en cs de sk es

TECH pedia

INTERNET VĚCÍ

JORDI SALAZAR, SANTIAGO SILVESTRE

Název díla: Internet věcí
Autor: Jordi Salazar, Santiago Silvestre
Přeložil: Jaromír Hrad
Vydalo: České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktní adresa: Technická 2, Praha 6
Tel.: +420 224352084
Tisk: (pouze elektronicky)
Počet stran: 32
Edice (vydání): 1. vydání, 2017

ISBN 978-80-01-06231-9

TechPedia
European Virtual Learning Platform for Electrical and Information Engineering
http://www.techpedia.eu

Erasmus+

Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací odpovídá výlučně autor.
Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

Vysvětlivky

	Definice
	Zajímavost
	Poznámka
	Příklad
	Shrnutí
	Výhody
	Nevýhody

ANOTACE

Tento kurz je úvodem do problematiky internetu věcí (IoT – Internet of Things). V prvních kapitolách najdete základní informace týkající se IoT. Následuje přehled nejdůležitějších vlastností protokolu, který se v oblasti IoT nejčastěji používá, dále pak hlavních aplikací, současného stavu na trhu a technologií, které samotnou existenci IoT umožňují. Závěr je věnován nejdůležitějším problémům, které bude třeba řešit v blízké budoucnosti.

CÍLE

Po absolvování tohoto kurzu studenti porozumí základům IoT a získají přehled o možnostech a aplikacích, které jsou na tomto prostředí založeny.

LITERATURA

[1] R. H. Weber, (2010). "Internet of Things - New Security and Privacy Challenges". Computer Law & Security Review 26: 23-30.

[2] Dave Evans. (2011). How the Next Evolution of the Internet Is Changing Everything. Cisco Internet of Things White Paper.

[3] Stephen E. Deering and Robert M. Hinden (1998). RFC 2460, Internet Protocol, Version 6 (IPv6) Specification.

[4] Charith Perera et. al. (2014). Sensing as a Service Model for Smart Cities Supported by Internet of Things. Transactions on Emerging Telecommunications Technology 25 (1): 81–93.

[5] Ma HD. (2011). “Internet of things: Objectives and scientific challenges”. Journal of computer science and technology 26 (6): 919-924.

[6] In Lee and Kyoochun Lee (2015) “The Internet of Things (IoT): Applications, investments, and challenges for enterprises, *Business Horizons*, 58, 431-440.

[7] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.

[8] Ala Al-Fuqaha et al. (2015) “Internet of Things: A survey on enabling technologies, protocols and applications”, *IEEE Communications Surveys & Tutorials*. DOI 10.1109/COMST.2015.2444095

[9] The European Technology Platform on Smart Systems Integration (2008). "Internet of Things in 2020: A Roadmap for the future"

Obsah

1 Co je internet věcí (IoT)? Definice, historie a vlastnosti IoT

Tato kapitola je věnována některým důležitým milníkům v historii **IoT** (*Internet of Things – internetu věcí*). V současnosti umožňuje informační architektura založená na internetu výměnu služeb a zboží mezi veškerými prvky, zařízeními a objekty připojenými k síti. IoT využívá síťové připojení předmětů každodenní potřeby, které bývají často vybaveny určitým druhem inteligence. V tomto kontextu může být internet platformou, jejímž prostřednictvím různá zařízení elektronicky komunikují a vyměňují si informace s okolním světem. Na IoT tedy můžeme nahlížet jako na skutečnou evoluci všeho, co známe pod názvem internet – s mnohem větší vzájemnou konektivitou, lepším zpracováním informací a dokonalejšími inteligentními službami. V minulosti byl internet většinou využíván pro spojově orientované aplikační protokoly jako **HTTP** (*Hypertext Transfer Protocol*) a **SMTP** (*Simple Mail Transfer Protocol*). Dnes však velké množství inteligentních zařízení komunikuje mezi sebou navzájem, jakož i s dalšími řídicími systémy. Tato koncepce je známa jako **M2M** (*Machine-to-Machine communications – komunikace stroj–stroj*).

IoT (***Internet of Things – internet věcí***) je nově vznikající globální síťová architektura založená na internetu, která usnadňuje výměnu zboží a služeb v rámci globálních dodavatelských sítí a má vliv na bezpečnost a soukromí všech zúčastněných stran [1].

Podívejme se na některé významné milníky ve vývoji IoT:

- Termín „internet věcí“ poprvé použil v roce 1999 Kevin Ashton, který pracoval v oboru síťové RFID (radiofrekvenční identifikace) a nových senzorových technologií.
- Samotný IoT se však „zrodil“ někdy v období 2008 až 2009 [2].
- V roce 2010 dosáhl počet fyzických objektů a zařízení každodenně připojených k internetu zhruba 12,5 miliardy. V současnosti je do IoT zapojeno asi 25 miliard zařízení, což znamená přibližně tři inteligentní („chytrá“) zařízení na každou osobu [2].
- Očekává se, že počet inteligentních zařízení či „věcí“ připojených k IoT vzroste do roku 2020 až na 50 miliard.

IoT představuje skokovou změnu v kvalitě života, neboť nabízí nové možnosti týkající se přístupu k datům, specifických vzdělávacích služeb, bezpečnosti, zdravotní péče či dopravy, abychom jmenovali alespoň některé oblasti. Na druhé straně může být pro firmy klíčem ke zvýšení produktivity, neboť představuje široce distribuovanou síť „chytrých“ zařízení a nových služeb s lokální inteligencí, které mohou být upraveny (personalizovány) podle konkrétních potřeb zákazníků. IoT čerpá své výhody z vylepšeného managementu a sledování pohybu majetku a výrobků. Pracuje s velkým množstvím dat, a umožňuje tak optimalizaci používaného vybavení i využívání zdrojů, což se obojí promítá do úspor. Dále pak

směřuje ke vzniku nových vzájemně propojených inteligentních zařízení a nových obchodních modelů.

2 IPv6

Tato kapitola nabízí základní seznámení s IPv6 (internetovým protokolem verze 6), který je pro IoT klíčový.

2.1 Úvod do IPv6

Ať už používáme internet pro posílání e-mailů, přenos dat, prohlížení webových stránek, stahování souborů, obrázků, videa, nebo pro jakékoli další služby či aplikace, využívá se pro komunikaci mezi jednotlivými síťovými prvky a naším vlastním počítačem, notebookem nebo chytrým telefonem protokol **IP** (*Internet Protocol*), kterým je definován technický formát paketů a systém adresování pro všechna zařízení, která v síti komunikují.

IPv6 (*Internet protocol version 6*) je nejnovější verze protokolu IP, tedy komunikačního protokolu, který představuje systém identifikace a lokalizace pro počítače v síti a slouží ke směrování datového provozu v internetu.

