Zeszyty Naukowe Politechniki Częstochowskiej
Zarządzanie Nr 31 (2018) s. 212-221
dostępne na: http://www.wz.pcz.pl/znwz

SKALOWALNOŚĆ, BEZPIECZEŃSTWO I INTEROPERACYJNOŚĆ JAKO KLUCZOWE WYZWANIA DLA PROJEKTOWANIA SYSTEMÓW INTERNETU RZECZY

Artur Rot, Małgorzata Sobińska

Uniwersytet Ekonomiczny we Wrocławiu
Wydział Zarządzania, Informatyki i Finansów

Streszczenie: Badania rynkowe pokazują, iż organizacje dostrzegają coraz częściej konkretne korzyści płynące z zastosowania Internetu rzeczy. W obszarze biznesowym stwarza on nowe możliwości rynkowe, umożliwiając m.in. zwiększanie wydajności procesów produkcyjnych i biznesowych oraz stanowiąc sprawne narzędzie komunikacji z klientami. Obszarów zastosowania Internetu rzeczy może być wiele oraz mogą one przenikać wiele aspektów życia. Jednakże podobnie jak w przypadku implementacji większości nowych koncepcji, również w odniesieniu do Internetu rzeczy istnieje cały szereg różnego rodzaju wyzwań. Związane jest to głównie z faktem, że systemy te są rozwiązaniami skomplikowanymi, opartymi na różnych technologiach, a ich skala oraz heterogeniczność jest bardzo duża. Z punktu widzenia rozwiązań technologicznych autorzy dostrzegają kilka zasadniczych obszarów, stanowiących największe wyzwanie dla Internetu rzeczy. Dotyczą one technologii niezbędnych dla tworzenia infrastruktury Internetu rzeczy, a w szczególności skalowalności, interoperacyjności i elastyczności zastosowanych rozwiązań. Kolejna kwestia dotyczy bezpieczeństwa danych. Celem artykułu jest prezentacja potencjału omawianej koncepcji, ale przede wszystkim zwrócenie uwagi na wyzwania, przed jakimi ona stoi. Zastosowane metody badań to przegląd aktualnej literatury przedmiotu, analiza istniejących badań i wybranych przypadków zastosowań Internetu rzeczy oraz identyfikacja i analiza najważniejszych wyzwań stojących przed tą koncepcją.

Słowa kluczowe: bezpieczeństwo, elastyczność, interoperacyjność, Internet rzeczy, skalowalność

DOI: 10.17512/znpcz.2018.3.18

Wprowadzenie

Raport *The Changing Landscape of Disruptive Technologies. Innovation Convergence Unlocks New Paradigms* (Zanni i in. 2017), przygotowany przez firmę KPMG, przewiduje, iż w perspektywie najbliższych kilku lat dominującym trendem technologicznym IT będzie wykorzystanie chmur obliczeniowych w połączeniu z platformami i aplikacjami mobilnymi. Systematycznie będzie też rosła rola Internetu rzeczy (ang. *Internet of Things* – IoT), analizy dużych zbiorów danych (ang. *Big Data*) i inżynierii biomedycznej. Z kolei według raportu opracowanego przez firmę Cisco (Cisco 2017) zagadnienia, takie jak cyfryzacja, bezpieczeństwo technologii informacyjnych oraz Internet rzeczy, to zjawiska, które będą wyznaczać kierunek rozwoju poszczególnym branżom gospodarki w kolejnych latach. Wśród obu prognoz ważne miejsce zajmuje Internet rzeczy, który jest połą-

czeniem urządzeń w sieć, tak aby umożliwić ich zdecentralizowaną komunikację między sobą.

