Internet věcí

Maturitní práce

Informační a komunikační technologie

Terezie Hrubanová
Gymnázium Velké Meziříčí
Duben 2019

Prohlašuji, že jsem svou maturitní práci napsala samostatně a výhradně s použitím citovaných pramenů.

Ve Velkém Meziříčí dne 5. 4. 2019 *Terezie Hrubanová*

Obsah

1 Úvod

Internet věcí, častěji známý pod anglickým názvem Internet of Things nebo zkratkou IoT, je síť propojených elektronických zařízení. Tato zařízení jsou vybavena senzory, softwarem a síťovou konektivitou, aby mohla sbírat data a následně je sdílet s ostatními zařízeními bez nutného zásahu člověka. Každé zařízení v síti lze jednoznačně určit díky jeho identifikátoru, ale zároveň je schopné fungovat v Internetu.

2 Historie IoT

Přestože IoT je fenoménem dnešní doby, již o mnoho let zpátky se objevily první pokusy rozvíjející myšlenku připojení běžných zařízení do sítě.

Prvním zařízením připojeným na Internet byl automat na Coca Colu v Carnegie Mellon University. Programátoři z oddělení Computer Science ho v roce 1982 upravili tak, aby se k němu mohli připojit a zjistit, zda je plný a nápoje v něm vychlazené.

Dále pak roku 1990 Američan John Romkey vytvořil toaster, který se dal zapnout a vypnout přes Internet pomocí TCP/IP protokolu. Tento toaster byl prezentován na veletrhu informačních technologií Interop v San Jose v USA. Dalším z brzkých IoT zařízení byl tzv. Trojan Room coffee pot, tedy konvička na kávu v počítačové laboratoři na University of Cambridge roku 1993. Quentin Stafford-Fraser a Paul Jardetzky vytvořili systém, který monitoroval stav konvičky s kávou a třikrát za minutu tento obrázek posílal na server, aby si ostatní kolegové mohli zjistit, kolik je v konvičce kávy.

Experimentem se síťovou konektivitou byla Wearcam Steva Manna. Američan v roce 1994 vytvořil kameru, kterou mohl nosit na brýlích a tedy vysílat, co zrovna vidí.

Jako další se objevil projekt inTouch na Massachusetts Institute of Technology v roce 1998. Scott Brave, Andrew Dahley a Hiroshi Ishii vytvořili technologii simulující interakci se sdíleným fyzickým objektem dvou uživatelů na dálku. Tento objekt tak obohacuje komunikaci o haptické prožitky.

V tomtéž roce také Mark Weiser zkonstruoval fontánu, jejíž tok a výška kopírovaly ceny akciového trhu. Rok 1999 byl průlomový, protože určil směr dalšího vývoje. Poprvé bylo použito slovní spojení Internet of Things, toto označení se připisuje Kevinu Ashtonovi, toho času výkonným ředitelem Auto-ID Center (centrum zabývající se identifikací pomocí rádiové frekvence). Při své prezentaci v Procter & Gamble termín zmínil právě v souvislosti s rádiovou identifikací dodávek firmy.

Pak už se IoT dostalo do komerční sféry, firma LG uvedla na trh lednici připojenou na Internet. Toto zařízení mělo být naprogramováno tak, aby dokázalo zachytit, jaké potraviny se uvnitř nacházejí a případně tedy zjistit, kdy je potřeba některý produkt doplnit. První chytrá lednice také poskytovala informace o teplotě, čerstvosti a výživové hodnotě skladovaných potravin. Tento projekt byl ovšem neúspěšný, a to kvůli vysoké ceně (cca 20 000 dolarů) a nezájmu spotřebitelů.

Jedním z nápadů roku 2002 byl podle New York Times Ambient Orb. Tato koule, vytvořená Davidem Rosem, sloužila k vizualizaci dat stažených z Internetu (například počasí).

V následujících letech se slovní spojení Internet of Things objevilo v mainstreamových médiích jako The Guardian nebo Scientific American. Tím se IoT dostalo do povědomí širší veřejnosti. Roku 2005 vydala Mezinárodní komunikační unie (při OSN) zprávu na toto téma. Další mezinárodní organizací zabývající se vznikající technologií byla Evropská unie se svou konferencí v roce 2008. Tato třídenní akce zahrnovala přednášky a workshopy od zástupců světových firem, jako například Amazon, BMW nebo Siemens.

Důležitou událostí byl také vznik IPSO Alliance (2008), tedy organizace podporující zavedení internetového protokolu (IP) v IoT jako standardní způsob komunikace. Členy této organizace jsou dnes společnosti jako Bosch, Cisco, Intel, Google a Fujitsu.

Rok 2008 je také podle společnosti Cisco rokem zrození IoT, neboť v něm počet zařízení připojených na Internet překročil počet lidí na Zemi. V roce 2011 na jednoho člověka průměrně připadalo 1,84 zařízení.

Pro IoT bylo zásadní i zavedení IPv6 roku 2011, protože s rostoucím počtem připojených zařízení roste i počet používaných adres. Adresování IPv6 umožňuje až 2^{128} zařízení, tedy zhruba $340 \cdot 10^{36}$.

Pak už se IoT rozšiřuje do běžného života, kromě odborníků (IBM, Ericsson) i mezi laickou veřejnost. Kromě běžného spotřebitelského využití (chytré hodinky Fitbit) minipočítače jako Arduino či Raspberry Pi umožnily amatérské vyvíjení IoT.