Má-li být jakékoliv zařízení připojeno k internetu, je třeba mu přidělit IP adresu. První verzí internetového protokolu pro veřejné použití byl **IPv4** (*Internet protocol version 4*). Tento protokol byl vyvinut agenturou **DARPA** (*Defense Advanced Research Projects Agency*), která byla založena roku 1958, patří pod americké ministerstvo obrany a zodpovídá za rozvoj nových technologií, zejména pro vojenské účely. IPv4 pracuje se systémem 32bitových číselných adres. Právě délka 32 bitů omezuje celkový počet použitelných adres na přibližně 4,3 miliardy – pro všechna zařízení připojená k internetu na celém světě. Počet těchto zařízení však uvedenou hranici dávno překročil. Proto začalo sdružení **IETF** (*Internet Engineering Task Force*), které se zabývá tvorbou standardů pro internet, již v roce 1998 pracovat na nové verzi IP protokolu. IPv6, který je nástupcem protokolu IPv4, byl poprvé formálně popsán v dokumentu RFC 2460 [3].

IPv6 používá 128bitový formát adresy, takže celkový počet adres může být 2^{128} (přibližně $3{,}4 \cdot 10^{38}$), tedy asi $8 \cdot 10^{28}$ krát více než IPv4. Toto rozšíření adresního prostoru je jedním z nejpodstatnějších přínosů IPv6. Další technologické změny směřující k vylepšení protokolu IP jsou však rovněž důležité – mimo jiné jednodušší správa, lepší směrování pro multicast a efektivnější směrování obecně, jednodušší formát záhlaví, zabudované mechanismy pro autentizaci či podpora soukromí.

Nasazování IPv6 probíhá postupně a po určité přechodné období bude IPv6 používán souběžně se starší verzí IPv4. Klientská zařízení, síťové prvky, aplikace, obsah a služby budou přizpůsobeny novému internetového protokolu verze 6. Kromě toho bude přechod IPv4 na IPv6 znamenat zavedení společné množiny standardů pro použití mezi podniky, vzdělávacími systémy i na celém světě.

IPv6 adresu představuje osm skupin po čtyřech hexadecimálních znacích; skupiny jsou odděleny dvojtečkou. Jelikož adresa je poměrně dlouhá, byly definovány způsoby, jak lze tuto plnou verzi zápisu zkrátit. Formát záhlaví protokolu IPv6 je znázorněn na Obr. 1.

Obr. 1. Formát záhlaví protokolu IPv6 [3]

Struktura záhlaví protokolu IPv6	
Verze	4 bity: verze internetového protokolu = 6
Třída provozu	8 bitů: třída provozu
Značka toku	20 bitů: značka toku
Délka datového bloku	16 bitů: celé číslo bez znaménka – délka bloku užitečných dat, tzn. zbytku paketu následujícího po tomto záhlaví, udávaná v oktetech
Další záhlaví	8 bitů: selektor, který identifikuje typ záhlaví následujícího bezprostředně po záhlaví IPv6; používají se stejné hodnoty jako u protokolu IPv4
Maximální počet skoků	8 bitů: celé kladné číslo, které se sníží o 1 při každém průchodu paketu síťovým uzlem; dosáhne-li hodnoty 0, je paket zahozen
Zdrojová adresa	128 bitů: adresa odesílatele paketu
Cílová adresa	128 bitů: adresa zamýšleného příjemce paketu (nemusí jít o konečného příjemce, je-li přítomno směrovací záhlaví)

Nejdůležitější novinky dané použitím protokolu IPv6 jsou následující: nový formát záhlaví, efektivní a hierarchická infrastruktura pro adresování a směrování, mnohem větší adresní prostor a bezestavová i stavová konfigurace adres, zabezpečení IP, rozšiřitelnost, lepší podpora jakosti služeb (QoS) a nový protokol pro interakci sousedních uzlů.

Protokol IPv6 vyřešil některé z bezpečnostních problémů, které se objevovaly v sítích IPv4, zavedením povinného (dnes již volitelného) používání **IPsec** (*IP Security*). Díky tomu je IPv6 podstatně efektivnější. IPsec rozšiřuje původní IP protokol tím, že zajišťuje autenticitu, integritu, důvěrnost a řízení přístupu pro každý paket s využitím dvou protokolů: **AH** (*Authentication Header*) a **ESP** (*Encapsulating Security Payload*). Kromě toho představuje zvětšení počtu bitů v adresním poli na 128 podstatnou překážku pro útočníky, kteří mají v úmyslu provádět komplexní skenování portů. Na druhé straně je možné vázat veřejný klíč na IPv6 adresu: pak hovoříme o **CGA** (*Cryptographically Generated Address*).

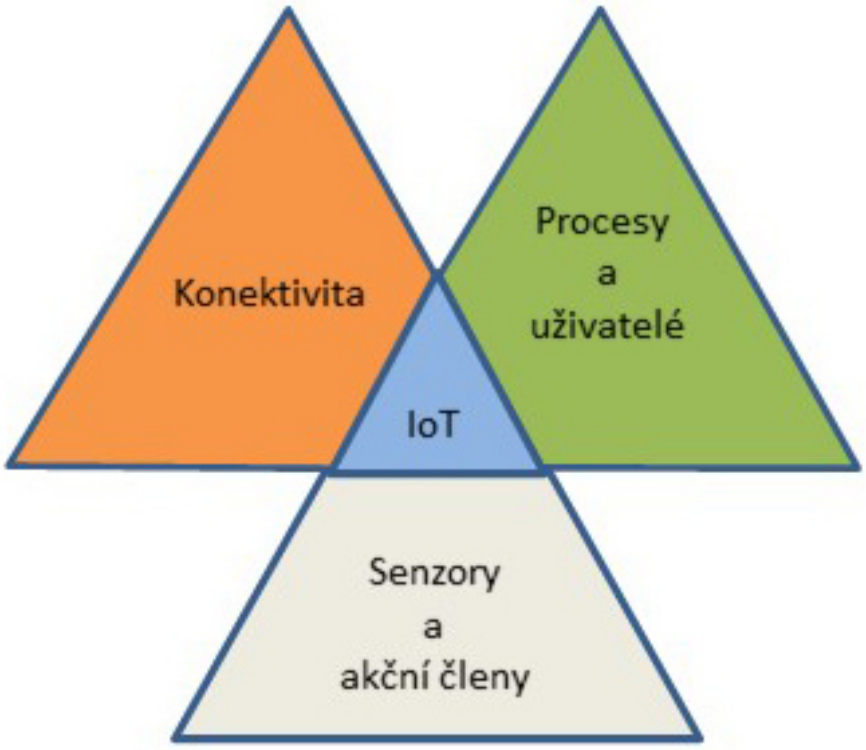
IPv6 přináší také vyšší bezpečnost mobilního připojení. Ačkoliv internetový protokol MobileIP byl k dispozici i v IPv4, v IPv6 je přímo integrovanou, nikoli pouze přidanou novou funkcí jako v IPv4. To znamená, že každý uzel IPv6 může podle potřeby použít mobilní IP. Mobilní IPv6 používá v záhlaví dvě rozšíření: směrovací záhlaví pro registraci a záhlaví cíle pro doručování dat mezi mobilními uzly a odpovídajícími uzly pevnými.

