Wstęp

Na początku 1926 r. Nikola Tesla wyobraził sobie „połączony świat". Powiedział Colliers Magazine w wywiadzie (Kennedy, 1926):

„Kiedy technologia bezprzewodowa zostanie doskonale zastosowana, cała Ziemia zamieni się w ogromny mózg, którym w rzeczywistości jest, wszystkie rzeczy będące cząstkami rzeczywistej i rytmicznej całości [...], a instrumenty, dzięki którym będziemy mogli to zrobić, będą zdumiewająco proste w porównaniu z naszym obecnym telefonem. Mężczyzna będzie mógł nosić jeden w kieszeni kamizelki.

Kevin Ashton jako pierwszy użył terminu Internet rzeczy (IoT) w 1999 r. w kontekście zarządzania łańcuchem dostaw z elementami oznaczonymi lub kodami kreskowymi (rzeczami) z identyfikacją radiową (RFID), oferującymi większą wydajność i odpowiedzialność za biznes. Jak napisał Ashton w dzienniku RFID (22 czerwca 2009):

„Gdybyśmy mieli komputery, które wiedziałyby wszystko o rzeczach - korzystając z danych, które zebrały bez naszej pomocy - bylibyśmy w stanie śledzić i liczyć wszystko, a także znacznie redukować straty, straty i koszty. Wiedzielibyśmy, kiedy rzeczy wymagają wymiany, naprawy lub przywołania i czy były świeże, czy przeszły.

W tym samym roku Gershenfeld opublikował swoją pracę „Kiedy rzeczy zaczynają myśleć", w której wyobrażał sobie ewolucję sieci WWW jako stan, w którym „rzeczy zaczynają korzystać z sieci, aby ludzie nie musieli tego robić. " Bankomaty można uznać za jeden z pierwszych inteligentnych obiektów, które pojawiły się w sieci już w 1974 roku. Ponadto wczesne przykłady różnych prototypowych urządzeń obejmują automaty sprzedające z lat 80. XX wieku wykonane przez Wydział Informatyki Uniwersytetu Carnegie Mellon. Od tego czasu zrozumienie możliwego zakresu IoT stało się znacznie bardziej wszechstronne, obejmując szeroki zakres domen aplikacji, w tym opiekę zdrowotną, usługi komunalne, transport itd., a także scenariusze aplikacji osobistych, domowych i mobilnych. Niedawno „Industrial Internet of Things" (IIoT) jeszcze bardziej rozszerzył zakres IoT. Dzięki IoT wyobrażamy sobie świat połączonych w sieć, „inteligentnych" lub „inteligentnych" obiektów. Ostatnio pojawiły się nowe rozszerzenia IoT, które obejmują nie tylko obiekty fizyczne, ale także obiekty wirtualne (co może zamazać podstawową koncepcję IoT, która koncentruje się głównie na rzeczach i obiektach fizycznych). Wspólnym mianownikiem tych różnorodnych koncepcji IoT jest to, że „rzeczy" mają stać się aktywnymi elementami w biznesie, informacjach i procesach społecznych. Biorąc pod uwagę szerokie spektrum scenariuszy zastosowań, bardziej adekwatny byłby bardziej ogólny termin „sieć" niż „internet", ponieważ nie cała komunikacja odbywa się przez Internet. Komunikacja również zachodzi nie tylko między rzeczami/urządzeniami, ale także między rzeczami a ludźmi. Dlatego bardziej odpowiednie byłoby użycie terminów „Internet wszystkiego" lub „Sieć wszystkiego" zamiast „Internet rzeczy". Jako najbardziej znany wizjoner skomputeryzowanego i połączonego świata fizycznego, Mark Weiser twierdzi, że połączony świat rzeczy ma pomagać ludziom w ich działaniach w dyskretny sposób. Interakcja zachodzi z artefaktami codziennymi - ale wzmocnionymi obliczeniowo poprzez naturalne interakcje, nasze zmysły i słowo mówione. W trakcie miniaturyzacji coraz mniejsze komponenty techniczne będą osadzane w komponentach fizycznych, z jak najmniejszą ingerencją dla użytkowników lub bez zwracania na siebie uwagi. Na przykład zminiaturyzowane komputery (lub ich elementy) oraz urządzenia do noszenia z czujnikami są bezpośrednio wbudowane w elementy odzieży. W swoim eseju z 1991 r. „Komputer na miarę XXI wieku" Mark Weiser po raz pierwszy wyraził tę wizję, gdy był głównym technologem w Xerox Palo Alto Research Center pod koniec lat 80. Od tego czasu ta praca plasuje się wśród najczęściej cytowanych artykułów naukowych w pokrewnych dyscyplinach akademickich, które przedstawiają połączony świat codziennych rzeczy. Ta wizja i związane z nią

zmiany są określane przez firmę Weiser jako „UbiquitousComputing" (znany również jako „Ubicomp"). Od momentu powstania koncepcji pojawiło się wiele innych powiązanych i zmodyfikowanych koncepcji, w tym wszechobecne, koczownicze, spokojne, niewidzialne, uniwersalne i wartościowe komputery, a także inteligencja otoczenia. Klaster Europejskich Projektów Badawczych dotyczących Internetu Rzeczy (CERP-IoT) łączy elementy konstrukcyjne wywodzące się z wyżej wymienionych koncepcji i podkreśla symbiotyczną interakcję świata rzeczywistego i fizycznego ze światem cyfrowym i wirtualnym. Z ich perspektywy obiekty fizyczne mają reprezentujące je wirtualne odpowiedniki, które przekładają je na obliczalne części świata fizycznego. Wizja CERP-IoT stała się ostatnio jeszcze bardziej wszechstronna, obejmując kwestie mediów społecznościowych, przewidując masową interakcję użytkowników z rzeczami i łącząc się z dodatkowymi informacjami dotyczącymi tożsamości, statusu, lokalizacji lub jakichkolwiek innych informacji biznesowych, społecznych lub prywatnych. Zasadniczo ITU (2005) definiuje IoT jako koncepcję, która umożliwia ludziom i rzeczom łączenie się w dowolnym czasie i miejscu, z czymkolwiek i kimkolwiek (i dodając - zgodnie z CERP-IoT, 2009 - najlepiej przy użyciu dowolnej ścieżki/sieci i dowolnej usługi). Inna linia spopularyzowana przez CISCO głosi prostą koncepcję: IoT rodzi się, gdy więcej rzeczy jest połączonych przez Internet jako istoty ludzkie. W związku z tym pojawienie się IoT może datować się na około 2008/2009 lub 2011. Zgodnie z prognozą Worldwide Internet of Things Forecast firmy International Data Corporation (IDC) na lata 2015–2020 przewiduje się, że do 2020 r. 30 miliardów podłączonych (autonomicznych) urządzeń stanie się częścią IoT. Inne szacunki przewidują około 1000 urządzeń na osobę do 2025 r. IoT znajduje się w centrum nakładających się na siebie wizji zorientowanych na Internet (oprogramowanie pośrednie), zorientowanych na rzeczy (czujniki) i zorientowanych na semantykę (wiedza). W szczególności (i) zorientowany na Internet, który kładzie nacisk na paradygmat sieciowy i wykorzystanie ustalonej infrastruktury sieciowej opartej na protokole IP w celu osiągnięcia wydajnego połączenia między urządzeniami oraz na opracowywaniu lekkich protokołów w celu spełnienia specyfiki Internetu Rzeczy; (ii) zorientowany na rzeczy, która koncentruje się na obiektach fizycznych i poszukiwaniu środków, które są w stanie je zidentyfikować i zintegrować z wirtualnym (cyber) światem; oraz (iii) zorientowany na semantykę, który ma na celu wykorzystanie technologii semantycznych, nadawanie sensu obiektom i ich danym do reprezentowania, przechowywania, łączenia i zarządzania ogromną ilością informacji dostarczanych przez rosnącą liczbę obiektów IoT. Ponieważ Internet Rzeczy nadal ewoluuje, prawdopodobnie rozwinie się również jego kompleksowa definicja. W związku z tym inicjatywa IEEE IoT daje członkom społeczności możliwość wniesienia wkładu w definicję IoT (IEEE, 2015, 2017). W dokumencie przedstawiono dwie definicje, jedną dla scenariuszy na małą skalę: „IoT to sieć, która łączy jednoznacznie identyfikowalne „Rzeczy" z Internetem. „Rzeczy" mają wykrywanie/uruchamianie i potencjalne możliwości programowania. Poprzez wykorzystanie unikalnej identyfikacji i wyczuwania, informacje o „Rzeczy" mogą być gromadzone, a stan „Rzeczy" może być zmieniany z dowolnego miejsca, w dowolnym czasie i przez cokolwiek." Druga definicja dotyczy scenariuszy na dużą skalę: „Internet rzeczy przewiduje samokonfigurującą się, adaptacyjną, złożoną sieć, która łączy „Rzeczy" z Internetem poprzez wykorzystanie standardowych protokołów komunikacyjnych. Połączone ze sobą rzeczy mają fizyczną lub wirtualną reprezentację w świecie cyfrowym, zdolność wykrywania/uruchamiania, cechę programowalności i są jednoznacznie identyfikowalne. Oświadczenie zawiera informacje, w tym tożsamość rzeczy, status, lokalizację lub wszelkie inne informacje biznesowe, społeczne lub prywatne. Rzeczy oferują usługi, z interwencją człowieka lub bez niej, poprzez wykorzystanie unikalnej identyfikacji, przechwytywania i komunikacji danych oraz możliwości uruchamiania. Usługa jest wykorzystywana za pomocą inteligentnych interfejsów i jest udostępniana w dowolnym miejscu, o każdej porze i ze względu na bezpieczeństwo". Uwzględniając różne perspektywy, odsłaniając jej jądro, możemy skonsolidować i zdefiniować: Gershenfeldz

IoT to świat połączonych ze sobą rzeczy, które są w stanie wykrywać, uruchamiać i komunikować się między sobą oraz z otoczeniem (tj. inteligentne rzeczy lub inteligentne obiekty), zapewniając jednocześnie możliwość dzielenia się informacjami i działania w częściach autonomicznie w stosunku do wydarzeń ze świata rzeczywistego/fizycznego i poprzez uruchamianie procesów i tworzenie usług z lub bez bezpośredniej interwencji człowieka.

Celowo pomijamy, czy ta „wielka fabuła" będzie koniecznie realizowana na standardowych protokołach komunikacyjnych, czy na zunifikowanych ramach. Chociaż zunifikowana struktura byłaby z pewnością optymalna, może nie być konieczna ani nawet niemożliwa do osiągnięcia, biorąc pod uwagę wymiarowość i złożoność prawdopodobnie bardzo heterogenicznego skomputeryzowanego świata wzajemnie powiązanych rzeczy.

Koncepcje Internetu Rzeczy

Wraz z postępem technicznym zmienia się nasza interakcja z systemami informatycznymi, zarówno w pracy, jak i w czasie wolnym. Technologie informacyjne, sensorowe i sieciowe stają się coraz mniejsze, wydajniejsze i coraz częściej wykorzystywane. Ludzie stykają się już nie tylko z technologią informacyjną w wspólnych punktach swojego życia, na przykład w biurach czy przy biurkach, ale z infrastrukturą informacyjno-komunikacyjną, która jest obecna w coraz większej liczbie obszarów życia codziennego. Infrastruktury te charakteryzują się tym, że obejmują nie tylko klasyczne urządzenia, na przykład komputery osobiste i telefony komórkowe, ale również technologie informacyjne i komunikacyjne są osadzone w obiektach i środowiskach. Wizja Ubiquitous Computing Marka Weisera sugeruje, że komputery, jakie znamy obecnie, „znikają", a dokładniej odsuwają się na dalszy plan. Przedmioty codziennego użytku i nasze najbliższe otoczenie przejmują wtedy zadania i możliwości komputerów. W swoim przełomowym artykule Weiser opisuje to następująco: „Najgłębsze technologie to te, które znikają. Wplatają się w tkankę codziennego życia, aż stają się od niej nie do odróżnienia". Poprzez fizyczne osadzenie IT przedmioty codziennego użytku i nasze codzienne środowisko stają się „inteligentne", to znaczy zdolne do przetwarzania i dostarczania informacji, ale niekoniecznie inteligentne w sensie ludzkiej inteligencji poznawczej. W innym wysoko cenionym artykule Weiser wraz z Brownem wprowadzili pojęcie „spokojnego przetwarzania". Odnoszą się również do połączonego świata pełnego komputerów. Jednak tylko w przypadku świadczenia usług lub gdy istnieje potrzeba interakcji, te komputery lub ich odpowiednie usługi stają się „widoczne"; innym razem te możliwości są „spokojne" w tle i nie są nachalne ani nawet niewidoczne dla użytkowników. Podstawowe koncepcje obejmujące IoT, a także powiązane koncepcje i modele zostaną przedstawione w kolejnych sekcjach.

Podstawowe pojęcia: inteligentne obiekty i inteligentne środowiska

Inteligentny obiekt to obiekt fizyczny, w którym osadzony jest procesor, system przechowywania danych, system czujników i technologia sieciowa. Niektóre inteligentne obiekty mogą również wpływać na swoje otoczenie za pomocą siłowników. W zasadzie wszystkie przedmioty fizyczne można zamienić w inteligentne przedmioty, na przykład konwencjonalne przedmioty codziennego użytku, takie jak długopisy, zegarki na rękę (istnieje wiele modeli zegarków na rękę z czujnikami i procesorami, na przykład do pomiaru tętna lub określenia położenia geograficznego), lub samochody (od niedawna samochody autonomiczne). W kontekście przemysłowym może to być maszyna lub produkt, którym należy manipulować. Inteligentne obiekty również mogą znajdować się w dowolnym miejscu. W rzeczywistości nie ma prawie żadnych ograniczeń dotyczących dziedzin: urządzeń elektroniki użytkowej, sprzętu AGD, urządzeń medycznych, aparatów fotograficznych oraz wszelkiego rodzaju czujników i urządzeń generujących dane. Większość obiektów inteligentnych posiada interfejs użytkownika i możliwości interakcji umożliwiające komunikację z otoczeniem lub innymi urządzeniami

(np. wyświetlaczami). Zdolność inteligentnych obiektów do komunikowania się z innymi obiektami i ich środowiskiem jest podstawowym elementem IoT. Zgodnie z tym pomysłem jest to, że określone informacje można pobrać za pomocą dowolnego inteligentnego obiektu podłączonego do sieci, który jest jednoznacznie zidentyfikowany i zlokalizowany i może mieć „własną stronę główną", czyli unikalny adres. Dziś można skorzystać z szerokiej gamy dość niedrogich, małych i stosunkowo wydajnych komponentów, w tym czujników, siłowników i komputerów jednopłytkowych (SBC), aby wzbogacić rzeczy fizyczne i połączyć je z Internetem. SBC, takie jak Raspberry Pi, BeagleBone Black i Intel Edison Open, a także elektronika open-source, taka jak Arduino, która pojawiła się na rynku w latach 2005-2008, była katalizatorem milionów nowych pomysłów i projektów. Tworzenie i zbieranie danych o stanie fizycznych obiektów może stanowić podstawę ciekawych projektów automatyki domowej i biurowej, edukacji i zajęć rekreacyjnych z wizualizacjami w czasie rzeczywistym informacji generowanych z danych „w biegu". Co więcej, można wykorzystać zdalne sieci inteligentnych urządzeń rozmieszczonych gdzie indziej. Z „inteligentnymi obiektami" ściśle wiąże się koncepcja „inteligentnych środowisk". Jedna definicja podkreśla fizyczny zakres, w jakim inteligentne obiekty są wdrażane i wchodzą w interakcje. Kompilacja inteligentnych obiektów w obrębie danej przestrzeni, takiej jak przestrzeń zamknięta (samochód, dom, pokój) lub teren zewnętrzny, na przykład dzielnica lub całe miasto, zamienia wspólne środowisko w inteligentne. Inna definicja mówi, że czujniki są kluczowym czynnikiem w inteligentnym środowisku. Niezbędne dla inteligentnego środowiska są informacje kontekstowe gromadzone przez czujniki w celu zapewnienia dostosowanych aplikacji i usług. Weiser zdefiniował inteligentne środowisko jako „fizyczny świat, który jest bogato i niewidocznie przeplatany czujnikami, siłownikami, wyświetlaczami i elementami obliczeniowymi, płynnie osadzony w codziennych przedmiotach naszego życia i połączony przez ciągłą sieć".