3 Základní funkce IoT systémů

IoT sytémy musí mít tyto základní funkce: sběr informací, jejich zpracování, odesílání a přijímání. V další části se tedy budu věnovat různým způsobům implementace těchto požadavků.

3.1 Sběr informací

Zařízení sbírají informace pomocí nejrůznějších senzorů. Senzor je zařízení, které je schopné detekovat změny v prostředí a převést tuto informaci na elektrický signál.

Dobrý senzor by měl splňovat tato tři základní kritéria:

1. měl by zachycovat veškeré změny měřené veličiny
2. neměl by být ovlivněn změnami jiných aspektů prostředí
3. neměl by ovlivňovat měřenou vlastnost prostředí

U senzorů také rozlišujeme základní parametry – rozsah a citlivost. Tedy maximální a minimální hodnoty, které je senzor schopen detekovat a nejmenší změna prostředí, kterou senzor zaznamená a která se projeví změnou výstupu senzoru.

Senzory se dají klasifikovat podle různých kritérií, nejběžnějšími rozděleními jsou:

1. aktivní a pasivní
    - aktivní senzory vyžadují ke svému fungování externí zdroj energie, pasivní nikoliv
2. analogové a digitální
    - analogové vysílají spojitý signál, digitální signál diskrétní (může nabývat jen omezeného počtu hodnot)
3. podle metody měření jevu a použitých technologií
    - mechanické, chemické, infračervené záření, radiové vlny atd.

Existuje mnoho druhů senzorů, IoT zařízení obvykle používají kombinaci několika, aby podávala ucelený obraz prostředí. Zde je přehled několika nečastěji používaných senzorů.

3.1.1 Teplotní senzor

Teplotní senzory byly hojně využívány již před nástupem IoT například v lednicích, klimatizaci a podobně. V IoT se používají nejen k samotnému

určení teploty, ale také k detekci pohybu – pohyb člověka či zvířete změní teplotu prostředí. Rozlišujeme různé teplotní senzory podle technologie, jakou používají. Základními jsou termočlánek, pracující na bázi termoelektrického jevu (přeměna rozdílu teplot na elektrické napětí a naopak); termistory a RTD senzory (Resistance Temperature Detectors), které mění hodnotu odporu na základě teplotních změn; integrované obvody využívající vlastnosti polovodičů; pasivní infračervený senzor (PIR) měřící teplo ve formě záření.

3.1.2 Senzor přiblížení (proximity)

Senzor přiblížení snímá přítomnost nebo absenci objektů ve své blízkosti. Své využití nalezl například v obchodním průmyslu, kdy se pomocí něj dá monitorovat, kam se zákazník pohybuje a o jaké zboží má tedy zájem. Dalším známým využitím je kupříkladu detekce překážek při couvání. Mezi obvyklé typy senzorů přiblížení patří indukční senzory na zachycení kovových objektů díky elektromagnetickému poli; kapacitní snímače, které detekují velmi malé objekty, a to kovové i nekovové; fotoelektrické senzory (fotobuňky), ty zaznamenají změnu osvětlení; ultrazvukové senzory, které pomocí odraženého vlnění zjišťují překážky v prostoru.

3.1.3 Tlakový senzor

Tento senzor je často používám již v současnosti (například meteorologie), ale s IoT může najít své využití v mnoha dalších oblastech (tlakové senzory v namáhaných stavbách, v zavlažovacích systémech apod.). Existuje mnoho druhů tlakových senzorů, jedním z nich je například senzor pracující na bázi piezoelektrického jevu (zaznamenání deformace při vyrovnávání tlaku s okolím).

3.1.4 Senzor kvality vody

Tyto senzory mohou měřit hned několik různých vlastností vody, jsou jimi pH, vodivost, odpor, oxidačně-redukční potenciál a obsah konkrétních látek (kyslík, chlor, organická složka). Senzory kvality vody mají široké využití v průmyslu, protože téměř každá výroba potřebuje ke správnému fungování vodu.

3.1.5 Chemický senzor

Do této kategorie lze zahrnout i dříve zmíněné senzory složení vody, obecně ale chemické senzory mohou zjišťovat složení vzduchu nebo i jiných kapalin. Pomocí nich lze včas zjistit znečištění nebo únik nebezpečných látek

do ovzduší. Nejpoužívanějšími senzory jsou senzor oxidu uhličitého a uhelnatého, senzor vodíku, elektrochemický senzor plynu, senzor ozonu, znečištění vzduchu.

3.1.6 Senzor kouře

Jeden z dalších senzorů rozšířených před IoT, s jeho nástupem ale roste i jeho efektivita, díky možnosti okamžitého varování ohrožených osob. Kromě kouře detekují senzory také plyny a oheň. Snímají obvykle opticky, fyzickou detekcí částic nebo kombinací obojího. Optický senzor (fotoelektrický) zkoumá rozptyl světla v místnosti, nelze ho používat v místnostech, kde i za běžných podmínek dochází ke vzniku kouře, par nebo v prašném prostředí. Ionizační kouřový senzor využívá ionizaci malého množství radioaktivního materiálu a je častějším v domácích detektorech kouře.

3.1.7 Infračervený senzor (IR)

Kromě již zmíněného využití při měření teploty se dá infračervené záření využít mnoha dalšími způsoby. IR senzory usnadňují monitorování krevního oběhu a tlaku ve zdravotnictví, vizualizaci generovaného tepla v elektronických zařízeních nebo detekci slepého úhlu při řízení. Dají se také použít v zabezpečovacích systémech nebo při zkoumání historických děl.