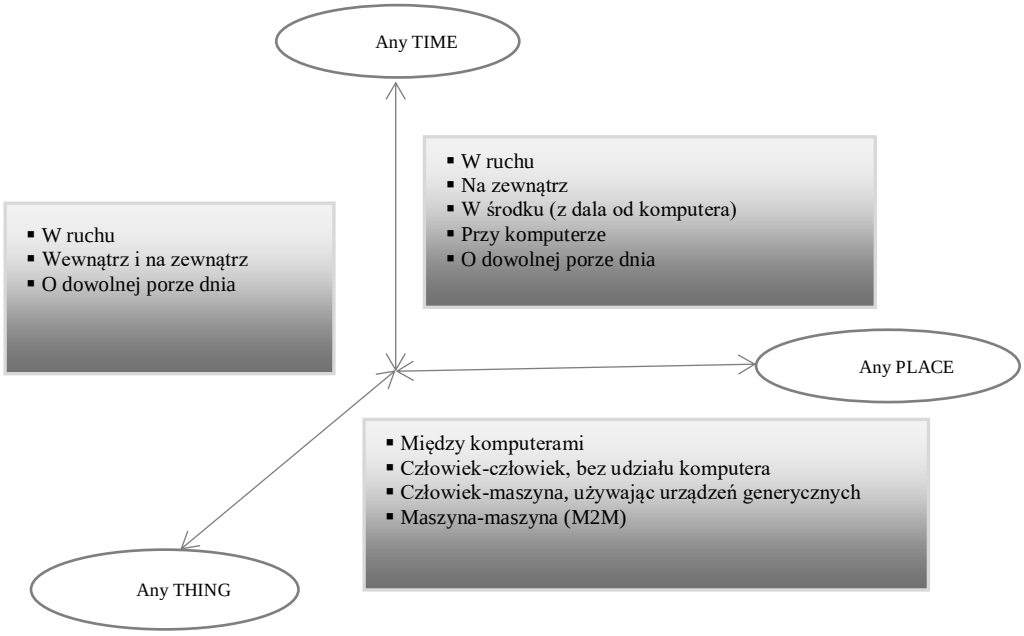
Korzyści płynące z IoT są niezaprzeczalne, jednak „inteligentne" rzeczy stawiają przed nami wiele wyzwań. Według danych IHS Markit, firmy specjalizującej się w analizie rynków, na świecie jest już ponad 20 miliardów urządzeń podłączonych do sieci. Generują one ogromną ilość danych, a według niektórych szacunków już niebawem, bo w 2020 roku, na każdego człowieka będzie przypadać około 5,2 PB danych (1 PB = 10^{15} bajtów) (Evans 2016). Zatem w Internecie rzeczy funkcjonować będą niezliczone urządzenia, przedmioty oraz różnego rodzaju sensory, które będą rejestrować ruch, obraz, dźwięk oraz sterować innymi urządzeniami. Liczba, rodzaj i zastosowania urządzeń komunikujących się z Internetem rosną aktualnie i dalej lawinowo będą się zwiększać. Wobec tego infrastruktura obsługująca Internet rzeczy musi połączyć miliony urządzeń oraz serwerów, sprawnie przeprowadzać transmisje danych, przetwarzać oraz przesyłać ogromne zbiory danych. Transmisja i przetwarzanie danych pochodzących z tak olbrzymiej liczby urządzeń staje się problemem o charakterze megaskali, gdyż żadna chmura obliczeniowa nie będzie w stanie sprawnie obsłużyć aż tak złożonej rzeczywistości (Nowakowski 2015). Kolejne wyzwanie związane z Internetem rzeczy, ograniczające jego dynamiczny rozwój, to jeden z największych problemów branży technologicznej, jakim jest interoperacyjność. Trzecie zagadnienie, stanowiące zdaniem autora największe wyzwanie, to zapewnienie odpowiedniego poziomu bezpieczeństwa i prywatności danych w Internecie rzeczy. Liczne przypadki cyberataków na systemy Internetu rzeczy, masowe wycieki danych i coraz częstsze dowody na projektowanie tychże systemów bez brania pod uwagę wymogów cyberbezpieczeństwa są bardzo niepokojące (Rot 2016). Problemy te mogą pociągnąć za sobą bardzo niebezpieczne zagrożenia na skalę dotychczas niespotykaną. Celem artykułu jest prezentacja potencjału koncepcji Internetu rzeczy, ale przede wszystkim zwrócenie uwagi na wyzwania, przed jakimi stoimy, korzystając z tych rozwiązań. Wśród najważniejszych wyzwań autor wymienia bezpieczeństwo danych, skalowalność rozwiązań i związaną z nimi interoperacyjność.

Koncepcja Internetu rzeczy

Koncepcję Internetu rzeczy stworzył K. Ashton, a ideę tę sformułował już prawie 20 lat temu, w 1999 roku, w celu opisania systemu, w którym świat materialny komunikuje się z komputerami za pomocą wszechobecnych sensorów. Dziesięć lat później, w 2009 roku, liczba urządzeń podłączonych do sieci przekroczyła liczbę mieszkańców Ziemi i według ekspertów Cisco wtedy właśnie narodził się IoT (Kolenda (red.) 2015).