Pojęcia pokrewne: Komunikacja maszyna-maszyna, Przemysłowy Internet Rzeczy i Przemysł 4.0

IoT nie jest konstruktem, który pojawił się nagle lub bez prekursorów. Technologiczni prekursorzy i różne konceptualizacje istnieją przed stosunkowo nową etykietą „IoT", na przykład komunikacja maszyna-maszyna (M2M). Ponadto istnieją najnowsze pochodne, na przykład Przemysłowy Internet Rzeczy i Przemysł 4.0. W kolejnych sekcjach podjęto próbę rozeznania ich podobieństw i różnic oraz wzajemnego powiązania tych pojęć.

Komunikacja maszyna-maszyna

Komunikacja M2M odnosi się do bezpośredniej przewodowej lub bezprzewodowej komunikacji między urządzeniami przy użyciu dowolnego kanału komunikacyjnego, która niekoniecznie wymaga bezpośredniej interwencji człowieka. W związku z tym firma M2M może być postrzegana jako prekursor IoT. Komunikacja M2M może obejmować przemysłowe zakłady produkcyjne, umożliwiając czujnikowi lub licznikowi przekazywanie danych, które rejestruje (np. temperatury, przepustowości i poziomu zapasów) do oprogramowania aplikacyjnego, które może je dalej przetwarzać (np. dostosowywać proces przemysłowy na podstawie parametrów technicznych , takich jak temperatura lub uruchamianie nowych procesów, takich jak składanie zamówień w celu uzupełnienia zapasów). Taka komunikacja miała na celu monitorowanie zdalnych maszyn, z których dane były odbierane, przetwarzane na jakiejś stacji centralnej i ostatecznie przekazywane z powrotem do tych maszyn z dostosowanymi parametrami, jeśli to konieczne. Główną motywacją wielu organizacji jest zmniejszenie kosztów zarządzania usługami poprzez zdalną diagnostykę, zdalne rozwiązywanie problemów, zdalne aktualizacje i inne zdalne funkcje, które zmniejszają potrzebę rozmieszczania personelu serwisowego w terenie. IoT obsługuje te same urządzenia/zasoby/maszyny, co aplikacje M2M, ale także bardzo małe (o niskim poborze mocy), osobiste i niedrogie urządzenia z czasami bardzo ograniczoną funkcjonalnością, które mogą nie uzasadniać zastosowania dedykowanego modułu sprzętowego M2M. Chociaż komunikacja IoT i M2M zapewnia zdalny dostęp do maszyn lub ogólniej

„urządzeń", nie ma innych istotnych podobieństw. Na przykład tradycyjne rozwiązania M2M zazwyczaj opierają się na komunikacji punkt-punkt z wykorzystaniem wbudowanych modułów sprzętowych i dedykowanych protokołów. W przeciwieństwie do tego rozwiązania IoT zależą głównie od sieci opartych na protokole IP, aby łączyć dane urządzenia z platformą chmury lub oprogramowania pośredniczącego, głównie przy użyciu wspólnych/otwartych protokołów (w celu zapewnienia maksymalnej interoperacyjności, w znaczeniu zdalnego urządzenia połączonego z jakimś centralnym koncentratorem, a także szczególna interoperacyjność między samymi urządzeniami). Kolejną różnicą jest to, że rozwiązania M2M oferują zdalny dostęp do danych maszynowych, które tradycyjnie są ukierunkowane na rozwiązania punktowe w aplikacjach zarządzania usługami. W przeszłości dane te rzadko, jeśli w ogóle, były integrowane z aplikacjami korporacyjnymi w celu poprawy ogólnej wydajności firmy. Wreszcie dostarczanie danych w oparciu o IoT w coraz większym stopniu obejmuje usługi w chmurze umożliwiające dostęp za pośrednictwem dowolnej aplikacji korporacyjnej objętej sankcjami, podczas gdy M2M zazwyczaj wykorzystuje bezpośrednią komunikację punkt-punkt. Architektura oparta na chmurze sprawia również, że IoT jest z natury bardziej skalowalny, eliminując potrzebę przyrostowych połączeń przewodowych lub instalacji kart SIM. M2M jest często określane jako „hydraulika", podczas gdy IoT jest postrzegany jako uniwersalny czynnik. Można argumentować, że granice pojęciowe i wizje IoT i M2M coraz bardziej się nakładają. Wskazuje na to, że nowsza komunikacja M2M przekształciła się w system sieci, które przesyłają dane do urządzeń osobistych. W tym sensie komunikacja M2M w coraz większym stopniu korzysta z ekspansji sieci IP na całym świecie, przełączając się z zastrzeżonych połączeń typu punkt-punkt na komunikację wielopunktową opartą na protokole IP. Możemy wywnioskować, że kwestie M2M skupiają się bardziej na warstwie infrastruktury technicznej. W przeciwieństwie do tego, wyłaniający się Internet Rzeczy ma znacznie większy zakres. IoT wymaga integracji danych z urządzeń i czujników z inteligencją biznesową, analizą i innymi aplikacjami korporacyjnymi, aby osiągnąć liczne korzyści w przedsiębiorstwach produkcyjnych, z silnym naciskiem na ulepszanie produktów, procesów i modeli biznesowych.

Internet Przemysłowy i Przemysł 4.0

Szeroka segmentacja IoT obejmuje (i) perspektywę zorientowaną na konsumenta, w tym smartfony, samochody połączone, inteligentne telewizory i urządzenia do noszenia, oraz (ii) perspektywę przemysłową. Do tych ostatnich należą m.in. sieci i elektrownie, transport, turbiny wiatrowe, urządzenia przemysłowe. Prostą analogią jest przełożenie obiektów z kontekstu przemysłowego (produkcyjnego) na obiekty inteligentne. Obiekty produkcyjne, takie jak narzędzia, przenośniki, a nawet produkty, które mają być manipulowane lub budowane, staną się inteligentnymi obiektami, jak określono tutaj koncepcyjnie. Zgodnie z tym wyobrażeniem „wspólna fabryka" zamienia się w inteligentną fabrykę. Można by twierdzić, że może to stanowić podstawę nowego, fundamentalnego sposobu koordynowania i wytwarzania dóbr. Te oczekiwania łączą się, określając nadchodzącą erę „Czwartą Rewolucją Przemysłową". W związku z tym zwykle używany jest termin Industrial Internet of Things lub po prostu Industrial Internet. Co więcej, w kontekście IIoT termin ten jest często używany jako synonim Przemysł 4.0 lub oryginalnego niemieckiego terminu „Industrie 4.0", który jest etykietą dla różnych inicjatyw rządowych w Niemczech (Światowe Forum Ekonomiczne, 2015). Różnice między terminami lub inicjatywami dotyczą głównie interesariuszy, ukierunkowania geograficznego i reprezentacji . IIoT również semantycznie opisuje ruch technologiczny, podczas gdy Przemysł 4.0 jest bardziej związany z oczekiwanymi skutkami ekonomicznymi. Przewiduje się, że wizja Przemysłu 4.0 zostanie zrealizowana przez IIoT. Ogłoszone implikacje i korzyści IIoT są wielorakie i są zakorzenione w „cechach pochodnych" nowoczesnych ICT, w szczególności wrażliwości na kontekst, zdolności adaptacyjnych, proaktywności i zwiększonej jakości danych. Ostatecznie te cechy pochodne mogą pomóc w osiągnięciu większej wydajności zasobów, krótszego czasu wprowadzania produktów na rynek, produktów o wyższej wartości i nowych usług

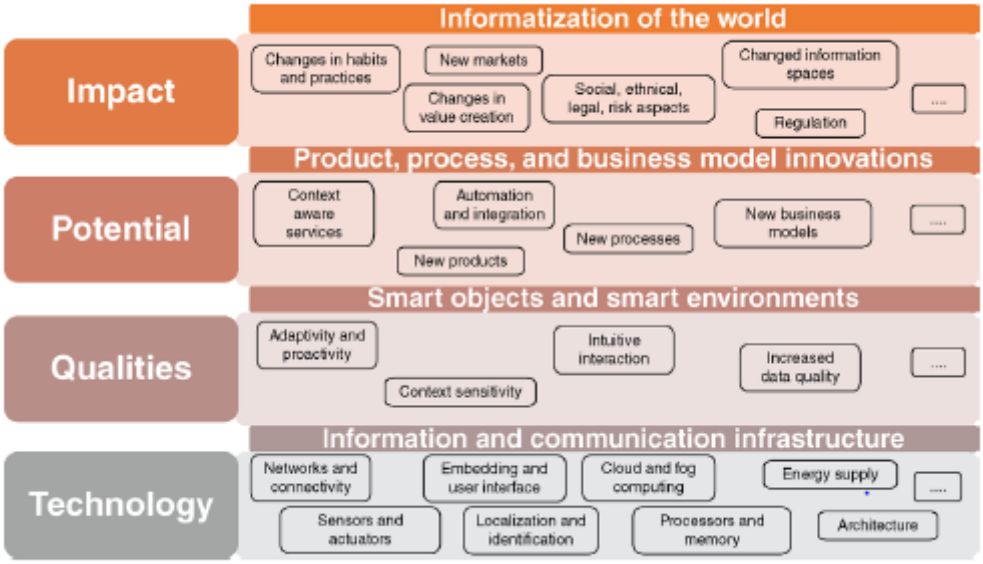
Kto pracuje w Internecie Rzeczy?

Prawdziwie połączony świat pod względem IoT nie został jeszcze w pełni osiągnięty. Jednak wiele organizacji i sojuszy z branży, środowisk akademickich i różnych szczebli rządowych pracuje nad Internetem Rzeczy i ściśle powiązanymi strumieniami, często w częściach pod różnymi nazwami. W tej sekcji znajdują się wybitni krajowi i międzynarodowi przedstawiciele organów rządowych, środowisk akademickich i przemysłu. Dzięki wsparciu 7 programu ramowego Komisji Europejskiej sfinansowano znaczną liczbę inicjatyw i projektów, takich jak projekt architektury Internetu przedmiotów (IoT-A) i inicjatywa Internetu przedmiotów (IoT-i). Ważną organizacją w tym obszarze jest Europejski Klaster Badawczy Internetu Rzeczy (IERC), który koordynuje bieżące działania w obszarze IoT w całej Europie. Witryna internetowa towarzysząca wydaniu specjalnemu poświęconemu interoperacyjności IoT zawiera między innymi wykazy projektów finansowanych przez UE rozpoczętych od 1 stycznia 2016 r. oraz międzynarodowych projektów IoT. Sojusz na rzecz innowacji Internetu rzeczy (AIOTI) został zainicjowany przez Komisję Europejską w celu wspierania rozwoju europejskiego ekosystemu IoT, w tym polityki standaryzacji. Ich grupy robocze odpowiadają obszarom zastosowań IoT, w tym inteligentnym środowiskom życia dla osób starszych, inteligentnych rolnictwo i bezpieczeństwo żywności, urządzenia do noszenia, inteligentne miasta, inteligentna mobilność, inteligentne zarządzanie wodą, inteligentna energia oraz inteligentne budynki i architektura. ETSI wraz z programem Connecting Things opracowuje standardy bezpieczeństwa danych, zarządzania danymi, przesyłania danych i przetwarzania danych związanych z potencjalnym połączeniem miliardów inteligentnych obiektów w jedną sieć komunikacyjną. IEEE posiada dedykowaną inicjatywę IoT i zbiór informacji dla społeczności technicznej zaangażowanej w badania, wdrażanie, stosowanie i użytkowanie technologii IoT. Internet Engineering Task Force (IETF) jest najważniejszym organem ustanawiającym standardy Internetu i posiada dyrekcję IoT, która koordynuje powiązane działania w swoich grupach roboczych, przegląda specyfikacje pod kątem spójności i monitoruje działania związane z Internetem Rzeczy w innych grupach normalizacyjnych. Ponieważ istnieje potrzeba osiągnięcia konsensusu w kwestiach technicznych IoT, utworzono Sojusz IPSO (Internet Protocol for Smart Objects). Zrzesza ponad 60 firm członkowskich z wiodących firm telekomunikacyjnych i energetycznych współpracujących z organami normalizacyjnymi, takimi jak IETF, IEEE i ITU. Chiny postawiły IoT w swoim strategicznym programie, w tym inicjatywy państwowe i finansowane przez przemysł (np. „Internet of Things Union Sensing China" w Wuxi). Ponadto Industrial Internet Consortium (IIC) pracuje nad przemysłową architekturą IoT i opublikowało architekturę referencyjną dla IoT w 2015 roku. Ponadto dosłownie wszystkie główne krajowe i ponadnarodowe organy normalizacyjne pracują nad kwestiami IoT, w tym ISO/IECJTC-1 . Na przykład ITU utworzyło „Grupę badawczą 20". The Manufacturers Alliance for Productivity and Innovation (MAPI) opracowuje Przemysł 4.0 dla przemysłowych zastosowań IoT. OASIS opracowuje otwarte protokoły, aby zapewnić interoperacyjność dla IoT, zwłaszcza w oparciu o Message Queuing Telemetry Transport (MQTT) jako preferowany protokół przesyłania wiadomości dla IoT. Online Trust Alliance, grupa dostawców zabezpieczeń, opracowała projekt struktury zaufania dla aplikacji IoT, koncentrując się na bezpieczeństwie, prywatności i zrównoważonym rozwoju. Open Management Group to konsorcjum standardów technicznych, które opracowuje kilka standardów IoT, w tym usługę dystrybucji danych (DDS) i język modelowania przepływu interakcji (IFML), wraz z platformami niezawodności, modelowaniem zagrożeń i ujednoliconym modelem komponentów dla czasu rzeczywistego i wbudowanego systemy. Jednocześnie w Japonii, Korei, Stanach Zjednoczonych i Australii trwają inicjatywy na dużą skalę, w których przemysł, powiązane organizacje i agencje rządowe współpracują przy różnych programach, takich jak inicjatywy dotyczące inteligentnych miast, programy inteligentnych sieci obejmujące technologie inteligentnych pomiarów (w niektórych krajach

europejskich inteligentne opomiarowanie stało się prawnie wymagane w przypadku nowych budynków) oraz wdrażanie szybkiej infrastruktury szerokopasmowej (np. w Niemczech).