3.1.8 Snímač hladiny

Nejtypičtější příklad snímání hladiny můžeme najít v dopravních prostředcích, které mají senzor na snímání hladiny paliva. Tyto senzory se samozřejmě používají i v mnoha dalších odvětvích nakládajících s tekutinami, například při výrobě nápojů nebo ve zdravotnictví. Rozlišujeme dva základní typy senzorů: bodový snímač hladiny, který upozorní uživatele pouze když hladina dosáhne určitého bodu a kontinuální snímač, který zasílá naměřenou hodnotu hladiny nepřetržitě v pravidelných časových intervalech.

3.1.9 Obrazový snímač

Převod optického obrazu na elektronický signál se využívá hlavně ve fotoaparátech, kamerách. V IoT však většinou není použita běžná kamera, ale obrazový snímač vylepšený množstvím dalších funkcí a připojený k jiným zařízením. Příkladem mohou být třeba lékařské zobrazovací metody nebo snímače překážek u autonomních vozidel. Hlavní typy senzorů CCD (zařízení se zdvojeným nábojem) a CMOS (komplementární kovovo-oxidový polovodič) používají odlišné metody zachytávání obrazu, kvalita je ale podobná.

3.1.10 Snímač pohybu

Snímače pohybu jsou používány k detekci fyzického pohybu osob a objektů v určené oblasti. Nejčastěji je můžeme nalézt v různých typech zabezpečovacích systémů, lze se s nimi setkat i jinde, kupříkladu v automatických parkovacích systémech, při automatickém osvětlení, u automatických dveří. Senzory také mohou být schopné rozlišovat různé typy pohybu a tím třeba umožnit uživateli ovládat zařízení na dálku bez jakéhokoliv ovladače. Kromě PIR senzoru již zmíněného jako senzoru na měření teploty existují snímače ultrazvukové nebo mikrovlnné. Mikrovlnné dokáží pokrýt největší plochu, ale jsou citlivé na rušivé vnější vlivy.

3.1.11 Senzor zrychlení (akcelerometr)

Senzor zrychlení měří fyzické zrychlení objektu vůči inerciálním objektům (zejména vůči Zemi). Dá se definovat jako velikost změny rychlosti vůči vztažnému objektu za určitý čas. Akcelerometr by měl kromě samotného zvýšení rychlosti detekovat i vibrace nebo naklonění. Využívá se v letectví, automobilovém průmyslu nebo třeba ve spotřební elektronice (chytré telefony). Z mnoha akcelerometrů používaných v IoT jsou zásadní Hallův snímač zrychlení (využívající Hallova jevu); kapacitní akcelerometr, který je méně náchylný na výkyvy teplot a piezoelektrický akcelerometr, který je z uvedených nejlepší na zaznamenání vibrací a náhlých otřesů.

3.1.12 Gyroskop

Gyroskop je určen k měření úhlové rychlosti, tedy rychlosti rotace kolem nějaké osy. Tento senzor se používá k navigaci a k určení orientace objektu. Gyroskop se využívá ve spotřební elektronice, v robotice, v navigačních systémech. Gyroskop je téměř vždy spojen i s akcelerometrem, protože spojením informací z obou těchto senzorů lze získat mnohem přesnější obraz toho, co se s objektem děje. Jako hlavní typy gyroskopů můžeme jmenovat rotační gyroskop, CVG (Coriolisův vibrační gyroskop), optický gyroskop, MEMS (mikro elektro mechanický) gyroskop.

3.1.13 Senzor vlhkosti

Senzor vlhkosti měří množství vody rozptýlené ve vzduchu. Své využití nalezne v meteorologii nebo v továrnách, kde vlhkost vzduchu ovlivňuje kvalitu výrobku. Podle způsobu měření se dají rozlišit senzory kapacitní, odporové a termální.

3.1.14 Optický senzor

Účelem optického senzoru je monitorovat množství světla v prostředí například při těžebních pracích. Základními typy optických senzorů jsou fotodetektor, optické vlákno nebo pyrometr.

3.2 Komunikace (odesílání a příjem informací)

Komunikační protokoly IoT zařízení se většinou drží rozložení TCP/IP, obsahují tedy vrstvu síťového rozhraní (fyzická), síťovou, transportní a aplikační vrstvu. Volba konkrétní technologie pro jednotlivé vrstvy závisí na účelu IoT systému. Při výběru je nutné zvážit požadavky na faktory jako jsou dosah přenosu, šířka pásma (ovlivňuje maximální množství dat posílaných současně), spotřeba energie, interoperabilita (schopnost různých systémů nebo zařízení vzájemně spolupracovat), zabezpečení.

3.2.1 Technologie vrstvy síťového rozhraní

Wifi Wifi je v současné době hojně používána mnohými zařízeními, pravděpodobně bude v budoucnu nahrazena specializovanými technologiemi. Kromě výhod jako je přenos velkého množství dat a dalekému dosahu nese i nevýhody v podobě velké spotřeby energie.

Ethernet Tato technologie se dá využít pro některé specifické případy, kdy systém nevyžaduje bezdrátovou komunikaci. Pro většinu IoT systémů však Ethernetové připojení není optimální.

Celulární sítě Některé IoT systémy využívají na bezdrátovou dalekodosahovou komunikaci již existujících celulárních sítí. Jsou jimi 2G, které je na ústupu, dále CDMA, 3G, 4G a v budoucnu pravděpodobně 5G.

LPWAN (Low Power Wide Area Network) Jak napovídá název, LPWAN technologie jsou určené pro bezdrátovou komunikaci na velké rozloze při spotřebování malého množství energie. Do této kategorie spadá například SigFox, Lora, Haystack nebo celulární sítě využívající LTE-M či NB-IoT (Narrowband IoT).

