy, kopalnie etc.).

Ale jak to działa w praktyce?

Ano tak, że dane, które spływają do takiego noda zostają przeanalizowane pod kątem przydatności oraz możliwości obróbki.

Na bazie tych dwóch informacji zostają one przekazane do najbliższego centrum, które będzie w stanie się nimi zająć:

- Najbardziej czułe dane są analizowane w samym fog node najbliższym dla źródła nadawania ze szczególnym akcentem na

bezpieczeństwo oraz kontrolę np. informacje o przekroczeniu temperatury zbiornika, który mógłby doprowadzić do eksplozji

- Dane, które mogą poczekać są transmitowane do agregowalnych fog nodów czyli punktów kontrolnych, które mogą zbierać informacje, analizować je i odsyłać do źródła lub dalszej obróbki
- Dane, które mogą bardzo długo poczekać są emitowane wprost do chmury, w której będą poddane analizie historycznej, przekazane do big data lub przetrzymane do chwili kiedy ktoś będzie chciał z nich skorzystać

Rzecz jasna każde z tych rozwiązań ma swoje specyficzne cechy charakteru:

- Najbliższe dane są ulotne, lokalne oraz przekazywane w mniej niż kilka milisekund
- Dane, które mogą poczekać „żyją" do kilku godzin (lub dni), są szeroko dostępne oraz transportowane są w ułamku sekund lub minut.
- Dane, które mogą długo poczekać przetrzymywane są do paru miesięcy lub lat, składowane są globalnie, a przede wszystkim ich wysyłka i komunikacja może trwać od kilku dni do nawet tygodni.

Pomijając strukturę danych IoT warto podkreślić niebywałe cechy tego, jakże by się zdawało prostego, rozwiązania.

W pierwszej kolejności fog nody zezwalają na lepszą mobilność biznesu, który nie musi martwić się przestojami lub trudnościami w postaci zaników działania. Maszyny działają w locie, tak samo szybko korygują niedoskonałości, a przede wszystkim informują i zapobiegają zamiast leczyć po fakcie.

Do tego wzrasta bezpieczeństwo skoro dane mogą być analizowane przez urządzenie znajdujące się bezpośrednio przy danej jednostce.

Nic nie musi wypływać poza struktury sieci, a kwestie ochrony i wewnętrznej polityki prywatności kontrolowane są jeszcze w centralnym ośrodku nadawczym.

Wzmocniony zostaje monitoring przepływu danych i tego jaki rodzaj delikatnych danych mógłby potencjalnie wypłynąć poza firmę narażając ją w ten sposób na niebezpieczeństwo. Monitoring może objąć skalę dotychczas niespotykaną uniemożliwiając przypadkowe wycieki.

I w końcu, co najważniejsze, maleją koszty – koszty związane z kupnem i maintenancem sieci i związanych z nią urządzeń. Konserwacja jest rzadsza, mniej skomplikowana oraz szybsza biorąc pod uwagę mniejsze ilości danych (lub danych, które nie muszą być wkoło przesyłane do chmury).

A stąd jest już tylko kawałek do poprawy wizerunku firmy, która działa nieprzerwanie, bezproblemowo oraz z uwzględnieniem potrzeb i wymagań klientów.

Wizerunek ulega poprawie, jakość usługi może znacząco wzrosnąć, bezpieczeństwo postawione zostaje na pierwszym miejscu, a, koniec końców, klienci cieszą się, że ich produkty działają responsywnie, gładko i tak jak by sobie tego zażyczyli.

Pytanie tylko do kiedy ten stan pozytywnego letargu będzie trwać i jakie skutki przyniesie moment, w którym nastąpi przerwa w dostawie usług, niespodziewanie przybędzie jeszcze więcej urządzeń do obsługi lub, ot tak po prostu, ktoś nie dopatrzy się uchybienia w systemie, który opublikuje zbierane o użytkownikach dane.

A, że wolumen i waga takich danych już dawno przekroczył zdrową normę to pasmo licznych skandali mamy wliczone w koszt gwarancji zakupionych przez nas urządzeń.

SMART ZABAWKI

Nośnym tematem jest narzekanie na współczesnych rodziców, którzy z uporem maniaka i świadomością laika wyznają wychowanie przez ignorowanie.