Ramy Internetu Rzeczy

Krótkie omówienie zagadnień technicznych, ekonomicznych i społecznych w następnym akapicie pokazuje, że IoT obejmuje szeroki zakres tematów i dyscyplin. Mając na celu uporządkowanie pola, proponujemy następującą czterowarstwową „strukturę Internetu rzeczy".



W istocie, nowoczesne technologie informacyjne i komunikacyjne stanowią techniczną podstawę IoT (objętą warstwą 1). IoT generuje sieć jednoznacznie identyfikowalnych obiektów fizycznych (rzeczy). Networking, a co za tym idzie także umiejętność komunikowania się, odnosi się nie tylko do ludzkich uczestników, ale także do zaangażowanych obiektów (lub rzeczy). Te rzeczy są wyposażone w zminiaturyzowane procesory i siłowniki, na przykład elementy mechaniczne, regulatory temperatury i urządzenia wyjściowe audio lub wideo, które można wykorzystać do sterowania obiektami i środowiskiem. Pozwala to na dostosowywanie obiektów i środowisk do naszych potrzeb, interakcję z sytuacją oraz dostarczanie informacji i usług zgodnie z określonymi wymaganiami sytuacyjnymi, czyli stają się „inteligentnymi obiektami" i „inteligentnymi środowiskami" (opisanymi w warstwie 2). Automatyczna identyfikacja za pomocą RFID jest często uważana za podstawę IoT. Czujniki i aktuatory rozszerzają funkcjonalność poprzez przechwytywanie stanów i wykonywanie działań lub efektów na rzeczywistość. Skutkuje to potencjałem dla nowych usług, w tym produktów konsumenckich, a także nowych procesów biznesowych i modeli biznesowych (opisanych w warstwie 3). Na przykład produkty dla konsumentów mogą zawierać i dostarczać dużą ilość informacji, a także oferować klientom dodatkowe usługi specyficzne dla kontekstu w fazie posprzedażowej. IoT zapewnia również wyższy poziom jakości danych dla procesów biznesowych, umożliwiając organizacjom szybsze i właściwe reagowanie na zdarzenia oraz może przyczynić się do poprawy wydajności, dokładności i korzyści ekonomicznych .Potencjały te doprowadzą do różnych innowacji w zakresie produktów, procesów i modeli biznesowych. Ponieważ te innowacje wpływają na nasze codzienne życie, mają szeroki wpływ na jednostki, społeczeństwo, rynki i firmy (opisane w warstwie 4). Z jednej strony firmy są pod presją dostosowywania się do zmieniających się form tworzenia wartości i struktur rynkowych, a także zmieniających się potrzeb klientów. Z drugiej strony innowacyjne firmy mają możliwość opracowywania nowych produktów, procesów i modeli biznesowych, które pozwalają im lepiej zaspokajać potrzeby swoich klientów, a tym samym uczestniczyć w projektowaniu

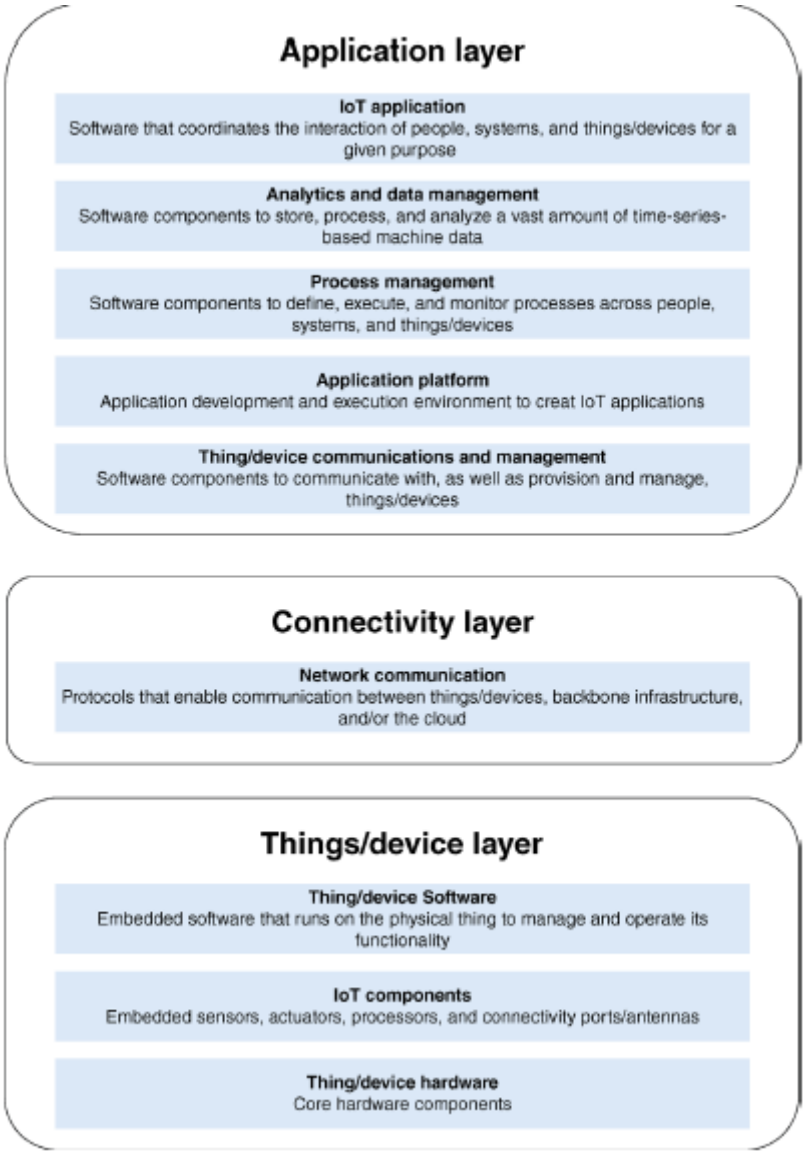
skomputeryzowanego świata. Efekty są wielorakie i nie zawsze wyłącznie pozytywne dla każdego. Rzeczywiście, Internet Rzeczy stanowi poważne wyzwanie dla firm, osób i społeczeństw jako całości. Główne wyzwania i problemy obejmują (i) bezpieczeństwo, prywatność, interoperacyjność i standardy; (ii) prawne, regulacyjne i prawa; oraz (iii) gospodarki wschodzące i skutki społeczne, na przykład niektóre miejsca pracy znikną, pojawią się nowe miejsca pracy, większe wykorzystanie technologii może prowadzić do mniejszej liczby interakcji międzyludzkich i manualnych, różne formy życia społecznego mogą ewoluować itd.

Infrastruktura teleinformatyczna

Warstwa „Technologia" opisuje elementy składowe infrastruktury technologii informacyjno-komunikacyjnych (ICT) do komputeryzacji (codziennego) świata. Te bloki konstrukcyjne obejmują wiele komponentów oprogramowania i sprzętu, a także wysoce rozwinięte i nowatorskie technologie. Służą do łączenia wirtualnych informacji o rzeczach lub z rzeczy z fizycznym światem rzeczywistym. Obejmują one technologie przetwarzania, przechowywania, osadzania oraz sieci mobilnych i bezprzewodowych, a także czujniki i siłowniki. Ponadto ulepszone metody dostarczania, identyfikacji i lokalizacji energii stanowią podstawowe elementy IoT. Zazwyczaj, aby poradzić sobie z ogromną złożonością wynikową, stosuje się podejście warstwowe. Kolejne sekcje opisują elementy składowe warstwy technologicznej, które są podstawowym wymiarem IoT.

Modele architektoniczne i referencyjne

Szczególnie w przypadku warstwy technologicznej istniejąca literatura obejmuje wiele propozycji architektonicznych, modeli referencyjnych i opisów technicznych obecnego lub przewidywanego stanu IoT. Rysunek



przedstawia widok wysokiego poziomu w kategoriach trójwarstwowego stosu technologii istotnych dla IoT: (i) warstwa rzeczy lub urządzenia, (ii) warstwa łączności oraz (iii) warstwa aplikacji. W warstwie urządzenia sprzęt specyficzny dla IoT, taki jak czujniki, siłowniki, pamięć i procesory, jest dodawany do istniejących podstawowych komponentów sprzętowych, a wbudowane oprogramowanie ma za zadanie zarządzać funkcjonalnością konkretnej rzeczy fizycznej i obsługiwać ją. W warstwie łączności protokoły komunikacyjne umożliwiają komunikację między rzeczami a połączoną infrastrukturą, na przykład za pośrednictwem usług w chmurze. W związku z tym w warstwie aplikacji IoT zapewniona jest komunikacja z urządzeniami i powiązana funkcjonalność, podczas gdy platforma aplikacji umożliwia tworzenie i wykonywanie aplikacji IoT. Jak pokazały najnowsze osiągnięcia, oprogramowanie do analizy i zarządzania danymi ma coraz większe znaczenie dla obsługi ogromnych ilości danych, czyli przechowywania, przetwarzania i analizowania danych generowanych przez połączone elementy. Co więcej, oprogramowanie do zarządzania procesami pomaga definiować, wykonywać i monitorować procesy w ludziach, systemach i rzeczach. Wśród wyższych warstw oprogramowanie aplikacji IoT koordynuje interakcję ludzi, systemów i rzeczy w określonym celu. We wszystkich warstwach komponenty oprogramowania zarządzają aspektami tożsamości i bezpieczeństwa, a także integracją z systemami biznesowymi, np. ERP czy CRM oraz z zewnętrznymi

źródłami informacji. IoT otrzymał impuls dzięki komercyjnemu zaangażowaniu dużych graczy z różnych branż: Google ogłosił Brillo jako system operacyjny dla urządzeń IoT w inteligentnych domach; coraz więcej urządzeń jest wyposażonych w standardy komunikacji M2M, takie jak Bluetooth, ZigBee i Wi-FI o niskim poborze mocy; Microsoft ogłosił, że Windows będzie obsługiwał systemy wbudowane i tak dalej.

Sieci i łączność

Technologie sieciowe łączą obiekty wyposażone w technologię informatyczną i mogące znajdować się w różnych lokalizacjach. W tym celu dostępna jest duża liczba technologii sieciowych, w zależności od aplikacji. Cechą wyróżniającą związaną z aplikacją jest skalowanie zakresu. Obejmuje ona sieci globalne (satelity), sieci regionalne i lokalne, a także tak zwane sieci osobiste, cielesne i wewnątrzciałowe. Sieci osobiste (PAN) mogą na przykład łączyć się za pośrednictwem urządzeń WLAN, zwykle na obszarze do 10m² wokół jednej lub dwóch osób. W przeciwieństwie do komputerów PC, smartfonów i podobnych urządzeń, urządzenia loT są zwykle ograniczone pod względem przestrzeni pamięci, dostępu do stałego źródła zasilania i mocy obliczeniowej. Tradycyjne protokoły (w szczególności stos protokołów TCP/IP) nie zostały zaprojektowane z myślą o tych wymaganiach. W rezultacie w ciągu ostatnich lat opracowano wiele tak zwanych lekkich protokołów komunikacyjnych na praktycznie wszystkich warstwach stosu protokołów, aby zapewnić interoperacyjność między urządzeniami IoT. Jednym z podejść do interoperacyjności IoT jest rozważenie warstwowej struktury stosu sprzętu/oprogramowania:

* Niższe warstwy (zgodnie z modelem OSI, warstwa fizyczna i warstwa łącza danych; w kontekście innym niż OSI, czasami oznaczane jako warstwa urządzenia) mają na celu bezproblemową integrację nowych urządzeń z istniejącym ekosystemem IoT.

*Warstwa sieciowa obsługuje mobilność obiektów i routing informacji.

* Warstwa oprogramowania pośredniego ułatwia bezproblemowe wykrywanie usług i zarządzanie inteligentnymi obiektami.

* Warstwa aplikacji ponownie wykorzystuje heterogeniczne usługi aplikacji z heterogenicznych platform.

* Warstwa danych i semantyki wprowadza wspólne rozumienie danych i informacji.

