

UNIWERSYTET GDAŃSKI
Wydział Matematyki, Fizyki i Informatyki

Michał Lipiński

nr albumu: 105229

Mariusz Piątek

nr albumu: 205176

Paweł Ponieważ

nr albumu: 228254

**Dom Przyszłości w kontekście
Internetu rzeczy**

Praca licencjacka na kierunku:

INFORMATYKA

Promotor:

dr Włodzimierz Bzyl

Gdańsk 2016

Streszczenie

Celem niniejszej pracy było udowodnienie, że idea Inteligentnego Domu już dawno przestała być czymś zarezerwowanym dla najbogatszych a stała się czymś dużo bardziej przystępny. Niewielkim lub czasem nawet zerowym kosztem można zaimplementować w swoim domu rozwiązania, które w znacznym stopniu ułatwią funkcjonowanie mieszkańcom. W ramach niniejszej pracy udało nam się stworzyć kilka komponentów, które w połączeniu tworzą solidną podstawę pod zbudowanie Inteligentnego Domu. Pierwszym komponentem naszego „Inteligentnego Domu na każdą kieszeń” jest system monitoringu. Udało nam się przy pomocy 2 starych telefonów z aparatem oraz laptopa stworzyć system nadzoru domowego. Przy pomocy framework'a *Meteor* oraz modułu *node-cam*, zabezpieczając wszystko modułem *basic-auth* osiągnęliśmy zerowym kosztem rozwiązania porównywalne z dostępnymi na rynku komercyjnych solucji. Następnie, również niewielkim kosztem, stworzyliśmy system inteligentnych światel. Zamówione z serwisu *AliExpress* sterowniki, kierowane za pomocą aplikacji *Magic Home*, umożliwiły sterowanie oświetleniem w sposób nieosiągalny dla tradycyjnych rozwiązań. Możemy nie tylko sterować oświetleniem z poziomu aplikacji na telefon, ale również ustawać czasowe przełączniki, sterować światłem przy pomocy klaśniecia dłoni, czy włączyć tryb muzyki, w którym oświetlenie pulsuje w rytm aktualnie słuchanego utworu. Możemy przyciemnić światło bez wychodzenia z łóżka – jest to coś, co do niedawna mogliśmy oglądać tylko w filmach. Rozwój technologiczny postępuje w zawiartym tempie. Inteligentny Dom nie musi być drogi, a nasze rozwiązania jeszcze bardziej utwierdziły nas w tym przekonaniu.

Słowa kluczowe

dom inteligentny, zdalny dom, inteli home, internet of things, arduino, dom XXI wieku, dom multimedialny, zdalne zarządzanie, mikrokontrolery, sterowany dom, zakodowany dom, internet rzeczy, technihouse, remote home-

stead, smarthome, nfc, iot, security iot, wearables, wearable technology, smart clothes, raspberry pi, arduino, avr, LED strips

Spis treści

Wprowadzenie	6
1. Internet rzeczy	8
1.1. Informacje ogólne o Internecie rzeczy	8
1.2. Warunki istnienia IoT	9
1.3. Korzyści wynikające z wykorzystania Internetu Rzeczy	10
2. Kierunki rozwoju Internetu Rzeczy	13
2.1. Warunki rozwoju IoT	13
2.2. Idea rozwoju Internetu Rzeczy	14
2.3. Zagrożenia płynące z rozwoju IoT	16
3. Doświadczenia praktyczne	20
3.1. Wykorzystanie Arduino przy budowaniu własnych projektów	20
3.2. Projekt inteligentnego nawadniania roślin	22
3.3. Budowa własnego systemu monitoringu	24
3.4. Budowa inteligentnego oświetlenia	27
Zakończenie	31
Bibliografia	33
Spis rysunków	35
Oświadczenie	36

Wprowadzenie

Internet jest znany na całym świecie, przeciętnemu użytkownikowi kojarzy się on z siecią komputerów, które są ze sobą połączone. Dziś internet oznacza dużo więcej niż tylko komputery, przy których siedzą ludzie. Co raz częściej to również urządzenia i maszyny, z których każdy na co dzień korzysta. Takie połączenia miliardów różnych czujników, komputerów i innych urządzeń jest dużą zmianą w życiu nas wszystkich, dlatego też często mówi się o tym jako o kolejnej rewolucji internetowej. Termin „*Internet rzeczy*” z ang. „*Internet of Things*”, w skrócie *IoT*, to koncepcja stworzona przez *Kevina Ashton*a podczas prezentacji przygotowanej dla *Procter & Gamble* w 1999 roku [1]. Można ją tłumaczyć na wiele różnych sposobów, natomiast najlepiej określa się ją jako ekosystem, w którym przedmioty, dzięki wyposażeniu w sensory, komunikują się z komputerami. Dla wielu ludzi to nadal coś niewyobrażalnego, ale niedługo w jedną sieć będą połączone ze sobą praktycznie wszystko. Wiele nowych możliwości staje otworem dla ludzi, którzy zajmują się marketingiem i komunikacją, lecz nie tylko. Tematem naszej pracy jest przybliżenie ideologii *Inteligentnego Domu* z wykorzystaniem *Internet of Things*. Cel jaki obraliśmy to przybliżenie w/w tematyki i obalenie mitu, głoszącego iż rozwiązania muszą być kosztowne i skomplikowane do zaimplementowania. Inteligentny Dom to określenie, które mówi o bardzo zaawansowanym technicznie budynku. Nie zawsze jest to budynek mieszkalny, mogą to być także biura, firmy czy hale produkcyjne. Inteligentny budynek charakteryzuje się posiadaniem dużej ilości detektorów i czujników, zamieszczonych w ścianach, podłodze czy przy suficie. Wszystkie instalacje, połączone ze sobą, tworzą jeden zintegrowany system zarządzania budynku. Systemy te pozwalają na to, aby budynek mógł reagować na zmiany środowiska. Wszystkie te działania maksymalizują komfort użytkowania, funkcjonalność oraz bezpieczeństwo. Dzięki nim możemy także zaoszczędzić energię czy wodę, zmniejszając w ten sposób koszty eksploatacji, a także pozwalają na zmniej-

szenie emisji zanieczyszczeń do środowiska. Inspiracją do pochylenia się nad przedstawionym zagadnieniem był projekt, na który wpadł mój kolega parę lat temu (www.windfreaks.pl), który miał wspierać naszą pasję, jaką jest kiteboarding, poprzez budowę kilku stacji pogodowych oraz kamer HD rozciągniętych wzdłuż wybrzeża zatoki Gdańskiej oraz półwyspu Helskiego. Miało to na celu dostarczanie rzetelnych danych pogodowych. Jednym z głównych źródeł była książka Michaela Millera pt. „The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World” [2]. W przygotowaniu pracy ważną rolę odegrał raport „Internet Rzeczy w Polsce” [3] oraz książka „Internet rzeczy, Bezpieczeństwo w Smart City”, wydawnictwa C.H. Beck [4]. Praca składa się ze wstępu, trzech rozdziałów merytorycznych oraz podsumowania. Wstęp zawiera ogólny opis problematyki pracy i celów w niej postawionych. Pierwszy rozdział to bardziej szczegółowy opis terminu „*Internet of Things*”, warunki jego istnienia oraz jego korzyści i wyzwania prywatności w Internecie Rzeczy. Drugi rozdział to zagłębienie się w temat warunków i idei rozwoju *IoT* oraz zagrożeń zeń płynących. W trzecim rozdziale opisane zostały rozwiązania praktyczne w oparciu o solucje dostępne na rynku oraz trzy projekty naszego autorstwa podzielone na systemy:

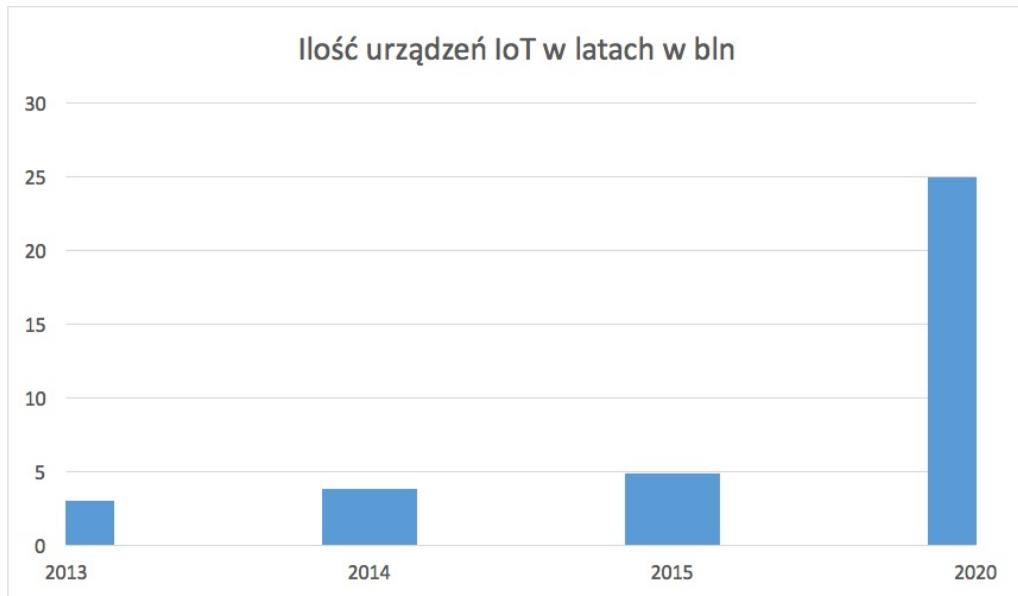
- inteligentnego nawadniania roślin
- własnego systemu monitoringu
- inteligentnego systemu oświetleniowego

ROZDZIAŁ 1

Internet rzeczy

1.1. Informacje ogólne o Internecie rzeczy

Żyjąc w XXI wieku, jesteśmy świadkami wielu cyfrowych rewolucji. W 1990 John Romney podłączył toster do sieci internet, dzięki temu mógł włączać i wyłączać to urządzenie zdalnie[5]. Było to pierwsze na świecie urządzenie podłączone do internetu, które zapoczątkowało rewolucję znaną nam jako Internet Rzeczy. Są one szybsze, łatwiejsze i jeszcze bardziej efektywne niż były dotychczas.



Rysunek 1.1. Ilość urządzeń IoT , źródło: Gartner, listopad 2014r.

Pewna część społeczeństwa widzi w *IoT* szanse, inni boją się, że po- stępująca cyfryzacja za bardzo rozpowszechnia się w naszym życiu. Mi- mo wszystko, liczba urządzeń podłączonych do Internetu wzrasta w bar- dzo szybkim tempie i szacuje się, że do 2020 roku osiągnie ponad 25 mld urządzeń na całym świecie (rys. 1.1). Stefan Ferber, na łamach portalu *Harvard Business Review*, twierdzi, że w 2015 roku nie tylko ponad 75% populacji będzie korzystać z Internetu, ale również około 6 miliardów urzą- dzeń [6]. Możemy do nich zaliczyć smartfony i laptopy, a także samochody, fabryki, a nawet całe miasta [7], gospodarkę wodną czy systemy obronne. IoT wpływa między innymi na projektowanie i serwis, a także na zarządzanie zasobami ludzkimi, dzięki czemu stwarza ogromne szanse na „lepsze jutro” w dziedzinie biznesu.

1.2. Warunki istnienia IoT

Jak już wcześniej wspomniano, *IoT* może być rozumiany jako ekosystem, w którym komunikacja występuje z udziałem człowieka, lub bez niego. Aby móc wymienić informacje między dwoma przedmiotami, należy speł- nić określone warunki. Pierwszą ważną rzeczą jest fakt, iż przedmiot, który



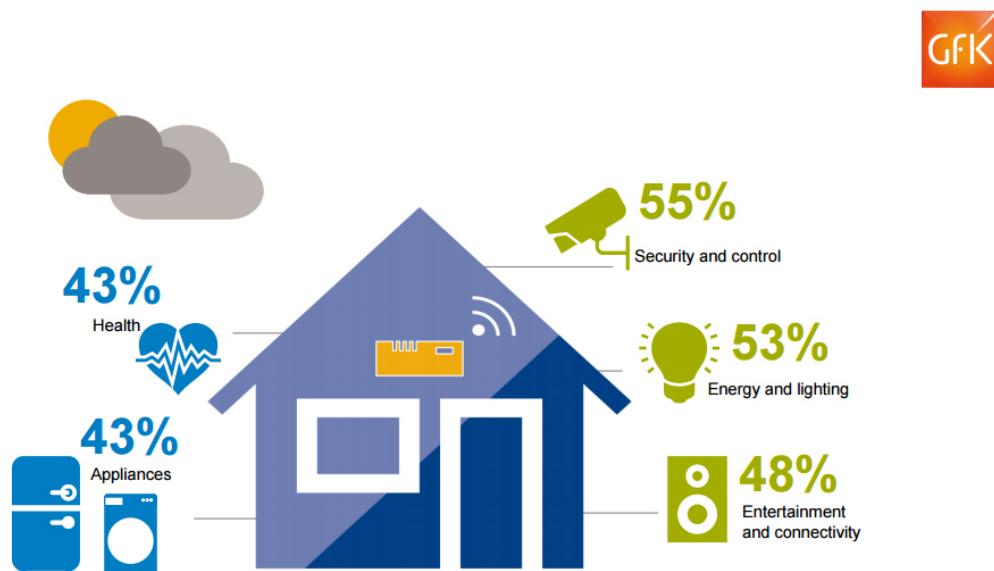
Rysunek 1.2. Opracowanie własne

ma wysyłać informacje, musi być wyposażony w sensor. Dzięki niemu jest w stanie zebrać potrzebne dane z otoczenia, aby móc je przekazać odbior- cy (rys 1.2). Jako nadajniki mogą posłużyć smartfony, czujniki wilgotności,

temperatury czy ruchu. Różnica między tymi czujnikami a smartfonami jest taka, iż ze smartfona dane są wysyłane dzięki akcji, którą wyzwała człowiek, a w przypadku czujników dzieje się to automatycznie. Przykładem mogą być modne ostatnimi czasami opaski mierzące tętno, czy liczące ilość wykonanych w ciągu dnia kroków. Kolejnym warunkiem, jaki musi być spełniony jest fakt, że przedmiot, który będzie odbierał sygnał przesłany przez nadawcę, musi być w stanie go odczytać, przetworzyć i wywołać odpowiednią relację. Przy odbiornikach takich jak komputer czy telefon, przesłana informacja wyświetli się na ekranie. Odbiornikami mogą być również urządzenia, które wykonają określoną czynność, a nie wyświetlą samej informacji. Przykładem może być układ nawadniania, który automatycznie włączy dopływ wody, bądź kontroler oświetlenia, który o zmierzchu włączy światło, czy też rolety, które zasłonią się lub odsłonią o odpowiedniej porze. Bardziej abstrakcyjnymi przykładami mogą być książki, które wyświetżą planowaną datę zwrotu do biblioteki. Trzecią rzeczą potrzebną do stworzenia takiej relacji jest sposób komunikacji, czyli to w jaki sposób dane zostaną przesłane od nadawcy do odbiorcy. Najbardziej popularnymi w dzisiejszych czasach środkami wymiany danych są WiFi, Bluetooth, oraz mniej znane NFC czy Z-WAVE, które wykorzystywane są w systemach budynków. Relację opisanych wyżej trzech rzeczy obrazuje rysunek 1.2.