International Telecommunications Union (ITU) określa IoT jako globalną infrastrukturę dla społeczeństwa informacyjnego, umożliwiającą dostęp do zaawansowanych usług poprzez połączenie (fizyczne lub wirtualne) przedmiotów (obiektów), bazujące na istniejących i rozwijanych interoperacyjnych technologiach ICT (ITU 2006). Zatem pojęcie to może być przedstawione jako rozszerzenie koncepcji Internetu o wszystkie wyżej wymienione kategorie urządzeń lub jako sieć łącząca

różne sieci (wirtualne oraz fizyczne) będące w stanie komunikować się. Koncepcję Internetu rzeczy można również przedstawić jako sieć umożliwiającą komunikację w trzech wymiarach: zawsze (ang. *Any TIME*), wszędzie (ang. *Any PLACE*) oraz ze wszystkim (ang. *Any THING*) (*Rysunek 1*).



Rysunek 1. Ogólny model Internetu rzeczy

Źródło: Opracowanie własne na podstawie (Niyato i in. 2015)

Inne definicje określają Internet rzeczy jako ogół inteligentnych przedmiotów, mogących reagować na środowisko oraz przetwarzać informacje, a także przesyłać je do innych obiektów (i użytkowników) za pośrednictwem protokołów internetowych (Nowakowski 2015). Nie jest to koncepcja przyszłości, gdyż jest już ona w pewnym zakresie aktualnie realizowana, a obszarów jej zastosowania może być wiele oraz mogą one przenikać wiele aspektów życia, np. (Rot, Blaicke 2017):

- miasto – środowisko miejskie z publiczną infrastrukturą, np. inteligentne parkometry, kontrola jakości wody czy świateł ulicznych i inne rozwiązania składające się na koncepcję inteligentnego miasta (ang. *smart city*) (Rot 2017);
- człowiek – np. monitorowanie i polepszanie zdrowia, samopoczucia;
- środowisko pracy – np. systemy monitorowania warunków pracy;
- dom – inteligentny dom, systemy zabezpieczeń;
- handel i usługi – miejsca sprzedaży i oferowania usług, jak hotele, restauracje, banki, sklepy, np. promocje oparte na lokalizacji;
- środowisko produkcyjne – środowisko produkcji, takie jak fabryki, np. monitorowanie procesu produkcyjnego;
- transport – środki lokomocji, takie jak samochody, motory, rowery;

- biuro – np. inteligentne termostaty i klimatyzatory;
- świat zewnętrzny – inne środowiska zewnętrzne, zdefiniowane jako przestrzeń powietrzna i kosmiczna, logistyka, np.: zarządzanie lokalizacją floty.

Internet rzeczy staje się powoli obowiązkowym elementem technologii w biznesie, a dzięki sieci połączonych urządzeń, zasobów ludzkich i zgromadzonych danych firmy będą mogły lepiej zrozumieć wymagania klientów i szybciej wprowadzać zmiany w łańcuchu dostaw czy implementować innowacje. Może on też wpłynąć na poprawę jakości życia ludzi, którzy będą mogli wykonywać zdalne płatności, monitorować swój stan zdrowia, sprawdzać dostępność miejsc parkingowych itp. Inteligentne systemy zarządzania odpadami, energią czy ruchem ulicznym stają się powoli codzienną rzeczywistością (EY 2015).

Potencjał Internetu rzeczy

Według firmy badawczej McKinsey&Company Internet rzeczy ma szanse generować znaczące korzyści ekonomiczne dla światowej gospodarki szacowane miedzy 2,7 a 6,2 tryliona USD w 2025 roku (McKinsey&Company 2015). Gałęzie przemysłu, które mają największy potencjał wygenerować taką wartość, uwzględniają szeroko pojęte zastosowania medyczne, infrastrukturalne oraz usługi w ramach sektora publicznego. Zdalne monitorowanie stanu pacjentów może mieć olbrzymi wpływ na życie milionów ludzi borykających się z przewlekłymi chorobami, jednocześnie zmniejszając koszty obsługi medycznej. Możliwość kontroli oraz analizy sieci energetycznych oraz wodno-kanalizacyjnych może znacząco wpłynąć na ich efektywniejsze wykorzystanie, zmniejszając emisje gazów cieplarnianych czy minimalizując niepotrzebne zużycie wody. Możliwość podłączenia dosłownie każdego elementu codziennego życia, takiego jak pralka, lodówka czy oświetlenie, do globalnej sieci tworzy możliwości biznesowe i znaczne oszczędności zasobów dla gospodarstw domowych czy organizacji.