Oto najważniejsze przykłady znormalizowanych protokołów komunikacyjnych opartych na protokole IP dla urządzeń IoT: (i) w warstwie aplikacji, silnik IETF Constrained Application Protocol (CoAP)/REST i Message Queuing Telemetry Transport (MQTT); (ii) w warstwie sieciowej, IPv6 i RPL (oraz pochodne dla bezprzewodowych sieci osobistych o małej mocy „6LoWPAN"); (iii) w warstwie fizycznej, IEEE 802.15. Przykłady protokołów zorientowanych semantycznie obejmują OPC UA (OPC Unified Architecture), UPnP (Universal Plug and Play), DPWS (Devices Profile for Web Services), CoAP (Constrained Application Protocol) i EXI (Efficient XML Interchange) (Weyrich i Ebert, 2016). Interoperacyjność ma kilka wymiarów. Warto zauważyć, że nawet wysoki stopień standaryzacji protokołów nie oznacza wysokiego stopnia standaryzacji formatów danych czy kompatybilności urządzeń. W rzeczywistości interoperacyjność jest obecnie utrudniona przez ten warunek. W idealnej sytuacji komunikacja musi być niezależna od twórcy danego fragmentu infrastruktury. W rzeczywistości jednak różni gracze (w tym dostawcy) mają własne rozwiązania IoT, które są mniej lub bardziej niekompatybilne z innymi rozwiązaniami, tworząc w ten sposób lokalne „silosy IoT". Duża część ostatnich badań nad Internetem Rzeczy poświęcona jest zatem interoperacyjności. Przykładem może być unijny projekt Unify-IoT: szacują oni ponad 360 dostępnych dostawców platform IoT i

ustalają, że około 20 jest dość popularnych. Wskazuje to wyraźnie, że masowe wysiłki badawcze niekoniecznie są zbieżne. Do wymiany danych między aplikacjami, urządzeniami i obiektami istnieją dobrze znane standardy komunikacji, w tym Bluetooth, Wi-Fi23 i różne standardy komunikacji mobilnej , takich jak GSM. W oparciu o przypadki użycia komunikacji mobilnej osiągnięto duży postęp technologiczny w zakresie większej przepustowości (i odpowiednio wyższych przepływności), możliwości przesyłania strumieniowego multimediów i tak dalej. Jednak, jak wspomniano wcześniej, większość przypadków użycia IoT dotyczy urządzeń o ograniczonych zasobach. W związku z tym cel „Sieci o małej mocy, rozległe sieci" (LPWAN) stał się głównym tematem w IoT w ciągu ostatnich kilku lat. LPWAN to szerokie określenie różnych technologii używanych do łączenia czujników i kontrolerów z Internetem bez korzystania z tradycyjnych sieci Wi-Fi lub komórkowych. Jednocześnie jednak główni gracze w branży sieci komórkowych również dalej rozwijają standardy sieci komórkowych, na przykład LTE-M i NB-IoT. Ten ostatni jest wspierany przez wiodących producentów i 20 największych operatorów telefonii komórkowej na świecie. Kolejne przykłady działań tworzących nowe standardy lepiej dopasowane do przypadków użycia IoT to LoRa i N-Wave oraz Sigbox. Głównymi względami projektowymi są niskie zużycie energii (do ponad 10 lat autonomii), silna penetracja w środowiskach wewnętrznych oraz podłączanie dużej liczby czujników i urządzeń o małych wymaganiach w zakresie przepustowości.

Osadzanie

Przewidywanej wszechobecności skomputeryzowanego świata nie da się jednak urzeczywistnić poprzez ustawianie komputerów na rogach każdej ulicy. Zamiast tego funkcjonalności są osadzone w obiektach i przestrzeniach. Na przykład materiały przewodzące są tkane lub drukowane na tekstyliach. Obiekty są następnie komputeryzowane w ten sposób, co pozwala nam na natychmiastowe otrzymywanie informacji o nich i ich przetwarzanie. Miniaturyzacja sprzętu jest niezbędnym warunkiem wbudowania IT w obiekty. Zgodnie z wciąż obowiązującym prawem Moore′a miniaturyzacji towarzyszy poprawa wydajności procesorów i zwiększenie pojemności pamięci masowej, przy niezmienionych lub nawet obniżonych kosztach wytwarzania komponentów. Te osiągnięcia sprzyjają powszechnemu rozpowszechnianiu technologii informacyjnych i komunikacyjnych oraz pozwalają na ich osadzenie w dowolnych, nawet małych i krótkotrwałych obiektach. Nie zawsze dotyczy to zwiększonej wydajności, ale może obejmować inne czynniki, na przykład efektywność energetyczną komponentów. Podczas osadzania komputerów lub komponentów w rzeczach fizycznych często pojawiają się nowe wyzwania dla interfejsu użytkownika. Na przykład, jak można komunikować się z „znikającymi" komputerami? Wyświetlacze, klawiatury i inne powszechnie używane urządzenia wejściowe i wyjściowe mogą nie zawsze stanowić optymalne rozwiązanie. Istnieje potrzeba nowych metafor i interfejsów użytkownika, w szczególności dostosowanych do intuicyjnej interakcji

Czujniki

Czujniki są komponentami technicznymi do jakościowego lub ilościowego pomiaru pewnych zmiennych i właściwości chemicznych lub fizycznych, na przykład temperatury, światła (natężenia i barwy), przyspieszenia, elektryczności i tak dalej. Zarejestrowane wartości pomiarowe są zwykle przekształcane na sygnały elektroniczne. Obecnie jesteśmy już otoczeni czujnikami w wielu miejscach. Na przykład nowoczesne samochody zawierają setki czujników, na przykład czujniki deszczu do wycieraczek przedniej szyby, czujniki zderzeniowe do systemów zwalniania poduszek powietrznych oraz czujniki wspomagania pasa ruchu i parkowania. Rzeczywiście, nowoczesne samochody, niektóre z ponad 200 czujnikami i kilkudziesięcioma mikroprocesorami, są tego dobrym przykładem. W rzeczywistości zwykły samochód staje się w coraz większym stopniu jednym zunifikowanym skomputeryzowanym obiektem. Ponadto, gdy czujnik jest używany razem z procesorem

(sterownikiem), zasilaczem i jednostką do transmisji danych, nazywa się to węzłem czujnika. Podstawową funkcją węzła czujnikowego jest zbieranie, wstępne przetwarzanie i przesyłanie danych czujnika z jego otoczenia do innych węzłów czujnikowych lub stacji bazowej. Przykłady kategorii czujników obejmują następujące:

* Lokalizacja: GPS, GLONASS, Galileo

* Biometryczne: odcisk palca, tęczówka, twarz

* Akustyka: mikrofon

* Środowisko: temperatura, wilgotność, ciśnienie

* Ruch: akcelerometr, żyroskop

Węzły czujnikowe mogą tworzyć bezprzewodowe sieci czujnikowe (WSN) za pomocą ich jednostki transmisyjnej. Przykładowo są one wykorzystywane do (i) wykrywania trzęsień ziemi, pożarów lasów, lawin, a także ataków terrorystycznych; (ii) monitorować ruch pojazdów, zwłaszcza w tunelach; (iii) śledzić ruchy dzikich zwierząt; (iv) chronić własność; (v) sprawnie obsługiwać i zarządzać maszynami i pojazdami; (vi) ustanowić strefy bezpieczeństwa; (vii) monitorować zarządzanie łańcuchem dostaw; oraz (viii) odkryć materiał chemiczny, biologiczny i radiologiczny. Do obsługi sieci czujników wymagane jest specjalne oprogramowanie, które zapewnia dynamiczną i solidną samoorganizację sieci czujników, która działa w bezpieczny i skalowalny sposób. Dzieje się tak, ponieważ węzły czujników mogą ulec awarii, zmienić swoją pozycję lub być w trybie online tylko sporadycznie. WSN może składać się z kilkuset lub setek tysięcy węzłów sensorowych, które są rozmieszczone wewnątrz zjawiska lub bardzo blisko niego. Węzły czujnikowe są połączone z siecią pośredniczącą, która przekazuje zebrane dane do komputera w celu analizy. Węzły czujnikowe są instalowane w ich przestrzeni roboczej, aby działały przez lata, najlepiej bez konieczności konserwacji lub interwencji człowieka. Dlatego muszą mieć niskie zapotrzebowanie na energię i mieć baterie, które działają przez kilka lat. Konstrukcja typowego WSN jest warstwowa. W szczególności zaczyna się od czujników na niższym poziomie i prowadzi do węzłów najwyższego poziomu w celu gromadzenia, analizy i przechowywania danych. Proste i złożone dane są kierowane przez sieć do zautomatyzowanego obiektu, który zapewnia ciągłe monitorowanie i kontrolę dedykowanego środowiska. WSN niekoniecznie działają na wszystkich warstwach ze wspólnym stosem TCP/IP i mogą zamiast tego używać dedykowanych, lekkich protokołów. Każda klasa platformy obsługuje różne rodzaje wykrywania. Ponieważ czujniki są podstawą zarówno inteligentnych obiektów, jak i węzłów czujników, są kluczowym elementem świata IoT. W rzeczywistości sieci WSN ułatwią rozprzestrzenianie się wielu aplikacji. Małe, solidne, niedrogie i energooszczędne czujniki WSN doprowadzą IoT do nawet najmniejszych obiektów zainstalowanych w dowolnym środowisku, przy rozsądnych kosztach

Siłowniki

Siłowniki przekształcają sygnały elektryczne (np. polecenia pochodzące z komputera sterującego) na ruch mechaniczny lub inne zmienne fizyczne (np. ciśnienie lub temperaturę), a tym samym aktywnie interweniują w system sterowania i/lub ustawiane zmienne. W dziedzinie inżynierii pomiarowej i sterującej siłowniki są związanymi z sygnałami odpowiednikami czujników. Rodzaje siłowników obejmują hydrauliczne, pneumatyczne, elektryczne, mechaniczne i piezoelektryczne. Przetwarzają sygnały lub parametry nastawcze i regulacyjne sterowania na (głównie) pracę mechaniczną. Prostym przykładem tego jest otwieranie i zamykanie zaworu, na przykład w systemie grzewczym lub w przypadku sterowania silnikiem. Wyprowadzenie sygnałów optycznych (poprzez wyświetlacze) lub akustycznych może być również podpięte pod elementy wykonawcze, ponieważ mogą one wywołać

efekt w rzeczywistym środowisku. W robotyce termin efektor jest często używany jako odpowiednik dla siłowników. Efektory pozwalają robotowi chwytać i manipulować przedmiotami, a tym samym wytwarzać efekt. W skomputeryzowanym świecie rzeczy aktuatory odgrywają coraz ważniejszą rolę w realizacji działań i efektów jako odpowiednik (wcześniej) wykrywanych sensorycznie odpowiednich kontekstów. Siłowniki są kluczowym elementem w nowszym postrzeganiu „Czwartej Rewolucji Przemysłowej" w produkcji jako postulatu konceptualizacji Przemysłu 4.0.

Zasilacz

Chociaż wiele technologii jest już dostępnych na rynku lub przynajmniej zostało przetestowanych w kontekstach badawczych, nierozwiązane problemy techniczne pozostają. Bardzo ograniczającym czynnikiem mobilności inteligentnych obiektów jest ich zaopatrzenie w energię. Chociaż baterie stają się coraz mniejsze i wydajniejsze, dzisiejsze urządzenia mobilne wciąż mają bardzo ograniczoną pojemność baterii. Intensywne badania nad ulepszonymi technologiami akumulatorów przyniosły stosunkowo niewielki postęp w wydajności akumulatorów. W rzeczywistości stale pozostaje w tyle za innymi istotnymi osiągnięciami technologicznymi. Niektórzy twierdzą, że wkrótce będzie (lub nawet istnieje dzisiaj, jak mogą świadczyć wstępne doniesienia o spalaniu smartfonów) osiągnięty limit, przy którym gęstość energii stanie się tak wysoka, że poszczególne urządzenia staną się poważnym zagrożeniem dla bezpieczeństwa. Aby przeciwdziałać tym wyzwaniom, prowadzi się kilka badań, w tym inteligentne projekty, które wymagają mniejszej mocy baterii. Można to osiągnąć, odchodząc od idei, że wszystko musi być cały czas online. Czasami wystarczy tylko sporadycznie wiedzieć o zmianie statusu obiektu. Można to komunikować przy znacznie mniejszym względnym wysiłku i zapotrzebowaniu na przepustowość i energię. Inną strategią jest zbieranie energii „w locie". Rozwój technologii wykorzystania alternatywnych źródeł energii, takich jak słońce, wiatr i woda, postępuje bardzo szybko, częściowo z powodu nacisków politycznych. Byliśmy już świadkami tego typu integracji z urządzeniami przenośnymi, np. smartfonami z panelem słonecznym. komórki. Ponadto znane są już podejścia do pozyskiwania energii z zewnętrznych źródeł energii słonecznej, termicznej, piezoelektrycznej, mechanicznej i kinetycznej, określane mianem pozyskiwania energii. Podejścia te są szczególnie odpowiednie (ze względu na ich niezależność od infrastruktury stacjonarnej) do zasilania urządzeń mobilnych i autonomicznych, takich jak węzły czujnikowe. Obiecującym pomysłem na osobiście używane urządzenia mobilne jest wykorzystanie energii, którą człowiek naturalnie wytwarza i emituje. Poprzez ruch i metabolizm (ciepło) człowiek zużywa kilka kilowatogodzin (ciepło i moc ruchu). Jednocześnie można wygenerować i zmagazynować od kilkuset do nawet 1000 W, co teoretycznie mogłoby generować moc wystarczającą do pracy notebooka. Możliwe jest również wytwarzanie energii z glukozy we krwi lub innych potencjałów energetycznych, takich jak poziom pH płynów ustrojowych. W rzeczywistości jednak tylko ułamek z tego jest obecnie dostępny, jeśli w ogóle, a upośledzenie nałożone przez wymagane urządzenia na użytkownika może, w niektórych przypadkach, być nadal zbyt duże. Inne innowacyjne podejścia to ogniwa biopaliwowe, które współpracują z bakteriami. Dzięki produktom rozkładu bakterii energia może być wytwarzana z substancji organicznych. Zastosowaniem tego jest instalowanie ogniw biopaliwowych w oczyszczalniach ścieków i oczyszczalniach ścieków, w których obecne są duże ilości wysokoenergetycznych substancji organicznych.

Identyfikacja

Ważną przesłanką powiązania informacji z realnymi podmiotami w naszym otoczeniu jest jednoznaczna identyfikacja rzeczy i osób. Ogólny termin „technologie automatycznej identyfikacji (Auto-ID) i mobilności (AIM) opisuje zróżnicowaną rodzinę technologii, które mają wspólny cel, jakim jest identyfikowanie, śledzenie, rejestrowanie, przechowywanie i przekazywanie podstawowych danych biznesowych, osobistych i produktowych. Istnieje kilka technologii identyfikacji, na przykład

biometria, kody kreskowe i RFID. Zastosowania RFID, znane od lat 60., stały się szczególnie katalizatorem scenariuszy IoT.