1.3. Korzyści wynikające z wykorzystania Internetu Rzeczy

Tak szybki rozwój technologii i łączności otwiera drogę na coraz bardziej nowatorskie i zaawansowane rozwiązania ułatwiające ludziom życie. Największy potencjał w tej dziedzinie ma inteligentny dom. Dom jest miejscem, w którym czujemy się bezpiecznie i zawsze możemy do niego wrócić. Nic więc dziwnego, że stale chcemy ułatwiać sobie życie dostosowując otaczającą nas elektronikę do naszych potrzeb. O ile do niedawna możliwość posiadania inteligentnego domu zarezerwowana była tylko dla osób, które byłyby w stanie sobie taki dom skonstruować to teraz jest coraz więcej firm



Rysunek 1.3. Raport GfK na temat Internetu Rzeczy

które zrobią to za nas. Koncepcja tzw. *smart home* jest najszybciej rozwijającą się ideą w dziedzinie Internetu Rzeczy. Niemiecki koncern zajmujący się badaniem opinii publicznej GfK przeprowadził w 2015 roku analizę rynku inteligentnych domów. Gwałtowny rozwój technologii, coraz więcej przedsiębiorstw interesujących się tematem oraz prognozy firmy GSMA, która w 2011 roku oszacowała rynek inteligentnych domów na 40 miliardów dolarów [8], przyczyniły się do powstania raportu GfK. Badaniu poddanych zostało ponad 7.000 respondentów z 7 krajów – USA, Wielkiej Brytanii, Niemiec, Japonii, Chin, Brazylii oraz Korei Południowej. Według przeprowadzonego badania aż 91% respondentów było świadomych co oznacza idea inteligentnego domu, a 68% badanych posiadało ogólną wiedzę na ten temat. To bardzo dobry wynik jak na koncepcje, o której do niedawna w ogóle się nie mówiło. Raport ukazuje również, że 55% badanych uważa bezpieczeństwo za jeden z ważniejszych aspektów. Mowa oczywiście o monitoringu, alarmach i systemach zapobiegawczych. Jednak rozwiąz-

zanie to ma swoje wady, które zostaną dokładnie opisane w następnym rozdziale. [9] Głównym kierunkiem rozwoju jest spotęgowanie relacji pomiędzy człowiekiem, a przedmiotem, a to wywołuje potrzebę analizy coraz większej ilości danych. Jest wiele korzyści wynikających z korzystania z rozwiązań *IoT*. Zalicza się do nich lepsza kondycja fizyczna oraz zdrowie własne i bliskich. Ważną rzeczą jest też większe poczucie kontroli nad urządzeniami. Inną korzyścią jest podwyższenie produktywności i bezpieczeństwa kadry pracowniczej oraz poprawa relacji z klientem, dzięki zwiększonej komunikacji.

ROZDZIAŁ 2

Kierunki rozwoju Internetu Rzeczy

2.1. Warunki rozwoju IoT

Są trzy poziomy dojrzałości [3], dzięki którym możemy zauważać bezpośrednie korzyści biznesowe.

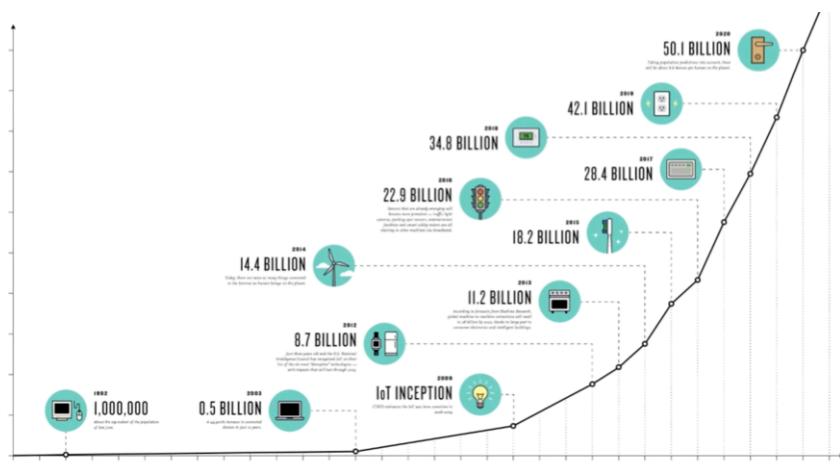
- Pierwszy poziom „Data to Discovery”, mówi o bazie nowych danych i ich wykorzystaniu, w celu zdobycia informacji o rzeczach, o których nie wiedziano dotychczas. Przykładem może być odnalezienie nowych wzorców choroby dzięki informacji z maszyn medycznych.
- Drugim poziomem dojrzałości jest „Data to Decisions”, w którym mowa o tym, że na bazie odpowiednich danych można podjąć autonomiczne akcje, na przykład awaryjne wyłączenie urządzenia w momencie awarii.
- Ostatnim poziomem jest „Data To Dollars-Dividends”, gdzie widać korzyść finansową dla firmy bądź szanse jej rozwoju, gdy połączy się dwa wcześniejsze poziomy ze sobą oraz wprowadzi usługi i produkty innowacyjne.

Media społecznościowe wpłynęły znacząco na to jak zaczęto organizować swoje życie, oraz zmieniły one modele biznesowe. Tak samo Internet rzeczy znalazł już swoje miejsce. Można powiedzieć, że jest on etapem rewolucji informacyjnej. Dostarczamy techniki i narzędzia, dzięki którym możemy budować wiedzę. Na dużych i szybkich strumieniach danych, nowoczesne urządzenia są w stanie podejmować odpowiednie decyzje. Sukcesu można się spodziewać, jeżeli wprowadzi się innowacyjne zastosowania w nowej przestrzeni. Na rozwój IoT miało wpływ wiele rzeczy. Jedną z nich

i najważniejszą jest miniaturyzacja. Dzięki niej możemy wszędzie umieścić mikroelementy (czujniki, komputery). Ważną rolę odegrała też technologia mobilna, która ciągle się rozwija. Ostatnią znaczącą rolą, bez której IoT by nie istniało jest bezprzewodowa sieć internetowa. Niestety istnieje kilka barier rozwojowych dla tematu IoT. Pierwsza to problem zasilania. Każde urządzenie, nawet to, w którym jest bardzo mocna bateria, wymagać będzie w końcu podłączenia do źródła zasilania. Kolejną barierą jest ilość tylko 4 mld urządzeń, które mogą posiadać adres IPv4 (przy założeniu że wszystkie będą wykorzystane przez zdresacje IPv4). Aby rozwiązać ten problem należy używać adresacji w wersji IPv6, który w obecnej prognoście rozwoju Internetu powinien być wystarczający. Ostatnią barierą, która zostanie przytoczona jest bezpieczeństwo danych i prywatność. Przekonanie ludzi, że informacje są chronione jest bardzo trudne, ale możliwe. Przykładem tego zjawiska są banki. Jeżeli dane między urządzeniami będą tak samo zabezpieczone jak środki na internetowym rachunku bankowym to Internet of Things stanie się rzeczywisty [10].

2.2. Idea rozwoju Internetu Rzeczy

Dla przeciętnego człowieka internet to połączone w sieć komputery, które wymieniają się danymi. Internet jest dla niego miejscem czerpania wiedzy i rozrywki, komunikowania się ze znajomymi i wrażenia swoich opinii. Jest to dla niego otwarty, częściowo anonimowy wirtualny świat, zupełnie inny od tego w którym żyje na co dzień. Początki internetu były bardzo skromne ale teraz jest to ogromna sieć łącząca ze sobą już nie tylko komputery, ale też telefony czy nawet urządzenia gospodarstwa domowego. Internet rozrasta się w tempie wykładniczym – jego rozwój niesie za sobą ogromne korzyści, ale również poważne zagrożenia. Największym motorem napędowym ekspansji Internetu Rzeczy jest chęć ludzi do ułatwiania sobie życia. Najlepszym tego przykładem jest koncepcja tzw. „Inteligentnego Domu”. Już w tym momencie możemy ustawić pralkę, aby rozpoczęła swoją pracę z opóźnieniem dzięki czemu możemy wrócić do domu akurat gdy pranie się