Bluetooth Low Energy (BLE) BLE je verzí klasického Bluetooth, spotřebovává však méně energie. Používá stejnou rádiovou frekvenci (2,4 GHz)

jako jeho předchůdce. BLE je používáno na krátkou vzdálenost (do 100 metrů), často s jedním centrálním zařízením kontrolujícím ostatním (hvězdicová topologie).

ZigBee ZigBee se od BLE liší svou smíšenou topologií (mesh), díky které může vysílat na delší vzdálenosti. Používá stejnou frekvenci 2,4 GHz a je určeno především na IoT v domácnosti (kontrola osvětlení apod.).

Z-Wave Z-Wave je ve svém fungování a užití velmi podobné ZigBee, používá rádiovou frekvenci 800 až 900 MHz.

NFC (Near Field Communication) NFC je určené na opravdu malou vzdálenost (4 cm). Používá se typicky pro bezkontaktní platby.

RFID (Radio Frequency Identification) RFID slouží pro identifikaci zařízení pomocí tzv. tagů. Tyto tagy mohou být aktivní, pasivní nebo asistovaně pasivní. Aktivní tagy svůj identifikátor neustále vysílají, z pasivních tuto informaci musí přečíst čtečka a asistovaně pasivní se stanou aktivními v přítomnosti čtečky. RFID má dosah do jednoho metru.

3.2.2 Technologie síťové vrstvy

IPv6 S nárůstem počtu připojených zařízení se zvýšil počet požadovaných adres, proto byl přechod z IPv4 na IPv6 nevyhnutelný. IPv6 nabízí 2^{128} adres, tedy zhruba $3,4 \cdot 10^{38}$, což už je pro potřeby IoT dostačující.

6LoWPAN (IPv6 Low Power Wireless Personal Network) 6LoWPAN umožňuje použití IPv6 na sítě dle IEEE 802.15.4 (norma definující rádiovou komunikaci sítí). 6LoWPAN používá také Thread, což je technologie pro domácí automatizaci vyvinutá ve spolupráci 50 firem.

RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) Tato technologie se používá na sítě, které jsou nějakým způsobem omezené, kupříkladu sítě s vysokou ztrátovostí packetů nebo sítě, kde všechna zařízení nejsou neustále dosažitelná. RPL odděluje zpracování a posílání paketů od snahy optimalizovat jejich směrování (snížení latence, spotřeby energie).

3.2.3 Technologie transportní vrstvy

TCP TCP je spojovaný protokol (data přichází ve správném pořadí) a používá se u aplikací, které vyžadují vysokou spolehlivost přenosu dat, ale doba přenosu není až tak důležitým faktorem. Při přenosu si TCP ukládá byty do vyrovnávací paměti (buffer), aby pak posílal celé pakety.

UDP UDP je rychlejší, ale méně spolehlivý. Proto je vhodný pro aplikace vyžadující okamžitý přenos dat. Přenášené packety nejsou seřazené, je-li vyžadováno jejich uspořádání, musí se tak stát v aplikační vrstvě.

3.2.4 Technologie aplikační vrstvy

HTTP, HTTPS (Hypertext Transfer Protocol Secure) Tyto protokoly jsou v IoT často využívány, kvůli požadavkům na nízkou cenu mnoho zařízení používá nešifrovaný HTTP, čímž může ohrožovat integritu dat, s kterými tato zařízení nakládají. Na rozdíl od toho, HTTPS umožňuje autentifikaci a zabraňuje porušení přenášených dat.

CoAP (Constrained Application Protocol) CoAP je založený na podobném principu jako HTTP, používá REST (Representational State Transfer) architekturu. CoAP je specializovaným protokolem pro IoT.

MQTT (Message Queue Telemetry Transport) MQTT předává informace pomocí centrálního bodu – brokeru, který rozlišuje zprávy podle témat. Ostatní zařízení na něm mohou zprávy buď publikovat (publish) nebo je odebírat (subscribe).

AMQP (Advanced Message Queuing Protocol) Jedná se o otevřený (veřejně dostupný, lze ho používat i s produkty jiných firem) protokol zaměřený na tzv. message-oriented middleware (MOM), tedy technologii posílání zpráv mezi distribuovanými systémy.

XMPP (Extensible Messaging and Presence Protocol) XMPP je dalším otevřeným MOM protokolem, původně byl určen pro komunikaci lidí v reálném čase (instant messaging). Tento protokol založený na XML (Extensible Markup Language) byl později upraven na komunikaci M2M (stroj se strojem).

3.3 Zpracování informací

S velkým množstvím zařízení roste také rozsah dat, která je potřeba zpracovávat. Informace z IoT systémů jsou typickým příkladem tzv. Big Data. Big Data (velká data) jsou charakterizována třemi V.
Jsou to:

- volume (objem) – množství dat
- variety (rozmanitost) – kombinace více druhů dat
- velocity (rychlost) – rychlost přílivu nových dat

Někdy se k těmto třem základním charakteristikám přidávají ještě value (hodnota) a veracity (pravdivost). Při práci s daty můžeme rozlišovat dva přístupy, a to batch processing (dávkové zpracování) a stream processing (zpracování proudu dat). Batch processing zpracovává data nashromážděná za nějakou dobu, stream processing neustále odebírá proud dat.

K analýze takového množství dat je zapotřebí velké výpočetní síly, pro uživatele se nevyplatí pracovat se získanými daty na vlastních zařízeních. Proto se v IoT používá cloud nebo fog computing.

