en cs de sk es

TECH pedia

INTERNET VECÍ

JORDI SALAZAR, SANTIAGO SILVESTRE

Názov: Internet vecí
Autor: Jordi Salazar, Santiago Silvestre
Preložil: Ivan Drozd, Ivan Minárik, Marek Vančo
Vydalo: České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktná adresa: Technická 2, Praha 6, Česká republika
Tel.: +420 224352084
Tlač: (iba elektronická)
Počet strán: 32
Edícia (vydanie): 1. vydanie, 2017

ISBN 978-80-01-06235-7

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

Erasmus+

Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

VYSVETLIVKY

	Definícia
	Zaujímavosť
	Poznámka
	Príklad
	Zhrnutie
	Výhody
	Nevýhody

ANOTÁCIA

Jedná sa o úvodný kurz do oblasti Internetu vecí (IoT, Internet of things). V prvých kapitolách sú načrtnuté základné informácie o IoT. Neskôr sa kurz venuje internetovému protokolu verzie 6 (IPv6), ktorý je najpoužívanejší v prostredí IoT a ďalej kurz charakterizuje hlavné aplikácie, súčasný stav na trhu a technológie, ktoré umožňujú existenciu IoT. Nakoniec sú diskutované výzvy a prekážky, ktoré sa javia ako najdôležitejšie v spojitosti s rozmachom siete IoT.

CIELE

Na konci štúdia tohto kurzu bude študent schopný porozumieť základom IoT, dôležitým otázkam týkajúcim sa prenosu a bude schopný identifikovať hlavné zariadenia a aplikácie ako aj základné výzvy a prekážky spojené s nasadením IoT.

LITERATÚRA

[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 Čo je Internet vecí (IoT)? Definícia, história a vlastnosti IoT.

Táto kapitola opisuje dôležité míľniky z histórie **IoT** (*Internet of things*). V súčasnosti architektúra založená na Internete dovoľuje výmenu služieb a tovarov medzi prvkami, zariadeniami a objektami pripojenými do siete. IoT sa odvoláva na sieťové pripojenie každodenných objektov, ktoré sú často vybavené určitým druhom inteligencie. V tomto kontexte môže byť Internet taktiež platforma pre zariadenia na elektronickú komunikáciu, zdieľanie informácií a špecifických dát so svetom okolo nich. Takže IoT môže byť vnímaný ako reálna evolúcia toho, čo rozumieme pod slovom Internet. Internet bol z väčšej časti využívaný na spojovo orientované aplikačné protokoly ako **HTTP** (*Hypertext Transfer Protocol*) a **SMTP** (*Simple Mail Transfer Protocol*). Napriek tomu v dnešnej dobe veľké množstvo inteligentných zariadení komunikuje medzi sebou a ďalšími riadiacimi systémami. Tento koncept je známy ako **M2M** (*Machine-to-Machine communications*).

IoT (Internet of things) je novo vznikajúca globálna Internetovo založená technická architektúra zľahčujúca výmenu tovarov a služieb v globálnych dodávateľských sieťach a má vplyv na bezpečnosť a súkromie zúčastnených strán [1].

Niektoré významné míľniky v histórii IoT:

- Pojem Internet vecí bol prvýkrát použitý Kevinom Ashtonom v roku 1999, ktorý pracoval v oblasti sieťovej **RFID** (*radio frequency identification*) a vznikajúcich snímacích technológií.
- Samotný IoT sa zrodil niekedy medzi rokmi 2008 a 2009 [2].
- V roku 2010 bol počet každodenne pripojených fyzických objektov a zariadení do Internetu okolo 12,5 miliardy. V súčasnosti je do IoT pripojených okolo 25 miliárd zariadení. Takmer jedno inteligentné zariadenie na osobu [2].
- Očakáva sa, že počet inteligentných zariadení alebo "vecí všeobecne" pripojených do IoT sa do roku 2020 zväčší na viac ako 50 miliárd.

IoT predstavuje zmenu v kvalite života jednotlivca tým, že ponúka nové príležitosti prístupu k dátam, špecifické služby vo vzdelávaní, bezpečnosť, starostlivosť o zdravie alebo okrem iného aj dopravu. Na druhej strane bude kľúčový pre firmy na zvýšenie produktivity tým, že budú ponúkať široko distribuované lokálne inteligentné siete inteligentných zariadení a nových služieb, ktoré môžu byť personalizované podľa potrieb zákazníka. IoT prináša výhody vylepšeného riadenia a sledovania majetku a produktov. Zvyšuje množstvo informačných dát a dovoľuje optimalizáciu zariadení a využívania prostriedkov, ktoré môžu byť premietnuté do úspor. Navyše ponúka možnosť vytvoriť nové inteligentné prepojené zariadenia a preskúmať nové obchodné modely.

2 IPv6

Táto kapitola poskytuje základný úvod do protokolu IPv6: Internetový protokol verzie 6, ktorý je nevyhnutný pre IoT.

2.1 Úvod do IPv6

Keď používame Internet, či už je to odosielanie e-mailov, prenos dát, prehliadanie webových stránok, sťahovanie súborov, obrázkov, videa resp. na akékoľvek iné služby alebo aplikácie, na komunikáciu medzi rôznymi sieťovými prvkami a naším vlastným počítačom, notebookom alebo inteligentným telefónom sa využíva protokol **IP** (*Internet Protocol*), ktorý špecifikuje technický formát paketov a adresovanie pre počítače komunikujúce v sieti.

IPv6 (*Internet protocol version 6*) je najnovšia verzia protokolu IP, komunikačného protokolu, ktorý poskytuje systém identifikácie a lokalizácie pre počítače v sieti a smerovanie na Internete.

Aby bolo možné pripojiť akékoľvek zariadenie k Internetu je nutné prideliť tomuto zariadeniu IP adresu. Prvá verzia verejne použitého internetového protokolu bola **IPv4** (*Internet protocol version 4*). Tento protokol bol vyvinutý agentúrou *Defense Advanced Research Projects Agency* (**DARPA**). DARPA je agentúra amerického ministerstva obrany zodpovedná za rozvoj nových technológií predovšetkým pre vojenské aplikácie vytvorená v roku 1958. IPv4 zahŕňal adresný systém, ktorý používal numerické identifikátory skladajúce sa z 32 bitov. Použitie adries s dĺžkou 32 bitov obmedzuje celkový počet možných adries na množstvo približne 4,3 miliardy adries pre zariadenia pripojené k Internetu po celom svete. Počet zariadení pripojených k Internetu bude čoskoro väčší ako počet adries, ktoré poskytuje IPv4. Z tohto dôvodu agentúra zodpovedná za štandardizáciu internetových protokolov **IETF** (*Internet Engineering Task Force*) pracovala na novej verzii IP protokolu od roku 1998. IPv6, ktorého úlohou je nahradiť protokol IPv4 bol prvýkrát formálne popísaný v dokumente RFC 2460 [3].