Rysunek 2.1. Interet Rzeczy: Rozwój możliwości (IoT: An explosion of connected possibility) [11]

skończy. Możemy zainstalować przełączniki światła sterowane dźwiękiem, dzięki czemu możemy zgasić lub zapalić światło nie wstając z łóżka. Mamy czasowe przełączniki, które symulują obecność domowników podczas ich nieobecności, żelazka, które same się wyłączają po pewnym okresie nieaktywności i tak dalej. Przykładów jest dużo więcej, a codziennie dochodzą nowe urządzenia, które w mniejszym lub większym stopniu ułatwiają nam życie w domu. Jeśli połączymy te wszystkie urządzenia w jedną sieć zarządzaną centralnie możemy mówić o inteligentnym domu. Jest on inteligentny na swój sposób – jest zaprogramowany aby zachowywać się w określony sposób lecz nie jest do końca autonomiczny. Co raz bardziej rozpoczęjący się postęp technologiczny w połączeniu z nieograniczoną ludzką wyobraźnią tworzy mieszankę wybuchową co wcale nie oznacza najgorszego. Wszak dynamit jest teraz kojarzony z bandytami napadającymi na banki, został wynaleziony w celu ułatwienia wydobywania naturalnych zasobów Ziemi [12]. Internet Rzeczy rozwija się w wielu kierunkach, nawet w dziedzinach które w ogóle nie kojarzą się z elektroniką. Doskonałym przykładem są tzw. *wearables*, czyli przedmioty osobiste które użytkownik nosi na sobie. Są to na przykład *smart watch'e*, które mają wbudowane

moduły łączności bezprzewodowej. Takie urządzenia mogą mieć dodatkowo wbudowane moduły GPS, co w teorii może znacząco ułatwić wezwanie pomocy w odpowiednie miejsce. Jednak taki zegarek może też przysporzyć wielu kłopotów – gdy osoba trzecia uzyska dostęp do danych lokalizacyjnych może z łatwością śledzić użytkownika i wykorzystać tę wiedzę do złych celów. Jeśli włamywacz ma absolutną pewność, że dana osoba znajduje się setki kilometrów od domu to bez większego ryzyka nakrycia może ten dom okraść. Na szczęście rynek *wearables* jeszcze raczuje, a najczęściej urządzeń mogących tworzyć Internet of Things powstaje w dziale RTV/AGD. Urządzenia domowe już dawno przyćmiły swoich protoplastów swoją mocą obliczeniową i możliwościami. Współczesne telewizory nie tylko są w stanie wyświetlać obraz nadawany z zewnętrznego urządzenia, ale same potrafią rozkodować sygnał z anteny. Mają własne systemy operacyjne, które implementują możliwości będące do niedawna ekskluzywną domeną komputerów osobistych. Posiadają przeglądarki internetowe, komunikatory a nawet gry. Niektóre mają wbudowane kamerki internetowe, a większość z nich obsługuje peryferyjne urządzenia rejestrujące. Tutaj znowu pojawia się problem, ponieważ owszem te urządzenia wykorzystywane są do prowadzenia video-rozmów ale gdy dostęp do nich uzyska niepowołana osoba stwarza to realne zagrożenie dla domowników, nie mówiąc już o utracie jakiejkolwiek prywatności. Udział sprzętu RTV/AGD w ekosystemie IoT przekracza 30% [13]. Nic w tym dziwnego, skoro cała idea Internetu Rzeczy zrodziła się właśnie w urządzeniach tego typu. Są to na razie tradycyjne sprzęty użytku domowego, czyli np. skanery, telewizory, urządzenia audio. Nowości na rynku sprzętu elektronicznego, takie jak smart lodówki, stanowią znakomity ułamek całego udziału sprzętu RTV/AGD w urządzeniach uważanych jako mogące być częścią IoT.

2.3. Zagrożenia płynące z rozwoju IoT

Urządzenia, z których korzystamy na co dzień są co raz bardziej złożone. Ma to na celu oczywiście ułatwienie życia i umożliwienie dokonywania

rzeczy które wcześniej istniały tylko w sferze fantastyki. Najbardziej niebezpieczne wydają się wspomniane wcześniej *wearables*. z definicji nosimy je zawsze przy sobie i to one stanowią największe niebezpieczeństwo dla użytkownika oraz są najbardziej podatne na utratę prywatności. Przykładem nasuwającym się od razu na myśl jest *Google Glass*. Dodatkowo zaciera się granica między rodzajami Rzeczy Internetu – *Google Glass* może być używane do kontrolowania domu, i osoby trzecie, które uzyskają dostęp do urządzenia, będą w stanie kontrolować cały dom i potencjalnie szpiegować domowników. To urządzenie może wkrótce zrewolucjonizować rynek urządzeń mobilnych. Jednak niesie to za sobą poważne zagrożenia. *Google Glass* do komunikacji z siecią może używać albo połączenia *Bluetooth* albo *Wi-Fi*. w przypadku tego pierwszego potrzebne jest dodatkowe urządzenie służące jako punkt dostępowy dla okularów od internetowego giganta. Druga opcja jest bardziej przystępna, gdyż nie wymaga od użytkownika posiadania przy sobie innego urządzenia mobilnego z dostępem do sieci. Jednak jak zauważa Roberto Martinez, badacz z Kaspersky Lab, który przyjrzał się sprawie bezpieczeństwa *Google Glass*, komunikacja *Wi-Fi* naraża urządzenie na ataki hakerów. Martinez i Juan Andres Guerrero – kolega z zespołu badawczego – przeprowadzili eksperyment w monitorowanej sieci. Odkryli, że tylko część danych wymienianych między urządzeniem a punktem dostępowym była szyfrowana. Badaczom udało się ustalić, że „ofiara” szukała połączeń lotniczych oraz miejscowości turystycznych. Potencjalny haker prawdopodobnie mógłby wyciągnąć jeszcze więcej informacji, gdyby tylko poświęcił na to więcej czasu [14]. “We admit that it is not a very damaging vulnerability, but even so, profiling via meta data from Web traffic exchange could become the first step of a more complex attack against the device’s owner.” - Roberto Martinez Kolejnym całkiem nowym na rynku urządzeniem które potencjalnie może przysporzyć właścielowi kłopotów jest *Galaxy Gear 2* od Samsunga. Jest to tzw. *smartwatch* – zegarek, który potrafi dużo więcej niż tylko wskazać godzinę. Eksperci z Kaspersky Lab również przyjrzaли się temu akcesorium i zarówno jak i w przypadku *Google Glass* jak i tutaj znaleźli potencjalne zagrożenia dla użytkownika. Pierwszą rzeczą, na jaką zwróciли uwagę ba-

dacze był aparat. Samsung dobrze zdawał sobie sprawę, że umieszczenie miniaturowego aparatu w bardzo małym, niepozornym urządzeniu może narobić komuś szkody. Dlatego zegarek wydaje głośny dźwięk za każdym razem gdy robione jest zdjęcie i nie umożliwia wyłączenia tej opcji w żaden sposób. Ma to na celu ostrzeżenie ludzi dookoła, że potencjalnie zostało zrobione im zdjęcie. Jednak pracownicy Kaspersky Lab znaleźli obejście tego zabezpieczenia. Wystarczy tylko uzyskać dostęp administratora (tzw. *root*) co jest trywialnie proste mając fizyczny dostęp do urządzenia i użyć ogólnodostępnego narzędzia *ODIN* od Samsunga. Wyłączając dźwięk migawki nie tylko umożliwiamy właścicielowi zegarka robienie tajnych zdjęć innym osobom, ale też umożliwiamy hakerowi robienie zdjęć właścicielowi, tego co robi i gdzie jest – bez jego wiedzy. Innym problemem *Galaxy Gear 2* jest sposób, w jaki instalowane są aplikacje. Używane jest do tego oficjalne oprogramowanie od Samsunga – *Gear Manager* – jednak sposób w jaki aplikacja wgrywa inne programy do akcesorium pozostawia duży potencjał hakerski. Na zegarku nie wyświetla się żadna informacja o instalowanym oprogramowaniu, co umożliwia instalowanie złośliwych aplikacji bez wiedzy posiadacza. W połączeniu z wiedzą jak ukrywać zainstalowane już aplikacje na systemie Android, na którym *Galaxy Gear 2* operuje, daje to nieograniczone możliwości dla hakerów. Na szczęście są to urządzenia dosyć młode na rynku sprzętu elektronicznego i zagrożenia związane z włamywaniem się na nie nie są aż tak powszechnne. Jak zaznacza Juan Andres Guerrero na chwilę obecną nie ma żadnych dowodów sugerujących, że wearables są celem hakerów jednak to może się zmienić w przyszłości, gdy staną się bardziej powszechnne. “At this time there is no evidence to suggest that wearables are currently being targeted by professional APT actors. However there is a twofold appeal presented by wearables that make them a likely future target if they are widely adopted by consumers. In future the data collected by wearable devices is going to attract new players to the cyber-espionage scene.” - Juan Andres Guerrero Aby „poczuć ducha” inteligentnego domu wcale nie trzeba wydawać dużych pieniędzy – każdy z minimalną wiedzą informatyczną jest w stanie samego stworzyć sobie taki dom, na większą lub mniejszą skalę. Wystarczy