3 Aplikace IoT

V této kapitole jsou popsány některé důležité aplikace, které s IoT souvisejí. Jsou zde rovněž představeny hlavní prvky architektury IoT a očekávaný vývoj na trhu.

3.1 Úvod

IoT můžeme považovat za kombinaci senzorů a akčních členů poskytujících a přijímajících specifické údaje – ty jsou digitalizovány a obousměrně přenášeny prostřednictvím komunikačních sítí, aby mohly být využívány množstvím nejrůznějších služeb a koncových uživatelů [4].



Obr. 2. Koncepce IoT

K objektu či zařízení může být připojeno větší množství senzorů, které pak mohou měřit širokou škálu fyzikálních veličin nebo jevů, a následně předávat získaná data do cloudu. Takové měření můžeme považovat za model služby.

Klasifikace senzoru	
Poskytovatelé snímaných dat	Podnikatelské subjekty, které se samy zabývají nasazováním a správou senzorů
Organizace	Veřejné nebo soukromé. Veřejná infrastruktura. Komerční organizace. Soukromé společnosti. Poskytovatelé technologií a služeb.
Osoby a domácnosti	Mobilní telefony, inteligentní hodinky, gyroskopy, kamery, GPS, akcelerometry, mikrofony, notebooky, stejně jako kuchyňské a domácí spotřebiče, například televizory, kamery, mrazničky, mikrovlnné trouby, myčky nádobí, inteligentní spotřebiče atd.

V současnosti jsou nejmodernější zařízení (obvykle domácí spotřebiče – například chladničky či televizory) vybavena komunikačními a snímacími systémy. Tyto jejich schopnosti se budou nadále rozšiřovat díky využívání inteligentnějších technologií.

Možnosti propojených inteligentních zařízení	
Monitorování	Vnější prostředí. Stav, provoz a využití produktu.
Řízení	Řízení funkcí produktu. Personalizace uživatelských nastavení. Programování.
Optimalizace	Prediktivní diagnostika. Optimalizace výkonnosti produktu. Snižování nákladů.
Autonomie	Autonomní vylepšování a personalizace produktu. Autodiagnostika a autonomní opravy. Koordinace provozu s dalšími produkty.
Efektivní rozhodování	Získávání dat v reálném čase pro správné rozhodování.

Architekturu systémů IoT můžeme rozdělit do čtyř vrstev: vrstvu snímací, vrstvu výměny dat, vrstvu integrace informací a vrstvu aplikačních služeb [5].

V současnosti mohou být inteligentní zařízení propojena pomocí běžného internetového spojení. IoT však obsahuje snímací vrstvu, která snižuje požadavky na schopnosti těchto zařízení a umožňuje jejich vzájemné propojení. Příjemci senzorových dat komunikují se senzory či s jejich majiteli prostřednictvím vrstvy integrace informací, která obstarává veškerou komunikaci a transakce. Mezitím přicházejí nové požadavky a výzvy týkající se výměny dat, filtrování a integrace informací, vymezování nových služeb pro uživatele a složitosti síťové architektury. Kromě toho míra využívání cloudových technologií exponenciálně roste. V internetu věcí jsou nabízeny nové platformy a softwarové aplikace. Mezi hlavní výhody a přínosy IoT bude patřit vytvoření nových efektivnějších služeb a řešení s přidanou hodnotou, spolu se snížením nákladů na sběr dat v rámci stávajících služeb, a možnost vytvářet nové zdroje příjmů v rámci udržitelného obchodního modelu. Tyto aplikace mohou být orientovány na spotřebitele, obchod, reklamu, stejně jako průzkum trhu, průmyslovou a vědeckou komunitu – stačí dát vývojářům správné pokyny.

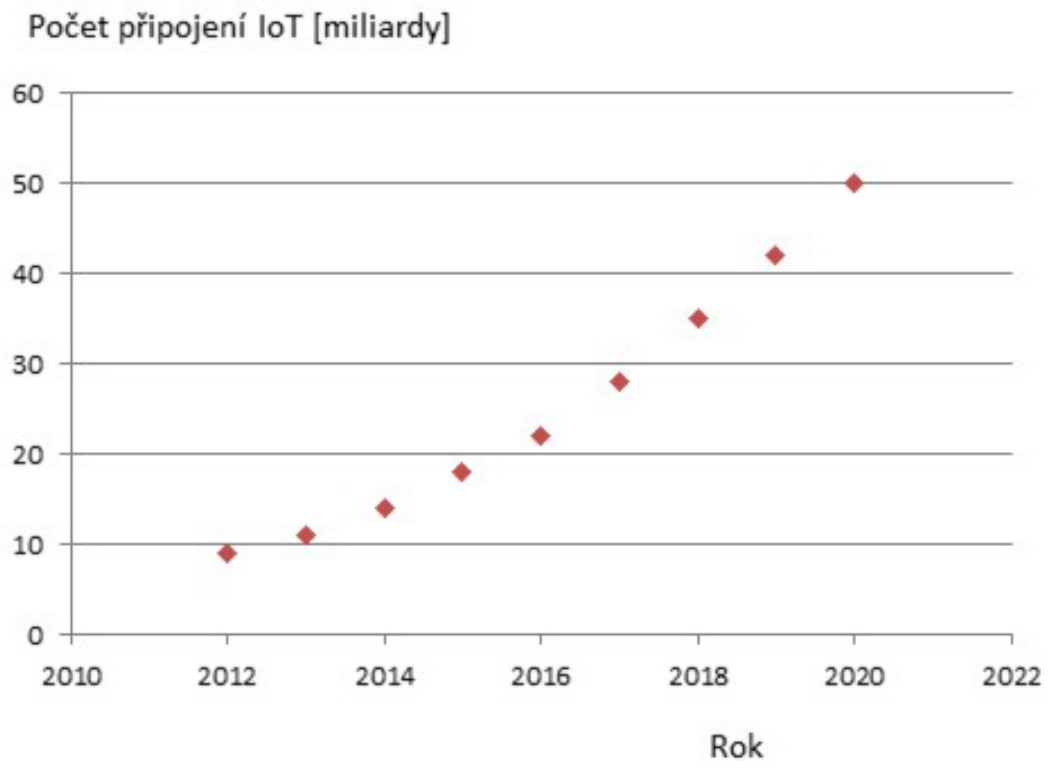
Čtyřvrstvá architektura IoT	
Vrstva snímání objektů	Snímání fyzických objektů a získávání dat.
Vrstva výměny dat	Transparentní přenos dat prostřednictvím komunikačních sítí.
Vrstva integrace informací	Zpracování nejednoznačných informací získaných ze sítí, filtrování nežádoucích dat a transformace klíčových informací do znalostí využitelných službami a koncovými uživateli.
Vrstva aplikačních služeb	Poskytování služeb založených na obsahu koncovým uživatelům.