Identyfikacja częstotliwości radiowej

Systemy identyfikacji radiowej wykorzystują małe, tak zwane znaczniki z wbudowanymi mikroczipami, które zazwyczaj zawierają niewielką ilość pamięci komputera i przesyłają swoją zawartość za pomocą sygnałów radiowych na niewielką odległość do określonych czytników RFID. Czytnik przechwytuje te dane, dekoduje je i wysyła do komputera hosta w celu dalszego przetwarzania za pośrednictwem sieci przewodowej lub bezprzewodowej. W rzeczywistości tagi RFID można uznać za elektroniczne kody kreskowe. Jednak w przeciwieństwie do kodów kreskowych, tagi RFID nie wymagają kontaktu wzrokowego w celu ich odczytania. Czytnik RFID składa się z anteny oraz nadajnika radiowego z funkcją dekodowania i mocowany jest do urządzenia stacjonarnego lub przenośnego. W zależności od mocy wyjściowej, częstotliwości radiowej oraz warunków otoczenia czytnik emituje fale radiowe w zakresie od 2,5 cm do 30m. Jeżeli pasywny tag RFID osiągnie zasięg czytnika, tag jest aktywowany i zaczyna przesyłać dane, czyli wcześniej nagrany numer(y) w tagu. W przypadku aktywnych tagów, które są zasilane bateryjnie, sam tag jest w stanie przesyłać dane. Ponieważ tagi RFID mogą przechowywać (unikalny) numer i mogą być fizycznie przymocowane do obiektu, obiekt jest automatycznie i bezdotykowo identyfikowany. Ze względu na te główne funkcje, RFID jest uważane za kluczową technologię, ponieważ łączy świat fizyczny i wirtualny, co oznacza, że obiekty fizyczne stają się jednoznacznie identyfikowalne. Zarządzanie materiałami i zarządzanie łańcuchem dostaw, systemy RFID mogą rejestrować i zarządzać bardziej szczegółowymi informacjami o określonych pozycjach w magazynach lub na produkcji znacznie lepiej niż systemy kodów kreskowych. Gdy duża liczba pozycji jest wysyłana razem, systemy RFID śledzą każdą paletę, partię lub pojedynczy element w dostawie. Ponadto liczba punktów do czytania jest technicznie nieograniczona. Gdy istnieje więcej punktów do czytania, producenci mogą lepiej śledzić cykl życia każdego produktu, mając na celu zrozumienie braków i sukcesów produktu. Innym przykładem są książki w bibliotekach, które wykorzystują chip RFID, aby umożliwić użytkownikom, za pomocą systemów odczytu RFID, wypożyczanie i zwracanie książek bez innej pomocy. W ten sposób unika się ograniczeń godzin pracy i oczekiwania w kolejkach. RFID jest dostępne od dziesięcioleci, ale powszechne stosowanie tagów było opóźnione, o ile koszt każdego tagu wahał się od 1 do 20 euro. Obecnie najprostsze tagi – kupowane w dużych ilościach – kosztują mniej niż 0,10 euro i prawdopodobnie tylko kilka lat będzie kosztować mniej niż 0,01 euro. Dzięki temu dramatycznemu obniżeniu kosztów tagów technologia RFID stała się opłacalna w wielu innych zastosowaniach. W szczególności wdrożenie dużej liczby tagów stało się ekonomicznie wykonalne, nawet w przypadku przedmiotów o niskiej wartości. Jednak czynniki kosztowe systemu RFID obejmują również instalację czytników RFID i systemów tagowania. Ponadto firmy prawdopodobnie będą musiały zmodernizować swoje systemy sprzętowe i programowe w celu przetwarzania ogromnych ilości danych generowanych przez systemy RFID. W rzeczywistości monitorowane transakcje mogą z łatwością sumować się do setek terabajtów. Aby filtrować, gromadzić i zapobiegać przeciążaniu sieci korporacyjnych i aplikacji systemowych przez dane RFID, wymagane jest specjalne oprogramowanie pośredniczące. Aplikacje muszą zostać przeprojektowane, aby pomieścić ogromne ilości danych generowanych przez RFID, a także udostępniać dane innym aplikacjom. Duzi dostawcy oprogramowania dla przedsiębiorstw, w tym SAP i Oracle, oferują wersje swoich aplikacji do zarządzania łańcuchem dostaw z obsługą RFID. Moc RFID dla IoT jest wzmacniana, gdy jest używana razem ze schematami adresowania, w szczególności z elektronicznym kodem produktu.

Schematy adresowania oparte na IPv6 i elektronicznym kodzie produktu

Schematy adresowania stały się kluczowym zadaniem w identyfikacji rzeczy. Wyzwaniem w scenariuszu IoT jest unikalna identyfikacja miliardów urządzeń i, w przypadku wielu scenariuszy aplikacji, również ich kontrolowanie. Najważniejsze wyzwania techniczne to unikalność, niezawodność, trwałość i skalowalność. Protokół internetowy w wersji 6 (IPv6) i elektroniczny kod produktu są ważnymi elementami konstrukcyjnymi IoT. IPv6 to najnowsza wersja protokołu internetowego (IP), który jest protokołem komunikacyjnym, który zapewnia system identyfikacji i lokalizacji komputerów w sieci oraz pomaga kierować ruch w Internecie. Ideą IP jest podłączenie każdego urządzenia do sieci przy jednoczesnym przypisaniu unikalnego adresu IP w celu identyfikacji i określenia lokalizacji. Wraz z szybkim rozwojem Internetu po komercjalizacji w latach 90. stało się jasne, że do połączenia wszystkich urządzeń potrzeba znacznie więcej adresów niż jego poprzednik - IPv4. Pod koniec lat 90. grupa zadaniowa ds. inżynierii internetowej (IETF) sformalizowała następny protokół, czyli IPv6. IPv6 używa 128-bitowego adresu, teoretycznie dopuszczając 2128, czyli około 3,4 × 1038 adresów. Innymi słowy, całkowita liczba możliwych adresów IPv6 jest ponad 7,9 × 1028 razy większa niż IPv4, który wykorzystuje adresy 32-bitowe i zapewnia około 4,3 miliarda adresów. Wydawało się, że jest to więcej niż wystarczające, aby przypisać unikalny adres dowolnej liczbie istniejących lub przeznaczonych do zbudowania obiektów stworzonych przez człowieka. IPv6 zawiera zarówno bogaty schemat adresowania, jak i wiele zaawansowanych funkcji (do dynamicznego zarządzania adresami, inteligentnego routingu itp.), co zwiększa tak zwany narzut protokołu i sprawia, że IPv6 jest stosunkowo ciężkim protokołem. Ponadto IPv6 nie pasuje dobrze, zwłaszcza w przypadku scenariuszy aplikacji WSN, które mogą koordynować bardzo dużą liczbę czujników sieciowych i nie wymagałyby wszystkich funkcji sieciowych, które są dostarczane z protokołem IP. Jednak nie wszystkie warstwy typowego WSN zwykle działają w ramach ustalonego stosu IP i dlatego nie mogą korzystać ze schematu adresowania zapewnianego przez IPv6. Wymaga to dodatkowej warstwy podsieci lub opracowania lekkiej formy IPv6 (np. 6LoWPAN), które są lepiej dostosowane do scenariuszy IoT. Centrum Auto-ID w MIT (obecnie Auto-ID Labs, międzynarodowa sieć badawcza) oraz społeczność programistów wokół RFID odegrały kluczową rolę w konceptualizacji i identyfikacji potrzebnych wysiłków standaryzacyjnych. Główną ideą jest odkrycie informacji o obiekcie oznaczonym (RFID) poprzez przeglądanie adresu internetowego lub wpisu w bazie danych odpowiadającego konkretnemu kodowi zapisanemu w tagu RFID. Pracowali nad opracowaniem elektronicznego kodu produktu (EPC), czyli uniwersalnego identyfikatora, który zapewnia niepowtarzalną tożsamość dla każdego obiektu fizycznego przez cały czas. Obecnie koncepcje są bardziej ogólne i nie ograniczają się tylko do RFID. Rzeczą może być dowolny rzeczywisty/fizyczny przedmiot, ale także wirtualna/cyfrowa jednostka, która porusza się w czasie i przestrzeni i może być jednoznacznie identyfikowana przez przypisane numery identyfikacyjne, nazwy i/lub adresy lokalizacji. W przypadku obiektów wirtualnych odpowiednimi pojęciami są jednolite identyfikatory zasobów (URI) i adresy IP, które umożliwiają identyfikację i wykrywanie obecności obiektu w sieci. W oparciu o ugruntowany system nazw domen (DNS), w kontekście IoT, adresy IP mogą być również wykorzystywane jako identyfikatory obiektów sieciowych wraz z etykietami nazw. Główną ideą jest rozszerzenie istniejących interfejsów programowania i formatów DNS na małe sieci, w których nie ma dostępnych serwerów nazw. Jedną z kluczowych koncepcji jest multiemisja systemu nazw domen (mDNS), która zamienia nazwy hostów na adresy IP w małych sieciach, które nie zawierają lokalnego serwera nazw

Lokalizacja

Poza identyfikacją, pozycja przedmiotu lub człowieka jest istotną informacją kontekstową. Do określania pozycji można zastosować techniki lokalizacji, które albo lokalizują obiekt na zewnątrz, albo za pomocą których obiekt sam określa swoją pozycję. Przykładami „globalnych" systemów pozycjonowania są globalny system pozycjonowania (GPS) Stanów Zjednoczonych, GLONASS (Rosja), Galileo (Unia Europejska) i BeiDou (Chiny). Rozróżnia się cztery typy. W trilateracji odległości są

mierzone do co najmniej trzech punktów, których położenie jest znane, a do określenia położenia używa się przecięcia geometrycznego. Można to przeprowadzić w sieciach po prostu za pomocą czasów propagacji przesyłanych sygnałów. Podobnie istnieje triangulacja, w której do obliczania odległości i położenia wykorzystuje się kąty lub wymiary kierunkowe. Z drugiej strony pozycja jest mierzona z określeniem otoczenia za pomocą następnego znanego punktu. Ta metoda jest już dziś wykorzystywana w lokalizacji radiotelefonów komórkowych w sieciach GSM przez przypisanie do komórki radiotelefonu ruchomego. Inna technika, analiza sceny, określa pozycję na podstawie określonych cech punktu widzenia (tzw. footprint). Te cechy mogą być rzeczywistymi obrazami krajobrazu z odpowiedniego kąta patrzenia lub mogą być przechowywane wcześniej w tabeli z określonymi zmierzonymi wartościami punktu widzenia, na przykład wartościami elektromagnetycznymi lub specyfikacjami promieniowania w jednej lub kilku obecnych sieciach WLAN. Wyzwania w procedurach lokalizacyjnych to śledzenie poruszających się obiektów i obsługa obiektów zakrytych lub znajdujących się w pomieszczeniach (problem z pozycjonowaniem GPS) lub promieniowanie i fałszowanie fal radiowych. Jednak w ostatnich latach wiele wysiłku włożono w technologie lokalizacji wewnętrznej

Przetwarzanie w chmurze i przetwarzanie we mgle

Duża i rosnąca liczba urządzeń IoT doprowadzi do szybkiego wzrostu gromadzonych danych. Często takie dane mają związek urządzenie - czas - przestrzeń (tj. dane czasu i pozycji, które ściśle odnoszą się do konkretnego urządzenia). W scenariuszach IoT prawdopodobne jest, że takie dane są współużytkowane przez kilka aplikacji, co wymaga większej interoperacyjności. Co więcej, dodatkowe wymiary obiektów mogą być interesujące, w tym różne typy danych z czujników lub metadanych dotyczących obiektu. Stwarza to nowe problemy z zarządzaniem danymi i może zmienić dominujący sposób przetwarzania. W szczególności przetwarzanie może odejść od poprzednio „offline" lub trybu wsadowego, w którym przechowywanie i zapytania, a także przetwarzanie i transakcje mogą odbywać się z pewnym opóźnieniem bez negatywnego wpływu na aplikacje lub usługi w kierunku bardziej „online" lub w czasie rzeczywistym , gdzie gromadzenie, przetwarzanie i działanie na danych może nie powodować większych opóźnień. Oprócz potrzeb związanych z „przetwarzaniem w czasie rzeczywistym" archiwizacja danych za pomocą inteligentnych zasad destylacji, indeksowania i celowego usuwania danych w wydajny sposób nadal stanowi poważne wyzwanie. Istnieje kilka alternatywnych rozwiązań, w tym podejścia centralne, zdecentralizowane lub zorientowane na dane magazyny, które znajdują się jak najbliżej jego punktów produkcyjnych lub - jako rodzaj mieszanki - dynamicznie dostosowują pozycję przechowywania danych do określonych warunków. Aby sprostać wyzwaniom związanym z zarządzaniem danymi32, przetwarzanie w chmurze i mgła jest jednym z najważniejszych podejść do radzenia sobie z problemami zarządzania danymi IoT. Przetwarzanie w chmurze to koncepcja, w której wydajność obliczeniowa, pamięć masowa, oprogramowanie i inne usługi są dostarczane jako grupa zwirtualizowanych zasobów w sieci, głównie w Internecie. Oprócz tego „chmurę" zasobów można uzyskać w dowolnym momencie z dowolnego podłączonego urządzenia i witryny. Zazwyczaj użytkownicy automatycznie otrzymują zasoby w chmurze, takie jak czas serwera lub pamięć sieciowa, bez konieczności dalszych negocjacji z usługodawcą w trybie „samoobsługi na żądanie" i w sposób „elastyczny". Ma to ogromną wartość dla użytkownika, który nie musi posiadać dostępnych zasobów nawet w przypadku dużego zapotrzebowania. Zasoby te, aw szczególności zarządzanie skalowaniem w górę i w dół, są delegowane na dostawcę usług w chmurze. Najczęściej usługi w chmurze są usługą mierzoną: opłaty za zasoby w chmurze są oparte na rzeczywistych zasobach . Przetwarzanie w chmurze jest postrzegane jako główny element scenariuszy Ubicomp w celu sprostania wyzwaniom wydajnego, bezpiecznego, skalowalnego i zorientowanego rynkowo przetwarzania i przechowywania danych. Zasadniczo przetwarzanie w chmurze osiąga doskonałe wyniki w zakresie zasobów sieciowych oraz przechowywania i uzyskiwania dostępu do

danych związanych lub pochodzących z połączonych rzeczy. Jednak w odniesieniu do aplikacji wrażliwych na opóźnienia, które wymagają węzłów w pobliżu, aby sprostać ich opóźnieniom wymagań, przetwarzanie w chmurze może mieć pewne ograniczenia – zwłaszcza gdy miliony urządzeń mają być obsługiwane w sposób krytyczny czasowo. Mogą pojawić się nowe przypadki użycia, które wymagają ścisłej kontroli fizycznie rozproszonych, ale specjalnie zlokalizowanych czujników lub elementów wykonawczych (np. zakład z maszynami, które muszą reagować na nagłe zmiany w środowisku lub procesie produkcyjnym). W odpowiedzi na te wyzwania proponuje się paradygmat przetwarzania mgły (zwany także „przetwarzaniem brzegowym"), który nie powinien zastępować paradygmatu przetwarzania w chmurze, ale go rozszerzać. Przetwarzanie mgły, jako wysoce zwirtualizowana platforma, zapewnia usługi obliczeniowe, przechowywania i sieciowe między urządzeniami końcowymi a tradycyjnymi centrami przetwarzania danych w chmurze, które są zazwyczaj, ale nie tylko, zlokalizowane na obrzeżach sieci. Jednak skupienie się bardziej na „brzegu sieci" implikuje szereg cech, które sprawiają, że przetwarzanie we mgle jest nietrywialnym rozszerzeniem przetwarzania w chmurze. Oczekuje się, że obliczenia mgły będą na przykład radzić sobie z szeroko rozpowszechnionymi i mobilnymi wdrożeniami, w których zaangażowana jest bardzo duża liczba węzłów, na przykład szybko poruszające się i duże grupy pojazdów wzdłuż autostrad lub wielkoskalowe sieci czujników monitorujące środowisko) . Od momentu powstania koncepcji, zaledwie kilka lat temu, obliczenia mgły cieszą się niezwykłym zainteresowaniem w środowisku akademickim i przemysłowym

Pochodne cechy nowoczesnych technologii informacyjno-komunikacyjnych

Nowoczesna infrastruktura technologii informacyjno-komunikacyjnych zapewnia następujące cechy: świadomość kontekstu, zdolność adaptacji, proaktywność, wysoka jakość danych i intuicyjna interakcja.