Korzyści wynikające z IoT w organizacjach można zebrać w kilka kategorii: zwiększenia produktywności pracowników, redukcji kosztów, lepszej alokacji kapitału i poprawy relacji z klientami. Według P. Kotlera i J.E. Heppemanna (Kotler, Heppemann 2014) korzyści wynikające z tej rewolucji można podzielić na cztery obszary:

- monitoring – możliwość obserwacji i kontroli stanu przedmiotu, które dokonuje on sam, zbiera także informacje o otoczeniu i dane o swoim działaniu;
- optymalizacja – zwiększenie wydajności produktu oraz diagnostyka, obsługa i naprawa;
- kontrola – „inteligentne" rzeczy uczą się także swoich użytkowników oraz kontrolują swoje funkcje;
- autonomia – „inteligentny" przedmiot może samodzielnie zwiększać swoją wydajność i efektywność (także poprzez łączenie się z innymi urządzeniami).

Jak wynika z powyższych rozważań, korzyści płynących z IoT jest wiele, jednak koncepcja ta stawia przed nami wiele wyzwań, których identyfikację i analizę zawarto w kolejnej części niniejszego artykułu.

Internet rzeczy – kluczowe wyzwania i zagrożenia

Jeśli chodzi o kwestie natury technicznej, związane z tworzeniem systemów IoT, mogące zarówno ograniczać, jak i stymulować ich rozwój, wskazać można następujące kluczowe obszary:

- zastosowane technologie, tak w zakresie sprzętu, jak i oprogramowania, niezbędne dla tworzenia infrastruktury Internetu rzeczy, a przede wszystkim jej skalowalność, przepustowość i elastyczność;
- bezpieczeństwo danych;
- interoperacyjność systemów IoT, standaryzacja oprogramowania i aktualizacje.

Skalowalność, przepustowość i elastyczność rozwiązań

Dane pochodzące z urządzeń IoT przetwarzane są w chmurze, która swoją popularność zawdzięcza m.in. wysokiej elastyczności. Jednakże ma ona swoje granice, zwłaszcza przy lawinowym wzroście liczby urządzeń mobilnych i inteligentnych przedmiotów podłączanych do sieci Internet. Dane, które już przytaczano w artykule, mówią, iż w 2020 roku do Internetu podłączonych będzie ponad 26 mld urządzeń, co oznacza ogromny przyrost ilości danych, które trzeba będzie odpowiednio przesyłać, przechowywać i przetwarzać (Middleton, Kjeldsen, Tully 2013). Według kolejnych szacunków w 2020 roku chmury będą przetwarzać 8,6 ZB danych, z których znaczna część pochodzić będzie z urządzeń i czujników Internetu rzeczy. Rosnąca liczba aplikacji i połączeń IoT generuje duże wolumeny danych, które już niebawem, w 2019 roku, osiągną 507,5 ZB rocznie (ok. 42,3 ZB miesięcznie) (Cisco 2017). Wśród tych urządzeń generujących dane będą laptopy, smartfony, tablety, czujniki w budynkach, samochodach, zegarkach i szereg inteligentnych etykiet na różnych przedmiotach. Transmisja i przetwarzanie danych pochodzących z tak olbrzymiej liczby urządzeń staje się problemem o charakterze megaskali, gdyż żadna chmura obliczeniowa nie będzie w stanie sprawnie obsłużyć aż tak złożonej rzeczywistości (Nowakowski 2015). To duże wyzwanie dla centrów danych, które będą musiały poradzić sobie z przetwarzaniem i przechowywaniem danych. Zdaniem niektórych ekspertów centralizacja, będąca właściwością chmury, nie jest w tym przypadku najlepszym rozwiązaniem. Chmura nie charakteryzuje się na tyle dużą elastycznością, przepustowością czy skalowalnością, żeby sprostać wymaganiom nowych technologii, w tym Internetu rzeczy. Zatem aby zoptymalizować koncepcję chmury obliczeniowej, potrzebny jest nowy sposób przesyłania, przechowywania i przetwarzania danych. Takim rozwiązaniem staje się koncepcja mgły obliczeniowej (ang. *fog computing*), dotycząca zbudowania takiego środowiska, w którym większość decyzji będzie podejmowana na brzegu sieci, bez potrzeby przesyłania olbrzymich zbiorów danych do chmury obliczeniowej, by dopiero stamtąd oczekiwać na dalsze instrukcje. Pojęcie mgły obliczeniowej zostało wprowadzone przez firmę Cisco jako nowy paradygmat wsparcia transmisji i przetwarzania danych do wspierania rozproszonych urządzeń w koncepcji Internetu rzeczy. Można ją określić jako wirtualną platformę, która zapewnia możliwości obliczeniowe, pamięci masowe i usługi sieciowe między urządzeniami końcowymi i tradycyjnym centrum danych chmury obliczeniowej (Billewicz 2016).