komputer i dobry pomysł, aby przekształcić swoje cztery kąty w coś wyjątkowego. Urządzenia, z których korzystamy na co dzień są coraz bardziej złożone. Ma to na celu oczywiście ułatwienie życia i umożliwienie dokonywania rzeczy, które wcześniej istniały tylko w sferze fantastyki. Najbardziej niebezpieczne wydają się wspomniane wcześniej wearables. Z definicji nosimy je zawsze przy sobie i to one stanowią największe bezpieczeństwo dla użytkownika oraz stanowią największe zagrożenie utraty prywatności. Przykładem nasuwającym się od razu na myśl jest *Google Glass*. Dodatkowo zaciera się granica między rodzajami Rzeczy Internetu – okulary mogą być używane do kontrolowania domu, i osoby trzecie, które uzyskają dostęp do urządzenia, będą w stanie kontrolować cały dom i potencjalnie szpiegować domowników. [15] Niebezpieczeństwa niesione przez IoT można rozpatrywać na dwa sposoby: bezpieczeństwa związane z informatyzacją świata konsumenckiego oraz optymalizacją sektora przemysłowego [16]. W czasach rozpoczęjącego się rozwoju Internetu Rzeczy, ludzie skazani są na informatyzację większości dziedzin życia. Inteligentny sprzęt gospodarstwa domowego, elektroniczne zamki do drzwi lub okien, liczniki energii, itd. Wszystkie te sprzęty niosą za sobą spore bezpieczeństwo, a ich przeciętni użytkownicy nie zdają sobie sprawy z powagi zagrożenia. Bo przecież dlaczego ktoś miałby się bać swojej lodówki? Otóż wszystko wskazuje na to, że niedługo lodówki będą w stanie gromadzić informacje na temat ich zawartości. Wiedza ta w niepowołanych rękach może zaszkodzić użytkownikowi. Na pewno nie w bezpośredni sposób, bo dieta ofiary nie może być wykorzystana np. do kradzieży pieniędzy z konta bankowego. Umożliwi tzw. profilowanie ofiary. Tak niepozorna wiedza jak to co je na śniadanie, w połączeniu z innymi, teoretycznie bezpiecznymi informacjami jak np. godzina o której ofiara rano wstaje (wykradziona ze smartwatch'a) oraz np. ile ciepłej wody zużywa ofiara (wiedza wykradziona z elektronicznych liczników wody). Tak nagromadzona wiedza, pozornie nieprzydatna z punktu widzenia hakera, pozwala na dokładną inwigilację ofiary, poznanie jej nawyków oraz sposobu w jaki żyje stylu życia. Taka wiedza może narobić ofierze wielu problemów gdy znajdzie się w niepowołanych rękach.

ROZDZIAŁ 3

Doświadczenia praktyczne

3.1. Wykorzystanie Arduino przy budowaniu własnych projektów

Przygodę z Internetem rzeczy możemy zacząć od kupienia gotowych rozwiązań. Daje nam to możliwość stworzenia inteligentnego domu całkowicie samodzielnie. Zakup przykładowego zestawu inteligentnych żarówek pozwala nam na sterowania oświetleniem w całym mieszkaniu za pomocą aplikacji na telefon. Jeżeli zaopatrzymy się w odpowiedni model żarówki, możemy również zmieniać kolor oświetlenia oraz jego intensywność. Zaopatrywanie się w gotowe przedmioty ma też swoje wady. Jesteśmy ograniczeni przez producenta funkcjonalnością. Programy obsługujące inteligentne rzeczy są pisane pod konkretny ekosystem (Android, iOS, Windows Phone) aplikacja może nie działać na naszym urządzeniu. Narażeni jesteśmy wtedy na dodatkowe koszty - zakup sprzętu, lub musimy szukać innego, często gorszego rozwiązania. Jako osoba studiująca na kierunku Informatyki postanowiłem stworzyć inteligentny przedmiot, który będzie działał tak jak go zaprogramuje. Na przeciw moim oczekiwaniom wyszedł Projekt Arduino. Powstał on w 2005 roku we Włoszech. Jest to platforma dla systemów wbudowanych, oparta o 8-bitowe mikrokontrolery Atmel AVR. Płytki posiada ustandaryzowany układ wyjścia-wejścia (ang. input-output circuit, I/O circuit) umożliwia nam to korzystanie z urządzeń zewnętrznych takich jak: czujniki, sterowników, silniki, wyświetlacze itp. Istnieje kilka wersji płyt Arduino jednak większość z nich nie wymaga żadnego zewnętrznego programatora. Do wgrania oprogramowania wystarczy podłączyć mikrokontroler do komputera. Arduino posiada własne darmowe środowisko - Arduino IDE. Ogromną zaletą platformy jest jej popularność. Dzięki niej

w sieci istnieje duża ilość bibliotek do obsługi różnych urządzeń zewnętrznych. Jest także sporo poradników i przykładów zastosowania mikrokontrolera AVR. Jest to idealne środowisko dla programistów, którzy są pasjonatami elektroniki ale nie lubią konfiguracji programatorów, sprawdzania układów i instalacji sterowników. Do napisania pierwszego programu i uruchomieniu go na Arduino wystarczy nam komputer, przewód miniUSB-USB oraz sama płytka. Na początku przygody z płytą Arduino zazwyczaj nie mamy zbyt wiele sprzętu którego moglibyśmy wykorzystać do stworzenia czegoś użytecznego. Dlatego pierwszym programem dzięki którym poznajemy się z samym językiem programowania oraz samym mikrokontrolerem jest miganie wbudowaną diodą. Inteligentny Dom w praktyce – Stacja Meteorologiczna Jednym z najprostszych a dającym największej satysfakcji projektów jest stacja meteorologiczna zbudowana przy pomocy Arduino oraz kilku czujników. Poziom zaawansowania układu zależy tutaj od budującego taką stację. Możemy po prostu mierzyć temperaturę oraz wilgotność powietrza za pomocą cyfrowego czujnika DHT11 lub DHT22. Różnice między czujnikami znajdują się poniżej. Jednak taka prosta stacja to nic innego jak domowy termometr. W inteligentnym domu chodzi o coś więcej. Wspomniany projekt możemy rozbudować o kilka dodatkowych sensorów i stworzyć coś na prawdę fajnego. Dorzucając takie funkcjonalności jak: wykrywanie burzy, pomiar ciśnienia, sprawdzanie prędkości oraz kierunku wiatru. Jednocześnie wysyłając wszystkie dane do sieci tak, żeby mieć wgląd w historię pogody. Możemy wykorzystać naszą stację jako centrum informacji dla osób zainteresowanych sportami w których wiatr odgrywa kluczową rolę np. windsurfing, kitesurfing. Inteligentny Dom w praktyce - Sterowanie oświetleniem Za pomocą Arduino jesteśmy w stanie sterować oświetleniem w całym mieszkaniu. Wystarczy, że odpowiednio podłączymy moduły z przekaźnikiem do sterownika. Możliwości tego rozwiązania są dużo większe niż wspomniane na początku rozdziału gotowe urządzenia. Tutaj cała konfiguracja i pole manewru leży w naszych rękach. Możemy odwzorować sklepową wersję intelligentnej żarówki i ograniczyć się do centralnego sterowania oświetleniem w domu z poziomu aplikacji na komórce. Fajnym pomysłem na urozmaicenie takiego projektu jest zaprogra-