IPv6 používa 128-bitový formát adries dovoľujúci 2^{128} alebo približne $3{,}4 \cdot 10^{38}$ adries, teda asi $8 \cdot 10^{28}$ násobne viac ako IPv4. Zväčšenie počtu internetových adries je jedna z najdôležitejších výhod IPv6. Existujú aj ďalšie dôležité technologické zmeny v protokole IPv6, ktoré vylepšia IP protokol: jednoduchšia administrácia, lepšie multicast smerovanie, jednoduchší formát hlavičky, jednoduchšie smerovanie, vstavaná autentifikácia a podpora anonymity.

IPv6 bude určitý čas koexistovať so starším IPv4. Nasadzovanie IPv6 bude prebiehať postupne. Klientské zariadenia, sieťové zariadenia, aplikácie, obsah a služby by mali byť prispôsobené novému internetového protokolu verzie IPv6. Okrem toho prechod z IPv4 na IPv6 zavedie spoločnú sadu štandardov medzi spoločnosťami a vzdelávacími systémami na celom svete.

IPv6 adresy sú reprezentované ako osem skupín štyroch hexadecimálnych znakov. Tieto skupiny sú oddelené dvojbodkou, ale existujú metódy na skrátenie tejto plnej notácie. Formát hlavičky protokolu IPv6 je vyobrazený na Obr. 1.

Obr. 1 - Formát hlavičky protokolu IPv6 [3]

Štruktúra hlavičky protokolu IPv6

Verzia	4-bitové pole pre verziu IP protokolu = 6
Trieda prevádzky	8-bitové pole pre triedu prevádzky
Značka toku	20-bitové pole pre značku toku
Veľkosť užitočných dát	16-bitov pre celé kladné číslo. Veľkosť užitočných dát protokolu IPv6, t.j. zvyšná časť paketu nasledujúca hlavičku protokolu IPv6 v oktetoch.
Ďalšia hlavička	8-bitový selektor, ktorý identifikuje typ hlavičky nasledujúci IPv6 hlavičku. Používa rovnaké hodnoty ako pole protokolu IPv4.
Maximálny počet skokov	8-bitov pre celé kladné číslo. Zníži sa o 1 pri každom prechode sieťovým uzlom. Paket je zahodený, ak toto pole dosiahne hodnotu nula.
Zdrojová adresa	128-bitová adresa odosielateľa paketu.
Cieľová adresa	128-bitová adresa prijímateľa paketu (ak je prítomná smerovacia hlavička, nie nevyhnutne adresa konečného príjemcu).

Nové funkcie zavedené s protokolom IPv6 sú v podstate nasledovné: nový formát hlavičky, efektívna a hierarchická adresovacia a smerovacia infraštruktúra, omnoho väčší adresný priestor a bezstavová aj stavová autokonfiguráciu adries, zabezpečenie IP, rozšíriteľnosť, lepšia podpora kvality služby (QoS) a nový protokol na interakciu susedných uzlov.

Protokol IPv6 vyriešil niektoré z bezpečnostných problémov zistených v sieťach IPv4 pridaním povinného (*IP Security*) **IPsec**. Vďaka tomuto je IPv6 podstatne efektívnejší. IPsec rozširuje pôvodný IP protokol tým, že poskytuje autentifikáciu, integritu, dôveryhodnosť a riadenie prístupu každého paketu pomocou využitia dvoch protokolov: **AH** (*authentication header*) a **ESP** (*encapsulating security*

payload). Rozšírenie počtu bitov v adresnom poli na 128 bitov, ktoré ponúka IPv6, tvorí významnú prekážku pre útočníkov, ktorí chcú vykonávať komplexné skenovanie portov. Na druhej strane je možné viazať verejný kľúč na IPv6 adresu: **CGA** (*Cryptographically Generated Address*).

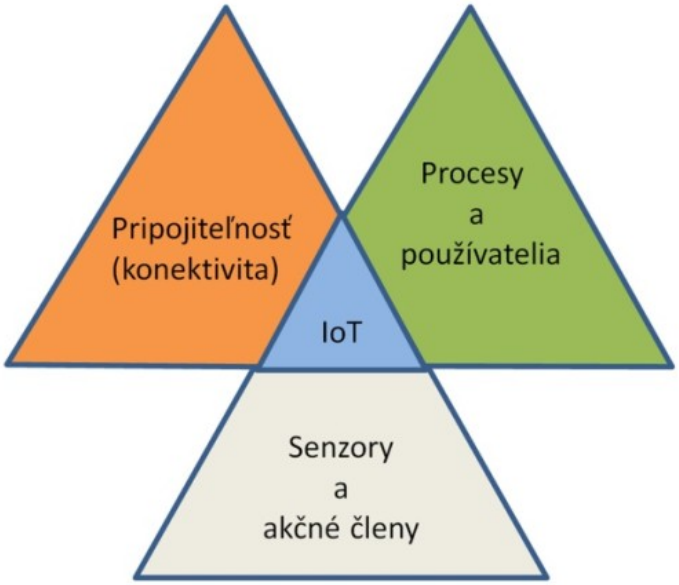
IPv6 poskytuje tiež zlepšenie v oblasti zabezpečenia mobility. Internet protokol MobileIP je k dispozícii v IPv4 aj IPv6 a bol vstavaný do protokolu IPv6, nie pridaný do protokolu IPv4 ako nová funkcia. To znamená, že každý uzol IPv6 môže použiť mobile IP podľa potreby. Mobilný IPv6 protokol používa dve rozšírenia v hlavičke: Smerovaciu hlavičku pre registráciu a hlavný cieľ na doručenie dát medzi mobilnými uzlami a zodpovedajúcimi fixnými uzlami.

3 IoT aplikácie

V tejto kapitole sú popísané niektoré dôležité aplikácie súvisiace s IoT. Sú uvedené hlavné prvky IoT architektúry a prezentovaný očakávaný vývoj IoT trhu.

3.1 Úvod

IoT môže byť považovaný za kombináciu senzorov a akčných členov poskytujúcu a prijímajúcu informáciu, ktorá je digitalizovaná a odoslaná na obojsmernú sieť schopnú preniesť všetky dáta určené na použitie rôznymi službami a koncovými používateľmi [4].



Obr. 2 - Koncept IoT

Viacero senzorov môže byť pripojených na objekt alebo zariadenie za účelom merania širokej škály fyzikálnych premenných alebo javov a dáta následne prenesené na cloud. Snímanie môže byť chápané ako model služby.

Klasifikácia senzorov

Poskytovateľ senzorových dát	Podnikateľské subjekty nasadzujúce a manažujúce senzory
Organizácie	Verejná alebo súkromná. Verejné infraštruktúry. Komerčné organizácie. Súkromné spoločnosti. Poskytovatelia technológií a služieb.
Osoby a domácnosti	Mobilné telefóny, inteligentné hodinky, gyroskopy, kamery, GPS, akcelerometre, mikrofóny, notebooky rovnako ako televízie, kamery, mrazničky, mikrovlnky, sporáky, umývačky riadu, inteligentné spotrebiče atď.