Świadomość kontekstu, zdolność adaptacji i proaktywność

Świadomość kontekstu (również kontekst zależności) to zachowanie, które zależy od informacji o kontekście dowolnego podmiotu (programów, ludzi, obiektów). Informacje o kontekstach można uzyskać z wielu różnych źródeł, w szczególności za pośrednictwem czujników. Informacje te służą do wyciągania wniosków na temat kontekstu i odpowiedniego dostosowania zachowania. Wykorzystanie informacji kontekstowych jest najczęściej związane z aspektami czasu i lokalizacji, w tym ostatnim przypadku określane jako usługi lokalizacyjne. Jednak wszelkie dalsze aspekty mogą być zawarte w modelu kontekstowym, jeśli istnieją odpowiednie źródła informacji lub czujniki. Mogą to być na przykład dane archiwalne lub dane biometryczne, temperatura w środowisku lub relacje między ludźmi. Wrażliwość na kontekst pozwala na adaptację i proaktywność. Jest jeszcze mniej inwazyjny i destrukcyjny, gdy usługi i funkcje dostarczane przez inteligentne środowiska dostosowują się do kontekstu i są proaktywnie oferowane poza inteligentnym środowiskiem. Obecnie stopień dostosowania konwencjonalnych komputerów i telefonów komórkowych jest bardzo niski. Zwyczajowe są dostosowania do warunków regionalnych, takich jak ustawienia języka i czasu. Oczekuje się, że w przyszłości zostanie wykorzystanych więcej informacji kontekstowych, a ustawienia i usługi urządzenia będą się automatycznie odpowiednio dostosowywać, takie jak pozycja użytkownika, jego stan zdrowia lub stan emocjonalny, jego plany, zadania do wykonania, oraz inne czynniki w środowisku, które wpływają na użytkownika. Proaktywność łączy w sobie adaptacyjność aplikacji w tle oraz przewidywaną interakcję wyznaczonego użytkownika z oferowaną usługą. Usługi są automatycznie oferowane użytkownikowi w idealnym przypadku, gdziekolwiek i kiedykolwiek są potrzebne. Inicjatorem jest samo inteligentne środowisko, a nie potencjalny użytkownik. Ta jakość pociąga za sobą główne wymaganie: inteligentne środowisko musi być w stanie prawidłowo rozpoznać kontekst i intencje użytkownika. Wątpliwe jest, czy można to osiągnąć niezawodnie również w złożonych sytuacjach. Prosty przykład pokazuje tylko jedną z trudności w niezawodnym wdrożeniu: Jeśli osoba

padnie nieświadomie na ziemię, przydatne jest automatyczne wysłanie wezwania alarmowego, ale ten przypadek różni się od „podobnych" zdarzeń, na przykład gdy osoba spada nagle i celowo na kanapę, aby odpocząć. Rozpoznanie sytuacji i „właściwego" kontekstu (świadomość kontekstu) jest jednym z podstawowych wyzwań realizacji skomputeryzowanego świata.

Zwiększona jakość danych

Poprawa dostępności danych w ujęciu ilościowym („wiemy więcej o stanie rzeczy lub związanym z nią procesie") i jakości („wiemy więcej szczegółów na ten temat") może stanowić najbardziej oczywistą zmianę wynikającą z wszechobecnego gromadzenia informacji głównie za pomocą sensorów. dane o rzeczach ogólnie mają fundamentalne znaczenie dla wszelkich ulepszeń związanych z produktami, procesami i modelami biznesowymi. W kolejnych rozdziałach zostaną wyodrębnione cztery wymiary (poprawy) jakości danych i jej efekty, czyli efekt substytucji i elastyczności.

Wymiary jakości danych

Platformy IoT pozwalają na podniesienie jakości danych przy mniej więcej tym samym koszcie iw prostszy sposób niż dotychczas. Ulepszenia te można opisać czterema wymiarami jakości danych.

1) Szczegółowość i typ obiektu. Spadające koszty sprzętu i miniaturyzacja upraszczają wykorzystanie komponentów technicznych na poszczególnych obiektach przy niższych kosztach. Granularność odnosi się do liczby obiektów grupy lub klasy, za pomocą których agregowane są informacje. Dzięki pewnym koncepcjom, takim jak przetwarzanie wszechobecne, można pozyskiwać szczegółowe dane dotyczące osób, a nawet bardzo małych obiektów. Obecnie kontenery i palety są śledzone na trasach dostaw za pomocą RFID i GPS. Wkrótce pozyskiwanie danych dla każdego z produktów na paletach, w tym małego elementu, takiego jak kubek po jogurcie, staje się przystępne. Oznacza to, że wszystkie rodzaje obiektów, w tym produkty o małej wartości i krótkim okresie życia, są również rejestrowane w granicach ekonomicznych.

2) Szczegółowość czasu. Wydajna transmisja danych i sieci bezprzewodowe w inteligentnych środowiskach umożliwiają proste, ciągłe gromadzenie danych w czasie rzeczywistym. Chociaż w wielu firmach inwentaryzacja jest nadal przeprowadzana okresowo i ręcznie, może być prowadzona w sposób ciągły i automatyczny dzięki systemowi RFID. Oznacza to, że w każdej chwili można wywołać aktualne dane inwentaryzacyjne, a zmiany można przeglądać w czasie rzeczywistym lub bardzo szybko. Jednak zbieranie danych w czasie rzeczywistym jest problematyczne, na przykład w przypadku lotów, w których transmisja danych może zakłócać ruch lotniczy, gdy obiekty poruszają się bardzo szybko lub istotne cechy otoczenia zmieniają się bardzo szybko.

3) Zawartość danych. RFID to opłacalna, sprawdzona technologia do bezdotykowej identyfikacji pojedynczych obiektów. Oferuje kilka zalet w porównaniu z konwencjonalnymi kodami kreskowymi i identyfikatorami seryjnymi, które można odczytać tylko poprzez kontakt wzrokowy. Dzięki RFID indywidualny identyfikator może być jednocześnie połączony z obiektem zarówno fizycznie, jak i cyfrowo. EPC to taki unikalny identyfikator. W zależności od typu tagu, na tagu RFID mogą zostać zapisane dodatkowe dane, takie jak data produkcji i miejsce produkcji. Jednak przestrzeń dyskowa jest zwykle ograniczona do kilku kilobajtów. Dopiero wykorzystanie dodatkowych magazynów danych i czujników na obiekcie i w środowisku pozwala na uzyskanie bardziej kompleksowych danych obiektowych lub kontekstowych.

4) Osiągnij. Zasięg wymiarów jest mniej zależny od technologii niż od koncepcji aplikacji. Dzięki sieci integracja aplikacji i systemów informatycznych jest ogólnie możliwa w całej firmie lub w sposób międzyorganizacyjny. Jednak kluczowe dla powodzenia wdrożeń są porozumienia kooperacyjne i

porozumienia dotyczące standardów. W zarządzaniu łańcuchem dostaw szczególnie rozpowszechnione są standardy danych, takie jak EAN i EPC z GS1. Inne standardy, takie jak XML, standardy sieci semantycznej i usługi sieci Web, ułatwiają wdrażanie tych aplikacji.

Skutki zwiększonej jakości danych

Wyposażenie infrastruktury w czujniki i elementy wykonawcze ma dwa skutki. Po pierwsze, występuje efekt substytucji. Konwencjonalne zbieranie i odzyskiwanie danych (np. ręczne lub kod kreskowy) jest zautomatyzowane i unika się nieciągłości mediów. Po drugie, istnieje efekt elastyczności. Ponadto można teraz zbierać i wykorzystywać nowe dane. W rezultacie firmy mogą mapować informacje ze świata rzeczywistego w czasie rzeczywistym, a tym samym wykorzystywać je do bezpośredniej kontroli procesów i działań. Pozwala to na cyfryzację systemów zarządzania i prowadzi do lepszego podejmowania decyzji. Biznes może z łatwością zebrać więcej danych i wzbogacić istniejące kolekcje z nową jakością danych. Dane mogą być również wykorzystywane do wyzwalaczy i funkcji alarmowych dla określonych zdarzeń, na przykład, jeśli transport dostawczy utknął w dużym natężeniu ruchu. Jeżeli koncepcja ta zostanie wdrożona wspólnie z partnerami biznesowymi i przeniesiona do zintegrowanego systemu informatycznego, można wdrożyć tzw. zarządzanie łańcuchem dostaw sterowane zdarzeniami. Ponadto zautomatyzowane procesy prowadzą do niezależnego monitorowania i kontroli, na przykład w procesach produkcyjnych. Dzięki bardzo wysokiej jakości danych, w szczególności wysokiej ziarnistości czasowej, kontrola procesów firmy w czasie rzeczywistym może być realizowana na podstawie automatycznie rejestrowanych danych, które są bezpośrednio dostępne do zarządzania za pośrednictwem szybkich połączeń sieciowych, niezależnie od tego, gdzie decydenci chciałby je odzyskać. Kluczowe jest rozważenie, czy dane w czasie rzeczywistym są rzeczywiście wymagane dla wszystkich procesów i zadań, czy też podsumowywanie danych w większych cyklach raportowania jest już wystarczająco odpowiednie.

Intuicyjna interakcja

Technologia znika, osadzając ją w środowisku fizycznym, tak że nie jest już dostrzegalna. To sprawia, że jeszcze bardziej konieczne jest, aby funkcjonalność i funkcjonalność pozostały rozpoznawalne dla użytkownika. Można to nazwać „dylematem niewidzialności". Rozwiązaniem tego dylematu jest projekt intuicyjnej interakcji człowiek-komputer. Kluczową koncepcją jest niejawne wykorzystanie systemów informacyjnych. Działa jak automatyczne drzwi przesuwne, które otwierają się, gdy tylko ktoś się zbliży, bez wyraźnego polecenia. Wykorzystywane są na przykład naturalne zachowania ludzi, które można rozpoznać np. po języku, spojrzeniach, mimice, ruchach.

Potencjał innowacji w zakresie produktów, procesów i modeli biznesowych

Możliwości innowacji produktów, procesów i modeli biznesowych tkwią w dwóch obszarach: (i) innowacje w ramach ekosystemu IoT; oraz (ii) innowacje oparte na ekosystemie IoT. Skupiamy się tutaj na tym ostatnim. Przedstawione cechy nowoczesnej infrastruktury teleinformatycznej, a także zbieżność inteligentnych obiektów i inteligentnych środowisk, oferują duży potencjał dla innowacji w prawie każdej dziedzinie. Wynika to głównie z nowych lub wzbogaconych „cech", które zapewnia skomputeryzowana infrastruktura. Firmy mogą opracowywać nowe lub ulepszone procesy lub produkty (w tym usługi) w celu uzyskania przewagi nad konkurencją. Istniejące modele biznesowe również mogą ulec zmianie. Jak jednak firmy mogą tworzyć takie innowacje? W przypadku rozwoju aplikacji można określić dwa podejścia: innowacje inicjowane przez problem oraz innowacje oparte na technologii. W przypadku innowacji zainicjowanych problemami nowe technologie są opracowywane lub wykorzystywane w sposób ukierunkowany w celu rozwiązania konkretnego problemu. Prowadzi to często do stopniowych innowacji, które początkowo zwiększają wydajność istniejących procesów biznesowych, produktów lub usług. W swoim przełomowym artykule March mówi o „wyzysku".

Innowacje te są zwykle wywoływane przez użytkownika, który wyraża chęć ulepszeń. Dzięki IoT można ulepszyć procesy kontroli i przetwarzania informacji. Dzięki wykorzystaniu RFID, czujników i procedur lokalizacyjnych łańcuchy dostaw można zautomatyzować i kontrolować w czasie rzeczywistym. Pozwala to uniknąć lub zmniejszyć koszty z powodu nieoczekiwanych zakłóceń. Ponadto można poprawić ochronę przed kradzieżą i zwiększyć środki zapobiegające podrabianiu. Innowacje oparte na technologii mają czasem radykalny charakter, ponieważ pomagają rozwiązywać istniejące problemy w zupełnie nowy sposób. Jeśli chodzi o marzec , wysoko cytowany badacz zarządzania technologią, jest to oznaczone jako „Eksploracja". W typowym przypadku programista (wynalazca) lub ekspert w danej technologii ma pomysł, jak ją w wartościowy sposób wykorzystać. Koncentruje się na szczególnych cechach technologii. Przedstawiono już cechy inteligentnych środowisk. W rezultacie można opracować nowe usługi i produkty, które oferują klientom wartość dodaną w stosunku do starych i porównywalnych produktów. Dzięki IoT można oferować skomputeryzowane produkty i usługi kontekstowe. Ponieważ innowacja oparta na technologii nie pochodzi od użytkownika, istnieje niebezpieczeństwo, że nie spełni ona potrzeb użytkownika. Dlatego użytkownicy powinni być jak najwcześniej włączani w proces innowacji. Jeśli innowacje są dostosowane do rzeczywistych potrzeb ich użytkowników, procesy biznesowe i produkty można nie tylko ulepszać, ale także wprowadzać fundamentalne innowacje. Siłę innowacji można zilustrować trzema kategoriami: (i) nowe produkty; (ii) nowe procesy; oraz (iii) nowe modele biznesowe.