3.2 Trh IoT

IoT je nově vznikající globální architektura na bázi internetu, která má zjednodušit výměnu zboží v rámci globálních síti dodavatelských řetězců [1]. Jelikož se technologické trendy přesouvají směrem k vyšším přenosovým rychlostem a nižšímu zpoždění přenosu, očekává se zdvojnásobení velikosti internetu každých 5,3 let a cloud computing může v tomto růstu hrát klíčovou roli. Cloud computing je jednou z platforem, které jsou pro podporu IoT klíčové. Většina „věcí“ reálného světa bude integrována do světa virtuálního díky nabídce plnohodnotné konektivity kdykoli a kdekoli.

Cloud computing je model umožňující přístup ke sdílenému souboru konfigurovatelných výpočetních prostředků, který nabízí uživatelům možnost využívat výhody všech dostupných technologií, aniž by museli mít podrobné znalosti o kterékoli z nich.

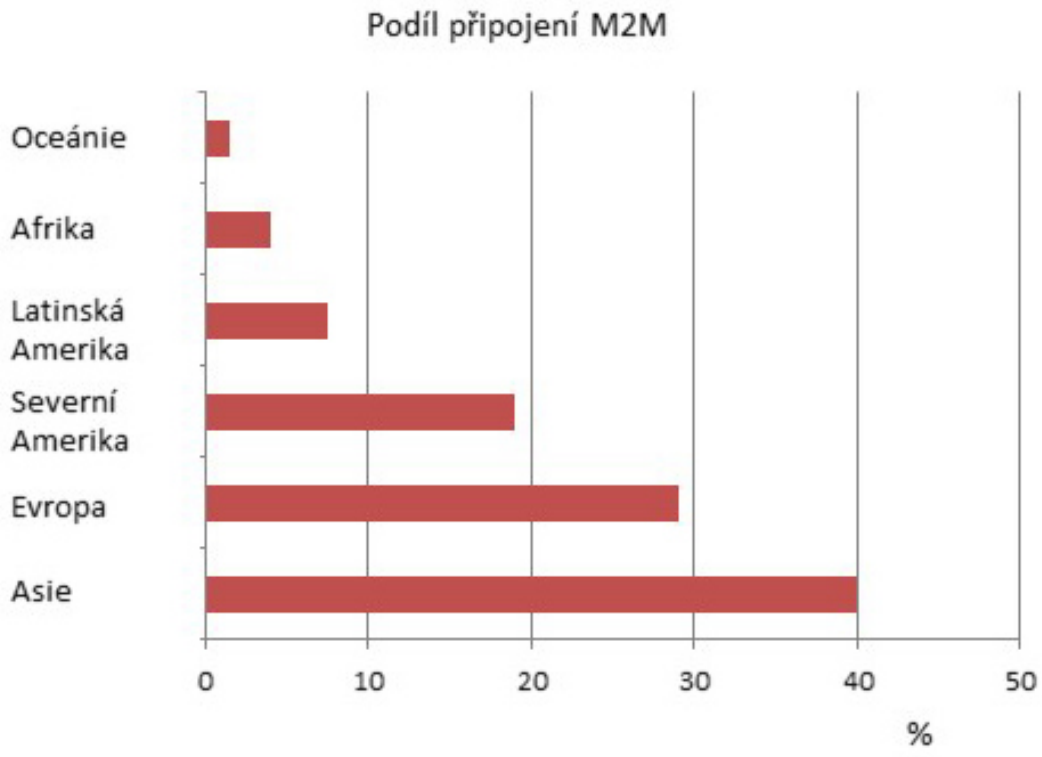
V roce 2010 byl počet fyzických objektů a zařízení každodenně připojených k internetu přibližně 12,5 miliardy. Předpokládá se, že tento počet se do roku 2015 zdvojnásobil na 25 miliard díky nárůstu počtu mobilních zařízení připadajících na osobu, a že se do roku 2020 opět zdvojnásobí na 50 miliard [2].



Obr. 3. Počet připojení IoT [2]

Propojený svět	
31 %	Telefony
29 %	Notebooky
10 %	Inteligentní („chytré“) telefony
8 %	Inteligentní televizory
5 %	Tablety
5 %	Herní konzole
5 %	Multimediální přehrávače
5 %	Čtečky elektronických knih
3 %	Jiné

V současnosti má nejvíce M2M připojení Asie, díky značnému úsilí některých zemí, například Japonska nebo Číny. Technologické společnosti v USA a v Evropě však v oblasti IoT rovněž dělají významné pokroky, takže i zde lze očekávat nárůst trhu i počtu těchto připojení. V návaznosti na vznik tak důležitého fenoménu, jakým je IoT, musí být definovány nové regulační postupy pro zajištění soukromí a bezpečnosti uživatelů i dat.



Obr. 4. Podíl připojení M2M [2]

3.3 Aplikace

IoT může nabídnout prakticky neomezené množství aplikací a služeb přizpůsobených pro mnoho oblastí lidské činnosti – může různými způsoby usnadňovat život a zvyšovat jeho kvalitu. Tato kapitola předkládá stručný seznam aplikací a služeb založených na IoT. Obsahuje však jen jejich základní popis, jehož cílem je ozřejmit, o jaké nejrůznější aplikace a služby se vlastně v IoT jedná. Odhadovaná hodnota, které IoT aplikace a služby dosáhnou do roku 2020, je 19 biliónů dolarů.

Aplikace a služby IoT:

- Připojené inteligentní budovy: Zlepšení účinnosti (management spotřeby a úspora energie) a bezpečnosti (senzory a alarmy). Domovní aplikace včetně inteligentních senzorů a akčních členů pro řízení domácích spotřebičů. Služby domácí péče o zdraví a vzdělávání. Dálková kontrola péče o pacienty. Kabelové/satelitní služby. Systémy ukládání/výroby energie. Automatické vypínání elektroniky v době, kdy není používána. Inteligentní termostaty. Detektory a hlásiče kouře. Aplikace pro řízení přístupu (do budov a místností). Inteligentní dveřní zámky. Senzory zabudované do infrastruktury budov pro navádění záchranných složek. Bezpečnost pro všechny rodinné příslušníky.