V dnešnej dobe sú najmodernejšie zariadenia, obvykle domové spotrebiče ako chladničky alebo televízory, vybavené komunikačnými a snímacími zariadeniami. Ich schopnosti budú neustále rozširované začlenením čoraz väčšieho počtu inteligentných komunikačných a snímacích nástrojov.

Schopnosti prepojených inteligentných zariadení

Monitorovanie	Vonkajšie prostredie. Stav, prevádzka a používanie produktu.
Riadenie	Riadenie funkcií produktu. Personalizácia používateľského komfortu. Programovanie.
Optimalizácia	Prediktívna diagnostika. Optimalizácia výkonu produktu. Redukcia nákladov.
Autonómia	Autonómne vylepšenie produktu a personalizácia. Samodiagnostika a oprava. Koordinácia spolupráce s ďalšími produktami.
Efektívny rozhodovací proces.	Dáta v reálnom čase na vykonávanie rozhodnutí.

Architektúra IoT systémov môže byť rozdelená do štyroch vrstiev: Snímacia vrstva, vrstva dátovej výmeny, informačno-integračná vrstva a vrstva aplikačných služieb [5].

Inteligentné zariadenia môžu byť už v súčasnosti prepojené pomocou tradičného Internetu. IoT zahŕňa snímaciu vrstvu, ktorá znižuje požiadavky na schopnosti týchto zariadení a umožňuje prepojenie medzi nimi. Používatelia využívajúci senzorové dáta komunikujú so senzormi alebo majiteľmi senzorov prostredníctvom informačno-integračnej vrstvy, ktorá je zodpovedná za všetku komunikáciu a transakcie. Medzitým prichádzajú nové požiadavky a výzvy na výmenu dát, filtrovanie informácií a integráciu, vymedzenie nových služieb používateľom a zložitosť sieťovej architektúry. Navyše využívanie cloudových technológií exponenciálne rastie. Nové platformy a softvérové aplikácie sú ponúkané v rámci Internetu vecí. Niektoré z hlavných výhod a prínosov Internetu vecí budú: vytvorenie inovatívnych služieb s lepším výkonom, riešenia s pridanou hodnotou spolu s redukciou nákladov na zber dát existujúcich služieb a príležitosť na vytvorenie nových zdrojov príjmov v kontexte udržateľného podnikateľského modelu. Tieto aplikácie môžu byť orientované na spotrebiteľov, obchody, reklamy, prieskumné činnosti, priemyselnú a vedeckú komunitu s využitím vývojárov aplikácií.

Štvorvrstvová architektúra IoT

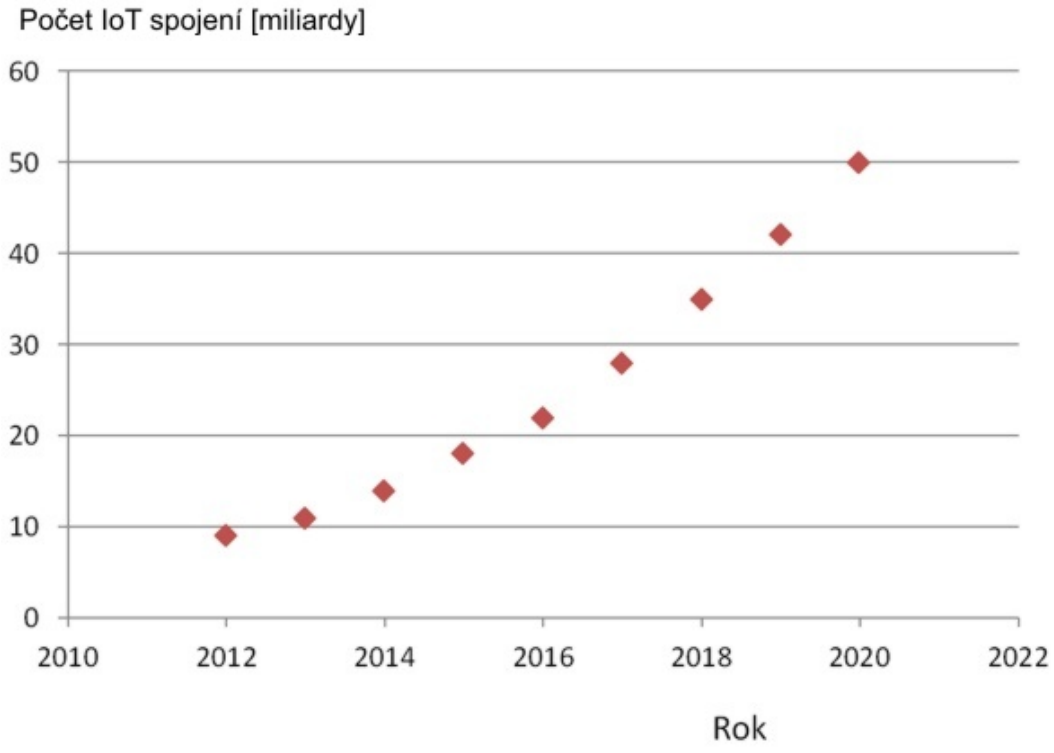
Vrstva snímania objektov	Snímanie fyzických objektov a získavanie dát
Vrstva výmeny dát	Transparentný prenos dát cez komunikačnú sieť
Informačno-integračná vrstva	Spracovanie nejednoznačných informácií zo siete, filtrovanie nežiadúcich dát a integrácia hlavnej informacie do využiteľných znalostí pre koncových používateľov a služby.
Vrstva aplikačných služieb	Poskytuje používateľovi služby obsahu

3.2 Trh IoT

IoT je vznikajúca technická architektúra na báze Internetu zjednodušujúca výmenu tovarov v globálnej dodávateľskej sieti [1]. Pretože technologický trend sa posúva smerom k poskytovaniu vyšších prenosových rýchlostí a menších prenosových oneskorení, očakáva sa zdvojnásobenie veľkosti Internetu každých 5,3 roka a cloud computing môže hrať kľúčovú úlohu v tomto raste. Cloud computing je jednou z platforiem, ktoré sprístupňujú podporu IoT. Väčšina "things" reálneho sveta bude integrovaná do virtuálneho sveta sprístupňujúc konektivitu kedykoľvek a kdekoľvek.

Cloud computing je model umožňujúci prístup ku zdieľanému úložisku konfigurovateľných výpočtových prostriedkov, ktorý umožňuje používateľom využívať výhody všetkých existujúcich technológií bez potreby ich hlbšej znalosti alebo odborných poznatkov.