3.3.1 Cloud computing

Cloud funguje na principu pronájmu úložiště či výpočetní síly uživatelem. Můžeme rozlišovat tři typy služeb: IaaS (Infrastructure as a Service), kdy uživatel využívá celou infrastrukturu a zařizuje si tedy i její údržbu; při PaaS (Platform as a Service) je uživateli již poskytnuta základní infrastruktura, konkrétní implementace však závisí na něm a SaaS (Software as s Service) nabízí uživateli přístup přes webové rozhraní.

Cloud přináší do IoT významnou úsporu – uživatel nemusí investovat do vlastního hardwaru u svých zařízení a může si pronajmout levnější cloud. Většina poskytovatelů cloudu také používá systém pay-as-you-go, tedy uživatel zaplatí jen za výpočetní sílu, kterou skutečně využije. Je tak vhodný pro systémy, kde množství zpracovávaných dat není konstantní.

3.3.2 Fog computing (Edge computing)

Název fog computingu vychází z názvu cloudu: cloud, tedy oblak je posunut blíže k zemi a tím se z něj stává mlha (fog). V praxi to znamená, že se část dat nepřenáší až do cloudu, ale je zpracovávána blíže ke zdroji. Fog computing probíhá na tzv. edge zařízeních, tedy na zařízeních umožňujících vstup do sítě. Tím se podstatně zrychlí analýza dat, fog computing je tedy

vhodný pro systémy, kde je nejvyšší prioritou rychlost zpracování. Fog computing se většinou používá v kombinaci s cloudem, fog rychle zpracovává jednodušší data, cloud dlouhodobější a složitější.

4 Využití IoT

IoT v budoucnosti zasáhne celou řadu odvětví, například průmysl, zdravotnictví, marketing. V současnosti je však využíváno zejména ve čtyřech níže popsaných oblastech.

4.1 Chytré domácnosti

Běžnému uživateli nejbližší využití IoT jsou právě chytré domácnosti. Konkrétně se IoT může používat třeba na ovládání osvětlení, garážových dveří nebo třeba kuchyňských spotřebičů. Uživatel by mohl všechna tato zařízení ovládat pomocí svého chytrého telefonu, pomocí hlasového asistenta Alexa či Google Home nebo se IoT síť naučí jeho návyky (machine learning) a bude jim přizpůsobovat prostředí. Typickým příkladem tak může být domácnost, kde kávovar začne vařit kávu ještě před nastaveným budíkem, senzor v garáži zaregistruje nastupující osobu do auta a otevře garážová vrata. Při nepřítomnosti majitele je dům chráněn zabezpečovacím systémem, který pošle upozornění v případě pokusu o vniknutí, nebo rovnou zavolá policii. IoT tak může nejen zajistit uživatelům vetší pohodlí, úsporu energií a lepší zabezpečení domácnosti.

4.2 Zemědělství

Pro zemědělství může IoT přinést opravdu významné benefity, monitoring rozsáhlých ploch, který je jinak téměř nesplnitelným úkolem usnadní velké množství distribuovaných zařízení komunikujících s centrální jednotkou. Senzory mohou zasílat informace o vlhkosti, teplotě a podle toho se určí optimální míra zavlažování. Pokročilejším využitím by byly samořídicí zemědělské stroje, pracující buď podle příkazů uživatele nebo vlastních informací ze senzorů. U IoT v zemědělství je potřeba vzít v úvahu některé omezující faktory, jako je třeba způsob přenosu dat (přenos na velkou vzdálenost s překážkami), dodávání energie nebo aktualizace firmwaru. Kvůli rozsáhlosti zemědělských ploch musí být umožněno aktualizovat zařízení i bez fyzického přístupu k nim, takzvaný over-the-air update

4.3 Chytrá města

IoT v chytrých městech může zahrnovat kontrolu osvětlení, spotřeby vody, produkce škodlivých látek nebo monitoring volných parkovacích míst. Prvky IoT se do svého fungování snaží zařadit například Barcelona. Ve městě fungují chytré semafory, které optimalizují provoz na vytížených trasách a zvýhodňují vozidla záchranné služby. Barcelona také monitoruje zavlažení rostlin v městských parcích a tím šetří až 25 % svých zásob vody.

V České republice se v tomto oboru nejdál dostal Zlín. Fungují zde chytré semafory, které upřednostňují vozidla MHD, čímž se jejich průjezd městem zrychlil až o 20 %. Chytrým městem se chce stát i Praha, která pracuje na několik projektech zahrnujících třeba inteligentní řízení svozu odpadu za využití senzorů v kontejnerech.

4.4 Maloobchod

Maloobchodní využití se dá nejlépe ilustrovat na příkladu obchodu Amazon Go. Při příchodu zákazník naskenuje QR kód, který má v mobilní aplikaci. V celém obchodě jsou senzory, které detekují, kdy bylo zboží z regálu odstraněno. Zákazníkem vybrané zboží se mu započítá do jeho virtuálního nákupního košíku a po opuštění odchodu se zaplatí z jeho Amazon účtu. V současnosti existuje 10 Amazon Go obchodů ve třech amerických městech.