Innowacja produktowa

Większość tradycyjnych produktów może stać się inteligentnymi przedmiotami poprzez wzbogacenie ich o technologię informacyjną. Następnie produkty mogą przechowywać informacje o całym cyklu życia produktu od wytworzenia do utylizacji i ewentualnie wymieniać je z innymi produktami, inteligentnymi środowiskami lub użytkownikami. Wyposażone w odpowiednie procesory i program sterujący, mogą nawet dostosowywać swoje zachowanie do określonych kontekstów lub uruchamiać autonomiczne działania. Prawdziwym przykładem są patelnie, które wczytują przepisy za pomocą RFID i przygotowują żywność o określonej temperaturze i czasie gotowania. W tym celu mogą komunikować się z piecem (który musi mieć odpowiednie, skoordynowane standardy komunikacyjne) i regulować stopień nagrzania. Nowe produkty i powiązane usługi o wartości dodanej korzystają z danych o większej szczegółowości

Innowacje procesowe

W połączeniu z nowatorskimi infrastrukturami technologii informacyjno-komunikacyjnych, które osiągają bezprecedensowy poziom jakości danych, procesy mogą być dokładniej rejestrowane i oceniane, a także przetwarzane szybciej oraz w bardziej zintegrowany i zautomatyzowany sposób. Ponadto osiągnięcia te można zdobyć w skrajnych przypadkach w czasie zbliżonym do rzeczywistego lub w czasie rzeczywistym. Wiele procesów korzysta z informacji kontekstowych. Kluczowym czynnikiem dla ulepszonych procesów są ulepszone dane lub dane, które zostały poddane destylacji do bardziej znaczących informacji. Wszechobecności gromadzenia i prezentacji informacji towarzyszy zmniejszenie liczby i rozmiarów nieciągłości medialnych między światem wirtualnym a rzeczywistym. Zamyka to przepaść między światem realnym a wirtualnym. Otwiera to również drogę do lepszej automatyzacji i integracji. Gdy dane są wprowadzane do systemu ręcznie za pomocą klawiatury, błędy mogą wystąpić przy każdej nieciągłości mediów; poza innym problemem upłynie ten czas, zanim dane zostaną zapisane i gotowe do dalszego przetwarzania. Podejściem technicznym jest kodowanie danych za pomocą kodów kreskowych. Pomysł ten pojawił się po raz pierwszy w latach 30. XX wieku. Następcami pierwszych, jednowymiarowych kodów kreskowych są kody dwuwymiarowe, zwane również kodami 2D. Informacje są przechowywane nie tylko na jednej osi, ale w pionie i poziomie. Istnieje wiele schematów kodowania, z których jednym z najbardziej znanych jest „kod QR" – kod

szybkiej odpowiedzi. Akceptacja kolejnych wymiarów (kolor, czas) skutkuje kodem 3D lub 4D, który może również przechowywać więcej informacji w zwarty sposób. Dzięki RFID nieciągłości mediów są znacznie zredukowane, a dane są natychmiast przesyłane do podłączonego systemu zaplecza po bezdotykowym wykryciu. To samo dotyczy danych z węzłów czujników bezprzewodowych. Pozyskiwanie, przetwarzanie i dystrybucja danych są zautomatyzowane w skomputeryzowanym świecie, co oznacza, że nie jest już wymagana interwencja człowieka. Jednak punkty interwencyjne, na przykład do konfiguracji, późniejszej kontroli lub w przypadku awarii, powinny być nadal dostępne. Dzięki automatycznej transmisji danych między obiektami sieciowymi i środowiskami można wdrożyć beznośną integrację aplikacji i systemów przedsiębiorstwa. Oznacza to, że dane są przekazywane do autoryzowanych systemów według zdefiniowanych reguł i tam przetwarzane zgodnie z aplikacją. Warunkiem tego są jednolite formaty danych i zasady komunikacji (protokoły). Innymi słowy, systemy muszą być zdolne do wzajemnego zrozumienia. Na przykład, które dane kontekstowe należą do jakiego obiektu i jak interpretować specjalne wartości pomiarowe czujnika muszą być znane. Jeśli inteligentne obiekty są wyposażone w sztuczną inteligencję, można realizować procesy samokontrolujące. W tym kontekście, na przykład, paczki dostawcze lub produkty „podążają własną drogą do miejsca przeznaczenia" i przekazują informacje produkcyjne do maszyn lub pojazdów transportowych. Te inteligentne obiekty podejmują autonomiczne decyzje i organizują się w sposób zdecentralizowany. Jednym ze sposobów osadzenia tych umiejętności w obiektach są agenci oprogramowania, czyli samoczynnie wykonujący się program, który podejmuje decyzje w oparciu o zasady i wyuczoną wiedzę, które w pewien sposób kontrolują lub wpływają na swoje środowisko za pomocą elementów wykonawczych, dostosowują się do zmian i reagować na oczekiwane i nieoczekiwane zdarzenia.

Innowacje w modelu biznesowym

Modele biznesowe są również zmieniane przez skomputeryzowane światy lub mogą być realizowane tylko za ich pośrednictwem. Na przykład: Firmy mają możliwość przeprojektowania swoich cen dzięki ulepszonej bazie informacji. W ten sposób różne opcje płatności klientów mogłyby być lepiej rozpoznawane dzięki dyskryminacji cenowej. Na przykład w trakcie wykorzystywania poszczególnych kontekstów można dokonać odpowiedniej wyceny. Faktycznym wdrożeniem takich modeli cenowych są taryfy „płać za jazdę" na ubezpieczenie komunikacyjne. Przedsiębiorstwa mogą na nowo zdefiniować istniejące łańcuchy wartości. Jednym z przykładów jest Zipcar, jedna z największych na świecie firm współdzielących samochody. Dostępne samochody lub ich dane pozycyjne są automatycznie przesyłane do centrum kontroli, dzięki czemu członkowie carsharingu mogą szybko identyfikować możliwości jazdy za pośrednictwem interfejsu internetowego. Firma postrzega siebie nie tyle jako wypożyczalnię samochodów, ile jako elastycznego dostawcę usług mobilności. Komputeryzacja codziennego świata może doprowadzić do powstania nowych usług opiekuńczych, na przykład w sektorze zdrowia. Wraz z prezentowanym „inteligentnym domem" osoby wymagające intensywnej opieki mogłyby żyć lepiej i dłużej w znajomym środowisku. Zwłaszcza w dziedzinie komunikacji mobilnej wykorzystywane są już usługi lokalizacyjne, które uwzględniają pozycję użytkownika i na przykład wyświetlają restauracje w obecnym środowisku użytkownika. Kontekstowe usługi obejmują nie tylko informacje o lokalizacji, ale także inne istotne informacje o środowisku i użytkowniku. W inteligentnych środowiskach dane kontekstowe mogą być wykorzystywane do świadczenia usług dostosowanych do sytuacji, użytkownika, jego zadań, życzeń, planów i innych czynników lub reagowania na konkretny kontekst za pomocą znaczących działań lub sugestii. Systemy nawigacyjne, które otrzymują w czasie rzeczywistym informacje o warunkach drogowych i ruchu na docelowej trasie, są w stanie pogodzić te informacje kontekstowe z docelowymi danymi użytkownika, a następnie dokonać elastycznych korekt trasy. Może to również ostrzec kierowcę o zbliżających się krótkotrwałych wypadkach lub nieuchronnym uszkodzeniu opony (jeśli czujniki są zainstalowane w układzie opona/koło samochodu). Ponadto marketing kontekstowy jest dostosowany do klientów, ich

miejsca pobytu i innych czynników kontekstowych, aby jak najmniej losowości powodowały nieodpowiednie kampanie reklamowe, na przykład oferty parasoli, które można kupić w okolicy podczas deszczowa pogoda. Dane osobowe klientów mogą być również wykorzystywane do rozróżniania grup klientów. W przypadku ograniczonych zasobów można przeprowadzić zróżnicowanie usług. Ważni klienci są traktowani preferencyjnie. Indywidualizacja produktów i informacji również tworzy wartość dodaną. Informacje są indywidualnie dopasowywane i dostosowywane, a właściwości produktu dopasowywane do indywidualnych preferencji, dzięki czemu klient może osiągnąć wyższy poziom zadowolenia. Wspomniane przykłady i główny trend polegający na tym, że coraz więcej rzeczy tworzy więcej danych, zaowocowały konceptualizacjami, w tym „zorientowaniem na dane", „konkurowaniem w zakresie analityki", „modelami biznesowymi opartymi na Big Data" i tak dalej. IoT i jego implikacje dla czujników i tworzenia coraz większej ilości danych stanowią nową szansę na kreatywność ukierunkowaną na przekształcenie danych w działania tworzące wartość.

Implikacje i wyzwania

Informatyzacji (codziennego) świata towarzyszą poważne implikacje i wyzwania, które można scharakteryzować jako (i) nowe rynki; (ii) zmienione tworzenie wartości; (iii) zwiększona świadomość przestrzeni informacyjnych; oraz (iv) oraz aspekty społeczne, etyczne, prawne i związane z ryzykiem.

Nowe rynki

Skomputeryzowany świat połączonych rzeczy otwiera drzwi dla innowacji, które ułatwiają nowe interakcje między rzeczami i ludźmi oraz umożliwiają realizację inteligentnych miast, infrastruktury i usług, które obiecują poprawę jakości życia. Do 2025 r. IoT może mieć wpływ gospodarczy w wysokości 11 bilionów dolarów rocznie, co stanowiłoby około 11% światowej gospodarki; i że użytkownicy wdrożą 1 bilion urządzeń IoT. Wiele raportów i białych ksiąg zawiera scenariusze wpływu na szpitale, systemy transportowe, usługi kurierskie, supermarkety, biura i inne obszary życia codziennego. Ilustracyjnym przykładem wpływu skomputeryzowanych światów na nasze codzienne życie jest „inteligentny dom". W inteligentnym domu urządzenia, przedmioty i pomieszczenia są skomputeryzowane i połączone w sieć. Mieszkańcy mogą sterować meblami, takimi jak światła, drzwi, lodówki, zasłony itd., za pomocą pilota, poleceń głosowych lub ruchów rąk. Mogą też za pomocą Internetu sprawdzić, czy w domu wszystko działa dobrze i jest akceptowalne. Inteligentny dom rozpoznaje również czujniki, które wskazują, kiedy ktoś jest w domu i może automatycznie włączyć światło, gdy mieszkaniec wejdzie do ciemnego pokoju. Potrafi także rozpoznawać i przechowywać preferencje mieszkańców. Na przykład w przypadku mieszkańca, który ogląda swój ulubiony serial telewizyjny w każdą sobotę po południu, telewizor jest włączany odpowiednim nadajnikiem lub, jeśli mieszkańca nie ma w domu, sekwencja jest nagrywana automatycznie. Dodatkowo, gdy żywność i związane z nią artykuły są codziennie wykorzystywane, czujnik po sprawdzeniu zawartości lodówki wysyła wiadomość do cyfrowego notatnika w kuchni i umieszcza produkty na liście zakupów, do której każdy z mieszkańców ma dostęp poprzez na przykład smartfon, gdy są w supermarkecie. Bardziej zintegrowane scenariusze mogą uruchomić autonomiczne systemy uzupełniania, składające się z robotów dostarczanych przez strony trzecie, które fizycznie uzupełniają zapasy, na przykład lodówki. Ten i inne scenariusze można rozwijać znacznie dalej. Najważniejsze jest jednak to, że aktorzy w skomputeryzowanym świecie są świadomi potencjalnego wpływu na funkcje o wartości dodanej i rynki. Wynika to w szczególności z faktu, że, jak pokazuje przykładowy scenariusz, w tworzenie wartości dla klienta zaangażowanych jest znacznie więcej podmiotów.

Zmienione tworzenie wartości

Wraz z wyższą jakością danych (jak pokazano powyżej) znaczenie danych i informacji jako źródła tworzenia wartości jest jasne. Można to zobaczyć po prostu obserwując wpływ skomputeryzowanego

świata na tworzenie wartości na różnych poziomach. Na poziomie indywidualnym konsumenci i producenci żyją w skomputeryzowanym świecie. Z jednej strony konsumentom dostarcza się informacje jako dobra konsumpcyjne (w formie usług informacyjnych lub w połączeniu z produktami skomputeryzowanymi), a z drugiej strony jako dane wejściowe do decyzji. Informacje mogą obniżyć koszty wyszukiwania i ułatwić racjonalne działanie, ponieważ decyzje można ważyć dokładniej przy użyciu bardziej trafnych informacji. Z drugiej strony, dla wygody ofert kontekstowych, wymagane jest ujawnienie osobistych preferencji, danych osobowych i potrzeb w zakresie płatności. Oprócz poprawy wydajności i korzyści kosztowych, producenci mogą również skorzystać na zróżnicowaniu, dyskryminacji cenowej i strategiach sprzedaży pakietowej poprzez ulepszenie bazy informacyjnej. Stwarza to ogromny potencjał do zoptymalizowanej eliminacji skłonności konsumenta do płacenia. W przypadku grup osób i organizacji ułatwiona jest koordynacja i kontrola niektórych procesów. Ułatwia to ustalenie miejsca i czynności pracowników. Członkowie organizacji mogą uzyskać ten sam poziom informacji dzięki lepszej sieci. Tworzy to punkty wyjścia do analizy i poprawy koordynacji grupy. Kontrakty w dziedzinie dystrybucji ryzyka i zachęt można uczynić bardziej sprawiedliwymi poprzez wychwytywanie zachowań, których nie dało się jeszcze zaobserwować przy niskich kosztach. Pozwala to na bardziej sprawiedliwy rozkład ryzyka. Przykładami tego są umowy o pracę i umowy ubezpieczeniowe, gwarancje na produkty (np. „Czy klient starannie konserwował swój samochód?") oraz monitorowanie emisji szkodliwych spalin. Na podstawie analiz ekonomicznych można przewidywać wzrost efektywności handlu gospodarczego. Jednym z głównych efektów skomputeryzowanych światów w kontekście tworzenia wartości jest redukcja asymetrii informacji. Na realnych rynkach, opartych na asymetrycznym rozkładzie informacji, mogą wystąpić dwa skutki: niekorzystna selekcja i pokusa nadużycia. Selekcja negatywna występuje, ponieważ niektóre informacje nie są widoczne dla dostawców. W przypadku ubezpieczenia komunikacyjnego jest to informacja o tym, czy nowy ubezpieczający jest dobrym czy słabym kierowcą. Wadą dobrych kierowców, która wynika z negatywnej selekcji, jest to, że zasadniczo płacą oni tak samo wysokie składki ubezpieczeniowe jak słabi (o ile ubezpieczyciel samochodowy nie jest w stanie odróżnić dobrego kierowcy od słabego). Ryzyko moralne powoduje zmianę zachowania, ponieważ zmniejsza się ryzyko wykrycia szczególnie złego zachowania. W ten sposób kierowca może celowo zmniejszyć ryzyko wypadku, jadąc z rozsądną prędkością, nie pijąc alkoholu, obserwując odległość i tak dalej. W wyniku zawarcia polisy ubezpieczeniowej motywacja do unikania wypadków jest przynajmniej teoretycznie zmniejszona. Astereotypowa forma pokusy moralnej polega na tym, że kierowcy stają się jeszcze bardziej awersją do ryzyka, ponieważ czują, że są już dobrze zabezpieczeni na ryzyko finansowe nieostrożnej lub ryzykownej jazdy. Czujniki są również w stanie obserwować zachowanie w obiektywny sposób. Zasadniczo można zmierzyć prędkość, czas podróży i odległości, zachowanie podczas hamowania, a także uwagę i poziom alkoholu. Firma ubezpieczeniowa może teraz wprowadzić zróżnicowanie cen w zależności od rzeczywistego zachowania i umiejętności kierowców. Miało to miejsce już w 2004 roku w Wielkiej Brytanii w towarzystwie ubezpieczeniowym Norwich Union, które oferowało kierowcom samochodów taryfę „płać za jazdę". W ramach programu zainstalowali w samochodzie czarną skrzynkę, która zbierała odpowiednie dane dotyczące stylu jazdy i przesłał je do Norwich Union. Nie tylko techniczne, ale także społeczno-gospodarcze sieci będą znacznie bardziej obfite między firmami, użytkownikami, konsumentami, a nawet przedmiotami. Z ekonomicznego punktu widzenia powoduje to efekty sieciowe na konsumpcję i produkcję. Oznacza to, że korzyści płynące z technologii będą rosły wraz ze wzrostem liczby użytkowników na rynku. Aby uzyskać udział w rynku dla produktów lub norm związanych z efektami sieciowymi, na samym początku należy spodziewać się niskich cen, aby zbudować masę krytyczną.