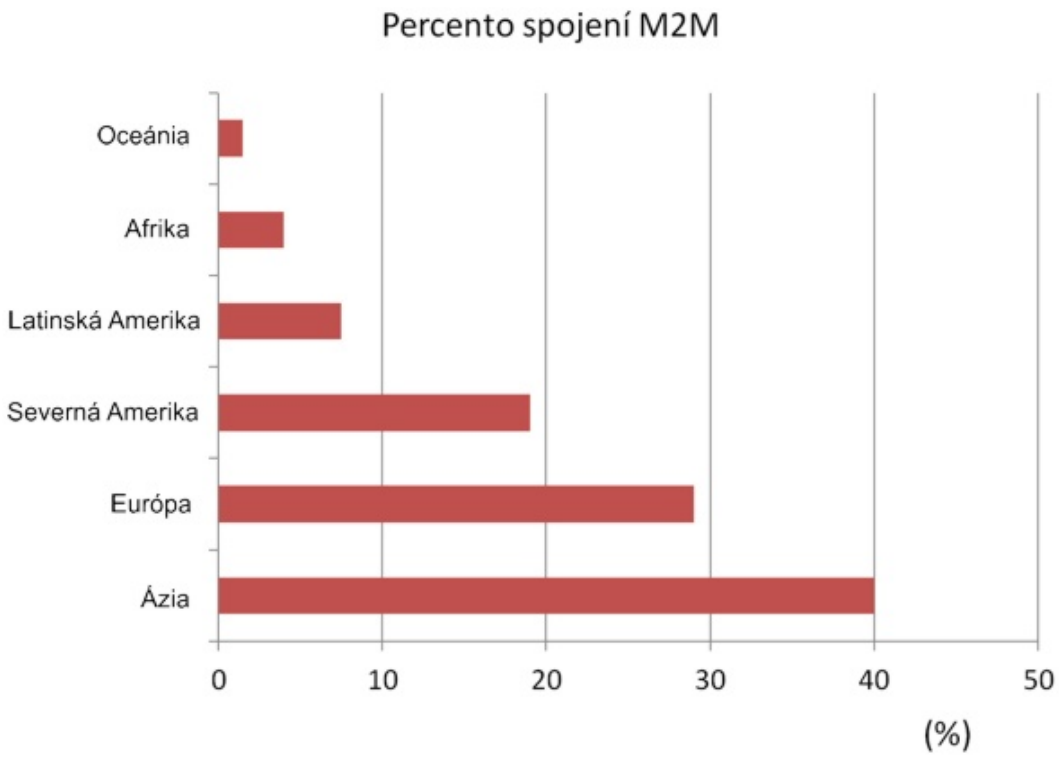
V roku 2010 bol počet fyzických objektov a zariadení každodenne pripojených k Internetu okolo 12,5 miliardy. Očakáva sa, že toto číslo sa s počtom inteligentných zariadení na osobu po zdvojnásobnení na 25 miliárd v roku 2015, ďalej zdvojnásobní na 50 miliárd v roku 2020 [2].



Obr. 3 - Počet IoT pripojení [2]

31 %	Telefóny
29%	Notebooky
10%	Inteligentné telefóny
8%	Inteligentné televízory
5%	Tablety
5%	Herné konzoly
5%	Multimediálne prehrávače
5%	eČítačky
3%	Iné

Ázia má v súčasnej dobe najviac M2M pripojení z dôvodu veľkého úsilia v krajinách akými sú Japonsko a Čína. Americké a európske technologické spoločnosti robia významný pokrok v oblasti IoT a prinesú na trh nárast M2M pripojení aj v týchto krajinách. S dôležitosťou vzniku IoT musia byť definované nové regulačné prístupy s cieľom zaistiť súkromie a bezpečnosť používateľov a dát.



Obr. 4 - Percento M2M pripojení [2]

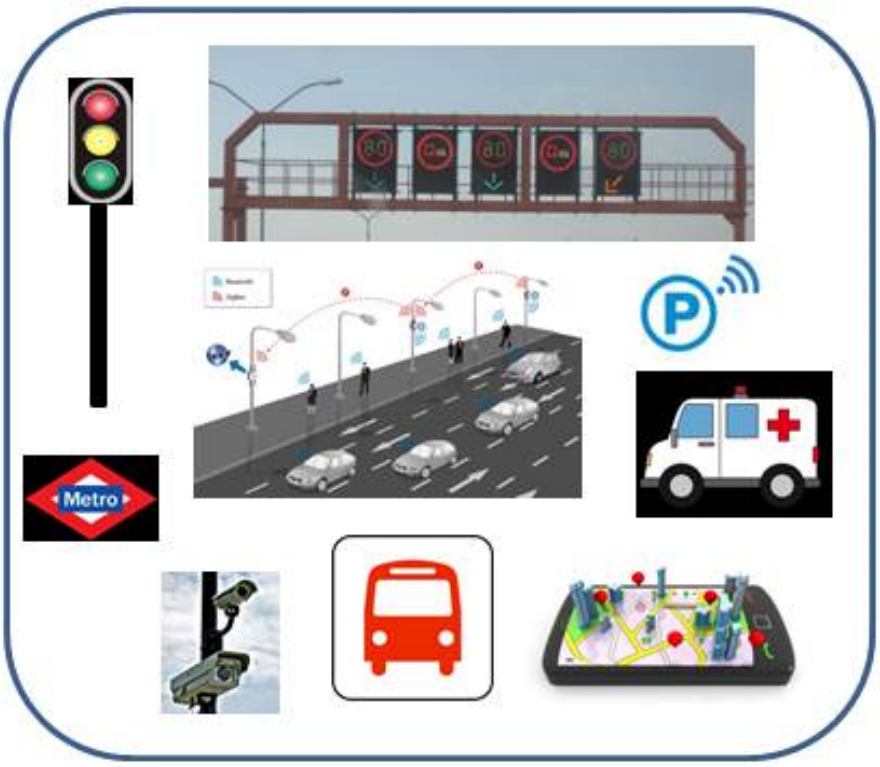
3.3 Aplikácie

Počet aplikácií a služieb, ktoré môže poskytovať IoT je prakticky neobmedzený a môže byť prispôsobený mnohým oblastiam ľudskej činnosti. Uľahčí a zlepší kvalitu života niekoľkými spôsobmi. Táto kapitola ponúka stručný zoznam aplikácií a služieb založených na IoT. Obsahuje len ich stručný opis s cieľom pochopiť všetky možné aplikácie a služby, ktoré môže IoT poskytovať. Odhadovaná hodnota dosiahnutá IoT aplikáciami a službami do roku 2020 je 19 miliárd.

IoT aplikácie a služby:

- Pripojené inteligentné budovy: Zlepšenie účinnosti (manažment spotreby energie a úspory) a bezpečnosti (senzory a alarmy). Domové aplikácie vrátane inteligentných senzorov a akčných členov na ovládanie domácich spotrebičov. Zdravotné a vzdelávacie služby doma. Diaľkové ovládanie liečby pacientov. Káblové/satelitné služby. Systém ukladania/generovania energie. Automatické vypínanie elektroniky v prípade jej nevyužívania. Inteligentné termostaty. Detektory dymu a alarmy. Aplikácia na kontrolu prístupu. Inteligentné zámky. Senzory zabudované v infraštruktúre budovy na výpomoc a asistenciu záchranárom. Bezpečnosť pre všetkých členov rodiny.