- Inteligentní města a dopravní systémy: Integrace bezpečnostních služeb. Optimalizace veřejné a soukromé dopravy. Parkovací senzory. Inteligentní správa parkovacích služeb a provozu v reálném čase. Inteligentní řízení semaforů v závislosti na hustotě provozu. Identifikace vozidel, která překročila povolenou dobu parkování. Inteligentní energetické sítě. Zabezpečení (kamery, inteligentní senzory, informace pro občany). Vodohospodářství. Zavlažování parků a zahrad. Inteligentní odpadové nádoby. Kontrola znečištění. Získávání okamžité zpětné vazby a názorů od občanů. Inteligentní veřejná správa. Volební systémy. Monitorování nehod, koordinace záchranných akcí.

Obr. 5. Příklad aplikací IoT: Inteligentní města

- Vzdělávání: Propojení virtuálních a fyzických učeben pro zajištění efektivnějšího a dostupnějšího vzdělávání, e-learning. Služby přístupu k virtuálním knihovnám a vzdělávacím portálům. Výměna zpráv a výsledků v reálném čase. Celoživotní vzdělávání. Výuka cizím jazykům. Správa docházky.

- Spotřební elektronika: Inteligentní telefony. Inteligentní TV. Notebooky, počítače a tablety. Inteligentní ledničky, myčky a sušičky. Inteligentní systémy domácího kina. Inteligentní spotřebiče. Obojkové (pet collar) senzory. Personalizace uživatelských nastavení. Autonomní provoz zařízení. Osobní lokátory. Inteligentní brýle.

- Zdraví: Monitorování chronických onemocnění. Zlepšování kvality péče a kvality života pacientů. Sledovače činností. Vzdálená diagnostika. Připojené náramky. Interaktivní pásy. Monitorováni sportovních aktivit. Inteligentní štítky na léky. Kontrola užívání léků. Biočipy. Rozhraní mozek-počítač. Monitorování stravovacích návyků.

- Automobilismus: Inteligentní automobily. Řízení provozu. Pokročilá diagnostika vadných součástí. Bezdrátové sledování tlaku vzduchu v pneumatikách. Inteligentní sledování a řízení spotřeby energie. Autodiagnostika. Akcelerometry. Senzory polohy, přítomnosti a přiblížení.

Analýza optimální cesty k cíli v reálném čase. Sledování GPS. Řízení rychlosti vozidla. Autonomní vozidla využívající služby IoT.

- Zemědělství a životní prostředí: Měření a monitorování znečistění životního prostředí (CO2, hluk, různé druhy kontaminace prostředí). Předpovídání klimatických změn s využitím inteligentních senzorů. Pasivní RFID štítky na zemědělských produktech. Senzory v paletách na produkty. Odpadové hospodářství. Určování nutriční hodnoty.

- Energetické služby: Přesné údaje o spotřebě energie. Inteligentní měření (Smart Metering). Inteligentní sítě (Smart Grids). Analýza a predikce chování a vzorců týkajících se spotřeby energie. Předpovídáni budoucích energetických trendů a potřeb. Bezdrátové senzorové sítě. Získávání energie (energy harvesting) a její recyklace.

- Inteligentní připojení: Správa dat a poskytování služeb. Využití sociálních sítí a médií. Přístup ke službám e-mailu, přenosu hlasu a videa. Interaktivní skupinová komunikace. Streaming v reálném čase. Interaktivní hry. Rozšířená realita. Sledování zabezpečení sítě. Nositelná uživatelská rozhraní. Rozpoznávání emocí. Biometrické metody autentizace. Spotřebitelská telematika. Komunikační služby M2M. Analýza velkých dat. Virtuální realita. Služby cloudu. Všudypřítomné počítače. Počítačové vidění. Inteligentní antény.

- Výroba: Snímače průtoku plynu a kapalin. Inteligentní senzory vlhkosti, teploty, pohybu, síly, zatížení, úniku/hladiny. Strojové vidění. Snímání hluku a vibrací. Složené aplikace. Inteligentní řízení robotů. Řízení a optimalizace výrobních procesů. Rozpoznávaní vzorů. Strojové učení. Prediktivní analýza. Mobilní logistika. Skladové hospodářství. Prevence nadvýroby. Efektivní logistika.

- Nakupovaní: Inteligentní nakupování. RFID a jiné elektronické štítky a čtečky. Čárové kódy v maloobchodě. Řízení zásobování. Kontrola geografického původu potravin a dalších produktů. Kontrola kvality a nezávadnosti potravin.

4 Klíčové technologie

Úspěšné uplatnění koncepce IoT v reálném světě je podmíněno pokrokem v oblasti technologií na nižších úrovních. V této části budou probrány nejrelevantnější podpůrné technologie, abychom získali ucelený obraz o roli, kterou budou v rámci IoT pravděpodobně mít [6], [7].

4.1 Energie

Technologie pro ukládání energie patří k těm, které umožňují nasazení aplikací IoT. Otázky energetiky ve všech jejích fázích, od získávání či výroby přes skladování až po využívání, jsou klíčové pro rozvoj IoT. Od těchto technologií se očekávají řešení pro získávání a výrobu energie s vysokou hustotou, která ve spojení s dnešní nanoelektronikou o nízké spotřebě umožní konstrukci samonapájecích bezdrátových identifikovatelných zařízení na bázi inteligentních senzorů. Stále trvá potřeba výzkumu a vývoje v této oblasti (nanoelektronika, polovodiče, senzorová technika, mikrosystémová integrace), jejichž cílem jsou jednak zařízení s ultranízkou spotřebou, jednak účinnější a kompaktní úložiště energie jako baterie, palivové články a tištěné/polymerové baterie. Současná zařízení nevyhovují budoucím kritériím týkajícím se zejména potřebného výpočetního výkonu a omezené energetické spotřeby. Kromě toho nám systémová integrace pomůže zvýšit účinnost stávajících systémů a nabídne celou řadu řešení pro potřeby budoucnosti.

4.2 Senzory

Senzory jsou jedním z klíčových stavebních prvků IoT. Coby všudypřítomné systémy mohou být nasazeny prakticky kdekoli. Lze je též implantovat pod kůži člověka, mohou být instalovány do peněženky či na tričko. Některé z nich měří jen čtyři milimetry, ale data, která snímají, můžeme přijímat na vzdálenost stovek kilometrů. Doplňují lidské smysly a staly se nenahraditelnými v řadě odvětví, od zdravotní péče po strojírenství. Jejich nespornou výhodou je schopnost předvídat potřeby lidí na základě kontextových informací získaných z jejich okolí. Inteligence těchto systémů, podpořená síťovou konektivitou, jim umožňuje nejen informovat o stavu jejich vnějšího prostředí, ale i provádět potřebné činnosti bez zásahu člověka.