Rośnie przekonanie, że potrzeby oraz atencję dziecka można zminimalizować za pomocą zwyczajnego tabletu, konsoli, robota, drona lub innej elektroniki.

Brzdąc jest nią zajęty, oni mają święty spokój, a świat, choć na jakiś czas, staje się jakby lepszym miejscem.

Pomijając już zasadność takiego (anty)wychowania jestem święcie przekonany, że mało który z tych wapniaków zdaje sobie sprawę jakie zagrożenie “zapraszają” do swego życia gasząc ogień ogniem.

Sęk w tym, że obecne smart zabawki są ekstremalnie niebezpiecznymi bublami wykonanymi i zabezpieczonymi w sposób nieadekwatny do oferowanych usług.

Dla przykładu reklamodawcy twierdzą, że oferują edukacyjne produkty skierowane do stymulowania dziecka i zainteresowania go programowaniem, technologią lub empatią i tolerancją (jeśli mamy do czynienia z wszelkiego rodzaju wariacjami gadających lalek).

Używają haseł pokroju „pobudzenia dziecięcej wyobraźni” lub „aktywizacji młodego umysłu” przy jednoczesnym i nieustannym podkreślaniu potencjału swych produktów („Nasze smart zegarki pozwolą Ci bezpiecznie monitorować dziecko”).

Jak na ironię, i jak to w życiu bywa, rzeczywistość jest wręcz odwrotna.

Posłużmy się paroma dowodami.

Zacznijmy od federalnego i zbiorowego pozwu skierowanego przeciw firmie Genesis, która wtłoczyła na rynek smart lalkę My Friend Cayla

– lalkę, która ma wbudowaną obsługę rozpoznawania głosu, interakcji głosowej z dzieckiem, wykorzystywania zewnętrznych peryferiów (grzebienie etc.) i umożliwia kilka innych „smart" funkcji, które mają aktywizować dziecko.

Szkoda jedynie, że producenci nie pokusili się o zareklamowanie dodatkowych funkcji, które wychodzą na jaw dopiero po wnikliwej analizie dokumentu.

Wynika z niego m.in. iż lalka:

- Została zaprogramowana dziesiątkami fraz, które odnoszą się bezpośrednio (lub pośrednio) do produktów Disneya. Lalka opowiada o swoich ulubionych animacjach Disneya, nuci znane piosenki oraz przekonuje jak bardzo lubi Disneyland i jak dobrym pomysłem byłoby udanie się tam wraz z dzieckiem.
- Posiada szereg zapytań, które mają „zacieśnić więź" z dzieckiem, a które to pytania weryfikują imię dziecka, imiona jego rodziców, najczęściej spożywane posiłki, miejscowość, w której żyje latorośl, do jakiej chodzi szkoły etc.
- Przetwarza zapytania na zwyczajne, niezabezpieczone stringi, które przesyłane są do predefiniowanych wyszukiwarek internetowych.
- Posiada politykę prywatności głoszącą, iż „Polityka prywatności może być okazjonalnie aktualizowana więc możesz chcieć ją weryfikować ilekroć decydujesz się przesłać do nas swoje dane".
- Korzysta z dedykowanej aplikacji, której jedynym zabezpieczeniem weryfikującym wiek i prawa użytkownika jest rozwiązanie zadania („suma 11+16 to…"), które za KAŻDYM razem jest jednakowe.
- Opisuje użycie danych na poziomie „absolutnej niezbędności nie dłużej niż jest to wymagane" ale z uwzględnieniem, że dane te mogą być w przyszłości wykorzystane do szeregu „biznesowych zleceń i projektów".

- Mimo, że korzysta z usługi Bluetooth i nawiązuje połączenie z urządzeniami nie informuje użytkownika ani o tym procesie ani o zakończonym sukcesem połączeniu.
- Zbiera dane głosowe, które następnie, za „zgodą” użytkownika, są przekazywane do agencji wywiadowczych i jednostek wojskowych.

A to tylko wybrane i wyselekcjonowane przypadki opisane w dokumencie.

Interesujące w tym wszystkim jest to, że mimo, iż rząd niemiecki uznał tę zabawkę za narzędzie szpiegująco-inwigilujące, które należy zniszczyć, a sama firma posiada szereg spraw sądowych dotyczących etyczności i bezpieczeństwa produktu, tak nadal jest ono dostępne do kupienia.