- Inteligentné mestá a doprava: Integrácia bezpečnostných služieb. Optimalizácia verejnej a súkromnej dopravy. Parkovacie senzory. Inteligentná správa parkovacích služieb a premávky v reálnom čase. Inteligentné riadenie semaforov v závislosti od dopravných zápch. Zabezpečenie (kamery, inteligentné senzory, informácie pre občanov). Vodné hospodárstvo. Zavlažovanie parkov a záhrad. Inteligentné popolnice. Kontrola znečistenia. Získavanie okamžitej spätnej väzby a názorov od občanov. Inteligentná správa. Volebné systémy. Monitorovanie nehôd, koordinácia záchranných akcií a tiesňových volaní.



Obr. 5 - Príklad IoT aplikácií: Inteligentné mestá.

- Vzdelávanie: Prepojenie virtuálnych a fyzických učební na zabezpečenie efektívnejšieho a dostupnejšieho vzdelávania, e-learning. Prístupové služby k virtuálnym knižniciam a vzdelávacím portálom. Výmena správ a výsledkov v reálnom čase. Celoživotné vzdelávanie. Učenie sa cudzích jazykov. Správa účasti.

- Spotrebná elektronika: Inteligentné telefóny. Inteligentná TV. Notebooky, počítače a tablety. Inteligentné chladničky, umývačky a sušičky. Inteligentné domáce kino. Inteligentné spotrebiče. Obojkové (Pet collar) senzory. Personalizácia používateľského komfortu. Autonómna prevádzka výrobku. Osobné lokátory. Inteligentné okuliare.

- Zdravie: Monitorovanie chronických ochorení. Zlepšenie kvality starostlivosti a kvality života pacientov. Sledovače aktivity. Vzdialená diagnostika. Pripojené náramky. Interaktívne pásy. Monitorovanie športovej aktivity. Inteligentné štítky na drogy. Sledovanie užívania omamných látok (drog). Biočipy. Rozhranie mozog-počítač. Sledovanie stravovacích návykov.

- Automobilový priemysel: Inteligentné autá. Kontrola premávky. Pokročilé informácie o tom čo je pokazené. Bezdrôtové monitorovanie tlaku vzduchu v pneumatikách. Inteligentné riadenie a kontrola energie. Samodiagnostika.

Akcelerometer. Senzory pozície a priblíženia. Analýza najefektívnejšej cesty v reálnom čase. GPS sledovače. Riadenie rýchlosti vozidla. Autonómne vozidlá využívajúce služby IoT.

- Poľnohospodárstvo a životné prostredie: Meranie a monitorovanie znečistenia prostredia (CO_2, hluk, prvky kontaminujúce okolité prostredie). Predpovede klimatických zmien založené na inteligentných senzoroch. Pasívne RFID štítky pripojené k poľnohospodárskym produktom. Senzory v paletách výrobkov. Nakladanie s odpadom. Výpočet výživovej hodnoty výrobkov.

- Energetické služby: Presné údaje o spotrebe energie. Inteligentné meranie. Inteligentné siete. Analýza a predikcia spotreby energie a vzory. Predpovedanie budúcich trendov v spotrebe energie. Bezdrôtové sieťové senzory. Výroba energie a jej recyklácia.

- Inteligentné pripojenie: Správa dát a poskytovanie služieb. Využitie sociálnych sietí a médií. Prístup k e-mailom, hlasovým a video službám. Interaktívna skupinová komunikácia. Streamovanie v reálnom čase. Interaktívne hranie sa. Rozšírená realita. Sledovanie zabezpečenia siete. Nositeľné používateľské rozhrania. Efektívne spracovanie. Biometrické autentifikačné metódy. Spotrebiteľská telematika. M2M komunikačné služby. Analýza veľkých dát. Virtuálna realita. Služby cloudového spracovania. Všadeprítomné spracovanie. Počítačové videnie. Inteligentné antény.

- Výroba: Snímače plynu a prietoku. Inteligentné senzory vlhkosti, teploty, pohybu, sily, zaťaženia, netesnosti, úrovniach. Strojové videnie. Snímanie akustiky a vibrácií. Kompozitné aplikácie. Inteligentné riadenie robotov. Riadenie a optimalizácia výrobných procesov. Rozpoznávanie vzorov. Strojové učenie. Prediktívna analýza. Mobilná logistika. Správa skladu. Zabránenie nadprodukcii. Efektívna logistika.

- Nakupovanie: Inteligentné nakupovanie. RFID a ďalšie elektronické štítky a čítačky. Čiarové kódy v maloobchode. Riadenie zásob. Kontrola geografického pôvodu jedla a produktov. Kontrola kvality jedla a bezpečnosti.

4 Sprístupňujúce technológie

Úspešné uplatnenie koncepcie IoT do reálneho sveta je možné vďaka pokroku v nižšie uvedených technológiách. V tejto časti budú uvedené najrelevantnejšie podporné technológie s cieľom poskytnúť obraz o úlohe, ktorú budú pravdepodobne zohrávať v IoT [6], [7].

4.1 Energia

Ukladanie energie je jednou z technológií, ktoré umožňujú nasadenie IoT aplikácií. Otázky energetiky vo všetkých jej fázach, od výroby po skladovanie a využitie, sú kľúčové pre rozvoj IoT. Tieto technológie musia poskytovať vysoký výkon generovania energie a jej výroby. Spolu s dnešnou nízkovýkonovou nanoelektronikou nám umožnia návrh samonapájacích inteligentných senzorov na báze bezdrôtového identifikačného zariadenia. Stále je potrebný výskum a vývoj riešení v oblastiach (nanoelektronika, polovodiče, senzorová technológia, mikrosystémová integrácia), ktoré majú za cieľ ultranízkoenergetické zariadenia, účinnejšie a kompaktné úložiská energie ako batérie, palivové články a tlačené polymérové batérie. Súčasné zariadenia sa zdajú nedostatočné vzhľadom na potrebný výpočtový výkon a energetické obmedzenia budúcnosti. Okrem toho systémová integrácia zvýši účinnosť existujúcich systémov a bude poskytovať celý rad riešení pre budúce potreby.

4.2 Senzory

Senzory sú jedným z kľúčových stavebných prvkov IoT, ktoré môžu byť nasadené všade. Môžu byť tiež implantované pod kožu človeka, v kabelke alebo na tričku. Niektoré môžu byť malé okolo štyroch milimetrov ale dáta, ktoré zbierajú možno prijímať stovky míľ ďaleko. Dopĺňajú ľudské zmysly a stali sa nevyhnutnými v mnohých priemyselných odvetviach, od zdravotnej starostlivosti po výrobu. Senzory majú kľúčovú výhodu, že môžu predvídať ľudské potreby na základe informácií zhromaždených z ich okolia. Ich inteligencia znásobená početnými sieťami im umožňuje nielen hlásiť stav vonkajšieho prostredia, ale aj konať bez ľudského zásahu.