Miniaturizované křemíkové čipy jsou navrhovány s novými možnostmi, v menších rozměrech, s vyšším výpočetním výkonem a lepší účinností. Náklady klesají ve shodě s Mooreovým zákonem. Cena za šířku pásma rovněž klesla, a stejně tak i náklady na zpracování. Tak lze větší počet zařízení nejen navzájem propojit, ale i vybavit dostatečnou inteligencí k tomu, aby mohla správně naložit se všemi daty, která poskytují nebo dostávají.

Takové schopnosti jako znalost kontextu a vzájemná komunikace mezi stroji jsou pro IoT velkou prioritou. Dalšími prioritami jsou pak integrace paměti a výpočetního výkonu, schopnost odolávat nežádoucím vnějším vlivům a cenově dostupné zabezpečení. Mezi klíčové technologie můžeme počítat i vývoj nízkoenergetických procesorových/mikrokontrolérových jader určených speciálně pro mobilní zařízení IoT a novou třídu jednoduchých a dostupných inteligentních systémů zaměřených na IoT. Řešení v tomto směru se bude pohybovat od mikroprogramových konečných automatů po mikrokontroléry. Konkrétní volba je kompromisem mezi flexibilitou, programovatelností, plochou čipu a spotřebou elektrické energie. Tato zařízení vyžadují nějaký druh stálé paměti (EEPROM/FRAM/polymer), bez ohledu na to, zda bude vypálena laserem při výrobě, jednorázově programovatelná nebo elektricky přepisovatelná. Přepisovatelné energeticky nezávislé paměti jsou doporučovány vzhledem k vysoké propustnosti dosažené během výrobních zkoušek; navíc v sobě spojují funkce uživatelské paměti, programové paměti a úložiště pro data snímaná senzory.

4.3 Cloud computing

Cloud computing je model přístupu ke sdíleným konfigurovatelným zdrojům na požádání (jde například o počítače, sítě, servery, úložiště, aplikace, služby, software), a to buď v podobě infrastruktury jako služby (**IaaS** – *Infrastructure as a Service*), nebo software jako služby (**SaaS** – *Software as a Service*). Jedním z nejzávažnějších důsledků zavádění IoT je enormní množství dat generovaných zařízeními připojenými k internetu [7]. Mnohé z aplikací IoT vyžadují obrovská úložiště dat, velkou rychlost zpracování kvůli schopnosti rozhodování v reálném čase a vysokorychlostní širokopásmové sítě pro streaming dat nebo audiovizuálních informací. Cloud computing nabízí ideální back-end řešení pro nakládání s velkými datovými toky a jejich zpracování v reálném čase pro bezprecedentní počet IoT zařízení i lidí.

4.4 Komunikace

Nové inteligentní vícepásmové antény integrované na čipu a vyrobené z nových materiálů jsou prostředky, které umožní zařízením vzájemnou komunikaci. Antény umístěné přímo na čipu musí být optimalizovány co do velikosti, ceny a účinnosti. Mohou být dostupné v různých formách – jako cívky na čipu, tištěné antény, vestavěné antény a vícenásobné antény – díky použití různých substrátů a 3D struktur. Vzhledem ke snahám využívat energeticky úsporné komunikační protokoly pro vícepásmový přenos je třeba řešit i otázky týkající se použitých modulačních schémat a přenosových rychlostí. Komunikační protokoly budou navrženy pro webově orientované architektury platformy IoT, kde jsou všechny objekty, bezdrátová zařízení, kamery, počítače atd. zkombinovány, aby bylo možno analyzovat umístění, záměry, a dokonce i emoce prostřednictvím sítě. Je zapotřebí nových metod efektivního řízení spotřeby energie na různých úrovních sítě, od směrování až po architekturu jednotlivých zařízení.

4.5 Integrace

Integrace inteligentních zařízení do obalů, či ještě lépe do samotných výrobků, umožní značné snížení nákladů a zvýšení šetrnosti k životnímu prostředí. Bude pokračovat trend integrace čipů a antén do nestandardních nosičů, jako je například textil a papír, a vývoje nových typů nosičů, vodivých cest a spojovacích materiálů, které budou vhodné do náročných provozních podmínek a ekologicky zlikvidovatelné. Technologie **SiP** (*System-in-Package*) umožňuje flexibilní a 3D integrovat do obalu různé prvky, jako jsou antény, senzory, aktivní i pasivní součástky, což vede ke zvýšení výkonnosti a snížení nákladů. RFID vložky páskovými vodiči se používají k propojení čipů a antén; tak lze dosáhnout nejrůznějších tvarů a velikostí etiket, které pak není nutno přidávat dodatečně.

4.6 Standardy

IoT zařízení jsou velmi rozmanitá a měří nejrůznější parametry podle různých standardů a v jim odpovídajících jednotkách. Ačkoli v současnosti stále vznikají konkurenční proprietární protokoly, je pravděpodobné, že cestou k interoperabilitě se stanou řešení založená na otevřených standardech.

Je zřejmé, že otevřené standardy jsou klíčové pro úspěch bezdrátových komunikačních technologií, stejně jako pro jakýkoliv typ komunikace stroj-stroj obecně. Pro nasazování aplikací IoT je nezbytné rychlejší zavádění standardů zajišťujících interoperabilitu. Je třeba ujasnit požadavky týkající se jednoznačné identifikace, přidělování jmen (adres) a jejich překladu v globálním měřítku. V nejbližší budoucnosti bude nutno řešit otázky týkající se nedostatečného popisu obecných referenčních modelů, referenční architektury pro tzv. sítě budoucnosti, internet budoucnosti a IoT, a rovněž integrace starších systémů a sítí.

5 Problémy a překážky IoT

Stále zůstává k dořešení řada důležitých otázek. Nalezení správných odpovědí bude pro poskytovatele služeb a programátory aplikací důležitým vodítkem na cestě k efektivním řešením. V následujícím textu nabídneme stručnou diskusi týkající se nejdůležitějších problémů, s nimiž se během vývoje a zavádění IoT musíme vypořádat [8].