5 Bezpečnost

S rostoucím počtem zařízení se zvětšuje i pravděpodobnost, že se někomu podaří proniknout do sítě. Některá zařízení v IoT jsou velmi jednoduchá a levná, proto se při jejich výrobě neklade takový důraz na zabezpečení. Protože jsou však zařízení propojená, může se hacker přes jedno zařízení dostat k informacím na ostatních. Vzhledem k tomu, že některá data sbíraná IoT systémy mohou být citlivá (kamerové záznamy, informace o zdravotním stavu), jedná se o závažný problém. Kromě získání citlivých dat mohou být také zařízení zneužita na DDoS (Distributed Denial of Service) útok, jako se tomu stalo v případě útoku na Dyn, poskytovatele služby DNS (Domain Name Server), v roce 2016. Hackeři využili desítky milionů zařízení připojených na Internet, a to včetně tiskáren, kamer apod.
Při budování IoT je třeba dbát několika zásad, které zajistí bezpečnost systému.

- Zabezpečení hardwaru

  IoT zařízení často nejsou v dosahu nebo pod neustálým dohledem, proto je zapotřebí vytvářet takový hardware, který nelze zneužít ani při fyzickém přístupu nebo u kterého bude cizí zásah okamžitě rozpoznatelný.

- Identifikace zařízení

  Každé zařízení musí být jednoznačně identifikovatelné a tento identifikátor nesmí být možné falšovat.

- Zabezpečení sítě

  V síti je nutné používat antimalware, firewall a blokovat neautorizovaný přístup do ní.

- Šifrování

  Všechna posílaná nebo uchovávaná data musí být šifrována pomocí algoritmů, které nejdou prolomit hrubou silou.

- Autentizace

  Při přístupu do systému bude po uživateli vyžadována autentizace, buď ve formě silného hesla nebo biometrie. Uživatel si při zakoupení zařízení musí změnit heslo přednastavené výrobcem.

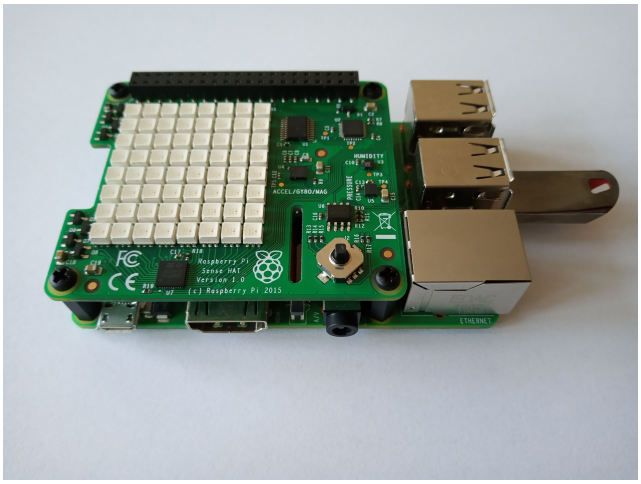
- Managament aktualizací

  Zařízení musí být možno neustále aktualizovat a spravovat případné objevené zranitelnosti.

6 Demonstrace na Raspberry Pi

6.1 Hardware

Raspberry Pi je malý počítač určený k hobby projektům. V ukázce je použito Raspberry Pi 3, Model B+ s nástavcem Sense HAT. Raspberry Pi 3 má 1,2 GHz 64bitový čtyřjádrový procesor ARM Cortex-A53. Kromě toho má několik portů (USB, HDMI), slot na SD kartu a napájení přes micro USB. Na základní desku se dá připojit nástavec SenseHat s LED displejem 8x8 a několika senzory, z nichž jsou v projektu používány senzor vlhkosti a teploty.



Obrázek 1: Raspberry Pi s nástavcem Sense Hat

6.2 Software

Pro Raspberry Pi je dostupná řada operačních systémů (LibreElec, Windows 10 IoT Core), nejrozšířenějším a i při vytváření projektu použitým je linuxová distribuce Raspbian.

Projekt je simulací meteostanice, která měří každou hodinu teplotu a vlhkost okolí, za 24 hodin vykreslí graf a pošle jej uživateli na e-mail. Byl použit programovací jazyk Python 3.

6.2.1 Měření teploty a vlhkosti

Soubor `collect.py`

K měření těchto faktorů se využívají senzory z nástavce Sense HAT, je tedy zapotřebí importovat balíček `sense_hat`. Dalšími balíčky jsou `time` (funkce `sleep()`) a `os`. Program obsahuje nekonečnou smyčku, ve které dojde ke změření veličin a jejich zapsání do textového souboru. Jednorázové změření teploty a její zápis do souboru by vypadal takto:

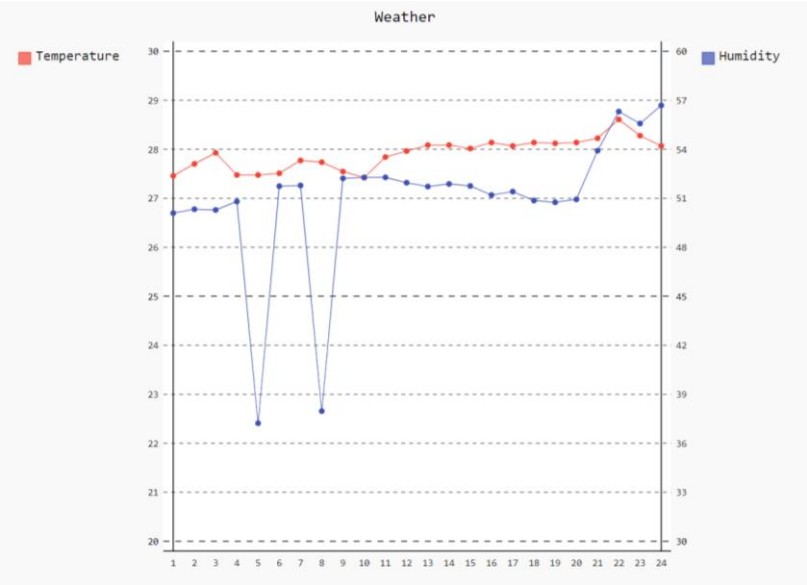
```
from sense_hat import SenseHat
sense = SenseHat()
file_temp = open("temp_log.txt","a")
file_temp.truncate(0)
file_temp.write(str(sense.get_temperature())+"\n")
file_temp.close()
```

Dále jsou v programu volány funkce na vykreslení grafu a odeslání e-mailu.