Miniaturizované kremíkové čipy sú navrhnuté s novými schopnosťami v menších tvarových rozmeroch, lepším výkonom spracovania a účinnosťou. Náklady klesajú podľa Moorovho pravidla. Náklady na šírku pásma tiež klesli. Podobne náklady na spracovanie. To umožňuje viac zariadení, ktoré majú byť nielen pripojené ale aj dostatočne inteligentné aby vedeli, čo robiť so všetkými novými údajmi, ktoré generujú alebo prijímajú.

Schopnosti ako je kontextové uvedomenie a vnútrostrojová komunikácia sú považované za vysoko prioritné v IoT. Ďalšie priority sú integrácia pamäte a výpočtový výkon, schopnosť odolávať drsným podmienkam prostredia a cenovo dostupné zabezpečenie. Okrem toho môže byť vývoj nízkoenergetických procesorových/mikrokontrolérových jadier určených špeciálne pre mobilné zariadenia IoT novou triedou jednoduchých a prostých IoT-centrických inteligentných systémov dôležitým činiteľom uplatnenia. Riešenie v tomto smere sa bude pohybovať v rozmedzí od mikro naprogramovaných strojov z konečným počtom stavov po použitie mikrokontrolérov. Voľba je kompromis medzi flexibilitou, programovateľnosťou, kremíkovou plochou a spotrebou elektrickej energie. Tieto zariadenia vyžadujú určitú formu stálej pamäte (EEPROM/FRAM/polymér), nezávisle na tom, či bude laserom vypálená v čase výroby, raz programovateľná alebo elektricky prepisovateľná. Prepisovateľné energeticky nezávislé pamäte sú výhodné pre dosiahnutie vysokej priepustnosti a umožňujú súčasne výhodu používateľských pamätí, programovateľnosti a ukladanie dát zo senzorov.

4.3 Cloud computing

Cloud computing je model prístupu k zdieľaným konfigurovateľným zdrojom na požiadanie (napríklad počítače, siete, servery, úložiská, aplikácie, služby, software), ktorý môže byť tvorený ako **IaaS** (*Infrastructure as a Service*) alebo **SaaS** (*Software as a Service*). Jedným z najdôležitejších výstupov IoT je obrovské množstvo dát generovaných zo zariadení pripojených k Internetu [7]. Veľa aplikácií IoT vyžaduje obrovské úložiská dát, obrovskú rýchlosť spracovania na to, aby boli schopné rozhodovať v reálnom čase a vysokorýchlostné širokopásmové siete pre streamovanie dát audia alebo videa. Cloud computing poskytuje ideálne back-end riešenie pre manipuláciu s veľkými dátovými tokmi a ich spracovanie v reálnom čase pre bezprecedentný počet zariadení IoT a ľudí.

4.4 Komunikácia

Nové inteligentné viacpásmové antény integrované na čipe a vyrobené z nových materiálov sú komunikačné prostriedky, ktoré umožnia zariadeniam komunikovať. Antény umiestnené priamo na čipe musia byť optimalizované veľkosťou, cenou a efektivitou. Môžu byť dostupné v rôznych formách ako sú cievky na čipe, tlačené antény, vstavané antény a viacnásobné antény vďaka rôznym substrátom a 3D štruktúram. Aby boli efektívne viacpásmové komunikačné protokoly a prenosové rýchlosti je potrebné riešiť aj otázky použitých modulačných schém a prenosových rýchlostí. Komunikačné protokoly budú navrhnuté pre webové architektúry orientované na IoT platformy, kde sú všetky objekty, bezdrôtové zariadenia, kamery, počítače atď. kombinované z dôvodu analýzy umiestnenia, zámeru a dokonca aj emócie prostredníctvom siete. Sú potrebné nové metódy efektívneho riadenia spotreby energie na rôznych úrovniach sieťového konceptu od sieťového smerovania až po architektúru jednotlivých zariadení.

4.5 Integrácia

Integrácia inteligentných zariadení do tzv. balíkov alebo lepšie do vlastných produktov samotných umožní značné zníženie nákladov a zvýšenie šetrnosti k životnému prostrediu. Využitie integrácie čipov a antén do neštandardných substrátov ako textilu a papiera. Rozvoj nových substrátov, vodivých ciest a spojovacích materiálov vhodných pre drsné prostredie s možnosťou ekologického odstránenia bude pokračovať. **SIP** (*System-in-Package*) technológia umožňuje flexibilitu a 3D integráciu rôznych prvkov ako sú antény, senzory, aktívne a pasívne prvky do obalu, zlepšenie výkonu a zníženie nákladov. RFID čipy so štruktúrovanými spojovacími pásikmi sa používajú pre pripojenie obvodových čipov a antén za účelom vytvorenia rôznych tvarov a veľkostí etikiet namiesto priamej montáže.

4.6 Štandardy

IoT zariadenia sú veľmi rozmanité a merajú rôzne parametre podľa rôznych dohovorov a meracích jednotiek. Aj keď v súčasnosti sa navrhujú rôzne proprietárne protokoly je pravdepodobné, že opensource štandardy budú jedným zo spôsobov ako dosiahnuť dátovú interoperabilitu.

Je zrejmé, že otvorené štandardy sú kľúčové prvky, ktoré umožňujú úspech bezdrôtových komunikačných technológií a všeobecne pre akýkoľvek druh komunikácie stroj-stroj. Dôležitým pre zavádzanie IoT aplikácií je rýchlejšie zavádzanie interoperabilných štandardov. Je potrebné vyjasniť si požiadavku ako unikátna globálna identifikácia. Pre rýchlejšie zavádzanie interoperabilných noriem je potrebné, aby bola uznaná ako dôležitý prvok pre nasadenie aplikácií IoT. Musia sa vyjasniť požiadavky nielen na unikátnu globálnu identifikáciu, ale aj na systém mien a prekladačov adries (resolvers). Nedostatočná konvergencia definície spoločných referenčných modelov, referenčná architektúra pre Siete budúcnosti, Internet budúcnosti, IoT a integrácia starších systémov a sietí sú výzvou, ktoré treba riešiť v budúcnosti.

5 Výzvy a prekážky v IoT

Ešte treba riešiť rad náročných otázok. Riešenie týchto problémov umožňuje poskytovateľom služieb a programátorom aplikácií implementovať ich služby efektívne. V nasledujúcich odsekoch, ponúkame stručnú diskusiu ohľadom hlavných výziev, ktorým sa čelí vo fáze vývoja a zavádzania IoT [8].