5.1 Problémy

Spolehlivost

Spolehlivost má za cíl zvýšit úspěšnost poskytování služeb IoT. Má blízký vztah s dostupností, jelikož jejím smyslem je zaručit dostupnost informací a služeb v daném časovém období. Spolehlivost je dokonce ještě důležitější a má přísnější požadavky, pokud se jedná o oblast aplikací pro nouzové situace. Klíčovou součástí těchto systémů je komunikační síť, která musí být dostatečně odolná vůči chybám, aby byl zajištěn spolehlivý přenos informací. Spolehlivost musí být implementována softwarově i hardwarově na všech vrstvách IoT. Mají-li služby IoT fungovat efektivně, pak komunikace, která je jejich základem, musí být spolehlivá, neboť například nespolehlivé snímání, sběr dat, jejich zpracování a přenos mohou vést k velkým zpožděním, ztrátě dát, a následně k chybným rozhodnutím; to může mít za následek až katastrofální dopady a ve výsledku i nižší spolehlivost IoT.

Spolehlivost znamená správnou funkci systému ve shodě s jeho specifikacemi.

Výkonnost

Hodnocení výkonnosti služeb IoT je velká výzva, jelikož se odvíjí od výkonnosti mnoha různých komponent a také od výkonnosti technologií, na nichž IoT stojí. IoT, stejně jako jiné systémy, se musí neustále rozvíjet a zlepšovat své služby, aby byly uspokojeny požadavky zákazníků. Stav zařízení pro IoT musí být monitorován a vyhodnocován, aby poskytovala zákazníkům nejlepší možné služby za dostupnou cenu. Pro hodnocení výkonnosti IoT je možno použít mnoho různých metrik – mimo jiné například rychlost procesoru, komunikační rychlost, provedení zařízení či jeho cenu.

Popis hodnocení výkonnosti jednotlivých dílčích protokolů a technologií, protokolů aplikační vrstvy a QoS lze nalézt v literatuře. Otevřenou otázkou však i nadále zůstává chybějící důkladné hodnocení výkonnosti aplikací IoT.

Jakost služby (**QoS** – *Quality of Service*) je celková výkonnost telefonní či počítačové sítě, zejména z pohledu jejího uživatele.

Interoperabilita

Dalším důležitým problémem IoT je interoperabilita od konce ke konci, a to vzhledem k potřebě obsáhnout velké množství nejrůznějších objektů na různých platformách. Na potřebnost interoperability musí pamatovat vývojáři aplikací i výrobci IoT zařízení, aby bylo poskytování služeb zajištěno pro všechny zákazníky, bez ohledu na specifické vlastnosti hardwarové platformy, kterou používají. Například většina dnešních inteligentních telefonů podporuje běžné komunikační technologie, jako je Wi-Fi, NFC a GSM, aby byla zajištěna interoperabilita v různých prostředích a situacích. Programátoři IoT by měli své

aplikace navrhovat s možností snadného přidávání nových funkcí, aniž by tyto způsobovaly problémy či ztrátu funkcí, při zachování integrace s různými komunikačními technologiemi. Proto je interoperabilita významným kritériem při návrhu a zavádění IoT služeb, aby byly splněny požadavky zákazníků. Kromě celé řady protokolů představují v tomto směru výzvu i různé interpretace týchž standardů implementované různými společnostmi. Vhodným opatřením, které pomáhá podobným nejednoznačnostem předcházet, je testování vzájemné interoperability mezi různými produkty například s využitím platformy ETSI Plugtest. Cílem výzkumného projektu PROBE-IT je zase zajištění interoperability ověřených IoT řešení s využitím testů interoperability, jako je CoAP či 6LoWPAN, a sémantické interoperability IoT.

Jak známo, dvě různá zařízení nemusí spolupracovat ani tehdy, splňují-li stejné standardy. To je pravděpodobně největší překážka pro masivní nasazení technologií IoT. Zařízení budoucnosti v sobě musí spojovat různé komunikační standardy a protokoly, které využívají různá frekvenční pásma a podporují různé architektury, ať už centralizované, nebo distribuované, musí být schopna komunikovat s jinými sítěmi, dokud nevzniknou globální a propracované standardy.

Bezpečnost a soukromí

Bezpečnost je dalším významným problémem při implementaci IoT, a to kvůli nedostatku společných standardů a architektury. V heterogenních sítích, podobně jako v případě IoT, není snadné zajistit bezpečnost a soukromí uživatelů. Klíčová funkcionalita IoT je založena na výměně informací mezi miliardami, či dokonce bilióny objektů připojených k internetu. Jedním z otevřených problémů týkajících se bezpečnosti IoT, který dosud nebyl v rámci standardů ošetřen, je distribuce klíčů mezi zařízeními. Otázky soukromí a operace přístupu k profilům mezi zařízeními IoT s vyloučením neautorizovaných zásahů jsou přitom velmi naléhavé. Zabezpečení vzájemné výměny dat proto zůstává nezbytným krokem, jenž má zabránit ztrátě či ohrožení soukromí. Neustále rostoucí počet inteligentních objektů, které pracují s citlivými daty, vyžaduje transparentní a jednoduché řízení přístupu, tak, aby například jeden prodejce směl údaje pouze číst, zatímco jiný mohl příslušné zařízení ovládat. V tomto směru již bylo navrženo několik řešení, například seskupovat vestavná zařízení do virtuálních sítí a v každé z těchto sítí zpřístupňovat pouze požadovaná zařízení. Další možností je podpora řízení přístupu na aplikační vrstvě podle jednotlivých prodejců.

Správa

Propojení miliard až biliónů inteligentních zařízení staví poskytovatele služeb před obrovské problémy týkající se řízení chyb, konfigurace, účtování, výkonnosti a bezpečnosti (Fault, Configuration, Accounting, Performance and Security – FCAPS) těchto zařízení. Snaha o řízení těchto aspektů vyžaduje vývoj nových nenáročných protokolů pro správu, aby bylo možno zvládnout manažerskou noční můru, která může potenciálně nastat v nejbližších letech po nasazení IoT. Správa zařízení a aplikací IoT se může stát účinným nástrojem pro růst IoT. Například monitorování M2M komunikace objektů IoT je důležité kvůli zajištění nepřetržité konektivity pro poskytování služeb na požádání. Standard pro „odlehčenou“ M2M komunikaci (Light-Weight M2M – LWM2M), který je vyvíjen sdružením Open

Mobile Alliance, má za cíl vytvořit rozhraní mezi M2M zařízeními a M2M servery, a tím i aplikačně nezávislý systém pro správu široké škály různých zařízení. Takový systém pak nabídne aplikacím M2M možnost vzdálené správy M2M zařízení, služeb a dalších aplikací. Protokol NETCONF Light je výsledkem snah IETF (Internet Engineering Task Force) o řešení pro správu zařízení s omezenými funkcemi. Definuje postupy pro instalaci, změny a mazání konfigurace síťových zařízení. Může rovněž sloužit ke správě širokého spektra zařízení – od těch, která disponují omezenými zdroji, až po plně vybavená. Nezávisle vyvíjená platforma MASH IoT je příkladem systému, který usnadňuje správu (sledování, řízení a konfiguraci) zdrojů IoT, a to kdekoli a v reálném čase, s využitím IoT ovládacího panelu na inteligentních telefonech. Vhodnou správu vyžaduje rovněž udržování kompatibility napříč vrstvami IoT, a to kvůli optimalizaci rychlosti připojení a zajištění bezchybného poskytování služeb. Pracovní skupina pro správu zařízení v rámci sdružení Open Mobile Alliance (OMA) vytváří specifikace protokolů a postupů pro správu mobilních zařízení a služeb v prostředí s omezenými zdroji.