Zwiększona świadomość przestrzeni informacyjnej

W przypadku usług kontekstowych często wymagane są informacje, które są własnością różnych podmiotów. Dlatego takie usługi mogą opierać się na informacjach od użytkownika, na przykład jego imieniu i alergiach, na informacjach od właściciela środowiska, na przykład , pozycję użytkownika w supermarkecie, a także produkty w jego otoczeniu oraz informacje od usługodawcy, np. informacje o substancjach uczulających w konkretnym produkcie. Dlatego usługi kontekstowe nie mogą być oferowane, jeśli każdy aktor chroniłby swoje informacje przed dostępem z zewnątrz. Należy raczej stworzyć przestrzenie informacyjne, w których różne systemy informacyjne są gromadzone przez różne podmioty. Przestrzeń informacyjna obejmuje zatem wszystkie dane i istotne informacje uzyskane w inteligentnym środowisku, aby zapewnić użytkownikom usługi i aplikacje kontekstowe. Dostęp do przestrzeni informacyjnej może być ograniczony do określonych podmiotów, ale może być ona również publicznie dostępna, tak aby osoby trzecie mogły wykorzystywać informacje do innowacyjnych usług. Głównym wyzwaniem jest zrozumienie informacji przez osoby trzecie dostępne w przestrzeniach informacyjnych. W tym celu przydatne mogą być technologie semantyczne. Zarządzanie przestrzeniami informacyjnymi można postrzegać jako zadanie zarządzania informacją. Jak wskazano, świadczenie inteligentnych, kontekstowych usług wymaga przestrzeni informacyjnych obejmujących systemy informacyjne różnych podmiotów. To stawia przed firmami wyzwanie zarządzania tymi przestrzeniami informacyjnymi w celu zapewnienia wspólnej wartości z partnerami i dla ich własnej korzyści. Zarządzanie to odbywa się w relacji napięcia między potencjałem innowacji wywołanym przez otwieranie przestrzeni informacyjnych a chęcią czerpania korzyści wyłącznie z zamkniętych przestrzeni informacyjnych przy założeniu zachowania pełnej kontroli i integralności danych. Z jednej strony otwarcie przestrzeni informacyjnych oznacza, że osoby trzecie mogą uzyskać dostęp do informacji i zintegrować je z nowymi, innowacyjnymi usługami. Jest to już widoczne jako otwarcie systemów informatycznych, takich jak GoogleMaps i Facebook, co doprowadziło do ogromnej liczby mashupów i opracowanych zewnętrznie, innowacyjnych aplikacji. W skomputeryzowanym świecie, w którym dane o rzeczywistości są dostępne na znacznie wyższym poziomie jakości, należy oczekiwać dramatycznie większego potencjału innowacji, jeśli dane są swobodnie dostępne. Z drugiej strony pojawia się pytanie, w jaki sposób firma może skorzystać na tym, że osoby trzecie wykorzystują ich informacje do tworzenia innowacji. Firmy mogłyby zatem polegać na zamknięciu swoich przestrzeni informacyjnych w celu wykluczenia konkurencji i wykorzystania dostępu do przestrzeni informacyjnej jako źródła przychodów. Takie przestrzenie informacyjne byłyby jednak sprzeczne z urzeczywistnieniem skomputeryzowanego świata. W przypadku zarządzania przestrzenią informacyjną pojawia się pytanie, jak daleko należy otworzyć przestrzenie informacyjne, aby zwiększyć potencjał innowacji, az drugiej strony, aby maksymalnie czerpać zyski. Ponadto rodzi to pytanie, kto powinien posiadać i kontrolować urządzenia i ich dane? Prosty przypadek użycia ilustruje konflikt, czyli rozszerzone termostaty domowe (renderujące je jako inteligentne obiekty) podłączone do inteligentnej sieci energetycznej. Kto powinien być właścicielem danych generowanych przez termostat domowy w domu użytkownika: użytkownika końcowego lub usługodawcy? Co się dzieje, gdy użytkownik (lokalny) chce czuć się komfortowo w konflikcie z (globalnymi) celami dostawcy w zakresie oszczędzania energii?

Aspekty społeczne, etyczne, prawne i związane z ryzykiem

Zinformatyzowane światy istnieją w ciągłym napięciu między innowacjami (technicznie wykonalne) a indywidualną i społeczną akceptacją (społecznie pożądane). Trudności z wyżej wymienionymi strategiami cenowymi to przede wszystkim akceptacja klienta i związane z tym obawy dotyczące naruszenia prywatności. Uzyskiwanie szczegółowych danych o podmiotach, a zwłaszcza o osobach, ujawnia podstawowy dylemat współczesnego Internetu Rzeczy. W szczególności wszelkie informacje dotyczące osoby mogą zarówno wzbogacać indywidualne usługi kontekstowe, jak i osobowe, a także stanowić potencjalną ingerencję w prywatność, prowadzącą do oporu. Oprócz prywatności istnieje wiele innych podstawowych wyzwań związanych z bezpieczeństwem (informatycznym), zaufaniem i

tak dalej. Brak bezpieczeństwa w całym IoT, a w szczególności w Przemysłowym Internecie Rzeczy, wyszedł na jaw w dużej mierze dzięki eksperymentalnej wyszukiwarce o nazwie Shodan. Uruchomiona w 2009 r. usługa indeksuje prawie cztery miliardy urządzeń, z których w dowolnym momencie włącza się kilkaset milionów urządzeń (w zależności od łączności sieciowej). Jak analiza zagrożeń oparta na Shodan wykazała, że ponad 100 000 urządzeń IT może być łatwo zaatakowane, wśród nich są specjalne komputery przemysłowe do regulacji przepływu wody, systemy transportowe, a nawet cała sieć energetyczna. Wiele z tych systemów zostało zaprojektowanych przed nadejściem IoT, a zatem nie uwzględniono tego typu zagrożenia bezpieczeństwa. IoT z pewnością ma do czynienia z dosłownie wszystkimi problemami bezpieczeństwa znanymi już z innych koncepcji i artefaktów związanych z IT - i może dodać kilka dodatkowych aspektów, jeśli nie tylko ze względu na wagę i wagę. Oto kilka przykładów naglących pytań badawczych:

* Jak powinniśmy radzić sobie z problemami prywatności w scenariuszach Ubicomp, skupiając się na rozważaniach dotyczących projektowania systemu?

* Kto odpowiada za decyzje podejmowane przez systemy autonomiczne?

* Jak promujemy etyczne korzystanie z technologii IoT?

* Jaką rolę odgrywa zarządzanie zaufaniem w scenariuszach IoT?

* Co może zrobić oprogramowanie pośredniczące w przypadku problemów z bezpieczeństwem i prywatnością?

* Jakie są wymagania bezpieczeństwa dotyczące poufności danych?

* Jakie są istotne wyzwania legislacyjne?

* Jakie są odpowiednie opcje architektoniczne dla bezpieczeństwa i prywatności, w szczególności zalety i wady architektur scentralizowanych i rozproszonych?

* Jakie są główne modele ataków i zagrożenia?

Aby uwzględnić pewną wrażliwość w skali i zakresie społecznych, etycznych, prawnych i związanych z ryzykiem aspektów IoT, kładzie się nacisk na „dane” i związane z nimi kwestie prywatności danych . Warto zauważyć, że ta lista pytań nie jest wyczerpująca.

* Kiedy możemy wnioskować z pewnością? Musimy wziąć pod uwagę, że wyczuwane dane lub interakcje to nieprecyzyjne obserwacje świata, często pobierane z wielu czujników i w różnym czasie. Środowiska IoT muszą wziąć pod uwagę te dowody i ocenić, kiedy i jak zareagować. Pełne zrozumienie wartości i znaczenia danych jest z pewnością zależne od aplikacji i kontekstu. Czy mamy maszyny (a dokładniej oprogramowanie), które są na tyle zaawansowane, aby właściwie „zrozumieć” taki kontekst i dane?

* Gdzie znajdują się dane? Łatwiej odpowiedzieć na to pytanie w kontekście technicznych aspektów architektury cloud i fog computing. Jednak w odniesieniu do własności, kontroli danych i dostępu do danych uzyskanie odpowiedzi jest znacznie trudniejsze. W wielu środowiskach, takich jak pokoje, domy, firmy i szpitale, zapotrzebowanie na bezpieczeństwo i prywatność wymaga egzekwowania konwencjonalnych, prawnych i fizycznych granic.

* Jak długo dane powinny być przechowywane? Co wie o nas środowisko? Co powinna wiedzieć i czym ufać? Jak długo należy przechowywać dane? Co jest przejściowe, a co powinno trwać? Czy możemy usunąć dane i czy można o nich zapomnieć? Kto ma (prawo) dostępu do danych? Kto jest właścicielem

wykrywanych danych? Czy jest to właściciel czujnika, właściciel środowiska, w którym czujnik pracuje, czy zbieracz danych?

Większość, jeśli nie wszystkie, z tych pytań zyskały ostatnio na znaczeniu wraz z pojawieniem się „Big Data" i ich bezprecedensowej skali przechowywania, przetwarzania i wykonywania danych oraz uzyskiwania z nich wglądu. Ponadto istnieją pytania, które dotyczą tego, kto zapłaci za infrastrukturę IoT (mniej oczywiście, ale ostatecznie zwykły obywatel ze swoimi pieniędzmi z podatków). Potrzebne są regulacje dotyczące tego, kto jest odpowiedzialny za zarządzanie i utrzymanie infrastruktury lokalnej, regionalnej, krajowej i ponadnarodowej, iw dużej mierze nie zostały jeszcze zdefiniowane. Ze względu na kwestie techniczne i ogólną niechęć to nie zwykły użytkownik będzie zarządzał własnymi danymi, a więc usługodawcami. Usługi zarządzane z pewnością ograniczyłyby złożoność dla użytkownika końcowego i przesłoniłyby skomplikowane interfejsy technologiczne. Jednak usługi zarządzane wprowadzają również własne napięcie między możliwościami zarządzania i kosztami dla dostawcy a elastycznością i kontrolą dla użytkownika końcowego. Jednym z przykładów inicjatywy, która zajmuje się kwestiami politycznymi i regulacyjnymi, jest Deklaracja z Mauritiusa w sprawie Internetu Rzeczy. Wyciągnięte przykładowe instrukcje obejmują następujące elementy:

* Dane z czujników IoT charakteryzują się dużą ilością, jakością i czułością, dlatego należy je traktować i traktować jako dane osobowe.

* Przejrzystość dla wszystkich interesariuszy ma kluczowe znaczenie. Ci, którzy oferują urządzenia IoT, powinni poinformować użytkownika, aby wiedział, jakie dane są gromadzone, w jakim celu i jak długo te dane są przechowywane.

* Prywatność w fazie projektowania powinna być domyślną zasadą projektowania.

* Aby sprostać wyzwaniom związanym z bezpieczeństwem, jednym ze sposobów zminimalizowania ryzyka dla osób fizycznych jest zapewnienie, że dane mogą być przetwarzane na samym urządzeniu (przetwarzanie lokalne). Jeżeli nie jest to możliwe, firmy powinny zapewnić szyfrowanie typu end-to-end, aby chronić dane przed nieuzasadnioną ingerencją i/lub manipulacją.

* Organy ochrony danych i prywatności powinny zapewnić zgodność z przepisami o ochronie danych i prywatności w swoich krajach, a także z międzynarodowymi zasadami prywatności, w tym odpowiednimi działaniami egzekucyjnymi, zarówno jednostronnie, jak i poprzez współpracę międzynarodową.

Biorąc pod uwagę ogromne wyzwania stojące przed twórcami IoT, organy ochrony danych i osoby fizyczne powinny zaangażować się w silną, aktywną i konstruktywną debatę na temat społecznych, etycznych, prawnych i związanych z ryzykiem aspektów IoT.

Wniosek

Chociaż koncepcja łączenia komputerów, czujników i sieci w celu monitorowania i sterowania urządzeniami istnieje od dziesięcioleci, ostatnie zbieg kluczowych technologii i trendów rynkowych katalizuje ideę IoT. Aby lepiej ustrukturyzować skalę i zakres IoT, przedstawiono wstępny przegląd i pokrótce naszkicowano podstawowe idee koncepcyjne przedstawione przed IoT z „przetwarzaniem wszechobecnym". Przedstawiono czterowarstwowe ramy „Internetu rzeczy", które obejmują nie tylko techniczne, ale także nietechniczne kwestie IoT. IoT obiecuje stworzyć podstawę dla nowych produktów, procesów i modeli biznesowych i może fundamentalnie wpłynąć zarówno na rynki B2C, jak i B2B, a także na sposób, w jaki produkujemy towary zgodnie z przewidywaniami z pochodnymi, w tym Przemysłowym Internetem Rzeczy i Przemysłem 4.0. Chociaż konsekwencje są bardzo prawdopodobne, wiele potencjalnych wyzwań może utrudniać tę wizję, szczególnie w obszarach

bezpieczeństwa, prywatności, interoperacyjności, standardów, a także kwestii prawnych, regulacyjnych i praw, a także włączenia gospodarek wschodzących. IoT obejmuje nie tylko kwestie technologiczne, ale także społeczne i polityczne. IoT już szybko staje się coraz bardziej rzeczywistością, a obecnie istnieje ogromna przestrzeń dla nowych projektów i realizacji twórców i programistów.