Mgła obliczeniowa będzie bazować na lokalnych zasobach obliczeniowych, a nie, jak jest to w usłudze chmury obliczeniowej, znajdujących się gdzieś w odległym (często nieznanym użytkownikowi) miejscu. Takie przetwarzanie zapewni większe bezpieczeństwo i większą wydajność. Podstawową właściwością mgły jest instalacja serwerów na granicach chmury, które będą odbierać dane z urządzeń Internetu rzeczy, a następnie je przechowywać, przetwarzać i odpowiednio analizować, uporządkowując w ten sposób dane pozyskane z bardzo wielu urządzeń i czujników (Billewicz 2016). Wsparcie to osiągnięte zostanie dzięki temu, iż router łączący urządzenia w IoT ma zajmować się nie tylko transmisją danych, ale przede wszystkim odciążać chmurę, wykonując za nią część obliczeń lokalnie.

Właśnie zdefiniowanie mgły jako warstwy pośredniej do chmury obliczeniowej stworzy możliwości szybszego rozwoju Internetu rzeczy. Chmura obliczeniowa ma bowiem wiele wad, z których najważniejsze to ograniczona przepustowość, brak mobilności, strumieniowego przesyłania danych oraz bezprzewodowego dostępu (Rot, Sobińska 2017). Proponowane rozwiązanie ma wiele innych cech charakterystycznych istotnych z punktu widzenia Internetu rzeczy, wśród których warto wymienić m.in. (Bonomi i in. 2012):

- małe opóźnienia transmisji;
- uwzględnienie wielkich sieci komunikacyjnych z czujnikami, zwykle będą to sieci bezprzewodowe mogące dostarczać różnorodnych danych;
- obsługę wielkiej liczby czujników wykorzystywanych w celach monitorowania otoczenia oraz obsługi inteligentnych sieci energetycznych (*smart grids*);
- heterogeniczność – węzły sieci w mgle obliczeniowej występują w różnej formie i postaci oraz są wdrożone w różnych środowiskach;
- interoperacyjność i konsolidację – bezproblemowa obsługa niektórych usług (np. strumieniowanie wideo) wymaga współpracy różnych dostawców, stąd elementy mgły muszą być w stanie współdziałać ze sobą.

Według szacunków Cisco 40% danych pochodzących z Internetu rzeczy będzie do roku 2018 przetwarzanych właśnie w mgle obliczeniowej.

Bezpieczeństwo systemów Internetu rzeczy

Internet rzeczy z pewnością wprowadzi wiele nowych zmiennych do kwestii szeroko pojętego cyberbezpieczeństwa. Będzie on stanowić duże wyzwanie dla specjalistów zajmujących się tą problematyka, a zarazem będzie to okazja do przemyślenia całego ekosystemu zapewniającego akceptowalny poziom ryzyka. Badania przeprowadzone przez Instytut SANS wykazały, że największymi zagrożeniami związanymi z rosnącą popularnością Internetu rzeczy są (Pescatore 2014):

- trudności z aktualizacją oprogramowania „przedmiotów", która bardzo często jest zależna od producentów sprzętu, a użytkownicy nie mają żadnej możliwości ingerencji w tę część oprogramowania;
- wykorzystanie przedmiotów, jako najsłabiej zabezpieczonych punktów wejścia do sieci, co daje możliwość rozprzestrzeniania się i dalszej infekcji;
- wykonywanie ataków związanych z utrudnieniem bądź zaprzestaniem świadczenia danych usług (ang. *Denial of Service*), które zwłaszcza w kontekście in-

frastruktury krytycznej, takiej jak sieć energetyczna czy urządzenia medyczne, może prowadzić do poważnych konsekwencji;
- celowy sabotaż i fizyczne niszczenie przedmiotów poprzez cyfrowy dostęp i modyfikacje parametrów działania;
- błędy użytkowników i przypadkowe modyfikacje, które mogą prowadzić do trudnych do przewidzenia konsekwencji w skali całego systemu.