mowanie różnych scen. Jednym kliknięciem możemy ustawić oświetlenie tak by sprzyjało czytaniu książki lub oglądaniu filmów. Kolejnym ciekawym rozwiązaniem jest podpięcie całego systemu oświetlenia do sieci i umożliwienie sterowania przez stronę www. Możemy w ten sposób na przykład sprawdzić czy na pewno zgasiliśmy światło w domu, będąc jednocześnie w zupełnie innym miejscu. Oczywiście trzeba uwzględnić zabezpieczenie takiego projektu tak, żeby osoby niepożądane nie mogły przejąć kontroli nad naszym systemem. Zdalne sterowanie oświetleniem daje nam możliwość symulowania obecności w domu gdy jesteśmy np. na wczasach. Możemy zdalnie włączać i wyłączać światło, ale nic nie stoi na przeszkodzie by ten proces zautomatyzować i ustawić godziny w których nasz dom będzie zapalał i gasił oświetlenie. W ubiegłym roku powstała strona na której można było sterować oświetleniem świątecznym rozwieszonym na domu. Był jednocześnie podgląd online dzięki któremu na żywo mogliśmy obserwować wszystkie czynności które wykonywaliśmy.

3.2. Projekt inteligentnego nawadniania roślin

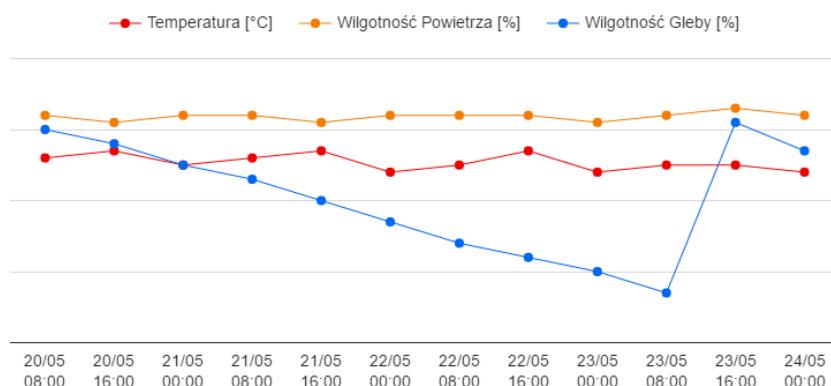
Pamięć o podlewaniu kwiatów domowych nigdy nie była naszą mocną stroną. Postanowiliśmy więc stworzyć system, który będzie nas informował drogą mailową o potrzebie nawodnienia rośliny. Chcieliśmy również zbierać informacje o temperaturze, wilgotności powietrza i poziomie wilgotności gleby. Wszystkie dane wysypane są na serwer i dzięki stronie internetowej będziemy mogli w przyszłości analizować wyniki które ułatwią nam ponowne wyhodowanie rośliny. Pierwszym krokiem jaki wykonaliśmy to skompletowanie listy rzeczy które były niezbędne do wykonania tego systemu. Należą do nich:

- Płytką Arduino UNO: 2,7\$
- Sensor wilgotności gleby: 0,86\$
- Sensor temperatury i wilgotności powietrza: 3,01\$

- Moduł Wifi: 2,70\$
- Zestaw kabli i rezystorów: 2,00\$
- Płytką stykową dedykowana do Arduino: 1,31\$

Koszt takiego zestawu na rynku polskim wynosiłby około 130 PLN. Jednak w celu zminimalizowania kosztów, zakupu dokonaliśmy w serwisie AliExpress. Zredukowało to koszt projektu do kwoty około 54 PLN (14\$ przy kursie dolara wynoszącym 3,84 PLN). Przed przystąpieniem do składania projektu musieliśmy zainstalować IDE (ang. Integrated Development Environment) czyli zintegrowane środowisko do pisania programów, dzięki któremu będziemy mogli wgrywać programy na naszą płytę. Następnie sprawdziliśmy czy wszystkie sensory działają poprawnie. Zaczęliśmy od podstawowego czujnika DHT11. Jest to układ odpowiadający za pomiar temperatury i wilgotności powietrza. W celu sprawdzenia napisaliśmy prosty program wykorzystujący bibliotekę "DHT.h". Po podłączeniu zgodnie z opisem sensora nie byliśmy w stanie odczytać poprawnych wartości. Po głębszej analizie okazało się, że czujnik który dostaliśmy ma inaczej poprowadzone PINy (info). Kolejną rzeczą która musieliśmy sprawdzić to podłączenie sensora wilgotności gleby do naszej płytki. Po wstępnej analizie danych z czujnika, porównując wyniki z innymi użytkownikami tego samego czujnika uznaliśmy, że zachowuje się on prawidłowo. Ostatnim krokiem przygotowawczym było sprawdzenie modułu WiFi. Pozornie najtrudniejszy moduł nie sprawił nam najmniejszych problemów. Wszystko działało poprawnie i mogliśmy zabrać się za tworzenie inteligentnego systemu nawadniania roślin. Po sprawdzeniu każdego czujnika z osobna mogliśmy przystąpić do pracy. Musieliśmy tylko napisać program który będzie obsługiwał wszystkie moduły naraz. W pierwszej kolejności podłączylismy czujniki odpowiadające za pomiar temperatury, wilgotności gleby i powietrza. Następnie zajęliśmy się konfigurowaniem połączenia sieciowego. Nasz program sprawdzał wszystkie pomiary trzy razy w trakcie doby – w nocy o godzinie 00:00, o 8:00 nad ranem oraz po południu o godzinie

16:00. Dane za każdym razem wysyłane były na serwer. Na rysunku [x] przedstawiony został wykres przedstawiający dane z trzech dni.



Rysunek 3.1. Dane z czujników przedstawione na wykresie, źródło:
Opracowanie własne

Ostatnim krokiem było dodanie powiadomień na maila. Skorzystaliśmy z gotowego rozwiązania PushingBox (źródło). Jest to dedykowane rozwiązanie dla urządzeń z dziedziny Internet of Things. Posiada zaimplementowane już rozwiązania między innymi na Arduino. Wystarczy wykorzystać kod udostępniony przez twórców na stronie i wdrożyć go w swoim rozwiązaniu. System informował nas drogą mailową gdy wilgotność gleby spadała poniżej 10

3.3. Budowa własnego systemu monitoringu

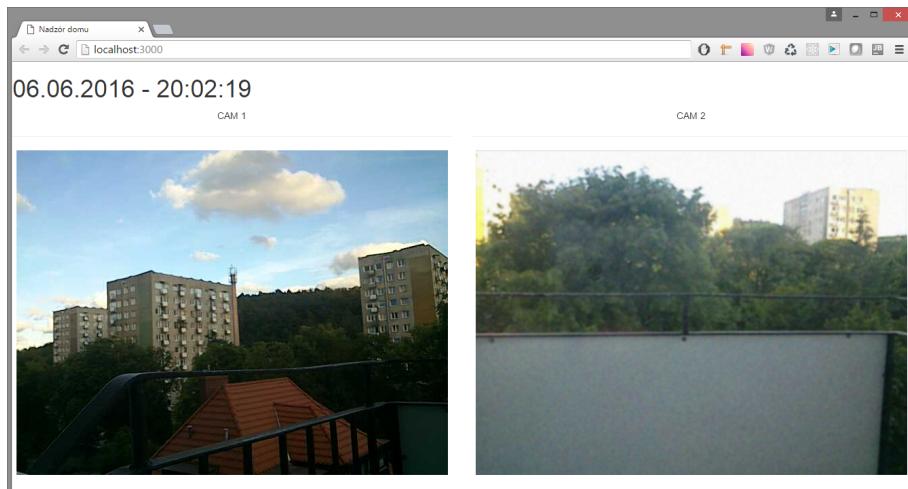
Wygodny nadzór nad domem podczas nieobecności do niedawna kojarzył się z czymś ekskluzywnym. Powszechnie monitoring znajdował się jedynie w bogatych domach. Jednak z tak szybkim postępem technologicznym na tego typu luksusy może pozwolić sobie niemalże każdy, praktycznie zero wym kosztem. Większość ludzi posiada jakiś stary, nieużywany telefon komórkowy z aparatem. Można go wykorzystać jako kamerę IP, dostępną

w sieci lokalnej domu. Specjalne oprogramowanie będzie przesyłać obraz z dobrze umiejscowionego telefonu do serwera. To może być dowolne urządzenie, jednak na potrzeby naszego eksperymentu będzie nazywany serwerem. w naszym przypadku użyliśmy 2 aparatów i laptopa [17]. Za strumienianie wideo z kamery odpowiedzialny jest program IP Webcam1. Aplikacja jest dostępna za darmo, z możliwością wykupienia wersji pro. w cenie ok. 12 zł znajdują się dodatkowe funkcje:

- Integracja z Taskerem,
- Konfigurowalny UI,
- Bezpośredni skrót na ekranie głównym do uruchomienia aplikacji,
- Brak znaku wodnego,
- Brak reklam,

To niewielki koszt w porównaniu z tym, co aplikacja ma do zaoferowania. Autor programu, Pavel Khlebovich, do wersji pro podchodzi bardziej jak do dobrowolnej dotacji. IP Webcam posiada ogrom funkcji. Oprócz najważniejszej, czyli wystawiania zwykłego interfejsu kamery IP, sama w sobie posiada funkcję serwera, i to bardzo przemyślanego. Na wstępie zaskakuje ilość sposobów w jaki można odbierać obraz i/lub dźwięk z urządzenia. Można też zapisywać pliki w archiwum, albo skonfigurować Taskera. Wszystko jest zrobione w Bootstrap'ie i działa bardzo dobrze na prawie każdym urządzeniu, dzięki możliwości wyboru sposobu transmisji. Ma to niestety podstawowy problem. Ciężko mówić o monitoringu, mając obraz z jednej kamery. Wiele kamer oznacza wiele serwerów, każdy nadający obraz tylko ze swojego aparatu. Aby będąc na urlpie podejrzeć obraz z domu, należałoby zalogować się na każdą kamerę z osobna, co w przypadku większej ilości kamer byłoby zupełnie niepraktyczne. Zaprogramowaliśmy serwer w technologii Meteor, który odbiera sygnał z wielu kamer, inaczej, zapisuje migawki do pliku i serwuje je klientowi [18]. Aby to wszystko było możliwe najpierw zainstalowano Meteora. Po początkowych nieudanych próbach uruchomienia frameworka na wirtualnej maszynie VirtualBox +

Vagrant spowodowanych brakiem sympatii sterownika MongoDB do monitorowanych folderów, postawiliśmy serwer na Windowsie 8.1. Główną wadą tego rozwiązania był brak programu npm, co stanowiło spory problem, gdyż najlepszy naszym zdaniem sterownik do kamer IP jest modułem Node.js. Jednak wszystko jest możliwe z odrobiną hacks'ów. z pomocą przyszedł moduł meteorhacks/npm, który wbrew nazwie w odpowiedni sposób dodaje obsługę npm do Meteora, co zresztą potwierdzają doświadczeni programiści [19]. Potrzebna była jeszcze tylko aplikacja do obsługi naszego usta-



Rysunek 3.2. Działający system monitoringu.

wienia. z założenia aplikacja miała obsługiwać wiele kamer, i to w dodatku wyświetlać obraz na dowolnym urządzeniu w dowolnym miejscu. Zatem nie było mowy o strumieniu na żywo, gdyż rozmiar przesyłanych danych byłby zbyt wielki. Postawiliśmy na prostotę: serwer co sekundę odpytuje wszystkie kamery o zrzut ekranu. Zapisuje je potem do odpowiednich plików i wysyła je do klienta, gdzie stanowią one zwykłe obrazki okraszone Bootstrapem dla obsługi urządzeń mobilnych. Obrazki zmieniające się co sekundę dają wrażenie oglądania nagrania na żywo, co technicznie jest prawdą. Wiele problemów sprawił też sam node-cam, który jest w wersji 0.0.1 i sam autor przestrzega przed tym, że projekt nie jest ukończony.

Jednak spodobało nam się proste API i dzięki wspólnemu wysiłkowi udało nam się skonfigurować ten moduł rys 3.2 .

Niskie tempo odświeżania rekompensuje fakt, iż możemy podłączyć wiele kamer i mieć odczyt na żywo z każdej z nich. w naszym przypadku całkowicie zerowym kosztem stworzyliśmy system nadzoru domu, do którego można się zalogować. Do zabezpieczenia aplikacji użyliśmy standardowej autoryzacji poprzez HTTP, której obsługę do Meteora dodaliśmy przy pomocy modułu Jabbslad/basic-auth.

3.4. Budowa inteligentnego oświetlenia

Budowa systemu oświetlenia, miała na celu znaczące obniżenie kosztów energii elektrycznej oraz prostotę i użyteczność które to wspierałyby nasze *wrodzone lenistwo*. We wszystkich pokojach w całym mieszkaniu wliczając łazienkę i korytarz. Jak mawiał klasyk, "*Do zrobienia rzeczy trudnej wybrałbym osobę leniwą, gdyż taka to właśnie osoba znajdzie najprostszy sposób aby to wykonać [20]*". w myśl owej zasady, postanowiliśmy kontrolować oświetleniem za pomocą specjalnych sterowników WiFi spręgniętych z aplikacją na smartfony/tablety oraz zdalnego kontrolera RGB, aby móc kontrolować oświetleniem w całym domu za naciśnięciem jednego *kciuka*. Źródłem światła w tym przypadku postanowiliśmy użyć wydajnych i energooszczędnich taśm LED'owych opartych o najnowsze diody 5760 oraz w przypadku pokoju dla młodzieży taśm z diodami 5050 RGB. w połączeniu z wyżej wymienionymi sterownikami WiFi będą duszą naszego projektu. Całość będzie sterowana zdalnie z dwu źródeł, sensorycznego kontrolera zdalnego rys 3.4, 3.5, 3.6 oraz/i aplikacji zainstalowanej na smartfonie rys . Niestety nie było się bez problemów "wieku niemowlęcego" projektu, gdyż inicjalnie mieliśmy bazować na sterownikach firmy "Milight" które niestety nie są pozbawione wad... Jednakże po dłuższych poszukiwaniach dobraliśmy sterowniki firmy "Fancy Lighting", które to spełniały założenia projektowe naszego rozwiązania. Tradycyjnie w celu obniżenia kosztów przedsięwzięcia wszystkie komponenty zostały zakupione u źródła najtańs-



Rysunek 3.3. Aplikacja MagicHome . Opracowanie własne.

szej produkcji światowej czyli w Chinach na portalu *Aliexpress.com*. W skład wszystkich potrzebnych do budowy zdalnego sterowania oświetleniem komponentów wchodzą:

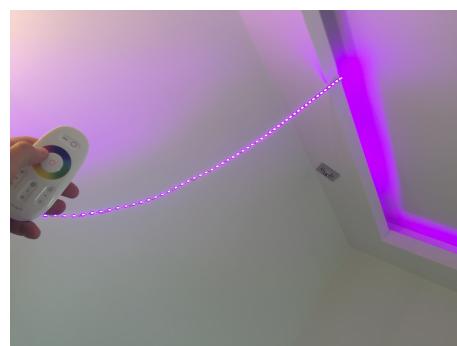
- Taśmy LED'owe *Warm yellow light* oraz *RGB* 8 taśm po 5m każda -> 30\$
- sterowniki WiFi szt. 5 -> 50\$
- zasilacze 220V->12V -> 20\$
- kontroler (pilot) oświetlenia RGB -> 8\$
- aplikacja *MagicHome* rys 3.3 -> 0\$ aplikacja jest darmowa!