6.2.2 Vykreslení grafu

Soubor `draw_graph.py`, ukázkový graf `graph.svg`

Zde je použit balíček pygal, konkrétně spojnicový graf Line. Funkce `new_graph()` vytvoří graf s dvěma vertikálními osami a nastaví jejich rozmezí. Funkce `add()` načte hodnoty z textového souboru do proměnné a následně tyto hodnoty přidá do grafu, který pak funkce `draw()` vykreslí do souboru `graph.svg`.



Obrázek 2: Ukázka grafu

6.2.3 Zasílání e-mailu

Soubor `mail_sender.py`

Pro zasílání e-mailu jsou použity balíčky `email`, `smtplib`, `ssl` a balíček `datetime` pro získání aktuálního data. Zasílaný e-mail je sestavený podle MIME (Multipurpose Internet Mail Extensions) neboli víceúčelová rozšíření internetové pošty. Tento standard umožňuje kromě přenášení prostého textu také přenos příloh, lze tedy díky němu poslat vykreslený graf. MIME také specifikuje rozdělení e-mailu na části - odesílatel, příjemce, atd. (viz níže).

```
message = MIMEMultipart()
message["From"] = "Raspberry Pi weather station"
message["To"] = "You"
message["Subject"] = "Weather summary"

body = "Hello,\n this is your yesterday\'s weather summary."
message.attach(MIMEText(body, "plain"))
```

V případě, kdy je odesílatelem gmail, jak je tomu v ukázce, je nutné povolit v nastavení e-mailu odesílání pošty méně zabezpečených aplikací. V případě použití jiného e-mailu je potřeba změnit druhý argument funkce `SMTP_SSL()`, tedy číslo portu.

6.2.4 Spuštění při startu

Pro automatické spuštění meteostanice při startu zařízení stačí v `etc/rc.local`, zavolat program `collect.py` jako superuživatel:

```
sudo python3 /home/pi/Documents/weather_station/collect.py &
```

6.3 Závěr

Projekt demonstruje jedno z mnoha použití Raspberry Pi pro Internet věcí. Ukázka je pouze zjednodušujícím příkladem, jak by takové zařízení mohlo fungovat. Pro použití v reálném životě by bylo nutné upravit snímání teploty, aby nebylo ovlivněno zahříváním procesoru a zabezpečení (management hesel apod.). Raspberry Pi je však určeno především k hobby projektům a využití např. v průmyslu se u něj nepředpokládá.

Zdroje

[1] BUYYA, Rajkumar a Amir Vahid DASTJERDI, ed. Internet of Things Principles and Paradigms [online]. 2016 [cit. 2019-03-24]. ISBN 978-0-12-805395-9.

[2] LEVEREGE. An Introduction to the Internet of Things [online]. 2018 [cit. 2019-03-24].

[3] Internet of Things (IoT) History. Postscapes [online]. [cit. 2019-03-22]. Dostupné z: https://www.postscapes.com/internet-of-things-history/

[4] Internet věcí. Wikipedia [online]. 2019 [cit. 2019-03-22]. Dostupné z: https://cs.wikipedia.org/wiki/Internet_v%C4%9Bc%C3%AD

[5] Internet of Things. Wikipedia [online]. 2019 [cit. 2019-03-22]. Dostupné z: https://en.wikipedia.org/wiki/Internet_of_things?oldid=808022410

[6] How a Coke Machine and the Industrial Internet of Things Can Give Birth to a Planetary Computer. Engineers Rule [online]. 2016 [cit. 2019-03-22]. Dostupné z: https://www.engineersrule.com/how-a-coke-machine-and-the-industrial-internet-of-things-can-give-birth-to-a-planetary-computer/

[7] InTouch. Tangible Media Group [online]. [cit. 2019-03-22]. Dostupné z: http://tangible.media.mit.edu/project/intouch/

[8] The History of IoT. Bill McCabe Iot Recruiter [online]. 2015 [cit. 2019-03-22]. Dostupné z: http://internetofthingsrecruiting.com/the-history-of-iot/

[9] A complete history of internet-connected fridges. Buisness Insider [online]. 2016 [cit. 2019-03-22]. Dostupné z: https://www.businessinsider.com/the-complete-history-of-internet-fridges-and-connected-refrigerators-2016-1#2007-whirlpool-launches-yet-another-internet-fridge-with-a-special-docking-port-for-your-jabil-6

[10] LG Internet Refridgerator. New Atlas - New Technology & Science News [online]. 2004 [cit. 2019-03-22]. Dostupné z: https://newatlas.com/go/1132/

[11] Introduction to IoT Sensors. Dzone [online]. 2018 [cit. 2019-03-22]. Dostupné z: https://dzone.com/articles/introduction-to-iot-sensors

[12] Odporové teplotní snímače na flexibilním substrátu [online]. [cit. 2019-03-22]. Dostupné z: https://dspace5.zcu.cz/bitstream/11025/27800/1/BP_Michal_Kopejska.pdf. Bakalářská práce.