Niezależne zrzeszenie OWASP (Open Web Application Security Project) w 2014 roku wydało zestawienie 10 największych uchybień bezpieczeństwa wśród najpopularniejszych urządzeń wchodzących w skład Internetu rzeczy. W *Tabeli 1* zaprezentowano najczęściej występujące problemy bezpieczeństwa w tych urządzeniach i ich klasyfikację względem czterech kryteriów.

Tabela 1. Najważniejsze podatności i zagrożenia urządzeń Internetu rzeczy

Lp.	Podatność/zagrożenie	Łatwość wykorzystania do ataku	Częstość występowania	Łatwość wykrycia	Potencjalne skutki
1.	Niezabezpieczony interfejs sieciowy	Łatwo	Często	Łatwo	Znaczące
2.	Zbyt słaba autoryzacja	Średnio	Często	Łatwo	Znaczące
3.	Niezabezpieczone usługi sieciowe	Średnio	Rzadko	Średnio	Średnie
4.	Brak szyfrowania warstwy transportowej	Średnio	Często	Łatwo	Znaczące
5.	Problemy z prywatnością	Średnio	Często	Łatwo	Znaczące
6.	Niezabezpieczona transmisja z chmurą	Średnio	Często	Łatwo	Znaczące
7.	Niezabezpieczone interfejsy bezprzewodowe	Średnio	Często	Łatwo	Znaczące
8.	Niewystarczające opcje konfiguracji zabezpieczeń	Średnio	Często	Łatwo	Średnie
9.	Niebezpieczne oprogramowanie *firmware*	Trudno	Często	Łatwo	Znaczące
10.	Niewystarczające zabezpieczenia fizyczne	Średnio	Często	Średnio	Znaczące

Źródło: Opracowanie własne na podstawie (OWASP 2017)

Jak pokazują badania przeprowadzone przez specjalistów firmy HP (HP 2014), wiele urządzeń IoT jest podatnych na atak, a każde z nich posiada słabe punkty – dotyczące bezpieczeństwa haseł, kryptografii, braku odpowiedniego zarządzania kontrolą dostępu – które rozszerzają możliwości nadużyć przez intruzów. Eksperci HP przetestowali 10 najbardziej popularnych urządzeń Internetu rzeczy, odkrywając łącznie ok. 250 zagrożeń bezpieczeństwa we wszystkich produktach. Najczęstsze problemy bezpieczeństwa obejmowały następujące zagadnienia:
- problemy z prywatnością danych – zanotowano podatności dotyczące prywatności związanej z gromadzeniem danych osobowych, badane systemy przechowywały nieodpowiednio zabezpieczone dane osobowe w samym produkcie, w chmurze lub w obsługującej urządzenie aplikacji mobilnej;

– słabe punkty w systemie autoryzacji i uwierzytelnienia – systemy nie wymagały haseł o odpowiedniej długości i złożoności;
– brak szyfrowania transmisji danych – większość urządzeń nie szyfrowała komunikacji z Internetem i sieciami lokalnymi, a połowa aplikacji mobilnych obsługujących te urządzenia przesyłała niezaszyfrowane komunikaty;
– niebezpieczne interfejsy WWW – w sześciu z dziesięciu testowanych urządzeń zanotowano obawy związane z bezpieczeństwem interfejsów użytkownika;
– niewystarczający poziom bezpieczeństwa oprogramowania – część urządzeń nie stosowała szyfrowania podczas pobierania aktualizacji oprogramowania.

Przytoczone powyżej badania i dane ukazują, że najważniejszym wyzwaniem dla twórców rozwiązań w ramach IoT powinna być kwestia cyberbezpieczeństwa. Dlatego też od ciągłego zwiększania liczby urządzeń w infrastrukturze IoT ważniejsze jest to, aby budować od samego początku bezpieczne rozwiązania, tak aby uniknąć narażania konsumentów na poważne zagrożenia.