Największymi możliwościami jednak dysponuje sterownik WiFi "Fancy Lighting" gdyż pozwala nam na kompletne sterowanie z aplikacji *MagicHome*, którą mamy dostępną pod większość systemów mobilnych (*iOS, Android, etc*). Jest to najbardziej wygodna funkcjonalność z jaką do tej pory się spotkaliśmy. Pozwala na pełną kontrolę oświetlenia w całym domu

jak i grupowania sterowników w obrębie jednego pomieszczenia (*np możemy oddziennie zapalić oświetlenie aneksu kuchennego oraz połączonego zeń pokoju*). Sam sterownik posiada również pare innych ciekawych funkcji zaimplementowanych inicjalnie (*out of the box*), pierwszą jest możliwość uruchomienia zaprogramowanej przez nas symulacji "pobytu" podczas naszej nieobecności. Jest to skrypt który możemy uruchomić podczas naszego wyjazdu i każdego wieczoru będzie o zmierzchu zapalał i gasił światła w zdefiniowanych wcześniej grupach "*duży pokój*", "*mały pokój*", "*kuchnia*", *etc.* co pozwoli na zmylenie potencjalnych włamywaczy obserwujących nasze mieszkanie.

System posiada również tzw. *party mode* czyli wbudowany system mikrofonów i podczas puszczenia muzyki możemy dla przykładu zamienić duży pokój w salę taneczną z piękną iluminacją świetlną która reaguje na puszczone dźwięki.

Jak widać na przedstawionym zestawieniu powyżej, zestaw nie jest rząco drogi oraz w wersji podstawowej funkcjonalności jakoś mocno skomplikowany do wdrożenia, jeśli natomiast będziemy chcieli zaimplementować więcej funkcjonalności to w tym momencie ogranicza nas tylko nasza wyobraźnia.



Rysunek 3.4. Oświetlenie RGB oparte o kontroler . Opracowanie własne.



Rysunek 3.5. Oświetlenie RGB oparte o kontroler . Opracowanie własne.



Rysunek 3.6. Oświetlenie RGB oparte o kontroler . Opracowanie własne.

Zakończenie

Stworzenie systemu monitoringu pozwoliło nam lepiej poznać Node.js oraz samego Meteora. Pomimo, że aplikacja jest bardzo prosta w założeniach poświęciliśmy mnóstwo czasu na szukanie informacji w internecie jak rozwiązywać kolejno napotykane problemy. Jednak takie udogodnienia niosą za sobą spore ryzyko. O ile my naszą aplikację zabezpieczyliśmy najprostszym i najskuteczniejszym sposobem, być może w przyszłości będziemy chcieli prowadzić logowanie wielu użytkowników co może otworzyć furtkę dla hakera. Jednak z drugiej strony warto korzystać z technologii aby ułatwić sobie życie w każdym możliwym aspekcie. Uważamy, że wybrane do tej części projektu technologie idealnie sprawdzają się do naszych zastosowań. Node.js jest bardzo szybki w porównaniu do starszych technologii i idealnie sprawdza się w naszym zastosowaniu. Zbudowanie od podstaw systemu inteligentnego nawadniania roślin pozwoliło nam poznać lepiej zasady działania sensorów w rozwiązaniach Internet of Things. Utwierdziliśmy się w przekonaniu, że rozwiązania inteligentnych przedmiotów wcale nie muszą być drogie. Nie są też trudne w budowie. W internecie jest dużo poradników i materiałów na temat różnych projektów, dzięki którym bez problemu możemy zbudować podobne systemy u siebie w domu. Wprowadzenie powiadomień mailowych znacznie ułatwiło nam wyhodowanie rośliny, ale po zagłębieniu się w temat internetu rzeczy zrozumieliśmy, że nie chodzi o to by przedmioty były tylko podłączone do sieci. Cała idea polega na tym by rzeczy zaczęły same wykonywać niektóre czynności. Dlatego w przyszłości zamierzamy dodać funkcjonalność która sprawi, że nasz projekt stanie się prawdziwym intelligentnym systemem. Mamy w planach dodanie silniczka - małej pompy wodnej która będzie automatycznie podlewać rośliny. Dzięki temu ograniczymy naszą aktywność, tylko do uzupełniania pojemnika z woda. Uważam, że wykorzystanie Arduino pozwoliło nam na zrozumieć jak działa większość rzeczy IoT. Dowiedzieliśmy się czym tak naprawdę są inteligentne rzeczy i w jakim kierunku rozwija się

ta dziedzina. Potrafimy spojrzeć na urządzenia z innej strony i łatwiej jest nam zrozumieć działania tych przedmiotów.

Bibliografia

- [1] Kevin Ashton. That 'internet of things' thing. 2009.
- [2] Michael Miller. *The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World.* QUE, QUE:800East 96th street Indianapolis, Indiana 46240 USA, first edition, 2015.
- [3] P. Kolenda K. Krejitz A. Legoń P. Rytel R. Wierzbiński M. Grodner, W. Kokot. Raport - internet rzeczy w polsce. 2015.
- [4] Benduch Dorota Badowski Mateusz. *Internet rzeczy. Bezpieczeństwo w Smart City.* C.H. BECK, pierwsze edition, 2016.
- [5] pragya singh p. lot & internet of things applications online – smart living but safety first! 2015.
- [6] STEFAN FERBER. Jak internet rzeczy wpływa na naszą rzeczywistość. 2015.
- [7] Piotr Prajsnar. Internet rzeczy? to nie to, co myślisz... 2015.
- [8] GSMA. Vision of smart home: The role of mobile in the home of the future. 2011.
- [9] GfK. Smart home: Making the smart home a reality. 2015.
- [10] Osmar Elloumi Olivier Hersent, David Boswarthick. *The Internet of Things: Key applications and protocols.* John Wiley & Sons Ltd, 2012.
- [11] Alan Crisp. Internet of things: prime time for satellite? 2015.
- [12] Francis daCosta. *Rethinking the Internet of Things: A Scalable Approach to Connecting Everything.* Apress Media, 2013.

- [13] P. Kolenda K. Krejtz A. Legoń P. Rytel R. Wierzbiński M. Grodner, W. Kokot. Internet rzeczy w polsce. 2015.
- [14] Nitesh Dhanjani. *Abusing the Internet of Things*. O'REILLY, 2015.
- [15] J. A. Guerrero R. Martinez. Wear the danger. 2014.
- [16] Komputer Świat. Internet rzeczy - czym jest i jakie niesie zagrożenia. 2016.
- [17] Peter Waher. *Learning Internet of Things*. Packt Publishing, 2015.
- [18] Cuno Pfister. *Getting Started with the Internet of Things*. O'REILLY, 2011.
- [19] Stefan Baumgartner. Using npm packages. 2014.
- [20] Bill Gates. Cytat bill'a gates'a. 2012.

Spis rysunków

1.1. Ilość urządzeń IoT , źródło: Gartner, listopad 2014r.	8
1.2. Opracowanie własne	9
1.3. Raport GfK na temat Internetu Rzeczy	11
2.1. Interet Rzeczy: Rozwój możliwości (IoT: An explosion of connected possibility) [11]	15
3.1. Dane z czujników przedstawione na wykresie, źródło: Opracowanie własne	24
3.2. Działający system monitoringu.	26
3.3. Aplikacja MagicHome . Opracowanie własne.	28
3.4. Oświetlenie RGB oparte o kontroler . Opracowanie własne.	29
3.5. Oświetlenie RGB oparte o kontroler . Opracowanie własne.	30
3.6. Oświetlenie RGB oparte o kontroler . Opracowanie własne.	30

Oświadczenie

Ja, ni?ej podpisany(a) o?wiadcza?am, i? przed?o?ona praca dyplomowa zo-
sta?a wykonana przeze mnie samodzielnie, nie narusza praw autorskich,
interesów prawnych i materialnych innych osób.

.....

data

podpis