Výroba

Problémy, kterým čelí výrobní sektor, musí být řešeny přesvědčivě. Náklady na jeden pasivní RFID štítek (tag) musí klesnout pod jeden cent a produkce musí dosáhnout mimořádně vysokého objemu; celý výrobní proces však musí mít jen minimální dopady na životní prostředí, musí být založen na recyklaci a opakovaném využívání, a zohledňovat kompletní životní cyklus digitálních zařízení i dalších výrobků, které mohou být opatřeny visačkami či jinak podporovat senzorové technologie.

5.2 Překážky

Pro IoT však existují i překážky, zejména v oblasti předpisů, zabezpečení a bezpečnosti. Hlavním cílem je lépe chránit soukromí lidí a donutit firmy, aby využívaly zabezpečené způsoby správy dat [8], [9].

Absence dohledu

Neexistence dohledu je jednou z významných překážek, které brání širšímu rozmachu technologie internetu věcí. Dokud nebude ustanoven nezávislý dohledový orgán, nebude možno dosáhnout skutečně globálního IoT, který by byl uznáván a přijímán vládami, firmami, obchodními organizacemi a obyvatelstvem. V současnosti neexistuje jednotný a univerzální číslovací systém; EPCglobal a Ubiquitous Networking Lab prosazují dva odlišné a nekompatibilní způsoby identifikace objektů, a existuje reálné nebezpečí, že si v následujících letech budou na světovém trhu konkurovat. Dále je třeba udržovat dohled v co nejširším kontextu, protože zavádění samostatných dohledových orgánů pro každou specifickou oblast by vedlo ke kompetenčním sporům a zmatku ve standardech. Objekty mohou mít různé identity pro různý kontext; existence vícerých dohledových orgánů by tedy způsobila jistý druh vícenásobného směrování (multi-homing), což by mohlo vést až ke katastrofálním důsledkům.

Soukromí a zabezpečení

Má-li se jakýkoliv systém identifikace objektů stát všeobecně přijímaným, musí být založen na kvalitním technickém řešení, které je schopno zaručit soukromí a bezpečnost zákazníků. Jelikož v mnoha případech bylo zabezpečení realizováno dodatečně jako přídavná funkce, převládá dojem, že internet věcí bude veřejností akceptován pouze tehdy, budou-li pro něj existovat dostatečně robustní řešení pro bezpečnost a soukromí. Zejména je třeba zachytávat útoky, autentizovat data, řídit přístup a zaručit soukromí zákazníků (fyzických i právnických osob). Může se jednat o hybridní bezpečnostní mechanismy, které například kombinují hardwarové zabezpečení s diverzifikací klíčů. Tak lze zajistit vynikající úroveň zabezpečení, která případné útoky značně ztěžuje, nebo dokonce zcela znemožňuje. Výběr bezpečnostních funkcí a mechanismů bude i nadále záviset na jejich vlivu na obchodní procesy; vždy se bude hledat kompromis mezi velikostí čipů, cenou, funkcionalitou, interoperabilitou, bezpečností a soukromím.

Problémy týkající se bezpečnosti a soukromí by měly být řešeny v budoucích standardech, které musí definovat dílčí bezpečnostní funkce pro podporu důvěrnosti, integrity či dostupnosti služeb.

Existuje také celá řada problémů týkajících se identity osob. Ty je třeba řešit v rámci politiky a legislativy, neboť jsou klíčové pro efektivní fungování veřejné správy v budoucnosti.

6 Budoucnost IoT

Pro období nejbližších let je možno určit čtyři hlavní trendy, které budou určovat podobu internetových technologií společně s prudkým nástupem všudypřítomných zařízení vytvářejících budoucí internet věcí [9]:

1. V první řadě jde o tzv. „exaflood“ neboli „záplavu dat“, tedy explozivní nárůst objemu sbíraných a navzájem vyměňovaných dat. Jelikož současné sítě nejsou na takovýto exponenciální nárůst provozu připraveny, je třeba, aby všechny zúčastněné strany důkladně zvážily úpravy současné architektury sítí a úložišť. Bude vrcholně důležité nalézt nové způsoby a mechanismy pro vyhledávání, získávání a přenos dat. Jednou z podstatných příčin této datové záplavy je extrémní nárůst počtu zařízení sbírajících a vyměňujících si informace, jak se internet věcí postupně stává realitou.

Pojem **exaflood** zavedl Bret Swanson z Nadace pro pokrok a svobodu (Progress & Freedom Foundation); označuje se jím rostoucí objem datových toků na internetu.

2. Množství energie potřebné k provozu inteligentních zařízení dramaticky poklesne. Již dnes dosáhla mnohá datová centra maximální možné úrovně spotřeby energie, takže přidávání nových zařízení je kategoricky podmíněno vyřazováním starých. Zde tedy můžeme spatřovat druhý trend, který se týká veškerých zařízení a systémů – od nejmenšího inteligentního „prachu“ až po obrovská datová centra: hledání nulové entropie jakožto stavu, kdy zařízení či systém bude získávat energii od sebe sama.

3. Miniaturizace zařízení rovněž probíhá překvapivě rychle. Přibližujeme se k cíli v podobě jednoelektronového tranzistoru. To se zdá být nejzazší hranicí, alespoň dokud nedojde k novým převratným objevům na poli fyziky.

4. Další důležitý trend ukazuje k autonomním zdrojům. Neustále rostoucí složitost systémů se časem stane nezvládnutelnou a bude bránit vzniku nových služeb a aplikací, pokud systémy nezačnou disponovat určitým druhem samostatnosti – například samo-spravovatelností, samo-opravitelností a samo-konfigurovatelností.

Vzhledem k tomu, že integrace technologií do fyzických objektů se postupně stává levnějším řešením, budeme pozorovat větší využití i přijetí IoT, následkem čehož pak bude IoT mít v následujících letech výrazné dopady na firmy podnikající jak směrem k dalším firmám (business-to-business – B2B), tak ke koncovými zákazníkům (business-to-consumer – B2C).