5.1 Výzvy

Spoľahlivosť

Spoľahlivosť má za cieľ zvýšiť úspešnosť poskytovania služieb prostredníctvom IoT. Má blízky vzťah s dostupnosťou. Garantujeme dostupnosť informácií a služieb v definovanom časovom horizonte. Spoľahlivosť je ešte kritickejšia a má prísnejšie požiadavky, pokiaľ ide o oblasť aplikácií reagujúcich na mimoriadne udalosti. Dôležitou súčasťou týchto systémov je komunikačná sieť, ktorá musí byť dostatočne odolná voči chybám za účelom spoľahlivého prenosu informácií. Spoľahlivosť musí byť implementovaná softvérovo ale aj hardvérovo všetkými vrstvami IoT. Ak chcete mať efektívny IoT, komunikácia musí byť spoľahlivá. Napríklad nespoľahlivé snímanie, zber dát, spracovanie a prenos môžu viesť k dlhým oneskoreniam, strate dát a nakoniec chybným rozhodnutiam. To môže viesť ku katastrofálnym scenárom v dôsledku čoho môže byť IoT menej spoľahlivé.

Spoľahlivosť súvisí so správnym fungovaním systému založenom na jeho špecifikáciách.

Výkon

Hodnotenie výkonnosti služieb IoT je veľká výzva, pretože je závislé od výkonnosti mnohých komponentov a tiež od výkonnosti uvedených technológií. IoT rovnako ako aj iné systémy je potrebné neustále rozvíjať. Zlepšovať jeho služby za účelom vyhovenia požiadavkám zákazníkov. IoT zariadenia musia byť monitorované a vyhodnocované, aby poskytovali zákazníkom najlepší možný výkon za dostupnú cenu. Mnoho metrík je možné použiť na hodnotenie výkonnosti IoT vrátane rýchlosti spracovania, komunikačnej rýchlosti, formy zariadenia a nákladov.

Hodnotenia výkonu jednotlivých spomínaných protokolov a technológií, protokolov aplikačnej vrstvy, QoS boli popísané v literatúre. Nedostatočné a dôkladné hodnotenie výkonu aplikácií IoT je stále predmetom riešenia.

QoS (*Quality of service*) je celkový výkon telefónnej alebo počítačovej siete a najmä výkon vnímaný používateľom tejto siete.

Interoperabilita

Pre IoT je ďalšou výzvou interoperabilita (spolupráca) práve kvôli potrebe zvládnutia veľkého množstva rozličných vecí patriacich k rôznym platformám. Interoperabilitu musia brať do úvahy tvorcovia aplikácií aj výrobcovia IoT zariadení, aby zaistili dodanie služieb pre všetkých zákazníkov nezávisle od špecifikácií hardvérovej platformy, ktorú používajú. Napríklad väčšina dnešných inteligentných telefónov podporuje bežné komunikačné technológie ako sú Wi-Fi, NFC a GSM, aby zaistili interoperabilitu v rôznych situáciách. Programátori IoT by tiež mali svoje aplikácie budovať tak, aby umožnili pridávanie nových funkcií bez spôsobovania problémov alebo straty funkcií pri zachovaní integrácie s rozličnými

komunikačnými technológiami. Preto je interoperabilita významným kritériom v návrhu a budovaní IoT služieb na zabezpečenie požiadaviek zákazníkov. Okrem plejády protokolov predstavujú výzvu pre interoperabilitu rôzne interpretácie tých istých štandardov implementované rôznymi spoločnosťami. Aby sa predišlo týmto odlišnostiam, bolo by vhodné testovať interoperabilitu medzi rôznymi produktami v testoch ako je ETSI Plugtest. Cieľom výskumného projektu PROBE-IT je zaistenie interoperability overených IoT riešení, ktoré vykonajú testy interoperability ako CoAP, 6LoWPAN a sémantickej interoperability IoT.

Je známym faktom, že dve rozličné zariadenia nemusia spolupracovať ani v prípade, že by dodržiavali rovnaký štandard. Toto je najväčšou brzdou širokého prijatia IoT technológií. Zariadenia budúcnosti musia integrovať rôzne komunikačné štandardy a protokoly, pracovať na rôznych frekvenciách a podporovať rôzne architektúry, či už centralizované alebo distribuované. Musia byť schopné komunikovať s inými sieťami až dovtedy, kým nevzniknú globálne dobre definované štandardy.

Bezpečnosť a súkromie

Bezpečnosť predstavuje významnú výzvu pre implementáciu IoT kvôli nedostatku spoločných štandardov a architektúry pre IoT bezpečnosť. V heterogénnych sieťach, ako v prípade IoT, nie je jednoduché zabezpečiť bezpečnosť a súkromie používateľov. Kľúčová funkcionalita IoT je založená na výmene informácií medzi miliardami či biliónmi objektov pripojenými k Internetu. Jedným z otvorených problémov bezpečnosti IoT, ktorý v štandardoch nebol vzatý do úvahy, je distribúcia kľúčov medzi zariadeniami. Na druhej strane sú kritické najmä otázky súkromia a operácie prístupu k profilom medzi IoT zariadeniami bez vzájomného ovplyvňovania. Bezpečnosť výmeny dát preto zostáva nevyhnutnou podmienkou zabráneniu strate alebo ohrozeniu súkromia. Zvýšené množstvo inteligentných (smart) vecí okolo nás s citlivými dátami vyžaduje transparentný a jednoduchý manažment kontroly prístupu tak, aby napríklad jedno pripojené zariadenie mohlo iba čítať údaje a iné mohlo zariadenie ovládať. V tomto smere už bolo navrhnutých niekoľko riešení, napríklad zoskupovanie vstavaných zariadení do virtuálnych sietí a ich sprístupňovanie iba v rámci týchto sietí. Ďalšou možnosťou je podpora riadenia prístupu na aplikačnej vrstve pre jednotlivé zariadenia samostatne.

Manažment

Prepojenie miliárd až biliónov inteligentných zariadení predstavuje pre poskytovateľov služieb obrovské problémy týkajúce sa manažmentu chýb, konfigurácie, účtovania, výkonu a bezpečnosti (FCAPS) týchto zariadení. Snaha o takéto manažovanie si vyžaduje vývoj nových nenáročných manažovacích protokolov, aby sa zvládla potenciálna manažérska nočná mora, ktorá môže nastať po nasadení IoT v najbližších rokoch. Správa IoT zariadení a aplikácií môže byť efektívnym faktorom pre rast nasadenia IoT. Napríklad monitorovanie M2M komunikácie IoT objektov je dôležité pre zaistenie nepretržitej konektivity na poskytovanie služieb na požiadanie. Štandard Light-weight M2M (LWM2M) vyvíjaný organizáciou Open Mobile Alliance má za cieľ poskytnúť rozhranie medzi M2M zariadeniami a servermi na vybudovanie schémy nezávislej od aplikácie určenej na správu rozličných zariadení. Schéma poskytne M2M aplikáciám

možnosti vzdialenej správy zariadení, služieb a aplikácií stroj-stroj. Protokol NETCONF Light je snahou konzorcia Internet Engineering Task Force (IETF) o správu obmedzených zariadení a poskytuje nástroje na inštaláciu, manipuláciu a odstraňovanie sieťových zariadení. Môže zabezpečiť správu širokého spektra zariadení od menej vybavených až po funkčne bohaté zariadenia. Nezávisle vyvíjaná platforma MASH IoT je príkladom platformy, ktorá uľahčuje správu (monitorovanie, riadenie a konfiguráciu) IoT zdrojov kdekoľvek v reálnom čase s použitím IoT ovládacieho panela na inteligentnom telefóne. Správu tiež vyžaduje údržba kompatibility naprieč vrstvami IoT na zlepšenie rýchlosti pripojenia a zabezpečenie poskytnutia služieb. Pracovná skupina Správa zariadení Open Mobile Alliance (OMA) špecifikuje protokoly a mechanizmy na správu mobilných zariadení a služieb v prostrediach s obmedzenými zdrojmi.