Interoperacyjność i standaryzacja

IoT stanowi źródło inspiracji dla tworzenia nowych i innowacyjnych urządzeń, jednak postęp jest hamowany przez jeden z największych problemów branży technologicznej, a mianowicie interoperacyjność. Eksperci wskazują na brak standaryzacji w obszarze IoT, co powoduje problemy zarówno dla biznesu, jak i użytkowników. Zanim Internet rzeczy osiągnie swój pełny potencjał, to prawdopodobnie muszą powstać odpowiednie standardy, które uproszczą i uregulują rynek, a także zmniejszą koszty dla konsumentów i producentów. Jednakże uniwersalne rozwiązania w obszarze IT zostają powszechnie zaakceptowane na ogół dopiero po pewnym czasie. Stąd też na takie powszechne standardy IoT trzeba prawdopodobnie jeszcze zaczekać. Jeśli chodzi o zagadnienia związane z zapewnieniem interoperacyjności, to według ocen firmy konsultingowej McKinsey&Company jest to krytyczny aspekt w kontekście przyszłości i rozwoju systemów Internetu rzeczy (McKinsey&Company 2015). Wiążą się one z wypracowaniem otwartych standardów we wszystkich obszarach i na wszystkich poziomach, tak aby możliwa była płynna bezproblemowa współpraca oraz komunikowanie się urządzeń pochodzących od różnych dostawców i budowanie na ich bazie heterogenicznych systemów IoT (Wielki 2016).

Podsumowanie

Jednym z istotnych trendów, które mają potencjał, by w ciągu najbliższych lat wpłynąć na życie każdego człowieka i funkcjonowanie biznesu, jest Internet rzeczy. Jak wskazano w artykule, podłączenie urządzeń IoT do globalnej sieci niesie jednak ze sobą potencjalne zagrożenia, na które organizacje muszą zwracać uwagę. Rozważania zawarte w artykule można podsumować wnioskiem, iż Internet przedmiotów stanowi duże wyzwanie dla specjalistów, szczególnie że koncepcja ta wciąż się rozwija i powstają nowe idee, jak np. Internet wszechrzeczy. Jednakże, zdaniem autora, aby koncepcja ta urzeczywistniła się, musi powstać łatwa w zarzą-

dzaniu, a przede wszystkim elastyczna i bezpieczna infrastruktura, skalowalna tak, by mogła obsługiwać miliardy urządzeń, zachowując przy tym wysoki poziom bezpieczeństwa przechowywanych, przetwarzanych i przesyłanych danych.

Literatura

1. Billewicz K. (2016), *Possibility of Internet of Things Technology Implementation in Smart Power Grids*, „Energetyka", nr 5.
2. Bonomi F., Milito R., Zhu J., Addepalli S. (2012), *Fog Computing and Its Role in the Internet of Things*, [w:] *Proceedings of the First Edition of the MCC 2012 Workshop on Mobile Cloud Computing, Helsinki, Finland*, New York, http://conferences.sigcomm.org/sigcomm/2012/ paper/mcc/p13.pdf (dostęp: 15.06.2017). DOI: 10.1145/2342509.2342513
3. Cisco (2017), *Cisco Technology Radar Trends*, http://www.cisco.com/web/solutions/trends/tech-radar/ (dostęp: 18.02.2017).
4. Evans D. (2016), *The Internet of Things. How the Next Evolution of the Internet is Changing Everything*, Cisco Internet Business Solutions Group, http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (dostęp: 16.12.2016).
5. EY (2015), *Insights on Governance, Risk and Compliance: Cybersecurity and the Internet of Things*, http://www.ey.com/Publication/vwLUAssets/EY-cybersecurityand-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf (dostęp: 14.07.2017).
6. HP (2014), *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack*, http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676 (dostęp: 03.12.2016).
7. ITU (2006), *Overview of the Internet of Things*, Telecommunication Standardization Sector of ITU, International Telecommunication Union, Switzerland.
8. Kolenda P. (red.) (2015), *Raport: Internet Rzeczy w Polsce*, IAB Polska, https://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf (dostęp: 17.03.2018).
9. Kotler M.E., Heppelmann J.E. (2014), *How Smart, Connected Products Are Transforming Competition*, Harvard Business Review, November 2014, http://www.hbr.org/2014/11/how-smartconnected-products-are-transforming-competition (dostęp: 19.09.2016).
10. McKinsey&Company (2015), *The Internet of Things: Mapping the Value Beyond the Hype*, McKinsey Global Institute, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world (dostęp: 10.12.2017).
11. Middleton P., Kjeldsen P., Tully J. (2013), *Forecast: The Internet of Things, Worldwide 2013*, Gartner, http://www.gartner.com/doc/2625419/forecast-internet-things-worldwide- (dostęp: 23.02.2017).
12. Niyato D., Lu X., Wang P., Kim D.I., Han Z. (2015), *Economics of Internet of Things (IoT): An Information Market Approach*, „IEEE Wireless Communications", Vol. 23(4). DOI: 10.1109/MWC.2016.7553037
13. Nowakowski W. (2015), *Bliższa chmura, czyli usługi obliczeniowe we mgle*, „Elektronika – Konstrukcje, Technologie, Zastosowania", t. 56, nr 5. DOI: 10.15199/13.2015.5.6
14. OWASP (2017), *Internet of Things Project*, https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project (dostęp: 19.09.2017).
15. Pescatore J. (2014), *Securing the Internet of Things Survey, SANS Institute InfoSec Reading Room*, http://www.sans.org/reading-room/whitepapers/covert/securing-internetthings-survey-34785 (dostęp: 05.01.2017).
16. Rot A. (2016), *Zarządzanie ryzykiem w cyberprzestrzeni – wybrane zagadnienia teorii i praktyki*, [w:] Komorowski T.M., Swacha J. (red.), *Projektowanie i realizacja systemów informatycznych zarządzania. Wybrane aspekty*, PTI, Warszawa.