I nie przeszkadza całej sprawie czarny PR, z którego wynika, że produkt ten jest łatwo hakowalny, że stanowi niebezpieczeństwo dla użytkownika i jest ono wymyślone celem mamienia i niszczenia umysłów dziecka.

„Smart lalka” brzmi na tyle dumnie, że warto jest zaryzykować jej zdobycie.

Odmienną kategorię niedorzeczności wynieść można po analizie funkcjonalności smart zegarków dedykowanych dzieciom.

Mają one za zadanie śledzić dziecko (aby rodzic nie musiał się martwić), pozwalać na szybką komunikację z ojcem lub matką, a że do tego są wykonane z trwalszych materiałów to i mają służyć dziecku jako „niezniszczalny” czaso-odmierzacz.

I znów – okazuje się, że te produkty mają szereg dysfunkcji, o których mało który rodzic wie.

Poczynając od niezgodnych standardów wykorzystanych w urządzeniu, braku szyfrowania BT rozgłaszania (każdy w promieniu 25

metrów może odczytać nazwę zegarka informując tym samym, że jakieś dziecko jest w pobliżu), możliwości bezproblemowego location spoofingu lub zdalnego przechwycenia, aż po dane użytkownika, których nie można skasować (mogą być jedynie „nadpisywane", a dokładniej dopisywane).

Źródłem problemów są również ciągłe przetasowania pomiędzy producentami (jakby chcieli pozbyć się tego gorącego ziemniaka), braki w aktualizacjach sprzętu oraz współdziałanie z 3rd party apps, o których ani dziecko, ani rodzic nie mają zielonego pojęcia.

Dane są przekazywane w sposób „jawny" instytucjom, które z monitoringiem i bezpieczeństwem dziecka nie mają kompletnie nic wspólnego.

Pal licho czy mowa o Gator2, SeTracker, Xplora watch czy innym urządzeniu, które spełnia analogiczną funkcję.

Wszystkie z nich mają niewidoczne na pierwszy rzut oka defekty jawnie godzące w konsumenta.

Każdy z producentów nie posuwa się do odpowiedzialności za produkowane zegarki, a każda kolejna iteracja zdaje się być gorsza i bardziej wadliwa w stosunku do poprzedniej.

Chciałoby się pozostawić jakiś wniosek, z którego wynika, że może nie jest aż tak źle z branżą, a oferowane produkty, w większości, spełniają pewne standardy i normy. W praktyce jednak większość informacji zwrotnej napływającej z rynku wskazuje, że mamy do czynienia z niestabilnymi produktami, które przez specjalistów bezpieczeństwa oraz komentatorów odbierane są w negatywny sposób.

Uchybienia ze strony producentów, nieodpowiedzialne podejście rodziców, nielegalne zastosowania danych, niedopracowane rozwiązania – wszystko to wskazuje, że rynek nie jest gotowy na tego typu zabawki (albo przynajmniej powinien rozważyć zasadność ich tworzenia).

A nie poruszyłem nawet tematu innych nadużyć oraz upokorzeń, które mogą czekać użytkowników, którzy przez słabe zabezpieczenia mogą z dnia na dzień stać się ofiarami cyber przestępców.

Summa summarum potraktuj tę treść jako symboliczny głos sprzeciwu w dyskusji „czy warto bezmyślnie kupować dziecku smart zabawkę?”.

Zapewne nie zmienię nastawienia społeczeństwa ale może zasieję ziarenko wątpliwości przed podjęciem decyzji, która może spowodować destruktywne skutki.

CO DALEJ?

Brawo!

Zrobiłeś pierwszy krok w stronę IoT!

Moje gratulacje!

Mam nadzieję, że nie zanudziłem Cię zbytnio ;)

Jeżeli podobało (lub też nie) Ci się to co przeczytałeś – daj mi znać mailowo na kontakt@smartrzeczy.pl

Jeżeli zaś mało Ci informacji i doskwiera Ci potrzeba dalszego zgłębiania wiedzy na temat IoT wpadnij na www.smartrzeczy.pl !

Zawsze miło jest poznać innych entuzjastów Smart świata.

Do zobaczenia!

Marcin Sikorski