Výroba

Výzvy vo výrobe musia byť riešené presvedčivo. Je nutné znižovať náklady na menej než jeden cent za pasívny RFID tag (nosič informácií) a produkcia musí dosahovať vysoké objemy. Celý výrobný proces musí mať veľmi obmedzený vplyv na životné prostredie, byť založený na stratégiách pre opätovné využitie a recykláciu vzhľadom na celkový životný cyklus digitálnych zariadení a iných produktov, ktoré je možné označkovať alebo vybaviť snímačmi.

5.2 Prekážky

Pre IoT však existujú aj prekážky najmä na poli predpisov, zabezpečenia a bezpečnosti. Hlavným cieľom je lepšie chrániť súkromie ľudí a donútiť spoločnosti využívať na správu dát a informácií zabezpečené spôsoby [8], [9].

Chýbajúci dohľad

Významnou prekážkou širokého prijatia technológie Internetu vecí je neexistujúci dohľad. Bez nestrannej dohliadajúcej autority nebude možné mať skutočne globálny IoT akceptovaný štátmi, spoločnosťami, obchodnými organizáciami a ľuďmi všeobecne. V súčasnosti neexistuje jednotná univerzálna číslovacia schéma. EPCglobal a Ubiquitous Networking Lab navrhujú dva odlišné nekompatibilné spôsoby identifikácie objektov a existuje nebezpečenstvo, že si v nasledujúcich rokoch budú na svetovom trhu konkurovať. Je tiež potrebné udržiavať všeobecný dohľad v takej miere ako je to len možné, pretože mať autoritu pre každú oblasť aplikácie isto povedie k prekrývaniu, zmätku a súpereniu štandardov. Objekty môžu mať rôzne identity v rôznych kontextoch. Existencia viacerých autorít by spôsobila istý druh viacnásobného smerovania. To môže viesť ku katastrofickým výsledkom.

Súkromie a zabezpečenie

Na všeobecné prijatie akéhokoľvek systému identifikácie objektov je potrebné mať technicky silné riešenie, ktoré zaručí súkromie a bezpečnosť zákazníkov. Pretože v mnohých prípadoch bolo zabezpečenie realizované ako prídavná funkcia prevláda pocit, že verejné prijatie Internetu vecí nastane iba v prípade ak preň budú existovať spoľahlivé riešenia zabezpečenia a súkromia. Obzvlášť je potrebné zachytávať útoky, autentifikovať dáta, riadiť prístup a zaručiť súkromie zákazníkov (fyzických aj právnických osôb). Môže to byť prostredníctvom hybridných bezpečnostných mechanizmov, ktoré napríklad kombinujú hardvérové zabezpečenie s diverzifikáciou kľúčov. To prináša vynikajúce zabezpečenie takmer alebo úplne znemožňujúce útoky. Výber bezpečnostných funkcií a mechanizmov bude naďalej závislý od ich vplyvu na biznis procesy. Medzi veľkosťou čipov, nákladmi, funkčnosťou, interoperabilitou, bezpečnosťou a súkromím sa vždy bude hľadať kompromis.

Problémy bezpečnosti a súkromia by mali riešiť prichádzajúce štandardy, ktoré musia definovať rozličné bezpečnostné funkcie na poskytnutie dôvernosti, integrity a dostupnosti služieb.

Existuje aj mnoho problémov týkajúcich sa identity osôb. V rámci nich je potrebné vysporiadať sa s politikou a legislatívou. Ich vyriešenie je kriticky dôležité pre efektívnu verejnú správu budúcnosti.

6 Budúcnosť IoT

V nadchádzajúcich rokoch je možné identifikovať štyri hlavné makro trendy, ktoré spoločne s explóziou všadeprítomných zariadení vytvárajúcich Internet vecí ovplyvnia budúcnosť internetových technológií:

1. V prvom rade ide o tzv. „exaflood“ alebo „záplavu dát“, teda explóziu množstva zbieraných a vymieňaných dát. Súčasné siete nie sú na takýto exponenciálny nárast premávky pripravené a tak je potrebné, aby všetky zúčastnené strany premysleli súčasné architektúry sietí a úložísk. Bude dôležité nájsť nové spôsoby a mechanizmy vyhľadávania, získavania a prenosu dát. Jedným z relevantných dôvodov tejto dátovej záplavy je nárast počtu zariadení zbierajúcich a vymieňajúcich si informácie, čím sa Internet vecí stáva realitou.

Pojem **exaflood** zaviedol Bret Swanson z Nadácie pre slobodu a pokrok (Progress & Freedom Foundation) a označuje sa ním rastúci prúd dát na Internete.

2. Energia potrebná na ovládanie inteligentných zariadení dramaticky poklesne. V súčasnosti mnoho datacentier dosiahlo maximálnu úroveň spotreby energie a za vyraďovaním starých zariadení tak nevyhnutne musí nasledovať získavanie nových. Druhý trend možno označiť ako pokrytie všetkých zariadení a systémov od najmenšieho smart prachu až po obrovské dátové centrá a hľadanie nulovej entropie, kde zariadenie alebo systém bude samé získavať svoju energiu.

3. Miniaturizácia zariadení sa deje tiež prekvapivo rýchlo. Cieľ v podobe jednoelektrónového tranzistora sa približuje. To sa zdá byť konečnou hranicou, aspoň kým vo fyzike nenastanú nové objavy.

4. Ďalším dôležitým trendom sú autonómne zdroje. Stále rastúca zložitosť systémov bude nemanažovateľná a bude brániť vzniku nových služieb a aplikácií až kým systémy nezačnú byť označované samo-* vlastnosťami. Napr. samo-manažment, samo-zotavenie a samo-konfigurácia.

Ako hlavný trend uvidíme viac aplikácií a prijatie IoT, keďže integrácia technológií do fyzických objektov sa stáva lacnejšou. IoT tak bude mať v nasledujúcich rokoch hlavný vplyv na spoločnosti v oblasti e-podnikania typu biznis s biznisom (B2B) aj biznis s koncovými zákazníkmi (B2C).