17. Rot A. (2017), *Zastosowania koncepcji Internetu rzeczy w kontekście inteligentnego miasta. Wybrane zagadnienia bezpieczeństwa*, „Problemy Zarządzania", vol. 15, nr 4(71). DOI: 10.7172/1644-9584.71.3
18. Rot A., Blaicke B. (2017), *Bezpieczeństwo Internetu rzeczy. Wybrane zagrożenia i sposoby zabezpieczeń na przykładzie systemów produkcyjnych*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie", nr 26. DOI:10.17512/znpcz.2017.2.17
19. Rot A., Sobińska M. (2017), *Cloud Computing jako nowy model biznesu. Korzyści, zagrożenia i wyzwania dla zarządzania*, „Ekonomika i Organizacja Przedsiębiorstwa", nr 3(806).
20. Wielki J. (2016), *Analiza szans, możliwości i wyzwań związanych z wykorzystaniem Internetu Rzeczy przez współczesne organizacje gospodarcze*, „Przedsiębiorczość i Zarządzanie", t. 17, z. 11, cz. 1.
21. Zanni T., Bolen K.N., Hanley R., Rios P. (2017), *The Changing Landscape of Disruptive Technologies. Innovation Convergence Unlocks New Paradigms*, KPMG, https://assets.kpmg.com/content/dam/kpmg/jm/pdf/KPMGTechInnovationUnlocksNewParadigms2017web.pdf (dostęp: 28.03.2018).

SCALABILITY, SECURITY AND INTEROPERABILITY AS KEY CHALLENGES FOR DESIGNING THE INTERNET OF THINGS SYSTEMS

Abstract: Market research shows that organizations increasingly recognize the benefits of the Internet of Things. In the business area, it creates new market opportunities, enabling the growth of the efficiency of production and business processes and being an effective communication tool with clients. There are many areas of IoT applications and they can penetrate many aspects of life. However, as it is with the implementation of each new concept, also in relation to the Internet of Things, there are different types of challenges. This is mainly due to the fact that IoT systems are complex solutions based on different types of technologies, and their scale and diversity are very large. From the technological point of view, the Author notices fundamental areas, which are the biggest challenges for IoT. They concern technologies, both in the field of hardware and software, necessary to create the infrastructure of IoT, in particular scalability, interoperability, and flexibility of solutions. Another key issue concerns security. The aim of the article is to present the potential of the discussed concept, but above all to draw attention to the challenges it faces. The applied research methods are a literature review, the analysis of the existing research and selected case studies, as well as the identification and analysis of the most important challenges of this concept.

Keywords: elasticity, Internet of Things, interoperability, scalability, security