[13] MEMS 2.0: IoT Pressure Sensors. IoT For All [online]. 2018 [cit. 2019-03-22]. Dostupné z: https://www.iotforall.com/mems-2-iot-pressure-sensors/

[14] Top 15 Sensor Types Being Used in IoT. IoT For All [online]. 2018 [cit. 2019-03-22]. Dostupné z: https://www.finoit.com/blog/top-15-sensor-types-used-iot/

[15] Humidity Sensor: Basics, Usage, Parameters and Applications. Electronics For You [online]. 2018 [cit. 2019-03-22]. Dostupné z: https://electronicsforu.com/resources/electronics-components/humidity-sensor-basic-usage-parameter

[16] SZCZOTKA, Roman. GYROSKOP - Senzor polohy [online]. 2004 [cit. 2019-03-22]. Dostupné z: http://www.umel.feec.vutbr.cz/bmms/.%5Cprojekty_2004%5CSzczotka%5Cindex.htm

[17] Gyroscope. Sensorwiki [online]. [cit. 2019-03-22]. Dostupné z: https://sensorwiki.org/sensors/gyroscope

[18] TRIPATHI, Sauratbh. A Quick Guide to Sensors Used in IoT Devices And Their Applications. IoTLeague [online]. 2016 [cit. 2019-03-22]. Dostupné z: http://www.iotleague.com/a-quick-guide-to-sensors-used-in-iot-devices-and-their-applications/

[19] Senzory v mobilních telefonech od A do Z. Beryko [online]. [cit. 2019-03-22]. Dostupné z: https://www.beryko.cz/blog/recenze/senzory-v-mobilnich-telefonech-od-a-do-z.html

[20] AGRAWAL, Tarun. Know about Different Types of Sensors with their Applications. Edgefx [online]. [cit. 2019-03-22]. Dostupné z: https://www.edgefx.in/different-types-of-sensors-with-applications/

[21] GERBER, Anna. Connecting all the things in the Internet of Things. IBM Developer [online]. 2017 [cit. 2019-03-22]. Dostupné z:

https://developer.ibm.com/articles/iot-lp101-connectivity-network-protocols/

[22] Z-Wave. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-03-23]. Dostupné z: https://en.wikipedia.org/wiki/Z-Wave

[23] Near field communication. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-03-23]. Dostupné z: https://en.wikipedia.org/wiki/Near-field_communication

[24] TCP vs. UDP. Diffen [online]. [cit. 2019-03-22]. Dostupné z: https://www.diffen.com/difference/TCP_vs_UDP

[25] PETERKA, Jiří. TCP a UDP. Diffen [online]. 1999 [cit. 2019-03-22]. Dostupné z: http://www.earchiv.cz/anovinky/ai1864.php3

[26] IEEE_802.15.4. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-03-23]. Dostupné z: https://en.wikipedia.org/wiki/IEEE_802.15.4

[27] 6LoWPAN. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2019-03-23]. Dostupné z: https://en.wikipedia.org/wiki/6LoWPAN

[28] Thread. Thread [online]. [cit. 2019-03-22]. Dostupné z: https://www.threadgroup.org/BUILT-FOR-IOT/Home

[29] ALBUSCHAT, Daniel. Where is HTTPS for IoT? (Update). Dev [online]. 2018 [cit. 2019-03-22]. Dostupné z: https://dev.to/danielkun/where-is-https-for-iot-49ao

[30] MALÝ, Martin. Protokol MQTT: komunikační standard pro IoT. Root [online]. 2016 [cit. 2019-03-22]. Dostupné z: https://www.root.cz/clanky/protokol-mqtt-komunikacni-standard-pro-iot/

[31] Message oriented middleware. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2019-03-23]. Dostupné z: https://en.wikipedia.org/wiki/Message-oriented_middleware

[32] Edge computing. SearchDataCenter [online]. [cit. 2019-03-22]. Dostupné z: https://searchdatacenter.techtarget.com/definition/edge-computing

[33] KŘIŽANOVSKÝ, Pavel. Fog Computing aneb Rozhodování blíže zdroji. SystemOnLine [online]. [cit. 2019-03-22]. Dostupné z: http://m.systemonline.cz/clanky/fog-computing-aneb-rozhodovani-blize-zdroji.htm

[34] INTELIGENTNÍ ŘÍZENÍ SVOZU ODPADU. Smart Prague [online]. 2017 [cit. 2019-03-22]. Dostupné z: https://smartprague.eu/projekty/inteligentni-rizeni-svozu-odpadu

[35] Chytré město. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2019-03-23]. Dostupné z: https://cs.wikipedia.org/wiki/Chytr%C3%A9_m%C4%9Bsto

[36] Amazon Go. Amazon [online]. [cit. 2019-03-22]. Dostupné z: https://www.amazon.com/b?node=16008589011

[37] SEKAR, Atavind. Top Uses of IoT. Analytics Training [online]. 2018 [cit. 2019-03-22]. Dostupné z: https://analyticstraining.com/top-uses-of-iot/

[38] GREENSTEIN, Bret. IoT devices used in DDoS attacks. IBM [online]. 2016 [cit. 2019-03-22]. Dostupné z: https://www.ibm.com/blogs/internet-of-things/ddos-iot-platform-security/

[39] ROUSE, Margaret. IoT security (internet of things security). IoT Agenda [online]. [cit. 2019-03-22]. Dostupné z: https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security

[40] Multipurpose Internet Mail Extensions. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2019-03-23]. Dostupné z: https://cs.wikipedia.org/wiki/Multipurpose_Internet_Mail_Extensions